

A Spectrum of Type Soundness and Performance

Supplementary Material

Ben Greenman
 PLT @ Northeastern University
 benjaminlgreenman@gmail.com

Matthias Felleisen
 PLT @ Northeastern University

CONTENTS

Contents	1	E.6.3 Forgetful Lemmas	105
A Benchmark Descriptions	2	E.7 Embeddings Summary	125
B Performance vs. Number of Typed Modules	3	E.8 Simulation Lemmas	126
C Implementing Tagged Racket	9	E.8.1 Definitions	126
C.1 Generating Type-Constructor Contracts	9	E.8.2 Theorems	128
C.2 Defending Typed Code	9	E.8.3 Lemmas	128
C.3 Diff vs. Racket v6.10.1	9		
D Existing Systems	10		
D.1 Thorn	11		
D.2 StrongScript	12		
D.3 Dart 2	13		
D.4 Pyret	14		
D.5 SafeTS	15		
D.6 Nom	16		
E Models	17		
E.1 Preliminaries	17		
E.2 (H) Higher-Order Embedding	18		
E.2.1 Higher-Order Definitions	18		
E.2.2 Higher-Order Theorems	20		
E.2.3 Higher-Order Lemmas	21		
E.3 (E) Erasure Embedding	43		
E.3.1 Erasure Definitions	43		
E.3.2 Erasure Theorems	45		
E.3.3 Erasure Lemmas	46		
E.4 (1) First-Order Embedding	56		
E.4.1 First-Order Definitions	56		
E.4.2 First-Order Theorems	59		
E.4.3 First-Order Lemmas	60		
E.5 (HC) Co-Natural Embedding	91		
E.5.1 Co-Natural Definitions	91		
E.5.2 Co-Natural Theorems	93		
E.5.3 Co-Natural Lemmas	94		
E.6 (HF) Forgetful Embedding	101		
E.6.1 Forgetful Definitions	101		
E.6.2 Forgetful Theorems	104		

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

NU-CCIS-2018-002, 2018, Northeastern University

© 2018 Copyright held by the owner/author(s).

Benchmark	Untyped LOC	Annotation LOC	# Modules
sieve	35	17 (49%)	2
fsm	182	56 (31%)	4
morsecode	159	38 (24%)	4
zombie	302	27 (9%)	4
jpeg	1432	165 (12%)	5
suffixtree	537	129 (24%)	6
kcfa	229	53 (23%)	7
snake	160	51 (32%)	8
tetris	246	107 (43%)	9
synth	835	139 (17%)	10

Fig. 1. Benchmark Size

A Benchmark Descriptions

sieve from Ben Greenman

Computes prime numbers using the sieve of Eratosthenes.

fsm from Linh Chi Nguyen

Simulates the interactions of economic agents modeled as finite-state automata.

morsecode from John B. Clements & Neil Van Dyke

Computes Levenshtein distances and morse code translations for a fixed sequence of pairs of words.

zombie from David Van Horn

Implements a game where players avoid enemies. The benchmark runs a fixed sequence of moves (representing user input).

jpeg from Andy Wingo

Parses a bytestream of JPEG data to an internal representation, then serializes the result.

suffixtree from Danny Yoo

Computes longest common subsequences between strings.

kcfa from Matt Might

Performs 1-CFA on a lambda calculus equation built from Church numerals.

snake from David Van Horn

Implements the Snake game; the benchmark replays a fixed sequence of moves.

tetris from David Van Horn

Replays a pre-recorded game of Tetris.

synth from Vincent St. Amour & Neil Toronto

Converts a description of notes and drum beats to WAV format.

For additional details about the benchmarks, their source code, and links to more (object-oriented) benchmarks, see: docs.racket-lang.org/gtp-benchmarks/index.html

B Performance vs. Number of Typed Modules

Figures 2, 3, 4, 5, and 6 plot every running time in the dataset. Each point represents one measurement; specifically, a point at position (X, Y) reports one running time of Y milliseconds for one configuration with X “typed units” — in this paper, one typed unit is one typed module. There are eight such points for each configuration. To make these points easier to see, the eight points for one configuration are evenly spaced along the x -axis within a bucket (delimited by solid vertical lines). The left-most point plots the running time of the first trial, the second-from-left point corresponds to the second trial, and so on.

The figures support three broad conclusions. First, the orange points for TR-1 are often lower (i.e., show better performance) than the points for TR-H. Second, the performance of TR-1 tends to degrade linearly as the number of typed modules increases. This slowdown tapers off at the right-most end because the implementation skips the codomain-check for calls to statically-typed identifiers. Third, the performance of TR-H has a steep umbrella shape. The worst performance is in the middle, but improves significantly as the number of typed modules approaches the maximum.

221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275

276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330

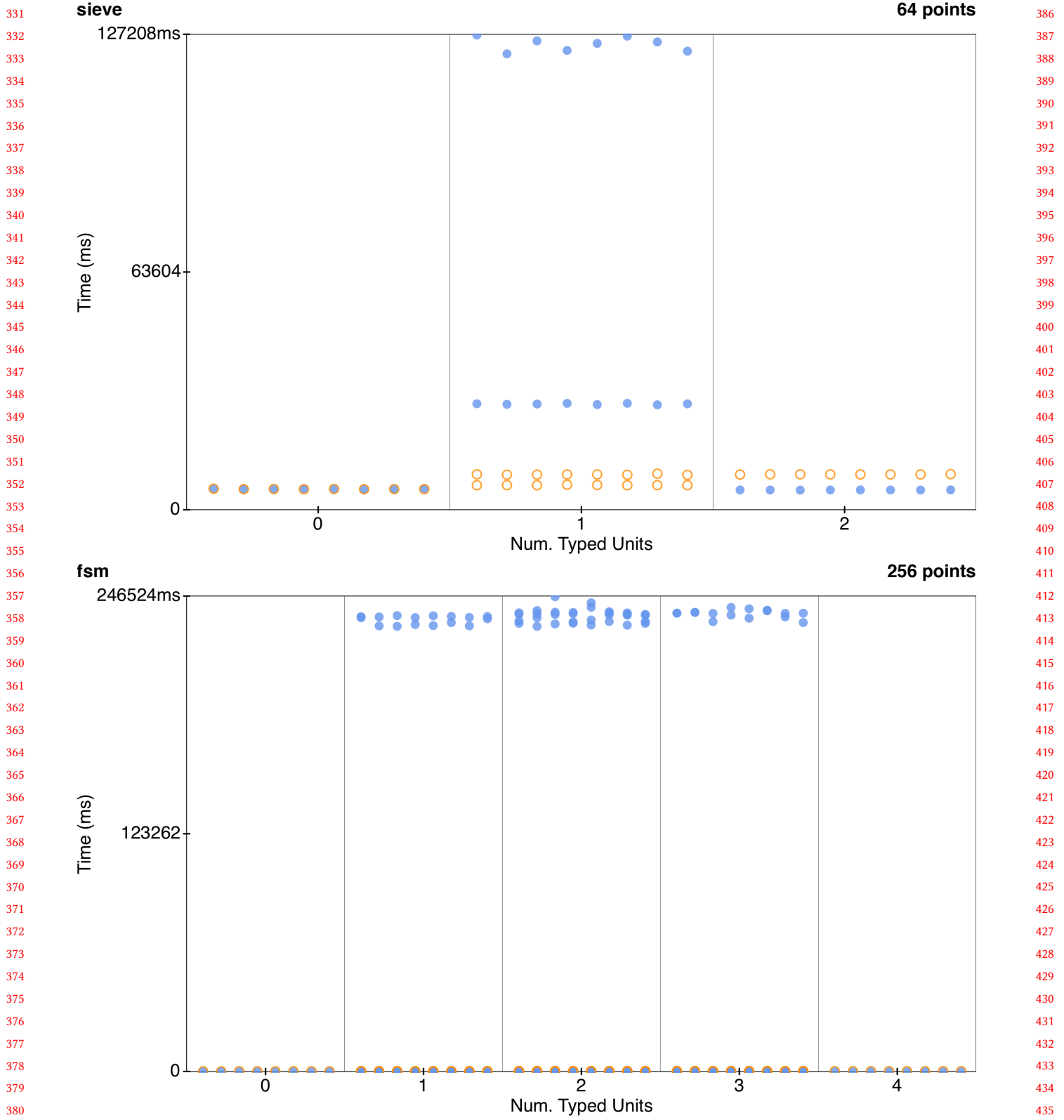


Fig. 2. Running time of TR-H configurations (blue \blacksquare) and TR-1 configurations (orange \square), part 1/5

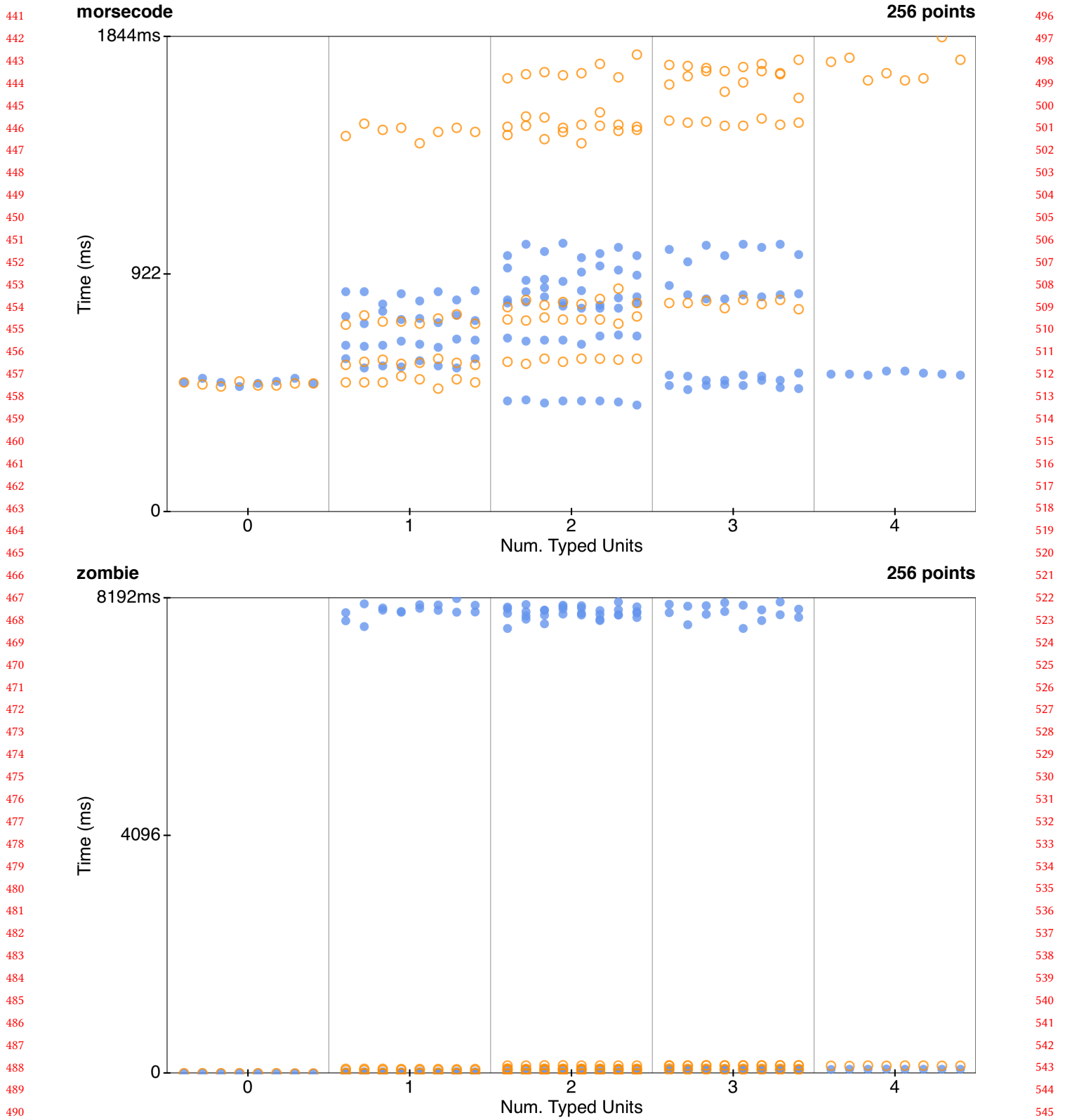


Fig. 3. Running time of TR-H configurations (blue \blacksquare) and TR-1 configurations (orange \circ), part 2/5

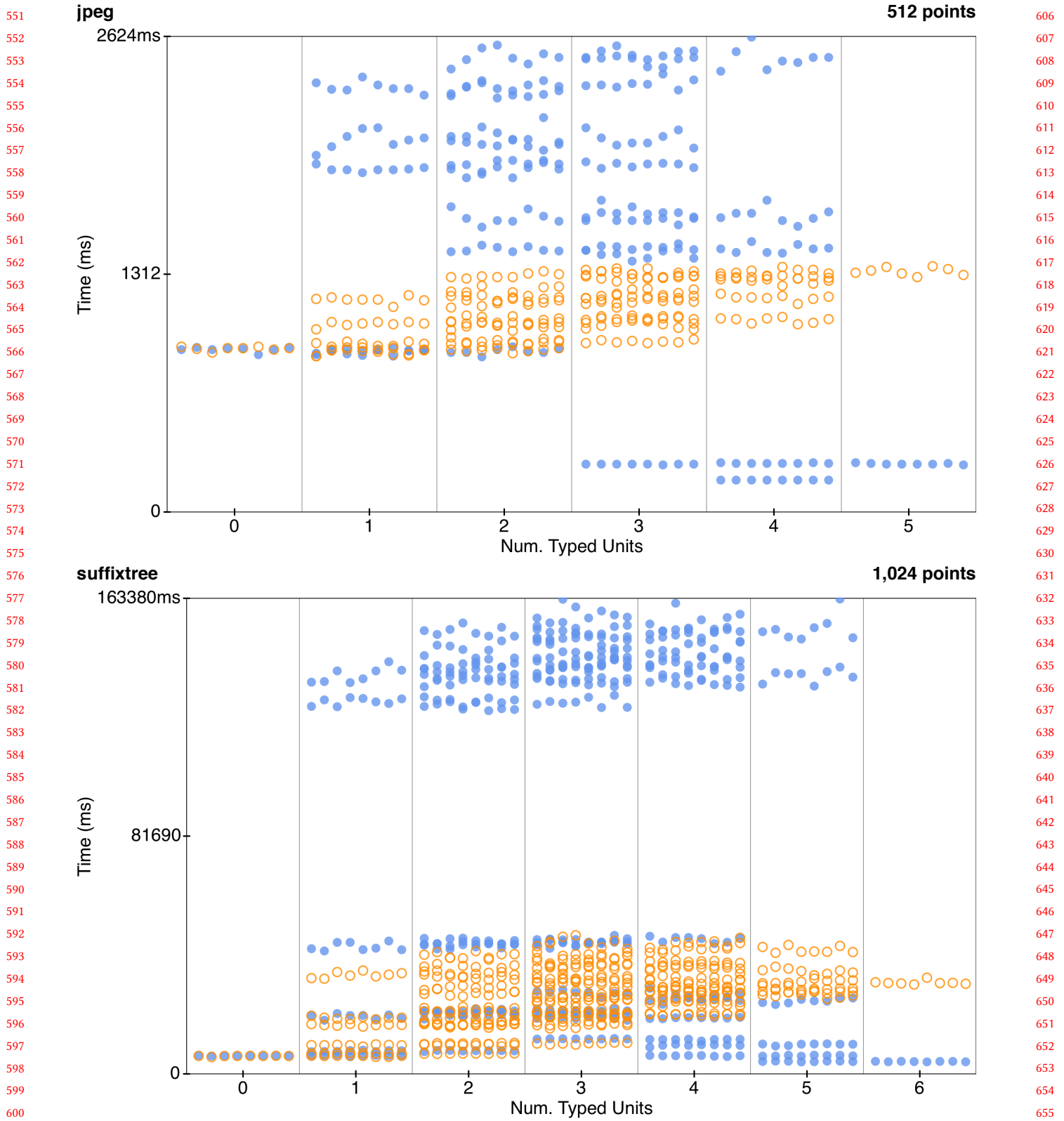


Fig. 4. Running time of TR-H configurations (blue ) and TR-1 configurations (orange ) , part 3/5

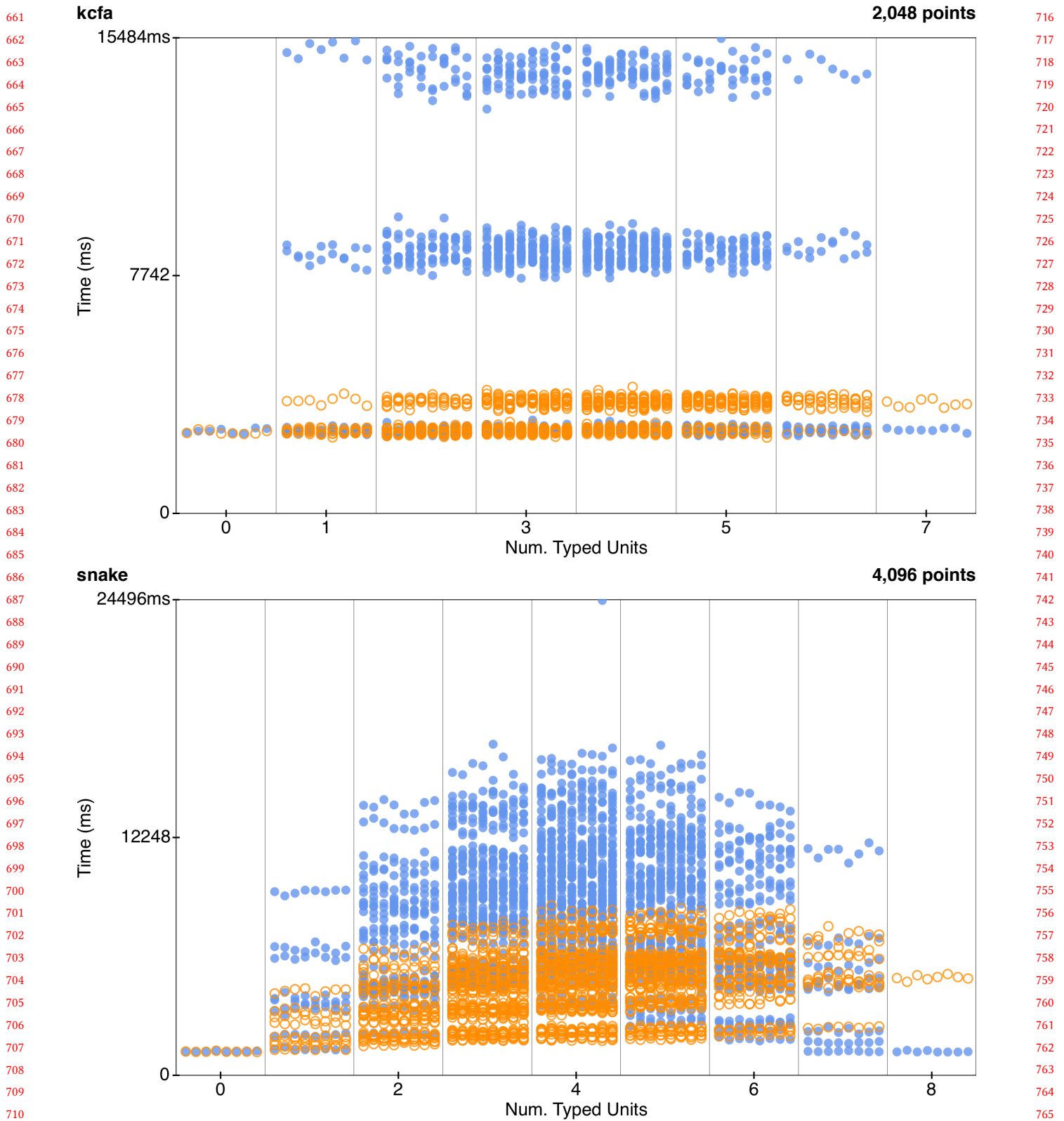


Fig. 5. Running time of TR-H configurations (blue \bullet) and TR-1 configurations (orange \circ), part 4/5

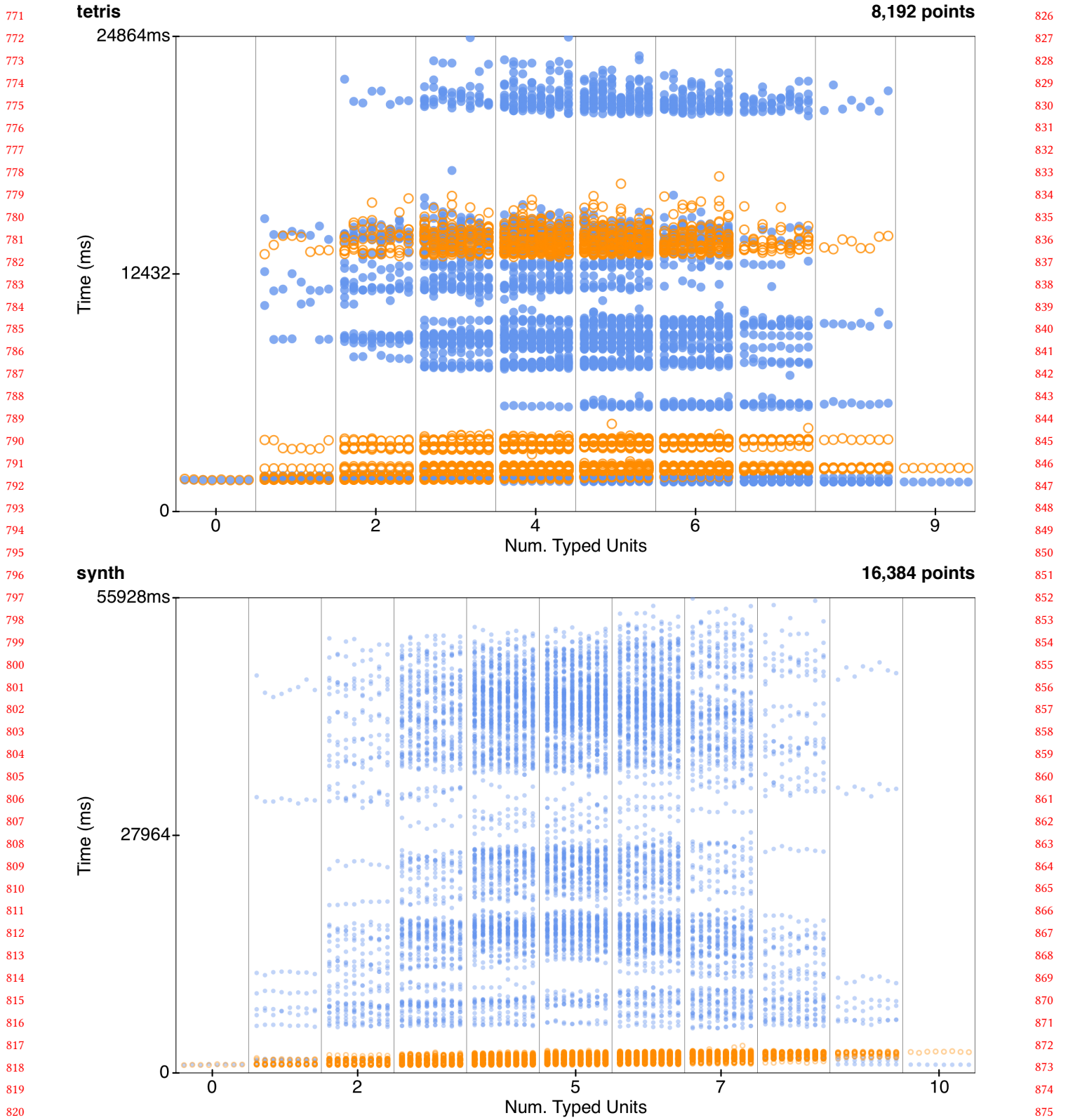


Fig. 6. Running time of TR-H configurations (blue ) and TR-1 configurations (orange ) , part 5/5

881 C Implementing Tagged Racket 936

882 The high-level architecture of TR-H is to: 937

- 883 1. type-check a module, 938
- 884 2. use the type environment to generate contracts, 939
- 885 3. optimize the contracts for the module, 940
- 886 4. output Racket bytecode. 941

887 For TR-1, we modified step 2 and replaced step 3. 942

889 C.1 Generating Type-Constructor Contracts 944

890 Typed Racket defines a function `type->contract` that (1) 945
 891 expects a type, (2) compiles the type to a so-called *static con-* 946
 892 *tract*, (3) optimizes the representation of the static contract, 947
 893 and (4) compiles the static contract to Racket code that will 948
 894 generate an appropriate contract. 949

895 We modified the `type->contract` function to generate 950
 896 type-constructor checks by adding a new method to the 951
 897 internal API for static contracts. For example, the method 952
 898 converts the contract for a list of elements into a contract 953
 899 that checks the `list?` predicate. 954
 900 955

901 C.2 Defending Typed Code 956

902 The TR-1 prototype replaces the Typed Racket optimizer 957
 903 with a completion function that adds type-constructor checks 958
 904 to typed code. The function implements a fold over the syn- 959
 905 tax of a type-annotated program, and performs two kinds of 960
 906 rewrites. 961

907 First, the completion function rewrites *most* applications 962
 908 $(f\ x)$ to $(\text{check } K\ (f\ x))$, where K is the static type of 963
 909 the application. If f is an identifier, however, there are two 964
 910 exceptional cases: 965

- 911 • f may be a built-in function that is certain to return a 966
 912 value of the correct type constructor (e.g., `map` always 967
 913 returns a list); and 968
- 914 • f may be statically typed, in which case soundness 969
 915 guarantees that f returns a value that matches its static 970
 916 type constructor. (there is one exception: accessor func- 971
 917 tions for user-defined `structs` are unsafe like any other 972
 918 accessor, e.g., `car`), 973
 919 974

920 For these exceptional cases, the completion function does 975
 921 not insert a type-constructor check. 976

922 Second, the completion function defends typed functions 977
 923 from dynamically-typed arguments by translating a function 978
 924 like $(\lambda\ (x)\ e)$ to $(\lambda\ (x)\ (\text{check } x)\ e)$. The structure of 979
 925 the check is based on the domain type of the function. 980
 926 981

927 C.3 Diff vs. Racket v6.10.1 982

928 The repository for this paper contains the TR-1 prototype 983
 929 and a diff between the prototype and Typed Racket v6.10.1. 984
 930 github.com/nuprl/tag-sound?path=src/locally-defensive.patch 985

D Existing Systems

This section illustrates prior work on gradual typing using the semantic framework of the paper. The goal is to demonstrate that the framework is able to express the *type boundaries* and *boundary checks* of existing systems, and to outline a formal comparison.

This section does not attempt to summarize the novelties and subtleties of each system. The interested reader must seek out the primary sources.

The subsections also give canonical forms lemmas for each system as a taste of their logical implications.

URLs All URLs accessed on 2018-06-28.

- Gradualtalk : <https://pleiad.cl/research/software/gradualtalk>
- Typed Racket : <https://github.com/racket/typed-racket>
- TPD : <https://github.com/jack-williams/tpd>
- StrongScript : <https://plg.uwaterloo.ca/~dynjs/strongscript/>
- ActionScript : <https://www.adobe.com/devnet/actionscript.html>
- mypy : <http://mypy-lang.org/>
- Flow : <https://flow.org/>
- Hack : <http://hacklang.org/>
- Pyre : <https://pyre-check.org/>
- Pytype : <https://opensource.google.com/projects/pytype>
- rtc : <https://github.com/plum-umd/rtc>
- Strongtalk : <http://strongtalk.org/>
- TypeScript : <https://www.typescriptlang.org/>
- Typed Clojure : <http://typedclojure.org/>
- Typed Lua : <https://github.com/andremm/typedlua>
- Pyret : <https://www.pyret.org/>
- Thorn : <http://janvitek.org/yearly.htm>
- Dart 2 : <https://www.dartlang.org/dart-2>
- Nom : <https://www.cs.cornell.edu/~ross/publications/nomalive/>
- Reticulated : <https://github.com/mvitousek/reticulated>
- SafeTS : <https://www.microsoft.com/en-us/research/publication/safe-efficient-gradual-typing-for-typescript-3/>
- TR-1 : <https://github.com/bennn/typed-racket/releases/tag/ld1.0>

1101	$\boxed{\text{Thorn}}$ (sketch)	1156
1102	$\tau = C \mid \text{like } C \mid \text{dyn}$	1157
1103	$v = p \mid (\text{dyn})p \mid (\text{like } C)p$	1158
1104	$p = C(f = v, \dots)$	1159
1105	$\boxed{\mathcal{D} : \tau \times v \rightarrow e}$ (undefined, all values have a static type)	1160
1106		1161
1107	$\boxed{\mathcal{S} : \tau \times v \rightarrow e}$ (via explicit type-cast)	1162
1108	$\mathcal{S}(C, v) = p$	1163
1109	if $v = p$ or $v = (\text{dyn})p$ or $v = (\text{like } C')p$	1164
1110	and $p = C''(f = v, \dots)$	1165
1111	and $C'' \leq C$	1166
1112	$\mathcal{S}(\text{like } C, v) = (\text{like } C)p$	1167
1113	if $v = p$ or $v = (\text{dyn})p$ or $v = (\text{like } C')p$	1168
1114	$\mathcal{S}(\text{dyn}, v) = (\text{dyn})p$	1169
1115	if $v = p$ or $v = (\text{dyn})p$ or $v = (\text{like } C')p$	1170
1116	$\mathcal{S}(\tau, v) = \text{BndryErr}$	1171
1117	otherwise	1172
1118		1173

Fig. 7. Thorn types, values, and boundary functions. The \mathcal{D} function is undefined for all inputs.

D.1 Thorn

Thorn (figure 7) is a nominally-typed object-oriented language. The idea is that a program may: declare typed classes, use the classes to create typed objects, and manipulate the objects in gradually-typed methods. If a method expects a dynamically-typed object, the type checker lets the method perform any operation on the object and the run-time system dynamically checks whether the operations are actually valid.

The types τ include *concrete* class names C , *like* class names ($\text{like } C$), and a dynamic type (dyn). The values are possibly-wrapped pointers to instances of classes; a value is either a direct pointer p , a dynamically-typed *view* to a pointer ($\text{dyn})p$, or a like-typed view to a pointer ($\text{like } C)p$. Informally, a view is a method-local pointer to an object.

One main invariant of Thorn is that every value comes with a type. In the figure, every value is an instance of a class and has the class name as its type. Because of this invariant, Thorn can efficiently check whether a value is compatible with some other type annotation at runtime. The \mathcal{S} function demonstrates this compatibility check.

The \mathcal{D} function is undefined for all inputs because there is no such thing as a dynamically-typed value. Put another way, the Thorn surface language is a single statically-typed language as opposed to a pair of languages. (The statically-typed language includes a dynamic to make it easy to experiment with statically-typed values, but nevertheless all values are statically typed to ensure safety and efficiency.)

Lemma 0.0 : *Thorn canonical forms*

- If $\vdash v : C$ then $v = C'(f = v_f, \dots)$ and $C' \leq C$.
- If $\vdash v : \text{like } C$ then $v = (\text{like } C')p$ and $C' \leq C$
- If $\vdash v : \text{dyn}$ then $v = (\text{dyn})p$

D.2 StrongScript

StrongScript (figure 8) adapts the ideas from Thorn to a type system for JavaScript. The types τ include concrete class names (!C), like class names (C), a dynamic type (any), and function types ($\tau \Rightarrow \tau$). The values are objects and functions.

Every object and function comes with an intrinsic type. For an object imported from JavaScript, this type is any. (For a function imported from JavaScript, this type is presumably $\text{any} \Rightarrow \text{any}$.) A typed object cannot inherit from a JavaScript object, and vice-versa.

The \mathcal{S} function checks the intrinsic type of a value against a type annotation. The idea is, if the check succeeds then a context may assume that the type annotation accurately describes the value.

The \mathcal{D} function is undefined for all inputs because the StrongScript paper does not directly model interactions with JavaScript. Instead, a JavaScript object is modeled as an object with type any, as mentioned above.

Lemma 0.1 : StrongScript *canonical forms*

- If $\vdash v : !C$ then $v = \{(s:v) \dots m \dots \parallel C'\}$ and $C' \leq C$
- If $\vdash v : C$ then either:
 - $v = \{(s:v) \dots m \dots \parallel C'\}$
 - $v = \{(s:v) \dots m \dots \parallel \text{any}\}$
- If $\vdash v : \tau_d \Rightarrow \tau_c$ then $v = \text{func}(x:\tau_d)\{\text{return } e:\tau_c\}$
- If $\vdash v : \text{any}$ then either:
 - $v = \{(s:v) \dots m \dots \parallel C'\}$
 - $v = \{(s:v) \dots m \dots \parallel \text{any}\}$
 - $v = \text{func}(x:\text{any})\{\text{return } e:\text{any}\}$

StrongScript (sketch)

$\tau = !C \mid C \mid \text{any} \mid \tau \Rightarrow \tau$

$v = \{(s:v) \dots m \dots \parallel \tau\} \mid \text{func}(x:\tau)\{\text{return } e:\tau\}$

$s \in \text{Strings}$

$m = x(x:\tau)\{\text{return } e:\tau\}$

$\mathcal{D} : \tau \times v \longrightarrow e$ (undefined, all values have a static type)

$\mathcal{S} : \tau \times v \longrightarrow e$ (via explicit type-cast)

$\mathcal{S}(\tau_d \Rightarrow \tau_c, v) = v'$

if $v = \text{func}(x:\tau_x)\{\text{return } e:\tau_v\}$

where $v' = \text{func}(x:\tau_d)\{\text{return}(\langle \tau_c \rangle (v(\langle \tau_x \rangle x))) : \tau_c\}$

$\mathcal{S}(C, v) = v$

if $v = \{(s:v) \dots m \dots \parallel C'\}$

and $C' \leq C$

$\mathcal{S}(\text{any}, v) = v$

if $v = \{(s:v) \dots m \dots \parallel \text{any}\}$

or $v = \{(s:v) \dots m \dots \parallel C\}$

$\mathcal{S}(\text{any}, v) = v'$

if $v = \text{func}(x:\tau_d)\{\text{return } e:\tau_c\}$

where $v' = \text{func}(x:\text{any})\{\text{return} \langle \text{any} \rangle (v(\langle \tau_d \rangle x)) : \text{any}\}$

$\mathcal{S}(\tau, v) = \text{BndryErr}$

otherwise

Fig. 8. StrongScript boundary functions. The \mathcal{D} function is undefined for all inputs.

1321 D.3 Dart 2

1322 Dart 2 is a new language with some support for dynamic
1323 typing. For details, see: dartlang.org/dart-2

1324 Figure 9 summarizes the key aspects of dynamic typing in
1325 Dart for a few types. The types represent integers (int), in-
1326 tegers and decimal numbers (num), lists (List< τ >), functions
1327 ($\tau \Rightarrow \tau$), and a dynamic type (dynamic). The base values b
1328 match these types.

1329 Dart programs do not directly interact with base values.
1330 Instead, base values are stored on a typed heap. The values v
1331 in figure 9 model this indirection by associating a base value
1332 with a compatible type.

1333 Just like in Thorn, a typed value may be used in a context
1334 that expects a less precise type. Also like Thorn, a value of
1335 type dynamic is an object that the type checker assumes can
1336 receive any method call. The run-time system checks that
1337 such method calls are actually safe for the given value.

1338 The \mathcal{S} boundary function checks a value against a type
1339 annotation by checking the value's associated type. The \mathcal{D}
1340 function is undefined for all inputs because it is not possible
1341 to define (or interact with) an untyped value.

1342 **Lemma 0.2** : *Dart canonical forms*

- 1343 • If $\vdash v : \tau$ then $v = b :: \tau'$ and $\tau' \leq \tau$

1344 *Remark*: a Dart function type must be declared explicitly.
1345 For example, to use the type $\text{int} \Rightarrow \text{int}$ one must first define
1346 an alias:

```
1347 typedef int IntFun(int _);
```

1348 Then the name IntFun may appear in other type annotations,
1349 e.g., in a method signature.

$\boxed{\text{Dart}}$ (sketch)

$\tau = \text{int} \mid \text{num} \mid \text{List}\langle\tau\rangle \mid \tau \Rightarrow \tau \mid \text{dynamic}$

$v = b :: \tau$

$b = i \mid d \mid [v \dots] \mid (\tau x) \Rightarrow e$

$\boxed{\mathcal{D} : \tau \times v \rightarrow e}$ (undefined, all values have a static type)

$\boxed{\mathcal{S} : \tau \times v \rightarrow e}$

$\mathcal{S}(\tau, b :: \tau') = b :: \tau'$

if $\tau' \leq \tau$

$\mathcal{S}(\tau, v) = \text{BndryErr}$

otherwise

Fig. 9. Dart boundary functions for a restricted grammar of types. The \mathcal{D} function is undefined for all inputs.

1431 D.4 Pyret

1432 Pyret is a dynamically-typed language with optional type
 1433 annotations and an optional static type checker. For details,
 1434 see: pyret.org.

1435 A type annotation in a Pyret program acts as a type-
 1436 constructor check at run-time. Figure 10 illustrates this as-
 1437 pect of Pyret in the \triangleright_S and \triangleright_D notions of reduction. Both
 1438 check the argument and result of a typed function against
 1439 the function's type. The \mathcal{X} boundary function performs the
 1440 check by matching a type constructor K against a value.

1441 One aspect of Pyret that is missing from figure 10 is the
 1442 translation that maps type annotations in the source code to
 1443 run-time constructor checks. This translation could be mod-
 1444 eled with a completion function (\rightsquigarrow), similar to the model of
 1445 the first-order embedding in the paper.

1446 Lemma 0.3 : Pyret assert-canonical forms

1447 If v is a value with the static type τ then v may be any
 1448 kind of value; however, if v is assigned to a variable x with
 1449 the programmer-assigned type τ , then one of the following
 1450 holds:

- 1451 • If $\vdash x : \tau_0 \times \tau_1$ then $v = \langle v_0, v_1 \rangle$
- 1452 • If $\vdash x : \tau_d \Rightarrow \tau_c$ then either:
 1453 - $v = \lambda y. e$
 1454 - $v = \lambda((y : \tau'_d) : \tau'_c). e$
- 1455 • If $\vdash x : \text{Int}$ then $v \in \mathbb{Z}$
- 1456 • If $\vdash x : \text{Nat}$ then $v \in \mathbb{N}$

1486 Pyret (sketch)

1487 $\tau = \text{Int} \mid \text{Nat} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 1488 $K = \text{Int} \mid \text{Nat} \mid \text{Pair} \mid \text{Fun}$
 1489 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda((x : \tau) : \tau). e$
 1490 $i \in \mathbb{Z}$
 1491 $e = \dots \mid \text{chk } K e$

1493 $\mathcal{D} : \tau \times v \rightarrow e$

1494 $\mathcal{D}(\tau, v) = \mathcal{X}(\lfloor \tau \rfloor, v)$

1493 $\mathcal{S} : \tau \times v \rightarrow e$

1494 $\mathcal{S}(\tau, v) = \mathcal{X}(\lfloor \tau \rfloor, v)$

1496 $\mathcal{X} : K \times v \rightarrow e$

1497 $\mathcal{X}(\text{Fun}, v) = v$
 1498 if $v = \lambda x. e$ or $v = \lambda((x : \tau'_d) : \tau'_c). e$
 1499 $\mathcal{X}(\text{Pair}, v) = v$
 1500 if $v = \langle v_0, v_1 \rangle$
 1501 $\mathcal{X}(\text{Int}, i) = i$
 1502 $\mathcal{X}(\text{Nat}, i) = i$
 1503 if $i \in \mathbb{N}$
 1504 $\mathcal{X}(K, v) = \text{BndryErr}$
 1505 otherwise

1506 $e \triangleright_S e$

1507 $(\lambda x. e) v \triangleright_S e[x \leftarrow v]$
 1508 $(\lambda((x : \tau_d) : \tau_c). e) v \triangleright_S \text{BndryErr}$
 1509 if $\mathcal{X}(\lfloor \tau_d \rfloor, v) = \text{BndryErr}$
 1510 $(\lambda((x : \tau_d) : \tau_c). e) v \triangleright_S \text{chk } \lfloor \tau_c \rfloor (e[x \leftarrow \mathcal{X}(\lfloor \tau_d \rfloor, v)])$
 1511 if $\mathcal{X}(\lfloor \tau_d \rfloor, v) \neq \text{BndryErr}$
 1512 $\text{chk } K v \triangleright_S \mathcal{X}(K, v)$

1513 $e \triangleright_D e$

1514 $(\lambda x. e) v \triangleright_D e[x \leftarrow v]$
 1515 $(\lambda((x : \tau_d) : \tau_c). e) v \triangleright_D \text{BndryErr}$
 1516 if $\mathcal{X}(\lfloor \tau_d \rfloor, v) = \text{BndryErr}$
 1517 $(\lambda((x : \tau_d) : \tau_c). e) v \triangleright_D \text{chk } \lfloor \tau_c \rfloor (e[x \leftarrow \mathcal{X}(\lfloor \tau_d \rfloor, v)])$
 1518 if $\mathcal{X}(\lfloor \tau_d \rfloor, v) \neq \text{BndryErr}$
 1519 $\text{chk } K v \triangleright_D \mathcal{X}(K, v)$

1520 Fig. 10. Pyret boundary functions and semantics for a re-
 1521 stricted grammar of types.

1541 D.5 SafeTS

1542 SafeTS is a core model of Safe TypeScript, which is a sound
1543 type system for JavaScript (as opposed to TypeScript).

1544 Figure 11 demonstrates SafeTS on three types: a type
1545 for numbers (number), a type for an object with two fields
1546 ($\{\text{fst} : \tau, \text{snd} : \tau\}$), and a type for an object with one method
1547 ($\{\text{call}(\tau) : \tau\}$). The latter types are intended to represent
1548 tuples and anonymous functions.

1549 Every value in a SafeTS program has an intrinsic type;
1550 there is no notion of a value that is defined in dynamically-
1551 typed code and imported to statically typed code. A typed
1552 value may, however, be used in a context that expects values
1553 with a different type by means of a type cast. The differ-
1554 ent type may contain new fields, but otherwise must be a
1555 supertype of the value's intrinsic type.

1556 The \mathcal{S} boundary function illustrates the run-time checks
1557 that SafeTS performs for our number, pair, and function types.
1558 For type number, SafeTS checks that the value is a number.
1559 For a pair type, SafeTS checks that the value is a pair of
1560 compatible type and recursively transports the components.
1561 For a function type, SafeTS checks that the value is a function
1562 of compatible type.

1563 The \mathcal{D} function is undefined because the SafeTS model
1564 does not define interactions with a model of JavaScript.

1565 Lemma 0.4 : SafeTS canonical forms

- 1566 • If $\vdash v : \{\text{fst} : \tau_0, \text{snd} : \tau_1\}$ then $v = \{\text{fst} :_{\tau'_0} v_0, \text{snd} :_{\tau'_1} v_1\}$ and
1567 $\tau'_0 \leq \tau_0$ and $\tau'_1 \leq \tau_1$
- 1568 • If $\vdash v : \{\text{call}(\tau_d) : \tau_c\}$ then $v = \{\text{call}(x : \tau'_d) : \tau'_c \{\text{return } e\}\}$
1569 and $\{\text{call}(\tau'_d) : \tau'_c\} \leq \{\text{call}(\tau_d) : \tau_c\}$
- 1570 • If $\vdash v : \text{number}$ then $v = i$

1571 *Remark:* if a SafeTS cast adds new fields to a value, the
1572 fields are recorded in an external “tag heap” of run-time type
1573 information. Figure 11 does not model the tag heap because
1574 it is not relevant to the types in the figure.
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595

SafeTS (sketch)

$\tau = \text{number} \mid \{\text{fst} : \tau, \text{snd} : \tau\} \mid \{\text{call}(\tau) : \tau\} \mid \text{any}$
 $v = i \mid \{\text{fst} :_{\tau} v, \text{snd} :_{\tau} v\} \mid \{\text{call}(x : \tau) : \tau \{\text{return } e\}\}$

$\mathcal{D} : \tau \times v \rightarrow e$ (undefined, all values have a static type)

$\mathcal{S} : \tau \times v \rightarrow e$

$\mathcal{S}(\{\text{call}(\tau_d) : \tau_c\}, v) = v$
if $v = \{\text{call}(x : \tau'_d) : \tau'_c \{\text{return } e\}\}$
and $\{\text{call}(\tau'_d) : \tau'_c\} \leq \{\text{call}(\tau_d) : \tau_c\}$
 $\mathcal{S}(\{\text{fst} : \tau_0, \text{snd} : \tau_1\}, v) = \{\text{fst} :_{\tau'_0} \mathcal{S}(\tau_0, v_0), \text{snd} :_{\tau'_1} \mathcal{S}(\tau_1, v_1)\}$
if $v = \{\text{fst} :_{\tau'_0} v_0, \text{snd} :_{\tau'_1} v_1\}$
and $\tau'_0 \leq \tau_0$ and $\tau'_1 \leq \tau_1$
 $\mathcal{S}(\text{number}, i) = i$
 $\mathcal{S}(\tau, v) = \text{BndryErr}$
otherwise

Fig. 11. SafeTS. The \mathcal{D} function is undefined for all inputs.

D.6 Nom

Nom is a nominal object oriented language. Types include a top type (\top), class names (C), and a dynamic type (**dynamic**). Values are instances of classes. Each value has an intrinsic type; namely, the name of its class.

The \mathcal{S} function checks that the intrinsic type of a value is compatible with a given type annotation. The \mathcal{D} function is undefined for all inputs because there way to define or import an untyped value.

Lemma 0.5 : *Nom canonical forms*

- If $\vdash v : C$ then $v = C'(v', \dots)$ and $C' \leqslant C$

Nom	(sketch)	1706
$\tau = \top \mid C \mid \mathbf{dynamic}$		1707
$v = C(v, \dots)$		1708
$\mathcal{D} : \tau \times v \rightarrow e$	(undefined, all values have a static type)	1709
$\mathcal{S} : \tau \times v \rightarrow e$		1710
$\mathcal{S}(\top, v)$	$= v$	1711
$\mathcal{S}(C, C'(v, \dots))$	$= C'(v, \dots)$	1712
	if $C' \leqslant C$	1713
$\mathcal{S}(\mathbf{dynamic}, v)$	$= v$	1714
$\mathcal{S}(\tau, v)$	$= \mathbf{BndryErr}$	1715
	otherwise	1716

Fig. 12. Nom. The \mathcal{D} function is undefined for all inputs.

1761 E Models 1816

1762 This section contains full definitions of the languages and 1817
 1763 full proofs of our claims about each language. 1818

1764 Aside from the common notions in section 5.1, the defi- 1819
 1765 nition and proofs of each model are independent and self- 1820
 1766 contained. 1821

1767 E.1 Preliminaries 1822

1768 Definition 1.0 : \rightarrow^* divergence 1823

1769 | Given a reduction relation \rightarrow^* , an expression e diverges if for 1824
 1770 all e' such that $e \rightarrow^* e'$ there exists an e'' such that $e' \rightarrow e''$. 1825
 1771 1826
 1772 1827

1773 Convention 1.1 : variable convention 1828

1774 | All λ -bound variables in an expression are distinct from one 1829
 1775 another, and from any free variables in the expression. 1830

1776 Assumption 1.2 : \vdash permutation 1831

1777 | For all typing judgments and properties \vdash : 1832
 1778 • If $x, x', \Gamma \vdash e$ then $x', x, \Gamma \vdash e$ 1833
 1779 • If $(x:\tau), (x':\tau'), \Gamma \vdash e$ then $(x':\tau'), (x:\tau), \Gamma \vdash e$ 1834
 1780 1835

1781 Definition 1.3 : \vdash boundary-free 1836

1782 | An expression e is *boundary free* if e does not contain a 1837
 1783 subterm of the form $(\text{dyn } \tau' e')$, nor a subterm of the form 1838
 1784 $(\text{stat } \tau' e')$. 1839
 1785 1840

1786 *Notes:* 1841

- 1787 • The upcoming models use a common surface syn- 1842
 1788 tax and typing system, but to keep each model self- 1843
 1789 contained we reprint this system in each definition. 1844
- 1790 • The proofs are written in a structured style, typically 1845
 1791 as a list of basic steps where each step is justified by an 1846
 1792 assumption, a lemma, or a previous step. Lemma names 1847
 1793 are *italicized* and hyperlinked to the actual lemma. 1848

E.2 (H) Higher-Order Embedding
E.2.1 Higher-Order Definitions
Language H

1871 $e = x \mid v \mid \langle e, e \rangle \mid e e \mid op^1 e \mid op^2 e e \mid$
 1872 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err}$
 1873 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e \mid$
 1874 $\text{mon}(\tau \Rightarrow \tau) v$
 1875 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 1876 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$
 1877 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$
 1878 $r = v \mid \text{Err}$
 1879 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 1880 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet$
 1881 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 1882 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E$

 $\Delta : op^1 \times \tau \longrightarrow \tau$

$$\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$$

$$\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$$

 $\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$

$$\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$$

$$\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$$

 $\tau \leqslant \tau$

$$\frac{}{\text{Nat} \leqslant \text{Int}} \quad \frac{\tau'_d \leqslant \tau_d \quad \tau_c \leqslant \tau'_c \quad \tau_0 \leqslant \tau'_0 \quad \tau_1 \leqslant \tau'_1}{\tau_d \Rightarrow \tau_c \leqslant \tau'_d \Rightarrow \tau'_c} \quad \frac{\tau_0 \leqslant \tau'_0 \quad \tau_1 \leqslant \tau'_1}{\tau_0 \times \tau_1 \leqslant \tau'_0 \times \tau'_1}$$

$$\frac{}{\tau \leqslant \tau} \quad \frac{\tau \leqslant \tau' \quad \tau' \leqslant \tau''}{\tau \leqslant \tau''}$$

 $\Gamma \vdash e$

$$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$$

$$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$$

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$$

 $\Gamma \vdash e : \tau$

$$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$$

$$\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$$

$$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$$

$$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$$

 $\Gamma \vdash_H e$

$$\frac{x \in \Gamma}{\Gamma \vdash_H x} \quad \frac{x, \Gamma \vdash_H e}{\Gamma \vdash_H \lambda x. e} \quad \frac{}{\Gamma \vdash_H i} \quad \frac{\Gamma \vdash_H e_0 \quad \Gamma \vdash_H e_1}{\Gamma \vdash_H \langle e_0, e_1 \rangle}$$

$$\frac{\Gamma \vdash_H e_0 \quad \Gamma \vdash_H e_1}{\Gamma \vdash_H e_0 e_1} \quad \frac{\Gamma \vdash_H e}{\Gamma \vdash_H op^1 e} \quad \frac{\Gamma \vdash_H e_0 \quad \Gamma \vdash_H e_1}{\Gamma \vdash_H op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash_H \text{Err}}$$

$$\frac{\Gamma \vdash_H e : \tau}{\Gamma \vdash_H \text{stat } \tau e} \quad \frac{\Gamma \vdash_H v : \tau_d \Rightarrow \tau_c}{\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v}$$

 $\Gamma \vdash_H e : \tau$

$$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash_H x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash_H e : \tau_c}{\Gamma \vdash_H \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash_H i : \text{Nat}}$$

$$\frac{}{\Gamma \vdash_H i : \text{Int}} \quad \frac{\Gamma \vdash_H e_0 : \tau_0 \quad \Gamma \vdash_H e_1 : \tau_1}{\Gamma \vdash_H \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash_H e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash_H e_1 : \tau_d}{\Gamma \vdash_H e_0 e_1 : \tau_c}$$

$$\frac{\Gamma \vdash_H e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash_H op^1 e_0 : \tau} \quad \frac{\Gamma \vdash_H e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash_H op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash_H e : \tau' \quad \tau' \leqslant \tau}{\Gamma \vdash_H e : \tau}$$

$$\frac{}{\Gamma \vdash_H \text{Err} : \tau} \quad \frac{\Gamma \vdash_H e}{\Gamma \vdash_H \text{dyn } \tau e : \tau}$$

$$\frac{\Gamma \vdash_H v}{\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v : (\tau_d \Rightarrow \tau_c)}$$

 $\delta(op^1, v) = e$

$$\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$$

$$\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$$

1981	$\delta(op^2, v, v) = e$	$e \rightarrow_{H-D} e$	2036
1982	$\delta(\text{sum}, i_0, i_1) = i_0 + i_1$	$E^\bullet[e] \rightarrow_{H-D} E^\bullet[e']$	2037
1983	$\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$	if $e \triangleright_{H-D} e'$	2038
1984	$\delta(\text{quotient}, i_0, i_1) = \lfloor i_0/i_1 \rfloor$	$E[\text{stat } \tau E^\bullet[e]] \rightarrow_{H-D} E[\text{stat } \tau E^\bullet[e']]$	2039
1985	if $i_1 \neq 0$	if $e \triangleright_{H-S} e'$	2040
1986	$\mathcal{D}_H : \tau \times v \rightarrow e$	$E[\text{dyn } \tau E^\bullet[e]] \rightarrow_{H-D} E[\text{dyn } \tau E^\bullet[e']]$	2041
1987	$\mathcal{D}_H(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v$	if $e \triangleright_{H-D} e'$	2042
1988	if $v = \lambda x. e$ or $v = \text{mon } \tau' v'$	$E[\text{Err}] \rightarrow_{H-D} \text{Err}$	2043
1989	$\mathcal{D}_H(\tau_0 \times \tau_1, \langle v_0, v_1 \rangle) = \langle \text{dyn } \tau_0 v_0, \text{dyn } \tau_1 v_1 \rangle$	$e \rightarrow_{H-S}^* e$ reflexive, transitive closure of \rightarrow_{H-S}	2044
1990	$\mathcal{D}_H(\text{Int}, i) = i$	2045	
1991	$\mathcal{D}_H(\text{Nat}, i) = i$	2046	
1992	if $i \in \mathbb{N}$	$e \rightarrow_{H-D}^* e$ reflexive, transitive closure of \rightarrow_{H-D}	2047
1993	$\mathcal{D}_H(\tau, v) = \text{BndryErr}$	2048	
1994	otherwise	2049	
1995	$\mathcal{S}_H : \tau \times v \rightarrow e$	2050	
1996	$\mathcal{S}_H(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v$	2051	
1997	$\mathcal{S}_H(\tau_0 \times \tau_1, \langle v_0, v_1 \rangle) = \langle \text{stat } \tau_0 v_0, \text{stat } \tau_1 v_1 \rangle$	2052	
1998	$\mathcal{S}_H(\text{Int}, v) = v$	2053	
1999	$\mathcal{S}_H(\text{Nat}, v) = v$	2054	
2000	$e \triangleright_{H-S} e$	2055	
2001	$\text{dyn } \tau v \triangleright_{H-S} \mathcal{D}_H(\tau, v)$	2056	
2002	$(\text{mon}(\tau_d \Rightarrow \tau_c) v_f) v \triangleright_{H-S} \text{dyn } \tau_c (v_f (\text{stat } \tau_d v))$	2057	
2003	$(\lambda(x:\tau). e) v \triangleright_{H-S} e[x \leftarrow v]$	2058	
2004	$op^1 v \triangleright_{H-S} \delta(op^1, v)$	2059	
2005	$op^2 v_0 v_1 \triangleright_{H-S} \delta(op^2, v_0, v_1)$	2060	
2006	$e \triangleright_{H-D} e$	2061	
2007	$\text{stat } \tau v \triangleright_{H-D} \mathcal{S}_H(\tau, v)$	2062	
2008	$v_0 v_1 \triangleright_{H-D} \text{TagErr}$	2063	
2009	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$	2064	
2010	$(\text{mon } \tau_d \Rightarrow \tau_c v_f) v \triangleright_{H-D} \text{stat } \tau_c (v_f (\text{dyn } \tau_d v))$	2065	
2011	$(\lambda x. e) v \triangleright_{H-D} e[x \leftarrow v]$	2066	
2012	$op^1 v \triangleright_{H-D} \text{TagErr}$	2067	
2013	if $\delta(op^1, v)$ is undefined	2068	
2014	$op^1 v \triangleright_{H-D} \delta(op^1, v)$	2069	
2015	$op^2 v_0 v_1 \triangleright_{H-D} \text{TagErr}$	2070	
2016	if $\delta(op^2, v_0, v_1)$ is undefined	2071	
2017	$op^2 v_0 v_1 \triangleright_{H-D} \delta(op^2, v_0, v_1)$	2072	
2018	$e \rightarrow_{H-S} e$	2073	
2019	$E^\bullet[e] \rightarrow_{H-S} E^\bullet[e']$	2074	
2020	if $e \triangleright_{H-S} e'$	2075	
2021	$E[\text{stat } \tau E^\bullet[e]] \rightarrow_{H-S} E[\text{stat } \tau E^\bullet[e']]$	2076	
2022	if $e \triangleright_{H-S} e'$	2077	
2023	$E[\text{dyn } \tau E^\bullet[e]] \rightarrow_{H-S} E[\text{dyn } \tau E^\bullet[e']]$	2078	
2024	if $e \triangleright_{H-D} e'$	2079	
2025	$E[\text{Err}] \rightarrow_{H-S} \text{Err}$	2080	
2026		2081	
2027		2082	
2028		2083	
2029		2084	
2030		2085	
2031		2086	
2032		2087	
2033		2088	
2034		2089	
2035		2090	

E.2.2 Higher-Order Theorems

Theorem 2.0 : static H-soundness

If $\vdash e : \tau$ then $\vdash_H e : \tau$ and one of the following holds:

- $e \rightarrow_{H-S}^* v$ and $\vdash_H v : \tau$
- $e \rightarrow_{H-S}^* E[\text{dyn } \tau' E^*[e']]$ and $e' \triangleright_{H-D} \text{TagErr}$
- $e \rightarrow_{H-S}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_H e : \tau$
by *static subset*
2. QED by *H static progress* and *H static preservation*.

Theorem 2.1 : dynamic H-soundness

If $\vdash e$ then $\vdash_H e$ and one of the following holds:

- $e \rightarrow_{H-D}^* v$ and $\vdash_H v$
- $e \rightarrow_{H-D}^* E[e']$ and $e' \triangleright_{H-D} \text{TagErr}$
- $e \rightarrow_{H-D}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_H e$
by *dynamic subset*
2. QED by *H dynamic progress* and *H dynamic preservation*.

Corollary 2.2 : H static soundness

If $\vdash e : \tau$ and e is boundary-free, then one of the following holds:

- $e \rightarrow_H^* v$ and $\vdash_H v : \tau$
- $e \rightarrow_H^* \text{BndryErr}$
- e diverges

Proof:

Consequence of the proof for *static H-soundness*

Corollary 2.3 : H compilation

If $\vdash e : \tau$

and \mathcal{D}'_H extends \mathcal{D}_H with a rule to monitor a typed function:

$$\mathcal{D}'_H(\tau_d \Rightarrow \tau_c, \lambda(x:\tau). e) = \text{mon}(\tau_d \Rightarrow \tau_c)(\lambda(x:\tau). e)$$

and \triangleright_{H-D}' extends \triangleright_{H-D} with a rule to apply a typed function:

$$(\lambda(x:\tau). e) v \triangleright_{H-D}' e[x \leftarrow v]$$

and $e \rightarrow_{H-D}' e$ is defined as:

$$E[e] \rightarrow_{H-D}' E[e']$$

if $e \triangleright_{H-D}' e'$

$$E[\text{stat } \tau v] \rightarrow_{H-D}' E[\mathcal{D}'_H(\tau, v)]$$

$$E[\text{dyn } \tau v] \rightarrow_{H-D}' E[\mathcal{D}'_H(\tau, v)]$$

$$E[\text{Err}] \rightarrow_{H-D}' \text{Err}$$

and $\rightarrow_{H-D}'^*$ is the reflexive transitive closure of \rightarrow_{H-D}'

then one of the following holds:

- $e \rightarrow_{H-D}'^* v$ and $\vdash_H v : \tau$
- $e \rightarrow_{H-D}'^* \text{TagErr}$
- $e \rightarrow_{H-D}'^* \text{BndryErr}$
- e diverges

Proof:

By *static H-soundness* and the fact that \mathcal{S}_H and \triangleright_{H-S} are subsets of \mathcal{D}'_H and \triangleright_{H-D}' , respectively.

□

2091		2146
2092		2147
2093		2148
2094		2149
2095		2150
2096		2151
2097		2152
2098		2153
2099		2154
2100		2155
2101		2156
2102		2157
2103		2158
2104		2159
2105		2160
2106		2161
2107		2162
2108		2163
2109		2164
2110		2165
2111		2166
2112		2167
2113		2168
2114		2169
2115		2170
2116		2171
2117		2172
2118		2173
2119		2174
2120		2175
2121		2176
2122		2177
2123		2178
2124		2179
2125		2180
2126		2181
2127		2182
2128		2183
2129		2184
2130		2185
2131		2186
2132		2187
2133		2188
2134		2189
2135		2190
2136		2191
2137		2192
2138		2193
2139		2194
2140		2195
2141		2196
2142		2197
2143		2198
2144		2199
2145		2200

E.2.3 Higher-Order Lemmas

Lemma 2.4 : \mathcal{D}_H soundness

If $\vdash_H v$ then $\vdash_H \mathcal{D}_H(\tau, v) : \tau$

Proof:

CASE $\mathcal{D}_H(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

1. $\vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v : \tau_d \Rightarrow \tau_c$
by $\vdash_H v$
2. QED

CASE $v = \langle v_0, v_1 \rangle$

$\wedge \mathcal{D}_H(\tau_0 \times \tau_1, v) = \langle \text{dyn } \tau_0 v_0, \text{dyn } \tau_1 v_1 \rangle :$

1. $\vdash_H v_0$
 $\wedge \vdash_H v_1$
by **H inversion**
2. $\vdash_H \text{dyn } \tau_0 v_0 : \tau_0$
 $\wedge \vdash_H \text{dyn } \tau_1 v_1 : \tau_1$
by (1)
3. QED (2)

CASE $v = i$

$\wedge \mathcal{D}_H(\text{Int}, v) = v :$

1. QED

CASE $v \in \mathbb{N}$

$\wedge \mathcal{D}_H(\text{Nat}, v) = v :$

1. QED

CASE $\mathcal{D}_H(\tau, v) = \text{BndryErr} :$

1. QED

□

Lemma 2.5 : \mathcal{S}_H soundness

If $\vdash_H v : \tau$ then $\vdash_H \mathcal{S}_H(\tau, v)$

Proof:

CASE $\vdash_H v : \tau_d \Rightarrow \tau_c$

$\wedge \mathcal{S}_H(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

1. QED

CASE $\vdash_H v : \tau_0 \times \tau_1$

$\wedge \mathcal{S}_H(\tau_0 \times \tau_1, v) = \langle \text{stat } \tau_0 v_0, \text{stat } \tau_1 v_1 \rangle :$

1. $v = \langle v_0, v_1 \rangle$
by **canonical forms**
2. $\vdash_H v_0 : \tau_0$
 $\wedge \vdash_H v_1 : \tau_1$
by **H inversion** (1)
3. $\vdash_H \text{stat } \tau_0 v_0 : \tau_0$
by the induction hypothesis (2)
4. $\vdash_H \text{stat } \tau_1 v_1 : \tau_1$
by the induction hypothesis (2)
5. QED

CASE $\vdash_H v : \text{Int}$

$\wedge \mathcal{S}_H(\text{Int}, v) = v :$

1. QED

CASE $\vdash_H v : \text{Nat}$

$\wedge \mathcal{S}_H(\text{Nat}, v) = v :$

1. QED

□

Lemma 2.6 : H static subset

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash_H e : \tau$.

Proof:

By structural induction on the derivation of $\Gamma \vdash e : \tau$.

CASE $\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} :$

1. $\Gamma \vdash_H x : \tau$
by $(x:\tau) \in \Gamma$
2. QED

CASE $\frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} :$

1. $(x:\tau_d), \Gamma \vdash_H e : \tau_c$
by the induction hypothesis
2. $\Gamma \vdash_H \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c$
3. QED

CASE $\frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}} :$

1. QED

CASE $\frac{}{\Gamma \vdash i : \text{Int}} :$

1. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} :$

1. $\Gamma \vdash_H e_0 : \tau_0$
 $\wedge \Gamma \vdash_H e_1 : \tau_1$
by the induction hypothesis
2. $\Gamma \vdash_H \langle e_0, e_1 \rangle : \tau_0 \times \tau_1$
3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c} :$

1. $\Gamma \vdash_H e_0 : \tau_d \Rightarrow \tau_c$
 $\wedge \Gamma \vdash_H e_1 : \tau_d$
by the induction hypothesis
2. $\Gamma \vdash_H e_0 e_1 : \tau_c$
3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(\text{op}^1, \tau_0) = \tau}{\Gamma \vdash \text{op}^1 e_0 : \tau} :$

1. $\Gamma \vdash_H e_0 : \tau_0$
by the induction hypothesis
2. $\Gamma \vdash_H \text{op}^1 e_0 : \tau$
3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \quad \Delta(\text{op}^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau} :$

1. $\Gamma \vdash_H e_0 : \tau_0$
 $\wedge \Gamma \vdash_H e_1 : \tau_1$
by the induction hypothesis
2. $\Gamma \vdash_H \text{op}^2 e_0 e_1 : \tau$
3. QED

2311 **CASE** $\frac{\Gamma \vdash e : \tau' \quad \tau' <: \tau}{\Gamma \vdash e : \tau}$:

- 2312
2313
2314 1. $\Gamma \vdash_{\text{H}} e : \tau'$
by the induction hypothesis
2315
2316 2. $\Gamma \vdash_{\text{H}} e : \tau$
2317 3. QED

2318 **CASE** $\frac{}{\Gamma \vdash \text{Err} : \tau}$:

2319
2320 1. QED
2321 **CASE** $\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$:

- 2322
2323
2324 1. $\Gamma \vdash_{\text{H}} e$
by *dynamic subset*
2325
2326 2. $\Gamma \vdash_{\text{H}} \text{dyn } \tau e : \tau$
by (1)
2327
2328 3. QED

2329 \square

2330 **Lemma 2.7** : H *dynamic subset*

2331 If $\Gamma \vdash e$ then $\Gamma \vdash_{\text{H}} e$.

2332 *Proof*:

2333 By structural induction on the derivation of $\Gamma \vdash e$.

2334 **CASE** $\frac{x \in \Gamma}{\Gamma \vdash x}$:

- 2335
2336
2337 1. $\Gamma \vdash_{\text{H}} x$
by $x \in \Gamma$
2338
2339 2. QED

2340 **CASE** $\frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e}$:

- 2341
2342
2343 1. $x, \Gamma \vdash_{\text{H}} e$
by the induction hypothesis
2344
2345 2. $\Gamma \vdash_{\text{H}} \lambda x. e$
by (1)
2346
2347 3. QED

2348 **CASE** $\frac{}{\Gamma \vdash i}$:

- 2349
2350 1. QED

2351 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$:

- 2352
2353
2354 1. $\Gamma \vdash_{\text{H}} e_0$
 $\wedge \Gamma \vdash_{\text{H}} e_1$
by the induction hypothesis
2355
2356 2. $\Gamma \vdash_{\text{H}} \langle e_0, e_1 \rangle$
by (1)
2357
2358 3. QED

2359
2360 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1}$:

2361
2362
2363
2364
2365

- 2366 1. $\Gamma \vdash_{\text{H}} e_0$
2367 $\wedge \Gamma \vdash_{\text{H}} e_1$
2368 by the induction hypothesis

- 2369 2. $\Gamma \vdash_{\text{H}} e_0 e_1$
2370 by (1)
2371 3. QED

2372 **CASE** $\frac{\Gamma \vdash e}{\Gamma \vdash \text{op}^1 e}$:

- 2373
2374
2375 1. $\Gamma \vdash_{\text{H}} e$
by the induction hypothesis
2376
2377 2. $\Gamma \vdash_{\text{H}} \text{op}^1 e$
by (1)
2378
2379 3. QED

2380 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \text{op}^2 e_0 e_1}$:

- 2381
2382
2383 1. $\Gamma \vdash_{\text{H}} e_0$
 $\wedge \Gamma \vdash_{\text{H}} e_1$
by the induction hypothesis
2384
2385 2. $\Gamma \vdash_{\text{H}} \text{op}^2 e_0 e_1$
by (1)
2386
2387 3. QED

2388 **CASE** $\frac{}{\Gamma \vdash \text{Err}}$:

- 2389
2390 1. QED

2391 **CASE** $\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$:

- 2392
2393
2394 1. $\Gamma \vdash_{\text{H}} e : \tau$
by *static subset*
2395
2396 2. $\Gamma \vdash_{\text{H}} \text{stat } \tau e$
by (1)
2397
2398 3. QED

2399 \square

2400 **Lemma 2.8** : H *static progress*

2401 If $\vdash_{\text{H}} e : \tau$ then one of the following holds:

- 2402 • e is a value
2403 • $e \in \text{Err}$
2404 • $e \rightarrow_{\text{H-S}} e'$
2405 • $e \rightarrow_{\text{H-S}} \text{BndryErr}$
2406 • $e = E[\text{dyn } \tau' E^\bullet[e']]$ and $e' \triangleright_{\text{H-D}} \text{TagErr}$
2407

2408 *Proof*:

2409 By the *boundary factoring* lemma, there are seven possible cases.

2410 **CASE** e is a value :

- 2411 1. QED

2412 **CASE** $e = E^\bullet[v_0 v_1]$:

- 2413 1. $\vdash_{\text{H}} v_0 v_1 : \tau'$
by *static hole typing*
2414
2415 2. $\vdash_{\text{H}} v_0 : \tau_d \Rightarrow \tau_c$
 $\wedge \vdash_{\text{H}} v_1 : \tau_d$
by *H inversion*
2416
2417
2418

2421	3. $v_0 = \lambda(x:\tau'_d). e'$	IF $e' \rightarrow_{H-D} \text{BndryErr}$:	2476
2422	$\vee v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_f$	a. $\text{QED } e \rightarrow_{H-S} E[\text{dyn } \tau' \text{ BndryErr}]$	2477
2423	by <i>canonical forms</i>	ELSE $e' = E'[e'']$ and $e'' \triangleright_{H-D} \text{TagErr}$:	2478
2424	4. IF $v_0 = \lambda(x:\tau'_d). e' :$	a. $E' \in E^\bullet$	2479
2425	a. $e \rightarrow_{H-S} E^\bullet[e'[x \leftarrow v_1]]$	by e' is boundary-free	2480
2426	by $v_0 v_1 \triangleright_{H-S} e'[x \leftarrow v_1]$	b. QED	2481
2427	b. QED	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	2482
2428	ELSE $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_f :$	1. e' is a value	2483
2429	a. $e \rightarrow_{H-S} E^\bullet[\text{dyn } \tau'_c (v_f (\text{stat } \tau'_d v_1))]$	$\vee e' \in \text{Err}$	2484
2430	by $v_0 v_1 \triangleright_{H-S} \text{dyn } \tau'_c (v_f (\text{stat } \tau'_d v_1))$	$\vee e' \rightarrow_{H-S} e''$	2485
2431	b. QED	$\vee e' \rightarrow_{H-S} \text{BndryErr}$	2486
2432	CASE $e = E^\bullet[\text{op}^1 v] :$	$\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{H-D} \text{TagErr}$	2487
2433	1. $\vdash_H \text{op}^1 v : \tau'$	by <i>H static progress</i>	2488
2434	by <i>static hole typing</i>	2. IF e' is a value :	2489
2435	2. $\vdash_H v : \tau_0 \times \tau_1$	a. $\text{QED } e \rightarrow_{H-S} E[\mathcal{S}_H(\tau', e')]$	2490
2436	by <i>H inversion</i>	IF $e' \in \text{Err}$:	2491
2437	3. $v = \langle v_0, v_1 \rangle$	a. $\text{QED } e \rightarrow_{H-S} e'$	2492
2438	by <i>canonical forms</i>	IF $e' \rightarrow_{H-S} e'' :$	2493
2439	4. IF $\text{op}^1 = \text{fst}$:	a. $\text{QED } e \rightarrow_{H-S} E[\text{stat } \tau' e'']$	2494
2440	a. $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$	IF $e' \rightarrow_{H-S} \text{BndryErr}$:	2495
2441	b. $e \rightarrow_{H-S} E^\bullet[v_0]$	a. $\text{QED } e \rightarrow_{H-S} E[\text{stat } \tau' \text{ BndryErr}]$	2496
2442	by $\text{op}^1 v \triangleright_{H-S} v_0$	ELSE $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{H-D} \text{TagErr}$	2497
2443	c. QED	:	2498
2444	ELSE $\text{op}^1 = \text{snd}$:	a. Contradiction by e' is boundary-free	2499
2445	a. $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$	CASE $e = E[\text{Err}] :$	2500
2446	b. $e \rightarrow_{H-S} E^\bullet[v_1]$	1. $\text{QED } e \rightarrow_{H-S} \text{Err}$	2501
2447	by $\text{op}^1 v \triangleright_{H-S} v_1$	\square	2502
2448	c. QED	Lemma 2.9 : <i>H dynamic progress</i>	2503
2449	CASE $e = E^\bullet[\text{op}^2 v_0 v_1] :$	If $\vdash_H e$ then one of the following holds:	2504
2450	1. $\vdash_H \text{op}^2 v_0 v_1 : \tau'$	• e is a value	2505
2451	by <i>static hole typing</i>	• $e \in \text{Err}$	2506
2452	2. $\vdash_H v_0 : \tau_0$	• $e \rightarrow_{H-D} e'$	2507
2453	$\wedge \vdash_H v_1 : \tau_1$	• $e \rightarrow_{H-D} \text{BndryErr}$	2508
2454	$\wedge \Delta(\text{op}^2, \tau_0, \tau_1) = \tau''$	• $e = E[e']$ and $e' \triangleright_{H-D} \text{TagErr}$	2509
2455	by <i>H inversion</i>	<i>Proof:</i>	2510
2456	3. $\delta(\text{op}^2, v_0, v_1) = e'$	By the <i>boundary factoring</i> lemma, there are seven cases.	2511
2457	by Δ <i>type soundness</i> (2)	CASE e is a value :	2512
2458	4. $\text{op}^2 v_0 v_1 \triangleright_{H-S} e'$	1. QED	2513
2459	by (3)	CASE $e = E^\bullet[v_0 v_1] :$	2514
2460	5. QED by $e \rightarrow_{H-S} E^\bullet[e']$	IF $v_0 = \lambda x. e' :$	2515
2461	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	1. $e \rightarrow_{H-D} E^\bullet[e'[x \leftarrow v_1]]$	2516
2462	1. e' is a value	by $v_0 v_1 \triangleright_{H-D} e'[x \leftarrow v_1]$	2517
2463	$\vee e' \in \text{Err}$	2. QED	2518
2464	$\vee e' \rightarrow_{H-D} e''$	IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f :$	2519
2465	$\vee e' \rightarrow_{H-D} \text{BndryErr}$	1. $e \rightarrow_{H-D} E^\bullet[\text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))]$	2520
2466	$\vee e' = E'[e'']$ and $e'' \triangleright_{H-D} \text{TagErr}$	by $v_0 v_1 \triangleright_{H-D} \text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))$	2521
2467	by <i>H dynamic progress</i>	2. QED	2522
2468	2. IF e' is a value :	ELSE $v_0 = i$	2523
2469	a. $\text{QED } e \rightarrow_{H-S} E[\mathcal{D}_H(\tau', e')]$	$\vee v_0 = \langle v, v' \rangle :$	2524
2470	IF $e' \in \text{Err}$:	1. $e \rightarrow_{H-D} \text{TagErr}$	2525
2471	a. $\text{QED } e \rightarrow_{H-S} e'$	by $(v_0 v_1) \triangleright_{H-D} \text{TagErr}$	2526
2472	IF $e' \rightarrow_{H-D} e'' :$	2. QED	2527
2473	a. $\text{QED } e \rightarrow_{H-S} E[\text{dyn } \tau' e'']$	CASE $e = E^\bullet[\text{op}^1 v] :$	2528
2474		IF $\delta(\text{op}^1, v) = e' :$	2529
2475			2530

2531 1. $(op^1 v) \triangleright_{H-D} e'$
 2532 2. QED
 2533 **ELSE** $\delta(op^1, v)$ is undefined :
 2534 1. $e \rightarrow_{H-D} \text{TagErr}$
 2535 by $(op^1 v) \triangleright_{H-D} \text{TagErr}$
 2536 2. QED
 2537 **CASE** $e = E^\bullet[op^2 v_0 v_1]$:
 2538 **IF** $\delta(op^2, v_0, v_1) = e''$:
 2539 1. $op^2 v_0 v_1 \triangleright_{H-D} e''$
 2540 2. QED
 2541 **ELSE** $\delta(op^2, v_0, v_1)$ is undefined :
 2542 1. $e \rightarrow_{H-D} \text{TagErr}$
 2543 by $op^2 v_0 v_1 \triangleright_{H-D} \text{TagErr}$
 2544 2. QED
 2545 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
 2546 1. e' is a value
 2547 $\vee e' \in \text{Err}$
 2548 $\vee e' \rightarrow_{H-D} e''$
 2549 $\vee e' \rightarrow_{H-D} \text{BndryErr}$
 2550 $\vee e' = E[e'']$ and $e'' \triangleright_{H-D} \text{TagErr}$
 2551 by **H dynamic progress**
 2552 2. **IF** e' is a value :
 2553 a. QED $e \rightarrow_{H-D} E[\mathcal{D}_H(\tau', e')]$
 2554 **IF** $e' \in \text{Err}$:
 2555 a. QED $e \rightarrow_{H-D} e'$
 2556 **IF** $e' \rightarrow_{H-D} e''$:
 2557 a. QED $e \rightarrow_{H-S} E[\text{dyn } \tau' e'']$
 2558 **IF** $e' \rightarrow_{H-D} \text{BndryErr}$:
 2559 a. QED $e \rightarrow_{H-D} E[\text{dyn } \tau' \text{BndryErr}]$
 2560 **ELSE** $e' = E[e'']$ and $e'' \triangleright_{H-D} \text{TagErr}$:
 2561 a. $E \in E^\bullet$
 2562 by e' is boundary-free
 2563 b. QED
 2564 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
 2565 1. e' is a value
 2566 $\vee e' \in \text{Err}$
 2567 $\vee e' \rightarrow_{H-S} e''$
 2568 $\vee e' \rightarrow_{H-S} \text{BndryErr}$
 2569 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{H-D} \text{TagErr}$
 2570 by **H static progress**
 2571 2. **IF** e' is a value :
 2572 a. QED $e \rightarrow_{H-S} E[\mathcal{S}_H(\tau', e')]$
 2573 **IF** $e' \in \text{Err}$:
 2574 a. QED $e \rightarrow_{H-S} e'$
 2575 **IF** $e' \rightarrow_{H-S} e''$:
 2576 a. QED $e \rightarrow_{H-S} E[\text{stat } \tau' e'']$
 2577 **IF** $e' \rightarrow_{H-S} \text{BndryErr}$:
 2578 a. QED $e \rightarrow_{H-S} E[\text{stat } \tau' \text{BndryErr}]$
 2579 **ELSE** $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{H-D} \text{TagErr}$
 2580 :
 2581 a. Contradiction by e' is boundary-free
 2582 **CASE** $e = E[\text{Err}]$:
 2583 1. QED $e \rightarrow_{H-D} \text{Err}$
 2584 \square
 2585

Lemma 2.10 : H static preservation 2586

If $\vdash_H e : \tau$ and $e \rightarrow_{H-S} e'$ then $\vdash_H e' : \tau$ 2587

Proof: 2588

By the *boundary factoring* lemma there are seven cases. 2589

CASE e is a value : 2590

1. Contradiction by $e \rightarrow_{H-S} e'$ 2591

CASE $e = E^\bullet[v_0 v_1]$: 2592

IF $v_0 = \lambda(x:\tau_x). e'$ 2593

$\wedge e \rightarrow_{H-S} E^\bullet[e'[x \leftarrow v_1]]$: 2594

1. $\vdash_H v_0 v_1 : \tau'$ 2595

by *static hole typing* 2596

2. $\vdash_H v_0 : \tau_d \Rightarrow \tau_c$ 2597

$\wedge \vdash_H v_1 : \tau_d$ 2598

$\wedge \tau_c \leq \tau'$ 2599

by **H inversion** 2600

3. $\tau_d \leq \tau_x$ 2601

by *canonical forms* (2) 2602

4. $(x:\tau_x) \vdash_H e' : \tau_c$ 2603

by **H inversion** (2) 2604

5. $\vdash_H v_1 : \tau_x$ 2605

by (2, 3) 2606

6. $\vdash_H e'[x \leftarrow v_1] : \tau_c$ 2607

by *substitution* (4, 5) 2608

7. $\vdash_H e'[x \leftarrow v_1] : \tau'$ 2609

by (2, 6) 2610

8. QED by *hole substitution* (7) 2611

ELSE $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f$ 2612

$\wedge e \rightarrow_{H-S} E^\bullet[\text{dyn } \tau_c (v_f (\text{stat } \tau_d v_1))]$: 2613

1. $\vdash_H v_0 v_1 : \tau'$ 2614

by *static hole typing* 2615

2. $\vdash_H v_0 : \tau'_d \Rightarrow \tau'_c$ 2616

$\wedge \vdash_H v_1 : \tau'_d$ 2617

$\wedge \tau'_c \leq \tau'$ 2618

by **H inversion** 2619

3. $\vdash_H v_f$ 2620

by **H inversion** (2) 2621

4. $\tau_d \Rightarrow \tau_c \leq \tau'_d \Rightarrow \tau'_c$ 2622

by *canonical forms* (2) 2623

5. $\tau'_d \leq \tau_d$ 2624

$\wedge \tau_c \leq \tau'_c$ 2625

by (4) 2626

6. $\vdash_H v_1 : \tau_d$ 2627

by (2, 5) 2628

7. $\vdash_H \text{stat } \tau_d v_1$ 2629

by (6) 2630

8. $\vdash_H v_f (\text{stat } \tau_d v_1)$ 2631

by (3, 7) 2632

9. $\vdash_H \text{dyn } \tau_c v_f (\text{stat } \tau_d v_1) : \tau_c$ 2633

by (8) 2634

10. $\vdash_H \text{dyn } \tau_c v_f (\text{stat } \tau_d v_1) : \tau'$ 2635

by (2, 5, 9) 2636

11. QED by *hole substitution* (10) 2637

CASE $e = E^\bullet[op^1 v]$: 2638

2586

2587

2588

2589

2590

2591

2592

2593

2594

2595

2596

2597

2598

2599

2600

2601

2602

2603

2604

2605

2606

2607

2608

2609

2610

2611

2612

2613

2614

2615

2616

2617

2618

2619

2620

2621

2622

2623

2624

2625

2626

2627

2628

2629

2630

2631

2632

2633

2634

2635

2636

2637

2638

2639

2640

2641	IF $v = \langle v_0, v_1 \rangle$	2. $\vdash_{\text{H}} \text{dyn } \tau' e' : \tau'$	2696
2642	$\wedge \text{op}^1 = \text{fst}$	by <i>boundary hole typing</i>	2697
2643	$\wedge e \rightarrow_{\text{H-S}} E^\bullet[v_0] :$	3. $\vdash_{\text{H}} e'$	2698
2644	1. $\vdash_{\text{H}} \text{fst } \langle v_0, v_1 \rangle : \tau'$	by H inversion (2)	2699
2645	by <i>static hole typing</i>	4. $\vdash_{\text{H}} e''$	2700
2646	2. $\vdash_{\text{H}} \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	by H dynamic preservation (3)	2701
2647	$\wedge \tau_0 \leq \tau'$	5. $\vdash_{\text{H}} \text{dyn } \tau' e'' : \tau'$	2702
2648	by H inversion (1)	by (4)	2703
2649	3. $\vdash_{\text{H}} v_0 : \tau_0$	6. QED by <i>hole substitution</i> (5)	2704
2650	by H inversion (2)	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	2705
2651	4. $\vdash_{\text{H}} v_0 : \tau'$	IF e' is a value :	2706
2652	by (2, 3)	1. $e \rightarrow_{\text{H-S}} E[\mathcal{S}_{\text{H}}(\tau', e')]$	2707
2653	5. QED by <i>hole substitution</i> (4)	2. $\vdash_{\text{H}} \text{stat } \tau' e'$	2708
2654	ELSE $v = \langle v_0, v_1 \rangle$	by <i>boundary hole typing</i>	2709
2655	$\wedge \text{op}^1 = \text{snd}$	3. $\vdash_{\text{H}} e' : \tau'$	2710
2656	$\wedge e \rightarrow_{\text{H-S}} E^\bullet[v_1] :$	by H inversion (2)	2711
2657	1. $\vdash_{\text{H}} \text{snd } \langle v_0, v_1 \rangle : \tau'$	4. $\vdash_{\text{H}} \mathcal{S}_{\text{H}}(\tau', e')$	2712
2658	by <i>static hole typing</i>	by \mathcal{S}_{H} <i>soundness</i> (3)	2713
2659	2. $\vdash_{\text{H}} \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	5. QED by <i>hole substitution</i> (4)	2714
2660	$\wedge \tau_1 \leq \tau'$	ELSE $e' \rightarrow_{\text{H-S}} e'' :$	2715
2661	by H inversion (1)	1. $e \rightarrow_{\text{H-S}} E[\text{stat } \tau' e'']$	2716
2662	3. $\vdash_{\text{H}} v_1 : \tau_1$	2. $\vdash_{\text{H}} \text{stat } \tau' e'$	2717
2663	by H inversion (2)	by <i>boundary hole typing</i>	2718
2664	4. $\vdash_{\text{H}} v_1 : \tau'$	3. $\vdash_{\text{H}} e' : \tau'$	2719
2665	by (2, 3)	by H inversion (2)	2720
2666	5. QED by <i>hole substitution</i> (4)	4. $\vdash_{\text{H}} e'' : \tau'$	2721
2667	CASE $e = E^\bullet[\text{op}^2 v_0 v_1] :$	by H static preservation (3)	2722
2668	1. $e \rightarrow_{\text{H-S}} E^\bullet[\delta(\text{op}^2, v_0, v_1)]$	5. $\vdash_{\text{H}} \text{stat } \tau' e''$	2723
2669	by $e \rightarrow_{\text{H-S}} e'$	by (4)	2724
2670	2. $\vdash_{\text{H}} \text{op}^2 v_0 v_1 : \tau'$	6. QED by <i>hole substitution</i> (5)	2725
2671	by <i>static hole typing</i>	CASE $e = E[\text{Err}] :$	2726
2672	3. $\vdash_{\text{H}} v_0 : \tau_0$	1. $e \rightarrow_{\text{H-S}} \text{Err}$	2727
2673	$\wedge \vdash_{\text{H}} v_1 : \tau_1$	2. QED by $\vdash_{\text{H}} \text{Err} : \tau$	2728
2674	$\wedge \Delta(\text{op}^2, \tau_0, \tau_1) = \tau''$		2729
2675	$\wedge \tau'' \leq \tau'$	\square	2730
2676	by H inversion (1)	Lemma 2.11 : H dynamic preservation	2731
2677	4. $\vdash_{\text{H}} \delta(\text{op}^2, v_0, v_1) : \tau''$	▮ If $\vdash_{\text{H}} e$ and $e \rightarrow_{\text{H-D}} e'$ then $\vdash_{\text{H}} e'$	2732
2678	by Δ <i>type soundness</i> (2)	<i>Proof</i> :	2733
2679	5. $\vdash_{\text{H}} \delta(\text{op}^2, v_0, v_1) : \tau'$	By the <i>boundary factoring</i> lemma, there are seven cases.	2734
2680	by (2, 3)	CASE e is a value :	2735
2681	6. QED by <i>hole substitution</i> (4)	1. Contradiction by $e \rightarrow_{\text{H-D}} e'$	2736
2682	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	CASE $e = E^\bullet[v_0 v_1] :$	2737
2683	IF e' is a value :	IF $v_0 = \lambda x. e'$	2738
2684	1. $e \rightarrow_{\text{H-S}} E[\mathcal{D}_{\text{H}}(\tau', e')]$	$\wedge e \rightarrow_{\text{H-D}} E^\bullet[e'[x \leftarrow v_1]] :$	2739
2685	2. $\vdash_{\text{H}} \text{dyn } \tau' e' : \tau'$	1. $\vdash_{\text{H}} v_0 v_1$	2740
2686	by <i>boundary hole typing</i>	by <i>dynamic hole typing</i>	2741
2687	3. $\vdash_{\text{H}} e'$	2. $\vdash_{\text{H}} v_0$	2742
2688	by H inversion (2)	$\wedge \vdash_{\text{H}} v_1$	2743
2689	4. $\vdash_{\text{H}} \mathcal{D}_{\text{H}}(\tau', e') : \tau'$	by H inversion (1)	2744
2690	by \mathcal{D}_{H} <i>soundness</i> (3)	3. $x \vdash_{\text{H}} e'$	2745
2691	5. QED by <i>hole substitution</i> (4)	by H inversion (2)	2746
2692	ELSE $e' \rightarrow_{\text{H-D}} e'' :$	4. $\vdash_{\text{H}} e'[x \leftarrow v_1]$	2747
2693	1. $e \rightarrow_{\text{H-S}} E[\text{dyn } \tau' e'']$	by <i>substitution</i> (2, 3)	2748
2694		5. QED <i>hole substitution</i> (4)	2749
2695			2750

2751	ELSE $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f$	4. $\vdash_{\text{H}} \mathcal{D}_{\text{H}}(\tau', e') : \tau'$	2806
2752	$\wedge e \rightarrow_{\text{H-D}} E^\bullet[\text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))]$:	by \mathcal{D}_{H} <i>soundness</i> (3)	2807
2753	1. $\vdash_{\text{H}} v_0 v_1$	5. QED by <i>hole substitution</i> (4)	2808
2754	by <i>dynamic hole typing</i>	ELSE $e' \rightarrow_{\text{H-D}} e''$:	2809
2755	2. $\vdash_{\text{H}} v_0$	1. $e \rightarrow_{\text{H-D}} E[\text{dyn } \tau' e'']$	2810
2756	$\wedge \vdash_{\text{H}} v_1$	2. $\vdash_{\text{H}} \text{dyn } \tau' e' : \tau'$	2811
2757	by H inversion (1)	by <i>boundary hole typing</i>	2812
2758	3. $\vdash_{\text{H}} v_f : \tau_d \Rightarrow \tau_c$	3. $\vdash_{\text{H}} e'$	2813
2759	by H inversion (2)	$\wedge \tau' \leq \tau''$	2814
2760	4. $\vdash_{\text{H}} \text{dyn } \tau_d v_1 : \tau_d$	by H inversion (2)	2815
2761	by (2)	4. $\vdash_{\text{H}} e''$	2816
2762	5. $\vdash_{\text{H}} v_f (\text{dyn } \tau_d v_1) : \tau_c$	by H dynamic preservation (3)	2817
2763	by (3, 4)	5. $\vdash_{\text{H}} \text{dyn } \tau' e'' : \tau'$	2818
2764	6. $\vdash_{\text{H}} \text{stat } \tau_c v_f (\text{dyn } \tau_d v_1)$	by (4)	2819
2765	by (5)	6. QED by <i>hole substitution</i> (5)	2820
2766	7. QED by <i>hole substitution</i>	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	2821
2767	CASE $e = E^\bullet[\text{op}^1 v]$:	IF $e' \in v$:	2822
2768	IF $v = \langle v_0, v_1 \rangle$	1. $e \rightarrow_{\text{H-D}} E[\mathcal{S}_{\text{H}}(\tau', e')]$	2823
2769	$\wedge \text{op}^1 = \text{fst}$	2. $\vdash_{\text{H}} \text{stat } \tau' e'$	2824
2770	$\wedge e \rightarrow_{\text{H-D}} E^\bullet[v_0]$:	by <i>boundary hole typing</i>	2825
2771	1. $\vdash_{\text{H}} \text{op}^1 v$	3. $\vdash_{\text{H}} e' : \tau'$	2826
2772	by <i>dynamic hole typing</i>	by H inversion (2)	2827
2773	2. $\vdash_{\text{H}} v$	4. $\vdash_{\text{H}} \mathcal{S}_{\text{H}}(\tau', e')$	2828
2774	by H inversion (1)	by \mathcal{S}_{H} <i>soundness</i> (3)	2829
2775	3. $\vdash_{\text{H}} v_0$	5. QED by <i>hole substitution</i> (5)	2830
2776	by H inversion (2)	ELSE $e' \rightarrow_{\text{H-S}} e''$:	2831
2777	4. QED by <i>hole substitution</i>	1. $e \rightarrow_{\text{H-D}} E[\text{stat } \tau' e'']$	2832
2778	ELSE $v = \langle v_0, v_1 \rangle$	2. $\vdash_{\text{H}} \text{stat } \tau' e'$	2833
2779	$\wedge \text{op}^1 = \text{snd}$	by <i>boundary hole typing</i>	2834
2780	$\wedge e \rightarrow_{\text{H-D}} E^\bullet[v_1]$:	3. $\vdash_{\text{H}} e' : \tau'$	2835
2781	1. $\vdash_{\text{H}} \text{op}^1 v$	by H inversion (2)	2836
2782	by <i>dynamic hole typing</i>	4. $\vdash_{\text{H}} e'' : \tau'$	2837
2783	2. $\vdash_{\text{H}} v$	by H static preservation (3)	2838
2784	by H inversion (1)	5. $\vdash_{\text{H}} \text{stat } \tau' e''$	2839
2785	3. $\vdash_{\text{H}} v_1$	by (4)	2840
2786	by H inversion (2)	6. QED by <i>hole substitution</i> (5)	2841
2787	4. QED by <i>hole substitution</i>	CASE $e = E[\text{Err}]$:	2842
2788	CASE $e = E^\bullet[\text{op}^2 v_0 v_1]$:	1. $e \rightarrow_{\text{H-D}} \text{Err}$	2843
2789	1. $e \rightarrow_{\text{H-D}} E^\bullet[\delta(\text{op}^2, v_0, v_1)]$	2. QED $\vdash_{\text{H}} \text{Err}$	2844
2790	2. $\vdash_{\text{H}} \text{op}^2 v_0 v_1$	□	2845
2791	by <i>dynamic hole typing</i>	Lemma 2.12 : H static boundary factoring	2846
2792	3. $\vdash_{\text{H}} v_0$	If $\vdash_{\text{H}} e : \tau$ then one of the following holds:	2847
2793	$\wedge \vdash_{\text{H}} v_1$	• e is a value	2848
2794	by H inversion (1)	• $e = E^\bullet[v_0 v_1]$	2849
2795	4. $\vdash_{\text{H}} \delta(\text{op}^2, v_0, v_1)$	• $e = E^\bullet[\text{op}^1 v]$	2850
2796	by δ <i>preservation</i> (2)	• $e = E^\bullet[\text{op}^2 v_0 v_1]$	2851
2797	5. QED by <i>hole substitution</i> (3)	• $e = E[\text{dyn } \tau e']$ where e' is boundary-free	2852
2798	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	• $e = E[\text{stat } \tau e']$ where e' is boundary-free	2853
2799	IF e' is a value :	• $e = E[\text{Err}]$	2854
2800	1. $e \rightarrow_{\text{H-D}} E[\mathcal{D}_{\text{H}}(\tau', e')]$	<i>Proof</i> :	2855
2801	2. $\vdash_{\text{H}} \text{dyn } \tau' e' : \tau'$	By the <i>unique static evaluation contexts</i> lemma, there are	2856
2802	by <i>boundary hole typing</i>	seven cases.	2857
2803	3. $\vdash_{\text{H}} e'$	CASE e is a value :	2858
2804	by H inversion (2)	1. QED	2859
2805			2860

<p>2971 1. $E = []$</p> <p>2972 2. QED $e = E[op^1 e_0]$</p> <p>2973 CASE $e = op^2 e_0 e_1$:</p> <p>2974 IF $e_0 \notin v$:</p> <p>2975 1. $\vdash_H e_0 : \tau_0$</p> <p>2976 by H inversion</p> <p>2977 2. $e_0 = E_0[e'_0]$</p> <p>2978 by the induction hypothesis (1)</p> <p>2979 3. $E = op^2 E_0 e_1$</p> <p>2980 4. QED $e = E[e'_0]$</p> <p>2981 IF $e_0 \in v$</p> <p>2982 $\wedge e_1 \notin v$:</p> <p>2983 1. $\vdash_H e_1 : \tau_1$</p> <p>2984 by H inversion</p> <p>2985 2. $e_1 = E_1[e'_1]$</p> <p>2986 by the induction hypothesis (1)</p> <p>2987 3. $E = op^2 e_0 E_1$</p> <p>2988 4. QED $e = E[e'_1]$</p> <p>2989 ELSE $e_0 \in v$</p> <p>2990 $\wedge e_1 \in v$:</p> <p>2991 1. $E = []$</p> <p>2992 2. QED $e = E[op^2 e_0 e_1]$</p> <p>2993 CASE $e = \text{dyn } \tau e_0$:</p> <p>2994 IF $e_0 \notin v$:</p> <p>2995 1. $\vdash_H e_0$</p> <p>2996 by H inversion</p> <p>2997 2. $e_0 = E_0[e'_0]$</p> <p>2998 by unique dynamic evaluation contexts (1)</p> <p>2999 3. $E = \text{dyn } \tau E_0$</p> <p>3000 4. QED $e = E[e'_0]$</p> <p>3001 ELSE $e_0 \in v$:</p> <p>3002 1. $E = []$</p> <p>3003 2. QED $e = E[\text{dyn } \tau e_0]$</p> <p>3004 CASE $e = \text{stat } \tau e_0$:</p> <p>3005 Contradiction by $\vdash_H e : \tau$</p> <p>3006 CASE $e = \text{Err}$:</p> <p>3007 1. $E = []$</p> <p>3008 2. QED $e = E[\text{Err}]$</p> <p>3009 \square</p> <p>3010 Lemma 2.14 : H inner boundary</p> <p>3011 For all contexts E, one of the following holds:</p> <p>3012 • $E = E^\bullet$</p> <p>3013 • $E = E'[\text{dyn } \tau E^\bullet]$</p> <p>3014 • $E = E'[\text{stat } \tau E^\bullet]$</p> <p>3015 <i>Proof</i>:</p> <p>3016 By induction on the structure of E.</p> <p>3017 CASE $E = E^\bullet$:</p> <p>3018 1. QED</p> <p>3019 CASE $E = E_0 e_1$:</p> <p>3020 1. $E_0 = E^\bullet$</p> <p>3021 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$</p> <p>3022 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$</p> <p>3023 by the induction hypothesis</p> <p>3024 2. IF $E_0 = E^\bullet$:</p> <p>3025</p>	<p>a. QED E is boundary-free</p> <p>IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:</p> <p>a. $E' = E'_0 e_1$</p> <p>b. QED $E = E'[\text{dyn } \tau E^\bullet]$</p> <p>ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:</p> <p>a. $E' = E'_0 e_1$</p> <p>b. QED $E = E'[\text{stat } \tau E^\bullet]$</p> <p>CASE $E = v_0 E_1$:</p> <p>1. $E_1 = E^\bullet$</p> <p>$\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$</p> <p>$\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$</p> <p>by the induction hypothesis</p> <p>2. IF $E_1 = E^\bullet$:</p> <p>a. QED E is boundary-free</p> <p>IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:</p> <p>a. $E' = v_0 E'_1$</p> <p>b. QED $E = E'[\text{dyn } \tau E^\bullet]$</p> <p>ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:</p> <p>a. $E' = v_0 E'_1$</p> <p>b. QED $E = E'[\text{stat } \tau E^\bullet]$</p> <p>CASE $E = \langle E_0, e_1 \rangle$:</p> <p>1. $E_0 = E^\bullet$</p> <p>$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$</p> <p>$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$</p> <p>by the induction hypothesis</p> <p>2. IF $E_0 = E^\bullet$:</p> <p>a. QED E is boundary-free</p> <p>IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:</p> <p>a. $E' = \langle E'_0, e_1 \rangle$</p> <p>b. QED $E = E'[\text{dyn } \tau E^\bullet]$</p> <p>ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:</p> <p>a. $E' = \langle E'_0, e_1 \rangle$</p> <p>b. QED $E = E'[\text{stat } \tau E^\bullet]$</p> <p>CASE $E = \langle v_0, E_1 \rangle$:</p> <p>1. $E_1 = E^\bullet$</p> <p>$\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$</p> <p>$\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$</p> <p>by the induction hypothesis</p> <p>2. IF $E_1 = E^\bullet$:</p> <p>a. QED E is boundary-free</p> <p>IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:</p> <p>a. $E' = \langle v_0, E'_1 \rangle$</p> <p>b. QED $E = E'[\text{dyn } \tau E^\bullet]$</p> <p>ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:</p> <p>a. $E' = \langle v_0, E'_1 \rangle$</p> <p>b. QED $E = E'[\text{stat } \tau E^\bullet]$</p> <p>CASE $E = op^1 E_0$:</p> <p>1. $E_0 = E^\bullet$</p> <p>$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$</p> <p>$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$</p> <p>by the induction hypothesis</p> <p>2. IF $E_0 = E^\bullet$:</p> <p>a. QED E is boundary-free</p> <p>IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:</p>	<p>3026</p> <p>3027</p> <p>3028</p> <p>3029</p> <p>3030</p> <p>3031</p> <p>3032</p> <p>3033</p> <p>3034</p> <p>3035</p> <p>3036</p> <p>3037</p> <p>3038</p> <p>3039</p> <p>3040</p> <p>3041</p> <p>3042</p> <p>3043</p> <p>3044</p> <p>3045</p> <p>3046</p> <p>3047</p> <p>3048</p> <p>3049</p> <p>3050</p> <p>3051</p> <p>3052</p> <p>3053</p> <p>3054</p> <p>3055</p> <p>3056</p> <p>3057</p> <p>3058</p> <p>3059</p> <p>3060</p> <p>3061</p> <p>3062</p> <p>3063</p> <p>3064</p> <p>3065</p> <p>3066</p> <p>3067</p> <p>3068</p> <p>3069</p> <p>3070</p> <p>3071</p> <p>3072</p> <p>3073</p> <p>3074</p> <p>3075</p> <p>3076</p> <p>3077</p> <p>3078</p> <p>3079</p> <p>3080</p>
---	---	---

3081 a. $E' = op^1 E'_0$
3082 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
3083 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
3084 a. $E' = op^1 E'_0$
3085 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
3086 **CASE** $E = op^2 E_0 e_1$:
3087 1. $E_0 = E^\bullet$
3088 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
3089 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
3090 by the induction hypothesis
3091 2. **IF** $E_0 = E^\bullet$:
3092 a. $\text{QED } E$ is boundary-free
3093 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
3094 a. $E' = op^2 E'_0 e_1$
3095 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
3096 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
3097 a. $E' = op^2 E'_0 e_1$
3098 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
3099 **CASE** $E = op^2 v_0 E_1$:
3100 1. $E_1 = E^\bullet$
3101 $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$
3102 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
3103 by the induction hypothesis
3104 2. **IF** $E_1 = E^\bullet$:
3105 a. $\text{QED } E$ is boundary-free
3106 **IF** $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
3107 a. $E' = op^2 v_0 E'_1$
3108 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
3109 **ELSE** $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
3110 a. $E' = op^2 v_0 E'_1$
3111 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
3112 **CASE** $E = \text{dyn } \tau E_0$:
3113 1. $E_0 = E^\bullet$
3114 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
3115 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
3116 by the induction hypothesis
3117 2. **IF** $E_0 = E^\bullet$:
3118 a. **QED**
3119 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
3120 a. $E' = \text{dyn } \tau E'_0$
3121 b. $\text{QED } E = E'[\text{dyn } \tau' E^\bullet]$
3122 **ELSE** $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
3123 a. $E' = \text{dyn } \tau E'_0$
3124 b. $\text{QED } E = E'[\text{stat } \tau' E^\bullet]$
3125 **CASE** $E = \text{stat } \tau E_0$:
3126 1. $E_0 = E^\bullet$
3127 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
3128 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
3129 by the induction hypothesis
3130 2. **IF** $E_0 = E^\bullet$:
3131 a. **QED**
3132 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
3133 a. $E' = \text{stat } \tau E'_0$

b. $\text{QED } E = E'[\text{dyn } \tau' E^\bullet]$
ELSE $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
a. $E' = \text{stat } \tau E'_0$
b. $\text{QED } E = E'[\text{stat } \tau' E^\bullet]$

□

Lemma 2.15 : H *dynamic boundary factoring*If $\vdash_H e$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[op^1 v]$
- $e = E^\bullet[op^2 v_0 v_1]$
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:By the *unique dynamic evaluation contexts* lemma, there are seven cases.**CASE** e is a value :1. **QED****CASE** $e = E[v_0 v_1]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. $\text{QED } e = E^\bullet[v_0 v_1]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$ **CASE** $e = E[op^1 v]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. $\text{QED } e = E^\bullet[op^1 v]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[op^1 v]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[op^1 v]]$ **CASE** $e = E[op^2 v_0 v_1]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. $\text{QED } e = E^\bullet[op^2 v_0 v_1]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[op^2 v_0 v_1]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[op^2 v_0 v_1]]$ **CASE** $e = E[\text{dyn } \tau v]$:1. **QED** v is boundary-free

3191	CASE $e = E[\text{stat } \tau v] :$	4. QED $e = E[e'_0]$	3246
3192	1. QED v is boundary-free	IF $e_0 \in v$	3247
3193	CASE $e = E[\text{Err}] :$	$\wedge e_1 \notin v :$	3248
3194	1. QED	1. $\vdash_H e_1$	3249
3195	□	by H inversion	3250
3196	Lemma 2.16 : H <i>unique dynamic evaluation contexts</i>	2. $e_1 = E_1[e'_1]$	3251
3197	If $\vdash_H e$ then one of the following holds:	by the induction hypothesis (1)	3252
3198	• e is a value	3. $E = e_0 E_1$	3253
3199	• $e = E[v_0 v_1]$	4. QED $e = E[e'_1]$	3254
3200	• $e = E[op^1 v]$	ELSE $e_0 \in v$	3255
3201	• $e = E[op^2 v_0 v_1]$	$\wedge e_1 \in v :$	3256
3202	• $e = E[\text{dyn } \tau v]$	1. $E = []$	3257
3203	• $e = E[\text{stat } \tau v]$	2. QED $e = E[e_0 e_1]$	3258
3204	• $e = E[\text{Err}]$	CASE $e = op^1 e_0 :$	3259
3205	<i>Proof</i> :	IF $e_0 \notin v :$	3260
3206	By induction on the structure of e .	1. $\vdash_H e_0$	3261
3207	CASE $e = x$	by H inversion	3262
3208	$\vee e = \lambda(x:\tau). e'$	2. $e_0 = E_0[e'_0]$	3263
3209	$\vee e = \text{dyn } \tau e' :$	by the induction hypothesis (1)	3264
3210	1. Contradiction by $\vdash_H e$	3. $E = op^1 E_0$	3265
3211	CASE $e = i$	4. QED $e = E[e'_0]$	3266
3212	$\vee e = \lambda x. e'$	ELSE $e_0 \in v :$	3267
3213	$\vee e = \text{mon}(\tau_d \Rightarrow \tau_c) v :$	1. $E = []$	3268
3214	1. QED e is a value	2. QED $e = E[op^1 e_0]$	3269
3215	CASE $e = \text{Err} :$	CASE $e = op^2 e_0 e_1 :$	3270
3216	1. $E = []$	IF $e_0 \notin v :$	3271
3217	2. QED $e = E[\text{Err}]$	1. $\vdash_H e_0$	3272
3218	CASE $e = \langle e_0, e_1 \rangle :$	by H inversion	3273
3219	IF $e_0 \notin v :$	2. $e_0 = E_0[e'_0]$	3274
3220	1. $\vdash_H e_0$	by the induction hypothesis (1)	3275
3221	by H inversion	3. $E = op^2 E_0 e_1$	3276
3222	2. $e_0 = E_0[e'_0]$	4. QED $e = E[e'_0]$	3277
3223	by the induction hypothesis (1)	IF $e_0 \in v$	3278
3224	3. $E = \langle E_0, e_1 \rangle$	$\wedge e_1 \notin v :$	3279
3225	4. QED $e = E[e'_0]$	1. $\vdash_H e_1$	3280
3226	IF $e_0 \in v$	by H inversion	3281
3227	$\wedge e_1 \notin v :$	2. $e_1 = E_1[e'_1]$	3282
3228	1. $\vdash_H e_1$	by the induction hypothesis (1)	3283
3229	by H inversion	3. $E = op^2 e_0 E_1$	3284
3230	2. $e_1 = E_1[e'_1]$	4. QED $e = E[e'_1]$	3285
3231	by the induction hypothesis (1)	ELSE $e_0 \in v$	3286
3232	3. $E = \langle e_0, E_1 \rangle$	$\wedge e_1 \in v :$	3287
3233	4. QED $e = E[e'_1]$	1. $E = []$	3288
3234	ELSE $e_0 \in v$	2. QED $e = E[op^2 e_0 e_1]$	3289
3235	$\wedge e_1 \in v :$	CASE $e = \text{stat } \tau e_0 :$	3290
3236	1. $E = []$	IF $e_0 \notin v :$	3291
3237	2. QED e is a value	1. $\vdash_H e_0$	3292
3238	CASE $e = e_0 e_1 :$	by H inversion	3293
3239	IF $e_0 \notin v :$	2. $e_0 = E_0[e'_0]$	3294
3240	1. $\vdash_H e_0$	by <i>unique static evaluation contexts</i> (1)	3295
3241	by H inversion	3. $E = \text{stat } \tau E_0$	3296
3242	2. $e_0 = E_0[e'_0]$	4. QED $e = E[e'_0]$	3297
3243	by the induction hypothesis (1)	ELSE $e_0 \in v :$	3298
3244	3. $E = E_0 e_1$	1. $E = []$	3299
3245			3300

3301 2. QED $e = E[\text{stat } \tau e_0]$

3302 \square

3303 **Lemma 2.17** : H *static hole typing*

3304 \blacksquare If $\vdash_{\text{H}} E^\bullet[e] : \tau$ then the derivation contains a sub-term $\vdash_{\text{H}} e : \tau'$

3305 *Proof*:

3306 By induction on the structure of E^\bullet .

3307 **CASE** $E^\bullet = []$:

3308 1. QED $E^\bullet[e] = e$

3309 **CASE** $E^\bullet = E^\bullet_0 e_1$:

3310 1. $E^\bullet[e] = E^\bullet_0[e] e_1$

3311 2. $\vdash_{\text{H}} E^\bullet_0[e] : \tau_d \Rightarrow \tau_c$

3312 by *H inversion*

3313 3. QED by the induction hypothesis (2)

3314 **CASE** $E^\bullet = v_0 E^\bullet_1$:

3315 1. $E^\bullet[e] = v_0 E^\bullet_1[e]$

3316 2. $\vdash_{\text{H}} E^\bullet_1[e] : \tau_d$

3317 by *H inversion*

3318 3. QED by the induction hypothesis (2)

3319 **CASE** $E^\bullet = \langle E^\bullet_0, e_1 \rangle$:

3320 1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$

3321 2. $\vdash_{\text{H}} E^\bullet_0[e] : \tau_0$

3322 by *H inversion*

3323 3. QED by the induction hypothesis (2)

3324 **CASE** $E^\bullet = \langle v_0, E^\bullet_1 \rangle$:

3325 1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$

3326 2. $\vdash_{\text{H}} E^\bullet_1[e] : \tau_1$

3327 by *H inversion*

3328 3. QED by the induction hypothesis (2)

3329 **CASE** $E^\bullet = op^1 E^\bullet_0$:

3330 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$

3331 2. $\vdash_{\text{H}} E^\bullet_0[e] : \tau_0$

3332 by *H inversion*

3333 3. QED by the induction hypothesis (2)

3334 **CASE** $E^\bullet = op^2 E^\bullet_0 e_1$:

3335 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$

3336 2. $\vdash_{\text{H}} E^\bullet_0[e] : \tau_0$

3337 by *H inversion*

3338 3. QED by the induction hypothesis (2)

3339 **CASE** $E^\bullet = op^2 v_0 E^\bullet_1$:

3340 1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$

3341 2. $\vdash_{\text{H}} E^\bullet_1[e] : \tau_1$

3342 by *H inversion*

3343 3. QED by the induction hypothesis (2)

3344 \square

3345 **Lemma 2.18** : H *dynamic hole typing*

3346 \blacksquare If $\vdash_{\text{H}} E^\bullet[e]$ then the derivation contains a sub-term $\vdash_{\text{H}} e$

3347 *Proof*:

3348 By induction on the structure of E^\bullet .

3349 **CASE** $E^\bullet = []$:

3350 1. QED $E^\bullet[e] = e$

3351 **CASE** $E^\bullet = E^\bullet_0 e_1$:

3352 1. $E^\bullet[e] = E^\bullet_0[e] e_1$

3354

3355

2. $\vdash_{\text{H}} E^\bullet_0[e]$

by *H inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = v_0 E^\bullet_1$:

1. $E^\bullet[e] = v_0 E^\bullet_1[e]$

2. $\vdash_{\text{H}} E^\bullet_1[e]$

by *H inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle$:

1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$

2. $\vdash_{\text{H}} E^\bullet_0[e]$

by *H inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle$:

1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$

2. $\vdash_{\text{H}} E^\bullet_1[e]$

by *H inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^1 E^\bullet_0$:

1. $E^\bullet[e] = op^1 E^\bullet_0[e]$

2. $\vdash_{\text{H}} E^\bullet_0[e]$

by *H inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^2 E^\bullet_0 e_1$:

1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$

2. $\vdash_{\text{H}} E^\bullet_0[e]$

by *H inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^2 v_0 E^\bullet_1$:

1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$

2. $\vdash_{\text{H}} E^\bullet_1[e]$

by *H inversion*

3. QED by the induction hypothesis (2)

\square

Lemma 2.19 : H *boundary hole typing*

\bullet If $\vdash_{\text{H}} E[\text{dyn } \tau e] : \tau'$ then the derivation contains a sub-term

$\vdash_{\text{H}} \text{dyn } \tau e : \tau$

\bullet If $\vdash_{\text{H}} E[\text{dyn } \tau e]$ then the derivation contains a sub-term

$\vdash_{\text{H}} \text{dyn } \tau e : \tau$

\bullet If $\vdash_{\text{H}} E[\text{stat } \tau e] : \tau'$ then the derivation contains a sub-term

$\vdash_{\text{H}} \text{stat } \tau e$

\bullet If $\vdash_{\text{H}} E[\text{stat } \tau e]$ then the derivation contains a sub-term

$\vdash_{\text{H}} \text{stat } \tau e$

Proof:

By the following four lemmas: *static dyn hole typing*,

dynamic dyn hole typing, *static stat hole typing*, and

dynamic stat hole typing.

\square

Lemma 2.20 : H *static dyn hole typing*

\blacksquare If $\vdash_{\text{H}} E[\text{dyn } \tau e] : \tau'$ then the derivation contains a sub-term

$\vdash_{\text{H}} \text{dyn } \tau e : \tau$.

Proof:

By induction on the structure of E .

3411 **CASE** $E \in E^\bullet$:
 3412 1. $\vdash_{\text{H}} \text{dyn } \tau e : \tau''$
 3413 by *static hole typing*
 3414 2. $\vdash_{\text{H}} \text{dyn } \tau e : \tau$
 3415 by *H inversion* (1)
 3416 3. QED
 3417 **CASE** $E = E_0 e_1$:
 3418 1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
 3419 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e] : \tau_0$
 3420 by *H inversion*
 3421 3. QED by the induction hypothesis (2)
 3422 **CASE** $E = v_0 E_1$:
 3423 1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
 3424 2. $\vdash_{\text{H}} E_1[\text{dyn } \tau e] : \tau_1$
 3425 by *H inversion*
 3426 3. QED by the induction hypothesis (2)
 3427 **CASE** $E = \langle E_0, e_1 \rangle$:
 3428 1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$
 3429 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e] : \tau_0$
 3430 by *H inversion*
 3431 3. QED by the induction hypothesis (2)
 3432 **CASE** $E = \langle v_0, E_1 \rangle$:
 3433 1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$
 3434 2. $\vdash_{\text{H}} E_1[\text{dyn } \tau e] : \tau_1$
 3435 by *H inversion*
 3436 3. QED by the induction hypothesis (2)
 3437 **CASE** $E = \text{op}^1 E_0$:
 3438 1. $E[\text{dyn } \tau e] = \text{op}^1 E_0[\text{dyn } \tau e]$
 3439 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e] : \tau_0$
 3440 by *H inversion*
 3441 3. QED by the induction hypothesis (2)
 3442 **CASE** $E = \text{op}^2 E_0 e_1$:
 3443 1. $E[\text{dyn } \tau e] = \text{op}^2 E_0[\text{dyn } \tau e] e_1$
 3444 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e] : \tau_0$
 3445 by *H inversion*
 3446 3. QED by the induction hypothesis (2)
 3447 **CASE** $E = \text{op}^2 v_0 E_1$:
 3448 1. $E[\text{dyn } \tau e] = \text{op}^2 v_0 E_1[\text{dyn } \tau e]$
 3449 2. $\vdash_{\text{H}} E_1[\text{dyn } \tau e] : \tau_1$
 3450 by *H inversion*
 3451 3. QED by the induction hypothesis (2)
 3452 **CASE** $E = \text{dyn } \tau_0 E_0$:
 3453 1. $E[\text{dyn } \tau e] = \text{dyn } \tau_0 E_0[\text{dyn } \tau e]$
 3454 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e] : \tau_0$
 3455 by *H inversion*
 3456 3. QED by *dynamic dyn hole typing* (2)
 3457 **CASE** $E = \text{stat } \tau_0 E_0$:
 3458 1. Contradiction by $\vdash_{\text{H}} E[\text{dyn } \tau e] : \tau'$
 3459 \square
 3460 **Lemma 2.21** : H *dynamic dyn hole typing*
 3461 If $\vdash_{\text{H}} E[\text{dyn } \tau e]$ then the derivation contains a sub-term
 3462 $\vdash_{\text{H}} \text{dyn } \tau e : \tau$.
 3463 *Proof*:

By induction on the structure of E .
CASE $E \in E^\bullet$:
 1. Contradiction by $\vdash_{\text{H}} E[\text{dyn } \tau e]$
CASE $E = E_0 e_1$:
 1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e]$
 by *H inversion*
 3. QED by the induction hypothesis (2)
CASE $E = v_0 E_1$:
 1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
 2. $\vdash_{\text{H}} E_1[\text{dyn } \tau e]$
 by *H inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle E_0, e_1 \rangle$:
 1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$
 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e]$
 by *H inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle v_0, E_1 \rangle$:
 1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$
 2. $\vdash_{\text{H}} E_1[\text{dyn } \tau e]$
 by *H inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{op}^1 E_0$:
 1. $E[\text{dyn } \tau e] = \text{op}^1 E_0[\text{dyn } \tau e]$
 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e]$
 by *H inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{op}^2 E_0 e_1$:
 1. $E[\text{dyn } \tau e] = \text{op}^2 E_0[\text{dyn } \tau e] e_1$
 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e]$
 by *H inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{op}^2 v_0 E_1$:
 1. $E[\text{dyn } \tau e] = \text{op}^2 v_0 E_1[\text{dyn } \tau e]$
 2. $\vdash_{\text{H}} E_1[\text{dyn } \tau e]$
 by *H inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{dyn } \tau E_0$:
 1. Contradiction by $\vdash_{\text{H}} E[\text{dyn } \tau e]$
CASE $E = \text{stat } \tau_0 E_0$:
 1. $E[\text{dyn } \tau e] = \text{stat } \tau_0 E_0[\text{dyn } \tau e]$
 2. $\vdash_{\text{H}} E_0[\text{dyn } \tau e] : \tau_0$
 by *H inversion*
 3. QED by *static dyn hole typing* (2)
 \square
Lemma 2.22 : H *static stat hole typing*
 If $\vdash_{\text{H}} E[\text{stat } \tau e] : \tau'$ then the derivation contains a sub-term
 $\vdash_{\text{H}} \text{stat } \tau e$.
Proof:
 By induction on the structure of E .
CASE $E \in E^\bullet$:
 1. Contradiction by $\vdash_{\text{H}} E[\text{stat } \tau e] : \tau'$

3521	CASE $E = E_0 e_1 :$	2. $\vdash_H E_0[\text{stat } \tau e]$	3576
3522	1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$	by H inversion	3577
3523	2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$	3. QED by the induction hypothesis (2)	3578
3524	by H inversion	CASE $E = v_0 E_1 :$	3579
3525	3. QED by the induction hypothesis (2)	1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$	3580
3526	CASE $E = v_0 E_1 :$	2. $\vdash_H E_1[\text{stat } \tau e]$	3581
3527	1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$	by H inversion	3582
3528	2. $\vdash_H E_1[\text{stat } \tau e] : \tau_1$	3. QED by the induction hypothesis (2)	3583
3529	by H inversion	CASE $E = \langle E_0, e_1 \rangle :$	3584
3530	3. QED by the induction hypothesis (2)	1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$	3585
3531	CASE $E = \langle E_0, e_1 \rangle :$	2. $\vdash_H E_0[\text{stat } \tau e]$	3586
3532	1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$	by H inversion	3587
3533	2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$	3. QED by the induction hypothesis (2)	3588
3534	by H inversion	CASE $E = \langle v_0, E_1 \rangle :$	3589
3535	3. QED by the induction hypothesis (2)	1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$	3590
3536	CASE $E = \langle v_0, E_1 \rangle :$	2. $\vdash_H E_1[\text{stat } \tau e]$	3591
3537	1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$	by H inversion	3592
3538	2. $\vdash_H E_1[\text{stat } \tau e] : \tau_1$	3. QED by the induction hypothesis (2)	3593
3539	by H inversion	CASE $E = op^1 E_0 :$	3594
3540	3. QED by the induction hypothesis (2)	1. $E[\text{stat } \tau e] = op^1 E_0[\text{stat } \tau e]$	3595
3541	CASE $E = op^1 E_0 :$	2. $\vdash_H E_0[\text{stat } \tau e]$	3596
3542	1. $E[\text{stat } \tau e] = op^1 E_0[\text{stat } \tau e]$	by H inversion	3597
3543	2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$	3. QED by the induction hypothesis (2)	3598
3544	by H inversion	CASE $E = op^2 E_0 e_1 :$	3599
3545	3. QED by the induction hypothesis (2)	1. $E[\text{stat } \tau e] = op^2 E_0[\text{stat } \tau e] e_1$	3600
3546	CASE $E = op^2 E_0 e_1 :$	2. $\vdash_H E_0[\text{stat } \tau e]$	3601
3547	1. $E[\text{stat } \tau e] = op^2 E_0[\text{stat } \tau e] e_1$	by H inversion	3602
3548	2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$	3. QED by the induction hypothesis (2)	3603
3549	by H inversion	CASE $E = op^2 v_0 E_1 :$	3604
3550	3. QED by the induction hypothesis (2)	1. $E[\text{stat } \tau e] = op^2 v_0 E_1[\text{stat } \tau e]$	3605
3551	CASE $E = op^2 v_0 E_1 :$	2. $\vdash_H E_1[\text{stat } \tau e]$	3606
3552	1. $E[\text{stat } \tau e] = op^2 v_0 E_1[\text{stat } \tau e]$	by H inversion	3607
3553	2. $\vdash_H E_1[\text{stat } \tau e] : \tau_1$	3. QED by the induction hypothesis (2)	3608
3554	by H inversion	CASE $E = \text{dyn } \tau E_0 :$	3609
3555	3. QED by the induction hypothesis (2)	1. Contradiction by $\vdash_H E[\text{stat } \tau e]$	3610
3556	CASE $E = \text{dyn } \tau_0 E_0 :$	CASE $E = \text{stat } \tau_0 E_0 :$	3611
3557	1. $E[\text{stat } \tau e] = \text{dyn } \tau_0 E_0[\text{stat } \tau e]$	1. $E[\text{stat } \tau e] = \text{stat } \tau_0 E_0[\text{stat } \tau e]$	3612
3558	2. $\vdash_H E_0[\text{stat } \tau e]$	2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$	3613
3559	by H inversion	by H inversion	3614
3560	3. QED by <i>dynamic stat hole typing</i> (2)	3. QED by <i>static stat hole typing</i> (2)	3615
3561	CASE $E = \text{stat } \tau_0 E_0 :$	□	3616
3562	1. Contradiction by $\vdash_H E[\text{stat } \tau e] : \tau'$	Lemma 2.24 : H <i>static boundary-free hole substitution</i>	3617
3563	□	If $\vdash_H E^\bullet[e] : \tau$ and the derivation contains a sub-term $\vdash_H e : \tau'$	3618
3564	Lemma 2.23 : H <i>dynamic stat hole typing</i>	and $\vdash_H e' : \tau'$ then $\vdash_H E^\bullet[e'] : \tau$.	3619
3565	If $\vdash_H E[\text{stat } \tau e]$ then the derivation contains a sub-term	<i>Proof</i> :	3620
3566	$\vdash_H \text{stat } \tau e$.	By induction on the structure of E^\bullet	3621
3567	<i>Proof</i> :	CASE $E^\bullet = [] :$	3622
3568	By induction on the structure of E .	1. $E^\bullet[e] = e$	3623
3569	CASE $E \in E^\bullet :$	$\wedge E^\bullet[e'] = e'$	3624
3570	1. QED by <i>dynamic hole typing</i>	2. $\vdash_H e : \tau$	3625
3571	CASE $E = E_0 e_1 :$	by (1)	3626
3572	1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$	3. $\tau' = \tau$	3627
3573		4. $\vdash_H e' : \tau$	3628
3574			3629
3575			3630

3741	1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$	4. $\vdash_H E^\bullet_0[e']$	3796
3742	$\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$	by the induction hypothesis (3)	3797
3743	2. $\vdash_H \langle v_0, E^\bullet_1[e] \rangle$	5. $\vdash_H op^2 E^\bullet_0[e'] e_1$	3798
3744	3. $\vdash_H v_0$	by (3, 4)	3799
3745	$\wedge \vdash_H E^\bullet_1[e]$	6. QED by (1, 5)	3800
3746	by <i>H inversion</i>	CASE $E^\bullet = op^2 v_0 E^\bullet_1 :$	3801
3747	4. $\vdash_H E^\bullet_1[e']$	1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$	3802
3748	by the induction hypothesis (3)	$\wedge E^\bullet[e'] = op^2 v_0 E^\bullet_1[e']$	3803
3749	5. $\vdash_H \langle v_0, E^\bullet_1[e'] \rangle$	2. $\vdash_H op^2 v_0 E^\bullet_1[e]$	3804
3750	by (3, 4)	3. $\vdash_H v_0$	3805
3751	6. QED by (1, 5)	$\wedge \vdash_H E^\bullet_1[e]$	3806
3752	CASE $E^\bullet = E^\bullet_0 e_1 :$	by <i>H inversion</i>	3807
3753	1. $E^\bullet[e] = E^\bullet_0[e] e_1$	4. $\vdash_H E^\bullet_1[e']$	3808
3754	$\wedge E^\bullet[e'] = E^\bullet_0[e'] e_1$	by the induction hypothesis (3)	3809
3755	2. $\vdash_H E^\bullet_0[e] e_1$	5. $\vdash_H op^2 v_0 E^\bullet_1[e']$	3810
3756	3. $\vdash_H E^\bullet_0[e]$	by (3, 4)	3811
3757	$\wedge \vdash_H e_1$	6. QED by (1, 5)	3812
3758	by <i>H inversion</i>	□	3813
3759	4. $\vdash_H E^\bullet_0[e']$	Lemma 2.26 : <i>H hole substitution</i>	3814
3760	by the induction hypothesis (3)	• If $\vdash_H E[e]$ and the derivation contains a sub-term $\vdash_H e : \tau'$	3815
3761	5. $\vdash_H E^\bullet_0[e'] e_1$	and $\vdash_H e' : \tau'$ then $\vdash_H E[e']$.	3816
3762	by (3, 4)	• If $\vdash_H E[e]$ and the derivation contains a sub-term $\vdash_H e$ and	3817
3763	6. QED by (1, 5)	$\vdash_H e'$ then $\vdash_H E[e']$.	3818
3764	CASE $E^\bullet = v_0 E^\bullet_1 :$	• If $\vdash_H E[e] : \tau$ and the derivation contains a sub-term $\vdash_H e :$	3819
3765	1. $E^\bullet[e] = v_0 E^\bullet_1[e]$	τ' and $\vdash_H e' : \tau'$ then $\vdash_H E[e'] : \tau$.	3820
3766	$\wedge E^\bullet[e'] = v_0 E^\bullet_1[e']$	• If $\vdash_H E[e] : \tau$ and the derivation contains a sub-term $\vdash_H e$	3821
3767	2. $\vdash_H v_0 E^\bullet_1[e]$	and $\vdash_H e'$ then $\vdash_H E[e'] : \tau$.	3822
3768	3. $\vdash_H v_0$	<i>Proof</i> :	3823
3769	$\wedge \vdash_H E^\bullet_1[e]$	By the following four lemmas: <i>dynamic context static hole</i>	3824
3770	by <i>H inversion</i>	<i>substitution</i> , <i>dynamic context dynamic hole substitution</i> ,	3825
3771	4. $\vdash_H E^\bullet_1[e']$	<i>static context static hole substitution</i> , and <i>static context</i>	3826
3772	by the induction hypothesis (3)	<i>dynamic hole substitution</i> .	3827
3773	5. $\vdash_H v_0 E^\bullet_1[e']$	□	3828
3774	by (3, 4)	Lemma 2.27 : <i>H dynamic context static hole substitution</i>	3829
3775	6. QED by (1, 5)	If $\vdash_H E[e]$ and contains $\vdash_H e : \tau'$, and furthermore $\vdash_H e' : \tau'$,	3830
3776	CASE $E^\bullet = op^1 E^\bullet_0 :$	then $\vdash_H E[e']$	3831
3777	1. $E^\bullet[e] = op^1 E^\bullet_0[e]$	<i>Proof</i> :	3832
3778	$\wedge E^\bullet[e'] = op^1 E^\bullet_0[e']$	By induction on the structure of E .	3833
3779	2. $\vdash_H op^1 E^\bullet_0[e]$	CASE $E \in E^\bullet :$	3834
3780	3. $\vdash_H E^\bullet_0[e]$	1. Contradiction by $\vdash_H E[e]$	3835
3781	by <i>H inversion</i>	CASE $E = E_0 e_1 :$	3836
3782	4. $\vdash_H E^\bullet_0[e']$	1. $E[e] = E_0[e] e_1$	3837
3783	by the induction hypothesis (3)	2. $\vdash_H E_0[e]$	3838
3784	5. $\vdash_H op^1 E^\bullet_0[e']$	by <i>H inversion</i>	3839
3785	by (4)	3. QED by the induction hypothesis (2)	3840
3786	6. QED by (1, 5)	CASE $E = v_0 E_1 :$	3841
3787	CASE $E^\bullet = op^2 E^\bullet_0 e_1 :$	1. $E[e] = v_0 E_1[e]$	3842
3788	1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$	2. $\vdash_H E_1[e]$	3843
3789	$\wedge E^\bullet[e'] = op^2 E^\bullet_0[e'] e_1$	by <i>H inversion</i>	3844
3790	2. $\vdash_H op^2 E^\bullet_0[e] e_1$	3. QED by the induction hypothesis (2)	3845
3791	3. $\vdash_H E^\bullet_0[e]$	CASE $E = \langle E_0, e_1 \rangle :$	3846
3792	$\wedge \vdash_H e_1$	1. $E[e] = \langle E_0[e], e_1 \rangle$	3847
3793	by <i>H inversion</i>		3848
3794			3849
3795			3850

3851 2. $\vdash_H E_0[e]$
 3852 by *H inversion*
 3853 3. QED by the induction hypothesis (2)
 3854 **CASE** $E = \langle v_0, E_1 \rangle :$
 3855 1. $E[e] = \langle v_0, E_1[e] \rangle$
 3856 2. $\vdash_H E_1[e]$
 3857 by *H inversion*
 3858 3. QED by the induction hypothesis (2)
 3859 **CASE** $E = op^1 E_0 :$
 3860 1. $E[e] = op^1 E_0[e]$
 3861 2. $\vdash_H E_0[e]$
 3862 by *H inversion*
 3863 3. QED by the induction hypothesis (2)
 3864 **CASE** $E = op^2 E_0 e_1 :$
 3865 1. $E[e] = op^2 E_0[e] e_1$
 3866 2. $\vdash_H E_0[e]$
 3867 by *H inversion*
 3868 3. QED by the induction hypothesis (2)
 3869 **CASE** $E = op^2 v_0 E_1 :$
 3870 1. $E[e] = op^2 v_0 E_1[e]$
 3871 2. $\vdash_H E_1[e]$
 3872 by *H inversion*
 3873 3. QED by the induction hypothesis (2)
 3874 **CASE** $E = dyn \tau'' E_0 :$
 3875 1. Contradiction by $\vdash_H E[e]$
 3876 **CASE** $E = stat \tau_0 E_0 :$
 3877 1. $E[e] = stat \tau_0 E_0[e]$
 3878 2. $\vdash_H E_0[e] : \tau_0$
 3879 by *H inversion*
 3880 3. QED by *static context static hole substitution* (2)
 3881 \square
 3882 **Lemma 2.28** : *H dynamic context dynamic hole substitution*
 3883 If $\vdash_H E[e]$ and contains $\vdash_H e$, and furthermore $\vdash_H e' : \tau'$, then
 3884 $\vdash_H E[e']$
 3885 *Proof*:
 3886 By induction on the structure of E .
 3887 **CASE** $E \in E^* :$
 3888 1. QED by *dynamic boundary-free hole substitution*
 3889 **CASE** $E = E_0 e_1 :$
 3890 1. $E[e] = E_0[e] e_1$
 3891 2. $\vdash_H E_0[e]$
 3892 by *H inversion*
 3893 3. QED by the induction hypothesis (2)
 3894 **CASE** $E = v_0 E_1 :$
 3895 1. $E[e] = v_0 E_1[e]$
 3896 2. $\vdash_H E_1[e]$
 3897 by *H inversion*
 3898 3. QED by the induction hypothesis (2)
 3899 **CASE** $E = \langle E_0, e_1 \rangle :$
 3900 1. $E[e] = \langle E_0[e], e_1 \rangle$
 3901 2. $\vdash_H E_0[e]$
 3902 by *H inversion*
 3903 3. QED by the induction hypothesis (2)
 3904
 3905

CASE $E = \langle v_0, E_1 \rangle :$
 3906 1. $E[e] = \langle v_0, E_1[e] \rangle$
 3907 2. $\vdash_H E_1[e]$
 3908 by *H inversion*
 3909 3. QED by the induction hypothesis (2)
 3910 **CASE** $E = op^1 E_0 :$
 3911 1. $E[e] = op^1 E_0[e]$
 3912 2. $\vdash_H E_0[e]$
 3913 by *H inversion*
 3914 3. QED by the induction hypothesis (2)
 3915 **CASE** $E = op^2 E_0 e_1 :$
 3916 1. $E[e] = op^2 E_0[e] e_1$
 3917 2. $\vdash_H E_0[e]$
 3918 by *H inversion*
 3919 3. QED by the induction hypothesis (2)
 3920 **CASE** $E = op^2 v_0 E_1 :$
 3921 1. $E[e] = op^2 v_0 E_1[e]$
 3922 2. $\vdash_H E_1[e]$
 3923 by *H inversion*
 3924 3. QED by the induction hypothesis (2)
 3925 **CASE** $E = dyn \tau'' E_0 :$
 3926 1. Contradiction by $\vdash_H E[e]$
 3927 **CASE** $E = stat \tau_0 E_0 :$
 3928 1. $E[e] = stat \tau_0 E_0[e]$
 3929 2. $\vdash_H E_0[e] : \tau_0$
 3930 by *H inversion*
 3931 3. QED by *static context dynamic hole substitution* (2)
 3932 \square
 3933 **Lemma 2.29** : *H static context static hole substitution*
 3934 If $\vdash_H E[e] : \tau$ and contains $\vdash_H e : \tau'$, and furthermore $\vdash_H e' : \tau'$,
 3935 then $\vdash_H E[e'] : \tau$
 3936 *Proof*:
 3937 By induction on the structure of E .
 3938 **CASE** $E \in E^* :$
 3939 1. QED by *static boundary-free hole substitution*
 3940 **CASE** $E = E_0 e_1 :$
 3941 1. $E[e] = E_0[e] e_1$
 3942 2. $\vdash_H E_0[e] : \tau_0$
 3943 by *H inversion*
 3944 3. QED by the induction hypothesis (2)
 3945 **CASE** $E = v_0 E_1 :$
 3946 1. $E[e] = v_0 E_1[e]$
 3947 2. $\vdash_H E_1[e] : \tau_1$
 3948 by *H inversion*
 3949 3. QED by the induction hypothesis (2)
 3950 **CASE** $E = \langle E_0, e_1 \rangle :$
 3951 1. $E[e] = \langle E_0[e], e_1 \rangle$
 3952 2. $\vdash_H E_0[e] : \tau_0$
 3953 by *H inversion*
 3954 3. QED by the induction hypothesis (2)
 3955 **CASE** $E = \langle v_0, E_1 \rangle :$
 3956 1. $E[e] = \langle v_0, E_1[e] \rangle$
 3957

3961 2. $\vdash_H E_1[e] : \tau_1$
 3962 by *H inversion*
 3963 3. QED by the induction hypothesis (2)
 3964 **CASE** $E = op^1 E_0 :$
 3965 1. $E[e] = op^1 E_0[e]$
 3966 2. $\vdash_H E_0[e] : \tau_0$
 3967 by *H inversion*
 3968 3. QED by the induction hypothesis (2)
 3969 **CASE** $E = op^2 E_0 e_1 :$
 3970 1. $E[e] = op^2 E_0[e] e_1$
 3971 2. $\vdash_H E_0[e] : \tau_0$
 3972 by *H inversion*
 3973 3. QED by the induction hypothesis (2)
 3974 **CASE** $E = op^2 v_0 E_1 :$
 3975 1. $E[e] = op^2 v_0 E_1[e]$
 3976 2. $\vdash_H E_1[e] : \tau_1$
 3977 by *H inversion*
 3978 3. QED by the induction hypothesis (2)
 3979 **CASE** $E = dyn \tau_0 E_0 :$
 3980 1. $E[e] = dyn \tau_0 E_0[e]$
 3981 2. $\vdash_H E_0[e]$
 3982 by *H inversion*
 3983 3. QED by *static dyn hole typing* (2)
 3984 **CASE** $E = stat \tau_0 E_0 :$
 3985 1. Contradiction by $\vdash_H E[e] : \tau$
 3986 \square
 3987 **Lemma 2.30** : *H static context dynamic hole substitution*
 3988 If $\vdash_H E[e] : \tau$ and contains $\vdash_H e$, and furthermore $\vdash_H e'$, then
 3989 $\vdash_H E[e'] : \tau$
 3990 *Proof*:
 3991 By induction on the structure of E .
 3992 **CASE** $E \in E^\bullet :$
 3993 1. Contradiction by $\vdash_H E[e] : \tau$
 3994 **CASE** $E = E_0 e_1 :$
 3995 1. $E[e] = E_0[e] e_1$
 3996 2. $\vdash_H E_0[e] : \tau_0$
 3997 by *H inversion*
 3998 3. QED by the induction hypothesis (2)
 3999 **CASE** $E = v_0 E_1 :$
 4000 1. $E[e] = v_0 E_1[e]$
 4001 2. $\vdash_H E_1[e] : \tau_1$
 4002 by *H inversion*
 4003 3. QED by the induction hypothesis (2)
 4004 **CASE** $E = \langle E_0, e_1 \rangle :$
 4005 1. $E[e] = \langle E_0[e], e_1 \rangle$
 4006 2. $\vdash_H E_0[e] : \tau_0$
 4007 by *H inversion*
 4008 3. QED by the induction hypothesis (2)
 4009 **CASE** $E = \langle v_0, E_1 \rangle :$
 4010 1. $E[e] = \langle v_0, E_1[e] \rangle$
 4011 2. $\vdash_H E_1[e] : \tau_1$
 4012 by *H inversion*
 4013 3. QED by the induction hypothesis (2)
 4014
 4015

CASE $E = op^1 E_0 :$ 4016
 1. $E[e] = op^1 E_0[e]$ 4017
 2. $\vdash_H E_0[e] : \tau_0$ 4018
 by *H inversion* 4019
 3. QED by the induction hypothesis (2) 4020
CASE $E = op^2 E_0 e_1 :$ 4021
 1. $E[e] = op^2 E_0[e] e_1$ 4022
 2. $\vdash_H E_0[e] : \tau_0$ 4023
 by *H inversion* 4024
 3. QED by the induction hypothesis (2) 4025
CASE $E = op^2 v_0 E_1 :$ 4026
 1. $E[e] = op^2 v_0 E_1[e]$ 4027
 2. $\vdash_H E_1[e] : \tau_1$ 4028
 by *H inversion* 4029
 3. QED by the induction hypothesis (2) 4030
CASE $E = dyn \tau_0 E_0 :$ 4031
 1. $E[e] = dyn \tau_0 E_0[e]$ 4032
 2. $\vdash_H E_0[e]$ 4033
 by *H inversion* 4034
 3. QED by *dynamic stat hole typing* (2) 4035
CASE $E = stat \tau_0 E_0 :$ 4036
 1. Contradiction by $\vdash_H E[e] : \tau$ 4037
 \square 4038

Lemma 2.31 : \vdash_H static inversion

- If $\Gamma \vdash_H x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$ 4040
- If $\Gamma \vdash_H \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash_H e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$ 4041
- If $\Gamma \vdash_H \langle e_0, e_1 \rangle : \tau$ then $\Gamma \vdash_H e_0 : \tau_0$ and $\Gamma \vdash_H e_1 : \tau_1$ and $\tau_0 \times \tau_1 \leq \tau$ 4042
- If $\Gamma \vdash_H e_0 e_1 : \tau_c$ then $\Gamma \vdash_H e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash_H e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$ 4043
- If $\Gamma \vdash_H fst e : \tau$ then $\Gamma \vdash_H e : \tau_0 \times \tau_1$ and $\Delta(fst, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$ 4044
- If $\Gamma \vdash_H snd e : \tau$ then $\Gamma \vdash_H e : \tau_0 \times \tau_1$ and $\Delta(snd, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$ 4045
- If $\Gamma \vdash_H op^2 e_0 e_1 : \tau$ then $\Gamma \vdash_H e_0 : \tau_0$ and $\Gamma \vdash_H e_1 : \tau_1$ and $\Delta(op^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$ 4046
- If $\Gamma \vdash_H mon \tau_d \Rightarrow \tau_c v' : \tau$ then $\Gamma \vdash_H v'$ and $\tau_d \Rightarrow \tau_c \leq \tau$ 4047
- If $\Gamma \vdash_H dyn \tau' e' : \tau$ then $\Gamma \vdash_H e'$ and $\tau' \leq \tau$ 4048

Proof:QED by the definition of $\Gamma \vdash_H e : \tau$ \square **Lemma 2.32** : \vdash_H dynamic inversion

- If $\Gamma \vdash_H x$ then $x \in \Gamma$ 4049
- If $\Gamma \vdash_H \lambda x. e'$ then $x, \Gamma \vdash_H e'$ 4050
- If $\Gamma \vdash_H \langle e_0, e_1 \rangle$ then $\Gamma \vdash_H e_0$ and $\Gamma \vdash_H e_1$ 4051
- If $\Gamma \vdash_H e_0 e_1$ then $\Gamma \vdash_H e_0$ and $\Gamma \vdash_H e_1$ 4052
- If $\Gamma \vdash_H op^1 e_0$ then $\Gamma \vdash_H e_0$ 4053
- If $\Gamma \vdash_H op^2 e_0 e_1$ then $\Gamma \vdash_H e_0$ and $\Gamma \vdash_H e_1$ 4054
- If $\Gamma \vdash_H mon \tau_d \Rightarrow \tau_c v'$ then $\Gamma \vdash_H v' : \tau_d \Rightarrow \tau_c$ 4055
- If $\Gamma \vdash_H stat \tau' e'$ then $\Gamma \vdash_H e' : \tau'$ 4056

Proof:QED by the definition of $\Gamma \vdash_H e$

4071 \square

 4072 **Lemma 2.33** : H *canonical forms*

- 4073 • If
- $\vdash_{\text{H}} v : \tau_0 \times \tau_1$
- then
- $v = \langle v_0, v_1 \rangle$
-
- 4074 • If
- $\vdash_{\text{H}} v : \tau_d \Rightarrow \tau_c$
- then either:
-
- 4075
- $v = \lambda(x:\tau_x). e'$
-
- 4076
- $\wedge \tau_d \leq \tau_x$
-
- 4077 – or
- $v = \text{mon}(\tau'_d \Rightarrow \tau'_c) v'$
-
- 4078
- $\wedge \tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
-
- 4079 • If
- $\vdash_{\text{H}} v : \text{Int}$
- then
- $v \in i$
-
- 4080 • If
- $\vdash_{\text{H}} v : \text{Nat}$
- then
- $v \in \mathbb{N}$

 4081 *Proof*:

 4082 QED by definition of $\vdash_{\text{H}} e : \tau$

 4083 \square

 4084 **Lemma 2.34** : Δ *type soundness*

 4085 If $\vdash_{\text{H}} v_0 : \tau_0$ and $\vdash_{\text{H}} v_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau$ then \vdash_{H}
 4086 $\delta(\text{op}^2, v_0, v_1) : \tau$.

 4087 *Proof*:

 4088 By case analysis on the definition of Δ .

 4089 **CASE** $\Delta(\text{sum}, \text{Nat}, \text{Nat}) = \text{Nat}$:

- 4090 1.
- $v_0 = i_0, i_0 \in \mathbb{N}$
-
- 4091
- $\wedge v_1 = i_1, i_1 \in \mathbb{N}$
-
- 4092 by
- canonical forms*
-
- 4093 2.
- $\delta(\text{sum}, i_0, i_1) = i_0 + i_1 \in \mathbb{N}$
-
- 4094 3. QED

 4095 **CASE** $\Delta(\text{sum}, \text{Int}, \text{Int}) = \text{Int}$:

- 4096 1.
- $v_0 = i_0$
-
- 4097
- $\wedge v_1 = i_1$
-
- 4098 by
- canonical forms*
-
- 4099 2.
- $\delta(\text{sum}, i_0, i_1) = i_0 + i_1 \in i$
-
- 4100 3. QED

 4101 **CASE** $\Delta(\text{quotient}, \text{Nat}, \text{Nat}) = \text{Nat}$:

- 4102 1.
- $v_0 = i_0, i_0 \in \mathbb{N}$
-
- 4103
- $\wedge v_1 = i_1, i_1 \in \mathbb{N}$
-
- 4104 by
- canonical forms*
-
- 4105 2.
- IF**
- $i_1 = 0$
- :
-
- 4106 a.
- $\delta(\text{quotient}, i_0, i_1) = \text{BndryErr}$
-
- 4107 b. QED by
- $\vdash_{\text{H}} \text{BndryErr} : \tau$
-
- 4108
- ELSE**
- $i_1 \neq 0$
- :
-
- 4109 a.
- $\delta(\text{quotient}, i_0, i_1) = [i_0/i_1] \in \mathbb{N}$
-
- 4110 b. QED

 4111 **CASE** $\Delta(\text{quotient}, \text{Int}, \text{Int}) = \text{Int}$:

- 4112 1.
- $v_0 = i_0$
-
- 4113
- $\wedge v_1 = i_1$
-
- 4114 by
- canonical forms*
-
- 4115 2.
- IF**
- $i_1 = 0$
- :
-
- 4116 a.
- $\delta(\text{quotient}, i_0, i_1) = \text{BndryErr}$
-
- 4117 b. QED by
- $\vdash_{\text{H}} \text{BndryErr} : \tau$
-
- 4118
- ELSE**
- $i_1 \neq 0$
- :
-
- 4119 a.
- $\delta(\text{quotient}, i_0, i_1) = [i_0/i_1] \in i$
-
- 4120 b. QED

 4121 \square

 4122 **Lemma 2.35** : δ *preservation*

4123

4124

4125

 • If $\vdash_{\text{H}} v$ and $\delta(\text{op}^1, v) = e$ then $\vdash_{\text{H}} e$ 4126

 • If $\vdash_{\text{H}} v_0$ and $\vdash_{\text{H}} v_1$ and $\delta(\text{op}^2, v_0, v_1) = e$ then $\vdash_{\text{H}} e$ 4127

Proof: 4128

CASE $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$: 4129

 1. $\vdash_{\text{H}} v_0$ 4130

 by *H inversion* 4131

2. QED 4132

CASE $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$: 4133

 1. $\vdash_{\text{H}} v_1$ 4134

 by *H inversion* 4135

2. QED 4136

CASE $\delta(\text{sum}, v_0, v_1) = v_0 + v_1$: 4137

1. QED 4138

CASE $\delta(\text{quotient}, v_0, v_1) = [v_0/v_1]$: 4139

1. QED 4140

CASE $\delta(\text{op}^2, v_0, v_1) = \text{BndryErr}$: 4141

1. QED 4142

 \square 4143

Lemma 2.36 : H *substitution* 4144

 • If $(x:\tau_x), \Gamma \vdash_{\text{H}} e$ and $\vdash_{\text{H}} v : \tau_x$ then $\Gamma \vdash_{\text{H}} e[x \leftarrow v]$ 4145

 • If $x, \Gamma \vdash_{\text{H}} e$ and $\vdash_{\text{H}} v$ then $\Gamma \vdash_{\text{H}} e[x \leftarrow v]$ 4146

 • If $(x:\tau_x), \Gamma \vdash_{\text{H}} e : \tau$ and $\vdash_{\text{H}} v : \tau_x$ then $\Gamma \vdash_{\text{H}} e[x \leftarrow v] : \tau$ 4147

 • If $x, \Gamma \vdash_{\text{H}} e : \tau$ and $\vdash_{\text{H}} v$ then $\Gamma \vdash_{\text{H}} e[x \leftarrow v] : \tau$ 4148

Proof: 4149

 By the following four lemmas: *dynamic context static* 4150

value substitution, dynamic context dynamic value substi- 4151

tution, static context static value substitution, and static 4152

context dynamic value substitution. 4153

 \square 4154

Lemma 2.37 : H *dynamic-static substitution* 4155

 If $(x:\tau_x), \Gamma \vdash_{\text{H}} e$ and $\vdash_{\text{H}} v : \tau_x$ then $\Gamma \vdash_{\text{H}} e[x \leftarrow v]$ 4156

Proof: 4157

 By induction on the structure of e . 4158

CASE $e = x$: 4159

 1. Contradiction by $(x:\tau_x), \Gamma \vdash_{\text{H}} x$ 4160

CASE $e = x'$: 4161

 1. QED by $(x'[x \leftarrow v]) = x'$ 4162

CASE $e = i$: 4163

 1. QED by $i[x \leftarrow v] = i$ 4164

CASE $e = \lambda x'. e'$: 4165

 1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$ 4166

 2. $x', (x:\tau_x), \Gamma \vdash_{\text{H}} e'$ 4167

 by *H inversion* 4168

 3. $x', \Gamma \vdash_{\text{H}} e'[x \leftarrow v]$ 4169

by the induction hypothesis (2) 4170

 4. $\Gamma \vdash_{\text{H}} \lambda x'. (e'[x \leftarrow v])$ 4171

by (3) 4172

5. QED 4173

CASE $e = \lambda(x':\tau'). e'$: 4174

 1. Contradiction by $(x:\tau_x), \Gamma \vdash_{\text{H}} e$ 4175

CASE $e = \text{mon}(\tau_d \Rightarrow \tau_c) v'$: 4176

 1. $e[x \leftarrow v] = \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$ 4177

4178

4179

4180

4181	2. $(x : \tau_x), \Gamma \vdash_H v' : \tau_d \Rightarrow \tau_c$	3. $\Gamma \vdash_H e'[x \leftarrow v] : \tau'$	4236
4182	by <i>H inversion</i>	by <i>static context static value substitution</i> (2)	4237
4183	3. $\Gamma \vdash_H v'[x \leftarrow v] : \tau_d \Rightarrow \tau_c$	4. $\Gamma \vdash_H \text{stat } \tau' e'[x \leftarrow v]$	4238
4184	by <i>static context static value substitution</i> (2)	by (3)	4239
4185	4. $\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$	5. QED	4240
4186	by (3)	CASE $e = \text{Err}$:	4241
4187	5. QED	1. QED $\text{Err} = \text{Err}[x \leftarrow v]$	4242
4188	CASE $e = \langle e_0, e_1 \rangle$:	□	4243
4189	1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	Lemma 2.38 : <i>H dynamic-dynamic substitution</i>	4244
4190	2. $(x : \tau_x), \Gamma \vdash_H e_0$	▮ If $x, \Gamma \vdash_H e$ and $\vdash_H v$ then $\Gamma \vdash_H e[x \leftarrow v]$	4245
4191	$\wedge (x : \tau_x), \Gamma \vdash_H e_1$	<i>Proof</i> :	4246
4192	by <i>H inversion</i>	By induction on the structure of e	4247
4193	3. $\Gamma \vdash_H e_0[x \leftarrow v]$	CASE $e = x$:	4248
4194	$\wedge \Gamma \vdash_H e_1[x \leftarrow v]$	1. $e[x \leftarrow v] = v$	4249
4195	by the induction hypothesis (2)	2. $\Gamma \vdash_H v$	4250
4196	4. $\Gamma \vdash_H \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	by <i>weakening</i>	4251
4197	by (3)	3. QED	4252
4198	5. QED	CASE $e = x'$:	4253
4199	CASE $e = e_0 e_1$:	1. QED by $(x'[x \leftarrow v]) = x'$	4254
4200	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$	CASE $e = i$:	4255
4201	2. $(x : \tau_x), \Gamma \vdash_H e_0$	1. QED by $i[x \leftarrow v] = i$	4256
4202	$\wedge (x : \tau_x), \Gamma \vdash_H e_1$	CASE $e = \lambda x'. e'$:	4257
4203	by <i>H inversion</i>	1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$	4258
4204	3. $\Gamma \vdash_H e_0[x \leftarrow v]$	2. $x', x, \Gamma \vdash_H e'$	4259
4205	$\wedge \Gamma \vdash_H e_1[x \leftarrow v]$	by <i>H inversion</i>	4260
4206	by the induction hypothesis (2)	3. $x', \Gamma \vdash_H e'[x \leftarrow v]$	4261
4207	4. $\Gamma \vdash_H e_0[x \leftarrow v] e_1[x \leftarrow v]$	by the induction hypothesis (2)	4262
4208	by (3)	4. $\Gamma \vdash_H \lambda x'. (e'[x \leftarrow v])$	4263
4209	5. QED	by (3)	4264
4210	CASE $e = \text{op}^1 e_0$:	5. QED	4265
4211	1. $e[x \leftarrow v] = \text{op}^1 e_0[x \leftarrow v]$	CASE $e = \lambda(x' : \tau'). e'$:	4266
4212	2. $(x : \tau_x), \Gamma \vdash_H e_0$	1. Contradiction by $x, \Gamma \vdash_H e$	4267
4213	by <i>H inversion</i>	CASE $e = \text{mon}(\tau_d \Rightarrow \tau_c) v'$:	4268
4214	3. $\Gamma \vdash_H e_0[x \leftarrow v]$	1. $e[x \leftarrow v] = \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$	4269
4215	by the induction hypothesis (2)	2. $x, \Gamma \vdash_H v' : \tau_d \Rightarrow \tau_c$	4270
4216	4. $\Gamma \vdash_H \text{op}^1 e_0[x \leftarrow v]$	by <i>H inversion</i>	4271
4217	by (3)	3. $\Gamma \vdash_H v'[x \leftarrow v] : \tau_d \Rightarrow \tau_c$	4272
4218	5. QED	by <i>static context dynamic value substitution</i> (2)	4273
4219	CASE $e = \text{op}^2 e_0 e_1$:	4. $\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$	4274
4220	1. $e[x \leftarrow v] = \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	by (3)	4275
4221	2. $(x : \tau_x), \Gamma \vdash_H e_0$	5. QED	4276
4222	$\wedge (x : \tau_x), \Gamma \vdash_H e_1$	CASE $e = \langle e_0, e_1 \rangle$:	4277
4223	by <i>H inversion</i>	1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	4278
4224	3. $\Gamma \vdash_H e_0[x \leftarrow v]$	2. $x, \Gamma \vdash_H e_0$	4279
4225	$\wedge \Gamma \vdash_H e_1[x \leftarrow v]$	$\wedge x, \Gamma \vdash_H e_1$	4280
4226	by the induction hypothesis (2)	by <i>H inversion</i>	4281
4227	4. $\Gamma \vdash_H \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	3. $\Gamma \vdash_H e_0[x \leftarrow v]$	4282
4228	by (3)	$\wedge \Gamma \vdash_H e_1[x \leftarrow v]$	4283
4229	5. QED	by the induction hypothesis (2)	4284
4230	CASE $e = \text{stat } \tau' e'$:	4. $\Gamma \vdash_H \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	4285
4231	1. $e[x \leftarrow v] = \text{stat } \tau' e'[x \leftarrow v]$	by (3)	4286
4232	2. $(x : \tau_x), \Gamma \vdash_H e' : \tau'$	5. QED	4287
4233	by <i>H inversion</i>	CASE $e = e_0 e_1$:	4288
4234			4289
4235			4290

4291	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$		4346
4292	2. $x, \Gamma \vdash_H e_0$		4347
4293	$\wedge x, \Gamma \vdash_H e_1$		4348
4294	by H inversion		4349
4295	3. $\Gamma \vdash_H e_0[x \leftarrow v]$		4350
4296	$\wedge \Gamma \vdash_H e_1[x \leftarrow v]$		4351
4297	by the induction hypothesis (2)		4352
4298	4. $\Gamma \vdash_H e_0[x \leftarrow v] e_1[x \leftarrow v]$		4353
4299	by (3)		4354
4300	5. QED		4355
4301	CASE $e = op^1 e_0$:		4356
4302	1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$		4357
4303	2. $x, \Gamma \vdash_H e_0$		4358
4304	by H inversion		4359
4305	3. $\Gamma \vdash_H e_0[x \leftarrow v]$		4360
4306	by the induction hypothesis (2)		4361
4307	4. $\Gamma \vdash_H op^1 e_0[x \leftarrow v]$		4362
4308	by (3)		4363
4309	5. QED		4364
4310	CASE $e = op^2 e_0 e_1$:		4365
4311	1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$		4366
4312	2. $x, \Gamma \vdash_H e_0$		4367
4313	$\wedge x, \Gamma \vdash_H e_1$		4368
4314	by H inversion		4369
4315	3. $\Gamma \vdash_H e_0[x \leftarrow v]$		4370
4316	$\wedge \Gamma \vdash_H e_1[x \leftarrow v]$		4371
4317	by the induction hypothesis (2)		4372
4318	4. $\Gamma \vdash_H op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$		4373
4319	by (3)		4374
4320	5. QED		4375
4321	CASE $e = stat \tau' e'$:		4376
4322	1. $e[x \leftarrow v] = stat \tau' e'[x \leftarrow v]$		4377
4323	2. $x, \Gamma \vdash_H e' : \tau'$		4378
4324	by H inversion		4379
4325	3. $\Gamma \vdash_H e'[x \leftarrow v] : \tau'$		4380
4326	by static context static value substitution (2)		4381
4327	4. $\Gamma \vdash_H stat \tau' e'[x \leftarrow v]$		4382
4328	by (3)		4383
4329	5. QED		4384
4330	CASE $e = Err$:		4385
4331	1. QED $Err = Err[x \leftarrow v]$		4386
4332	□		4387
4333	Lemma 2.39 : H static-static substitution		4388
4334	▮ If $(x : \tau_x), \Gamma \vdash_H e : \tau$ and $\vdash_H v : \tau_x$ then $\Gamma \vdash_H e[x \leftarrow v] : \tau$		4389
4335	<i>Proof</i> :		4390
4336	By induction on the structure of e .		4391
4337	CASE $e = x$:		4392
4338	1. $e[x \leftarrow v] = v$		4393
4339	2. $(x : \tau_x), \Gamma \vdash_H x : \tau$		4394
4340	3. $\tau_x \leq \tau$		4395
4341	by H inversion		4396
4342	4. $\vdash_H v : \tau$		4397
4343	by (3)		4398
4344			4399
4345			4400
	5. $\Gamma \vdash_H v : \tau$		4346
	by weakening		4347
	6. QED		4348
	CASE $e = x'$:		4349
	1. QED by $(x'[x \leftarrow v]) = x'$		4350
	CASE $e = i$:		4351
	1. QED by $i[x \leftarrow v] = i$		4352
	CASE $e = \lambda x'. e'$:		4353
	1. Contradiction by $(x : \tau_x), \Gamma \vdash_H e : \tau$		4354
	CASE $e = \lambda(x' : \tau'). e'$:		4355
	1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$		4356
	2. $(x' : \tau'), (x : \tau_x), \Gamma \vdash_H e' : \tau'_c$		4357
	$\wedge \tau' \Rightarrow \tau'_c \leq \tau$		4358
	3. $(x' : \tau'), \Gamma \vdash_H e'[x \leftarrow v] : \tau'_c$		4359
	by the induction hypothesis (2)		4360
	4. $\Gamma \vdash_H \lambda(x' : \tau'). e' : \tau$		4361
	5. QED		4362
	CASE $e = \text{mon}(\tau_d \Rightarrow \tau_c) v'$:		4363
	1. $e[x \leftarrow v] = \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$		4364
	2. $(x : \tau_x), \Gamma \vdash_H v'$		4365
	by H inversion		4366
	3. $\Gamma \vdash_H v'[x \leftarrow v]$		4367
	by dynamic context static value substitution (2)		4368
	4. $\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v] : \tau$		4369
	by (3)		4370
	5. QED		4371
	CASE $e = \langle e_0, e_1 \rangle$:		4372
	1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$		4373
	2. $(x : \tau_x), \Gamma \vdash_H e_0 : \tau_0$		4374
	$\wedge (x : \tau_x), \Gamma \vdash_H e_1 : \tau_1$		4375
	by H inversion		4376
	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$		4377
	$\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$		4378
	by the induction hypothesis (2)		4379
	4. $\Gamma \vdash_H \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle : \tau$		4380
	by (3)		4381
	5. QED		4382
	CASE $e = e_0 e_1$:		4383
	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$		4384
	2. $(x : \tau_x), \Gamma \vdash_H e_0 : \tau_0$		4385
	$\wedge (x : \tau_x), \Gamma \vdash_H e_1 : \tau_1$		4386
	by H inversion		4387
	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$		4388
	$\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$		4389
	by the induction hypothesis (2)		4390
	4. $\Gamma \vdash_H e_0[x \leftarrow v] e_1[x \leftarrow v] : \tau$		4391
	by (3)		4392
	5. QED		4393
	CASE $e = op^1 e_0$:		4394
	1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$		4395
	2. $(x : \tau_x), \Gamma \vdash_H e_0 : \tau_0$		4396
	by H inversion		4397
	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$		4398
	by the induction hypothesis (2)		4399

4401	4. $\Gamma \vdash_H op^1 e_0[x \leftarrow v] : \tau$	4. $\Gamma \vdash_H mon(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v] : \tau$	4456
4402	by (3)	by (3)	4457
4403	5. QED	5. QED	4458
4404	CASE $e = op^2 e_0 e_1 :$	CASE $e = \langle e_0, e_1 \rangle :$	4459
4405	1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	4460
4406	2. $(x : \tau_x), \Gamma \vdash_H e_0 : \tau_0$	2. $x, \Gamma \vdash_H e_0 : \tau_0$	4461
4407	$\wedge (x : \tau_x), \Gamma \vdash_H e_1 : \tau_1$	$\wedge x, \Gamma \vdash_H e_1 : \tau_1$	4462
4408	by <i>H inversion</i>	by <i>H inversion</i>	4463
4409	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$	4464
4410	$\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$	$\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$	4465
4411	by the induction hypothesis (2)	by the induction hypothesis (2)	4466
4412	4. $\Gamma \vdash_H op^2 e_0[x \leftarrow v] e_1[x \leftarrow v] : \tau$	4. $\Gamma \vdash_H \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle : \tau$	4467
4413	by (3)	by (3)	4468
4414	5. QED	5. QED	4469
4415	CASE $e = dyn \tau' e' :$	CASE $e = e_0 e_1 :$	4470
4416	1. $e[x \leftarrow v] = dyn \tau' e'[x \leftarrow v]$	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$	4471
4417	2. $(x : \tau_x), \Gamma \vdash_H e' :$	2. $x, \Gamma \vdash_H e_0 : \tau_0$	4472
4418	by <i>H inversion</i>	$\wedge x, \Gamma \vdash_H e_1 : \tau_1$	4473
4419	3. $\Gamma \vdash_H e'[x \leftarrow v]$	by <i>H inversion</i>	4474
4420	by <i>dynamic context static value substitution</i> (2)	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$	4475
4421	4. $\Gamma \vdash_H dyn \tau' e'[x \leftarrow v] : \tau$	$\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$	4476
4422	by (3)	by the induction hypothesis (2)	4477
4423	5. QED	4. $\Gamma \vdash_H e_0[x \leftarrow v] e_1[x \leftarrow v] : \tau$	4478
4424	CASE $e = Err :$	by (3)	4479
4425	1. QED by $Err = Err[x \leftarrow v]$	5. QED	4480
4426	□	CASE $e = op^1 e_0 :$	4481
4427	Lemma 2.40 : <i>H static-dynamic substitution</i>	1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$	4482
4428	▮ If $x, \Gamma \vdash_H e : \tau$ and $\vdash_H v$ then $\Gamma \vdash_H e[x \leftarrow v] : \tau$	2. $x, \Gamma \vdash_H e_0 : \tau_0$	4483
4429	<i>Proof</i> :	by <i>H inversion</i>	4484
4430	By induction on the structure of e .	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$	4485
4431	CASE $e = x :$	by the induction hypothesis (2)	4486
4432	1. Contradiction by $x, \Gamma \vdash_H x : \tau$	4. $\Gamma \vdash_H op^1 e_0[x \leftarrow v] : \tau$	4487
4433	CASE $e = x' :$	by (3)	4488
4434	1. QED by $(x'[x \leftarrow v]) = x'$	5. QED	4489
4435	CASE $e = i :$	CASE $e = op^2 e_0 e_1 :$	4490
4436	1. QED by $i[x \leftarrow v] = i$	1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	4491
4437	CASE $e = \lambda x'. e' :$	2. $x, \Gamma \vdash_H e_0 : \tau_0$	4492
4438	1. Contradiction by $(x : \tau_x), \Gamma \vdash_H e : \tau$	$\wedge x, \Gamma \vdash_H e_1 : \tau_1$	4493
4439	CASE $e = \lambda(x' : \tau'). e' :$	by <i>H inversion</i>	4494
4440	1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$	4495
4441	2. $(x' : \tau'), x, \Gamma \vdash_H e' : \tau'_c$	$\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$	4496
4442	$\wedge \tau' \Rightarrow \tau'_c \leq \tau$	by the induction hypothesis (2)	4497
4443	3. $(x' : \tau'), \Gamma \vdash_H e'[x \leftarrow v] : \tau'_c$	4. $\Gamma \vdash_H op^2 e_0[x \leftarrow v] e_1[x \leftarrow v] : \tau$	4498
4444	by the induction hypothesis (2)	by (3)	4499
4445	4. $\Gamma \vdash_H \lambda(x' : \tau'). e' : \tau$	5. QED	4500
4446	5. QED	CASE $e = dyn \tau' e' :$	4501
4447	CASE $e = mon(\tau_d \Rightarrow \tau_c) v' :$	1. $e[x \leftarrow v] = dyn \tau' e'[x \leftarrow v]$	4502
4448	1. $e[x \leftarrow v] = mon(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$	2. $x, \Gamma \vdash_H e' :$	4503
4449	2. $x, \Gamma \vdash_H v' :$	by <i>H inversion</i>	4504
4450	by <i>H inversion</i>	3. $\Gamma \vdash_H e'[x \leftarrow v]$	4505
4451	3. $\Gamma \vdash_H v'[x \leftarrow v]$	by <i>dynamic context dynamic value substitution</i> (2)	4506
4452	by <i>dynamic context dynamic value substitution</i> (2)	4. $\Gamma \vdash_H dyn \tau' e'[x \leftarrow v] : \tau$	4507
4453		by (3)	4508
4454		5. QED	4509
4455			4510

4511	CASE $e = \text{Err}$:	4566
4512	1. QED by $\text{Err} = \text{Err}[x \leftarrow v]$	4567
4513	□	4568
4514	Lemma 2.41 : <i>weakening</i>	4569
4515	• If $\Gamma \vdash_H e$ then $x, \Gamma \vdash_H e$	4570
4516	• If $\Gamma \vdash_H e : \tau$ then $(x : \tau'), \Gamma \vdash_H e : \tau$	4571
4517	<i>Proof</i> :	4572
4518	• e is closed under Γ	4573
4519	by $\Gamma \vdash_H e$	4574
4520	$\forall \Gamma \vdash_H e : \tau$	4575
4521	• QED x is unused in the derivation	4576
4522	□	4577
4523		4578
4524		4579
4525		4580
4526		4581
4527		4582
4528		4583
4529		4584
4530		4585
4531		4586
4532		4587
4533		4588
4534		4589
4535		4590
4536		4591
4537		4592
4538		4593
4539		4594
4540		4595
4541		4596
4542		4597
4543		4598
4544		4599
4545		4600
4546		4601
4547		4602
4548		4603
4549		4604
4550		4605
4551		4606
4552		4607
4553		4608
4554		4609
4555		4610
4556		4611
4557		4612
4558		4613
4559		4614
4560		4615
4561		4616
4562		4617
4563		4618
4564		4619
4565		4620

4621 E.3 (E) Erasure Embedding

4622 E.3.1 Erasure Definitions

4623 $\boxed{\text{Language E}}$

4624 $e = x \mid v \mid \langle e, e \rangle \mid ee \mid op^1 e \mid op^2 ee \mid$
 4625 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err}$

4626 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e$

4627 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$

4628 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$

4629 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$

4630 $r = v \mid \text{Err}$

4631 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 4632 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet$

4633 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 4634 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E$

4635 $\boxed{\Delta : op^1 \times \tau \longrightarrow \tau}$

4636 $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$

4637 $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$

4638 $\boxed{\Delta : op^2 \times \tau \times \tau \longrightarrow \tau}$

4639 $\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$

4640 $\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$

4641 $\boxed{\tau \leqslant: \tau}$

4642 $\text{Nat} \leqslant: \text{Int} \quad \frac{\tau'_d \leqslant: \tau_d \quad \tau_c \leqslant: \tau'_c}{\tau_d \Rightarrow \tau_c \leqslant: \tau'_d \Rightarrow \tau'_c} \quad \frac{\tau_0 \leqslant: \tau'_0 \quad \tau_1 \leqslant: \tau'_1}{\tau_0 \times \tau_1 \leqslant: \tau'_0 \times \tau'_1}$

4643 $\frac{\tau \leqslant: \tau' \quad \tau' \leqslant: \tau''}{\tau \leqslant: \tau''}$

4644 $\boxed{\Gamma \vdash e}$

4645 $\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$

4646 $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$

4647 $\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$

4676 $\boxed{\Gamma \vdash e : \tau}$

4677 $\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$

4678 $\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$

4679 $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant: \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$

4680 $\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$

4681 $\boxed{\Gamma \Vdash e}$

4682 $\frac{x \in \Gamma}{\Gamma \Vdash x} \quad \frac{(x:\tau) \in \Gamma}{\Gamma \Vdash x} \quad \frac{x, \Gamma \Vdash e}{\Gamma \Vdash \lambda x. e} \quad \frac{(x:\tau), \Gamma \Vdash e}{\Gamma \Vdash \lambda(x:\tau). e} \quad \frac{}{\Gamma \Vdash i}$

4683 $\frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash \langle e_0, e_1 \rangle} \quad \frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash e_0 e_1} \quad \frac{\Gamma \Vdash e}{\Gamma \Vdash op^1 e}$

4684 $\frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \Vdash \text{Err}} \quad \frac{\Gamma \Vdash e}{\Gamma \Vdash \text{dyn } \tau e} \quad \frac{\Gamma \Vdash e}{\Gamma \Vdash \text{stat } \tau e}$

4685 $\boxed{\delta(op^1, v) = e}$

4686 $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$

4687 $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$

4688 $\boxed{\delta(op^2, v, v) = e}$

4689 $\delta(\text{sum}, i_0, i_1) = i_0 + i_1$

4690 $\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$

4691 $\delta(\text{quotient}, i_0, i_1) = [i_0/i_1]$
 4692 if $i_1 \neq 0$

4693 $\boxed{\mathcal{D}_E : \tau \times v \longrightarrow e}$

4694 $\mathcal{D}_E(\tau, v) = v$

4695 $\boxed{\mathcal{S}_E : \tau \times v \longrightarrow e}$

4696 $\mathcal{S}_E(\tau, v) = v$

4731	$e \triangleright_{E-S} e$	4786
4732	dyn $\tau v \triangleright_{E-S} \mathcal{D}_E(\tau, v)$	4787
4733	stat $\tau v \triangleright_{E-S} \mathcal{S}_E(\tau, v)$	4788
4734	$v_0 v_1 \triangleright_{E-S} \text{TagErr}$	4789
4735	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$	4790
4736	$(\lambda(x:\tau). e) v \triangleright_{E-S} e[x \leftarrow v]$	4791
4737	$(\lambda x. e) v \triangleright_{E-S} e[x \leftarrow v]$	4792
4738	$op^1 v \triangleright_{E-S} \text{TagErr}$	4793
4739	if $\delta(op^1, v)$ is undefined	4794
4740	$op^1 v \triangleright_{E-S} \delta(op^1, v)$	4795
4741	$op^2 v_0 v_1 \triangleright_{E-S} \text{TagErr}$	4796
4742	if $\delta(op^2, v_0, v_1)$ is undefined	4797
4743	$op^2 v_0 v_1 \triangleright_{E-S} \delta(op^2, v_0, v_1)$	4798
4744	$e \triangleright_{E-D} e$	4799
4745	stat $\tau v \triangleright_{E-D} \mathcal{S}_E(\tau, v)$	4800
4746	dyn $\tau v \triangleright_{E-D} \mathcal{D}_E(\tau, v)$	4801
4747	$v_0 v_1 \triangleright_{E-D} \text{TagErr}$	4802
4748	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$	4803
4749	$(\lambda(x:\tau). e) v \triangleright_{E-D} e[x \leftarrow v]$	4804
4750	$(\lambda x. e) v \triangleright_{E-D} e[x \leftarrow v]$	4805
4751	$op^1 v \triangleright_{E-D} \text{TagErr}$	4806
4752	if $\delta(op^1, v)$ is undefined	4807
4753	$op^1 v \triangleright_{E-D} \delta(op^1, v)$	4808
4754	$op^2 v_0 v_1 \triangleright_{E-D} \text{TagErr}$	4809
4755	if $\delta(op^2, v_0, v_1)$ is undefined	4810
4756	$op^2 v_0 v_1 \triangleright_{E-D} \delta(op^2, v_0, v_1)$	4811
4757	$e \rightarrow_{E-S} e$	4812
4758	$E[e] \rightarrow_{E-S} E[e']$	4813
4759	if $e \triangleright_{E-S} e'$	4814
4760	$E[\text{Err}] \rightarrow_{E-S} \text{Err}$	4815
4761	$e \rightarrow_{E-D} e$	4816
4762	$E[e] \rightarrow_{E-D} E[e']$	4817
4763	if $e \triangleright_{E-D} e'$	4818
4764	$E[\text{Err}] \rightarrow_{E-D} \text{Err}$	4819
4765	$e \rightarrow_{E-S}^* e$ reflexive, transitive closure of \rightarrow_{E-S}	4820
4766	$e \rightarrow_{E-S}^* e$	4821
4767	$e \rightarrow_{E-D}^* e$ reflexive, transitive closure of \rightarrow_{E-D}	4822
4768	$e \rightarrow_{E-D}^* e$	4823
4769		4824
4770		4825
4771		4826
4772		4827
4773		4828
4774		4829
4775		4830
4776		4831
4777		4832
4778		4833
4779		4834
4780		4835
4781		4836
4782		4837
4783		4838
4784		4839
4785		4840

4841 E.3.2 Erasure Theorems

4842 **Theorem 3.0** : *static E-soundness*

4843 If $\vdash e : \tau$ then $\vdash_E e$ and one of the following holds:

- 4844 • $e \rightarrow_{E-S}^* v$ and $\vdash_E v$
- 4845 • $e \rightarrow_{E-S}^* \text{TagErr}$
- 4846 • $e \rightarrow_{E-S}^* \text{BndryErr}$
- 4847 • e diverges

4848 *Proof*:

- 4849 1. $\vdash_E e$
4850 by *static subset*
- 4851 2. QED by *E progress* and *E preservation*

4852 □

4853 **Theorem 3.1** : *dynamic E-soundness*

4854 If $\vdash e$ then $\vdash_E e$ and one of the following holds:

- 4855 • $e \rightarrow_{E-D}^* v$ and $\vdash_E v$
- 4856 • $e \rightarrow_{E-D}^* \text{TagErr}$
- 4857 • $e \rightarrow_{E-D}^* \text{BndryErr}$
- 4858 • e diverges

4859 *Proof*:

- 4860 1. $\rightarrow_{E-D}^* \Rightarrow \rightarrow_{E-S}^*$
4861 by definition
- 4862 2. QED by *static E soundness*

4863 □

4864 **Remark 3.2** : *E-compilation*

4865 The \rightarrow_{E-S}^* and \rightarrow_{E-D}^* relations are identical. In practice, uses
4866 of \rightarrow_{E-S}^* may be replaced with \rightarrow_{E-D}^* .

4869 **Theorem 3.3** : *boundary-free E-soundness*

4870 If $\vdash e : \tau$ and e is boundary-free then one of the following
4871 holds:

- 4872 • $e \rightarrow_{E-S}^* v$ and $\vdash v : \tau$
- 4873 • $e \rightarrow_{E-S}^* \text{BndryErr}$
- 4874 • e diverges

4875 *Proof*:

4876 QED by *boundary-free progress* and *boundary-free preser-*
4877 *vation*.

4878 □

E.3.3 Erasure Lemmas
Lemma 3.4 : \mathcal{D}_E soundness

If $\vdash_E v$ then $\vdash_E \mathcal{D}_E(\tau, v)$.

Proof:

CASE $\mathcal{D}_E(\tau, v) = v$:

1. QED

□

Lemma 3.5 : \mathcal{S}_E soundness

If $\vdash_E v$ then $\vdash_E \mathcal{S}_E(\tau, v)$.

Proof:

CASE $\mathcal{S}_E(\tau, v) = v$:

1. QED

□

Lemma 3.6 : static subset

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash_E e$.

Proof:

By structural induction on the typing relation.

CASE $\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau}$:

1. $(x:\tau) \in \Gamma$
2. $\Gamma \vdash_E x$
by (1)
3. QED

CASE $\frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c}$:

1. $(x:\tau_d), \Gamma \vdash_E e$
by the induction hypothesis
2. $\Gamma \vdash_E \lambda(x:\tau_d). e$
by (1)
3. QED

CASE $\frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$:

1. QED

CASE $\frac{}{\Gamma \vdash_E i : \text{Int}}$:

1. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1}$:

1. $\Gamma \vdash_E e_0$
 $\wedge \Gamma \vdash_E e_1$
by the induction hypothesis
2. $\Gamma \vdash_E \langle e_0, e_1 \rangle$
by (1)
3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$:

1. $\Gamma \vdash_E e_0$
 $\wedge \Gamma \vdash_E e_1$
by the induction hypothesis

2. $\Gamma \vdash_E e_0 e_1$
by (1)

3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(\text{op}^1, \tau_0) = \tau}{\Gamma \vdash \text{op}^1 e_0 : \tau}$:

1. $\Gamma \vdash_E e_0$
by the induction hypothesis
2. $\Gamma \vdash_E \text{op}^1 e_0$
by (1)
3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \quad \Delta(\text{op}^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau}$:

1. $\Gamma \vdash_E e_0$
 $\wedge \Gamma \vdash_E e_1$
by the induction hypothesis
2. $\Gamma \vdash_E \text{op}^2 e_0 e_1$
by (1)
3. QED

CASE $\frac{\Gamma \vdash e : \tau' \quad \tau' <: \tau}{\Gamma \vdash e : \tau}$:

1. $\Gamma \vdash_E e$
by the induction hypothesis

2. QED

CASE $\frac{}{\Gamma \vdash \text{Err} : \tau}$:

1. QED

CASE $\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$:

1. $\Gamma \vdash_E e$
by *dynamic subset*
2. $\Gamma \vdash_E \text{dyn } \tau e$
by (1)
3. QED

□

Lemma 3.7 : dynamic subset

If $\Gamma \vdash e$ then $\Gamma \vdash_E e$.

Proof:

By structural induction on the \vdash relation.

CASE $\frac{x \in \Gamma}{\Gamma \vdash x}$:

1. $x \in \Gamma$
2. $\Gamma \vdash x$
by (1)
3. QED

CASE $\frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e}$:

1. $x, \Gamma \vdash e$
by the induction hypothesis

5061 2. $\Gamma \vdash_{\mathbb{E}} \lambda x. e$
 5062 by (1)
 5063 3. QED
 5064 **CASE** $\frac{}{\Gamma \vdash i}$:
 5065
 5066 1. QED
 5067 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$:
 5068
 5069 1. $\Gamma \vdash_{\mathbb{E}} e_0$
 5070 $\wedge \Gamma \vdash_{\mathbb{E}} e_1$
 5071 by the induction hypothesis
 5072 2. $\Gamma \vdash_{\mathbb{E}} \langle e_0, e_1 \rangle$
 5073 by (1)
 5074 3. QED
 5075 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1}$:
 5076
 5077 1. $\Gamma \vdash_{\mathbb{E}} e_0$
 5078 $\wedge \Gamma \vdash_{\mathbb{E}} e_1$
 5079 by the induction hypothesis
 5080 2. $\Gamma \vdash_{\mathbb{E}} e_0 e_1$
 5081 by (1)
 5082 3. QED
 5083 **CASE** $\frac{\Gamma \vdash e}{\Gamma \vdash op^1 e}$:
 5084
 5085 1. $\Gamma \vdash_{\mathbb{E}} e$
 5086 by the induction hypothesis
 5087 2. $\Gamma \vdash_{\mathbb{E}} op^1 e$
 5088 by (1)
 5089 3. QED
 5090 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1}$:
 5091
 5092 1. $\Gamma \vdash_{\mathbb{E}} e_0$
 5093 $\wedge \Gamma \vdash_{\mathbb{E}} e_1$
 5094 by the induction hypothesis
 5095 2. $\Gamma \vdash_{\mathbb{E}} op^2 e_0 e_1$
 5096 by (1)
 5097 3. QED
 5098 **CASE** $\frac{}{\Gamma \vdash \text{Err}}$:
 5099
 5100 1. QED
 5101 **CASE** $\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$:
 5102
 5103 1. $\Gamma \vdash_{\mathbb{E}} e$
 5104 by *static subset*
 5105 2. $\Gamma \vdash_{\mathbb{E}} \text{stat } \tau e$
 5106 by (1)
 5107 3. QED
 5108 \square

5113 **Lemma 3.8** : \mathbb{E} progress
 5114
 5115

If $\vdash_{\mathbb{E}} e$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{\mathbb{E}\text{-S}} e'$
- $e \rightarrow_{\mathbb{E}\text{-S}} \text{TagErr}$
- $e \rightarrow_{\mathbb{E}\text{-S}} \text{BndryErr}$

Proof:

By the *unique evaluation contexts* lemma, there are seven possible cases.

CASE e is a value :

1. QED

CASE $e = E[v_0 v_1]$:

IF $v_0 = \lambda x. e'$:

1. $e \rightarrow_{\mathbb{E}\text{-S}} E[e'[x \leftarrow v_1]]$

by $v_0 v_1 \triangleright_{\mathbb{E}\text{-S}} e'[x \leftarrow v_1]$

2. QED

IF $v_0 = \lambda(x:\tau). e'$:

1. $e \rightarrow_{\mathbb{E}\text{-S}} E[e'[x \leftarrow v_1]]$

by $v_0 v_1 \triangleright_{\mathbb{E}\text{-S}} e'[x \leftarrow v_1]$

2. QED

ELSE $v_0 = i$

$\vee v_0 = \langle v, v' \rangle$:

1. $e \rightarrow_{\mathbb{E}\text{-S}} \text{TagErr}$

by $v_0 v_1 \triangleright_{\mathbb{E}\text{-S}} \text{TagErr}$

2. QED

CASE $e = E[op^1 v]$:

IF $\delta(op^1, v) = e''$:

1. $e \rightarrow_{\mathbb{E}\text{-S}} E[e'']$

by $(op^1 v) \triangleright_{\mathbb{E}\text{-S}} e''$

2. QED

ELSE $\delta(op^1, v)$ is undefined :

1. $e \rightarrow_{\mathbb{E}\text{-S}} \text{TagErr}$

by $(op^1 v) \triangleright_{\mathbb{E}\text{-S}} \text{TagErr}$

2. QED

CASE $e = E[op^2 v_0 v_1]$:

IF $\delta(op^2, v_0, v_1) = e''$:

1. $e \rightarrow_{\mathbb{E}\text{-S}} E[e'']$

by $(op^2 v_0 v_1) \triangleright_{\mathbb{E}\text{-S}} e''$

2. QED

IF $\delta(op^2, v_0, v_1) = \text{BndryErr}$:

1. $e \rightarrow_{\mathbb{E}\text{-S}} \text{BndryErr}$

by $(op^2 v_0 v_1) \triangleright_{\mathbb{E}\text{-S}} \text{BndryErr}$

2. QED

ELSE $\delta(op^2, v_0, v_1)$ is undefined :

1. $e \rightarrow_{\mathbb{E}\text{-S}} \text{TagErr}$

by $(op^2 v_0 v_1) \triangleright_{\mathbb{E}\text{-S}} \text{TagErr}$

2. QED

CASE $e = E[\text{dyn } \tau v]$:

1. $e \rightarrow_{\mathbb{E}\text{-S}} E[\mathcal{D}_{\mathbb{E}}(\tau, v)]$

2. QED

CASE $e = E[\text{stat } \tau v]$:

1. $e \rightarrow_{\mathbb{E}\text{-S}} E[\mathcal{S}_{\mathbb{E}}(\tau, v)]$

2. QED

CASE $e \in E[\text{Err}]$:

5171 1. $e \rightarrow_{E-S} \text{Err}$
 5172 2. QED
 5173 \square
 5174 **Lemma 3.9** : E preservation
 5175 If $\vdash_E e$ and $e \rightarrow_{E-S} e'$ then $\vdash_E e'$.
 5176 *Proof*:
 5177 By *unique evaluation contexts* there are seven cases.
 5178 **CASE** e is a value :
 5179 1. Contradiction by $e \rightarrow_{E-S} e'$
 5180 **CASE** $e = E[v_0 v_1]$:
 5181 1. $v_0 = \lambda x. e'$ or $v_0 = \lambda(x:\tau). e'$
 5182 $\wedge E[v_0 v_1] \rightarrow_{E-S} E[e'[x \leftarrow v_1]]$
 5183 2. $\vdash_E v_0 v_1$
 5184 by *hole typing*
 5185 3. $\vdash_E v_0$
 5186 $\wedge \vdash_E v_1$
 5187 by **E inversion** (2)
 5188 4. $x \vdash_E e'$
 5189 by **E inversion** (3)
 5190 5. $\vdash_E e'[x \leftarrow v_1]$
 5191 by *substitution* (3, 4)
 5192 6. QED by *hole substitution* (5)
 5193 **CASE** $e = E[op^1 v]$:
 5194 1. $E[op^1 v] \rightarrow_{E-S} E[v']$
 5195 $\wedge \delta(op^1, v) = e''$
 5196 2. $\vdash_E op^1 v$
 5197 by *hole typing*
 5198 3. $\vdash_E v$
 5199 by **E inversion** (2)
 5200 4. $\vdash_E e''$
 5201 by δ preservation (1,3)
 5202 5. QED by *hole substitution* (4)
 5203 **CASE** $e = E[op^2 v_0 v_1]$:
 5204 1. $E[op^2 v_0 v_1] \rightarrow_{E-S} E[v']$
 5205 $\wedge \delta(op^2, v_0, v_1) = e''$
 5206 2. $\vdash_E op^2 v_0 v_1$
 5207 by *hole typing*
 5208 3. $\vdash_E v_0$
 5209 $\wedge \vdash_E v_1$
 5210 by **E inversion** (2)
 5211 4. $\vdash_E e''$
 5212 by δ preservation (3)
 5213 5. QED by *hole substitution* (4)
 5214 **CASE** $e = E[\text{dyn } \tau v]$:
 5215 1. $E[\text{dyn } \tau v] \rightarrow_{E-S} E[\mathcal{D}_E(\tau, v)]$
 5216 2. $\vdash_E \text{dyn } \tau v$
 5217 by *hole typing*
 5218 3. $\vdash_E v$
 5219 by **E inversion** (2)
 5220 4. $\vdash_E \mathcal{D}_E(\tau, v)$
 5221 by \mathcal{D}_E soundness (3)
 5222 5. QED by *hole substitution* (4)
 5223 **CASE** $e = E[\text{stat } \tau v]$:
 5224
 5225

1. $E[\text{stat } \tau v] \rightarrow_{E-S} \mathcal{S}_E(\tau, v)$ 5226
 2. $\vdash_E \text{stat } \tau v$ 5227
 by *hole typing* 5228
 3. $\vdash_E v$ 5229
 by **E inversion** (2) 5230
 4. $\vdash_E \mathcal{S}_E(\tau, v)$ 5231
 by **S_E soundness** (3) 5232
 5. QED by *hole substitution* (4) 5233
CASE $e = E[\text{Err}]$: 5234
 1. $E[\text{Err}] \rightarrow_{E-S} \text{Err}$ 5235
 2. QED 5236
 \square 5237
Lemma 3.10 : E boundary-free progress 5238
 If $\vdash e : \tau$ and e is boundary-free, then one of the following 5239
 holds: 5240

- e is a value 5241
- $e \in \text{Err}$ 5242
- $e \rightarrow_{E-S} e'$ 5243
- $e \rightarrow_{E-S} \text{BndryErr}$ 5244

 5245
Proof:
 By the *unique static evaluation contexts* lemma, there are 5246
 five cases: 5247
CASE $e = v$: 5248
 1. QED 5249
CASE $e = E[v_0 v_1]$: 5250
IF $v_0 = \lambda(x:\tau'). e'$: 5251
 1. $e \rightarrow_{E-S} E[e'[x \leftarrow v_1]]$ 5252
 by $v_0 v_1 \triangleright_{E-S} e'[x \leftarrow v_1]$ 5253
 2. QED 5254
ELSE $v_0 = \lambda x. e'$ 5255
 $\vee v_0 = i$ 5256
 $\vee v_0 = \langle v, v' \rangle$: 5257
 1. Contradiction by $\vdash e : \tau$ 5258
CASE $e = E[op^1 v]$: 5259
IF $\delta(op^1, v) = e''$: 5260
 1. $e \rightarrow_{E-S} E[e'']$ 5261
 by $(op^1 v) \triangleright_{E-S} e''$ 5262
 2. QED 5263
ELSE $\delta(op^1, v)$ is undefined : 5264
 1. Contradiction by $\vdash e : \tau$ 5265
CASE $e = E[op^2 v_0 v_1]$: 5266
IF $\delta(op^2, v_0, v_1) = e''$: 5267
 1. $e \rightarrow_{E-S} E[e'']$ 5268
 by $(op^2 v_0 v_1) \triangleright_{E-S} e''$ 5269
 2. QED 5270
IF $\delta(op^2, v_0, v_1) = \text{BndryErr}$: 5271
 1. $e \rightarrow_{E-S} \text{BndryErr}$ 5272
 by $(op^2 v_0 v_1) \triangleright_{E-S} \text{BndryErr}$ 5273
 2. QED 5274
ELSE $\delta(op^2, v_0, v_1)$ is undefined : 5275
 1. Contradiction by $\vdash e : \tau$ 5276
CASE $e = E[\text{Err}]$: 5277
 1. $E[\text{Err}] \rightarrow_{E-S} \text{Err}$ 5278
 2. QED 5279
 5280

5281 \square 5282 **Lemma 3.11** : E *boundary-free preservation*5283 If $\vdash e : \tau$ and e is boundary-free and $e \rightarrow_{E-S} e'$ then $\vdash e' : \tau$
5284 and e' is boundary-free.5285 *Proof*:5286 By the *unique static evaluation contexts* lemma, there are
5287 five cases.5288 **CASE** e is a value :5289 1. Contradiction by $e \rightarrow_{E-S} e'$ 5290 **CASE** $e = E[v_0 v_1]$:5291 **IF** $v_0 = \lambda(x:\tau_d). e'$:5292 1. $E[v_0 v_1] \rightarrow_{E-S} E[e'[x \leftarrow v_1]]$ 5293 2. $\vdash v_0 v_1 : \tau_c$ 5294 3. $\vdash v_0 : \tau_d \Rightarrow \tau_c$ 5295 $\wedge \vdash v_1 : \tau_d$

5296 by (2)

5297 4. $(x:\tau_d) \vdash e' : \tau_c$

5298 by (3)

5299 5. $\vdash e'[x \leftarrow v_1] : \tau_c$ 5300 by *substitution* (3, 4)5301 6. $e'[x \leftarrow v_1]$ is boundary-free5302 by e' and v_1 are boundary-free

5303 7. QED

5304 **ELSE** :5305 1. Contradiction by $\vdash e : \tau$ 5306 **CASE** $e = E[op^1 v]$:5307 1. $E[op^1 v] \rightarrow_{E-S} E[v']$ 5308 $\wedge \delta(op^1, v) = e''$ 5309 2. $\vdash op^1 v : \tau'$ 5310 3. $\vdash v : \tau_0$ 5311 4. $\vdash e'' : \tau'$ 5312 by δ *preservation* (3)

5313 5. QED

5314 **CASE** $e = E[op^2 v_0 v_1]$:5315 1. $E[op^2 v_0 v_1] \rightarrow_{E-S} E[v']$ 5316 $\wedge \delta(op^2, v_0, v_1) = e''$ 5317 2. $\vdash op^2 v_0 v_1 : \tau'$ 5318 3. $\vdash v_0 : \tau_0$ 5319 $\wedge \vdash v_1 : \tau_1$ 5320 4. $\vdash e'' : \tau'$ 5321 by δ *preservation* (3)

5322 5. QED

5323 **CASE** $e = E[Err]$:5324 1. $E[Err] \rightarrow_{E-S} Err$ 5325 2. QED by $\vdash Err : \tau$ 5326 \square 5327 **Lemma 3.12** : E *unique evaluation contexts*

5328

5329

5330

5331

5332

5333

5334

5335

If $\vdash_E e$ then one of the following holds:• e is a value• $e = E[v_0 v_1]$ • $e = E[op^1 v]$ • $e = E[op^2 v_0 v_1]$ • $e = E[\text{dyn } \tau v]$ • $e = E[\text{stat } \tau v]$ • $e = E[Err]$ *Proof*:By induction on the structure of e .**CASE** $e = x$:1. Contradiction by $\vdash_E e$ **CASE** $e = i$ $\vee e = \lambda x. e'$ $\vee e = \lambda(x:\tau_d). e'$:

1. QED

CASE $e = \langle e_0, e_1 \rangle$:**IF** $e_0 \notin v$:1. $\vdash_E e_0$ by *E inversion*2. $e_0 = E_0[e'_0]$

by the induction hypothesis

3. $E = \langle E_0, e_1 \rangle$ 4. QED $e = E[e'_0]$ **IF** $e_0 \in v$ $\wedge e_1 \notin v$:1. $\vdash_E e_1$ by *E inversion*2. $e_1 = E_1[e'_1]$

by the induction hypothesis

3. $E = \langle e_0, E_1 \rangle$ 4. QED $e = E[e'_1]$ **ELSE** $e_0 \in v$ $\wedge e_1 \in v$:

1. QED

CASE $e = e_0 e_1$:**IF** $e_0 \notin v$:1. $\vdash_E e_0$ by *E inversion*2. $e_0 = E_0[e'_0]$

by the induction hypothesis

3. $E = E_0 E_1$ 4. QED $e = E[e'_0]$ **IF** $e_0 \in v$ $\wedge e_1 \notin v$:1. $\vdash_E e_1$ by *E inversion*2. $e_1 = E_1[e'_1]$

by the induction hypothesis

3. $E = e_0 E_1$ 4. QED $e = E[e'_1]$ **ELSE** $e_0 \in v$ $\wedge e_1 \in v$:1. $E = []$

5336

5337

5338

5339

5340

5341

5342

5343

5344

5345

5346

5347

5348

5349

5350

5351

5352

5353

5354

5355

5356

5357

5358

5359

5360

5361

5362

5363

5364

5365

5366

5367

5368

5369

5370

5371

5372

5373

5374

5375

5376

5377

5378

5379

5380

5381

5382

5383

5384

5385

5386

5387

5388

5389

5390

5391	2. QED		
5392	CASE $e = op^1 e_0 :$		
5393	IF $e_0 \notin v :$		
5394	1. $\vdash_E e_0$		
5395	by E inversion		
5396	2. $e_0 = E_0[e'_0]$		
5397	by the induction hypothesis		
5398	3. $E = op^1 E_0$		
5399	4. QED $e = E[e'_0]$		
5400	ELSE $e_0 \in v :$		
5401	1. $E = []$		
5402	2. QED		
5403	CASE $e = op^2 e_0 e_1 :$		
5404	IF $e_0 \notin v :$		
5405	1. $\vdash_E e_0$		
5406	by E inversion		
5407	2. $e_0 = E_0[e'_0]$		
5408	by the induction hypothesis		
5409	3. $E = op^2 E_0 e_1$		
5410	4. QED $e = E[e'_0]$		
5411	IF $e_0 \in v$		
5412	$\wedge e_1 \notin v :$		
5413	1. $\vdash_E e_1$		
5414	by E inversion		
5415	2. $e_1 = E_1[e'_1]$		
5416	by the induction hypothesis		
5417	3. $E = op^2 e_0 E_1$		
5418	4. QED $e = E[e'_1]$		
5419	ELSE $e_0 \in v$		
5420	$\wedge e_1 \in v :$		
5421	1. $E = []$		
5422	2. QED		
5423	CASE $e = \text{dyn } \tau e_0 :$		
5424	IF $e_0 \notin v :$		
5425	1. $\vdash_E e_0$		
5426	by E inversion		
5427	2. $e_0 = E_0[e'_0]$		
5428	by the induction hypothesis		
5429	3. $E = \text{dyn } \tau E_0$		
5430	4. QED $e = E[e'_0]$		
5431	ELSE $e_0 \in v :$		
5432	1. $E = []$		
5433	2. QED		
5434	CASE $e = \text{stat } \tau e_0 :$		
5435	IF $e_0 \notin v :$		
5436	1. $\vdash_E e_0$		
5437	by E inversion		
5438	2. $e_0 = E_0[e'_0]$		
5439	by the induction hypothesis		
5440	3. $E = \text{stat } \tau E_0$		
5441	4. QED $e = E[e'_0]$		
5442	ELSE $e_0 \in v :$		
5443	1. $E = []$		
5444	2. QED		
5445			
		CASE $e = \text{Err} :$	5446
		1. $E = []$	5447
		2. QED	5448
		□	5449
		Lemma 3.13 : E hole typing	5450
		If $\vdash_E E[e]$ then the derivation contains a sub-term $\vdash_E e$	5451
		<i>Proof</i> :	5452
		By induction on the structure of E .	5453
		CASE $E = [] :$	5454
		1. QED $E[e] = e$	5455
		CASE $E = E_0 e_1 :$	5456
		1. $E[e] = E_0[e] e_1$	5457
		2. $\vdash_E E_0[e]$	5458
		by E inversion	5459
		3. QED by the induction hypothesis (2)	5460
		CASE $E = v_0 E_1 :$	5461
		1. $E[e] = v_0 E_1[e]$	5462
		2. $\vdash_E E_1[e]$	5463
		by E inversion	5464
		3. QED by the induction hypothesis (2)	5465
		CASE $E = \langle E_0, e_1 \rangle :$	5466
		1. $E[e] = \langle E_0[e], e_1 \rangle$	5467
		2. $\vdash_E E_0[e]$	5468
		by E inversion	5469
		3. QED by the induction hypothesis (2)	5470
		CASE $E = \langle v_0, E_1 \rangle :$	5471
		1. $E[e] = \langle v_0, E_1[e] \rangle$	5472
		2. $\vdash_E E_1[e]$	5473
		by E inversion	5474
		3. QED by the induction hypothesis (2)	5475
		CASE $E = op^1 E_0 :$	5476
		1. $E[e] = op^1 E_0[e]$	5477
		2. $\vdash_E E_0[e]$	5478
		by E inversion	5479
		3. QED by the induction hypothesis (2)	5480
		CASE $E = op^2 E_0 e_1 :$	5481
		1. $E[e] = op^2 E_0[e] e_1$	5482
		2. $\vdash_E E_0[e]$	5483
		by E inversion	5484
		3. QED by the induction hypothesis (2)	5485
		CASE $E = op^2 v_0 E_1 :$	5486
		1. $E[e] = op^2 v_0 E_1[e]$	5487
		2. $\vdash_E E_1[e]$	5488
		by E inversion	5489
		3. QED by the induction hypothesis (2)	5490
		CASE $E = \text{dyn } \tau E_0 :$	5491
		1. $E[e] = \text{dyn } \tau E_0[e]$	5492
		2. $\vdash_E E_0[e]$	5493
		by E inversion	5494
		3. QED by the induction hypothesis (2)	5495
		CASE $E = \text{stat } \tau E_0 :$	5496
		1. $E[e] = \text{stat } \tau E_0[e]$	5497
			5498
			5499
			5500

- 5501 2. $\vdash_E E_0[e]$
 5502 by **E inversion**
 5503 3. QED by the induction hypothesis (2)
 5504 \square

Lemma 3.14 : E hole substitution

5506 **|** If $\vdash_E E[e]$ and $\vdash_E e'$ then $\vdash_E E[e']$

5507 *Proof*:

5508 By induction on the structure of E .

5509 **CASE** $E = []$:

- 5510 1. QED $E[e'] = e'$

5511 **CASE** $E = \langle E_0, e_1 \rangle$:

- 5512 1. $E[e] = \langle E_0[e], e_1 \rangle$
 5513 $\wedge E[e'] = \langle E_0[e'], e_1 \rangle$
 5514 2. $\vdash_E \langle E_0[e], e_1 \rangle$
 5515 3. $\vdash_E E_0[e]$
 5516 $\wedge \vdash_E e_1$

5517 by **E inversion**

- 5518 4. $\vdash_E E_0[e']$
 5519 by the induction hypothesis (3)
 5520 5. $\vdash_E \langle E_0[e'], e_1 \rangle$
 5521 by (3, 4)
 5522 6. QED by (1, 5)

5523 **CASE** $E = \langle v_0, E_1 \rangle$:

- 5524 1. $E[e] = \langle v_0, E_1[e] \rangle$
 5525 $\wedge E[e'] = \langle v_0, E_1[e'] \rangle$
 5526 2. $\vdash_E \langle v_0, E_1[e] \rangle$
 5527 3. $\vdash_E v_0$

5528 $\wedge \vdash_E E_1[e]$

5529 by **E inversion**

- 5530 4. $\vdash_E E_1[e']$
 5531 by the induction hypothesis (3)
 5532 5. $\vdash_E \langle v_0, E_1[e'] \rangle$
 5533 by (3, 4)
 5534 6. QED by (1, 5)

5535 **CASE** $E = E_0 e_1$:

- 5536 1. $E[e] = E_0[e] e_1$
 5537 $\wedge E[e'] = E_0[e'] e_1$
 5538 2. $\vdash_E E_0[e] e_1$
 5539 3. $\vdash_E E_0[e]$
 5540 $\wedge \vdash_E e_1$

5541 by **E inversion**

- 5542 4. $\vdash_E E_0[e']$
 5543 by the induction hypothesis (3)
 5544 5. $\vdash_E E_0[e'] e_1$
 5545 by (3, 4)
 5546 6. QED by (1, 5)

5547 **CASE** $E = v_0 E_1$:

- 5548 1. $E[e] = v_0 E_1[e]$
 5549 $\wedge E[e'] = v_0 E_1[e']$
 5550 2. $\vdash_E v_0 E_1[e]$
 5551 3. $\vdash_E v_0$

5552 $\wedge \vdash_E E_1[e]$

5553 by **E inversion**

4. $\vdash_E E_1[e']$
 by the induction hypothesis (3)

5. $\vdash_E v_0 E_1[e']$
 by (3, 4)

6. QED by (1, 5)

5554 **CASE** $E = op^1 E_0$:

1. $E[e] = op^1 E_0[e]$
 $\wedge E[e'] = op^1 E_0[e']$

2. $\vdash_E op^1 E_0[e]$

3. $\vdash_E E_0[e]$
 by **E inversion**

4. $\vdash_E E_0[e']$
 by the induction hypothesis (3)

5. $\vdash_E op^1 E_0[e']$
 by (3, 4)

6. QED by (1, 5)

5555 **CASE** $E = op^2 E_0 e_1$:

1. $E[e] = op^2 E_0[e] e_1$
 $\wedge E[e'] = op^2 E_0[e'] e_1$

2. $\vdash_E op^2 E_0[e] e_1$

3. $\vdash_E E_0[e]$
 $\wedge \vdash_E e_1$

by **E inversion**

4. $\vdash_E E_0[e']$
 by the induction hypothesis (3)

5. $\vdash_E op^2 E_0[e'] e_1$
 by (3, 4)

6. QED by (1, 5)

5556 **CASE** $E = op^2 v_0 E_1$:

1. $E[e] = op^2 v_0 E_1[e]$
 $\wedge E[e'] = op^2 v_0 E_1[e']$

2. $\vdash_E op^2 v_0 E_1[e]$

3. $\vdash_E v_0$
 $\wedge \vdash_E E_1[e]$

by **E inversion**

4. $\vdash_E E_1[e']$
 by the induction hypothesis (3)

5. $\vdash_E op^2 v_0 E_1[e']$
 by (3, 4)

6. QED by (1, 5)

5557 **CASE** $E = dyn \tau E_0$:

1. $E[e] = dyn \tau E_0[e]$
 $\wedge E[e'] = dyn \tau E_0[e']$

2. $\vdash_E dyn \tau E_0[e]$

3. $\vdash_E E_0[e]$
 by **E inversion**

4. $\vdash_E E_0[e']$
 by the induction hypothesis (3)

5. $\vdash_E dyn \tau E_0[e']$
 by (3, 4)

6. QED by (1, 5)

5558 **CASE** $E = stat \tau E_0$:

1. $E[e] = stat \tau E_0[e]$
 $\wedge E[e'] = stat \tau E_0[e']$

- 5611 2. $\vdash_E \text{stat } \tau E_0[e]$
 5612 3. $\vdash_E E_0[e]$
 5613 by **E inversion**
 5614 4. $\vdash_E E_0[e']$
 5615 by the induction hypothesis (3)
 5616 5. $\vdash_E \text{stat } \tau E_0[e']$
 5617 by (3, 4)
 5618 6. QED by (1, 5)
 5619 \square

Lemma 3.15 : \vdash_E inversion

- 5620 • If $\Gamma \vdash_E e_0 e_1$ then $\Gamma \vdash_E e_0$ and $\Gamma \vdash_E e_1$
- 5621 • If $\Gamma \vdash_E \lambda x. e$ then $x, \Gamma \vdash_E e$
- 5622 • If $\Gamma \vdash_E \lambda(x:\tau). e$ then $(x:\tau), \Gamma \vdash_E e$
- 5623 • If $\Gamma \vdash_E \text{op}^1 e$ then $\Gamma \vdash_E e$
- 5624 • If $\Gamma \vdash_E \text{op}^2 e_0 e_1$ then $\Gamma \vdash_E e_0$ and $\Gamma \vdash_E e_1$
- 5625 • If $\Gamma \vdash_E \text{dyn } \tau e$ then $\Gamma \vdash_E e$
- 5626 • If $\Gamma \vdash_E \text{stat } \tau e$ then $\Gamma \vdash_E e$

5627 *Proof*:

5628 QED by the definition of $\vdash_E e$.

5629 \square

Lemma 3.16 : E substitution

5630 If $x, \Gamma \vdash_E e$ or $(x:\tau), \Gamma \vdash_E e$, and $\vdash_E v$ then $\Gamma \vdash_E e[x \leftarrow v]$

5631 *Proof*:

5632 By induction on the structure of e .

5633 **CASE** $e = x$:

- 5634 1. $e[x \leftarrow v] = v$
- 5635 2. $\Gamma \vdash_E v$

5636 by **weakening**

5637 3. QED

5638 **CASE** $e = x'$:

- 5639 1. QED by $x'[x \leftarrow v] = x'$

5640 **CASE** $e = i$:

- 5641 1. QED by $i[x \leftarrow v] = i$

5642 **CASE** $e = \lambda x. e'$:

- 5643 1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$

5644 **CASE** $e = \lambda(x:\tau'). e'$:

- 5645 1. QED by $(\lambda(x:\tau'). e')[x \leftarrow v] = \lambda(x:\tau'). e'$

5646 **CASE** $e = \lambda x'. e'$:

- 5647 1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$

- 5648 2. $x', x, \Gamma \vdash_E e'$

5649 by **E inversion**

- 5650 3. $x', \Gamma \vdash_E e'[x \leftarrow v]$

5651 by the induction hypothesis (2)

- 5652 4. $\Gamma \vdash_E \lambda x'. e'[x \leftarrow v]$

5653 by (3)

5654 5. QED

5655 **CASE** $e = \lambda(x':\tau'). e'$:

- 5656 1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$

- 5657 2. $(x':\tau'), x, \Gamma \vdash_E e'$

5658 by **E inversion**

- 5659 3. $(x':\tau'), \Gamma \vdash_E e'[x \leftarrow v]$

5660 by the induction hypothesis (2)

- 5661 4. $\Gamma \vdash_E \lambda(x':\tau'). (e'[x \leftarrow v])$

5662 by (3)

5663 5. QED

5664 **CASE** $e = \langle e_0, e_1 \rangle$:

- 5665 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$

- 5666 2. $x, \Gamma \vdash_E e_0$

5667 $\wedge x, \Gamma \vdash_E e_1$

5668 by **E inversion**

- 5669 3. $\Gamma \vdash_E e_0[x \leftarrow v]$

5670 $\wedge \Gamma \vdash_E e_1[x \leftarrow v]$

5671 by the induction hypothesis (2)

- 5672 4. $\Gamma \vdash_E \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$

5673 by (3)

5674 5. QED

5675 **CASE** $e = e_0 e_1$:

- 5676 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$

- 5677 2. $x, \Gamma \vdash_E e_0$

5678 $\wedge x, \Gamma \vdash_E e_1$

5679 by **E inversion**

- 5680 3. $\Gamma \vdash_E e_0[x \leftarrow v]$

5681 $\wedge \Gamma \vdash_E e_1[x \leftarrow v]$

5682 by the induction hypothesis (2)

- 5683 4. $\Gamma \vdash_E e_0[x \leftarrow v] e_1[x \leftarrow v]$

5684 by (3)

5685 5. QED

5686 **CASE** $e = \text{op}^1 e_0$:

- 5687 1. $e[x \leftarrow v] = \text{op}^1 e_0[x \leftarrow v]$

- 5688 2. $x, \Gamma \vdash_E e_0$

5689 by **E inversion**

- 5690 3. $\Gamma \vdash_E e_0[x \leftarrow v]$

5691 by the induction hypothesis (2)

- 5692 4. $\Gamma \vdash_E \text{op}^1 e_0[x \leftarrow v]$

5693 by (3)

5694 5. QED

5695 **CASE** $e = \text{op}^2 e_0 e_1$:

- 5696 1. $e[x \leftarrow v] = \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$

- 5697 2. $x, \Gamma \vdash_E e_0$

5698 $\wedge x, \Gamma \vdash_E e_1$

5699 by **E inversion**

- 5700 3. $\Gamma \vdash_E e_0[x \leftarrow v]$

5701 $\wedge \Gamma \vdash_E e_1[x \leftarrow v]$

5702 by the induction hypothesis (2)

- 5703 4. $\Gamma \vdash_E \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$

5704 by (3)

5705 5. QED

5706 **CASE** $e = \text{dyn } \tau' e'$:

- 5707 1. $e[x \leftarrow v] = \text{dyn } \tau' e'[x \leftarrow v]$

- 5708 2. $x, \Gamma \vdash_E e'$

5709 by **E inversion**

- 5710 3. $\Gamma \vdash_E e'[x \leftarrow v]$

5711 by the induction hypothesis (2)

- 5712 4. $\Gamma \vdash_E \text{dyn } \tau' (e'[x \leftarrow v])$

5713 by (3)

5714 5. QED

5665

5721	CASE $e = \text{stat } \tau' e' :$	5776
5722	1. $e[x \leftarrow v] = \text{stat } \tau' e'[x \leftarrow v]$	5777
5723	2. $x, \Gamma \vdash_{\mathbb{E}} e'$	5778
5724	by E inversion	5779
5725	3. $\Gamma \vdash_{\mathbb{E}} e'[x \leftarrow v]$	5780
5726	by the induction hypothesis (2)	5781
5727	4. $\Gamma \vdash_{\mathbb{E}} \text{stat } \tau' (e'[x \leftarrow v])$	5782
5728	by (3)	5783
5729	5. QED	5784
5730	CASE $e = \text{Err} :$	5785
5731	1. QED by $\text{Err}[x \leftarrow v] = \text{Err}$	5786
5732	□	5787
5733	Lemma 3.17 : δ preservation	5788
5734	• If $\Gamma \vdash_{\mathbb{E}} v$ and $\delta(\text{op}^1, v) = e'$ then $\vdash_{\mathbb{E}} e'$	5789
5735	• If $\Gamma \vdash_{\mathbb{E}} v_0$ and $\vdash_{\mathbb{E}} v_1$ and $\delta(\text{op}^2, v_0, v_1) = e'$ then $\vdash_{\mathbb{E}} v'$	5790
5736	<i>Proof</i> :	5791
5737	CASE $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0 :$	5792
5738	1. $\vdash_{\mathbb{E}} v_0$	5793
5739	by E inversion	5794
5740	2. QED	5795
5741	CASE $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1 :$	5796
5742	1. $\vdash_{\mathbb{E}} v_1$	5797
5743	by E inversion	5798
5744	2. QED	5799
5745	CASE $\delta(\text{sum}, v_0, v_1) = v_0 + v_1 :$	5800
5746	1. QED	5801
5747	CASE $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor :$	5802
5748	1. QED	5803
5749	CASE $\delta(\text{quotient}, v_0, v_1) = \text{BndryErr} :$	5804
5750	1. QED	5805
5751	□	5806
5752	Lemma 3.18 : <i>weakening</i>	5807
5753	• If $\Gamma \vdash_{\mathbb{E}} e$ then $x, \Gamma \vdash_{\mathbb{E}} e$	5808
5754	• If $\Gamma \vdash_{\mathbb{E}} e$ then $(x : \tau), \Gamma \vdash_{\mathbb{E}} e$	5809
5755	<i>Proof</i> :	5810
5756	QED because e is closed under Γ	5811
5757	□	5812
5758	Lemma 3.19 : <i>unique static evaluation contexts</i>	5813
5759	If $\vdash e : \tau$ then one of the following holds:	5814
5760	• e is a value	5815
5761	• $e = E[v_0 v_1]$	5816
5762	• $e = E[\text{op}^1 v]$	5817
5763	• $e = E[\text{op}^2 v_0 v_1]$	5818
5764	• $e = E[\text{Err}]$	5819
5765	<i>Proof</i> :	5820
5766	By induction on the structure of e .	5821
5767	CASE $e = x :$	5822
5768	1. Contradiction by $\vdash e : \tau$	5823
5769	CASE $e = i$	5824
5770	$\vee e = \lambda(x : \tau_d). e' :$	5825
5771	1. QED e is a value	5826
5772	CASE $e = \text{stat } \tau e' :$	5827
5773	1. Contradiction by $\vdash_1 e : K$	5828
5774		5829
5775		5830
	CASE $e = \langle e_0, e_1 \rangle :$	
	IF $e_0 \notin v :$	
	1. $e_0 = E_0[e'_0]$	
	by the induction hypothesis	
	2. $E = \langle E_0, e_1 \rangle$	
	3. QED by $e = E[e'_0]$	
	IF $e_0 \in v$	
	$\wedge e_1 \notin v :$	
	1. $e_1 = E_1[e'_1]$	
	by the induction hypothesis	
	2. $E = \langle e_0, E_1 \rangle$	
	3. QED by $e = E[e'_1]$	
	ELSE $e_0 \in v$	
	$\wedge e_1 \in v :$	
	1. $E = []$	
	2. QED $e = E[\langle e_0, e_1 \rangle]$	
	CASE $e = e_0 e_1 :$	
	IF $e_0 \notin v :$	
	1. $e_0 = E_0[e'_0]$	
	by the induction hypothesis	
	2. $E = E_0 e_1$	
	3. QED by $e = E[e'_0]$	
	IF $e_0 \in v$	
	$\wedge e_1 \notin v :$	
	1. $e_1 = E_1[e'_1]$	
	by the induction hypothesis	
	2. $E = e_0 E_1$	
	3. QED by $e = E[e'_1]$	
	ELSE $e_0 \in v$	
	$\wedge e_1 \in v :$	
	1. $E = []$	
	2. QED $e = E[e_0 e_1]$	
	CASE $e = \text{op}^1 e_0 :$	
	IF $e_0 \notin v :$	
	1. $e_0 = E_0[e'_0]$	
	by the induction hypothesis	
	2. $E = \text{op}^1 E_0$	
	3. QED $e = E[e'_0]$	
	ELSE $e_0 \in v :$	
	1. $E = []$	
	2. QED $e = E[\text{op}^1 e_0]$	
	CASE $e = \text{op}^2 e_0 e_1 :$	
	IF $e_0 \notin v :$	
	1. $e_0 = E_0[e'_0]$	
	by the induction hypothesis	
	2. $E = \text{op}^2 E_0 e_1$	
	3. QED $e = E[e'_0]$	
	IF $e_0 \in v$	
	$\wedge e_1 \notin v :$	
	1. $e_1 = E_1[e'_1]$	
	by the induction hypothesis	
	2. $E = \text{op}^2 e_0 E_1$	
	3. QED $e = E[e'_1]$	

5831	ELSE $e_0 \in v$	CASE $e = \lambda x. e'$	5886
5832	$\wedge e_1 \in v :$	1. Contradiction by $(x:\tau_x), \Gamma \vdash e : \tau$	5887
5833	1. $E = []$	CASE $e = \lambda(x:\tau'). e'$	5888
5834	2. QED $e = E[op^2 e_0 e_1]$	1. QED by $(\lambda(x:\tau'). e')[x \leftarrow v] = \lambda(x:\tau'). e'$	5889
5835	CASE $e = \text{dyn } \tau e_0 :$	CASE $e = \lambda(x':\tau'). e'$	5890
5836	1. Contradiction by e is boundary-free	1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$	5891
5837	CASE $e = \text{stat } \tau e_0 :$	2. $(x':\tau'), x, \Gamma \vdash e'$	5892
5838	1. Contradiction by $\vdash e : \tau$	by <i>static inversion forms</i>	5893
5839	CASE $e = \text{Err} :$	3. $(x':\tau'), \Gamma \vdash e'[x \leftarrow v]$	5894
5840	1. $E = []$	by the induction hypothesis (2)	5895
5841	2. QED $e = E[\text{Err}]$	4. $\Gamma \vdash \lambda(x':\tau'). (e'[x \leftarrow v])$	5896
5842	□	by (3)	5897
5843	Lemma 3.20 : \vdash <i>static inversion</i>	5. QED	5898
5844	• If $\Gamma \vdash x : \tau$ then $(x:\tau') \in \Gamma$ and $\tau' \leq \tau$	CASE $e = \langle e_0, e_1 \rangle :$	5899
5845	• If $\Gamma \vdash \lambda(x:\tau'_d). e' : \tau$ then $(x:\tau'_d), \Gamma \vdash e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$	1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	5900
5846	τ	2. $x, \Gamma \vdash e_0$	5901
5847	• If $\Gamma \vdash \langle e_0, e_1 \rangle : \tau$ then $\Gamma \vdash e_0 : \tau_0$ and $\Gamma \vdash e_1 : \tau_1$ and $\tau_0 \times \tau_1 \leq \tau$	$\wedge x, \Gamma \vdash e_1$	5902
5848	• If $\Gamma \vdash e_0 e_1 : \tau_c$ then $\Gamma \vdash e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$	by <i>static inversion forms</i>	5903
5849	• If $\Gamma \vdash \text{fst } e : \tau$ then $\Gamma \vdash e : \tau_0 \times \tau_1$ and $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$	3. $\Gamma \vdash e_0[x \leftarrow v]$	5904
5850	• If $\Gamma \vdash \text{snd } e : \tau$ then $\Gamma \vdash e : \tau_0 \times \tau_1$ and $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$	$\wedge \Gamma \vdash e_1[x \leftarrow v]$	5905
5851	• If $\Gamma \vdash \text{op}^2 e_0 e_1 : \tau$ then $\Gamma \vdash e_0 : \tau_0$ and $\Gamma \vdash e_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$	by the induction hypothesis (2)	5906
5852	• If $\Gamma \vdash \text{dyn } \tau' e' : \tau$ then $\Gamma \vdash e'$ and $\tau' \leq \tau$	4. $\Gamma \vdash \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	5907
5853	<i>Proof:</i>	by (3)	5908
5854	QED by the definition of $\Gamma \vdash e : \tau$	5. QED	5909
5855	□	CASE $e = e_0 e_1 :$	5910
5856	Lemma 3.21 : <i>canonical forms</i>	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$	5911
5857	• If $\vdash v : \tau_0 \times \tau_1$ then $v = \langle v_0, v_1 \rangle$	2. $x, \Gamma \vdash e_0$	5912
5858	• If $\vdash v : \tau_d \Rightarrow \tau_c$ then $v = \lambda(x:\tau_x). e'$	$\wedge x, \Gamma \vdash e_1$	5913
5859	$\wedge \tau_d \leq \tau_x$	by <i>static inversion forms</i>	5914
5860	• If $\vdash v : \text{Int}$ then $v = i$	3. $\Gamma \vdash e_0[x \leftarrow v]$	5915
5861	• If $\vdash v : \text{Nat}$ then $v = i$ and $v \in \mathbb{N}$	$\wedge \Gamma \vdash e_1[x \leftarrow v]$	5916
5862	<i>Proof:</i>	by the induction hypothesis (2)	5917
5863	QED by definition of $\vdash e : \tau$	4. $\Gamma \vdash e_0[x \leftarrow v] e_1[x \leftarrow v]$	5918
5864	□	by (3)	5919
5865	Lemma 3.22 : <i>substitution</i>	5. QED	5920
5866	If $(x:\tau_x), \Gamma \vdash e : \tau$, and e is boundary-free and $\vdash v : \tau_x$ then	CASE $e = \text{op}^1 e_0 :$	5921
5867	$\Gamma \vdash e[x \leftarrow v] : \tau$	1. $e[x \leftarrow v] = \text{op}^1 e_0[x \leftarrow v]$	5922
5868	<i>Proof:</i>	2. $x, \Gamma \vdash e_0$	5923
5869	By induction on the structure of e .	by <i>static inversion forms</i>	5924
5870	CASE $e = x :$	3. $\Gamma \vdash e_0[x \leftarrow v]$	5925
5871	1. $e[x \leftarrow v] = v$	by the induction hypothesis (2)	5926
5872	2. $\tau_x = \tau$	4. $\Gamma \vdash \text{op}^1 e_0[x \leftarrow v]$	5927
5873	3. $\Gamma \vdash v : \tau$	by (3)	5928
5874	by <i>weakening</i>	5. QED	5929
5875	4. QED	CASE $e = \text{op}^2 e_0 e_1 :$	5930
5876	CASE $e = x' :$	1. $e[x \leftarrow v] = \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	5931
5877	1. QED by $x'[x \leftarrow v] = x'$	2. $x, \Gamma \vdash e_0$	5932
5878	CASE $e = i :$	$\wedge x, \Gamma \vdash e_1$	5933
5879	1. QED by $i[x \leftarrow v] = i$	by <i>static inversion forms</i>	5934
5880		3. $\Gamma \vdash e_0[x \leftarrow v]$	5935
5881		$\wedge \Gamma \vdash e_1[x \leftarrow v]$	5936
5882		by the induction hypothesis (2)	5937
5883		4. $\Gamma \vdash \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	5938
5884		by (3)	5939
5885			5940

5941	5. QED	5996
5942	CASE $e = \text{dyn } \tau' e'$:	5997
5943	1. Contradiction by e is boundary-free	5998
5944	CASE $e = \text{stat } \tau' e'$:	5999
5945	1. Contradiction by e is boundary-free	6000
5946	CASE $e = \text{Err}$:	6001
5947	1. QED $\text{Err}[x \leftarrow v] = \text{Err}$	6002
5948	□	6003
5949	Lemma 3.23 : δ preservation	6004
5950	• If $\vdash v$ and $\delta(\text{op}^1, v) = v'$ then $\vdash e'$	6005
5951	• If $\vdash v_0$ and $\vdash v_1$ and $\delta(\text{op}^2, v_0, v_1) = e'$ then $\vdash v'$	6006
5952	<i>Proof</i> :	6007
5953	CASE $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$:	6008
5954	1. $\vdash v_0$	6009
5955	by <i>static inversion forms</i>	6010
5956	2. QED	6011
5957	CASE $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$:	6012
5958	1. $\vdash v_1$	6013
5959	by <i>static inversion forms</i>	6014
5960	2. QED	6015
5961	CASE $\delta(\text{sum}, v_0, v_1) = v_0 + v_1$:	6016
5962	1. QED	6017
5963	CASE $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor$:	6018
5964	1. QED	6019
5965	CASE $\delta(\text{quotient}, v_0, v_1) = \text{BndryErr}$:	6020
5966	1. QED	6021
5967	□	6022
5968	Lemma 3.24 : <i>weakening</i>	6023
5969	• If $\Gamma \vdash e$ then $x, \Gamma \vdash e$	6024
5970	• If $\Gamma \vdash e$ then $(x : \tau), \Gamma \vdash e$	6025
5971	<i>Proof</i> :	6026
5972	QED because e is closed under Γ	6027
5973	□	6028
5974		6029
5975		6030
5976		6031
5977		6032
5978		6033
5979		6034
5980		6035
5981		6036
5982		6037
5983		6038
5984		6039
5985		6040
5986		6041
5987		6042
5988		6043
5989		6044
5990		6045
5991		6046
5992		6047
5993		6048
5994		6049
5995		6050

E.4 (1) First-Order Embedding
E.4.1 First-Order Definitions
Language 1

$$\begin{aligned}
 e &= x \mid v \mid e e \mid \langle e, e \rangle \mid op^1 e \mid op^2 e e \mid \\
 &\quad dyn \tau e \mid stat \tau e \mid Err \mid chk K e \mid dyn e \mid stat e \\
 v &= i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e \\
 \tau &= Nat \mid Int \mid \tau \times \tau \mid \tau \Rightarrow \tau \\
 K &= Nat \mid Int \mid Pair \mid Fun \mid Any \\
 \Gamma &= \cdot \mid x, \Gamma \mid (x:\tau), \Gamma \\
 Err &= BndryErr \mid TagErr \\
 r &= v \mid Err \\
 E^\bullet &= [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid \\
 &\quad op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet \mid chk K E^\bullet \\
 E &= E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid \\
 &\quad op^2 E e \mid op^2 v E \mid dyn \tau E \mid stat \tau E \mid \\
 &\quad chk K E \mid dyn E \mid stat E
 \end{aligned}$$
 $\Delta : op^1 \times \tau \longrightarrow \tau$
 $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$
 $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$
 $\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$
 $\Delta(op^2, Nat, Nat) = Nat$
 $\Delta(op^2, Int, Int) = Int$
 $\tau \leqslant: \tau$

$$\frac{}{Nat \leqslant: Int} \quad \frac{\tau'_d \leqslant: \tau_d \quad \tau_c \leqslant: \tau'_c \quad \tau_0 \leqslant: \tau'_0 \quad \tau_1 \leqslant: \tau'_1}{\tau_d \Rightarrow \tau_c \leqslant: \tau'_d \Rightarrow \tau'_c \quad \tau_0 \times \tau_1 \leqslant: \tau'_0 \times \tau'_1}$$

$$\frac{}{\tau \leqslant: \tau} \quad \frac{\tau \leqslant: \tau' \quad \tau' \leqslant: \tau''}{\tau \leqslant: \tau''}$$
 $\Gamma \vdash e$

$$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$$

$$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash Err}$$

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash stat \tau e}$$
 $\Gamma \vdash e : \tau$

$$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : Nat}$$

$$\frac{}{\Gamma \vdash i : Int} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$$

$$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant: \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash Err : \tau}$$

$$\frac{\Gamma \vdash e}{\Gamma \vdash dyn \tau e : \tau}$$
 $K \leqslant: K$

$$\frac{}{K \leqslant: Any} \quad \frac{}{Nat \leqslant: Int} \quad \frac{}{K \leqslant: K} \quad \frac{K \leqslant: K' \quad K' \leqslant: K''}{K \leqslant: K''}$$
 $[\tau] = K$

$$\begin{aligned}
 [Nat] &= Nat \\
 [Int] &= Int \\
 [\tau_0 \times \tau_1] &= Pair \\
 [\tau_d \Rightarrow \tau_c] &= Fun
 \end{aligned}$$
 $\Gamma \vdash e \rightsquigarrow_d e$

$$\frac{}{\Gamma \vdash i \rightsquigarrow i} \quad \frac{\Gamma \vdash e_0 \rightsquigarrow_d e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow_d e'_1}{\Gamma \vdash \langle e_0, e_1 \rangle \rightsquigarrow_d \langle e'_0, e'_1 \rangle} \quad \frac{x, \Gamma \vdash e \rightsquigarrow_d e'}{\Gamma \vdash \lambda x. e \rightsquigarrow_d \lambda x. e'}$$

$$\frac{}{\Gamma \vdash x \rightsquigarrow x} \quad \frac{\Gamma \vdash e_0 \rightsquigarrow_d e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow_d e'_1}{\Gamma \vdash e_0 e_1 \rightsquigarrow_d e'_0 e'_1} \quad \frac{\Gamma \vdash e \rightsquigarrow_d e'}{\Gamma \vdash op^1 e \rightsquigarrow_d op^1 e'}$$

$$\frac{\Gamma \vdash e_0 \rightsquigarrow_d e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow_d e'_1}{\Gamma \vdash op^2 e_0 e_1 \rightsquigarrow_d op^2 e'_0 e'_1} \quad \frac{}{\Gamma \vdash Err \rightsquigarrow_d Err}$$

$$\frac{\Gamma \vdash e : \tau \rightsquigarrow_d e'}{\Gamma \vdash stat \tau e \rightsquigarrow_d stat \tau e'}$$

6161	$\Gamma \vdash e : \tau \rightsquigarrow e$
6162	
6163	$\frac{}{\Gamma \vdash i : \text{Nat} \rightsquigarrow i} \quad \frac{}{\Gamma \vdash i : \text{Int} \rightsquigarrow i}$
6164	
6165	$\frac{\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1 \rightsquigarrow \langle e'_0, e'_1 \rangle}$
6166	
6167	
6168	$\frac{(x : \tau_d), \Gamma \vdash e : \tau_c \rightsquigarrow e'}{\Gamma \vdash \lambda(x : \tau_d). e : \tau_d \Rightarrow \tau_c \rightsquigarrow \lambda(x : \tau_d). e'}$
6169	
6170	$\frac{}{\Gamma \vdash x : \tau \rightsquigarrow x}$
6171	
6172	$\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_d \rightsquigarrow e'_1 \quad [\tau_c] = K}{\Gamma \vdash e_0 e_1 : \tau_c \rightsquigarrow \text{chk } K(e'_0 e'_1)}$
6173	
6174	
6175	$\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad [\tau_0] = K}{\Gamma \vdash \text{fst } e : \tau_0 \rightsquigarrow \text{chk } K(\text{fst } e')}$
6176	
6177	
6178	$\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad [\tau_1] = K}{\Gamma \vdash \text{snd } e : \tau_1 \rightsquigarrow \text{chk } K(\text{snd } e')}$
6179	
6180	
6181	
6182	$\frac{\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e : \tau' \rightsquigarrow e'}{\Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1 \quad \tau' \leq \tau}$
6183	
6184	$\frac{}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau \rightsquigarrow \text{op}^2 e'_0 e'_1} \quad \frac{}{\Gamma \vdash e : \tau \rightsquigarrow e'}$
6185	
6186	$\frac{}{\Gamma \vdash \text{Err} : \tau \rightsquigarrow \text{Err}} \quad \frac{\Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash \text{dyn } \tau e : \tau \rightsquigarrow \text{dyn } \tau e'}$
6187	
6188	
6189	$\Gamma \vdash_1 e$
6190	$\frac{}{\Gamma \vdash_1 i} \quad \frac{\Gamma \vdash_1 e_0 \quad \Gamma \vdash_1 e_1}{\Gamma \vdash_1 \langle e_0, e_1 \rangle} \quad \frac{x, \Gamma \vdash_1 e}{\Gamma \vdash_1 \lambda x. e} \quad \frac{(x : \tau), \Gamma \vdash_1 e : \text{Any}}{\Gamma \vdash_1 \lambda(x : \tau). e}$
6191	
6192	
6193	
6194	$\frac{x \in \Gamma}{\Gamma \vdash_1 x} \quad \frac{(x : \tau) \in \Gamma}{\Gamma \vdash_1 x} \quad \frac{\Gamma \vdash_1 e_0 \quad \Gamma \vdash_1 e_1}{\Gamma \vdash_1 e_0 e_1} \quad \frac{\Gamma \vdash_1 e}{\Gamma \vdash_1 \text{op}^1 e}$
6195	
6196	
6197	$\frac{\Gamma \vdash_1 e_0 \quad \Gamma \vdash_1 e_1}{\Gamma \vdash_1 \text{op}^2 e_0 e_1} \quad \frac{}{\Gamma \vdash_1 \text{Err}} \quad \frac{\Gamma \vdash_1 e : [\tau]}{\Gamma \vdash_1 \text{stat } \tau e} \quad \frac{\Gamma \vdash_1 e : \text{Any}}{\Gamma \vdash_1 \text{stat } e}$
6198	
6199	
6200	
6201	
6202	
6203	
6204	
6205	
6206	
6207	
6208	
6209	
6210	
6211	
6212	
6213	
6214	
6215	

6216	$\Gamma \vdash_1 e : K$	6216
6217		6217
6218	$\frac{i \in \mathbb{N}}{\Gamma \vdash_1 i : \text{Nat}} \quad \frac{}{\Gamma \vdash_1 i : \text{Int}} \quad \frac{\Gamma \vdash_1 e_0 : \text{Any} \quad \Gamma \vdash_1 e_1 : \text{Any}}{\Gamma \vdash_1 \langle e_0, e_1 \rangle : \text{Pair}}$	6218
6219		6219
6220	$\frac{x, \Gamma \vdash_1 e}{\Gamma \vdash_1 \lambda x. e : \text{Fun}} \quad \frac{(x : \tau), \Gamma \vdash_1 e : \text{Any}}{\Gamma \vdash_1 \lambda(x : \tau). e : \text{Fun}} \quad \frac{x \in \Gamma}{\Gamma \vdash_1 x : \text{Any}}$	6220
6221		6221
6222		6222
6223		6223
6224		6224
6225	$\frac{(x : \tau) \in \Gamma}{[\tau] = K} \quad \frac{\Gamma \vdash_1 e_0 : \text{Fun}}{\Gamma \vdash_1 e_1 : \text{Any}} \quad \frac{\Gamma \vdash_1 e : \text{Pair}}{\Gamma \vdash_1 \text{fst } e : \text{Any}}$	6225
6226		6226
6227		6227
6228		6228
6229		6229
6230	$\frac{\Gamma \vdash_1 e : \text{Pair}}{\Gamma \vdash_1 \text{snd } e : \text{Any}} \quad \frac{\Gamma \vdash_1 e_0 : K_0 \quad \Gamma \vdash_1 e_1 : K_1 \quad \Delta(\text{op}^2, K_0, K_1) = K}{\Gamma \vdash_1 \text{op}^2 e_0 e_1 : K}$	6230
6231		6231
6232		6232
6233		6233
6234	$\frac{\Gamma \vdash_1 e : K' \quad K' \leq K}{\Gamma \vdash_1 e : K} \quad \frac{}{\Gamma \vdash_1 \text{Err} : K} \quad \frac{\Gamma \vdash_1 e \quad [\tau] = K}{\Gamma \vdash_1 \text{dyn } \tau e : K}$	6234
6235		6235
6236		6236
6237	$\frac{\Gamma \vdash_1 e}{\Gamma \vdash_1 \text{dyn } e : \text{Any}} \quad \frac{\Gamma \vdash_1 e : \text{Any}}{\Gamma \vdash_1 \text{chk } K e : K}$	6237
6238		6238
6239		6239
6240	$\delta(\text{op}^1, v) = e$	6240
6241	$\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$	6241
6242	$\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$	6242
6243	$\delta(\text{op}^2, v, v) = e$	6243
6244	$\delta(\text{sum}, i_0, i_1) = i_0 + i_1$	6244
6245	$\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$	6245
6246	$\delta(\text{quotient}, i_0, i_1) = \lfloor i_0 / i_1 \rfloor$	6246
6247	if $i_1 \neq 0$	6247
6248		6248
6249	$\mathcal{D}_1 : \tau \times v \rightarrow v$	6249
6250	$\mathcal{D}_1(\tau, v) = \mathcal{X}([\tau], v)$	6250
6251	$\mathcal{S}_1 : \tau \times v \rightarrow v$	6251
6252	$\mathcal{S}_1(\tau, v) = v$	6252
6253		6253
6254	$\mathcal{X} : K \times v \rightarrow v$	6254
6255	$\mathcal{X}(\text{Fun}, \lambda x. e) = \lambda x. e$	6255
6256	$\mathcal{X}(\text{Fun}, \lambda(x : \tau). e) = \lambda(x : \tau). e$	6256
6257	$\mathcal{X}(\text{Pair}, \langle v_0, v_1 \rangle) = \langle v_0, v_1 \rangle$	6257
6258	$\mathcal{X}(\text{Int}, i) = i$	6258
6259	$\mathcal{X}(\text{Nat}, i) = i$	6259
6260	if $i \in \mathbb{N}$	6260
6261	$\mathcal{X}(K, v) = \text{BndryErr}$	6261
6262	otherwise	6262
6263		6263
6264		6264
6265		6265
6266		6266
6267		6267
6268		6268
6269		6269
6270		6270

6271	$e \triangleright_{1-S} e$	
6272	$\text{dyn } v$	$\triangleright_{1-S} v$
6273	$\text{dyn } \tau v$	$\triangleright_{1-S} \mathcal{D}(\tau, v)$
6274	$\text{chk } K v$	$\triangleright_{1-S} \mathcal{X}(K, v)$
6275	$(\lambda(x:\tau). e) v$	$\triangleright_{1-S} \text{BndryErr}$
6276	if $\mathcal{X}(\lfloor \tau \rfloor, v) = \text{BndryErr}$	
6277	$(\lambda(x:\tau). e) v$	$\triangleright_{1-S} e[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v)]$
6278	$(\lambda x. e) v$	$\triangleright_{1-S} \text{dyn } (e[x \leftarrow v])$
6279	$op^1 v$	$\triangleright_{1-S} \delta(op^1, v)$
6280	$op^2 v_0 v_1$	$\triangleright_{1-S} \delta(op^2, v_0, v_1)$
6281	$e \triangleright_{1-D} e$	
6282	$\text{stat } v$	$\triangleright_{1-D} v$
6283	$\text{stat } \tau v$	$\triangleright_{1-D} \mathcal{S}(\tau, v)$
6284	$v_0 v_1$	$\triangleright_{1-D} \text{TagErr}$
6285	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$	
6286	$(\lambda(x:\tau). e) v$	$\triangleright_{1-D} \text{BndryErr}$
6287	if $\mathcal{X}(\lfloor \tau \rfloor, v) = \text{BndryErr}$	
6288	$(\lambda(x:\tau). e) v$	$\triangleright_{1-D} \text{stat } (e[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v)])$
6289	$(\lambda x. e) v$	$\triangleright_{1-D} e[x \leftarrow v]$
6290	$op^1 v$	$\triangleright_{1-D} \text{TagErr}$
6291	if $\delta(op^1, v)$ is undefined	
6292	$op^1 v$	$\triangleright_{1-D} \delta(op^1, v)$
6293	$op^2 v_0 v_1$	$\triangleright_{1-D} \text{TagErr}$
6294	if $\delta(op^2, v_0, v_1)$ is undefined	
6295	$op^2 v_0 v_1$	$\triangleright_{1-D} \delta(op^2, v_0, v_1)$
6296	$e \rightarrow_{1-S} e$	
6297	$E^*[e]$	$\rightarrow_{1-S} E^*[e']$
6298	if $e \triangleright_{1-S} e'$	
6299	$E[\text{stat } \tau E^*[e]]$	$\rightarrow_{1-S} E[\text{stat } \tau E^*[e']]$
6300	if $e \triangleright_{1-S} e'$	
6301	$E[\text{dyn } \tau E^*[e]]$	$\rightarrow_{1-S} E[\text{dyn } \tau E^*[e']]$
6302	if $e \triangleright_{1-D} e'$	
6303	$E[\text{Err}]$	$\rightarrow_{1-S} \text{Err}$
6304	$e \rightarrow_{1-D} e$	
6305	$E^*[e]$	$\rightarrow_{1-D} E^*[e']$
6306	if $e \triangleright_{1-D} e'$	
6307	$E[\text{stat } \tau E^*[e]]$	$\rightarrow_{1-D} E[\text{stat } \tau E^*[e']]$
6308	if $e \triangleright_{1-S} e'$	
6309	$E[\text{dyn } \tau E^*[e]]$	$\rightarrow_{1-D} E[\text{dyn } \tau E^*[e']]$
6310	if $e \triangleright_{1-D} e'$	
6311	$E[\text{Err}]$	$\rightarrow_{1-D} \text{Err}$
6312	$e \rightarrow_{1-S}^* e$	reflexive, transitive closure of \rightarrow_{1-S}
6313	$e \rightarrow_{1-D}^* e$	reflexive, transitive closure of \rightarrow_{1-D}
6314		
6315		
6316		
6317		
6318		
6319		
6320		
6321		
6322		
6323		
6324		
6325		

Definition 4.0 : 1 *boundary-free*

An expression e is *boundary free* if e does not contain a subterm of the form:

- $(\text{dyn } \tau' e')$,
- $(\text{stat } \tau' e')$,
- $(\text{dyn } e')$, or
- $(\text{stat } e')$.

6326
6327
6328
6329
6330
6331
6332
6333
6334
6335
6336
6337
6338
6339
6340
6341
6342
6343
6344
6345
6346
6347
6348
6349
6350
6351
6352
6353
6354
6355
6356
6357
6358
6359
6360
6361
6362
6363
6364
6365
6366
6367
6368
6369
6370
6371
6372
6373
6374
6375
6376
6377
6378
6379
6380

6381 E.4.2 First-Order Theorems

6382 Theorem 4.1 : static 1-soundness

6383 If $\vdash e : \tau$ then $\vdash e : \tau \rightsquigarrow e''$ and $\vdash_1 e'' : [\tau]$ and one of the
6384 following holds:

- 6385 • $e'' \rightarrow_{1-S}^* v$ and $\vdash_1 v : [\tau]$
- 6386 • $e'' \rightarrow_{1-S}^* E[\text{dyn } \tau' E^*[e'']]$ and $e' \triangleright_{1-D} \text{TagErr}$
- 6387 • $e'' \rightarrow_{1-S}^* E[\text{dyn } E^*[e'']]$ and $e' \triangleright_{1-D} \text{TagErr}$
- 6388 • $e'' \rightarrow_{1-S}^* \text{BndryErr}$
- 6389 • e'' diverges

6390 *Proof:*

- 6391 1. $\vdash_1 e : \tau \rightsquigarrow e''$
6392 $\wedge \vdash_1 e'' : [\tau]$
6393 by \rightsquigarrow *static soundness*
- 6394 2. QED by 1 *static progress* and 1 *static preservation*

6395 \square

6396 Theorem 4.2 : dynamic 1-soundness

6397 If $\vdash e$ then $\vdash e \rightsquigarrow e''$ and $\vdash_1 e''$ and one of the following holds:

- 6398 • $e'' \rightarrow_{1-D}^* v$ and $\vdash_1 v$
- 6399 • $e'' \rightarrow_{1-D}^* E[e']$ and $e' \triangleright_{1-D} \text{TagErr}$
- 6400 • $e'' \rightarrow_{1-D}^* \text{BndryErr}$
- 6401 • e'' diverges

6402 *Proof:*

- 6403 1. $\vdash_1 e \rightsquigarrow e''$
6404 $\wedge \vdash_1 e''$
6405 by \rightsquigarrow *dynamic soundness*
- 6406 2. QED by 1 *dynamic progress* and 1 *dynamic preservation*

6407 \square

6408 Theorem 4.3 : boundary-free 1-soundness

6409 If $\vdash e : \tau$ and e is boundary-free then one of the following
6410 holds:

- 6411 • $e \rightarrow_{1-S}^* v$ and $\vdash v : \tau$
- 6412 • $e \rightarrow_{1-S}^* \text{BndryErr}$
- 6413 • e diverges

6414 *Proof:*

6415 QED by *progress* and *preservation*

6416 \square

6417 Theorem 4.4 : H/1 base type equivalence

6418 If $\vdash e : \tau$ and all boundary terms in e are of the following
6419 four forms:

- 6420 • $\text{dyn Int } e'$
- 6421 • $\text{stat Int } e'$
- 6422 • $\text{stat Nat } e'$
- 6423 • $\text{dyn Nat } e'$

6424 and $\vdash e : \tau \rightsquigarrow e''$, then $e \rightarrow_{H-S}^* v$ if and only if $e'' \rightarrow_{1-S}^* v$.

6425 *Proof:*

- 6426 1. $\mathcal{D}_H(\text{Int}, v) = \mathcal{D}_1(\text{Int}, v)$
6427 by by definition
- 6428 2. $\mathcal{D}_H(\text{Nat}, v) = \mathcal{D}_1(\text{Nat}, v)$
6429 by by definition
- 6430 3. $\mathcal{S}_H(\text{Int}, v) = \mathcal{S}_1(\text{Int}, v)$
6431 by by definition
- 6432 4. $\mathcal{S}_H(\text{Nat}, v) = \mathcal{S}_1(\text{Nat}, v)$
6433 by by definition

6434

6435

5. QED

\square

Corollary 4.5 : 1 compilation

If $\vdash e : \tau$

and $\vdash e : \tau \rightsquigarrow e''$

and $\vdash_1 e'' : [\tau]$

and $\triangleright_{1-D'}$ is similar to \triangleright_{1-D} but without the no-op bound-
aries, as follows:

6444 $\text{chk } K v \quad \triangleright_{1-D'} \mathcal{X}(K, v)$

6445 $v_0 v_1 \quad \triangleright_{1-D'} \text{TagErr}$
6446 if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$

6447 $(\lambda(x:\tau). e) v \triangleright_{1-D'} \text{BndryErr}$
6448 if $\mathcal{X}([\tau], v) = \text{BndryErr}$

6449 $(\lambda(x:\tau). e) v \triangleright_{1-D'} e[x \leftarrow \mathcal{X}([\tau], v)]$

6450 $(\lambda x. e) v \quad \triangleright_{1-D'} e[x \leftarrow v]$

6451 $op^1 v \quad \triangleright_{1-D'} \text{TagErr}$
6452 if $\delta(op^1, v)$ is undefined

6453 $op^1 v \quad \triangleright_{1-D'} \delta(op^1, v)$

6454 $op^2 v_0 v_1 \quad \triangleright_{1-D'} \text{TagErr}$
6455 if $\delta(op^2, v_0, v_1)$ is undefined

6456 $op^2 v_0 v_1 \quad \triangleright_{1-D'} \delta(op^2, v_0, v_1)$

and $e \rightarrow_{1-D'} e$ is defined as:

6457 $E[e] \quad \rightarrow_{1-D'} E[e']$
6458 if $e \triangleright_{1-D'} e'$

6459 $E[\text{stat } \tau v] \rightarrow_{1-D'} E[\mathcal{D}_1(\tau, v)]$

6460 $E[\text{dyn } \tau v] \rightarrow_{1-D'} E[\mathcal{D}_1(\tau, v)]$

6461 $E[\text{Err}] \quad \rightarrow_{1-D'} \text{Err}$

and $\rightarrow_{1-D'}^*$ is the reflexive transitive closure of $\rightarrow_{1-D'}$

then one of the following holds:

- 6462 • $e'' \rightarrow_{1-D'}^* v$ and $\vdash_1 v : [\tau]$
- 6463 • $e'' \rightarrow_{1-D'}^* \text{TagErr}$
- 6464 • $e'' \rightarrow_{1-D'}^* \text{BndryErr}$
- 6465 • e'' diverges

6466 *Proof (sketch):* By *static 1-soundness* and the fact that \triangleright_{1-S} is a
6467 subset of $\triangleright_{1-D'}$ (modulo the dyn e and stat e boundaries). \square

E.4.3 First-Order Lemmas
Lemma 4.6 : \mathcal{D}_1 soundness

If $\vdash_1 v$ then $\vdash_1 \mathcal{D}_1(\tau, v) : \lfloor \tau \rfloor$.

Proof:

- $\mathcal{D}_1(\tau, v) = \mathcal{X}(\lfloor \tau \rfloor, v)$
- QED by *check soundness*

□

Lemma 4.7 : \mathcal{S}_1 soundness

If $\vdash_1 v : \tau$ then $\vdash_1 \mathcal{S}_1(\tau, v)$.

Proof:

- $\mathcal{S}_1(\tau, v) = \mathcal{X}(\lfloor \tau \rfloor, v)$
- QED *check soundness*

□

Lemma 4.8 : \rightsquigarrow static soundness

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash e : \tau \rightsquigarrow e'$ and $\Gamma \vdash_1 e' : \lfloor \tau \rfloor$.

Proof:

By induction on the structure of $\Gamma \vdash e : \tau$.

$$\text{CASE } \frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} :$$

1. $\Gamma \vdash x \rightsquigarrow x$
2. $\Gamma \vdash_1 x : \lfloor \tau \rfloor$
by $(x:\tau) \in \Gamma$
3. QED

$$\text{CASE } \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} :$$

1. $\Gamma \vdash e : \tau_c \rightsquigarrow e'$
 $\wedge (x:\tau_d), \Gamma \vdash e' : \lfloor \tau_c \rfloor$
by the induction hypothesis
2. $(x:\tau_d), \Gamma \vdash e' : \text{Any}$
by $\lfloor \tau_c \rfloor <: \text{Any}$
3. $\lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c \rightsquigarrow \lambda(x:\tau_d). e'$
4. $\Gamma \vdash_1 \lambda(x:\tau_d). e' : \text{Fun}$
by (2)
5. QED (3, 4)

$$\text{CASE } \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}} :$$

1. $\Gamma \vdash i : \text{Nat} \rightsquigarrow i$
2. QED by $\Gamma \vdash_1 i : \text{Nat}$

$$\text{CASE } \frac{}{\Gamma \vdash i : \text{Int}} :$$

1. $\Gamma \vdash i : \text{Int} \rightsquigarrow i$
2. QED by $\Gamma \vdash_1 i : \text{Int}$

$$\text{CASE } \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} :$$

1. $\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0$
 $\wedge \Gamma \vdash e'_0 : \lfloor \tau_0 \rfloor$
by the induction hypothesis

$$2. \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1$$

$\wedge \Gamma \vdash e'_1 : \lfloor \tau_1 \rfloor$

by the induction hypothesis

$$3. \Gamma \vdash_1 e_0 : \text{Any}$$

by $\lfloor \tau_0 \rfloor <: \text{Any}$

$$4. \Gamma \vdash_1 e_1 : \text{Any}$$

by $\lfloor \tau_1 \rfloor <: \text{Any}$

$$5. \Gamma \vdash \langle e_0, e_1 \rangle : \tau \rightsquigarrow \langle e'_0, e'_1 \rangle$$

by (1, 2)

$$6. \Gamma \vdash_1 \langle e'_0, e'_1 \rangle : \text{Pair}$$

by (3, 4)

$$7. \text{QED by (5, 6)}$$

$$\text{CASE } \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c} :$$

$$1. \Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \rightsquigarrow e'_0$$

$\wedge \Gamma \vdash_1 e'_0 : \lfloor \tau_d \Rightarrow \tau_c \rfloor$

by the induction hypothesis

$$2. \Gamma \vdash e_1 : \tau_d \rightsquigarrow e'_1$$

$\wedge \Gamma \vdash_1 e'_1 : \lfloor \tau_c \rfloor$

by the induction hypothesis

$$3. \Gamma \vdash_1 e'_0 : \text{Fun}$$

by $\lfloor \tau_d \Rightarrow \tau_c \rfloor = \text{Fun}$

$$4. \Gamma \vdash_1 e'_1 : \text{Any}$$

by $\lfloor \tau_c \rfloor <: \text{Any}$

$$5. \Gamma \vdash e_0 e_1 : \tau_c \rightsquigarrow \text{chk } \lfloor \tau_c \rfloor (e'_0 e'_1)$$

by (1, 2)

$$6. \Gamma \vdash_1 \text{chk } \lfloor \tau_c \rfloor (e'_0 e'_1) : \lfloor \tau_c \rfloor$$

by (3, 4)

$$7. \text{QED by (5, 6)}$$

$$\text{CASE } \frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(\text{op}^1, \tau_0) = \tau}{\Gamma \vdash \text{op}^1 e_0 : \tau} :$$

IF $\text{op}^1 = \text{fst}$:

$$1. \Delta(\text{fst}, \tau_0) = \tau$$

$$2. \tau_0 = \tau \times \tau'$$

by Δ *inversion*

$$3. \Gamma \vdash e_0 : \tau \times \tau' \rightsquigarrow e'_0$$

$\wedge \Gamma \vdash_1 e'_0 : \lfloor \tau \times \tau' \rfloor$

by the induction hypothesis

$$4. \Gamma \vdash_1 e'_0 : \text{Pair}$$

by $\lfloor \tau \times \tau' \rfloor = \text{Pair}$

$$5. \Gamma \vdash \text{fst } e_0 : \tau \rightsquigarrow \text{chk } \lfloor \tau \rfloor (\text{fst } e'_0)$$

by (2)

$$6. \Gamma \vdash_1 \text{chk } \lfloor \tau \rfloor (\text{fst } e'_0) : \lfloor \tau \rfloor$$

by (3)

$$7. \text{QED by 4,5}$$

ELSE $\text{op}^1 = \text{snd}$:

$$1. \Delta(\text{snd}, \tau_0) = \tau$$

$$2. \tau_0 = \tau' \times \tau$$

by Δ *inversion*

$$3. \Gamma \vdash e_0 : \tau' \times \tau \rightsquigarrow e'_0$$

$\wedge \Gamma \vdash_1 e'_0 : \lfloor \tau' \times \tau \rfloor$

by the induction hypothesis

6601 4. $\Gamma \vdash_1 e'_0 : \text{Pair}$
 6602 by $[\tau' \times \tau] = \text{Pair}$
 6603 5. $\Gamma \vdash \text{snd } e_0 : \tau \rightsquigarrow \text{chk } [\tau] (\text{snd } e'_0)$
 6604 by (2)
 6605 6. $\Gamma \vdash_1 \text{chk } [\tau] (\text{snd } e'_0) : [\tau]$
 6606 by (3)
 6607 7. QED by 4,5
 6608 **CASE** $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \quad \Delta(\text{op}^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau} :$
 6609
 6610
 6611 1. $\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0$
 6612 $\wedge \Gamma \vdash_1 e'_0 : [\tau_0]$
 6613 by the induction hypothesis
 6614 2. $\Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1$
 6615 $\wedge \Gamma \vdash_1 e'_1 : [\tau_1]$
 6616 by the induction hypothesis
 6617 3. $\Delta(\text{op}^2, [\tau_0], [\tau_1]) = [\tau]$
 6618 by Δ tag preservation
 6619 4. $\Gamma \vdash \text{op}^2 e_0 e_1 : \tau \rightsquigarrow \text{op}^2 e'_0 e'_1$
 6620 by (1, 2)
 6621 5. $\Gamma \vdash_1 \text{op}^2 e'_0 e'_1 : [\tau]$
 6622 by (1, 2, 3)
 6623 6. QED by (5, 6)
 6624 **CASE** $\frac{\Gamma \vdash e : \tau' \quad \tau' \leq \tau}{\Gamma \vdash e : \tau} :$
 6625
 6626
 6627 1. $\Gamma \vdash e : \tau' \rightsquigarrow e'$
 6628 $\wedge \Gamma \vdash_1 e' : [\tau']$
 6629 by the induction hypothesis
 6630 2. $[\tau'] \leq [\tau]$
 6631 by *subtyping preservation*
 6632 3. $\Gamma \vdash_1 e' : [\tau]$
 6633 by (2)
 6634 4. QED by (1, 3)
 6635 **CASE** $\frac{}{\Gamma \vdash \text{Err} : \tau} :$
 6636
 6637 1. $\Gamma \vdash \text{Err} : \tau \rightsquigarrow \text{Err}$
 6638 2. $\Gamma \vdash_1 \text{Err} : \tau$
 6639 3. QED
 6640 **CASE** $\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau} :$
 6641
 6642
 6643 1. $\Gamma \vdash e \rightsquigarrow e'$
 6644 $\wedge \Gamma \vdash_1 e'$
 6645 by \rightsquigarrow *dynamic soundness*
 6646 2. $\Gamma \vdash \text{dyn } \tau e : \tau \rightsquigarrow \text{dyn } \tau e'$
 6647 by (1)
 6648 3. $\Gamma \vdash_1 \text{dyn } \tau e' : [\tau]$
 6649 by (1)
 6650 4. QED by (2, 3)
 6651 \square

6652 **Lemma 4.9** : \rightsquigarrow *dynamic soundness*

6653 \blacksquare If $\Gamma \vdash e$ then $\Gamma \vdash e \rightsquigarrow e'$ and $\Gamma \vdash_1 e'$

6654 *Proof*:

6655

By induction on the structure of $\Gamma \vdash e$.

CASE $\frac{x \in \Gamma}{\Gamma \vdash x} :$

1. $\Gamma \vdash x \rightsquigarrow x$

2. $\Gamma \vdash_1 x$

by $x \in \Gamma$

3. QED

CASE $\frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} :$

1. $x, \Gamma \vdash e \rightsquigarrow e'$

$\wedge x, \Gamma \vdash_1 e'$

by the induction hypothesis

2. $\Gamma \vdash \lambda x. e \rightsquigarrow \lambda x. e'$

by (1)

3. $\Gamma \vdash_1 \lambda x. e'$

by (1)

4. QED by (2, 3)

CASE $\frac{}{\Gamma \vdash i} :$

1. $\Gamma \vdash i \rightsquigarrow i$

2. $\Gamma \vdash_1 i$

3. QED

CASE $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle} :$

1. $\Gamma \vdash e_0 \rightsquigarrow e'_0$

$\wedge \Gamma \vdash_1 e'_0$

by the induction hypothesis

2. $\Gamma \vdash e_1 \rightsquigarrow e'_1$

$\wedge \Gamma \vdash_1 e'_1$

by the induction hypothesis

3. $\Gamma \vdash \langle e_0, e_1 \rangle \rightsquigarrow \langle e'_0, e'_1 \rangle$

by (1, 2)

4. $\Gamma \vdash_1 \langle e'_0, e'_1 \rangle$

by (1, 2)

5. QED by (3, 4)

CASE $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} :$

1. $\Gamma \vdash e_0 \rightsquigarrow e'_0$

$\wedge \Gamma \vdash_1 e'_0$

by the induction hypothesis

2. $\Gamma \vdash e_1 \rightsquigarrow e'_1$

$\wedge \Gamma \vdash_1 e'_1$

by the induction hypothesis

3. $\Gamma \vdash e_0 e_1 \rightsquigarrow e'_0 e'_1$

by (1, 2)

4. $\Gamma \vdash_1 e'_0 e'_1$

by (1, 2)

5. QED by (3, 4)

6711	CASE $\frac{\Gamma \vdash e}{\Gamma \vdash op^1 e}$:	CASE $e = E^\bullet[v_0 v_1]$:	6766
6712		1. $\vdash_1 v_0 v_1 : K'$	6767
6713		by <i>static hole typing</i>	6768
6714	1. $\Gamma \vdash e \rightsquigarrow e'$	2. $\vdash_1 v_0 : \text{Fun}$	6769
6715	$\wedge \Gamma \vdash_1 e'$	by 1 inversion (1)	6770
6716	by the induction hypothesis	3. $v_0 = \lambda x. e'$	6771
6717	2. $\Gamma \vdash op^1 e \rightsquigarrow op^1 e'$	$\vee v_0 = \lambda(x:\tau_d). e'$	6772
6718	by (1)	by <i>canonical forms</i> (2)	6773
6719	3. $\Gamma \vdash_1 op^1 e'$	4. IF $v_0 = \lambda x. e'$:	6774
6720	by (1)	a. $e \rightarrow_{1-S} E^\bullet[\text{dyn}(e'[x \leftarrow v_1])]$	6775
6721	4. QED by (2, 3)	by $(\lambda x. e') v_1 \triangleright_{1-S} (\text{dyn}(e'[x \leftarrow v_1]))$	6776
6722	CASE $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1}$:	b. QED	6777
6723		IF $v_0 = \lambda(x:\tau_d). e'$	6778
6724	1. $\Gamma \vdash e_0 \rightsquigarrow e'_0$	$\wedge X([\tau_d], v_1) = v_1 :$	6779
6725	$\wedge \Gamma \vdash_1 e'_0$	a. $e \rightarrow_{1-S} E^\bullet[e'[x \leftarrow v_1]]$	6780
6726	by the induction hypothesis	by $(\lambda(x:\tau_d). e') v_1 \triangleright_{1-S} e'[x \leftarrow v_1]$	6781
6727	2. $\Gamma \vdash e_1 \rightsquigarrow e'_1$	b. QED	6782
6728	$\wedge \Gamma \vdash_1 e'_1$	ELSE $v_0 = \lambda(x:\tau_d). e'$	6783
6729	by the induction hypothesis	$\wedge X([\tau_d], v_1) = \text{BndryErr} :$	6784
6730	3. $\Gamma \vdash op^2 e_0 e_1 \rightsquigarrow op^2 e'_0 e'_1$	a. $e \rightarrow_{1-S} E^\bullet[\text{BndryErr}]$	6785
6731	by (1, 2)	by $(\lambda(x:\tau_d). e') v_1 \triangleright_{1-S} \text{BndryErr}$	6786
6732	4. $\Gamma \vdash_1 op^2 e'_0 e'_1$	b. QED	6787
6733	by (1, 2)	CASE $e = E^\bullet[op^1 v]$:	6788
6734	5. QED by 3,4	1. $op^1 = \text{fst}$	6789
6735	CASE $\frac{}{\Gamma \vdash \text{Err}}$:	$\vee op^1 = \text{snd}$	6790
6736		2. $\vdash_1 op^1 v : K'$	6791
6737	1. $\Gamma \vdash \text{Err} \rightsquigarrow \text{Err}$	by <i>static hole typing</i>	6792
6738	2. $\Gamma \vdash_1 \text{Err}$	3. $\vdash_1 v : \text{Pair}$	6793
6739	3. QED	by 1 inversion (2)	6794
6740	CASE $\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$:	4. $v = \langle v_0, v_1 \rangle$	6795
6741		by <i>canonical forms</i> (3)	6796
6742	1. $\Gamma \vdash e : \tau \rightsquigarrow e'$	5. $\delta(op^1, v) = v_i$ where $i \in \{0, 1\}$	6797
6743	$\wedge \Gamma \vdash_1 e' : [\tau]$	by (1, 3)	6798
6744	by \rightsquigarrow <i>static soundness</i>	6. $e \rightarrow_{1-S} E^\bullet[v_i]$	6799
6745	2. $\Gamma \vdash \text{stat } \tau e \rightsquigarrow \text{stat } \tau e'$	by $(op^1 v) \triangleright_{1-S} v_i$	6800
6746	by (1)	7. QED	6801
6747	3. $\Gamma \vdash_1 \text{stat } \tau e$	CASE $e = E^\bullet[op^2 v_0 v_1]$:	6802
6748	by (1)	1. $\vdash_1 op^2 v_0 v_1 : K'$	6803
6749	4. QED by (2,3)	by <i>static hole typing</i>	6804
6750	□	2. $\vdash_1 v_0 : K_0$	6805
6751		$\wedge \vdash_1 v_1 : K_1$	6806
6752		$\wedge \Delta(op^2, K_0, K_1) = K_2$	6807
6753	Lemma 4.10 : 1 <i>static progress</i>	by 1 inversion (1)	6808
6754	If $\vdash_1 e : K$ then one of the following holds:	3. $\delta(op^2, v_0, v_1) = e''$	6809
6755	• e is a value	by Δ <i>tag soundness</i>	6810
6756	• $e \in \text{Err}$	4. QED by $e \rightarrow_{1-S} E^\bullet[e'']$	6811
6757	• $e \rightarrow_{1-S} e'$	CASE $e = E^\bullet[\text{chk } K v_0]$:	6812
6758	• $e \rightarrow_{1-S} \text{BndryErr}$	1. $e \rightarrow_{1-S} E^\bullet[X(K, v)]$	6813
6759	• $e = E[\text{dyn } \tau' E^\bullet[e']]$ and $e' \rightarrow_{1-D} \text{TagErr}$	2. QED	6814
6760	• $e = E[\text{dyn } E^\bullet[e']]$ and $e' \rightarrow_{1-D} \text{TagErr}$	CASE $e = E[\text{dyn } e']$ where e' is boundary-free :	6815
6761	<i>Proof</i> :	1. e' is a value	6816
6762	By the <i>boundary factoring</i> lemma, there are ten cases.	$\vee e' \in \text{Err}$	6817
6763	CASE e is a value :	$\vee e' \rightarrow_{1-D} e''$	6818
6764	1. QED		6819
6765			6820

6821 $\vee e' \rightarrow_{1-D} \text{BndryErr}$
6822 $\vee e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$
6823 by 1 *dynamic progress*
6824 2. **IF** e' is a value :
6825 a. QED $e \rightarrow_{1-S} E[v]$
6826 **IF** $e' \in \text{Err}$:
6827 a. QED $e \rightarrow_{1-S} e'$
6828 **IF** $e' \rightarrow_{1-D} e''$:
6829 a. QED $e \rightarrow_{1-S} E[\text{dyn } e'']$
6830 **IF** $e' \rightarrow_{1-D} \text{BndryErr}$:
6831 a. QED $e \rightarrow_{1-S} E[\text{dyn BndryErr}]$
6832 **ELSE** $e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$:
6833 a. $E' \in E^\bullet$
6834 by e' is boundary-free
6835 b. QED
6836 **CASE** $e = E[\text{stat } e']$ where e' is boundary-free :
6837 1. e' is a value
6838 $\vee e' \in \text{Err}$
6839 $\vee e' \rightarrow_{1-S} e''$
6840 $\vee e' \rightarrow_{1-S} \text{BndryErr}$
6841 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
6842 $\vee e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
6843 by 1 *static progress*
6844 2. **IF** e' is a value :
6845 a. QED $e \rightarrow_{1-S} E[e']$
6846 **IF** $e' \in \text{Err}$:
6847 a. QED $e \rightarrow_{1-S} e'$
6848 **IF** $e' \rightarrow_{1-S} e''$:
6849 a. QED $e \rightarrow_{1-S} E[\text{stat } e'']$
6850 **IF** $e' \rightarrow_{1-S} \text{BndryErr}$:
6851 a. QED $e \rightarrow_{1-S} E[\text{stat BndryErr}]$
6852 **IF** $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
6853 :
6854 a. Contradiction by e' is boundary-free
6855 **ELSE** $e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
6856 :
6857 a. Contradiction by e' is boundary-free
6858 **CASE** $e = E[\text{dyn } \tau e']$ where e' is boundary-free :
6859 1. e' is a value
6860 $\vee e' \in \text{Err}$
6861 $\vee e' \rightarrow_{1-D} e''$
6862 $\vee e' \rightarrow_{1-D} \text{BndryErr}$
6863 $\vee e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$
6864 by 1 *dynamic progress*
6865 2. **IF** e' is a value :
6866 a. QED $e \rightarrow_{1-S} E[\mathcal{D}_1(\tau', e')]$
6867 **IF** $e' \in \text{Err}$:
6868 a. QED $e \rightarrow_{1-S} e'$
6869 **IF** $e' \rightarrow_{1-D} e''$:
6870 a. QED $e \rightarrow_{1-S} E[\text{dyn } \tau' e'']$
6871 **IF** $e' \rightarrow_{1-D} \text{BndryErr}$:
6872 a. QED $e \rightarrow_{1-S} E[\text{dyn } \tau' \text{BndryErr}]$
6873 **ELSE** $e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$:
6874 :
6875

a. $E' \in E^\bullet$
by e' is boundary-free
b. QED
CASE $e = E[\text{stat } \tau e']$ where e' is boundary-free :
1. e' is a value
 $\vee e' \in \text{Err}$
 $\vee e' \rightarrow_{1-S} e''$
 $\vee e' \rightarrow_{1-S} \text{BndryErr}$
 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
 $\vee e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
by 1 *static progress*
2. **IF** e' is a value :
a. QED $e \rightarrow_{1-S} E[\mathcal{S}_1(\tau', e')]$
IF $e' \in \text{Err}$:
a. QED $e \rightarrow_{1-S} e'$
IF $e' \rightarrow_{1-S} e''$:
a. QED $e \rightarrow_{1-S} E[\text{stat } \tau' e'']$
IF $e' \rightarrow_{1-S} \text{BndryErr}$:
a. QED $e \rightarrow_{1-S} E[\text{stat } \tau' \text{BndryErr}]$
IF $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
:
a. Contradiction by e' is boundary-free
ELSE $e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
:
a. Contradiction by e' is boundary-free
CASE $e = E[\text{Err}]$:
1. QED $e \rightarrow_{1-S} \text{Err}$

□

Lemma 4.11 : 1 *dynamic progress*If $\vdash_1 e : K$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{1-D} e'$
- $e \rightarrow_{1-D} \text{BndryErr}$
- $e = E[e']$ and $e' \rightarrow_{1-D} \text{TagErr}$

Proof:By the *boundary factoring* lemma, there are nine cases.**CASE** $e = v$:

1. QED

CASE $e = E^\bullet[v_0 v_1]$:**IF** $v_0 = \lambda x. e_0$:1. $e \rightarrow_{1-D} E^\bullet[e_0[x \leftarrow v_1]]$ by $(\lambda x. e_0) v_1 \triangleright_{1-D} e_0[x \leftarrow v_1]$

2. QED

IF $v_0 = \lambda(x:\tau_d). e_0$ $\wedge \mathcal{X}([\tau_d], v_1) = v_1$:1. $e \rightarrow_{1-D} E^\bullet[\text{stat } (e_0[x \leftarrow v_1])]$ by $(\lambda(x:\tau_d). e_0) v_1 \triangleright_{1-D} (\text{stat } e_0[x \leftarrow v_1])$

2. QED

IF $v_0 = \lambda(x:\tau_d). e_0$ $\wedge \mathcal{X}([\tau_d], v_1) = \text{BndryErr}$:1. $e \rightarrow_{1-D} E^\bullet[\text{BndryErr}]$ by $(\lambda(x:\tau_d). e_0) v_1 \triangleright_{1-D} \text{BndryErr}$

2. QED

6876
6877
6878
6879
6880
6881
6882
6883
6884
6885
6886
6887
6888
6889
6890
6891
6892
6893
6894
6895
6896
6897
6898
6899
6900
6901
6902
6903
6904
6905
6906
6907
6908
6909
6910
6911
6912
6913
6914
6915
6916
6917
6918
6919
6920
6921
6922
6923
6924
6925
6926
6927
6928
6929
6930

6931	ELSE $v_0 = i$	IF $e' \rightarrow_{1-S} e''$:	6986
6932	$\vee v_0 = \langle v, v' \rangle$:	a. QED $e \rightarrow_{1-S} E[\text{stat } e'']$	6987
6933	1. $e \rightarrow_{1-D} E^\bullet[\text{TagErr}]$	IF $e' \rightarrow_{1-S} \text{BndryErr}$:	6988
6934	by $v_0 v_1 \triangleright_{1-D} \text{TagErr}$	a. QED $e \rightarrow_{1-S} E[\text{stat BndryErr}]$	6989
6935	2. QED	IF $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$	6990
6936	CASE $e = E^\bullet[op^1 v]$:	:	6991
6937	IF $\delta(op^1, v) = v'$:	a. Contradiction by e' is boundary-free	6992
6938	1. $e \rightarrow_{1-D} E^\bullet[v']$	ELSE $e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$	6993
6939	by $(op^1 v) \triangleright_{1-D} v'$:	6994
6940	2. QED	a. Contradiction by e' is boundary-free	6995
6941	ELSE $\delta(op^1, v)$ is undefined :	CASE $e = E[\text{dyn } \tau e']$ where e' is boundary-free :	6996
6942	1. $e \rightarrow_{1-D} \text{TagErr}$	1. e' is a value	6997
6943	by $(op^1 v) \triangleright_{1-D} \text{TagErr}$	$\vee e' \in \text{Err}$	6998
6944	2. QED	$\vee e' \rightarrow_{1-D} e''$	6999
6945	CASE $e = E^\bullet[op^2 v_0 v_1]$:	$\vee e' \rightarrow_{1-D} \text{BndryErr}$	7000
6946	IF $\delta(op^2, v_0, v_1) = e''$:	$\vee e' = E[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$	7001
6947	1. QED by $e \rightarrow_{1-D} E[e'']$	by 1 dynamic progress	7002
6948	ELSE $\delta(op^2, v_0, v_1)$ is undefined :	2. IF e' is a value :	7003
6949	1. $e \rightarrow_{1-D} E^\bullet[\text{TagErr}]$	a. QED $e \rightarrow_{1-D} E[\mathcal{D}_1(\tau', e')]$	7004
6950	by $(op^2 v_0 v_1) \triangleright_{1-D} \text{TagErr}$	IF $e' \in \text{Err}$:	7005
6951	2. QED	a. QED $e \rightarrow_{1-D} e'$	7006
6952	CASE $e = E^\bullet[\text{chk } K v_0]$:	IF $e' \rightarrow_{1-D} e''$:	7007
6953	1. Contradiction by $\vdash_1 e$	a. QED $e \rightarrow_{1-S} E[\text{dyn } \tau' e'']$	7008
6954	CASE $e = E[\text{dyn } v]$ where e' is boundary-free :	IF $e' \rightarrow_{1-D} \text{BndryErr}$:	7009
6955	1. e' is a value	a. QED $e \rightarrow_{1-D} E[\text{dyn } \tau' \text{BndryErr}]$	7010
6956	$\vee e' \in \text{Err}$	ELSE $e' = E[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$:	7011
6957	$\vee e' \rightarrow_{1-D} e''$	a. $E \in E^\bullet$	7012
6958	$\vee e' \rightarrow_{1-D} \text{BndryErr}$	by e' is boundary-free	7013
6959	$\vee e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$	b. QED	7014
6960	by 1 dynamic progress	CASE $e = E[\text{stat } \tau e']$ where e' is boundary-free :	7015
6961	2. IF e' is a value :	1. e' is a value	7016
6962	a. QED $e \rightarrow_{1-S} E[v]$	$\vee e' \in \text{Err}$	7017
6963	IF $e' \in \text{Err}$:	$\vee e' \rightarrow_{1-S} e''$	7018
6964	a. QED $e \rightarrow_{1-S} e'$	$\vee e' \rightarrow_{1-S} \text{BndryErr}$	7019
6965	IF $e' \rightarrow_{1-D} e''$:	$\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$	7020
6966	a. QED $e \rightarrow_{1-S} E[\text{dyn } e'']$	$\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$	7021
6967	IF $e' \rightarrow_{1-D} \text{BndryErr}$:	by 1 static progress	7022
6968	a. QED $e \rightarrow_{1-S} E[\text{dyn BndryErr}]$	2. IF e' is a value :	7023
6969	ELSE $e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$:	a. QED $e \rightarrow_{1-S} E[\mathcal{S}_1(\tau', e')]$	7024
6970	a. $E' \in E^\bullet$	IF $e' \in \text{Err}$:	7025
6971	by e' is boundary-free	a. QED $e \rightarrow_{1-S} e'$	7026
6972	b. QED	IF $e' \rightarrow_{1-S} e''$:	7027
6973	CASE $e = E[\text{stat } e']$ where e' is boundary-free :	a. QED $e \rightarrow_{1-S} E[\text{stat } \tau' e'']$	7028
6974	1. e' is a value	IF $e' \rightarrow_{1-S} \text{BndryErr}$:	7029
6975	$\vee e' \in \text{Err}$	a. QED $e \rightarrow_{1-S} E[\text{stat } \tau' \text{BndryErr}]$	7030
6976	$\vee e' \rightarrow_{1-S} e''$	IF $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$	7031
6977	$\vee e' \rightarrow_{1-S} \text{BndryErr}$:	7032
6978	$\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$	a. Contradiction by e' is boundary-free	7033
6979	$\vee e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$	ELSE $e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$	7034
6980	by 1 static progress	:	7035
6981	2. IF e' is a value :	a. Contradiction by e' is boundary-free	7036
6982	a. QED $e \rightarrow_{1-S} E[e']$	CASE $e = E[\text{Err}]$:	7037
6983	IF $e' \in \text{Err}$:	1. $e \rightarrow_{1-D} \text{Err}$	7038
6984	a. QED $e \rightarrow_{1-S} e'$	2. QED	7039
6985			7040

□

Lemma 4.12 : 1 *static preservation*If $\vdash_1 e : K$ and $e \rightarrow_{1-S} e'$ then $\vdash_1 e' : K$ *Proof*:By the *boundary factoring* lemma, there are ten cases to consider.**CASE** e is a value :1. Contradiction by $e \rightarrow_{1-S} e'$ **CASE** $e = E^\bullet[v_0 v_1]$:**IF** $v_0 = \lambda x. e'$ $\wedge e \rightarrow_{1-S} E^\bullet[\text{dyn } e'[x \leftarrow v_1]]$:1. $\vdash_1 v_0 v_1 : \text{Any}$ by *static hole typing*2. $\vdash_1 v_0 : \text{Fun}$ $\wedge \vdash_1 v_1 : \text{Any}$ by *1 inversion*3. $x \vdash_1 e'$ by *1 inversion* (2)4. $\vdash_1 v_1$ by *static value inversion* (2)5. $\vdash_1 e'[x \leftarrow v_1]$ by *substitution* (3, 4)6. $\vdash_1 \text{dyn } (e'[x \leftarrow v_1]) : \text{Any}$

by (5)

7. QED by *hole substitution***IF** $v_0 = \lambda(x:\tau). e'$ $\wedge \mathcal{X}([\tau], v_1) = \text{BndryErr}$ $\wedge e \rightarrow_{1-D} E^\bullet[\text{BndryErr}]$:1. $\vdash_1 v_0 v_1 : \text{Any}$ by *static hole typing*2. $\vdash_1 \text{BndryErr} : \text{Any}$ 3. QED by *hole substitution* (2)**ELSE** $v_0 = \lambda(x:\tau). e'$ $\wedge e \rightarrow_{1-S} E^\bullet[e'[x \leftarrow \mathcal{X}([\tau], v_1)]]$:1. $\vdash_1 v_0 v_1 : \text{Any}$ by *static hole typing*2. $\vdash_1 v_0 : \text{Fun}$ $\wedge \vdash_1 v_1 : \text{Any}$ by *1 inversion* (1)3. $(x:\tau) \vdash_1 e' : \text{Any}$ by *1 inversion* (2)4. $\vdash_1 \mathcal{X}([\tau], v_1) : [\tau]$ by *check soundness* (2)5. $\vdash_1 e[x \leftarrow \mathcal{X}([\tau], v_1)] : \text{Any}$ by *substitution* (3, 4)6. QED by *hole substitution***CASE** $e = E^\bullet[op^1 v]$ $\wedge \delta(op^1, v) = v'$ $\wedge e \rightarrow_{1-S} E^\bullet[v']$:1. $\vdash_1 op^1 v : \text{Any}$ by *static hole typing*2. $\vdash_1 v : \text{Pair}$ by *1 inversion*3. $v = \langle v_0, v_1 \rangle$ by *canonical forms*4. $\vdash_1 v_0 : \text{Any}$ $\wedge \vdash_1 v_1 : \text{Any}$ by *1 inversion* (2, 3)5. $v' = v_0$ $\vee v' = v_1$ by $\delta(\text{fst}, v) = v_0$ $\wedge \delta(\text{snd}, v) = v_1$ 6. QED by *hole substitution* (5)**CASE** $e = E^\bullet[op^2 v_0 v_1]$ $\wedge \delta(op^2, v_0, v_1) = e''$ $\wedge e \rightarrow_{1-S} E^\bullet[e'']$:1. $\vdash_1 op^2 v_0 v_1 : K'$ by *static hole typing*2. $\vdash_1 v_0 : K_0$ $\wedge \vdash_1 v_1 : K_1$ $\wedge \Delta(op^2, K_0, K_1) = K''$ $\wedge K'' <: K'$ by *1 inversion* (1)3. $\vdash_1 e'' : K''$ by Δ *tag soundness* (3)4. $\vdash_1 e'' : K'$

by (2, 3)

5. QED by *hole substitution* (4)**CASE** $e = E^\bullet[\text{chk } K_0 v_0]$:1. $E^\bullet[\text{chk } K_0 v_0] \rightarrow_{1-S} E^\bullet[\mathcal{X}(K_0, v_0)]$ 2. $\vdash_1 \text{chk } K_0 v : K''$ by *static hole typing*3. $K_0 \leqslant: K''$ by *1 inversion*4. $\vdash_1 \mathcal{X}(K_0, v_0) : K_0$ by *check soundness*5. QED by (3, 4, *hole substitution*)**CASE** $e = E[\text{dyn } e']$ where e' is boundary-free :**IF** e' is a value :1. $e \rightarrow_{1-S} E[e']$ 2. $\vdash_1 \text{dyn } e' : \text{Any}$ by *boundary hole typing*3. $\vdash_1 e'$ by *1 inversion* (2)4. $\vdash_1 e' : \text{Any}$ by *dynamic value inversion* (3)5. QED by *hole substitution* (4)**ELSE** $e' \rightarrow_{1-D} e''$:1. $e \rightarrow_{1-S} E[\text{dyn } e'']$ 2. $\vdash_1 \text{dyn } e' : \text{Any}$ by *boundary hole typing*3. $\vdash_1 e'$ by *1 inversion* (2)4. $\vdash_1 e''$ by *1 dynamic preservation* (3)

7151	5. $\vdash_1 \text{dyn } e'' : \text{Any}$	5. QED by <i>hole substitution</i> (4)	7206
7152	by (4)	ELSE $e' \rightarrow_{1-S} e'' :$	7207
7153	6. QED by <i>hole substitution</i> (5)	1. $e \rightarrow_{1-S} E[\text{stat } \tau' e'']$	7208
7154	CASE $e = E[\text{stat } e']$ where e' is boundary-free :	2. $\vdash_1 \text{stat } \tau' e'$	7209
7155	IF e' is a value :	by <i>boundary hole typing</i>	7210
7156	1. $e \rightarrow_{1-S} E[e']$	3. $\vdash_1 e' : \lfloor \tau' \rfloor$	7211
7157	2. $\vdash_1 \text{stat } e'$	by 1 inversion (2)	7212
7158	by <i>boundary hole typing</i>	4. $\vdash_1 e'' : \lfloor \tau' \rfloor$	7213
7159	3. $\vdash_1 e' : \text{Any}$	by 1 static preservation (3)	7214
7160	by 1 inversion (2)	5. $\vdash_1 \text{stat } \tau' e''$	7215
7161	4. $\vdash_1 e'$	by (4)	7216
7162	by <i>static value inversion</i> (3)	6. QED by <i>hole substitution</i> (5)	7217
7163	5. QED by <i>hole substitution</i> (4)	CASE $e = E[\text{Err}] :$	7218
7164	ELSE $e' \rightarrow_{1-S} e'' :$	1. $e \rightarrow_{1-S} \text{Err}$	7219
7165	1. $e \rightarrow_{1-S} E[\text{stat } e'']$	2. QED $\vdash_1 \text{Err} : K$	7220
7166	2. $\vdash_1 \text{stat } e'$	□	7221
7167	by <i>boundary hole typing</i>		7222
7168	3. $\vdash_1 e' : \text{Any}$	Lemma 4.13 : 1 <i>dynamic preservation</i>	7223
7169	by 1 inversion (2)	▮ If $\vdash_1 e$ and $e \rightarrow_{1-D} e'$ then $\vdash_1 e'$	7224
7170	4. $\vdash_1 e'' : \text{Any}$	<i>Proof</i> :	7225
7171	by 1 static preservation (3)	By <i>boundary factoring</i> there are nine cases.	7226
7172	5. $\vdash_1 \text{stat } e''$	CASE e is a value :	7227
7173	by (4)	1. Contradiction by $e \rightarrow_{1-D} e'$	7228
7174	6. QED by <i>hole substitution</i> (5)	CASE $e = E^\bullet[v_0 v_1] :$	7229
7175	CASE $e = E[\text{dyn } \tau e']$ where e' is boundary-free :	IF $v_0 = \lambda x. e'$	7230
7176	IF e' is a value :	$\wedge e \rightarrow_{1-D} E^\bullet[e'[x \leftarrow v_1]] :$	7231
7177	1. $e \rightarrow_{1-S} E[\mathcal{D}_1(\tau', e')]$	1. $\vdash_1 v_0 v_1$	7232
7178	2. $\vdash_1 \text{dyn } \tau' e' : \lfloor \tau' \rfloor$	by <i>dynamic hole typing</i>	7233
7179	by <i>boundary hole typing</i>	2. $\vdash_1 v_0$	7234
7180	3. $\vdash_1 e'$	$\wedge \vdash_1 v_1$	7235
7181	by 1 inversion (2)	by 1 inversion (1)	7236
7182	4. $\vdash_1 \mathcal{D}_1(\tau', e') : \lfloor \tau' \rfloor$	3. $x \vdash_1 e'$	7237
7183	by \mathcal{D}_1 <i>soundness</i> (3)	by 1 inversion (2)	7238
7184	5. QED by <i>hole substitution</i> (4)	4. $\vdash_1 e'[x \leftarrow v_1]$	7239
7185	ELSE $e' \rightarrow_{1-D} e'' :$	by <i>substitution</i> (2, 3)	7240
7186	1. $e \rightarrow_{1-S} E[\text{dyn } \tau' e'']$	5. QED by <i>hole substitution</i>	7241
7187	2. $\vdash_1 \text{dyn } \tau' e' : \lfloor \tau' \rfloor$	IF $v_0 = \lambda(x:\tau). e'$	7242
7188	by <i>boundary hole typing</i>	$\wedge \mathcal{X}(\lfloor \tau \rfloor, v_1) = \text{BndryErr}$	7243
7189	3. $\vdash_1 e'$	$\wedge e \rightarrow_{1-D} E^\bullet[\text{BndryErr}] :$	7244
7190	by 1 inversion (2)	1. $\vdash_1 v_0 v_1$	7245
7191	4. $\vdash_1 e''$	by <i>dynamic hole typing</i>	7246
7192	by 1 dynamic preservation (3)	2. $\vdash_1 \text{BndryErr}$	7247
7193	5. $\vdash_1 \text{dyn } \tau' e'' : \lfloor \tau' \rfloor$	3. QED by <i>hole substitution</i> (2)	7248
7194	by (4)	ELSE $v_0 = \lambda(x:\tau). e'$	7249
7195	6. QED by <i>hole substitution</i> (5)	$\wedge e \rightarrow_{1-D} E^\bullet[\text{stat } (e'[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v_1)])] :$	7250
7196	CASE $e = E[\text{stat } \tau e']$ where e' is boundary-free :	1. $\vdash_1 v_0 v_1$	7251
7197	IF e' is a value :	by <i>dynamic hole typing</i>	7252
7198	1. $e \rightarrow_{1-S} E[\mathcal{S}_1(\tau', e')]$	2. $\vdash_1 v_0$	7253
7199	2. $\vdash_1 \text{stat } \tau' e'$	$\wedge \vdash_1 v_1$	7254
7200	by <i>boundary hole typing</i>	by 1 inversion (1)	7255
7201	3. $\vdash_1 e' : \lfloor \tau' \rfloor$	3. $(x:\tau) \vdash_1 e : \text{Any}$	7256
7202	by 1 inversion (2)	by 1 inversion (2)	7257
7203	4. $\vdash_1 \mathcal{S}_1(\tau', e')$	4. $\vdash_1 \mathcal{X}(\lfloor \tau \rfloor, v_1) : \lfloor \tau \rfloor$	7258
7204	by \mathcal{S}_1 <i>soundness</i> (3)	by <i>check soundness</i> (2)	7259
7205			7260

7261	5. $\vdash_1 e[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v_1)] : \text{Any}$	4. $\vdash_1 e'$	7316
7262	by <i>substitution</i> (3, 4)	by <i>static value inversion</i> (3)	7317
7263	6. $\vdash_1 \text{stat}(e[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v_1)])$	5. QED by <i>hole substitution</i> (5)	7318
7264	by (5)	ELSE $e' \rightarrow_{1-S} e'' :$	7319
7265	7. QED by <i>hole substitution</i> (6)	1. $e \rightarrow_{1-D} E[\text{stat } e'']$	7320
7266	CASE $e = E^\bullet[op^1 v]$	2. $\vdash_1 \text{stat } e'$	7321
7267	$\wedge \delta(op^1, v) = v'$	by <i>boundary hole typing</i>	7322
7268	$\wedge e \rightarrow_{1-D} E^\bullet[v'] :$	3. $\vdash_1 e' : \text{Any}$	7323
7269	1. $\vdash_1 op^1 v$	by <i>1 inversion</i> (2)	7324
7270	by <i>dynamic hole typing</i>	4. $\vdash_1 e'' : \text{Any}$	7325
7271	2. $\vdash_1 v$	by <i>1 static preservation</i> (3)	7326
7272	by <i>1 inversion</i> (1)	5. $\vdash_1 \text{stat } e''$	7327
7273	3. $\vdash_1 v'$	by (4)	7328
7274	by <i>δ preservation</i> (2)	6. QED by <i>hole substitution</i> (5)	7329
7275	4. QED by <i>hole substitution</i> (3)	CASE $e = E[\text{dyn } \tau e']$ where e' is boundary-free :	7330
7276	CASE $e = E^\bullet[op^2 v_0 v_1]$	IF e' is a value :	7331
7277	$\wedge \delta(op^2, v_0, v_1) = e''$	1. $e \rightarrow_{1-D} E[\mathcal{D}_1(\tau', e')]$	7332
7278	$\wedge e \rightarrow_{1-D} E^\bullet[e''] :$	2. $\vdash_1 \text{dyn } \tau' e' : \lfloor \tau' \rfloor$	7333
7279	1. $\vdash_1 op^2 v_0 v_1$	by <i>boundary hole typing</i>	7334
7280	by <i>dynamic hole typing</i>	3. $\vdash_1 e'$	7335
7281	2. $\vdash_1 v_0$	by <i>1 inversion</i> (2)	7336
7282	$\wedge \vdash_1 v_1$	4. $\vdash_1 \mathcal{D}_1(\tau', e') : \lfloor \tau' \rfloor$	7337
7283	by <i>1 inversion</i> (1)	by <i>\mathcal{D}_1 soundness</i> (3)	7338
7284	3. $\vdash_1 e''$	5. QED by <i>hole substitution</i> (4)	7339
7285	by <i>δ preservation</i> (2)	ELSE $e' \rightarrow_{1-D} e'' :$	7340
7286	4. QED by <i>hole substitution</i> (3)	1. $e \rightarrow_{1-D} E[\text{dyn } \tau' e'']$	7341
7287	CASE $e = E[\text{dyn } e']$ where e' is boundary-free :	2. $\vdash_1 \text{dyn } \tau' e' : \lfloor \tau' \rfloor$	7342
7288	IF e' is a value :	by <i>boundary hole typing</i>	7343
7289	1. $e \rightarrow_{1-D} E[e']$	3. $\vdash_1 e'$	7344
7290	2. $\vdash_1 \text{dyn } e' : \text{Any}$	$\wedge \tau' \leq: \tau''$	7345
7291	by <i>boundary hole typing</i>	by <i>1 inversion</i> (2)	7346
7292	3. $\vdash_1 e'$	4. $\vdash_1 e''$	7347
7293	by <i>1 inversion</i> (2)	by <i>1 dynamic preservation</i> (3)	7348
7294	4. $\vdash_1 e' : \text{Any}$	5. $\vdash_1 \text{dyn } \tau' e'' : \lfloor \tau' \rfloor$	7349
7295	by <i>\mathcal{D}_1 soundness</i> (3)	by (4)	7350
7296	5. QED by <i>hole substitution</i> (4)	6. QED by <i>hole substitution</i> (5)	7351
7297	ELSE $e' \rightarrow_{1-D} e'' :$	CASE $e = E[\text{stat } \tau e']$ where e' is boundary-free :	7352
7298	1. $e \rightarrow_{1-D} E[\text{dyn } e'']$	IF $e' \in v :$	7353
7299	2. $\vdash_1 \text{dyn } e' : \text{Any}$	1. $e \rightarrow_{1-D} E[\mathcal{S}_1(\tau', e')]$	7354
7300	by <i>boundary hole typing</i>	2. $\vdash_1 \text{stat } \tau' e'$	7355
7301	3. $\vdash_1 e'$	by <i>boundary hole typing</i>	7356
7302	by <i>1 inversion</i> (2)	3. $\vdash_1 e' : \lfloor \tau' \rfloor$	7357
7303	4. $\vdash_1 e''$	by <i>1 inversion</i> (2)	7358
7304	by <i>1 dynamic preservation</i> (3)	4. $\vdash_1 \mathcal{S}_1(\tau', e')$	7359
7305	5. $\vdash_1 \text{dyn } e'' : \text{Any}$	by <i>\mathcal{S}_1 soundness</i> (3)	7360
7306	by (4)	5. QED by <i>hole substitution</i> (5)	7361
7307	6. QED by <i>hole substitution</i> (5)	ELSE $e' \rightarrow_{1-S} e'' :$	7362
7308	CASE $e = E[\text{stat } e']$ where e' is boundary-free :	1. $e \rightarrow_{1-D} E[\text{stat } \tau' e'']$	7363
7309	IF $e' \in v :$	2. $\vdash_1 \text{stat } \tau' e'$	7364
7310	1. $e \rightarrow_{1-D} E[e']$	by <i>boundary hole typing</i>	7365
7311	2. $\vdash_1 \text{stat } e'$	3. $\vdash_1 e' : \lfloor \tau' \rfloor$	7366
7312	by <i>boundary hole typing</i>	by <i>1 inversion</i> (2)	7367
7313	3. $\vdash_1 e' : \text{Any}$	4. $\vdash_1 e'' : \lfloor \tau' \rfloor$	7368
7314	by <i>1 inversion</i> (2)	by <i>1 static preservation</i> (3)	7369
7315			7370

- 7371 5. \vdash_1 stat $\tau' e''$
 7372 by (4)
 7373 6. QED by *hole substitution* (5)
 7374 **CASE** $e = E[\text{Err}]$:
 7375 1. $e \rightarrow_{1-D} \text{Err}$
 7376 2. QED $\vdash_1 \text{Err}$

7377 \square

7378 **Lemma 4.14** : *boundary-free progress*

7379 If $\vdash e : \tau$ and e is boundary-free, then one of the following
 7380 holds:

- 7381 • e is a value
- 7382 • $e \rightarrow_{1-S} e'$
- 7383 • $e \rightarrow_{1-S} \text{BndryErr}$

7384 *Proof*:

7385 By the *L unique static evaluation contexts* lemma, there
 7386 are five cases:

7387 **CASE** $e = v$:

7388 1. QED

7389 **CASE** $e = E^*[v_0 v_1]$:

7390 **IF** $v_0 = \lambda(x:\tau'). e'$:

- 7391 1. $e \rightarrow_{1-S} E^*[e'[x \leftarrow v_1]]$
 7392 by $v_0 v_1 \triangleright_{1-S} e'[x \leftarrow v_1]$

7393 2. QED

7394 **ELSE** $v_0 = \lambda x. e'$

7395 $\vee v_0 = i$

7396 $\vee v_0 = \langle v, v' \rangle$:

- 7397 1. Contradiction by $\vdash e : \tau$

7398 **CASE** $e = E^*[op^1 v]$:

7399 **IF** $\delta(op^1, v) = e''$:

- 7400 1. $e \rightarrow_{1-S} E^*[e'']$
 7401 by $(op^1 v) \triangleright_{1-S} e''$

7402 2. QED

7403 **ELSE** $\delta(op^1, v)$ is undefined :

- 7404 1. Contradiction by $\vdash e : \tau$

7405 **CASE** $e = E^*[op^2 v_0 v_1]$:

7406 **IF** $\delta(op^2, v_0, v_1) = e''$:

- 7407 1. $e \rightarrow_{1-S} E^*[e'']$
 7408 by $(op^2 v_0 v_1) \triangleright_{1-S} e''$

7409 2. QED

7410 **IF** $\delta(op^2, v_0, v_1) = \text{BndryErr}$:

- 7411 1. $e \rightarrow_{1-S} \text{BndryErr}$
 7412 by $(op^2 v_0 v_1) \triangleright_{1-S} \text{BndryErr}$

7413 2. QED

7414 **ELSE** $\delta(op^2, v_0, v_1)$ is undefined :

- 7415 1. Contradiction by $\vdash e : \tau$

7416 **CASE** $e = E^*[\text{Err}]$:

- 7417 1. $E^*[\text{Err}] \rightarrow_{1-S} \text{Err}$
- 7418 2. QED

7419 \square

7420 **Lemma 4.15** : 1 *boundary-free preservation*

7421 If $\vdash e : \tau$ and e is boundary-free and $e \rightarrow_{1-S} e'$ then $\vdash e' : \tau$
 7422 and e' is boundary-free.

7423 *Proof*:

7424

7425

By the *L unique static evaluation contexts* lemma, there
 are five cases.

CASE e is a value :

- 7429 1. Contradiction by $e \rightarrow_{1-S} e'$

CASE $e = E^*[v_0 v_1]$:

IF $v_0 = \lambda(x:\tau_d). e'$:

7432 1. $E^*[v_0 v_1] \rightarrow_{1-S} E^*[e'[x \leftarrow v_1]]$

7433 2. $\vdash v_0 v_1 : \tau_c$

7434 3. $\vdash v_0 : \tau_d \Rightarrow \tau_c$

7435 $\wedge \vdash v_1 : \tau_d$

7436 by (2)

7437 4. $(x:\tau_d) \vdash e' : \tau_c$

7438 by (3)

7439 5. $\vdash e'[x \leftarrow v_1] : \tau_c$

7440 by *substitution* (3, 4)

7441 6. $e'[x \leftarrow v_1]$ is boundary-free

7442 by e' and v_1 are boundary-free

7443 7. QED

ELSE :

- 7445 1. Contradiction by $\vdash e : \tau$

CASE $e = E^*[op^1 v]$:

7447 1. $E^*[op^1 v] \rightarrow_{1-S} E^*[v']$

7448 $\wedge \delta(op^1, v) = e''$

7449 2. $\vdash op^1 v : \tau'$

7450 3. $\vdash v : \tau_0$

7451 4. $\vdash e'' : \tau'$

7452 by *δ preservation* (3)

7453 5. QED

CASE $e = E^*[op^2 v_0 v_1]$:

7455 1. $E^*[op^2 v_0 v_1] \rightarrow_{1-S} E^*[v']$

7456 $\wedge \delta(op^2, v_0, v_1) = e''$

7457 2. $\vdash op^2 v_0 v_1 : \tau'$

7458 3. $\vdash v_0 : \tau_0$

7459 $\wedge \vdash v_1 : \tau_1$

7460 4. $\vdash e'' : \tau'$

7461 by *δ preservation* (3)

7462 5. QED

CASE $e = E^*[\text{Err}]$:

7464 1. $E^*[\text{Err}] \rightarrow_{1-S} \text{Err}$

7465 2. QED by $\vdash \text{Err} : \tau$

7466 \square

Lemma 4.16 : \mathcal{X} *soundness*

For all K and v , $\vdash_1 \mathcal{X}(K, v) : K$.

Proof:

CASE $\vdash_1 v : K$:

7471 1. $\mathcal{X}(K, v) = v$

7472 2. QED

CASE $\nmid_1 v : K$:

7474 1. $\mathcal{X}(K, v) = \text{BndryErr}$

7475 2. QED

7476 \square

Lemma 4.17 : 1 *static boundary factoring*

7426

7427

7428

7429

7430

7431

7432

7433

7434

7435

7436

7437

7438

7439

7440

7441

7442

7443

7444

7445

7446

7447

7448

7449

7450

7451

7452

7453

7454

7455

7456

7457

7458

7459

7460

7461

7462

7463

7464

7465

7466

7467

7468

7469

7470

7471

7472

7473

7474

7475

7476

7477

7478

7479

7480

7481 If $\vdash_1 e : K$ then one of the following holds:

- 7482 • e is a value
- 7483 • $e = E^\bullet[v_0 v_1]$
- 7484 • $e = E^\bullet[op^1 v]$
- 7485 • $e = E^\bullet[op^2 v_0 v_1]$
- 7486 • $e = E^\bullet[\text{chk } K v]$
- 7487 • $e = E[\text{dyn } e']$ where e' is boundary-free
- 7488 • $e = E[\text{stat } e']$ where e' is boundary-free
- 7489 • $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- 7490 • $e = E[\text{stat } \tau e']$ where e' is boundary-free
- 7491 • $e = E[\text{Err}]$

7492 *Proof:*

7493 By the *unique evaluation contexts* lemma, there are ten cases.

7494 **CASE** e is a value :

7495 1. QED

7496 **CASE** $e = E[v_0 v_1]$:

7497 1. $E = E^\bullet$

7498 $\vee E = E'[\text{dyn } E^\bullet]$

7499 $\vee E = E'[\text{stat } E^\bullet]$

7500 $\vee E = E'[\text{dyn } \tau E^\bullet]$

7501 $\vee E = E'[\text{stat } \tau E^\bullet]$

7502 by *inner boundary*

7503 2. **IF** $E = E^\bullet$:

7504 a. QED $e = E^\bullet[v_0 v_1]$

7505 **IF** $E = E'[\text{dyn } E^\bullet]$:

7506 a. QED $e = E'[\text{dyn } E^\bullet[v_0 v_1]]$

7507 **IF** $E = E'[\text{stat } E^\bullet]$:

7508 a. QED $e = E'[\text{stat } E^\bullet[v_0 v_1]]$

7509 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:

7510 a. QED $e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$

7511 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:

7512 a. QED $e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$

7513 **CASE** $e = E[op^1 v]$:

7514 1. $E = E^\bullet$

7515 $\vee E = E'[\text{dyn } E^\bullet]$

7516 $\vee E = E'[\text{stat } E^\bullet]$

7517 $\vee E = E'[\text{dyn } \tau E^\bullet]$

7518 $\vee E = E'[\text{stat } \tau E^\bullet]$

7519 by *inner boundary*

7520 2. **IF** $E = E^\bullet$:

7521 a. QED $e = E^\bullet[op^1 v]$

7522 **IF** $E = E'[\text{dyn } E^\bullet]$:

7523 a. QED $e = E'[\text{dyn } E^\bullet[op^1 v]]$

7524 **IF** $E = E'[\text{stat } E^\bullet]$:

7525 a. QED $e = E'[\text{stat } E^\bullet[op^1 v]]$

7526 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:

7527 a. QED $e = E'[\text{dyn } \tau E^\bullet[op^1 v]]$

7528 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:

7529 a. QED $e = E'[\text{stat } \tau E^\bullet[op^1 v]]$

7530 **CASE** $e = E[op^2 v_0 v_1]$:

7531 1. $E = E^\bullet$

7532 $\vee E = E'[\text{dyn } E^\bullet]$

7533 $\vee E = E'[\text{stat } E^\bullet]$

7536 $\vee E = E'[\text{dyn } \tau E^\bullet]$

7537 $\vee E = E'[\text{stat } \tau E^\bullet]$

7538 by *inner boundary*

7539 2. **IF** $E = E^\bullet$:

7540 a. QED $e = E^\bullet[op^2 v_0 v_1]$

7541 **IF** $E = E'[\text{dyn } E^\bullet]$:

7542 a. QED $e = E'[\text{dyn } E^\bullet[op^2 v_0 v_1]]$

7543 **IF** $E = E'[\text{stat } E^\bullet]$:

7544 a. QED $e = E'[\text{stat } E^\bullet[op^2 v_0 v_1]]$

7545 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:

7546 a. QED $e = E'[\text{dyn } \tau E^\bullet[op^2 v_0 v_1]]$

7547 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:

7548 a. QED $e = E'[\text{stat } \tau E^\bullet[op^2 v_0 v_1]]$

7549 **CASE** $e = E[\text{dyn } v]$:

7550 1. QED v is boundary-free

7551 **CASE** $e = E[\text{stat } v]$:

7552 1. QED v is boundary-free

7553 **CASE** $e = E[\text{dyn } \tau v]$:

7554 1. QED v is boundary-free

7555 **CASE** $e = E[\text{stat } \tau v]$:

7556 1. QED v is boundary-free

7557 **CASE** $e = E[\text{Err}]$:

7558 1. QED

7559 \square

7560 **Lemma 4.18** : 1 *unique static evaluation contexts*

7561 If $\vdash_1 e : K$ then one of the following holds:

7562 • e is a value

7563 • $e = E[v_0 v_1]$

7564 • $e = E[op^1 v]$

7565 • $e = E[op^2 v_0 v_1]$

7566 • $e = E[\text{chk } K v]$

7567 • $e = E[\text{dyn } v]$

7568 • $e = E[\text{stat } v]$

7569 • $e = E[\text{dyn } \tau v]$

7570 • $e = E[\text{stat } \tau v]$

7571 • $e = E[\text{Err}]$

7572 *Proof:*

7573 By induction on the structure of e .

7574 **CASE** $e = x$:

7575 1. Contradiction by $\vdash_1 e : K$

7576 **CASE** $e = i$

7577 $\vee e = \lambda x. e'$

7578 $\vee e = \lambda(x:\tau_d). e'$

7579 1. QED e is a value

7580 **CASE** $e = \langle e_0, e_1 \rangle$:

7581 **IF** $e_0 \notin v$:

7582 1. $e_0 = E_0[e'_0]$

7583 by the induction hypothesis

7584 2. $E = \langle E_0, e_1 \rangle$

7585 3. QED by $e = E[e'_0]$

7586 **IF** $e_0 \in v$

7587 $\wedge e_1 \notin v$:

7588 1. $e_1 = E_1[e'_1]$

7589 by the induction hypothesis

7590

7591	2. $E = \langle e_0, E_1 \rangle$	1. $E = []$	7646
7592	3. QED by $e = E[e'_1]$	2. QED $e = E[\text{chk } K \ e_0]$	7647
7593	ELSE $e_0 \in v$	CASE $e = \text{dyn } e_0 :$	7648
7594	$\wedge e_1 \in v :$	IF $e_0 \notin v :$	7649
7595	1. $E = []$	1. $\vdash_1 e_0$	7650
7596	2. QED $e = E[\langle e_0, e_1 \rangle]$	by 1 <i>inversion</i>	7651
7597	CASE $e = e_0 \ e_1 :$	2. $e_0 = E_0[e'_0]$	7652
7598	IF $e_0 \notin v :$	by <i>unique evaluation contexts</i> (1)	7653
7599	1. $e_0 = E_0[e'_0]$	3. $E = \text{dyn } E_0$	7654
7600	by the induction hypothesis	4. QED $e = E[e'_0]$	7655
7601	2. $E = E_0 \ e_1$	ELSE $e_0 \in v :$	7656
7602	3. QED by $e = E[e'_0]$	1. $E = []$	7657
7603	IF $e_0 \in v$	2. QED $e = E[\text{dyn } e_0]$	7658
7604	$\wedge e_1 \notin v :$	CASE $e = \text{stat } e_0 :$	7659
7605	1. $e_1 = E_1[e'_1]$	1. Contradiction by $\vdash_1 e : K$	7660
7606	by the induction hypothesis	CASE $e = \text{dyn } \tau \ e_0 :$	7661
7607	2. $E = e_0 \ E_1$	IF $e_0 \notin v :$	7662
7608	3. QED by $e = E[e'_1]$	1. $\vdash_1 e_0$	7663
7609	ELSE $e_0 \in v$	by 1 <i>inversion</i>	7664
7610	$\wedge e_1 \in v :$	2. $e_0 = E_0[e'_0]$	7665
7611	1. $E = []$	by <i>unique evaluation contexts</i> (1)	7666
7612	2. QED $e = E[e_0 \ e_1]$	3. $E = \text{dyn } \tau \ E_0$	7667
7613	CASE $e = \text{op}^1 \ e_0 :$	4. QED $e = E[e'_0]$	7668
7614	1. IF $e_0 \notin v :$	ELSE $e_0 \in v :$	7669
7615	a. $e_0 = E_0[e'_0]$	1. $E = []$	7670
7616	by the induction hypothesis	2. QED $e = E[\text{dyn } \tau \ e_0]$	7671
7617	b. $E = \text{op}^1 \ E_0$	CASE $e = \text{stat } K' \ e_0 :$	7672
7618	c. QED $e = E[e'_0]$	1. Contradiction by $\vdash_1 e : K$	7673
7619	2. ELSE $e_0 \in v :$	CASE $e = \text{Err} :$	7674
7620	a. $E = []$	1. $E = []$	7675
7621	b. QED $e = E[\text{op}^1 \ e_0]$	2. QED $e = E[\text{Err}]$	7676
7622	CASE $e = \text{op}^2 \ e_0 \ e_1 :$	□	7677
7623	IF $e_0 \notin v :$	Lemma 4.19 : 1 <i>inner boundary</i>	7678
7624	1. $e_0 = E_0[e'_0]$	For all contexts E , one of the following holds:	7679
7625	by the induction hypothesis	• $E = E^\bullet$	7680
7626	2. $E = \text{op}^2 \ E_0 \ e_1$	• $E = E'[\text{dyn } v]$	7681
7627	3. QED $e = E[e'_0]$	• $E = E'[\text{stat } v]$	7682
7628	IF $e_0 \in v$	• $E = E'[\text{dyn } \tau \ E^\bullet]$	7683
7629	$\wedge e_1 \notin v :$	• $E = E'[\text{stat } \tau \ E^\bullet]$	7684
7630	1. $e_1 = E_1[e'_1]$	<i>Proof</i> :	7685
7631	by the induction hypothesis	By induction on the structure of E .	7686
7632	2. $E = \text{op}^2 \ e_0 \ E_1$	CASE $E = E^\bullet :$	7687
7633	3. QED $e = E[e'_1]$	1. QED	7688
7634	ELSE $e_0 \in v$	CASE $E = E_0 \ e_1 :$	7689
7635	$\wedge e_1 \in v :$	1. $E_0 = E^\bullet$	7690
7636	1. $E = []$	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	7691
7637	2. QED $e = E[\text{op}^2 \ e_0 \ e_1]$	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	7692
7638	CASE $e = \text{chk } K \ e_0 :$	$\vee E_0 = E'_0[\text{dyn } \tau \ E^\bullet]$	7693
7639	IF $e_0 \notin v :$	$\vee E_0 = E'_0[\text{stat } \tau \ E^\bullet]$	7694
7640	1. $e_0 = E_0[e'_0]$	by the induction hypothesis	7695
7641	by the induction hypothesis	2. IF $E_0 = E^\bullet :$	7696
7642	2. $E = \text{chk } K \ E_0$	a. QED E is boundary-free	7697
7643	3. QED $e = E[e'_0]$	IF $E_0 = E'_0[\text{dyn } E^\bullet] :$	7698
7644	ELSE $e_0 \in v :$	a. $E' = E'_0 \ e_1$	7699
7645			7700

7701	b. QED $E = E'[\text{dyn } E^\bullet]$	1. $E_1 = E^\bullet$	7756
7702	IF $E_0 = E'_0[\text{stat } E^\bullet]$:	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	7757
7703	a. $E' = E'_0 e_1$	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	7758
7704	b. QED $E = E'[\text{stat } E^\bullet]$	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	7759
7705	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	7760
7706	a. $E' = E'_0 e_1$	by the induction hypothesis	7761
7707	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	2. IF $E_1 = E^\bullet$:	7762
7708	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:	a. QED E is boundary-free	7763
7709	a. $E' = E'_0 e_1$	IF $E_1 = E'_1[\text{dyn } E^\bullet]$:	7764
7710	b. QED $E = E'[\text{stat } \tau E^\bullet]$	a. $E' = \langle v_0, E'_1 \rangle$	7765
7711	CASE $E = v_0 E_1$:	b. QED $E = E'[\text{dyn } E^\bullet]$	7766
7712	1. $E_1 = E^\bullet$	IF $E_1 = E'_1[\text{stat } E^\bullet]$:	7767
7713	$\vee E_1 = E'_1[\text{dyn } E^\bullet]$	a. $E' = \langle v_0, E'_1 \rangle$	7768
7714	$\vee E_1 = E'_1[\text{stat } E^\bullet]$	b. QED $E = E'[\text{stat } E^\bullet]$	7769
7715	$\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$	IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:	7770
7716	$\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$	a. $E' = \langle v_0, E'_1 \rangle$	7771
7717	by the induction hypothesis	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	7772
7718	2. IF $E_1 = E^\bullet$:	ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:	7773
7719	a. QED E is boundary-free	a. $E' = \langle v_0, E'_1 \rangle$	7774
7720	IF $E_1 = E'_1[\text{dyn } E^\bullet]$:	b. QED $E = E'[\text{stat } \tau E^\bullet]$	7775
7721	a. $E' = v_0 E'_1$	CASE $E = op^1 E_0$:	7776
7722	b. QED $E = E'[\text{dyn } E^\bullet]$	1. $E_0 = E^\bullet$	7777
7723	IF $E_1 = E'_1[\text{stat } E^\bullet]$:	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	7778
7724	a. $E' = v_0 E'_1$	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	7779
7725	b. QED $E = E'[\text{stat } E^\bullet]$	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	7780
7726	IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	7781
7727	a. $E' = v_0 E'_1$	by the induction hypothesis	7782
7728	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	2. IF $E_0 = E^\bullet$:	7783
7729	ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:	a. QED E is boundary-free	7784
7730	a. $E' = v_0 E'_1$	IF $E_0 = E'_0[\text{dyn } E^\bullet]$:	7785
7731	b. QED $E = E'[\text{stat } \tau E^\bullet]$	a. $E' = op^1 E'_0$	7786
7732	CASE $E = \langle E_0, e_1 \rangle$:	b. QED $E = E'[\text{dyn } E^\bullet]$	7787
7733	1. $E_0 = E^\bullet$	IF $E_0 = E'_0[\text{stat } E^\bullet]$:	7788
7734	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	a. $E' = op^1 E'_0$	7789
7735	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	b. QED $E = E'[\text{stat } E^\bullet]$	7790
7736	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:	7791
7737	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	a. $E' = op^1 E'_0$	7792
7738	by the induction hypothesis	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	7793
7739	2. IF $E_0 = E^\bullet$:	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:	7794
7740	a. QED E is boundary-free	a. $E' = op^1 E'_0$	7795
7741	IF $E_0 = E'_0[\text{dyn } E^\bullet]$:	b. QED $E = E'[\text{stat } \tau E^\bullet]$	7796
7742	a. $E' = \langle E'_0, e_1 \rangle$	CASE $E = op^2 E_0 e_1$:	7797
7743	b. QED $E = E'[\text{dyn } E^\bullet]$	1. $E_0 = E^\bullet$	7798
7744	IF $E_0 = E'_0[\text{stat } E^\bullet]$:	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	7799
7745	a. $E' = \langle E'_0, e_1 \rangle$	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	7800
7746	b. QED $E = E'[\text{stat } E^\bullet]$	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	7801
7747	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	7802
7748	a. $E' = \langle E'_0, e_1 \rangle$	by the induction hypothesis	7803
7749	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	2. IF $E_0 = E^\bullet$:	7804
7750	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:	a. QED E is boundary-free	7805
7751	a. $E' = \langle E'_0, e_1 \rangle$	IF $E_0 = E'_0[\text{dyn } E^\bullet]$:	7806
7752	b. QED $E = E'[\text{stat } \tau E^\bullet]$	a. $E' = op^2 E'_0 e_1$	7807
7753	CASE $E = \langle v_0, E_1 \rangle$:	b. QED $E = E'[\text{dyn } E^\bullet]$	7808
7754			7809
7755			7810

7811	IF $E_0 = E'_0[\text{stat } E^\bullet]$:	1. $E_0 = E^\bullet$	7866
7812	a. $E' = op^2 E'_0 e_1$	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	7867
7813	b. QED $E = E'[\text{stat } E^\bullet]$	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	7868
7814	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:	$\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$	7869
7815	a. $E' = op^2 E'_0 e_1$	$\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$	7870
7816	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	by the induction hypothesis	7871
7817	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:	2. IF $E_0 = E^\bullet$:	7872
7818	a. $E' = op^2 E'_0 e_1$	a. QED	7873
7819	b. QED $E = E'[\text{stat } \tau E^\bullet]$	IF $E_0 = E'_0[\text{dyn } E^\bullet]$:	7874
7820	CASE $E = op^2 v_0 E_1$:	a. $E' = \text{stat } E'_0$	7875
7821	1. $E_1 = E^\bullet$	b. QED $E = E'[\text{dyn } E^\bullet]$	7876
7822	$\vee E_1 = E'_1[\text{dyn } E^\bullet]$	IF $E_0 = E'_0[\text{stat } E^\bullet]$:	7877
7823	$\vee E_1 = E'_1[\text{stat } E^\bullet]$	a. $E' = \text{stat } E'_0$	7878
7824	$\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$	b. QED $E = E'[\text{stat } E^\bullet]$	7879
7825	$\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$	IF $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:	7880
7826	by the induction hypothesis	a. $E' = \text{stat } E'_0$	7881
7827	2. IF $E_1 = E^\bullet$:	b. QED $E = E'[\text{dyn } \tau' E^\bullet]$	7882
7828	a. QED E is boundary-free	ELSE $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:	7883
7829	IF $E_1 = E'_1[\text{dyn } E^\bullet]$:	a. $E' = \text{stat } E'_0$	7884
7830	a. $E' = op^2 v_0 E'_1$	b. QED $E = E'[\text{stat } \tau' E^\bullet]$	7885
7831	b. QED $E = E'[\text{dyn } E^\bullet]$	CASE $E = \text{dyn } \tau E_0$:	7886
7832	IF $E_1 = E'_1[\text{stat } E^\bullet]$:	1. $E_0 = E^\bullet$	7887
7833	a. $E' = op^2 v_0 E'_1$	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	7888
7834	b. QED $E = E'[\text{stat } E^\bullet]$	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	7889
7835	IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:	$\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$	7890
7836	a. $E' = op^2 v_0 E'_1$	$\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$	7891
7837	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	by the induction hypothesis	7892
7838	ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:	2. IF $E_0 = E^\bullet$:	7893
7839	a. $E' = op^2 v_0 E'_1$	a. QED	7894
7840	b. QED $E = E'[\text{stat } \tau E^\bullet]$	IF $E_0 = E'_0[\text{dyn } E^\bullet]$:	7895
7841	CASE $E = \text{dyn } E_0$:	a. $E' = \text{dyn } \tau E'_0$	7896
7842	1. $E_0 = E^\bullet$	b. QED $E = E'[\text{dyn } E^\bullet]$	7897
7843	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	IF $E_0 = E'_0[\text{stat } E^\bullet]$:	7898
7844	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	a. $E' = \text{dyn } \tau E'_0$	7899
7845	$\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$	b. QED $E = E'[\text{stat } E^\bullet]$	7900
7846	$\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$	IF $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:	7901
7847	by the induction hypothesis	a. $E' = \text{dyn } \tau E'_0$	7902
7848	2. IF $E_0 = E^\bullet$:	b. QED $E = E'[\text{dyn } \tau' E^\bullet]$	7903
7849	a. QED	ELSE $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:	7904
7850	IF $E_0 = E'_0[\text{dyn } E^\bullet]$:	a. $E' = \text{dyn } \tau E'_0$	7905
7851	a. $E' = \text{dyn } E'_0$	b. QED $E = E'[\text{stat } \tau' E^\bullet]$	7906
7852	b. QED $E = E'[\text{dyn } E^\bullet]$	CASE $E = \text{stat } \tau E_0$:	7907
7853	IF $E_0 = E'_0[\text{stat } E^\bullet]$:	1. $E_0 = E^\bullet$	7908
7854	a. $E' = \text{dyn } E'_0$	$\vee E_0 = E'_0[\text{dyn } E^\bullet]$	7909
7855	b. QED $E = E'[\text{stat } E^\bullet]$	$\vee E_0 = E'_0[\text{stat } E^\bullet]$	7910
7856	IF $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:	$\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$	7911
7857	a. $E' = \text{dyn } E'_0$	$\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$	7912
7858	b. QED $E = E'[\text{dyn } \tau' E^\bullet]$	by the induction hypothesis	7913
7859	ELSE $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:	2. IF $E_0 = E^\bullet$:	7914
7860	a. $E' = \text{dyn } E'_0$	a. QED	7915
7861	b. QED $E = E'[\text{stat } \tau' E^\bullet]$	IF $E_0 = E'_0[\text{dyn } E^\bullet]$:	7916
7862	CASE $E = \text{stat } E_0$:	a. $E' = \text{stat } \tau E'_0$	7917
7863		b. QED $E = E'[\text{dyn } E^\bullet]$	7918
7864		IF $E_0 = E'_0[\text{stat } E^\bullet]$:	7919
7865			7920

7921 a. $E' = \text{stat } \tau E'_0$
 7922 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 7923 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 7924 a. $E' = \text{stat } \tau E'_0$
 7925 b. $\text{QED } E = E'[\text{dyn } \tau' E^\bullet]$
 7926 **ELSE** $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 7927 a. $E' = \text{stat } \tau E'_0$
 7928 b. $\text{QED } E = E'[\text{stat } \tau' E^\bullet]$
 7929 **CASE** $E = \text{chk } K_0 E_0$:
 7930 1. $E_0 = E^\bullet$
 7931 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 7932 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 7933 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 7934 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 7935 by the induction hypothesis
 7936 2. **IF** $E_0 = E^\bullet$:
 7937 a. $\text{QED } E$ is boundary-free
 7938 **IF** $E_0 = E'_0[\text{dyn } E^\bullet]$:
 7939 a. $E' = \text{chk } K_0 E'_0$
 7940 b. $\text{QED } E = E'[\text{dyn } E^\bullet]$
 7941 **IF** $E_0 = E'_0[\text{stat } E^\bullet]$:
 7942 a. $E' = \text{chk } K_0 E'_0$
 7943 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 7944 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 7945 a. $E' = \text{chk } K_0 E'_0$
 7946 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
 7947 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 7948 a. $E' = \text{chk } K_0 E'_0$
 7949 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$

□

Lemma 4.20 : 1 *dynamic boundary factoring*If $\vdash_1 e$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[\text{op}^1 v]$
- $e = E^\bullet[\text{op}^2 v_0 v_1]$
- $e = E[\text{dyn } e']$ where e' is boundary-free
- $e = E[\text{stat } e']$ where e' is boundary-free
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:By the *unique evaluation contexts* lemma, there are ten cases.**CASE** e is a value :1. **QED****CASE** $e = E[v_0 v_1]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } E^\bullet]$ $\vee E = E'[\text{stat } E^\bullet]$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. $\text{QED } e = E^\bullet[v_0 v_1]$ **IF** $E = E'[\text{dyn } E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } E^\bullet[v_0 v_1]]$ **IF** $E = E'[\text{stat } E^\bullet]$:a. $\text{QED } e = E'[\text{stat } E^\bullet[v_0 v_1]]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$ **CASE** $e = E[\text{op}^1 v]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } E^\bullet]$ $\vee E = E'[\text{stat } E^\bullet]$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. $\text{QED } e = E^\bullet[\text{op}^1 v]$ **IF** $E = E'[\text{dyn } E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } E^\bullet[\text{op}^1 v]]$ **IF** $E = E'[\text{stat } E^\bullet]$:a. $\text{QED } e = E'[\text{stat } E^\bullet[\text{op}^1 v]]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[\text{op}^1 v]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[\text{op}^1 v]]$ **CASE** $e = E[\text{op}^2 v_0 v_1]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } E^\bullet]$ $\vee E = E'[\text{stat } E^\bullet]$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. $\text{QED } e = E^\bullet[\text{op}^2 v_0 v_1]$ **IF** $E = E'[\text{dyn } E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } E^\bullet[\text{op}^2 v_0 v_1]]$ **IF** $E = E'[\text{stat } E^\bullet]$:a. $\text{QED } e = E'[\text{stat } E^\bullet[\text{op}^2 v_0 v_1]]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[\text{op}^2 v_0 v_1]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[\text{op}^2 v_0 v_1]]$ **CASE** $e = E[\text{chk } K' v]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } E^\bullet]$ $\vee E = E'[\text{stat } E^\bullet]$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. $\text{QED } e = E^\bullet[\text{chk } K' v]$ **IF** $E = E'[\text{dyn } E^\bullet]$:a. $\text{QED } e = E'[\text{dyn } E^\bullet[\text{chk } K' v]]$

8031 **IF** $E = E'[\text{stat } E^\bullet]$:
 8032 a. QED $e = E'[\text{stat } E^\bullet[\text{chk } K' v]]$
 8033 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:
 8034 a. QED $e = E'[\text{dyn } \tau E^\bullet[\text{chk } K' v]]$
 8035 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:
 8036 a. QED $e = E'[\text{stat } \tau E^\bullet[\text{chk } K' v]]$
 8037 **CASE** $e = E[\text{dyn } v]$:
 8038 1. QED v is boundary-free
 8039 **CASE** $e = E[\text{stat } v]$:
 8040 1. QED v is boundary-free
 8041 **CASE** $e = E[\text{dyn } \tau v]$:
 8042 1. QED v is boundary-free
 8043 **CASE** $e = E[\text{stat } \tau v]$:
 8044 1. QED v is boundary-free
 8045 **CASE** $e = E[\text{Err}]$:
 8046 1. QED

8047 \square

8048 **Lemma 4.21** : 1 unique dynamic evaluation contexts

8049 If $\vdash_1 e$ then one of the following holds:

- 8050 • e is a value
- 8051 • $e = E[v_0 v_1]$
- 8052 • $e = E[op^1 v]$
- 8053 • $e = E[op^2 v_0 v_1]$
- 8054 • $e = E[\text{chk } K v]$
- 8055 • $e = E[\text{dyn } v]$
- 8056 • $e = E[\text{stat } v]$
- 8057 • $e = E[\text{dyn } \tau v]$
- 8058 • $e = E[\text{stat } \tau v]$
- 8059 • $e = E[\text{Err}]$

8060 *Proof*:

8061 By induction on the structure of e .

8062 **CASE** $e = x$:

- 8063 1. Contradiction by $\vdash_1 e$

8064 **CASE** $e = i$

- 8065 $\vee e = \lambda x. e'$
- 8066 $\vee e = \lambda(x:\tau_d). e'$

- 8067 1. QED e is a value

8068 **CASE** $e = \langle e_0, e_1 \rangle$:

8069 **IF** $e_0 \notin v$:

- 8070 1. $e_0 = E_0[e'_0]$
by the induction hypothesis
- 8071 2. $E = \langle E_0, e_1 \rangle$
- 8072 3. QED $e = E[e'_0]$

8073 **IF** $e_0 \in v$

8074 $\wedge e_1 \notin v$:

- 8075 1. $e_1 = E_1[e'_1]$
by the induction hypothesis
- 8076 2. $E = \langle e_0, E_1 \rangle$
- 8077 3. QED $e = E[e'_1]$

8078 **ELSE** $e_0 \in v$

8079 $\wedge e_1 \in v$:

- 8080 1. $E = []$
- 8081 2. QED $e = E[\langle e_0, e_1 \rangle]$

8082 **CASE** $e = e_0 e_1$:

8083 **IF** $e_0 \notin v$:

- 8084 1. $e_0 = E_0[e'_0]$
by the induction hypothesis
- 8085 2. $E = E_0 e_1$
- 8086 3. QED $e = E[e'_0]$

8087 **IF** $e_0 \in v$

8088 $\wedge e_1 \notin v$:

- 8089 1. $e_1 = E_1[e'_1]$
by the induction hypothesis
- 8090 2. $E = e_0 E_1$
- 8091 3. QED $e = E[e'_1]$

8092 **ELSE** $e_0 \in v$

8093 $\wedge e_1 \in v$:

- 8094 1. $E = []$
- 8095 2. QED $e = E[e_0 e_1]$

8096 **CASE** $e = op^1 e_0$:

8097 **IF** $e_0 \notin v$:

- 8098 1. $e_0 = E_0[e'_0]$
by the induction hypothesis
- 8099 2. $E = op^1 E_0$
- 8100 3. QED $e = E[e'_0]$

8101 **ELSE** $e_0 \in v$:

- 8102 1. $E = []$
- 8103 2. QED $e = E[op^1 e_0]$

8104 **CASE** $e = op^2 e_0 e_1$:

8105 **IF** $e_0 \notin v$:

- 8106 1. $e_0 = E_0[e'_0]$
by the induction hypothesis
- 8107 2. $E = op^2 E_0 e_1$
- 8108 3. QED $e = E[e'_0]$

8109 **IF** $e_0 \in v$

8110 $\wedge e_1 \notin v$:

- 8111 1. $e_1 = E_1[e'_1]$
by the induction hypothesis
- 8112 2. $E = op^2 e_0 E_1$
- 8113 3. QED $e = E[e'_1]$

8114 **ELSE** $e_0 \in v$

8115 $\wedge e_1 \in v$:

- 8116 1. $E = []$
- 8117 2. QED $e = E[op^2 e_0 e_1]$

8118 **CASE** $e = \text{chk } K e'$:

- 8119 1. Contradiction by $\vdash_1 e$

8120 **CASE** $e = \text{dyn } e_0$:

- 8121 1. Contradiction by $\vdash_1 e$

8122 **CASE** $e = \text{stat } e_0$:

8123 **IF** $e_0 \notin v$:

- 8124 1. $\vdash_1 e_0$
by 1 inversion
- 8125 2. $e_0 = E_0[e'_0]$
by unique evaluation contexts (1)
- 8126 3. $E = \text{stat } E_0$
- 8127 4. QED $e = E[e'_0]$

8128 **ELSE** $e_0 \in v$:

- 8129 1. $E = []$

8086
8087
8088
8089
8090
8091
8092
8093
8094
8095
8096
8097
8098
8099
8100
8101
8102
8103
8104
8105
8106
8107
8108
8109
8110
8111
8112
8113
8114
8115
8116
8117
8118
8119
8120
8121
8122
8123
8124
8125
8126
8127
8128
8129
8130
8131
8132
8133
8134
8135
8136
8137
8138
8139
8140

8141 2. QED $e = E[\text{stat } e_0]$

8142 **CASE** $e = \text{dyn } e_0$:

8143 Contradiction by $\vdash_1 e$

8144 **CASE** $e = \text{stat } K_0 e_0$:

8145 **IF** $e_0 \notin v$:

8146 1. $\vdash_1 e_0$

8147 by 1 *inversion*

8148 2. $e_0 = E_0[e'_0]$

8149 by *unique evaluation contexts* (1)

8150 3. $E = \text{stat } \tau E_0$

8151 4. QED $e = E[e'_0]$

8152 **ELSE** $e_0 \in v$:

8153 1. $E = []$

8154 2. QED $e = E[\text{stat } \tau e_0]$

8155 \square

8156 **Lemma 4.22** : 1 *static hole typing*

8157 **IF** $\vdash_1 E^\bullet[e] : K$ then the typing derivation contains a sub-term

8158 $\vdash_1 e : K'$ for some K' .

8159 *Proof*:

8160 By induction on the structure of E^\bullet .

8161 **CASE** $E^\bullet = []$:

8162 1. QED $E^\bullet[e] = e$

8163 **CASE** $E^\bullet = E^\bullet_0 e_1$:

8164 1. $E^\bullet[e] = E^\bullet_0[e] e_1$

8165 2. $\vdash_1 E^\bullet_0[e] : \text{Fun}$

8166 by 1 *inversion*

8167 3. QED by the induction hypothesis (2)

8168 **CASE** $E^\bullet = v_0 E^\bullet_1$:

8169 1. $E^\bullet[e] = v_0 E^\bullet_1[e]$

8170 2. $\vdash_1 E^\bullet_1[e] : \text{Any}$

8171 by 1 *inversion*

8172 3. QED by the induction hypothesis (2)

8173 **CASE** $E^\bullet = \langle E^\bullet_0, e_1 \rangle$:

8174 1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$

8175 2. $\vdash_1 E^\bullet_0[e] : \text{Any}$

8176 by 1 *inversion*

8177 3. QED by the induction hypothesis (2)

8178 **CASE** $E^\bullet = \langle v_0, E^\bullet_1 \rangle$:

8179 1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$

8180 2. $\vdash_1 E^\bullet_1[e] : \text{Any}$

8181 by 1 *inversion*

8182 3. QED the induction hypothesis (2)

8183 **CASE** $E^\bullet = op^1 E^\bullet_0$:

8184 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$

8185 2. $\vdash_1 E^\bullet_0[e] : \text{Pair}$

8186 by 1 *inversion*

8187 3. QED the induction hypothesis (2)

8188 **CASE** $E^\bullet = op^2 E^\bullet_0 e_1$:

8189 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$

8190 2. $\vdash_1 E^\bullet_0[e] : K_0$

8191 by 1 *inversion*

8192 3. QED the induction hypothesis (2)

8193 **CASE** $E^\bullet = op^2 v_0 E^\bullet_1$:

8194

8195

1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$ 8196

2. $\vdash_1 E^\bullet_1[e] : K_1$ 8197

by 1 *inversion* 8198

3. QED the induction hypothesis (2) 8199

CASE $E^\bullet = \text{chk } K E^\bullet_0$:

1. $E^\bullet[e] = \text{chk } K E^\bullet_0[e]$ 8201

2. $\vdash_1 E^\bullet_0[e] : \text{Any}$ 8202

by 1 *inversion* 8203

3. QED the induction hypothesis (2) 8204

\square 8205

Lemma 4.23 : 1 *dynamic hole typing* 8206

IF $\vdash_1 E^\bullet[e]$ then the derivation contains a sub-term $\vdash_1 e$ 8207

Proof: 8208

By induction on the structure of E^\bullet . 8209

CASE $E^\bullet = []$:

1. QED $E^\bullet[e] = e$ 8211

CASE $E^\bullet = E^\bullet_0 e_1$:

1. $E^\bullet[e] = E^\bullet_0[e] e_1$ 8213

2. $\vdash_1 E^\bullet_0[e]$ 8214

by 1 *inversion* 8215

3. QED the induction hypothesis (2) 8216

CASE $E^\bullet = v_0 E^\bullet_1$:

1. $E^\bullet[e] = v_0 E^\bullet_1[e]$ 8218

2. $\vdash_1 E^\bullet_1[e]$ 8219

by 1 *inversion* 8220

3. QED the induction hypothesis (2) 8221

CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle$:

1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$ 8223

2. $\vdash_1 E^\bullet_0[e]$ 8224

by 1 *inversion* 8225

3. QED the induction hypothesis (2) 8226

CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle$:

1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$ 8228

2. $\vdash_1 E^\bullet_1[e]$ 8229

by 1 *inversion* 8230

3. QED the induction hypothesis (2) 8231

CASE $E^\bullet = op^1 E^\bullet_0$:

1. $E^\bullet[e] = op^1 E^\bullet_0[e]$ 8233

2. $\vdash_1 E^\bullet_0[e]$ 8234

by 1 *inversion* 8235

3. QED the induction hypothesis (2) 8236

CASE $E^\bullet = op^2 E^\bullet_0 e_1$:

1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$ 8238

2. $\vdash_1 E^\bullet_0[e]$ 8239

by 1 *inversion* 8240

3. QED the induction hypothesis (2) 8241

CASE $E^\bullet = op^2 v_0 E^\bullet_1$:

1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$ 8243

2. $\vdash_1 E^\bullet_1[e]$ 8244

by 1 *inversion* 8245

3. QED the induction hypothesis (2) 8246

CASE $E^\bullet = \text{chk } K E^\bullet_0$:

1. Contradiction by $\vdash_1 E^\bullet[e]$ 8248

8249

8250

8251 □

8252 **Lemma 4.24** : 1 *boundary hole typing*

- 8253 • If $\vdash_1 E[\text{dyn } e]$ then the derivation contains a sub-term \vdash_1
- 8254 $\text{dyn } e : \text{Any}$
- 8255 • If $\vdash_1 E[\text{dyn } e] : K'$ then the derivation contains a sub-term
- 8256 $\vdash_1 \text{dyn } e : \text{Any}$
- 8257 • If $\vdash_1 E[\text{stat } e]$ then the derivation contains a sub-term \vdash_1
- 8258 $\text{stat } e$
- 8259 • If $\vdash_1 E[\text{stat } e] : K'$ then the derivation contains a sub-term
- 8260 $\vdash_1 \text{stat } e$
- 8261 • If $\vdash_1 E[\text{dyn } \tau e]$ then the derivation contains a sub-term
- 8262 $\vdash_1 \text{dyn } \tau e : [\tau]$
- 8263 • If $\vdash_1 E[\text{dyn } \tau e] : K'$ then the derivation contains a sub-term
- 8264 $\vdash_1 \text{dyn } \tau e : [\tau]$
- 8265 • If $\vdash_1 E[\text{stat } \tau e]$ then the derivation contains a sub-term
- 8266 $\vdash_1 \text{stat } \tau e$
- 8267 • If $\vdash_1 E[\text{stat } \tau e] : K'$ then the derivation contains a sub-term
- 8268 $\vdash_1 \text{stat } \tau e$

8269 *Proof*:

8270 By the following four lemmas: *static dyn hole typing*,

8271 *dynamic dyn hole typing*, *static stat hole typing*, and

8272 *dynamic stat hole typing*.

8273 □

8274 **Lemma 4.25** : 1 *static dyn hole typing*

- 8275 If $\vdash_1 E[\text{dyn } \tau e] : K'$ then the derivation contains a sub-term
- 8276 $\vdash_1 \text{dyn } \tau e : [\tau]$.

8277 *Proof*:

8278 By induction on the structure of E .

- 8279 **CASE** $E \in E^*$:
- 8280 1. $\vdash_1 \text{dyn } \tau e : K''$
- 8281 by *static hole typing*
- 8282 2. $\vdash_1 \text{dyn } \tau e : [\tau]$
- 8283 by 1 *inversion* (1)
- 8284 3. QED
- 8285 **CASE** $E = E_0 e_1$:
- 8286 1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
- 8287 2. $\vdash_1 E_0[\text{dyn } \tau e] : K_0$
- 8288 by 1 *inversion*
- 8289 3. QED by the induction hypothesis (2)
- 8290 **CASE** $E = v_0 E_1$:
- 8291 1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
- 8292 2. $\vdash_1 E_1[\text{dyn } \tau e] : K_1$
- 8293 by 1 *inversion*
- 8294 3. QED by the induction hypothesis (2)
- 8295 **CASE** $E = \langle E_0, e_1 \rangle$:
- 8296 1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$
- 8297 2. $\vdash_1 E_0[\text{dyn } \tau e] : K_0$
- 8298 by 1 *inversion*
- 8299 3. QED by the induction hypothesis (2)
- 8300 **CASE** $E = \langle v_0, E_1 \rangle$:
- 8301 1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$
- 8302 2. $\vdash_1 E_1[\text{dyn } \tau e] : K_1$
- 8303 by 1 *inversion*

8304

8305

- 3. QED by the induction hypothesis (2)

CASE $E = \text{op}^1 E_0$:

- 1. $E[\text{dyn } \tau e] = \text{op}^1 E_0[\text{dyn } \tau e]$
- 2. $\vdash_1 E_0[\text{dyn } \tau e] : K_0$
- by 1 *inversion*
- 3. QED by the induction hypothesis (2)

CASE $E = \text{op}^2 E_0 e_1$:

- 1. $E[\text{dyn } \tau e] = \text{op}^2 E_0[\text{dyn } \tau e] e_1$
- 2. $\vdash_1 E_0[\text{dyn } \tau e] : K_0$
- by 1 *inversion*
- 3. QED by the induction hypothesis (2)

CASE $E = \text{op}^2 v_0 E_1$:

- 1. $E[\text{dyn } \tau e] = \text{op}^2 v_0 E_1[\text{dyn } \tau e]$
- 2. $\vdash_1 E_1[\text{dyn } \tau e] : K_1$
- by 1 *inversion*
- 3. QED by the induction hypothesis (2)

CASE $E = \text{dyn } E_0$:

- 1. $E[\text{dyn } \tau e] = \text{dyn } E_0[\text{dyn } \tau e]$
- 2. $\vdash_1 E_0[\text{dyn } \tau e]$
- by 1 *inversion*
- 3. QED by *dynamic dyn hole typing* (2)

CASE $E = \text{stat } E_0$:

- 1. Contradiction by $\vdash_1 E[\text{dyn } \tau e] : \tau'$

CASE $E = \text{dyn } \tau_0 E_0$:

- 1. $E[\text{dyn } \tau e] = \text{dyn } \tau_0 E_0[\text{dyn } \tau e]$
- 2. $\vdash_1 E_0[\text{dyn } \tau e]$
- by 1 *inversion*
- 3. QED by *dynamic dyn hole typing* (2)

CASE $E = \text{stat } \tau_0 E_0$:

- 1. Contradiction by $\vdash_1 E[\text{dyn } \tau e] : \tau'$

CASE $E = \text{chk } K_0 E_0$:

- 1. $E[\text{dyn } \tau e] = \text{chk } K_0 E_0[\text{dyn } \tau e]$
- 2. $\vdash_1 E_0[\text{dyn } \tau e] : \text{Any}$
- by 1 *inversion*
- 3. QED by the induction hypothesis (2)

□

Lemma 4.26 : 1 *dynamic dyn hole typing*

- If $\vdash_1 E[\text{dyn } \tau e]$ then the derivation contains a sub-term \vdash_1
- $\text{dyn } \tau e : [\tau]$.

Proof:

By induction on the structure of E .

CASE $E \in E^*$:

- 1. Contradiction by $\vdash_1 E[\text{dyn } \tau e]$

CASE $E = E_0 e_1$:

- 1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
- 2. $\vdash_1 E_0[\text{dyn } \tau e]$
- by 1 *inversion*
- 3. QED by the induction hypothesis (2)

CASE $E = v_0 E_1$:

- 1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
- 2. $\vdash_1 E_1[\text{dyn } \tau e]$
- by 1 *inversion*
- 3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle$:

- 3. QED by the induction hypothesis (2)

8361	1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$		
8362	2. $\vdash_1 E_0[\text{dyn } \tau e]$		
8363	by 1 <i>inversion</i>		
8364	3. QED by the induction hypothesis (2)		
8365	CASE $E = \langle v_0, E_1 \rangle :$		
8366	1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$		
8367	2. $\vdash_1 E_1[\text{dyn } \tau e]$		
8368	by 1 <i>inversion</i>		
8369	3. QED by the induction hypothesis (2)		
8370	CASE $E = \text{op}^1 E_0 :$		
8371	1. $E[\text{dyn } \tau e] = \text{op}^1 E_0[\text{dyn } \tau e]$		
8372	2. $\vdash_1 E_0[\text{dyn } \tau e]$		
8373	by 1 <i>inversion</i>		
8374	3. QED by the induction hypothesis (2)		
8375	CASE $E = \text{op}^2 E_0 e_1 :$		
8376	1. $E[\text{dyn } \tau e] = \text{op}^2 E_0[\text{dyn } \tau e] e_1$		
8377	2. $\vdash_1 E_0[\text{dyn } \tau e]$		
8378	by 1 <i>inversion</i>		
8379	3. QED by the induction hypothesis (2)		
8380	CASE $E = \text{op}^2 v_0 E_1 :$		
8381	1. $E[\text{dyn } \tau e] = \text{op}^2 v_0 E_1[\text{dyn } \tau e]$		
8382	2. $\vdash_1 E_1[\text{dyn } \tau e]$		
8383	by 1 <i>inversion</i>		
8384	3. QED by the induction hypothesis (2)		
8385	CASE $E = \text{dyn } E_0 :$		
8386	1. Contradiction by $\vdash_1 E[\text{dyn } \tau e]$		
8387	CASE $E = \text{stat } E_0 :$		
8388	1. $E[\text{dyn } \tau e] = \text{stat } E_0[\text{dyn } \tau e]$		
8389	2. $\vdash_1 E_0[\text{dyn } \tau e] : \lfloor \tau_0 \rfloor$		
8390	by 1 <i>inversion</i>		
8391	3. QED by <i>static dyn hole typing</i> (2)		
8392	CASE $E = \text{dyn } \tau E_0 :$		
8393	1. Contradiction by $\vdash_1 E[\text{dyn } \tau e]$		
8394	CASE $E = \text{stat } \tau_0 E_0 :$		
8395	1. $E[\text{dyn } \tau e] = \text{stat } \tau_0 E_0[\text{dyn } \tau e]$		
8396	2. $\vdash_1 E_0[\text{dyn } \tau e] : \lfloor \tau_0 \rfloor$		
8397	by 1 <i>inversion</i>		
8398	3. QED by <i>static dyn hole typing</i> (2)		
8399	CASE $E = \text{chk } K_0 E_0 :$		
8400	1. Contradiction by $\vdash_1 E[\text{dyn } \tau e]$		
8401	□		
8402	Lemma 4.27 : 1 <i>static stat hole typing</i>		
8403	If $\vdash_1 E[\text{stat } \tau e] : K'$ then the derivation contains a sub-term		
8404	$\vdash_1 \text{stat } \tau e$.		
8405	<i>Proof</i> :		
8406	By induction on the structure of E .		
8407	CASE $E \in E^*$:		
8408	1. Contradiction by $\vdash_1 E[\text{stat } \tau e] : \tau'$		
8409	CASE $E = E_0 e_1 :$		
8410	1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$		
8411	2. $\vdash_1 E_0[\text{stat } \tau e] : K_0$		
8412	by 1 <i>inversion</i>		
8413	3. QED by the induction hypothesis (2)		
8414			
8415			
	CASE $E = v_0 E_1 :$		8416
	1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$		8417
	2. $\vdash_1 E_1[\text{stat } \tau e] : K_1$		8418
	by 1 <i>inversion</i>		8419
	3. QED by the induction hypothesis (2)		8420
	CASE $E = \langle E_0, e_1 \rangle :$		8421
	1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$		8422
	2. $\vdash_1 E_0[\text{stat } \tau e] : K_0$		8423
	by 1 <i>inversion</i>		8424
	3. QED by the induction hypothesis (2)		8425
	CASE $E = \langle v_0, E_1 \rangle :$		8426
	1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$		8427
	2. $\vdash_1 E_1[\text{stat } \tau e] : K_1$		8428
	by 1 <i>inversion</i>		8429
	3. QED by the induction hypothesis (2)		8430
	CASE $E = \text{op}^1 E_0 :$		8431
	1. $E[\text{stat } \tau e] = \text{op}^1 E_0[\text{stat } \tau e]$		8432
	2. $\vdash_1 E_0[\text{stat } \tau e] : K_0$		8433
	by 1 <i>inversion</i>		8434
	3. QED by the induction hypothesis (2)		8435
	CASE $E = \text{op}^2 E_0 e_1 :$		8436
	1. $E[\text{stat } \tau e] = \text{op}^2 E_0[\text{stat } \tau e] e_1$		8437
	2. $\vdash_1 E_0[\text{stat } \tau e] : K_0$		8438
	by 1 <i>inversion</i>		8439
	3. QED by the induction hypothesis (2)		8440
	CASE $E = \text{op}^2 v_0 E_1 :$		8441
	1. $E[\text{stat } \tau e] = \text{op}^2 v_0 E_1[\text{stat } \tau e]$		8442
	2. $\vdash_1 E_1[\text{stat } \tau e] : K_1$		8443
	by 1 <i>inversion</i>		8444
	3. QED by the induction hypothesis (2)		8445
	CASE $E = \text{dyn } E_0 :$		8446
	1. $E[\text{stat } \tau e] = \text{dyn } E_0[\text{stat } \tau e]$		8447
	2. $\vdash_1 E_0[\text{stat } \tau e]$		8448
	by 1 <i>inversion</i>		8449
	3. QED by <i>dynamic stat hole typing</i> (2)		8450
	CASE $E = \text{stat } E_0 :$		8451
	1. Contradiction by $\vdash_1 E[\text{stat } \tau e] : \tau'$		8452
	CASE $E = \text{dyn } \tau_0 E_0 :$		8453
	1. $E[\text{stat } \tau e] = \text{dyn } \tau_0 E_0[\text{stat } \tau e]$		8454
	2. $\vdash_1 E_0[\text{stat } \tau e]$		8455
	by 1 <i>inversion</i>		8456
	3. QED by <i>dynamic stat hole typing</i> (2)		8457
	CASE $E = \text{stat } \tau_0 E_0 :$		8458
	1. Contradiction by $\vdash_1 E[\text{stat } \tau e] : \tau'$		8459
	CASE $E = \text{chk } K_0 E_0 :$		8460
	1. $E[\text{stat } \tau e] = \text{chk } K_0 E_0[\text{stat } \tau e]$		8461
	2. $\vdash_1 E_0[\text{stat } \tau e] : \text{Any}$		8462
	by 1 <i>inversion</i>		8463
	3. QED by the induction hypothesis (2)		8464
	□		8465
	Lemma 4.28 : 1 <i>dynamic stat hole typing</i>		8466
	If $\vdash_1 E[\text{stat } \tau e]$ then the derivation contains a sub-term \vdash_1		8467
	$\text{stat } \tau e$.		8468
	<i>Proof</i> :		8469
			8470
			8471

8471 By induction on the structure of E .

8472 **CASE** $E \in E^\bullet$:

8473 1. QED by *dynamic hole typing*

8474 **CASE** $E = E_0 e_1$:

8475 1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$

8476 2. $\vdash_1 E_0[\text{stat } \tau e]$

8477 by 1 *inversion*

8478 3. QED by the induction hypothesis (2)

8479 **CASE** $E = v_0 E_1$:

8480 1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$

8481 2. $\vdash_1 E_1[\text{stat } \tau e]$

8482 by 1 *inversion*

8483 3. QED by the induction hypothesis (2)

8484 **CASE** $E = \langle E_0, e_1 \rangle$:

8485 1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$

8486 2. $\vdash_1 E_0[\text{stat } \tau e]$

8487 by 1 *inversion*

8488 3. QED by the induction hypothesis (2)

8489 **CASE** $E = \langle v_0, E_1 \rangle$:

8490 1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$

8491 2. $\vdash_1 E_1[\text{stat } \tau e]$

8492 by 1 *inversion*

8493 3. QED by the induction hypothesis (2)

8494 **CASE** $E = \text{op}^1 E_0$:

8495 1. $E[\text{stat } \tau e] = \text{op}^1 E_0[\text{stat } \tau e]$

8496 2. $\vdash_1 E_0[\text{stat } \tau e]$

8497 by 1 *inversion*

8498 3. QED by the induction hypothesis (2)

8499 **CASE** $E = \text{op}^2 E_0 e_1$:

8500 1. $E[\text{stat } \tau e] = \text{op}^2 E_0[\text{stat } \tau e] e_1$

8501 2. $\vdash_1 E_0[\text{stat } \tau e]$

8502 by 1 *inversion*

8503 3. QED by the induction hypothesis (2)

8504 **CASE** $E = \text{op}^2 v_0 E_1$:

8505 1. $E[\text{stat } \tau e] = \text{op}^2 v_0 E_1[\text{stat } \tau e]$

8506 2. $\vdash_1 E_1[\text{stat } \tau e]$

8507 by 1 *inversion*

8508 3. QED by the induction hypothesis (2)

8509 **CASE** $E = \text{dyn } E_0$:

8510 1. Contradiction by $\vdash_1 E[\text{stat } \tau e]$

8511 **CASE** $E = \text{stat } E_0$:

8512 1. $E[\text{stat } \tau e] = \text{stat } E_0[\text{stat } \tau e]$

8513 2. $\vdash_1 E_0[\text{stat } \tau e] : \lfloor \tau_0 \rfloor$

8514 by 1 *inversion*

8515 3. QED by *static stat hole typing* (2)

8516 **CASE** $E = \text{dyn } \tau E_0$:

8517 1. Contradiction by $\vdash_1 E[\text{stat } \tau e]$

8518 **CASE** $E = \text{stat } \tau_0 E_0$:

8519 1. $E[\text{stat } \tau e] = \text{stat } \tau_0 E_0[\text{stat } \tau e]$

8520 2. $\vdash_1 E_0[\text{stat } \tau e] : \lfloor \tau_0 \rfloor$

8521 by 1 *inversion*

8522 3. QED by *static stat hole typing* (2)

8523 **CASE** $E = \text{chk } K_0 E_0$:

8524 1. Contradiction by $\vdash_1 E[\text{stat } \tau e]$

8525

□

Lemma 4.29 : 1 *static hole substitution*

If $\vdash_1 E^\bullet[e] : K$ and the derivation contains a sub-term $\vdash_1 e : K'$ and $\vdash_1 e' : K'$, then $\vdash_1 E^\bullet[e'] : K$

Proof:

By induction on the structure of E^\bullet .

CASE $E^\bullet = []$:

1. $E^\bullet[e] = e$
 $\wedge E^\bullet[e'] = e'$

2. $\vdash_1 e : K$
 by (1)

3. $K' = K$

4. QED

CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle$:

1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$
 $\wedge E^\bullet[e'] = \langle E^\bullet_0[e'], e_1 \rangle$

2. $\vdash_1 \langle E^\bullet_0[e], e_1 \rangle : K$

3. $\vdash_1 E^\bullet_0[e] : K_0$

$\wedge \vdash_1 e_1 : K_1$

by 1 *inversion*

4. $\vdash_1 E^\bullet_0[e'] : K_0$

by the induction hypothesis (3)

5. $\vdash_1 \langle E^\bullet_0[e'], e_1 \rangle : K$

by (2, 3, 4)

6. QED by (1, 5)

CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle$:

1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$

$\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$

2. $\vdash_1 \langle v_0, E^\bullet_1[e] \rangle : K$

3. $\vdash_1 v_0 : K_0$

$\wedge \vdash_1 E^\bullet_1[e] : K_1$

by 1 *inversion*

4. $\vdash_1 E^\bullet_1[e'] : K_1$

by the induction hypothesis (3)

5. $\vdash_1 \langle v_0, E^\bullet_1[e'] \rangle : K$

by (2, 3, 4)

6. QED by (1, 5)

CASE $E^\bullet = E^\bullet_0 e_1$:

1. $E^\bullet[e] = E^\bullet_0[e] e_1$

$\wedge E^\bullet[e'] = E^\bullet_0[e'] e_1$

2. $\vdash_1 E^\bullet_0[e] e_1 : K$

3. $\vdash_1 E^\bullet_0[e] : K_0$

$\wedge \vdash_1 e_1 : K_1$

by 1 *inversion*

4. $\vdash_1 E^\bullet_0[e'] : K_0$

by the induction hypothesis (3)

5. $\vdash_1 E^\bullet_0[e'] e_1 : K$

by (2, 3, 4)

6. QED by (1, 5)

CASE $E^\bullet = v_0 E^\bullet_1$:

1. $E^\bullet[e] = v_0 E^\bullet_1[e]$

$\wedge E^\bullet[e'] = v_0 E^\bullet_1[e']$

2. $\vdash_1 v_0 E^\bullet_1[e] : K$

8526

8527

8528

8529

8530

8531

8532

8533

8534

8535

8536

8537

8538

8539

8540

8541

8542

8543

8544

8545

8546

8547

8548

8549

8550

8551

8552

8553

8554

8555

8556

8557

8558

8559

8560

8561

8562

8563

8564

8565

8566

8567

8568

8569

8570

8571

8572

8573

8574

8575

8576

8577

8578

8579

8580

8581 3. $\vdash_1 v_0 : K_0$
8582 $\wedge \vdash_1 E^{\bullet}_1[e] : K_1$
8583 by 1 *inversion*
8584 4. $\vdash_1 E^{\bullet}_1[e'] : K_1$
8585 by the induction hypothesis (3)
8586 5. $\vdash_1 v_0 E^{\bullet}_1[e'] : K$
8587 by (2, 3, 4)
8588 6. QED by (1, 5)
8589 **CASE** $E^{\bullet} = op^1 E^{\bullet}_0 :$
8590 1. $E^{\bullet}[e] = op^1 E^{\bullet}_0[e]$
8591 $\wedge E^{\bullet}[e'] = op^1 E^{\bullet}_0[e']$
8592 2. $\vdash_1 op^1 E^{\bullet}_0[e] : K$
8593 3. $\vdash_1 E^{\bullet}_0[e] : K_0$
8594 by 1 *inversion*
8595 4. $\vdash_1 E^{\bullet}_0[e'] : K_0$
8596 by the induction hypothesis (3)
8597 5. $\vdash_1 op^1 E^{\bullet}_0[e'] : K$
8598 by (2, 3, 4)
8599 6. QED by (1, 5)
8600 **CASE** $E^{\bullet} = op^2 E^{\bullet}_0 e_1 :$
8601 1. $E^{\bullet}[e] = op^2 E^{\bullet}_0[e] e_1$
8602 $\wedge E^{\bullet}[e'] = op^2 E^{\bullet}_0[e'] e_1$
8603 2. $\vdash_1 op^2 E^{\bullet}_0[e] e_1 : K$
8604 3. $\vdash_1 E^{\bullet}_0[e] : K_0$
8605 $\wedge \vdash_1 e_1 : K_1$
8606 by 1 *inversion*
8607 4. $\vdash_1 E^{\bullet}_0[e'] : K_0$
8608 by the induction hypothesis (3)
8609 5. $\vdash_1 op^2 E^{\bullet}_0[e'] e_1 : K$
8610 by (2, 3, 4)
8611 6. QED by (1, 5)
8612 **CASE** $E^{\bullet} = op^2 v_0 E^{\bullet}_1 :$
8613 1. $E^{\bullet}[e] = op^2 v_0 E^{\bullet}_1[e]$
8614 $\wedge E^{\bullet}[e'] = op^2 v_0 E^{\bullet}_1[e']$
8615 2. $\vdash_1 op^2 v_0 E^{\bullet}_1[e] : K$
8616 3. $\vdash_1 v_0 : K_0$
8617 $\wedge \vdash_1 E^{\bullet}_1[e] : K_1$
8618 by 1 *inversion*
8619 4. $\vdash_1 E^{\bullet}_1[e'] : K_1$
8620 by the induction hypothesis (3)
8621 5. $\vdash_1 op^2 v_0 E^{\bullet}_1[e'] : K$
8622 by (2, 3, 4)
8623 6. QED by (1, 5)
8624 **CASE** $E^{\bullet} = chk K_c E^{\bullet}_0 :$
8625 1. $E^{\bullet}[e] = chk K_c E^{\bullet}_0[e]$
8626 $\wedge E^{\bullet}[e'] = chk K_c E^{\bullet}_0[e']$
8627 2. $\vdash_1 chk K_c E^{\bullet}_0[e] : K$
8628 3. $\vdash_1 E^{\bullet}_0[e] : K_0$
8629 by 1 *inversion*
8630 4. $\vdash_1 E^{\bullet}_0[e'] : K_0$
8631 by the induction hypothesis (3)
8632 5. $\vdash_1 chk K_c E^{\bullet}_0[e'] : K$
8633 by (2, 3, 4)
8634 6. QED by (1, 5)
8635

□

Lemma 4.30 : 1 *dynamic hole substitution*If $\vdash_1 E^{\bullet}[e]$ and $\vdash_1 e'$ then $\vdash_1 E^{\bullet}[e']$ *Proof*:By induction on the structure of E^{\bullet} .**CASE** $E^{\bullet} = [] :$ 1. QED $E^{\bullet}[e'] = e'$ **CASE** $E^{\bullet} = \langle E^{\bullet}_0, e_1 \rangle :$ 1. $E^{\bullet}[e] = \langle E^{\bullet}_0[e], e_1 \rangle$ $\wedge E^{\bullet}[e'] = \langle E^{\bullet}_0[e'], e_1 \rangle$ 2. $\vdash_1 \langle E^{\bullet}_0[e], e_1 \rangle$ 3. $\vdash_1 E^{\bullet}_0[e]$ $\wedge \vdash_1 e_1$ by 1 *inversion*4. $\vdash_1 E^{\bullet}_0[e']$

by the induction hypothesis (3)

5. $\vdash_1 \langle E^{\bullet}_0[e'], e_1 \rangle$

by (3, 4)

6. QED by (1, 5)

CASE $E^{\bullet} = \langle v_0, E^{\bullet}_1 \rangle :$ 1. $E^{\bullet}[e] = \langle v_0, E^{\bullet}_1[e] \rangle$ $\wedge E^{\bullet}[e'] = \langle v_0, E^{\bullet}_1[e'] \rangle$ 2. $\vdash_1 \langle v_0, E^{\bullet}_1[e] \rangle$ 3. $\vdash_1 v_0$ $\wedge \vdash_1 E^{\bullet}_1[e]$ by 1 *inversion*4. $\vdash_1 E^{\bullet}_1[e']$

by the induction hypothesis (3)

5. $\vdash_1 \langle v_0, E^{\bullet}_1[e'] \rangle$

by (3, 4)

6. QED by (1, 5)

CASE $E^{\bullet} = E^{\bullet}_0 e_1 :$ 1. $E^{\bullet}[e] = E^{\bullet}_0[e] e_1$ $\wedge E^{\bullet}[e'] = E^{\bullet}_0[e'] e_1$ 2. $\vdash_1 E^{\bullet}_0[e] e_1$ 3. $\vdash_1 E^{\bullet}_0[e]$ $\wedge \vdash_1 e_1$ by 1 *inversion*4. $\vdash_1 E^{\bullet}_0[e']$

by the induction hypothesis (3)

5. $\vdash_1 E^{\bullet}_0[e'] e_1$

by (3, 4)

6. QED by (1, 5)

CASE $E^{\bullet} = v_0 E^{\bullet}_1 :$ 1. $E^{\bullet}[e] = v_0 E^{\bullet}_1[e]$ $\wedge E^{\bullet}[e'] = v_0 E^{\bullet}_1[e']$ 2. $\vdash_1 v_0 E^{\bullet}_1[e]$ 3. $\vdash_1 v_0$ $\wedge \vdash_1 E^{\bullet}_1[e]$ by 1 *inversion*4. $\vdash_1 E^{\bullet}_1[e']$

by the induction hypothesis (3)

8691 5. $\vdash_1 v_0 E^{\bullet}_1[e']$
 8692 by (3, 4)
 8693 6. QED by (1, 5)
 8694 **CASE** $E^{\bullet} = op^1 E^{\bullet}_0$:
 8695 1. $E^{\bullet}[e] = op^1 E^{\bullet}_0[e]$
 8696 $\wedge E^{\bullet}[e'] = op^1 E^{\bullet}_0[e']$
 8697 2. $\vdash_1 op^1 E^{\bullet}_0[e]$
 8698 3. $\vdash_1 E^{\bullet}_0[e]$
 8699 by 1 *inversion*
 8700 4. $\vdash_1 E^{\bullet}_0[e']$
 8701 by the induction hypothesis (3)
 8702 5. $\vdash_1 op^1 E^{\bullet}_0[e']$
 8703 by (3, 4)
 8704 6. QED by (1, 5)
 8705 **CASE** $E^{\bullet} = op^2 E^{\bullet}_0 e_1$:
 8706 1. $E^{\bullet}[e] = op^2 E^{\bullet}_0[e] e_1$
 8707 $\wedge E^{\bullet}[e'] = op^2 E^{\bullet}_0[e'] e_1$
 8708 2. $\vdash_1 op^2 E^{\bullet}_0[e] e_1$
 8709 3. $\vdash_1 E^{\bullet}_0[e]$
 8710 $\wedge \vdash_1 e_1$
 8711 by 1 *inversion*
 8712 4. $\vdash_1 E^{\bullet}_0[e']$
 8713 by the induction hypothesis (3)
 8714 5. $\vdash_1 op^2 E^{\bullet}_0[e'] e_1$
 8715 by (3, 4)
 8716 6. QED by (1, 5)
 8717 **CASE** $E^{\bullet} = op^2 v_0 E^{\bullet}_1$:
 8718 1. $E^{\bullet}[e] = op^2 v_0 E^{\bullet}_1[e]$
 8719 $\wedge E^{\bullet}[e'] = op^2 v_0 E^{\bullet}_1[e']$
 8720 2. $\vdash_1 op^2 v_0 E^{\bullet}_1[e]$
 8721 3. $\vdash_1 v_0$
 8722 $\wedge \vdash_1 E^{\bullet}_1[e]$
 8723 by 1 *inversion*
 8724 4. $\vdash_1 E^{\bullet}_1[e']$
 8725 by the induction hypothesis (3)
 8726 5. $\vdash_1 op^2 v_0 E^{\bullet}_1[e']$
 8727 by (3, 4)
 8728 6. QED by (1, 5)
 8729 **CASE** $E^{\bullet} = chk K_c E^{\bullet}_0$:
 8730 1. Contradiction by $\vdash_1 E^{\bullet}[e]$
 8731 \square

Lemma 4.31 : 1 *hole substitution*

- If $\vdash_1 E[e] : K$ and the derivation contains a sub-term $\vdash_1 e : K'$ and $\vdash_1 e' : K'$ then $\vdash_1 E[e'] : K$.
- If $\vdash_1 E[e] : K$ and the derivation contains a sub-term $\vdash_1 e$ and $\vdash_1 e'$ then $\vdash_1 E[e'] : K$.
- If $\vdash_1 E[e]$ and the derivation contains a sub-term $\vdash_1 e : K'$ and $\vdash_1 e' : K'$ then $\vdash_1 E[e']$.
- If $\vdash_1 E[e]$ and the derivation contains a sub-term $\vdash_1 e$ and $\vdash_1 e'$ then $\vdash_1 E[e']$.

Proof:

By the following four lemmas: *dynamic context static hole substitution*, *dynamic context dynamic hole substitution*,

static context static hole substitution, and *static context dynamic hole substitution*. 8746
8747

\square 8748

Lemma 4.32 : 1 *dynamic context static hole substitution* 8749

If $\vdash_1 E[e]$ and contains $\vdash_1 e : K'$, and furthermore $\vdash_1 e' : K'$, then $\vdash_1 E[e']$ 8750
8751

Proof:

By induction on the structure of E . 8753

CASE $E \in E^{\bullet}$: 8754

1. Contradiction by $\vdash_1 E[e]$ 8755

CASE $E = E_0 e_1$: 8756

1. $E[e] = E_0[e] e_1$ 8757

2. $\vdash_1 E_0[e]$ 8758

by 1 *inversion* 8759

3. QED by the induction hypothesis (2) 8760

CASE $E = v_0 E_1$: 8761

1. $E[e] = v_0 E_1[e]$ 8762

2. $\vdash_1 E_1[e]$ 8763

by 1 *inversion* 8764

3. QED by the induction hypothesis (2) 8765

CASE $E = \langle E_0, e_1 \rangle$: 8766

1. $E[e] = \langle E_0[e], e_1 \rangle$ 8767

2. $\vdash_1 E_0[e]$ 8768

by 1 *inversion* 8769

3. QED by the induction hypothesis (2) 8770

CASE $E = \langle v_0, E_1 \rangle$: 8771

1. $E[e] = \langle v_0, E_1[e] \rangle$ 8772

2. $\vdash_1 E_1[e]$ 8773

by 1 *inversion* 8774

3. QED by the induction hypothesis (2) 8775

CASE $E = op^1 E_0$: 8776

1. $E[e] = op^1 E_0[e]$ 8777

2. $\vdash_1 E_0[e]$ 8778

by 1 *inversion* 8779

3. QED by the induction hypothesis (2) 8780

CASE $E = op^2 E_0 e_1$: 8781

1. $E[e] = op^2 E_0[e] e_1$ 8782

2. $\vdash_1 E_0[e]$ 8783

by 1 *inversion* 8784

3. QED by the induction hypothesis (2) 8785

CASE $E = op^2 v_0 E_1$: 8786

1. $E[e] = op^2 v_0 E_1[e]$ 8787

2. $\vdash_1 E_1[e]$ 8788

by 1 *inversion* 8789

3. QED by the induction hypothesis (2) 8790

CASE $E = dyn E_0$: 8791

1. Contradiction by $\vdash_1 E[e]$ 8792

CASE $E = stat E_0$: 8793

1. $E[e] = stat E_0[e]$ 8794

2. $\vdash_1 E_0[e] : Any$ 8795

by 1 *inversion* 8796

3. QED by *static context static hole substitution* (2) 8797

CASE $E = dyn \tau'' E_0$: 8798

8744

8745

8799

8800

8801 1. Contradiction by $\vdash_1 E[e]$

8802 **CASE** $E = \text{stat } \tau_0 E_0$:

8803 1. $E[e] = \text{stat } \tau_0 E_0[e]$

8804 2. $\vdash_1 E_0[e] : \lfloor \tau_0 \rfloor$

8805 by 1 *inversion*

8806 3. QED by *static context static hole substitution* (2)

8807 **CASE** $E = \text{chk } K_0 E_0$:

8808 1. Contradiction by $\vdash_1 E[e]$

8809 \square

8810 **Lemma 4.33** : 1 *dynamic context dynamic hole substitution*

8811 If $\vdash_1 E[e]$ and contains $\vdash_1 e$, and furthermore $\vdash_1 e'$, then $\vdash_1 E[e']$

8812 *Proof*:

8813 By induction on the structure of E .

8814 **CASE** $E \in E^*$:

8815 1. QED by *dynamic boundary-free hole substitution*

8816 **CASE** $E = E_0 e_1$:

8817 1. $E[e] = E_0[e] e_1$

8818 2. $\vdash_1 E_0[e]$

8819 by 1 *inversion*

8820 3. QED by the induction hypothesis (2)

8821 **CASE** $E = v_0 E_1$:

8822 1. $E[e] = v_0 E_1[e]$

8823 2. $\vdash_1 E_1[e]$

8824 by 1 *inversion*

8825 3. QED by the induction hypothesis (2)

8826 **CASE** $E = \langle E_0, e_1 \rangle$:

8827 1. $E[e] = \langle E_0[e], e_1 \rangle$

8828 2. $\vdash_1 E_0[e]$

8829 by 1 *inversion*

8830 3. QED by the induction hypothesis (2)

8831 **CASE** $E = \langle v_0, E_1 \rangle$:

8832 1. $E[e] = \langle v_0, E_1[e] \rangle$

8833 2. $\vdash_1 E_1[e]$

8834 by 1 *inversion*

8835 3. QED by the induction hypothesis (2)

8836 **CASE** $E = \text{op}^1 E_0$:

8837 1. $E[e] = \text{op}^1 E_0[e]$

8838 2. $\vdash_1 E_0[e]$

8839 by 1 *inversion*

8840 3. QED by the induction hypothesis (2)

8841 **CASE** $E = \text{op}^2 E_0 e_1$:

8842 1. $E[e] = \text{op}^2 E_0[e] e_1$

8843 2. $\vdash_1 E_0[e]$

8844 by 1 *inversion*

8845 3. QED by the induction hypothesis (2)

8846 **CASE** $E = \text{op}^2 v_0 E_1$:

8847 1. $E[e] = \text{op}^2 v_0 E_1[e]$

8848 2. $\vdash_1 E_1[e]$

8849 by 1 *inversion*

8850 3. QED by the induction hypothesis (2)

8851 **CASE** $E = \text{dyn } E_0$:

8852 1. Contradiction by $\vdash_1 E[e]$

8853 **CASE** $E = \text{stat } E_0$:

8854

8855

1. $E[e] = \text{stat } E_0[e]$ 8856

2. $\vdash_1 E_0[e] : \text{Any}$ 8857

by 1 *inversion* 8858

3. QED by *static context dynamic hole substitution* (2) 8859

CASE $E = \text{dyn } \tau'' E_0$: 8860

1. Contradiction by $\vdash_1 E[e]$ 8861

CASE $E = \text{stat } \tau_0 E_0$: 8862

1. $E[e] = \text{stat } \tau_0 E_0[e]$ 8863

2. $\vdash_1 E_0[e] : \lfloor \tau_0 \rfloor$ 8864

by 1 *inversion* 8865

3. QED by *static context dynamic hole substitution* (2) 8866

CASE $E = \text{chk } K_0 E_0$: 8867

1. Contradiction by $\vdash_1 E[e]$ 8868

\square 8869

Lemma 4.34 : 1 *static context static hole substitution*

If $\vdash_1 E[e] : K$ and contains $\vdash_1 e : K'$, and furthermore $\vdash_1 e' : K'$,

then $\vdash_1 E[e'] : K$ 8871

Proof: 8873

By induction on the structure of E . 8874

CASE $E \in E^*$: 8875

1. QED by *static boundary-free hole substitution* 8876

CASE $E = E_0 e_1$: 8877

1. $E[e] = E_0[e] e_1$ 8878

2. $\vdash_1 E_0[e] : K_0$ 8879

by 1 *inversion* 8880

3. QED by the induction hypothesis (2) 8881

CASE $E = v_0 E_1$: 8882

1. $E[e] = v_0 E_1[e]$ 8883

2. $\vdash_1 E_1[e] : K_1$ 8884

by 1 *inversion* 8885

3. QED by the induction hypothesis (2) 8886

CASE $E = \langle E_0, e_1 \rangle$: 8887

1. $E[e] = \langle E_0[e], e_1 \rangle$ 8888

2. $\vdash_1 E_0[e] : K_0$ 8889

by 1 *inversion* 8890

3. QED by the induction hypothesis (2) 8891

CASE $E = \langle v_0, E_1 \rangle$: 8892

1. $E[e] = \langle v_0, E_1[e] \rangle$ 8893

2. $\vdash_1 E_1[e] : K_1$ 8894

by 1 *inversion* 8895

3. QED by the induction hypothesis (2) 8896

CASE $E = \text{op}^1 E_0$: 8897

1. $E[e] = \text{op}^1 E_0[e]$ 8898

2. $\vdash_1 E_0[e] : K_0$ 8899

by 1 *inversion* 8900

3. QED by the induction hypothesis (2) 8901

CASE $E = \text{op}^2 E_0 e_1$: 8902

1. $E[e] = \text{op}^2 E_0[e] e_1$ 8903

2. $\vdash_1 E_0[e] : K_0$ 8904

by 1 *inversion* 8905

3. QED by the induction hypothesis (2) 8906

CASE $E = \text{op}^2 v_0 E_1$: 8907

1. $E[e] = \text{op}^2 v_0 E_1[e]$ 8908

8909

8910

8911 2. $\vdash_1 E_1[e] : K_1$
 8912 by 1 *inversion*
 8913 3. QED by the induction hypothesis (2)
 8914 **CASE** $E = \text{dyn } E_0 :$
 8915 1. $E[e] = \text{dyn } E_0[e]$
 8916 2. $\vdash_1 E_0[e]$
 8917 by 1 *inversion*
 8918 3. QED by *static dyn hole typing* (2)
 8919 **CASE** $E = \text{stat } E_0 :$
 8920 1. Contradiction by $\vdash_1 E[e] : K$
 8921 **CASE** $E = \text{dyn } \tau_0 E_0 :$
 8922 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 8923 2. $\vdash_1 E_0[e]$
 8924 by 1 *inversion*
 8925 3. QED by *static dyn hole typing* (2)
 8926 **CASE** $E = \text{stat } \tau_0 E_0 :$
 8927 1. Contradiction by $\vdash_1 E[e] : K$
 8928 **CASE** $E = \text{chk } K_0 E_0 :$
 8929 1. $E[e] = \text{chk } K_0 E_0[e]$
 8930 2. $\vdash_1 E_0[e] : \text{Any}$
 8931 by 1 *inversion*
 8932 3. QED by the induction hypothesis (2)
 8933 \square
 8934 **Lemma 4.35** : 1 *static context dynamic hole substitution*
 8935 If $\vdash_1 E[e] : K$ and contains $\vdash_1 e$, and furthermore $\vdash_1 e'$, then
 8936 $\vdash_1 E[e'] : K$
 8937 *Proof*:
 8938 By induction on the structure of E .
 8939 **CASE** $E \in E^* :$
 8940 1. Contradiction by $\vdash_1 E[e] : K$
 8941 **CASE** $E = E_0 e_1 :$
 8942 1. $E[e] = E_0[e] e_1$
 8943 2. $\vdash_1 E_0[e] : K_0$
 8944 by 1 *inversion*
 8945 3. QED by the induction hypothesis (2)
 8946 **CASE** $E = v_0 E_1 :$
 8947 1. $E[e] = v_0 E_1[e]$
 8948 2. $\vdash_1 E_1[e] : K_1$
 8949 by 1 *inversion*
 8950 3. QED by the induction hypothesis (2)
 8951 **CASE** $E = \langle E_0, e_1 \rangle :$
 8952 1. $E[e] = \langle E_0[e], e_1 \rangle$
 8953 2. $\vdash_1 E_0[e] : K_0$
 8954 by 1 *inversion*
 8955 3. QED by the induction hypothesis (2)
 8956 **CASE** $E = \langle v_0, E_1 \rangle :$
 8957 1. $E[e] = \langle v_0, E_1[e] \rangle$
 8958 2. $\vdash_1 E_1[e] : K_1$
 8959 by 1 *inversion*
 8960 3. QED by the induction hypothesis (2)
 8961 **CASE** $E = \text{op}^1 E_0 :$
 8962 1. $E[e] = \text{op}^1 E_0[e]$

2. $\vdash_1 E_0[e] : K_0$
 by 1 *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{op}^2 E_0 e_1 :$
 1. $E[e] = \text{op}^2 E_0[e] e_1$
 2. $\vdash_1 E_0[e] : K_0$
 by 1 *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{op}^2 v_0 E_1 :$
 1. $E[e] = \text{op}^2 v_0 E_1[e]$
 2. $\vdash_1 E_1[e] : K_1$
 by 1 *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{dyn } E_0 :$
 1. $E[e] = \text{dyn } E_0[e]$
 2. $\vdash_1 E_0[e]$
 by 1 *inversion*
 3. QED by *dynamic stat hole typing* (2)
CASE $E = \text{stat } E_0 :$
 1. Contradiction by $\vdash_1 E[e] : K$
CASE $E = \text{dyn } \tau_0 E_0 :$
 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 2. $\vdash_1 E_0[e]$
 by 1 *inversion*
 3. QED by *dynamic stat hole typing* (2)
CASE $E = \text{stat } \tau_0 E_0 :$
 1. Contradiction by $\vdash_1 E[e] : K$
CASE $E = \text{chk } K_0 E_0 :$
 1. $E[e] = \text{chk } K_0 E_0[e]$
 2. $\vdash_1 E_0[e] : \text{Any}$
 by 1 *inversion*
 3. QED by the induction hypothesis (2)
 \square
Lemma 4.36 : 1 *static inversion*

- If $\vdash_1 \langle e_0, e_1 \rangle : K$ then $\vdash_1 e_0 : \text{Any}$ and $\vdash_1 e_1 : \text{Any}$
- If $\vdash_1 \lambda x. e : K$ then $x \vdash_1 e$
- If $\vdash_1 \lambda(x:\tau). e : K$ then $(x:\tau) \vdash_1 e : \text{Any}$
- If $\vdash_1 e_0 e_1 : K$ then $K = \text{Any}$ and $\vdash_1 e_0 : \text{Fun}$ and $\vdash_1 e_1 : \text{Any}$
- If $\vdash_1 \text{op}^1 e_0 : K$ then $K = \text{Any}$ and $\vdash_1 e_0 : \text{Pair}$
- If $\vdash_1 \text{op}^2 e_0 e_1 : K$ then $\vdash_1 e_0 : K_0$ and $\vdash_1 e_1 : K_1$ and $\Delta(\text{op}^2, K_0, K_1) = K'$ and $K' <: K$
- If $\vdash_1 \text{dyn } \tau e : K$ then $\vdash_1 e$ and $[\tau] \leqslant K$
- If $\vdash_1 \text{chk } K' e_0 : K$ then $\vdash_1 e_0 : \text{Any}$ and $K' \leqslant K$

Proof:
 QED by the definition of $\Gamma \vdash_1 e : \tau$
 \square
Lemma 4.37 : 1 *dynamic inversion*

- 9021 • If $\vdash_1 \langle e_0, e_1 \rangle$ then $\vdash_1 e_0$ and $\vdash_1 e_1$
- 9022 • If $\vdash_1 \lambda x. e$ then $x \vdash_1 e$
- 9023 • If $\vdash_1 \lambda(x:\tau). e$ then $(x:\tau) \vdash_1 e : \text{Any}$
- 9024 • If $\vdash_1 e_0 e_1$ then $\vdash_1 e_0$ and $\vdash_1 e_1$
- 9025 • If $\vdash_1 op^1 e_0$ then $\vdash_1 e_0$
- 9026 • If $\vdash_1 op^2 e_0 e_1$ then $\vdash_1 e_0$ and $\vdash_1 e_1$
- 9027 • If $\vdash_1 \text{stat } \tau e$ then $\vdash_1 e : \lfloor \tau \rfloor$
- 9028 • If $\vdash_1 \text{stat } e$ then $\vdash_1 e : \text{Any}$

9029 *Proof:*

9030 QED by the definition of $\vdash_1 e$.

9031 \square

9032 **Lemma 4.38** : 1 canonical forms

- 9033 • If $\vdash_1 v : \text{Pair}$ then $v = \langle v_0, v_1 \rangle$
- 9034 • If $\vdash_1 v : \text{Fun}$ then $v = \lambda x. e'$ or $v = \lambda(x:\tau_d). e'$
- 9035 • If $\vdash_1 v : \text{Int}$ then $v = i$
- 9036 • If $\vdash_1 v : \text{Nat}$ then $v \in \mathbb{N}$

9037 *Proof:*

9038 QED by definition of $\vdash_1 \cdot : K$

9039 \square

9040 **Lemma 4.39** : Δ tag soundness

- 9041 If $\vdash_1 v_0 : K_0$ and $\vdash_1 v_1 : K_1$ and $\Delta(op^2, K_0, K_1) = K$ then
- 9042 $\vdash_1 \delta(op^2, v_0, v_1) : K$.

9043 *Proof:*

9044 By case analysis on Δ .

9045 **CASE** $\Delta(\text{sum}, \text{Nat}, \text{Nat}) = \text{Nat} :$

- 9046 1. $v_0 = i_0, i_0 \in \mathbb{N}$
- 9047 $\wedge v_1 = i_1, i_1 \in \mathbb{N}$
- 9048 by *canonical forms*
- 9049 2. $\delta(\text{sum}, i_0, i_1) = i_0 + i_1 \in \mathbb{N}$
- 9050 3. QED

9051 **CASE** $\Delta(\text{sum}, \text{Int}, \text{Int}) = \text{Int} :$

- 9052 1. $v_0 = i_0$
- 9053 $\wedge v_1 = i_1$
- 9054 by *canonical forms*
- 9055 2. $\delta(\text{sum}, i_0, i_1) = i_0 + i_1 \in i$
- 9056 3. QED

9057 **CASE** $\Delta(\text{quotient}, \text{Nat}, \text{Nat}) = \text{Nat} :$

- 9058 1. $v_0 = i_0, i_0 \in \mathbb{N}$
- 9059 $\wedge v_1 = i_1, i_1 \in \mathbb{N}$
- 9060 by *canonical forms*
- 9061 2. **IF** $i_1 = 0 :$
 - 9062 a. $\delta(\text{quotient}, i_0, i_1) = \text{BndryErr}$
 - 9063 b. QED by $\vdash_1 \text{BndryErr} : K$
- 9064 **ELSE** $i_1 \neq 0 :$
 - 9065 a. $\delta(\text{quotient}, i_0, i_1) = \lfloor i_0/i_1 \rfloor \in \mathbb{N}$
 - 9066 b. QED

9067 **CASE** $\Delta(\text{quotient}, \text{Int}, \text{Int}) = \text{Int} :$

- 9068 1. $v_0 = i_0$
- 9069 $\wedge v_1 = i_1$
- 9070 by *canonical forms*
- 9071 2. **IF** $i_1 = 0 :$
 - 9072 a. $\delta(\text{quotient}, i_0, i_1) = \text{BndryErr}$
 - 9073 b. QED by $\vdash_1 \text{BndryErr} : K$
- 9074 **ELSE** $i_1 \neq 0 :$

9075

a. $\delta(\text{quotient}, i_0, i_1) = \lfloor i_0/i_1 \rfloor \in i$

b. QED

9076 \square

Lemma 4.40 : δ preservation

- 9080 • If $\vdash_1 v$ and $\delta(op^1, v) = e$ then $\vdash_1 e$
- 9081 • If $\vdash_1 v_0$ and $\vdash_1 v_1$ and $\delta(op^2, v_0, v_1) = e$ then $\vdash_1 e$

9082 *Proof:*

9083 **CASE** $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0 :$

- 9084 1. $\vdash_1 v_0$
- 9085 by 1 *inversion*

9086 2. QED

9087 **CASE** $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1 :$

- 9088 1. $\vdash_1 v_1$
- 9089 by 1 *inversion*

9090 2. QED

9091 **CASE** $\delta(\text{sum}, v_0, v_1) = v_0 + v_1 :$

9092 1. QED

9093 **CASE** $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor :$

9094 1. QED

9095 **CASE** $\delta(op^2, v_0, v_1) = \text{BndryErr} :$

9096 1. QED

9097 \square

Lemma 4.41 : Δ preservation

- 9099 If $\Delta(op^2, \tau_0, \tau_1) = \tau$ then $\Delta(op^2, \lfloor \tau_0 \rfloor, \lfloor \tau_1 \rfloor) = \lfloor \tau \rfloor$.

9100 *Proof:*

9101 By case analysis on the definition of Δ

9102 **CASE** $\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat} :$

9103 1. QED by $\lfloor \text{Nat} \rfloor = \text{Nat}$

9104 **CASE** $\Delta(op^2, \text{Int}, \text{Int}) = \text{Int} :$

9105 1. QED by $\lfloor \text{Int} \rfloor = \text{Int}$

9106 \square

Lemma 4.42 : Δ inversion

- 9108 • If $\Delta(\text{fst}, \tau) = \tau'$ then $\tau = \tau_0 \times \tau_1$ and $\tau' = \tau_0$
- 9109 • If $\Delta(\text{snd}, \tau) = \tau'$ then $\tau = \tau_0 \times \tau_1$ and $\tau' = \tau_1$

9110 *Proof:*

9111 QED by the definition of Δ

9112 \square

Lemma 4.43 : $<$: preservation

- 9114 If $\tau <: \tau'$ then $\lfloor \tau \rfloor \leq \lfloor \tau' \rfloor$

9115 *Proof:*

9116 By case analysis on the last rule used to show $\tau <: \tau'$.

9117 **CASE** $\text{Nat} <: \text{Int} :$

9118 1. QED $\lfloor \text{Nat} \rfloor <: \lfloor \text{Int} \rfloor$

9119 **CASE** $\tau_d \Rightarrow \tau_c <: \tau'_d \Rightarrow \tau'_c :$

- 9120 1. $\lfloor \tau_d \Rightarrow \tau_c \rfloor = \text{Fun}$
- 9121 $\wedge \lfloor \tau'_d \Rightarrow \tau'_c \rfloor = \text{Fun}$

9122 2. QED

9123 **CASE** $\tau_0 \times \tau_1 <: \tau'_0 \times \tau'_1 :$

- 9124 1. $\lfloor \tau_0 \times \tau_1 \rfloor = \text{Pair}$
- 9125 $\wedge \lfloor \tau'_0 \times \tau'_1 \rfloor = \text{Pair}$

9126 2. QED

9127 \square

Lemma 4.44 : 1 static value inversion

9128

9076

9077

9078

9079

9080

9081

9082

9083

9084

9085

9086

9087

9088

9089

9090

9091

9092

9093

9094

9095

9096

9097

9098

9099

9100

9101

9102

9103

9104

9105

9106

9107

9108

9109

9110

9111

9112

9113

9114

9115

9116

9117

9118

9119

9120

9121

9122

9123

9124

9125

9126

9127

9128

9129

9130

9131 If $\vdash v : \text{Any}$ then $\vdash v$

9132 *Proof:*

9133 By induction on the structure of v .

9134 **CASE** $v = i$:

9135 1. QED by $\vdash v$

9136 **CASE** $v = \langle v_0, v_1 \rangle$:

9137 1. $\vdash v_0 : \text{Any}$

9138 $\wedge \vdash v_1 : \text{Any}$

9139 by 1 *inversion*

9140 2. $\vdash v_0$

9141 $\wedge \vdash v_1$

9142 by the induction hypothesis

9143 3. QED by (2)

9144 **CASE** $v = \lambda x. e$:

9145 1. $x \vdash e$

9146 by 1 *inversion*

9147 2. QED

9148 **CASE** $v = \lambda(x:\tau). e$:

9149 1. $(x:\tau) \vdash e : \text{Any}$

9150 by 1 *inversion*

9151 2. QED

9152 \square

9153 **Lemma 4.45** : 1 *dynamic value inversion*

9154 If $\vdash v$ then $\vdash v : \text{Any}$

9155 *Proof:*

9156 By induction on the structure of v .

9157 **CASE** $v = i$:

9158 1. $\vdash v : \text{Int}$

9159 2. QED by $\text{Int} <: \text{Any}$

9160 **CASE** $v = \langle v_0, v_1 \rangle$:

9161 1. $\vdash v_0$

9162 $\wedge \vdash v_1$

9163 by 1 *inversion*

9164 2. $\vdash v_0 : \text{Any}$

9165 $\wedge \vdash v_1 : \text{Any}$

9166 by the induction hypothesis

9167 3. $\vdash \langle v_0, v_1 \rangle : \text{Pair}$

9168 by (2)

9169 4. QED by $\text{Pair} <: \text{Any}$

9170 **CASE** $v = \lambda x. e$:

9171 1. $x \vdash e$

9172 by 1 *inversion*

9173 2. $\vdash \lambda x. e : \text{Fun}$

9174 by (1)

9175 3. QED by $\text{Fun} <: \text{Any}$

9176 **CASE** $v = \lambda(x:\tau). e$:

9177 1. $(x:\tau) \vdash e : \text{Any}$

9178 by 1 *inversion*

9179 2. $\vdash \lambda(x:\tau). e : \text{Fun}$

9180 by (1)

9181 3. QED by $\text{Fun} <: \text{Any}$

9182 \square

9183 **Lemma 4.46** : 1 *substitution*

9184

9185

• If $(x:\tau), \Gamma \vdash e$ and $\vdash v : [\tau]$ then $\Gamma \vdash e[x \leftarrow v]$

• If $x, \Gamma \vdash e$ and $\vdash v$ then $\Gamma \vdash e[x \leftarrow v]$

• If $(x:\tau_x), \Gamma \vdash e : K$ and $\vdash v : [\tau_x]$ then $\Gamma \vdash e[x \leftarrow v] : K$

• If $x, \Gamma \vdash e : K$ and $\vdash v$ then $\Gamma \vdash e[x \leftarrow v] : K$

Proof:

By the following four lemmas: *dynamic context static value substitution, dynamic context dynamic value substitution, static context static value substitution, and static context dynamic value substitution.*

\square

Lemma 4.47 : 1 *dynamic-static substitution*

If $(x:\tau), \Gamma \vdash e$ and $\vdash v : [\tau]$ then $\Gamma \vdash e[x \leftarrow v]$

Proof:

By induction on the structure of e .

CASE $e = x$:

1. $e[x \leftarrow v] = v$

2. $\vdash v : \text{Any}$

by $[\tau] <: \text{Any}$

3. $\vdash v$

by *static value inversion* (2)

4. $\Gamma \vdash v$

by *weakening* (3)

5. QED

CASE $e = x'$:

1. QED by $x'[x \leftarrow v] = x'$

CASE $e = i$:

1. QED by $i[x \leftarrow v] = i$

CASE $e = \lambda x. e'$:

1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$

CASE $e = \lambda(x:\tau'). e'$:

1. QED by $(\lambda(x:\tau'). e')[x \leftarrow v] = \lambda(x:\tau'). e'$

CASE $e = \lambda x'. e'$:

1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$

2. $x', (x:\tau), \Gamma \vdash e'$

by 1 *inversion*

3. $x', \Gamma \vdash e'[x \leftarrow v]$

by *dynamic context static value substitution*

4. $\Gamma \vdash \lambda x'. e'[x \leftarrow v]$

by (3)

5. QED

CASE $e = \lambda(x':\tau'). e'$:

1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$

2. $(x':\tau'), (x:\tau), \Gamma \vdash e' : \text{Any}$

by 1 *inversion*

3. $(x':\tau'), \Gamma \vdash e'[x \leftarrow v] : \text{Any}$

by *static context static value substitution*

4. $\Gamma \vdash \lambda(x':\tau'). (e'[x \leftarrow v])$

5. QED

CASE $e = \langle e_0, e_1 \rangle$:

1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$

2. $(x:\tau), \Gamma \vdash e_0$

$\wedge (x:\tau), \Gamma \vdash e_1$

by 1 *inversion*

9241	3. $\Gamma \vdash_1 e_0[x \leftarrow v]$	3. $\Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$	9296
9242	$\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$	by <i>static context static value substitution</i> (2)	9297
9243	by the induction hypothesis (2)	4. $\Gamma \vdash_1 \text{stat}(e'[x \leftarrow v])$	9298
9244	4. $\Gamma \vdash_1 \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	by (3)	9299
9245	by (3)	5. QED	9300
9246	5. QED	□	9301
9247	CASE $e = e_0 e_1 :$	Lemma 4.48 : 1 <i>dynamic-dynamic substitution</i>	9302
9248	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$	■ If $x, \Gamma \vdash_1 e$ and $\Gamma \vdash_1 v$ then $\Gamma \vdash_1 e[x \leftarrow v]$	9303
9249	2. $(x : \tau), \Gamma \vdash_1 e_0$	<i>Proof</i> :	9304
9250	$\wedge (x : \tau), \Gamma \vdash_1 e_1$	By induction on the structure of e .	9305
9251	by 1 <i>inversion</i>	CASE $e = x :$	9306
9252	3. $\Gamma \vdash_1 e_0[x \leftarrow v]$	1. $e[x \leftarrow v] = v$	9307
9253	$\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$	2. $\Gamma \vdash_1 v$	9308
9254	by the induction hypothesis (2)	by <i>weakening</i> (3)	9309
9255	4. $\Gamma \vdash_1 e_0[x \leftarrow v] e_1[x \leftarrow v]$	3. QED	9310
9256	by (3)	CASE $e = x' :$	9311
9257	5. QED	1. QED by $x'[x \leftarrow v] = x'$	9312
9258	CASE $e = \text{op}^1 e_0 :$	CASE $e = i :$	9313
9259	1. $e[x \leftarrow v] = \text{op}^1 e_0[x \leftarrow v]$	1. QED by $i[x \leftarrow v] = i$	9314
9260	2. $(x : \tau), \Gamma \vdash_1 e_0$	CASE $e = \lambda x. e' :$	9315
9261	by 1 <i>inversion</i>	1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$	9316
9262	3. $\Gamma \vdash_1 e_0[x \leftarrow v]$	CASE $e = \lambda(x : \tau'). e' :$	9317
9263	by the induction hypothesis (2)	1. QED by $(\lambda(x : \tau'). e')[x \leftarrow v] = \lambda(x : \tau'). e'$	9318
9264	4. $\Gamma \vdash_1 \text{op}^1 e_0[x \leftarrow v]$	CASE $e = \lambda x'. e' :$	9319
9265	by (3)	1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$	9320
9266	5. QED	2. $x', x, \Gamma \vdash_1 e'$	9321
9267	CASE $e = \text{op}^2 e_0 e_1 :$	by 1 <i>inversion</i>	9322
9268	1. $e[x \leftarrow v] = \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	3. $x', \Gamma \vdash_1 e'[x \leftarrow v]$	9323
9269	2. $(x : \tau), \Gamma \vdash_1 e_0$	by the induction hypothesis (2)	9324
9270	$\wedge (x : \tau), \Gamma \vdash_1 e_1$	4. $\Gamma \vdash_1 \lambda x'. e'[x \leftarrow v]$	9325
9271	by 1 <i>inversion</i>	by (3)	9326
9272	3. $\Gamma \vdash_1 e_0[x \leftarrow v]$	5. QED	9327
9273	$\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$	CASE $e = \lambda(x' : \tau'). e' :$	9328
9274	by the induction hypothesis (2)	1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$	9329
9275	4. $\Gamma \vdash_1 \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	2. $(x' : \tau'), x, \Gamma \vdash_1 e' : \text{Any}$	9330
9276	by (3)	by 1 <i>inversion</i>	9331
9277	5. QED	3. $(x' : \tau'), \Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$	9332
9278	CASE $e = \text{dyn } \tau' e'$	by <i>static context dynamic value substitution</i>	9333
9279	$\vee e = \text{dyn } e'$	4. $\Gamma \vdash_1 \lambda(x' : \tau'). (e'[x \leftarrow v])$	9334
9280	$\vee e = \text{chk } K' e' :$	5. QED	9335
9281	1. Contradiction by $(x : \tau), \Gamma \vdash_1 e$	CASE $e = \langle e_0, e_1 \rangle :$	9336
9282	CASE $e = \text{stat } \tau' e' :$	1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	9337
9283	1. $e[x \leftarrow v] = \text{stat } \tau' e'[x \leftarrow v]$	2. $x, \Gamma \vdash_1 e_0$	9338
9284	2. $(x : \tau), \Gamma \vdash_1 e' : \lfloor \tau' \rfloor$	$\wedge x, \Gamma \vdash_1 e_1$	9339
9285	by 1 <i>inversion</i>	by 1 <i>inversion</i>	9340
9286	3. $\Gamma \vdash_1 e'[x \leftarrow v] : \lfloor \tau' \rfloor$	3. $\Gamma \vdash_1 e_0[x \leftarrow v]$	9341
9287	by <i>static context static value substitution</i> (2)	$\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$	9342
9288	4. $\Gamma \vdash_1 \text{stat } \tau' (e'[x \leftarrow v])$	by the induction hypothesis (2)	9343
9289	by (3)	4. $\Gamma \vdash_1 \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	9344
9290	5. QED	by (3)	9345
9291	CASE $e = \text{stat } e' :$	5. QED	9346
9292	1. $e[x \leftarrow v] = \text{stat } e'[x \leftarrow v]$	CASE $e = e_0 e_1 :$	9347
9293	2. $(x : \tau), \Gamma \vdash_1 e' : \text{Any}$	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$	9348
9294	by 1 <i>inversion</i>		9349
9295			9350

9351 2. $x, \Gamma \vdash_1 e_0$
 9352 $\wedge x, \Gamma \vdash_1 e_1$
 9353 by 1 *inversion*
 9354 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 9355 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$
 9356 by the induction hypothesis (2)
 9357 4. $\Gamma \vdash_1 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 9358 by (3)
 9359 5. QED
 9360 **CASE** $e = op^1 e_0$:
 9361 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 9362 2. $x, \Gamma \vdash_1 e_0$
 9363 by 1 *inversion*
 9364 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 9365 by the induction hypothesis (2)
 9366 4. $\Gamma \vdash_1 op^1 e_0[x \leftarrow v]$
 9367 by (3)
 9368 5. QED
 9369 **CASE** $e = op^2 e_0 e_1$:
 9370 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 9371 2. $x, \Gamma \vdash_1 e_0$
 9372 $\wedge x, \Gamma \vdash_1 e_1$
 9373 by 1 *inversion*
 9374 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 9375 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$
 9376 by the induction hypothesis (2)
 9377 4. $\Gamma \vdash_1 op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 9378 by (3)
 9379 5. QED
 9380 **CASE** $e = dyn \tau' e'$
 9381 $\vee e = dyn e'$
 9382 $\vee e = chk K' e'$:
 9383 1. Contradiction by $\Gamma \vdash_1 e$
 9384 **CASE** $e = stat \tau' e'$:
 9385 1. $e[x \leftarrow v] = stat \tau' e'[x \leftarrow v]$
 9386 2. $x, \Gamma \vdash_1 e' : [\tau']$
 9387 by 1 *inversion*
 9388 3. $\Gamma \vdash_1 e'[x \leftarrow v] : [\tau']$
 9389 by *static context dynamic value substitution* (2)
 9390 4. $\Gamma \vdash_1 stat \tau' (e'[x \leftarrow v])$
 9391 by (3)
 9392 5. QED
 9393 **CASE** $e = stat e'$:
 9394 1. $e[x \leftarrow v] = stat e'[x \leftarrow v]$
 9395 2. $x, \Gamma \vdash_1 e' : Any$
 9396 by 1 *inversion*
 9397 3. $\Gamma \vdash_1 e'[x \leftarrow v] : Any$
 9398 by *static context dynamic value substitution* (2)
 9399 4. $\Gamma \vdash_1 stat (e'[x \leftarrow v])$
 9400 by (3)
 9401 5. QED
 9402 \square

9403 **Lemma 4.49** : 1 *static-static substitution*
 9404
 9405

9406 **If** $(x:\tau), \Gamma \vdash_1 e : K$ and $\vdash_1 v : [\tau]$ then $\Gamma \vdash_1 e[x \leftarrow v] : K$

9407 *Proof*:

9408 By induction on the structure of e .

9409 **CASE** $e = x$:

- 9410 1. $[\tau] \leq K$
- 9411 by $(x:\tau), \Gamma \vdash_1 x : K$
- 9412 2. $e[x \leftarrow v] = v$
- 9413 3. $\vdash_1 v : K$
- 9414 by (1)
- 9415 4. $\Gamma \vdash_1 v : K$
- 9416 by *weakening* (3)
- 9417 5. QED

9418 **CASE** $e = x'$:

- 9419 1. QED by $(x'[x \leftarrow v]) = x'$

9420 **CASE** $e = i$:

- 9421 1. QED by $i[x \leftarrow v] = i$

9422 **CASE** $e = \lambda x. e'$:

- 9423 1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$

9424 **CASE** $e = \lambda x'. e'$:

- 9425 1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$
- 9426 2. $x', (x:\tau), \Gamma \vdash_1 e'$
- 9427 by 1 *inversion*
- 9428 3. $x', \Gamma \vdash_1 e'[x \leftarrow v]$
- 9429 by *dynamic context static value substitution*
- 9430 4. $\Gamma \vdash_1 \lambda x'. e'[x \leftarrow v] : K$
- 9431 by (3)
- 9432 5. QED

9433 **CASE** $e = \lambda(x':\tau'). e'$:

- 9434 1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$
- 9435 2. $(x':\tau'), (x:\tau), \Gamma \vdash_1 e' : Any$
- 9436 by 1 *inversion*
- 9437 3. $(x':\tau'), \Gamma \vdash_1 e'[x \leftarrow v] : Any$
- 9438 by the induction hypothesis (2)
- 9439 4. $\Gamma \vdash_1 \lambda(x':\tau'). (e'[x \leftarrow v]) : K$
- 9440 5. QED

9441 **CASE** $e = \langle e_0, e_1 \rangle$:

- 9442 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
- 9443 2. $(x:\tau), \Gamma \vdash_1 e_0 : Any$
- 9444 $\wedge (x:\tau), \Gamma \vdash_1 e_1 : Any$
- 9445 by 1 *inversion*
- 9446 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : Any$
- 9447 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : Any$
- 9448 by the induction hypothesis (2)
- 9449 4. $\Gamma \vdash_1 \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle : K$
- 9450 by (3)
- 9451 5. QED

9452 **CASE** $e = e_0 e_1$:

- 9453 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
- 9454 2. $(x:\tau), \Gamma \vdash_1 e_0 : K_0$
- 9455 $\wedge (x:\tau), \Gamma \vdash_1 e_1 : K_1$
- 9456 by 1 *inversion*
- 9457 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$
- 9458 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : K_1$
- 9459 by the induction hypothesis (2)

9461 4. $\Gamma \vdash_1 e_0[x \leftarrow v] e_1[x \leftarrow v] : K$
 9462 by (3)
 9463 5. QED
 9464 **CASE** $e = op^1 e_0$:
 9465 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 9466 2. $(x : \tau), \Gamma \vdash_1 e_0 : K_0$
 9467 by 1 *inversion*
 9468 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$
 9469 by the induction hypothesis (2)
 9470 4. $\Gamma \vdash_1 op^1 e_0[x \leftarrow v] : K$
 9471 by (3)
 9472 5. QED
 9473 **CASE** $e = op^2 e_0 e_1$:
 9474 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 9475 2. $(x : \tau), \Gamma \vdash_1 e_0 : K_0$
 9476 $\wedge (x : \tau), \Gamma \vdash_1 e_1 : K_1$
 9477 by 1 *inversion*
 9478 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$
 9479 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : K_1$
 9480 by the induction hypothesis (2)
 9481 4. $\Gamma \vdash_1 op^2 e_0[x \leftarrow v] e_1[x \leftarrow v] : K$
 9482 by (3)
 9483 5. QED
 9484 **CASE** $e = dyn \tau' e'$:
 9485 1. $e[x \leftarrow v] = dyn \tau' e'[x \leftarrow v]$
 9486 2. $(x : \tau), \Gamma \vdash_1 e'$
 9487 by 1 *inversion*
 9488 3. $\Gamma \vdash_1 e'[x \leftarrow v]$
 9489 by *dynamic context static value substitution* (2)
 9490 4. $\Gamma \vdash_1 dyn \tau' (e'[x \leftarrow v]) : K$
 9491 by (3)
 9492 5. QED
 9493 **CASE** $e = dyn e'$:
 9494 1. $e[x \leftarrow v] = dyn e'[x \leftarrow v]$
 9495 2. $(x : \tau), \Gamma \vdash_1 e'$
 9496 by 1 *inversion*
 9497 3. $\Gamma \vdash_1 e'[x \leftarrow v]$
 9498 by *dynamic context static value substitution* (2)
 9499 4. $\Gamma \vdash_1 dyn (e'[x \leftarrow v]) : K$
 9500 by (3)
 9501 5. QED
 9502 **CASE** $e = chk K' e'$:
 9503 1. $e[x \leftarrow v] = chk K' (e'[x \leftarrow v])$
 9504 2. $(x : \tau), \Gamma \vdash_1 e' : Any$
 9505 by 1 *inversion*
 9506 3. $\Gamma \vdash_1 e'[x \leftarrow v] : Any$
 9507 by the induction hypothesis (2)
 9508 4. $\Gamma \vdash_1 chk K' (e'[x \leftarrow v]) : K$
 9509 by (3)
 9510 5. QED
 9511 **CASE** $e = stat \tau' e'$
 9512 $\vee e = stat e'$:
 9513 1. Contradiction by $\Gamma \vdash_1 e : K$
 9514
 9515

□

Lemma 4.50 : 1 *static-dynamic substitution*If $x, \Gamma \vdash_1 e : K$ and $\vdash_1 v$ then $\Gamma \vdash_1 e[x \leftarrow v] : K$ *Proof*:By induction on the structure of e .**CASE** $e = x$:1. $K = Any$ by $x, \Gamma \vdash_1 x : K$ 2. $e[x \leftarrow v] = v$ 3. $\vdash_1 v : K$ by *dynamic value inversion*4. $\vdash_1 v : Any$ by $K \leq Any$ 5. $\Gamma \vdash_1 v : Any$ by *weakening* (3)

6. QED

CASE $e = x'$:1. QED by $x'[x \leftarrow v] = x'$ **CASE** $e = i$:1. QED by $i[x \leftarrow v] = i$ **CASE** $e = \lambda x. e'$:1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$ **CASE** $e = \lambda(x : \tau'). e'$:1. QED by $(\lambda(x : \tau'). e')[x \leftarrow v] = \lambda(x : \tau'). e'$ **CASE** $e = \lambda x'. e'$:1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$ 2. $x', x, \Gamma \vdash_1 e'$ by 1 *inversion*3. $x', \Gamma \vdash_1 e'[x \leftarrow v]$ by *dynamic context dynamic value substitution*4. $\Gamma \vdash_1 \lambda x'. e'[x \leftarrow v] : K$

by (3)

5. QED

CASE $e = \lambda(x' : \tau'). e'$:1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$ 2. $(x' : \tau'), x, \Gamma \vdash_1 e' : Any$ by 1 *inversion*3. $(x' : \tau'), \Gamma \vdash_1 e'[x \leftarrow v] : Any$ by *static context dynamic value substitution*4. $\Gamma \vdash_1 \lambda(x' : \tau'). (e'[x \leftarrow v]) : K$

5. QED

CASE $e = \langle e_0, e_1 \rangle$:1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$ 2. $x, \Gamma \vdash_1 e_0 : Any$ $\wedge x, \Gamma \vdash_1 e_1 : Any$ by 1 *inversion*3. $\Gamma \vdash_1 e_0[x \leftarrow v] : Any$ $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : Any$

by the induction hypothesis (2)

4. $\Gamma \vdash_1 \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle : K$

by (3)

5. QED

CASE $e = e_0 e_1$:

9571	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$	4. $\Gamma \vdash_1 \text{chk } K' (e'[x \leftarrow v]) : K$	9626
9572	2. $x, \Gamma \vdash_1 e_0 : K_0$	by (3)	9627
9573	$\wedge x, \Gamma \vdash_1 e_1 : K_1$	5. QED	9628
9574	by 1 <i>inversion</i>	CASE $e = \text{stat } \tau' e'$	9629
9575	3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$	$\vee e = \text{stat } e' :$	9630
9576	$\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : K_1$	1. Contradiction by $\Gamma \vdash_1 e : K$	9631
9577	by the induction hypothesis (2)	□	9632
9578	4. $\Gamma \vdash_1 e_0[x \leftarrow v] e_1[x \leftarrow v] : K$	Lemma 4.51 : <i>weakening</i>	9633
9579	by (3)	• If $\Gamma \vdash_1 e$ then $x, \Gamma \vdash_1 e$	9634
9580	5. QED	• If $\Gamma \vdash_1 e : \tau$ then $(x : \tau'), \Gamma \vdash_1 e : \tau$	9635
9581	CASE $e = \text{op}^1 e_0 :$	<i>Proof</i> :	9636
9582	1. $e[x \leftarrow v] = \text{op}^1 e_0[x \leftarrow v]$	• e is closed under Γ	9637
9583	2. $x, \Gamma \vdash_1 e_0 : K_0$	by $\Gamma \vdash_1 e$	9638
9584	by 1 <i>inversion</i>	$\vee \Gamma \vdash_1 e : \tau$ QED	9639
9585	3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$	□	9640
9586	by the induction hypothesis (2)	Lemma 4.52 : <i>unique static evaluation contexts</i>	9641
9587	4. $\Gamma \vdash_1 \text{op}^1 e_0[x \leftarrow v] : K$	If $\vdash e : \tau$ and e is boundary-free then one of the following	9642
9588	by (3)	holds:	9643
9589	5. QED	• e is a value	9644
9590	CASE $e = \text{op}^2 e_0 e_1 :$	• $e = E^\bullet[v_0 v_1]$	9645
9591	1. $e[x \leftarrow v] = \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	• $e = E^\bullet[\text{op}^1 v]$	9646
9592	2. $x, \Gamma \vdash_1 e_0 : K_0$	• $e = E^\bullet[\text{op}^2 v_0 v_1]$	9647
9593	$\wedge x, \Gamma \vdash_1 e_1 : K_1$	• $e = E^\bullet[\text{Err}]$	9648
9594	by 1 <i>inversion</i>	<i>Proof</i> :	9649
9595	3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$	By induction on the structure of e .	9650
9596	$\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : K_1$	CASE $e = x :$	9651
9597	by the induction hypothesis (2)	1. Contradiction by $\vdash e : \tau$	9652
9598	4. $\Gamma \vdash_1 \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v] : K$	CASE $e = i$	9653
9599	by (3)	$\vee e = \lambda(x : \tau_d). e' :$	9654
9600	5. QED	1. QED e is a value	9655
9601	CASE $e = \text{dyn } \tau' e' :$	CASE $e = \langle e_0, e_1 \rangle :$	9656
9602	1. $e[x \leftarrow v] = \text{dyn } \tau' e'[x \leftarrow v]$	IF $e_0 \notin v :$	9657
9603	2. $x, \Gamma \vdash_1 e' :$	1. $e_0 = E^\bullet_0[e'_0]$	9658
9604	by 1 <i>inversion</i>	by the induction hypothesis	9659
9605	3. $\Gamma \vdash_1 e'[x \leftarrow v]$	2. $E^\bullet = \langle E^\bullet_0, e_1 \rangle$	9660
9606	by <i>dynamic context dynamic value substitution</i> (2)	3. QED by $e = E^\bullet[e'_0]$	9661
9607	4. $\Gamma \vdash_1 \text{dyn } \tau' (e'[x \leftarrow v]) : K$	IF $e_0 \in v$	9662
9608	by (3)	$\wedge e_1 \notin v :$	9663
9609	5. QED	1. $e_1 = E^\bullet_1[e'_1]$	9664
9610	CASE $e = \text{dyn } e' :$	by the induction hypothesis	9665
9611	1. $e[x \leftarrow v] = \text{dyn } e'[x \leftarrow v]$	2. $E^\bullet = \langle e_0, E^\bullet_1 \rangle$	9666
9612	2. $x, \Gamma \vdash_1 e' :$	3. QED by $e = E^\bullet[e'_1]$	9667
9613	by 1 <i>inversion</i>	ELSE $e_0 \in v$	9668
9614	3. $\Gamma \vdash_1 e'[x \leftarrow v]$	$\wedge e_1 \in v :$	9669
9615	by <i>dynamic context dynamic value substitution</i> (2)	1. $E^\bullet = []$	9670
9616	4. $\Gamma \vdash_1 \text{dyn } (e'[x \leftarrow v]) : K$	2. QED $e = E^\bullet[\langle e_0, e_1 \rangle]$	9671
9617	by (3)	CASE $e = e_0 e_1 :$	9672
9618	5. QED	IF $e_0 \notin v :$	9673
9619	CASE $e = \text{chk } K' e' :$	1. $e_0 = E^\bullet_0[e'_0]$	9674
9620	1. $e[x \leftarrow v] = \text{chk } K' (e'[x \leftarrow v])$	by the induction hypothesis	9675
9621	2. $x, \Gamma \vdash_1 e' : \text{Any}$	2. $E^\bullet = E^\bullet_0 e_1$	9676
9622	by 1 <i>inversion</i>	3. QED by $e = E^\bullet[e'_0]$	9677
9623	3. $\Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$		9678
9624	by the induction hypothesis (2)		9679
9625			9680

9681 **IF** $e_0 \in v$
 9682 $\wedge e_1 \notin v :$
 9683 1. $e_1 = E^{\bullet}_1[e'_1]$
 9684 by the induction hypothesis
 9685 2. $E^{\bullet} = e_0 E^{\bullet}_1$
 9686 3. QED by $e = E^{\bullet}[e'_1]$
 9687 **ELSE** $e_0 \in v$
 9688 $\wedge e_1 \in v :$
 9689 1. $E^{\bullet} = []$
 9690 2. QED $e = E^{\bullet}[e_0 e_1]$
 9691 **CASE** $e = op^1 e_0 :$
 9692 **IF** $e_0 \notin v :$
 9693 1. $e_0 = E^{\bullet}_0[e'_0]$
 9694 by the induction hypothesis
 9695 2. $E^{\bullet} = op^1 E^{\bullet}_0$
 9696 3. QED $e = E^{\bullet}[e'_0]$
 9697 **ELSE** $e_0 \in v :$
 9698 1. $E^{\bullet} = []$
 9699 2. QED $e = E^{\bullet}[op^1 e_0]$
 9700 **CASE** $e = op^2 e_0 e_1 :$
 9701 **IF** $e_0 \notin v :$
 9702 1. $e_0 = E^{\bullet}_0[e'_0]$
 9703 by the induction hypothesis
 9704 2. $E^{\bullet} = op^2 E^{\bullet}_0 e_1$
 9705 3. QED $e = E^{\bullet}[e'_0]$
 9706 **IF** $e_0 \in v$
 9707 $\wedge e_1 \notin v :$
 9708 1. $e_1 = E^{\bullet}_1[e'_1]$
 9709 by the induction hypothesis
 9710 2. $E^{\bullet} = op^2 e_0 E^{\bullet}_1$
 9711 3. QED $e = E^{\bullet}[e'_1]$
 9712 **ELSE** $e_0 \in v$
 9713 $\wedge e_1 \in v :$
 9714 1. $E^{\bullet} = []$
 9715 2. QED $e = E^{\bullet}[op^2 e_0 e_1]$
 9716 **CASE** $e = chk K' e' :$
 9717 1. Contradiction by $\vdash e : \tau$
 9718 **CASE** $e = dyn e_0 :$
 9719 1. Contradiction by $\vdash e : \tau$
 9720 **CASE** $e = stat e' :$
 9721 1. Contradiction by $\vdash e : \tau$
 9722 **CASE** $e = dyn \tau e_0 :$
 9723 1. QED e is boundary-free
 9724 **CASE** $e = stat \tau e' :$
 9725 1. Contradiction by $\vdash e : \tau$
 9726 **CASE** $e = Err :$
 9727 1. $E^{\bullet} = []$
 9728 2. QED
 9729 \square

9730 **Lemma 4.53** : \vdash static inversion
 9731
 9732
 9733
 9734
 9735

- If $\Gamma \vdash x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$ 9736
- If $\Gamma \vdash \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$ 9737
- If $\Gamma \vdash \langle e_0, e_1 \rangle : \tau$ then $\Gamma \vdash e_0 : \tau_0$ and $\Gamma \vdash e_1 : \tau_1$ and $\tau_0 \times \tau_1 \leq \tau$ 9738
- If $\Gamma \vdash e_0 e_1 : \tau_c$ then $\Gamma \vdash e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$ 9739
- If $\Gamma \vdash fst e : \tau$ then $\Gamma \vdash e : \tau_0 \times \tau_1$ and $\Delta(fst, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$ 9740
- If $\Gamma \vdash snd e : \tau$ then $\Gamma \vdash e : \tau_0 \times \tau_1$ and $\Delta(snd, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$ 9741
- If $\Gamma \vdash op^2 e_0 e_1 : \tau$ then $\Gamma \vdash e_0 : \tau_0$ and $\Gamma \vdash e_1 : \tau_1$ and $\Delta(op^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$ 9742
- If $\Gamma \vdash dyn \tau' e' : \tau$ then $\Gamma \vdash e'$ and $\tau' \leq \tau$ 9743

9744 *Proof:*

9745 QED by the definition of $\Gamma \vdash e : \tau$

9746 \square

9747 **Lemma 4.54** : canonical forms

- If $\vdash v : \tau_0 \times \tau_1$ then $v = \langle v_0, v_1 \rangle$ 9748
- If $\vdash v : \tau_d \Rightarrow \tau_c$ then $v = \lambda(x : \tau_x). e'$ 9749
- $\wedge \tau_d \leq \tau_x$ 9750
- If $\vdash v : Int$ then $v = i$ 9751
- If $\vdash v : Nat$ then $v = i$ and $v \in \mathbb{N}$ 9752

9753 *Proof:*

9754 QED by definition of $\vdash e : \tau$

9755 \square

9756 **Lemma 4.55** : substitution

- If $(x : \tau_x), \Gamma \vdash e : \tau$, and e is boundary-free and $\vdash v : \tau_x$ then 9757
- $\Gamma \vdash e[x \leftarrow v] : \tau$ 9758

9759 *Proof:*

9760 By induction on the structure of e .

9761 **CASE** $e = x :$

9762 1. $e[x \leftarrow v] = v$ 9763

9764 2. $\tau_x = \tau$ 9765

9766 3. $\Gamma \vdash v : \tau$ 9767

9768 by *weakening* 9769

9770 4. QED 9771

9772 **CASE** $e = x' :$

9773 1. QED by $x'[x \leftarrow v] = x'$ 9774

9775 **CASE** $e = i :$

9776 1. QED by $i[x \leftarrow v] = i$ 9777

9778 **CASE** $e = \lambda x. e' :$

9779 1. Contradiction by $(x : \tau_x), \Gamma \vdash e : \tau$ 9780

9781 **CASE** $e = \lambda(x : \tau'). e' :$

9782 1. QED by $(\lambda(x : \tau'). e')[x \leftarrow v] = \lambda(x : \tau'). e'$ 9783

9784 **CASE** $e = \lambda(x' : \tau'). e' :$

9785 1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$ 9786

9787 2. $(x' : \tau'), x, \Gamma \vdash e'$ 9788

9789 by *static inversion forms* 9790

9791 3. $(x' : \tau'), \Gamma \vdash e'[x \leftarrow v]$ 9792

9793 by the induction hypothesis (2) 9794

9795 4. $\Gamma \vdash \lambda(x' : \tau'). (e'[x \leftarrow v])$ 9796

9797 by (3) 9798

9799 5. QED 9800

9791 **CASE** $e = \langle e_0, e_1 \rangle :$
 9792 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 9793 2. $x, \Gamma \vdash e_0$
 9794 $\wedge x, \Gamma \vdash e_1$
 9795 by *static inversion forms*
 9796 3. $\Gamma \vdash e_0[x \leftarrow v]$
 9797 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
 9798 by the induction hypothesis (2)
 9799 4. $\Gamma \vdash \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 9800 by (3)
 9801 5. QED
 9802 **CASE** $e = e_0 e_1 :$
 9803 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
 9804 2. $x, \Gamma \vdash e_0$
 9805 $\wedge x, \Gamma \vdash e_1$
 9806 by *static inversion forms*
 9807 3. $\Gamma \vdash e_0[x \leftarrow v]$
 9808 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
 9809 by the induction hypothesis (2)
 9810 4. $\Gamma \vdash e_0[x \leftarrow v] e_1[x \leftarrow v]$
 9811 by (3)
 9812 5. QED
 9813 **CASE** $e = op^1 e_0 :$
 9814 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 9815 2. $x, \Gamma \vdash e_0$
 9816 by *static inversion forms*
 9817 3. $\Gamma \vdash e_0[x \leftarrow v]$
 9818 by the induction hypothesis (2)
 9819 4. $\Gamma \vdash op^1 e_0[x \leftarrow v]$
 9820 by (3)
 9821 5. QED
 9822 **CASE** $e = op^2 e_0 e_1 :$
 9823 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 9824 2. $x, \Gamma \vdash e_0$
 9825 $\wedge x, \Gamma \vdash e_1$
 9826 by *static inversion forms*
 9827 3. $\Gamma \vdash e_0[x \leftarrow v]$
 9828 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
 9829 by the induction hypothesis (2)
 9830 4. $\Gamma \vdash op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 9831 by (3)
 9832 5. QED
 9833 **CASE** $e = \text{chk } K' e' :$
 9834 1. Contradiction by $\vdash e : \tau$
 9835 **CASE** $e = \text{dyn } e' :$
 9836 1. Contradiction by $\vdash e : \tau$
 9837 **CASE** $e = \text{stat } e' :$
 9838 1. Contradiction by $\vdash e : \tau$
 9839 **CASE** $e = \text{dyn } \tau' e' :$
 9840 1. Contradiction by e is boundary-free
 9841 **CASE** $e = \text{stat } \tau' e' :$
 9842 1. Contradiction by $\vdash e : \tau$
 9843 **CASE** $e = \text{Err} :$
 9844 1. QED $\text{Err}[x \leftarrow v] = \text{Err}$
 9845

□

Lemma 4.56 : δ preservation

- If $\vdash v$ and $\delta(op^1, v) = v'$ then $\vdash e'$
- If $\vdash v_0$ and $\vdash v_1$ and $\delta(op^2, v_0, v_1) = e'$ then $\vdash v'$

Proof:

CASE $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0 :$

1. $\vdash v_0$

by *static inversion forms*

2. QED

CASE $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1 :$

1. $\vdash v_1$

by *static inversion forms*

2. QED

CASE $\delta(\text{sum}, v_0, v_1) = v_0 + v_1 :$

1. QED

CASE $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor :$

1. QED

CASE $\delta(\text{quotient}, v_0, v_1) = \text{BndryErr} :$

1. QED

□

Lemma 4.57 : *weakening*

- If $\Gamma \vdash e$ then $x, \Gamma \vdash e$
- If $\Gamma \vdash e$ then $(x : \tau), \Gamma \vdash e$

Proof:

QED because e is closed under Γ

□

9846
9847
9848
9849
9850
9851
9852
9853
9854
9855
9856
9857
9858
9859
9860
9861
9862
9863
9864
9865
9866
9867
9868
9869
9870
9871
9872
9873
9874
9875
9876
9877
9878
9879
9880
9881
9882
9883
9884
9885
9886
9887
9888
9889
9890
9891
9892
9893
9894
9895
9896
9897
9898
9899
9900

E.5 (HC) Co-Natural Embedding

E.5.1 Co-Natural Definitions

Language HC

$e = x \mid v \mid \langle e, e \rangle \mid e e \mid op^1 e \mid op^2 e e \mid$
 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err}$
 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e$
 $\text{mon}(\tau \Rightarrow \tau) v \mid \text{mon}(\tau \times \tau) v$
 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$
 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$
 $r = v \mid \text{Err}$
 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet$
 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E$

 $\Delta : op^1 \times \tau \longrightarrow \tau$

$$\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$$

$$\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$$

 $\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$

$$\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$$

$$\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$$

 $\tau \leqslant: \tau$

$$\text{Nat} \leqslant: \text{Int} \quad \frac{\tau'_d \leqslant: \tau_d \quad \tau_c \leqslant: \tau'_c \quad \tau_0 \leqslant: \tau'_0 \quad \tau_1 \leqslant: \tau'_1}{\tau_d \Rightarrow \tau_c \leqslant: \tau'_d \Rightarrow \tau'_c} \quad \frac{\tau_0 \times \tau_1 \leqslant: \tau'_0 \times \tau'_1}{\tau_0 \times \tau_1 \leqslant: \tau'_0 \times \tau'_1}$$

$$\frac{\tau \leqslant: \tau'}{\tau \leqslant: \tau} \quad \frac{\tau \leqslant: \tau' \quad \tau' \leqslant: \tau''}{\tau \leqslant: \tau''}$$

 $\Gamma \vdash e$

$$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$$

$$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$$

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$$

 $\Gamma \vdash e : \tau$

$$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$$

$$\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$$

$$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e : \tau'}{\Delta(op^2, \tau_0, \tau_1) = \tau \quad \tau' \leqslant: \tau \quad \Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$$

$$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$$

 $\Gamma \vdash_C e$

$$\frac{x \in \Gamma}{\Gamma \vdash_C x} \quad \frac{x, \Gamma \vdash_C e}{\Gamma \vdash_C \lambda x. e} \quad \frac{}{\Gamma \vdash_C i} \quad \frac{\Gamma \vdash_C e_0 \quad \Gamma \vdash_C e_1}{\Gamma \vdash_C \langle e_0, e_1 \rangle}$$

$$\frac{\Gamma \vdash_C e_0 \quad \Gamma \vdash_C e_1}{\Gamma \vdash_C e_0 e_1} \quad \frac{\Gamma \vdash_C e}{\Gamma \vdash_C op^1 e} \quad \frac{\Gamma \vdash_C e_0 \quad \Gamma \vdash_C e_1}{\Gamma \vdash_C op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash_C \text{Err}}$$

$$\frac{\Gamma \vdash_C e : \tau}{\Gamma \vdash_C \text{stat } \tau e} \quad \frac{\Gamma \vdash_C v : \tau_0 \times \tau_1}{\Gamma \vdash_C \text{mon}(\tau_0 \times \tau_1) v} \quad \frac{\Gamma \vdash_C v : \tau_d \Rightarrow \tau_c}{\Gamma \vdash_C \text{mon}(\tau_d \Rightarrow \tau_c) v}$$

 $\Gamma \vdash_C e : \tau$

$$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash_C x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash_C e : \tau_c}{\Gamma \vdash_C \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash_C i : \text{Nat}}$$

$$\frac{}{\Gamma \vdash_C i : \text{Int}} \quad \frac{\Gamma \vdash_C e_0 : \tau_0 \quad \Gamma \vdash_C e_1 : \tau_1}{\Gamma \vdash_C \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash_C e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash_C e_1 : \tau_d}{\Gamma \vdash_C e_0 e_1 : \tau_c}$$

$$\frac{\Gamma \vdash_C e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash_C op^1 e_0 : \tau} \quad \frac{\Gamma \vdash_C e_0 : \tau_0 \quad \Gamma \vdash_C e_1 : \tau_1 \quad \Gamma \vdash_C e : \tau'}{\Delta(op^2, \tau_0, \tau_1) = \tau \quad \tau' \leqslant: \tau \quad \Gamma \vdash_C e : \tau} \quad \frac{}{\Gamma \vdash_C \text{Err} : \tau}$$

$$\frac{\Gamma \vdash_C e}{\Gamma \vdash_C \text{dyn } \tau e : \tau}$$

$$\frac{\Gamma \vdash_C v}{\Gamma \vdash_C \text{mon}(\tau_0 \times \tau_1) v : (\tau_0 \times \tau_1)}$$

$$\frac{\Gamma \vdash_C v}{\Gamma \vdash_C \text{mon}(\tau_d \Rightarrow \tau_c) v : (\tau_d \Rightarrow \tau_c)}$$

10011	$\delta(op^1, v) = e$	$e \rightarrow_{C-S} e$	10066
10012	$\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$	$E^*[e] \rightarrow_{C-S} E^*[e']$	10067
10013	$\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$	if $e \triangleright_{S-C} e'$	10068
10014	$\delta(op^2, v, v) = e$	$E[\text{stat } \tau E^*[e]] \rightarrow_{C-S} E[\text{stat } \tau E^*[e']]$	10069
10015		if $e \triangleright_{S-C} e'$	10070
10016	$\delta(\text{sum}, i_0, i_1) = i_0 + i_1$	$E[\text{dyn } \tau E^*[e]] \rightarrow_{C-S} E[\text{dyn } \tau E^*[e']]$	10071
10017	$\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$	if $e \triangleright_{D-C} e'$	10072
10018	$\delta(\text{quotient}, i_0, i_1) = \lfloor i_0 / i_1 \rfloor$	$E[\text{Err}] \rightarrow_{C-S} \text{Err}$	10073
10019	if $i_1 \neq 0$		10074
10020	$\mathcal{D}_C : \tau \times v \rightarrow e$	$e \rightarrow_{C-D} e$	10075
10021	$\mathcal{D}_C(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v$	$E^*[e] \rightarrow_{C-D} E^*[e']$	10076
10022	if $v = \lambda x. e$ or $v = \text{mon}(\tau'_d \Rightarrow \tau'_c) v'$	if $e \triangleright_{D-C} e'$	10077
10023	$\mathcal{D}_C(\tau_0 \times \tau_1, v) = \text{mon}(\tau_0 \times \tau_1) v$	$E[\text{stat } \tau E^*[e]] \rightarrow_{C-D} E[\text{stat } \tau E^*[e']]$	10078
10024	if $v = \langle v_0, v_1 \rangle$ or $v = \text{mon}(\tau'_0 \times \tau'_1) v'$	if $e \triangleright_{S-C} e'$	10079
10025	$\mathcal{D}_C(\text{Int}, i) = i$	$E[\text{dyn } \tau E^*[e]] \rightarrow_{C-D} E[\text{dyn } \tau E^*[e']]$	10080
10026	$\mathcal{D}_C(\text{Nat}, i) = i$	if $e \triangleright_{D-C} e'$	10081
10027	if $i \in \mathbb{N}$	$E[\text{Err}] \rightarrow_{C-D} \text{Err}$	10082
10028	$\mathcal{D}_C(\tau, v) = \text{BndryErr}$	$e \rightarrow_{C-S}^* e$ reflexive, transitive closure of \rightarrow_{C-S}	10083
10029	otherwise		10084
10030	$\mathcal{S}_C : \tau \times v \rightarrow e$	$e \rightarrow_{C-D}^* e$ reflexive, transitive closure of \rightarrow_{C-D}	10085
10031			10086
10032	$\mathcal{S}_C(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v$		10087
10033	$\mathcal{S}_C(\tau_0 \times \tau_1, v) = \text{mon}(\tau_0 \times \tau_1) v$		10088
10034	$\mathcal{S}_C(\tau, v) = v$		10089
10035	otherwise		10090
10036	$e \triangleright_{S-C} e$		10091
10037	$\text{dyn } \tau v \triangleright_{S-C} \mathcal{D}_C(\tau, v)$		10092
10038	$(\text{mon}(\tau_d \Rightarrow \tau_c) v_f) v \triangleright_{S-C} \text{dyn } \tau_c (v_f e')$		10093
10039	where $e' = \text{stat } \tau_d v$		10094
10040	$(\lambda(x:\tau). e) v \triangleright_{S-C} e[x \leftarrow v]$		10095
10041	$\text{fst}(\text{mon}(\tau_0 \times \tau_1) v) \triangleright_{S-C} \text{dyn } \tau_0 (\text{fst } v)$		10096
10042	$\text{snd}(\text{mon}(\tau_0 \times \tau_1) v) \triangleright_{S-C} \text{dyn } \tau_1 (\text{snd } v)$		10097
10043	$op^1 v \triangleright_{S-C} \delta(op^1, v)$		10098
10044	$op^2 v_0 v_1 \triangleright_{S-C} \delta(op^2, v_0, v_1)$		10099
10045	$e \triangleright_{D-C} e$		10100
10046	$\text{stat } \tau v \triangleright_{D-C} \mathcal{S}_C(\tau, v)$		10101
10047	$v_0 v_1 \triangleright_{D-C} \text{TagErr}$		10102
10048	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$		10103
10049	$(\text{mon}(\tau_d \Rightarrow \tau_c) v_f) v \triangleright_{D-C} \text{stat } \tau_c (v_f e')$		10104
10050	where $e' = \text{dyn } \tau_d v$		10105
10051	$(\lambda x. e) v \triangleright_{D-C} e[x \leftarrow v]$		10106
10052	$\text{fst}(\text{mon}(\tau_0 \times \tau_1) v) \triangleright_{D-C} \text{stat } \tau_0 (\text{fst } v)$		10107
10053	$\text{snd}(\text{mon}(\tau_0 \times \tau_1) v) \triangleright_{D-C} \text{stat } \tau_1 (\text{snd } v)$		10108
10054	$op^1 v \triangleright_{D-C} \text{TagErr}$		10109
10055	if $\delta(op^1, v)$ is undefined		10110
10056	$op^1 v \triangleright_{D-C} \delta(op^1, v)$		10111
10057	$op^2 v_0 v_1 \triangleright_{D-C} \text{TagErr}$		10112
10058	if $\delta(op^2, v_0, v_1)$ is undefined		10113
10059	$op^2 v_0 v_1 \triangleright_{D-C} \delta(op^2, v_0, v_1)$		10114
10060			10115
10061			10116
10062			10117
10063			10118
10064			10119
10065			10120

10121 E.5.2 Co-Natural Theorems

10122 Theorem 5.0 : static HC soundness

10123 If $\vdash e : \tau$ then $\vdash_C e : \tau$ and one of the following holds:

- 10124 • $e \rightarrow_{C-S}^* v$ and $\vdash_C v : \tau$
- 10125 • $e \rightarrow_{C-S}^* E[\text{dyn } \tau' e']$ and $e' \triangleright_{D-C} \text{TagErr}$
- 10126 • $e \rightarrow_{C-S}^* \text{BndryErr}$
- 10127 • e diverges

10128 *Proof:*

- 10129 1. $\vdash_C e : \tau$
by *static subset*
- 10130 2. QED by *static progress* and *static preservation*.

10132 □

10133 Theorem 5.1 : dynamic HC-soundness

10134 If $\vdash e$ then $\vdash_C e$ and one of the following holds:

- 10135 • $e \rightarrow_{C-D}^* v$ and $\vdash_C v$
- 10136 • $e \rightarrow_{C-D}^* E[e']$ and $e' \triangleright_{D-C} \text{TagErr}$
- 10137 • $e \rightarrow_{C-D}^* \text{BndryErr}$
- 10138 • e diverges

10139 *Proof:*

- 10140 1. $\vdash_C e$
by *dynamic subset*
- 10141 2. QED by *dynamic progress* and *dynamic preservation*.

10143 □

10144 Corollary 5.2 : HC static soundness

10145 If $\vdash e : \tau$ and e is boundary-free, then one of the following
10146 holds:

- 10147 • $e \rightarrow_{C-S}^* v$ and $\vdash_C v : \tau$
- 10148 • $e \rightarrow_{C-S}^* \text{BndryErr}$
- 10149 • e diverges

10150 *Proof:*

10151 Consequence of the proof for *static HC-soundness*

10152 □

10153
10154
10155
10156
10157
10158
10159
10160
10161
10162
10163
10164
10165
10166
10167
10168
10169
10170
10171
10172
10173
10174
10175

10176
10177
10178
10179
10180
10181
10182
10183
10184
10185
10186
10187
10188
10189
10190
10191
10192
10193
10194
10195
10196
10197
10198
10199
10200
10201
10202
10203
10204
10205
10206
10207
10208
10209
10210
10211
10212
10213
10214
10215
10216
10217
10218
10219
10220
10221
10222
10223
10224
10225
10226
10227
10228
10229
10230

E.5.3 Co-Natural Lemmas

Lemma 5.3 : \mathcal{D}_C soundness

 If $\vdash_C v$ then $\vdash_C \mathcal{D}_C(\tau, v) : \tau$
Proof:
CASE $\mathcal{D}_C(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

1. $\vdash_C \text{mon}(\tau_d \Rightarrow \tau_c) v : \tau_d \Rightarrow \tau_c$
by $\vdash_C v$

2. QED

CASE $\mathcal{D}_C(\tau_0 \times \tau_1, v) = \text{mon}(\tau_0 \times \tau_1) v :$

1. $\vdash_C \text{mon}(\tau_0 \times \tau_1) v : \tau_0 \times \tau_1$
by $\vdash_C v$

2. QED

CASE $v = i$
 $\wedge \mathcal{D}_C(\text{Int}, v) = v :$

1. QED

CASE $v \in \mathbb{N}$
 $\wedge \mathcal{D}_C(\text{Nat}, v) = v :$

1. QED

CASE $\mathcal{D}_C(\tau, v) = \text{BndryErr} :$

1. QED

□

Lemma 5.4 : \mathcal{S}_C soundness

 If $\vdash_C v : \tau$ then $\vdash_C \mathcal{S}_C(\tau, v)$
Proof:
CASE $\vdash_C v : \tau_d \Rightarrow \tau_c$
 $\wedge \mathcal{S}_C(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

1. QED

CASE $\vdash_C v : \tau_0 \times \tau_1$
 $\wedge \mathcal{S}_C(\tau_0 \times \tau_1, v) = \text{mon}(\tau_0 \times \tau_1) v :$

1. QED

CASE $\vdash_C v : \text{Int}$
 $\wedge \mathcal{S}_C(\text{Int}, v) = v :$

1. QED

CASE $\vdash_C v : \text{Nat}$
 $\wedge \mathcal{S}_C(\text{Nat}, v) = v :$

1. QED

□

Corollary 5.5 : HC static subset

 If $\Gamma \vdash e : \tau$ then $\Gamma \vdash_C e : \tau$.

Proof:

Consequence of the proof for the higher-order *static subset* lemma; both \vdash_C and \vdash_H have the same typing rules for surface-language expressions.

□

Corollary 5.6 : HC dynamic subset

 If $\Gamma \vdash e$ then $\Gamma \vdash_C e$.

Proof:

Consequence of the proof for the higher-order *dynamic subset* lemma.

□

Lemma 5.7 : HC static progress

 If $\vdash_C e : \tau$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{C-S} e'$
- $e \rightarrow_{C-S} \text{BndryErr}$
- $e = E[\text{dyn } \tau' e']$ and $e' \rightarrow_{C-D} \text{TagErr}$

Proof:

 By the *boundary factoring* lemma, there are seven possible cases.

CASE e is a value :

1. QED

CASE $e = E^*[v_0 v_1] :$

 1. $\vdash_C v_0 v_1 : \tau'$

 by *static hole typing*

 2. $\vdash_C v_0 : \tau_d \Rightarrow \tau_c$
 $\wedge \vdash_C v_1 : \tau_d$

 by *inversion*

 3. $v_0 = \lambda(x : \tau'_d). e'$
 $\vee v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_f$

 by *canonical forms*

 4. **IF** $v_0 = \lambda(x : \tau'_d). e' :$

 a. $e \rightarrow_{C-S} E^*[e'[x \leftarrow v_1]]$

 by $v_0 v_1 \triangleright_{S-C} e'[x \leftarrow v_1]$

b. QED

ELSE $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_f :$

 a. $e \rightarrow_{C-S} E^*[\text{dyn } \tau'_c (v_f (\text{stat } \tau'_d v_1))]$

 by $v_0 v_1 \triangleright_{S-C} \text{dyn } \tau'_c (v_f (\text{stat } \tau'_d v_1))$

b. QED

CASE $e = E^*[op^1 v] :$

 1. $\vdash_C op^1 v : \tau'$

 by *static hole typing*

 2. $\vdash_C v : \tau_0 \times \tau_1$

 by *inversion*

 3. $v = \langle v_0, v_1 \rangle$
 $\vee v = \text{mon}(\tau_0 \times \tau_1) v'$

 by *canonical forms*

 4. **IF** $v = \langle v_0, v_1 \rangle$
 $\wedge op^1 = \text{fst} :$

 a. $\delta(op^1, \langle v_0, v_1 \rangle) = v_0$

by definition

 b. $e \rightarrow_{C-S} E^*[v_0]$

 by $op^1 v \triangleright_{S-C} v_0$

c. QED

IF $v = \langle v_0, v_1 \rangle$
 $\wedge op^1 = \text{snd} :$

 a. $\delta(op^1, \langle v_0, v_1 \rangle) = v_1$

by definition

 b. $e \rightarrow_{C-S} E^*[v_1]$

 by $op^1 v \triangleright_{S-C} v_1$

c. QED

IF $v = \text{mon}(\tau_0 \times \tau_1) v'$
 $\wedge op^1 = \text{fst} :$

 a. $e \rightarrow_{C-S} E^*[\text{dyn } \tau_0 (op^1 v')]$

by definition

10341 b. QED

10342 **ELSE** $v = \text{mon}(\tau_0 \times \tau_1) v'$

10343 $\wedge \text{op}^1 = \text{snd} :$

10344 a. $e \rightarrow_{\text{C-S}} E^\bullet[\text{dyn } \tau_1 (\text{op}^1 v')]$

10345 by definition

10346 b. QED

10347 **CASE** $e = E^\bullet[\text{op}^2 v_0 v_1] :$

10348 1. $\vdash_{\text{C}} \text{op}^2 v_0 v_1 : \tau'$

10349 by *static hole typing*

10350 2. $\vdash_{\text{C}} v_0 : \tau_0$

10351 $\wedge \vdash_{\text{C}} v_1 : \tau_1$

10352 $\wedge \Delta(\text{op}^2, \tau_0, \tau_1) = \tau''$

10353 by *inversion*

10354 3. $\delta(\text{op}^2, v_0, v_1) = e'$

10355 by Δ *type soundness* (2)

10356 4. $\text{op}^2 v_0 v_1 \triangleright_{\text{S-C}} e'$

10357 by (3)

10358 5. QED by $e \rightarrow_{\text{C-S}} E^\bullet[e']$

10359 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :

10360 1. e' is a value

10361 $\vee e' \in \text{Err}$

10362 $\vee e' \rightarrow_{\text{C-D}} e''$

10363 $\vee e' \rightarrow_{\text{C-D}} \text{BndryErr}$

10364 $\vee e' = E'[e'']$ and $e'' \triangleright_{\text{D-C}} \text{TagErr}$

10365 by *dynamic progress*

10366 2. **IF** e' is a value :

10367 a. QED $e \rightarrow_{\text{C-S}} E[\mathcal{D}_{\text{C}}(\tau', e')]$

10368 **IF** $e' \in \text{Err} :$

10369 a. QED $e \rightarrow_{\text{C-S}} e'$

10370 **IF** $e' \rightarrow_{\text{C-D}} e'' :$

10371 a. QED $e \rightarrow_{\text{C-S}} E[\text{dyn } \tau' e'']$

10372 **IF** $e' \rightarrow_{\text{C-D}} \text{BndryErr} :$

10373 a. QED $e \rightarrow_{\text{C-S}} E[\text{dyn } \tau' \text{BndryErr}]$

10374 **ELSE** $e' = E'[e'']$ and $e'' \triangleright_{\text{D-C}} \text{TagErr} :$

10375 a. $E' \in E^\bullet$

10376 by e' is boundary-free

10377 b. QED

10378 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :

10379 1. e' is a value

10380 $\vee e' \in \text{Err}$

10381 $\vee e' \rightarrow_{\text{C-S}} e''$

10382 $\vee e' \rightarrow_{\text{C-S}} \text{BndryErr}$

10383 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{\text{D-C}} \text{TagErr}$

10384 by *static progress*

10385 2. **IF** e' is a value :

10386 a. QED $e \rightarrow_{\text{C-S}} E[\mathcal{S}_{\text{C}}(\tau', e')]$

10387 **IF** $e' \in \text{Err} :$

10388 a. QED $e \rightarrow_{\text{C-S}} e'$

10389 **IF** $e' \rightarrow_{\text{C-S}} e'' :$

10390 a. QED $e \rightarrow_{\text{C-S}} E[\text{stat } \tau' e'']$

10391 **IF** $e' \rightarrow_{\text{C-S}} \text{BndryErr} :$

10392 a. QED $e \rightarrow_{\text{C-S}} E[\text{stat } \tau' \text{BndryErr}]$

10393

10394

10395

ELSE $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{\text{D-C}} \text{TagErr}$

10396

10397

10398 a. Contradiction by e' is boundary-free

10399 **CASE** $e = E[\text{Err}] :$

10400 1. QED $e \rightarrow_{\text{C-S}} \text{Err}$

10401

10402

Lemma 5.8 : HC *dynamic progress*

10403 If $\vdash_{\text{C}} e$ then one of the following holds:

10404 • e is a value

10405 • $e \in \text{Err}$

10406 • $e \rightarrow_{\text{C-D}} e'$

10407 • $e \rightarrow_{\text{C-D}} \text{BndryErr}$

10408 • $e \rightarrow_{\text{C-D}} \text{TagErr}$

10409 *Proof:*

10410 By the *boundary factoring* lemma, there are seven cases.

10411 **CASE** e is a value :

10412 1. QED

10413 **CASE** $e = E^\bullet[v_0 v_1] :$

10414 **IF** $v_0 = \lambda x. e' :$

10415 1. $e \rightarrow_{\text{C-D}} E^\bullet[e'[x \leftarrow v_1]]$

10416 by $v_0 v_1 \triangleright_{\text{D-C}} e'[x \leftarrow v_1]$

10417 2. QED

10418 **IF** $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f :$

10419 1. $e \rightarrow_{\text{C-D}} E^\bullet[\text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))]$

10420 by $v_0 v_1 \triangleright_{\text{D-C}} \text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))$

10421 2. QED

10422 **ELSE** $v_0 = i$

10423 $\vee v_0 = \langle v, v' \rangle :$

10424 1. $e \rightarrow_{\text{C-D}} \text{TagErr}$

10425 by $(v_0 v_1) \triangleright_{\text{D-C}} \text{TagErr}$

10426 2. QED

10427 **CASE** $e = E^\bullet[\text{op}^1 v] :$

10428 **IF** $v = \text{mon}(\tau_0 \times \tau_1) v'$

10429 $\wedge \text{op}^1 = \text{fst} :$

10430 1. $e \rightarrow_{\text{C-D}} E^\bullet[\text{stat } \tau_0 \text{op}^1 v']$

10431 by $\text{op}^1 v \triangleright_{\text{D-C}} \text{stat } \tau_0 \text{op}^1 v'$

10432 2. QED

10433 **IF** $v = \text{mon}(\tau_0 \times \tau_1) v'$

10434 $\wedge \text{op}^1 = \text{snd} :$

10435 1. $e \rightarrow_{\text{C-D}} E^\bullet[\text{stat } \tau_1 \text{op}^1 v']$

10436 by $\text{op}^1 v \triangleright_{\text{D-C}} \text{stat } \tau_1 \text{op}^1 v'$

10437 2. QED

10438 **IF** $\delta(\text{op}^1, v) = e' :$

10439 1. $(\text{op}^1 v) \triangleright_{\text{D-C}} e'$

10440 2. QED

10441 **ELSE** $\delta(\text{op}^1, v)$ is undefined :

10442 1. $e \rightarrow_{\text{C-D}} \text{TagErr}$

10443 by $(\text{op}^1 v) \triangleright_{\text{D-C}} \text{TagErr}$

10444 2. QED

10445 **CASE** $e = E^\bullet[\text{op}^2 v_0 v_1] :$

10446 **IF** $\delta(\text{op}^2, v_0, v_1) = e'' :$

10447 1. $\text{op}^2 v_0 v_1 \triangleright_{\text{D-C}} e''$

10448 2. QED

10449 **ELSE** $\delta(\text{op}^2, v_0, v_1)$ is undefined :

10450

10451	1. $e \rightarrow_{C-D} \text{TagErr}$	1. $\vdash_C v_0 v_1 : \tau'$	10506
10452	by $op^2 v_0 v_1 \triangleright_{D-C} \text{TagErr}$	by <i>static hole typing</i>	10507
10453	2. QED	2. $\vdash_C v_0 : \tau_d \Rightarrow \tau_c$	10508
10454	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	$\wedge \vdash_C v_1 : \tau_d$	10509
10455	1. e' is a value	$\wedge \tau_c \leq \tau'$	10510
10456	$\vee e' \in \text{Err}$	by <i>inversion</i>	10511
10457	$\vee e' \rightarrow_{C-D} e''$	3. $\tau_d \leq \tau_x$	10512
10458	$\vee e' \rightarrow_{C-D} \text{BndryErr}$	by <i>canonical forms</i> (2)	10513
10459	$\vee e' = E[e'']$ and $e'' \triangleright_{D-C} \text{TagErr}$	4. $(x : \tau_x) \vdash_C e' : \tau_c$	10514
10460	by <i>dynamic progress</i>	by <i>inversion</i> (2)	10515
10461	2. IF e' is a value :	5. $\vdash_C v_1 : \tau_x$	10516
10462	a. QED $e \rightarrow_{C-D} E[\mathcal{D}_C(\tau', e')]$	by (2, 3)	10517
10463	IF $e' \in \text{Err}$:	6. $\vdash_C e'[x \leftarrow v_1] : \tau_c$	10518
10464	a. QED $e \rightarrow_{C-D} e'$	by <i>substitution</i> (4, 5)	10519
10465	IF $e' \rightarrow_{C-D} e''$:	7. $\vdash_C e'[x \leftarrow v_1] : \tau'$	10520
10466	a. QED $e \rightarrow_{C-S} E[\text{dyn } \tau' e'']$	by (2, 6)	10521
10467	IF $e' \rightarrow_{C-D} \text{BndryErr}$:	8. QED by <i>hole substitution</i> (7)	10522
10468	a. QED $e \rightarrow_{C-D} E[\text{dyn } \tau' \text{BndryErr}]$	ELSE $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f$	10523
10469	ELSE $e' = E[e'']$ and $e'' \triangleright_{D-C} \text{TagErr}$:	$\wedge e \rightarrow_{C-S} E^*[\text{dyn } \tau_c (v_f (\text{stat } \tau_d v_1))]$:	10524
10470	a. $E \in E^\bullet$	1. $\vdash_C v_0 v_1 : \tau'$	10525
10471	by e' is boundary-free	by <i>static hole typing</i>	10526
10472	b. QED	2. $\vdash_C v_0 : \tau'_d \Rightarrow \tau'_c$	10527
10473	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	$\wedge \vdash_C v_1 : \tau'_d$	10528
10474	1. e' is a value	$\wedge \tau'_c \leq \tau'$	10529
10475	$\vee e' \in \text{Err}$	by <i>inversion</i>	10530
10476	$\vee e' \rightarrow_{C-S} e''$	3. $\vdash_C v_f$	10531
10477	$\vee e' \rightarrow_{C-S} \text{BndryErr}$	by <i>inversion</i> (2)	10532
10478	$\vee e' = E''[\text{dyn } \tau'' E^*''[e'']]$ and $e'' \triangleright_{D-C} \text{TagErr}$	4. $\tau_d \Rightarrow \tau_c \leq \tau'_d \Rightarrow \tau'_c$	10533
10479	by <i>static progress</i>	by <i>canonical forms</i> (2)	10534
10480	2. IF e' is a value :	5. $\tau'_d \leq \tau_d$	10535
10481	a. QED $e \rightarrow_{C-S} E[\mathcal{S}_C(\tau', e')]$	$\wedge \tau_c \leq \tau'_c$	10536
10482	IF $e' \in \text{Err}$:	by (4)	10537
10483	a. QED $e \rightarrow_{C-S} e'$	6. $\vdash_C v_1 : \tau_d$	10538
10484	IF $e' \rightarrow_{C-S} e''$:	by (2, 5)	10539
10485	a. QED $e \rightarrow_{C-S} E[\text{stat } \tau' e'']$	7. $\vdash_C \text{stat } \tau_d v_1$	10540
10486	IF $e' \rightarrow_{C-S} \text{BndryErr}$:	by (6)	10541
10487	a. QED $e \rightarrow_{C-S} E[\text{stat } \tau' \text{BndryErr}]$	8. $\vdash_C v_f (\text{stat } \tau_d v_1)$	10542
10488	ELSE $e' = E''[\text{dyn } \tau'' E^*''[e'']]$ and $e'' \triangleright_{D-C} \text{TagErr}$	by (3, 7)	10543
10489	:	9. $\vdash_C \text{dyn } \tau_c (v_f (\text{stat } \tau_d v_1)) : \tau_c$	10544
10490	a. Contradiction by e' is boundary-free	by (8)	10545
10491	CASE $e = E[\text{Err}]$:	10. $\vdash_C \text{dyn } \tau_c (v_f (\text{stat } \tau_d v_1)) : \tau'$	10546
10492	1. QED $e \rightarrow_{C-D} \text{Err}$	by (2, 5, 9)	10547
10493	□	11. QED by <i>hole substitution</i> (10)	10548
10494	Lemma 5.9 : HC <i>static preservation</i>	CASE $e = E^*[op^1 v]$:	10549
10495	▮ If $\vdash_C e : \tau$ and $e \rightarrow_{C-S} e'$ then $\vdash_C e' : \tau$	IF $v = \text{mon}(\tau_0 \times \tau_1) v'$	10550
10496	<i>Proof</i> :	$\wedge op^1 = \text{fst}$	10551
10497	By the <i>boundary factoring</i> lemma there are seven cases.	$\wedge e \rightarrow_{C-S} E^*[\text{dyn } \tau_0 (\text{fst } v')]$:	10552
10498	CASE e is a value :	1. $\vdash_C \text{fst } v : \tau'$	10553
10499	1. Contradiction by $e \rightarrow_{C-S} e'$	by <i>static hole typing</i>	10554
10500	CASE $e = E^*[v_0 v_1]$:	2. $\vdash_C v : \tau'_0 \times \tau'_1$	10555
10501	IF $v_0 = \lambda(x : \tau_x). e'$	$\wedge \tau'_0 < \tau'$	10556
10502	$\wedge e \rightarrow_{C-S} E^*[e'[x \leftarrow v_1]]$:	by <i>inversion</i>	10557
10503		3. $\vdash_C v'$	10558
10504		by <i>inversion</i> (2)	10559
10505			10560

10561	4. $\tau_0 \times \tau_1 \leq: \tau'_0 \times \tau'_1$	4. $\vdash_C v_1 : \tau'$	10616
10562	by <i>canonical forms</i> (2)	by (2, 3)	10617
10563	5. $\tau_0 \leq: \tau'_0$	5. QED by <i>hole substitution</i> (4)	10618
10564	6. $\vdash_C \text{fst } v'$	CASE $e = E^\bullet[op^2 v_0 v_1] :$	10619
10565	by (3)	1. $e \rightarrow_{C-S} E^\bullet[\delta(op^2, v_0, v_1)]$	10620
10566	7. $\vdash_C \text{dyn } \tau_0 (\text{fst } v') : \tau_0$	by $e \rightarrow_{C-S} e'$	10621
10567	by (6)	2. $\vdash_C op^2 v_0 v_1 : \tau'$	10622
10568	8. $\vdash_C \text{dyn } \tau_0 (\text{fst } v') : \tau'$	by <i>static hole typing</i>	10623
10569	by (2, 5, 7)	3. $\vdash_C v_0 : \tau_0$	10624
10570	9. QED by <i>hole substitution</i>	$\wedge \vdash_C v_1 : \tau_1$	10625
10571	IF $v = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	$\wedge \Delta(op^2, \tau_0, \tau_1) = \tau''$	10626
10572	$\wedge op^1 = \text{snd}$	$\wedge \tau'' \leq: \tau'$	10627
10573	$\wedge e \rightarrow_{C-S} E^\bullet[\text{dyn } \tau_0 (\text{snd } v')]$	by <i>inversion</i> (1)	10628
10574	1. $\vdash_C \text{snd } v : \tau'$	4. $\vdash_C \delta(op^2, v_0, v_1) : \tau''$	10629
10575	by <i>static hole typing</i>	by Δ <i>type soundness</i> (2)	10630
10576	2. $\vdash_C v : \tau'_0 \times \tau'_1$	5. $\vdash_C \delta(op^2, v_0, v_1) : \tau'$	10631
10577	$\wedge \tau'_1 <: \tau'$	by (2, 3)	10632
10578	by <i>inversion</i>	6. QED by <i>hole substitution</i> (4)	10633
10579	3. $\vdash_C v'$	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	10634
10580	by <i>inversion</i> (2)	IF e' is a value :	10635
10581	4. $\tau_0 \times \tau_1 \leq: \tau'_0 \times \tau'_1$	1. $e \rightarrow_{C-S} E[\mathcal{D}_C(\tau', e')]$	10636
10582	by <i>canonical forms</i> (2)	2. $\vdash_C \text{dyn } \tau' e' : \tau'$	10637
10583	5. $\tau_1 \leq: \tau'_1$	by <i>boundary hole typing</i>	10638
10584	6. $\vdash_C \text{snd } v'$	3. $\vdash_C e'$	10639
10585	by (3)	by <i>inversion</i> (2)	10640
10586	7. $\vdash_C \text{dyn } \tau_0 (\text{snd } v') : \tau_0$	4. $\vdash_C \mathcal{D}_C(\tau', e') : \tau'$	10641
10587	by (5)	by \mathcal{D}_C <i>soundness</i> (3)	10642
10588	8. $\vdash_C \text{dyn } \tau_0 (\text{snd } v') : \tau'$	5. QED by <i>hole substitution</i> (4)	10643
10589	by (2, 5, 7)	ELSE $e' \rightarrow_{C-D} e'' :$	10644
10590	9. QED by <i>hole substitution</i>	1. $e \rightarrow_{C-S} E[\text{dyn } \tau' e'']$	10645
10591	IF $v = \langle v_0, v_1 \rangle$	2. $\vdash_C \text{dyn } \tau' e' : \tau'$	10646
10592	$\wedge op^1 = \text{fst}$	by <i>boundary hole typing</i>	10647
10593	$\wedge e \rightarrow_{C-S} E^\bullet[v_0] :$	3. $\vdash_C e'$	10648
10594	1. $\vdash_C \text{fst } \langle v_0, v_1 \rangle : \tau'$	by <i>inversion</i> (2)	10649
10595	by <i>static hole typing</i>	4. $\vdash_C e''$	10650
10596	2. $\vdash_C \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	by <i>dynamic preservation</i> (3)	10651
10597	$\wedge \tau_0 \leq: \tau'$	5. $\vdash_C \text{dyn } \tau' e'' : \tau'$	10652
10598	by <i>inversion</i> (1)	by (4)	10653
10599	3. $\vdash_C v_0 : \tau_0$	6. QED by <i>hole substitution</i> (5)	10654
10600	by <i>inversion</i> (2)	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	10655
10601	4. $\vdash_C v_0 : \tau'$	IF e' is a value :	10656
10602	by (2, 3)	1. $e \rightarrow_{C-S} E[\mathcal{S}_C(\tau', e')]$	10657
10603	5. QED by <i>hole substitution</i> (4)	2. $\vdash_C \text{stat } \tau' e'$	10658
10604	ELSE $v = \langle v_0, v_1 \rangle$	by <i>boundary hole typing</i>	10659
10605	$\wedge op^1 = \text{snd}$	3. $\vdash_C e' : \tau'$	10660
10606	$\wedge e \rightarrow_{C-S} E^\bullet[v_1] :$	by <i>inversion</i> (2)	10661
10607	1. $\vdash_C \text{snd } \langle v_0, v_1 \rangle : \tau'$	4. $\vdash_C \mathcal{S}_C(\tau', e')$	10662
10608	by <i>static hole typing</i>	by \mathcal{S}_C <i>soundness</i> (3)	10663
10609	2. $\vdash_C \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	5. QED by <i>hole substitution</i> (4)	10664
10610	$\wedge \tau_1 \leq: \tau'$	ELSE $e' \rightarrow_{C-S} e'' :$	10665
10611	by <i>inversion</i> (1)	1. $e \rightarrow_{C-S} E[\text{stat } \tau' e'']$	10666
10612	3. $\vdash_C v_1 : \tau_1$	2. $\vdash_C \text{stat } \tau' e'$	10667
10613	by <i>inversion</i> (2)	by <i>boundary hole typing</i>	10668
10614			10669
10615			10670

10671	3. $\vdash_C e' : \tau'$	2. $\vdash_C \text{mon}(\tau_0 \times \tau_1) v'$	10726
10672	by <i>inversion</i> (2)	by <i>inversion</i> (1)	10727
10673	4. $\vdash_C e'' : \tau'$	3. $\vdash_C v' : \tau_0 \times \tau_1$	10728
10674	by <i>static preservation</i> (3)	by <i>inversion</i> (2)	10729
10675	5. $\vdash_C \text{stat } \tau' e''$	4. $\vdash_C \text{fst } v' : \tau_0$	10730
10676	by (4)	by (3)	10731
10677	6. QED by <i>hole substitution</i> (5)	5. $\vdash_C \text{stat } \tau_0 (\text{fst } v')$	10732
10678	CASE $e = E[\text{Err}] :$	by (4)	10733
10679	1. $e \rightarrow_{C-S} \text{Err}$	6. QED by <i>hole substitution</i>	10734
10680	2. QED by $\vdash_C \text{Err} : \tau$	IF $v = \text{mon}(\tau_0 \times \tau_1) v'$	10735
10681	□	$\wedge \text{op}^1 = \text{snd}$	10736
10682	Lemma 5.10 : HC dynamic preservation	$\wedge e \rightarrow_{C-D} E[\text{stat } \tau_0 (\text{snd } v')] :$	10737
10683	▮ If $\vdash_C e$ and $e \rightarrow_{C-D} e'$ then $\vdash_C e'$	1. $\vdash_C \text{op}^1 v$	10738
10684	<i>Proof</i> :	by <i>dynamic hole typing</i>	10739
10685	By the <i>boundary factoring</i> lemma, there are seven cases.	2. $\vdash_C \text{mon}(\tau_0 \times \tau_1) v'$	10740
10686	CASE e is a value :	by <i>inversion</i> (1)	10741
10687	1. Contradiction by $e \rightarrow_{C-D} e'$	3. $\vdash_C v' : \tau_0 \times \tau_1$	10742
10688	CASE $e = E^*[v_0 v_1] :$	by <i>inversion</i> (2)	10743
10689	IF $v_0 = \lambda x. e'$	4. $\vdash_C \text{snd } v' : \tau_1$	10744
10690	$\wedge e \rightarrow_{C-D} E^*[e'[x \leftarrow v_1]] :$	by (3)	10745
10691	1. $\vdash_C v_0 v_1$	5. $\vdash_C \text{stat } \tau_1 (\text{snd } v')$	10746
10692	by <i>dynamic hole typing</i>	by (4)	10747
10693	2. $\vdash_C v_0$	6. QED by <i>hole substitution</i>	10748
10694	$\wedge \vdash_C v_1$	IF $v = \langle v_0, v_1 \rangle$	10749
10695	by <i>inversion</i> (1)	$\wedge \text{op}^1 = \text{fst}$	10750
10696	3. $x \vdash_C e'$	$\wedge e \rightarrow_{C-D} E^*[v_0] :$	10751
10697	by <i>inversion</i> (2)	1. $\vdash_C \text{op}^1 v$	10752
10698	4. $\vdash_C e'[x \leftarrow v_1]$	by <i>dynamic hole typing</i>	10753
10699	by <i>substitution</i> (2, 3)	2. $\vdash_C v$	10754
10700	5. QED <i>hole substitution</i> (4)	by <i>inversion</i> (1)	10755
10701	ELSE $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f$	3. $\vdash_C v_0$	10756
10702	$\wedge e \rightarrow_{C-D} E^*[\text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))] :$	by <i>inversion</i> (2)	10757
10703	1. $\vdash_C v_0 v_1$	4. QED by <i>hole substitution</i>	10758
10704	by <i>dynamic hole typing</i>	ELSE $v = \langle v_0, v_1 \rangle$	10759
10705	2. $\vdash_C v_0$	$\wedge \text{op}^1 = \text{snd}$	10760
10706	$\wedge \vdash_C v_1$	$\wedge e \rightarrow_{C-D} E^*[v_1] :$	10761
10707	by <i>inversion</i> (1)	1. $\vdash_C \text{op}^1 v$	10762
10708	3. $\vdash_C v_f : \tau_d \Rightarrow \tau_c$	by <i>dynamic hole typing</i>	10763
10709	by <i>inversion</i> (2)	2. $\vdash_C v$	10764
10710	4. $\vdash_C \text{dyn } \tau_d v_1 : \tau_d$	by <i>inversion</i> (1)	10765
10711	by (2)	3. $\vdash_C v_1$	10766
10712	5. $\vdash_C v_f (\text{dyn } \tau_d v_1) : \tau_c$	by <i>inversion</i> (2)	10767
10713	by (3, 4)	4. QED by <i>hole substitution</i>	10768
10714	6. $\vdash_C \text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))$	CASE $e = E^*[\text{op}^2 v_0 v_1] :$	10769
10715	by (5)	1. $e \rightarrow_{C-D} E^*[\delta(\text{op}^2, v_0, v_1)] :$	10770
10716	7. QED by <i>hole substitution</i>	2. $\vdash_C \text{op}^2 v_0 v_1$	10771
10717	CASE $e = E^*[\text{op}^1 v] :$	by <i>dynamic hole typing</i>	10772
10718	IF $v = \text{mon}(\tau_0 \times \tau_1) v'$	3. $\vdash_C v_0$	10773
10719	$\wedge \text{op}^1 = \text{fst}$	$\wedge \vdash_C v_1$	10774
10720	$\wedge e \rightarrow_{C-D} E[\text{stat } \tau_0 (\text{fst } v')] :$	by <i>inversion</i> (1)	10775
10721	1. $\vdash_C \text{op}^1 v$	4. $\vdash_C \delta(\text{op}^2, v_0, v_1)$	10776
10722	by <i>dynamic hole typing</i>	by δ <i>preservation</i> (2)	10777
10723		5. QED by <i>hole substitution</i> (3)	10778
10724		CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	10779
10725			10780

10781 **IF** e' is a value :

10782 1. $e \rightarrow_{C-D} E[\mathcal{D}_C(\tau', e')]$

10783 2. $\vdash_C \text{dyn } \tau' e' : \tau'$

10784 by *boundary hole typing*

10785 3. $\vdash_C e'$

10786 by *inversion* (2)

10787 4. $\vdash_C \mathcal{D}_C(\tau', e') : \tau'$

10788 by *\mathcal{D}_C soundness* (3)

10789 5. QED by *hole substitution* (4)

10790 **ELSE** $e' \rightarrow_{C-D} e''$:

10791 1. $e \rightarrow_{C-D} E[\text{dyn } \tau' e'']$

10792 2. $\vdash_C \text{dyn } \tau' e' : \tau'$

10793 by *boundary hole typing*

10794 3. $\vdash_C e'$

10795 $\wedge \tau' \leq \tau''$

10796 by *inversion* (2)

10797 4. $\vdash_C e''$

10798 by *dynamic preservation* (3)

10799 5. $\vdash_C \text{dyn } \tau' e'' : \tau'$

10800 by (4)

10801 6. QED by *hole substitution* (5)

10802 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :

10803 **IF** $e' \in v$:

10804 1. $e \rightarrow_{C-D} E[\mathcal{S}_C(\tau', e')]$

10805 2. $\vdash_C \text{stat } \tau' e'$

10806 by *boundary hole typing*

10807 3. $\vdash_C e' : \tau'$

10808 by *inversion* (2)

10809 4. $\vdash_C \mathcal{S}_C(\tau', e')$

10810 by *\mathcal{S}_C soundness* (3)

10811 5. QED by *hole substitution* (5)

10812 **ELSE** $e' \rightarrow_{C-S} e''$:

10813 1. $e \rightarrow_{C-D} E[\text{stat } \tau' e'']$

10814 2. $\vdash_C \text{stat } \tau' e'$

10815 by *boundary hole typing*

10816 3. $\vdash_C e' : \tau'$

10817 by *inversion* (2)

10818 4. $\vdash_C e'' : \tau'$

10819 by *static preservation* (3)

10820 5. $\vdash_C \text{stat } \tau' e''$

10821 by (4)

10822 6. QED by *hole substitution* (5)

10823 **CASE** $e = E[\text{Err}]$:

10824 1. $e \rightarrow_{C-D} \text{Err}$

10825 2. QED $\vdash_C \text{Err}$

10826 \square

10827 **Lemma 5.11** : HC *static boundary factoring*

10828

10829

10830

10831

10832

10833

10834

10835

If $\vdash_C e : \tau$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[\text{op}^1 v]$
- $e = E^\bullet[\text{op}^2 v_0 v_1]$
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:

By the *boundary factoring* lemma for the higher-order embedding. (The only difference is the meaning of e is a value.)

\square

Lemma 5.12 : HC *dynamic boundary factoring*

If $\vdash_C e$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[\text{op}^1 v]$
- $e = E^\bullet[\text{op}^2 v_0 v_1]$
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:

By the *boundary factoring* lemma for the higher-order embedding.

\square

Lemma 5.13 : HC *static hole typing*

If $\vdash_C E^\bullet[e] : \tau$ then the derivation contains a sub-term $\vdash_C e : \tau'$

Proof (sketch): Similar to the *static hole typing* lemma for the higher-order embedding. \square

Lemma 5.14 : HC *dynamic hole typing*

If $\vdash_C E^\bullet[e]$ then the derivation contains a sub-term $\vdash_C e$

Proof (sketch): Similar to the *static hole typing* lemma for the higher-order embedding. \square

Lemma 5.15 : HC *boundary hole typing*

• If $\vdash_C E[\text{dyn } \tau e] : \tau'$ then the derivation contains a sub-term

$\vdash_C \text{dyn } \tau e : \tau$

• If $\vdash_C E[\text{dyn } \tau e]$ then the derivation contains a sub-term

$\vdash_C \text{dyn } \tau e : \tau$

• If $\vdash_C E[\text{stat } \tau e] : \tau'$ then the derivation contains a sub-term

$\vdash_C \text{stat } \tau e$

• If $\vdash_C E[\text{stat } \tau e]$ then the derivation contains a sub-term

$\vdash_C \text{stat } \tau e$

Proof (sketch): Similar to the proof for the higher-order *boundary hole typing* lemma. \square

Lemma 5.16 : HC *hole substitution*

• If $\vdash_C E[e]$ and the derivation contains a sub-term $\vdash_C e : \tau'$ and $\vdash_C e' : \tau'$ then $\vdash_C E[e']$.

• If $\vdash_C E[e]$ and the derivation contains a sub-term $\vdash_C e$ and $\vdash_C e'$ then $\vdash_C E[e']$.

• If $\vdash_C E[e] : \tau$ and the derivation contains a sub-term $\vdash_C e : \tau'$ and $\vdash_C e' : \tau'$ then $\vdash_C E[e'] : \tau$.

• If $\vdash_C E[e] : \tau$ and the derivation contains a sub-term $\vdash_C e$ and $\vdash_C e'$ then $\vdash_C E[e'] : \tau$.

10891 *Proof (sketch):* Similar to the proof of the higher-order *hole*
 10892 *substitution* lemma, just replacing \vdash_H with \vdash_C . \square

10893 **Lemma 5.17 :** \vdash_C *static inversion*

- 10894 • If $\Gamma \vdash_C x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$
- 10895 • If $\Gamma \vdash_C \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash_C e' : \tau'_c$ and
 10896 $\tau'_d \Rightarrow \tau'_c \leq \tau$
- 10897 • If $\Gamma \vdash_C \langle e_0, e_1 \rangle : \tau_0 \times \tau_1$ then $\Gamma \vdash_C e_0 : \tau'_0$ and $\Gamma \vdash_C e_1 : \tau'_1$ and
 10898 $\tau'_0 \leq \tau_0$ and $\tau'_1 \leq \tau_1$
- 10899 • If $\Gamma \vdash_C e_0 e_1 : \tau_c$ then $\Gamma \vdash_C e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash_C e_1 : \tau'_d$ and
 10900 $\tau'_c \leq \tau_c$
- 10901 • If $\Gamma \vdash_C \text{fst } e : \tau$ then $\Gamma \vdash_C e : \tau_0 \times \tau_1$ and $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$
 10902 and $\tau_0 \leq \tau$
- 10903 • If $\Gamma \vdash_C \text{snd } e : \tau$ then $\Gamma \vdash_C e : \tau_0 \times \tau_1$ and $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$
 10904 and $\tau_1 \leq \tau$
- 10905 • If $\Gamma \vdash_C \text{op}^2 e_0 e_1 : \tau$ then $\Gamma \vdash_C e_0 : \tau_0$ and $\Gamma \vdash_C e_1 : \tau_1$ and
 10906 $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$
- 10907 • If $\Gamma \vdash_C \text{mon } \tau'_0 \times \tau'_1 v' : \tau_0 \times \tau_1$ then $\Gamma \vdash_C v'$ and $\tau'_0 \times \tau'_1 \leq \tau_0 \times \tau_1$
- 10908 • If $\Gamma \vdash_C \text{mon } \tau'_d \Rightarrow \tau'_c v' : \tau_d \Rightarrow \tau_c$ then $\Gamma \vdash_C v'$ and $\tau'_d \Rightarrow \tau'_c \leq$
 10909 $\tau_d \Rightarrow \tau_c$
- 10910 • If $\Gamma \vdash_C \text{dyn } \tau' e' : \tau$ then $\Gamma \vdash_C e'$ and $\tau' \leq \tau$

10911 *Proof:*

10912 QED by the definition of $\Gamma \vdash_C e : \tau$

10913 \square

10914 **Lemma 5.18 :** \vdash_C *dynamic inversion*

- 10915 • If $\Gamma \vdash_C x$ then $x \in \Gamma$
- 10916 • If $\Gamma \vdash_C \lambda x. e'$ then $x, \Gamma \vdash_C e'$
- 10917 • If $\Gamma \vdash_C \langle e_0, e_1 \rangle$ then $\Gamma \vdash_C e_0$ and $\Gamma \vdash_C e_1$
- 10918 • If $\Gamma \vdash_C e_0 e_1$ then $\Gamma \vdash_C e_0$ and $\Gamma \vdash_C e_1$
- 10919 • If $\Gamma \vdash_C \text{op}^1 e_0$ then $\Gamma \vdash_C e_0$
- 10920 • If $\Gamma \vdash_C \text{op}^2 e_0 e_1$ then $\Gamma \vdash_C e_0$ and $\Gamma \vdash_C e_1$
- 10921 • If $\Gamma \vdash_C \text{mon } \tau_d \Rightarrow \tau_c v'$ then $\Gamma \vdash_C v' : \tau_d \Rightarrow \tau_c$
- 10922 • If $\Gamma \vdash_C \text{mon } \tau_0 \times \tau_1 v'$ then $\Gamma \vdash_C v' : \tau_0 \times \tau_1$
- 10923 • If $\Gamma \vdash_C \text{stat } \tau' e'$ then $\Gamma \vdash_C e' : \tau'$

10924 *Proof:*

10925 QED by the definition of $\Gamma \vdash_C e$

10926 \square

10927 **Lemma 5.19 :** HC *canonical forms*

- 10928 • If $\vdash_C v : \tau_0 \times \tau_1$ then either:
 10929 - $v = \langle v_0, v_1 \rangle$
 10930 - or $v = \text{mon } (\tau'_0 \times \tau'_1) v'$
 10931 $\wedge \tau'_0 \times \tau'_1 \leq \tau_0 \times \tau_1$
- 10932 • If $\vdash_C v : \tau_d \Rightarrow \tau_c$ then either:
 10933 - $v = \lambda(x : \tau_x). e'$
 10934 $\wedge \tau_d \leq \tau_x$
 10935 - or $v = \text{mon } (\tau'_d \Rightarrow \tau'_c) v'$
 10936 $\wedge \tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- 10937 • If $\vdash_C v : \text{Int}$ then $v = i$
- 10938 • If $\vdash_C v : \text{Nat}$ then $v = i$ and $v \in \mathbb{N}$

10939 *Proof:*

10940 QED by definition of $\vdash_C e : \tau$

10941 \square

10942 **Lemma 5.20 :** Δ *type soundness*

10943

10944

10945

If $\vdash_C v_0 : \tau_0$ and $\vdash_C v_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau$ then one of the following holds:

- $\delta(\text{op}^2, v_0, v_1) = v$ and $\vdash_C v : \tau$, or
- $\delta(\text{op}^2, v_0, v_1) = \text{BndryErr}$

Proof (sketch): Similar to the proof for the higher-order Δ *type soundness* lemma. \square

Lemma 5.21 : δ *preservation*

- If $\vdash_C v$ and $\delta(\text{op}^1, v) = v'$ then $\vdash_C v'$
- If $\vdash_C v_0$ and $\vdash_C v_1$ and $\delta(\text{op}^2, v_0, v_1) = v'$ then $\vdash_C v'$

Proof (sketch): Similar to the proof for the higher-order δ *preservation* lemma. \square

Lemma 5.22 : HC *substitution*

- If $(x : \tau_x), \Gamma \vdash_C e$ and $\vdash_C v : \tau_x$ then $\Gamma \vdash_C e[x \leftarrow v]$
- If $x, \Gamma \vdash_C e$ and $\vdash_C v$ then $\Gamma \vdash_C e[x \leftarrow v]$
- If $(x : \tau_x), \Gamma \vdash_C e : \tau$ and $\vdash_C v : \tau_x$ then $\Gamma \vdash_C e[x \leftarrow v] : \tau$
- If $x, \Gamma \vdash_C e : \tau$ and $\vdash_C v$ then $\Gamma \vdash_C e[x \leftarrow v] : \tau$

Proof (sketch): Similar to the proof for the higher-order *substitution* lemma. \square

Lemma 5.23 : *weakening*

- If $\Gamma \vdash_C e$ then $x, \Gamma \vdash_C e$
- If $\Gamma \vdash_C e : \tau$ then $(x : \tau'), \Gamma \vdash_C e : \tau$

Proof:

QED because e is closed under Γ

\square

E.6 (HF) Forgetful Embedding

E.6.1 Forgetful Definitions

Language HF

$e = x \mid v \mid \langle e, e \rangle \mid e e \mid op^1 e \mid op^2 e e \mid$
 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err} \mid \text{chk } \tau e$
 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e \mid$
 $\text{mon}(\tau \Rightarrow \tau)(\lambda x. e) \mid \text{mon}(\tau \Rightarrow \tau)(\lambda(x:\tau). e) \mid$
 $\text{mon}(\tau \times \tau) \langle v, v \rangle$
 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$
 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$
 $r = v \mid \text{Err}$
 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet$
 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E$

 $\Delta : op^1 \times \tau \longrightarrow \tau$ $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$ $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$ $\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$ $\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$ $\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$ $\tau \leqslant: \tau$

$$\frac{}{\text{Nat} \leqslant: \text{Int}} \quad \frac{\tau'_d \leqslant: \tau_d \quad \tau_c \leqslant: \tau'_c \quad \tau_0 \leqslant: \tau'_0 \quad \tau_1 \leqslant: \tau'_1}{\tau_d \Rightarrow \tau_c \leqslant: \tau'_d \Rightarrow \tau'_c} \quad \frac{}{\tau_0 \times \tau_1 \leqslant: \tau'_0 \times \tau'_1}$$

$$\frac{}{\tau \leqslant: \tau} \quad \frac{\tau \leqslant: \tau' \quad \tau' \leqslant: \tau''}{\tau \leqslant: \tau''}$$
 $\Gamma \vdash e$

$$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$$

$$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$$

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$$
 $\Gamma \vdash e : \tau$

$$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$$

$$\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$$

$$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant: \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$$

$$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$$
 $\Gamma \Vdash e$

$$\frac{x \in \Gamma}{\Gamma \Vdash x} \quad \frac{x, \Gamma \Vdash e}{\Gamma \Vdash \lambda x. e} \quad \frac{}{\Gamma \Vdash i} \quad \frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash \langle e_0, e_1 \rangle}$$

$$\frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash e_0 e_1} \quad \frac{\Gamma \Vdash e}{\Gamma \Vdash op^1 e} \quad \frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \Vdash \text{Err}}$$

$$\frac{\Gamma \Vdash e : \tau}{\Gamma \Vdash \text{stat } \tau e} \quad \frac{\Gamma \Vdash v_0 : \tau'_0 \quad \Gamma \Vdash v_1 : \tau'_1}{\Gamma \Vdash \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle}$$

$$\frac{\Gamma \Vdash v_0 \quad \Gamma \Vdash v_1}{\Gamma \Vdash \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle} \quad \frac{\Gamma \Vdash \lambda x. e}{\Gamma \Vdash \text{mon}(\tau_d \Rightarrow \tau_c) \lambda x. e}$$

$$\frac{\Gamma \Vdash \lambda(x:\tau'_d). e : \tau'_d \Rightarrow \tau'_c}{\Gamma \Vdash \text{mon}(\tau_d \Rightarrow \tau_c) \lambda(x:\tau'_d). e}$$

11111	$\Gamma \vdash_{\mathbb{F}} e : \tau$
11112	$(x:\tau) \in \Gamma$
11113	$(x:\tau_d), \Gamma \vdash_{\mathbb{F}} e : \tau_c$
11114	$i \in \mathbb{N}$
11115	$\Gamma \vdash_{\mathbb{F}} x : \tau$
11116	$\Gamma \vdash_{\mathbb{F}} \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c$
11117	$\Gamma \vdash_{\mathbb{F}} i : \text{Nat}$
11118	$\Gamma \vdash_{\mathbb{F}} i : \text{Int}$
11119	$\Gamma \vdash_{\mathbb{F}} \langle e_0, e_1 \rangle : \tau_0 \times \tau_1$
11120	$\Gamma \vdash_{\mathbb{F}} e_0 e_1 : \tau_c$
11121	$\Gamma \vdash_{\mathbb{F}} e_0 : \tau_0$
11122	$\Gamma \vdash_{\mathbb{F}} e_1 : \tau_1$
11123	$\Gamma \vdash_{\mathbb{F}} e : \tau'$
11124	$\Delta(\text{op}^1, \tau_0) = \tau$
11125	$\Delta(\text{op}^2, \tau_0, \tau_1) = \tau$
11126	$\tau' <: \tau$
11127	$\Gamma \vdash_{\mathbb{F}} \text{op}^1 e_0 : \tau$
11128	$\Gamma \vdash_{\mathbb{F}} \text{op}^2 e_0 e_1 : \tau$
11129	$\Gamma \vdash_{\mathbb{F}} e : \tau$
11130	$\Gamma \vdash_{\mathbb{F}} \text{Err} : \tau$
11131	$\Gamma \vdash_{\mathbb{F}} \text{dyn } \tau e : \tau$
11132	$\Gamma \vdash_{\mathbb{F}} v_0 : \tau'_0$
11133	$\Gamma \vdash_{\mathbb{F}} v_1 : \tau'_1$
11134	$\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : (\tau_0 \times \tau_1)$
11135	$\Gamma \vdash_{\mathbb{F}} v_0$
11136	$\Gamma \vdash_{\mathbb{F}} v_1$
11137	$\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : (\tau_0 \times \tau_1)$
11138	$\Gamma \vdash_{\mathbb{F}} \lambda x. e$
11139	$\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) \lambda x. e : (\tau_d \Rightarrow \tau_c)$
11140	$\Gamma \vdash_{\mathbb{F}} \lambda(x:\tau'_d). e : \tau'_d \Rightarrow \tau'_c$
11141	$\Gamma \vdash_{\mathbb{F}} e : \tau'$
11142	$\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) \lambda(x:\tau'_d). e : (\tau_d \Rightarrow \tau_c)$
11143	$\Gamma \vdash_{\mathbb{F}} \text{chk } \tau e : \tau$
11144	$\delta(\text{op}^1, v) = e$
11145	$\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$
11146	$\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$
11147	$\delta(\text{op}^2, v, v) = e$
11148	$\delta(\text{sum}, i_0, i_1) = i_0 + i_1$
11149	$\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$
11150	$\delta(\text{quotient}, i_0, i_1) = \lfloor i_0 / i_1 \rfloor$
11151	if $i_1 \neq 0$
11152	$\mathcal{D}_{\mathbb{F}} : \tau \times v \longrightarrow e$
11153	$\mathcal{D}_{\mathbb{F}}(\tau, v) = \mathcal{X}(\tau, v)$
11154	$\mathcal{S}_{\mathbb{F}} : \tau \times v \longrightarrow e$
11155	$\mathcal{S}_{\mathbb{F}}(\tau, v) = \mathcal{X}(\tau, v)$

11166	$\mathcal{X} : \tau \times v \longrightarrow e$	
11167	$\mathcal{X}(\tau_d \Rightarrow \tau_c, \lambda x. e)$	$= \text{mon}(\tau_d \Rightarrow \tau_c) (\lambda x. e)$
11168	$\mathcal{X}(\tau_d \Rightarrow \tau_c, \lambda(x:\tau). e)$	$= \text{mon}(\tau_d \Rightarrow \tau_c) (\lambda(x:\tau). e)$
11169	$\mathcal{X}(\tau_d \Rightarrow \tau_c, \text{mon}(\tau'_d \Rightarrow \tau'_c) v')$	$= \text{mon}(\tau_d \Rightarrow \tau_c) v'$
11170	$\mathcal{X}(\tau_0 \times \tau_1, \langle v_0, v_1 \rangle)$	$= \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$
11171	$\mathcal{X}(\tau_0 \times \tau_1, \text{mon}(\tau'_0 \times \tau'_1) v')$	$= \text{mon}(\tau_0 \times \tau_1) v'$
11172	$\mathcal{X}(\text{Int}, i)$	$= i$
11173	$\mathcal{X}(\text{Nat}, i)$	$= i$
11174	if $i \in \mathbb{N}$	$= i$
11175	$\mathcal{X}(\tau, v)$	$= \text{BndryErr}$
11176	otherwise	$= \text{BndryErr}$
11177	$e \triangleright_{S-1} e$	
11178	$\text{dyn } \tau v$	$\triangleright_{S-1} \mathcal{D}_{\mathbb{F}}(\tau, v)$
11179	$\text{chk } \tau v$	$\triangleright_{S-1} \mathcal{X}(\tau, v)$
11180	$(\text{mon}(\tau_d \Rightarrow \tau_c) (\lambda x. e)) v$	$\triangleright_{S-1} \text{dyn } \tau_c e'$
11181	where $e' = (\lambda x. e) (\mathcal{X}(\tau_d, v))$	$\triangleright_{S-1} \text{dyn } \tau_c e'$
11182	$(\text{mon}(\tau_d \Rightarrow \tau_c) (\lambda(x:\tau). e)) v$	$\triangleright_{S-1} \text{chk } \tau_c e'$
11183	where $e' = (\lambda(x:\tau). e) (\mathcal{X}(\tau, v))$	$\triangleright_{S-1} \text{chk } \tau_c e'$
11184	$\text{fst}(\text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle)$	$\triangleright_{S-1} \mathcal{X}(\tau_0, v_0)$
11185	$\text{snd}(\text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle)$	$\triangleright_{S-1} \mathcal{X}(\tau_1, v_1)$
11186	$(\lambda(x:\tau). e) v$	$\triangleright_{S-1} e[x \leftarrow v]$
11187	$\text{op}^1 v$	$\triangleright_{S-1} \delta(\text{op}^1, v)$
11188	$\text{op}^2 v_0 v_1$	$\triangleright_{S-1} \delta(\text{op}^2, v_0, v_1)$
11189	$e \triangleright_{D-1} e$	
11190	$\text{stat } \tau v$	$\triangleright_{D-1} \mathcal{S}_{\mathbb{F}}(\tau, v)$
11191	$v_0 v_1$	$\triangleright_{D-1} \text{TagErr}$
11192	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$	$\triangleright_{D-1} \text{TagErr}$
11193	$(\text{mon}(\tau_d \Rightarrow \tau_c) (\lambda x. e)) v$	$\triangleright_{D-1} (\lambda x. e) v$
11194	$(\text{mon}(\tau_d \Rightarrow \tau_c) (\lambda(x:\tau). e)) v$	$\triangleright_{D-1} \text{stat } \tau_c e'$
11195	where $e' = \text{chk } \tau_c ((\lambda(x:\tau). e) (\mathcal{X}(\tau, v)))$	$\triangleright_{D-1} \text{stat } \tau_c e'$
11196	$(\lambda x. e) v$	$\triangleright_{H-D} e[x \leftarrow v]$
11197	$\text{fst}(\text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle)$	$\triangleright_{D-1} \mathcal{X}(\tau_0, v_0)$
11198	$\text{snd}(\text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle)$	$\triangleright_{D-1} \mathcal{X}(\tau_1, v_1)$
11199	$\text{op}^1 v$	$\triangleright_{H-D} \text{TagErr}$
11200	if $\delta(\text{op}^1, v)$ is undefined	$\triangleright_{H-D} \text{TagErr}$
11201	$\text{op}^1 v$	$\triangleright_{H-D} \delta(\text{op}^1, v)$
11202	$\text{op}^2 v_0 v_1$	$\triangleright_{H-D} \text{TagErr}$
11203	if $\delta(\text{op}^2, v_0, v_1)$ is undefined	$\triangleright_{H-D} \text{TagErr}$
11204	$\text{op}^2 v_0 v_1$	$\triangleright_{H-D} \delta(\text{op}^2, v_0, v_1)$
11205	$e \rightarrow_{F-S} e$	
11206	$E^*[e]$	$\rightarrow_{F-S} E^*[e']$
11207	if $e \triangleright_{S-1} e'$	$\rightarrow_{F-S} E^*[e']$
11208	$E[\text{stat } \tau E^*[e]]$	$\rightarrow_{F-S} E[\text{stat } \tau E^*[e']]$
11209	if $e \triangleright_{S-1} e'$	$\rightarrow_{F-S} E[\text{stat } \tau E^*[e']]$
11210	$E[\text{dyn } \tau E^*[e]]$	$\rightarrow_{F-S} E[\text{dyn } \tau E^*[e']]$
11211	if $e \triangleright_{D-1} e'$	$\rightarrow_{F-S} E[\text{dyn } \tau E^*[e']]$
11212	$E[\text{Err}]$	$\rightarrow_{F-S} \text{Err}$
11213	if $e \triangleright_{D-1} e'$	$\rightarrow_{F-S} \text{Err}$
11214	$E[\text{Err}]$	$\rightarrow_{F-S} \text{Err}$
11215	$E[\text{Err}]$	$\rightarrow_{F-S} \text{Err}$
11216	$E[\text{Err}]$	$\rightarrow_{F-S} \text{Err}$
11217	$E[\text{Err}]$	$\rightarrow_{F-S} \text{Err}$
11218	$E[\text{Err}]$	$\rightarrow_{F-S} \text{Err}$
11219	$E[\text{Err}]$	$\rightarrow_{F-S} \text{Err}$
11220	$E[\text{Err}]$	$\rightarrow_{F-S} \text{Err}$

11221	$e \rightarrow_{F-D} e$	11276
11222	$E^*[e] \rightarrow_{F-D} E^*[e']$	11277
11223	if $e \triangleright_{D-1} e'$	11278
11224	$E[\text{stat } \tau E^*[e]] \rightarrow_{F-D} E[\text{stat } \tau E^*[e']]$	11279
11225	if $e \triangleright_{S-1} e'$	11280
11226	$E[\text{dyn } \tau E^*[e]] \rightarrow_{F-D} E[\text{dyn } \tau E^*[e']]$	11281
11227	if $e \triangleright_{D-1} e'$	11282
11228	$E[\text{Err}] \rightarrow_{F-D} \text{Err}$	11283
11229	$e \rightarrow_{F-S}^* e$ reflexive, transitive closure of \rightarrow_{F-S}	11284
11230		11285
11231	$e \rightarrow_{F-D}^* e$ reflexive, transitive closure of \rightarrow_{F-D}	11286
11232		11287
11233		11288
11234		11289
11235		11290
11236		11291
11237		11292
11238		11293
11239		11294
11240		11295
11241		11296
11242		11297
11243		11298
11244		11299
11245		11300
11246		11301
11247		11302
11248		11303
11249		11304
11250		11305
11251		11306
11252		11307
11253		11308
11254		11309
11255		11310
11256		11311
11257		11312
11258		11313
11259		11314
11260		11315
11261		11316
11262		11317
11263		11318
11264		11319
11265		11320
11266		11321
11267		11322
11268		11323
11269		11324
11270		11325
11271		11326
11272		11327
11273		11328
11274		11329
11275		11330

11331 **E.6.2 Forgetful Theorems**

11332 **Theorem 6.0** : *static HF-soundness*

11333 If $\vdash e : \tau$ then $\vdash_F e : \tau$ and one of the following holds:

- 11334 • $e \rightarrow_{F-S}^* v$ and $\vdash_F v : \tau$
- 11335 • $e \rightarrow_{F-S}^* E[\text{dyn } \tau' e']$ and $e' \triangleright_{D-1} \text{TagErr}$
- 11336 • $e \rightarrow_{F-S}^* \text{BndryErr}$
- 11337 • e diverges

11338 *Proof*:

- 11339 1. $\vdash_F e : \tau$
11340 by *static subset*
- 11341 2. QED by *static progress* and *static preservation*.

11342 □

11343 **Theorem 6.1** : *dynamic HF-soundness*

11344 If $\vdash e$ then $\vdash_F e$ and one of the following holds:

- 11345 • $e \rightarrow_{F-D}^* v$ and $\vdash_F v$
- 11346 • $e \rightarrow_{F-D}^* E[e']$ and $e' \triangleright_{D-1} \text{TagErr}$
- 11347 • $e \rightarrow_{F-D}^* \text{BndryErr}$
- 11348 • e diverges

11349 *Proof*:

- 11350 1. $\vdash_F e$
11351 by *dynamic subset*
- 11352 2. QED by *dynamic progress* and *dynamic preservation*.

11353 □

11354 **Corollary 6.2** : *HF static soundness*

11355 If $\vdash e : \tau$ and e is boundary-free, then one of the following
11356 holds:

- 11357 • $e \rightarrow_{F-S}^* v$ and $\vdash_F v : \tau$
- 11358 • $e \rightarrow_{F-S}^* \text{BndryErr}$
- 11359 • e diverges

11360 *Proof*:

11361 Consequence of the proof for *static HF-soundness*

11362 □

11363

11364

11365

11366

11367

11368

11369

11370

11371

11372

11373

11374

11375

11376

11377

11378

11379

11380

11381

11382

11383

11384

11385

11386

11387

11388

11389

11390

11391

11392

11393

11394

11395

11396

11397

11398

11399

11400

11401

11402

11403

11404

11405

11406

11407

11408

11409

11410

11411

11412

11413

11414

11415

11416

11417

11418

11419

11420

11421

11422

11423

11424

11425

11426

11427

11428

11429

11430

11431

11432

11433

11434

11435

11436

11437

11438

11439

11440

11441 E.6.3 Forgetful Lemmas

11442 Lemma 6.3 : $\mathcal{X}(\cdot, \cdot)$ soundness

11443 If $\Gamma \vdash_{\mathbb{F}} v$ or $\Gamma \vdash_{\mathbb{F}} v : \tau$
 11444 and $\mathcal{X}(\tau', v) = v'$,
 11445 then $\Gamma \vdash_{\mathbb{F}} v'$ and $\Gamma \vdash_{\mathbb{F}} v' : \tau'$

11446 *Proof:*

11447 By case analysis of the definition of $\mathcal{X}(\cdot, \cdot)$.

11448 **CASE** $\mathcal{X}(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

11449 **IF** $v = \lambda x. e$

11450 $\wedge \Gamma \vdash_{\mathbb{F}} v :$

11451 1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v$

11452 by $\Gamma \vdash_{\mathbb{F}} v$

11453 2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v : \tau_d \Rightarrow \tau_c$

11454 by $\Gamma \vdash_{\mathbb{F}} v$

11455 3. QED

11456 **ELSE** $v = \lambda(x : \tau_x). e$

11457 $\wedge \Gamma \vdash_{\mathbb{F}} v : \tau'_d \Rightarrow \tau'_c :$

11458 1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v$

11459 by $\Gamma \vdash_{\mathbb{F}} v : \tau'_d \Rightarrow \tau'_c$

11460 2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v : \tau_d \Rightarrow \tau_c$

11461 by $\Gamma \vdash_{\mathbb{F}} v : \tau'_d \Rightarrow \tau'_c$

11462 3. QED

11463 **CASE** $\mathcal{X}(\tau_d \Rightarrow \tau_c, \text{mon}(\tau'_d \Rightarrow \tau'_c) v') = \text{mon}(\tau_d \Rightarrow \tau_c) v' :$

11464 **IF** $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau'_d \Rightarrow \tau'_c) v' :$

11465 **IF** $v' = \lambda x. e'$

11466 $\wedge \Gamma \vdash_{\mathbb{F}} v' :$

11467 1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v'$

11468 by $\Gamma \vdash_{\mathbb{F}} v'$

11469 2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v' : \tau_d \Rightarrow \tau_c$

11470 by $\Gamma \vdash_{\mathbb{F}} v'$

11471 3. QED

11472 **ELSE** $v' = \lambda(x : \tau_x). e'$

11473 $\wedge \Gamma \vdash_{\mathbb{F}} v' : \tau''_d \Rightarrow \tau''_c :$

11474 1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v'$

11475 by $\Gamma \vdash_{\mathbb{F}} v' : \tau''_d \Rightarrow \tau''_c$

11476 2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v' : \tau_d \Rightarrow \tau_c$

11477 by $\Gamma \vdash_{\mathbb{F}} v' : \tau''_d \Rightarrow \tau''_c$

11478 3. QED

11479 **ELSE** $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau'_d \Rightarrow \tau'_c) v' : \tau'_d \Rightarrow \tau'_c :$

11480 **IF** $v' = \lambda x. e'$

11481 $\wedge \Gamma \vdash_{\mathbb{F}} v' :$

11482 1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v'$

11483 by $\Gamma \vdash_{\mathbb{F}} v'$

11484 2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v' : \tau_d \Rightarrow \tau_c$

11485 by $\Gamma \vdash_{\mathbb{F}} v'$

11486 3. QED

11487 **ELSE** $v' = \lambda(x : \tau_x). e'$

11488 $\wedge \Gamma \vdash_{\mathbb{F}} v' : \tau''_d \Rightarrow \tau''_c :$

11489 1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v'$

11490 by $\Gamma \vdash_{\mathbb{F}} v' : \tau''_d \Rightarrow \tau''_c$

11491 2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_d \Rightarrow \tau_c) v' : \tau_d \Rightarrow \tau_c$

11492 by $\Gamma \vdash_{\mathbb{F}} v' : \tau''_d \Rightarrow \tau''_c$

11493 3. QED

11494

11495

CASE $\mathcal{X}(\tau_0 \times \tau_1, \langle v_0, v_1 \rangle) = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle :$

IF $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle :$

1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$

by $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle$

2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$

by $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle$

3. QED

ELSE $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau'_0 \times \tau'_1 :$

1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$

by $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau'_0 \times \tau'_1$

2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$

by $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau'_0 \times \tau'_1$

3. QED

CASE $\mathcal{X}(\tau_0 \times \tau_1, \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle) = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$

:

IF $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle :$

1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$

by $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle$

2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$

by $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle$

3. QED

ELSE $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau''_0 \times \tau''_1 :$

1. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$

by $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau''_0 \times \tau''_1$

2. $\Gamma \vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$

by $\Gamma \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau''_0 \times \tau''_1$

3. QED

CASE $\mathcal{X}(\text{Int}, i) = i :$

1. $\Gamma \vdash_{\mathbb{F}} i$

2. $\Gamma \vdash_{\mathbb{F}} i : \text{Int}$

3. QED

CASE $\mathcal{X}(\text{Nat}, i) = i :$

1. $\Gamma \vdash_{\mathbb{F}} i$

2. $\Gamma \vdash_{\mathbb{F}} i : \text{Nat}$

by $i \in \mathbb{N}$

3. QED

□

Corollary 6.4 : $\mathcal{D}_{\mathbb{F}}$ soundness

If $\vdash_{\mathbb{F}} v$ then $\vdash_{\mathbb{F}} \mathcal{D}_{\mathbb{F}}(\tau, v) : \tau$

Proof:

QED by \mathcal{X} soundness

□

Corollary 6.5 : $\mathcal{S}_{\mathbb{F}}$ soundness

If $\vdash_{\mathbb{F}} v : \tau$ then $\vdash_{\mathbb{F}} \mathcal{S}_{\mathbb{F}}(\tau, v)$

Proof:

QED by \mathcal{X} soundness

□

Corollary 6.6 : HF static subset

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash_{\mathbb{F}} e : \tau$.

Proof:

Consequence of the proof for the higher-order *static subset* lemma; both $\vdash_{\mathbb{F}}$ and $\vdash_{\mathbb{H}}$ have the same typing rules for surface-language expressions.

11551 \square

 11552 **Corollary 6.7** : HF *dynamic subset*

 11553 If $\Gamma \vdash e$ then $\Gamma \vdash_{\text{F}} e$.

 11554 *Proof*:

 11555 Consequence of the proof for the higher-order *dynamic*
 11556 *subset* lemma.

 11557 \square

 11558 **Lemma 6.8** : HF *static progress*

 11559 If $\vdash_{\text{F}} e : \tau$ then one of the following holds:

- 11560 • e is a value
- 11561 • $e \in \text{Err}$
- 11562 • $e \rightarrow_{\text{F-S}} e'$
- 11563 • $e \rightarrow_{\text{F-S}} \text{BndryErr}$
- 11564 • $e = E[\text{dyn } \tau' e']$ and $e' \rightarrow_{\text{F-D}} \text{TagErr}$

 11565 *Proof*:

 11566 By the *boundary factoring* lemma, there are eight possi-
 11567 ble cases.

 11568 **CASE** e is a value :

- 11569 1. QED

 11570 **CASE** $e = E^*[v_0 v_1]$:

- 11571 1.
- $\vdash_{\text{F}} v_0 v_1 : \tau'$

 11572 by *static hole typing*

- 11573 2.
- $\vdash_{\text{F}} v_0 : \tau_d \Rightarrow \tau_c$

 11574 $\wedge \vdash_{\text{F}} v_1 : \tau_d$

 11575 by *inversion*

- 11576 3.
- $v_0 = \lambda(x : \tau'_d). e'$

 11577 $\vee v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda x. e'$

 11578 $\vee v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda(x : \tau_x). e'$

 11579 by *canonical forms*

- 11580 4.
- IF**
- $v_0 = \lambda(x : \tau'_d). e'$
- :

- 11581 a.
- $e \rightarrow_{\text{F-S}} E^*[e'[x \leftarrow v_1]]$

 11582 by $v_0 v_1 \triangleright_{\text{S-1}} e'[x \leftarrow v_1]$

- 11583 b. QED

 11584 **IF** $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda x. e'$

 11585 $\wedge X(\tau'_d, v_1) = v'_1$:

- 11586 a.
- $e \rightarrow_{\text{F-S}} E^*[\text{dyn } \tau'_c (e'[x \leftarrow v'_1])]$

 11587 by $v_0 v_1 \triangleright_{\text{S-1}} \text{dyn } \tau'_c (e'[x \leftarrow v'_1])$

- 11588 b. QED

 11589 **IF** $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda x. e'$

 11590 $\wedge X(\tau'_d, v_1) = \text{BndryErr}$:

- 11591 a.
- $e \rightarrow_{\text{F-S}} \text{BndryErr}$

 11592 by $v_0 v_1 \triangleright_{\text{S-1}} \text{BndryErr}$

- 11593 b. QED

 11594 **IF** $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda(x : \tau_x). e'$

 11595 $\wedge X(\tau_x, v_1) = v'_1$:

- 11596 a.
- $e \rightarrow_{\text{F-S}} E^*[\text{stat } \tau'_c (\text{chk } \tau'_c e'[x \leftarrow v'_1])]$

 11597 by $v_0 v_1 \triangleright_{\text{S-1}} \text{stat } \tau'_c (\text{chk } \tau'_c e'[x \leftarrow v'_1])$

- 11598 b. QED

 11599 **ELSE** $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda(x : \tau_x). e'$

 11600 $\wedge X(\tau_x, v_1) = \text{BndryErr}$:

- 11601 a.
- $e \rightarrow_{\text{F-S}} \text{BndryErr}$

 11602 by $v_0 v_1 \triangleright_{\text{S-1}} \text{BndryErr}$

- 11603 b. QED

11604

11605

CASE $e = E^*[op^1 v]$:

- 1.
- $\vdash_{\text{F}} op^1 v : \tau'$

 by *static hole typing*

- 2.
- $\vdash_{\text{F}} v : \tau_0 \times \tau_1$

 by *inversion*

- 3.
- $v = \langle v_0, v_1 \rangle$

 $\vee v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$

 by *canonical forms*

- 4.
- IF**
- $v = \langle v_0, v_1 \rangle$

 $\wedge op^1 = \text{fst}$:

- a.
- $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$

- b.
- $e \rightarrow_{\text{F-S}} E^*[v_0]$

 by $op^1 v \triangleright_{\text{S-1}} v_0$

- c. QED

IF $v = \langle v_0, v_1 \rangle$
 $\wedge op^1 = \text{snd}$:

- a.
- $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$

- b.
- $e \rightarrow_{\text{F-S}} E^*[v_1]$

 by $op^1 v \triangleright_{\text{S-1}} v_1$

- c. QED

IF $v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$
 $\wedge op^1 = \text{fst}$
 $\wedge X(\tau'_0, v_0) = v'_0$:

- a.
- $e \rightarrow_{\text{F-S}} E^*[v'_0]$

 by $\text{fst } v \triangleright_{\text{S-1}} v'_0$

- b. QED

IF $v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$
 $\wedge op^1 = \text{fst}$
 $\wedge X(\tau'_0, v_0) = \text{BndryErr}$:

- a.
- $e \rightarrow_{\text{F-S}} \text{BndryErr}$

 by $\text{fst } v \triangleright_{\text{S-1}} \text{BndryErr}$

- b. QED

IF $v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$
 $\wedge op^1 = \text{snd}$
 $\wedge X(\tau'_1, v_1) = v'_1$:

- a.
- $e \rightarrow_{\text{F-S}} E^*[v'_1]$

 by $\text{snd } v \triangleright_{\text{S-1}} v'_1$

- b. QED

ELSE $v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$
 $\wedge op^1 = \text{snd}$
 $\wedge X(\tau'_1, v_1) = \text{BndryErr}$:

- a.
- $e \rightarrow_{\text{F-S}} \text{BndryErr}$

 by $\text{snd } v \triangleright_{\text{S-1}} \text{BndryErr}$

- b. QED

CASE $e = E^*[op^2 v_0 v_1]$:

- 1.
- $\vdash_{\text{F}} op^2 v_0 v_1 : \tau'$

 by *static hole typing*

- 2.
- $\vdash_{\text{F}} v_0 : \tau_0$

 $\wedge \vdash_{\text{F}} v_1 : \tau_1$
 $\wedge \Delta(op^2, \tau_0, \tau_1) = \tau''$

 by *inversion*

- 3.
- $\delta(op^2, v_0, v_1) = e'$

 by Δ *type soundness* (2)

11606

11607

11608

11609

11610

11611

11612

11613

11614

11615

11616

11617

11618

11619

11620

11621

11622

11623

11624

11625

11626

11627

11628

11629

11630

11631

11632

11633

11634

11635

11636

11637

11638

11639

11640

11641

11642

11643

11644

11645

11646

11647

11648

11649

11650

11651

11652

11653

11654

11655

11656

11657

11658

11659

11660

11661 4. $op^2 v_0 v_1 \triangleright_{S-1} e'$
 11662 by (3)
 11663 5. QED by $e \rightarrow_{F-S} E^\bullet[e']$
 11664 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
 11665 1. e' is a value
 11666 $\vee e' \in \text{Err}$
 11667 $\vee e' \rightarrow_{F-D} e''$
 11668 $\vee e' \rightarrow_{F-D} \text{BndryErr}$
 11669 $\vee e' = E'[e'']$ and $e'' \triangleright_{D-1} \text{TagErr}$
 11670 by *dynamic progress*
 11671 2. **IF** e' is a value :
 11672 a. QED $e \rightarrow_{F-S} E[\mathcal{D}_F(\tau', e')]$
 11673 **IF** $e' \in \text{Err}$:
 11674 a. QED $e \rightarrow_{F-S} e'$
 11675 **IF** $e' \rightarrow_{F-D} e''$:
 11676 a. QED $e \rightarrow_{F-S} E[\text{dyn } \tau' e'']$
 11677 **IF** $e' \rightarrow_{F-D} \text{BndryErr}$:
 11678 a. QED $e \rightarrow_{F-S} E[\text{dyn } \tau' \text{BndryErr}]$
 11679 **ELSE** $e' = E'[e'']$ and $e'' \triangleright_{D-1} \text{TagErr}$:
 11680 a. $E' \in E^\bullet$
 11681 by e' is boundary-free
 11682 b. QED
 11683 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
 11684 1. e' is a value
 11685 $\vee e' \in \text{Err}$
 11686 $\vee e' \rightarrow_{F-S} e''$
 11687 $\vee e' \rightarrow_{F-S} \text{BndryErr}$
 11688 $\vee e' = E''[\text{dyn } \tau'' E''[e'']]$ and $e'' \triangleright_{D-1} \text{TagErr}$
 11689 by *static progress*
 11690 2. **IF** e' is a value :
 11691 a. QED $e \rightarrow_{F-S} E[\mathcal{S}_F(\tau', e')]$
 11692 **IF** $e' \in \text{Err}$:
 11693 a. QED $e \rightarrow_{F-S} e'$
 11694 **IF** $e' \rightarrow_{F-S} e''$:
 11695 a. QED $e \rightarrow_{F-S} E[\text{stat } \tau' e'']$
 11696 **IF** $e' \rightarrow_{F-S} \text{BndryErr}$:
 11697 a. QED $e \rightarrow_{F-S} E[\text{stat } \tau' \text{BndryErr}]$
 11698 **ELSE** $e' = E''[\text{dyn } \tau'' E''[e'']]$ and $e'' \triangleright_{D-1} \text{TagErr}$
 11699 :
 11700 a. Contradiction by e' is boundary-free
 11701 **CASE** $e = E[\text{Err}]$:
 11702 1. QED $e \rightarrow_{F-S} \text{Err}$
 11703 **CASE** $e = E^\bullet[\text{chk } \tau' v]$:
 11704 **IF** $\mathcal{X}(\tau, v) = v'$:
 11705 1. $e \rightarrow_{F-S} E^\bullet[v']$
 11706 by $(\text{chk } \tau v) \triangleright_{S-1} v'$
 11707 2. QED
 11708 **ELSE** $\mathcal{X}(\tau, v) = \text{BndryErr}$:
 11709 1. $e \rightarrow_{F-S} \text{BndryErr}$
 11710 by $(\text{chk } \tau v) \triangleright_{S-1} \text{BndryErr}$
 11711 2. QED
 11712 \square

11713 **Lemma 6.9** : HF *dynamic progress*
 11714
 11715

If $\vdash_F e$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{F-D} e'$
- $e \rightarrow_{F-D} \text{BndryErr}$
- $e \rightarrow_{F-D} \text{TagErr}$

Proof:

By the *boundary factoring* lemma, there are seven cases.

CASE e is a value :

1. QED

CASE $e = E^\bullet[v_0 v_1]$:

IF $v_0 = \lambda x. e'$:

1. $e \rightarrow_{F-D} E^\bullet[e'[x \leftarrow v_1]]$
by $v_0 v_1 \triangleright_{D-1} e'[x \leftarrow v_1]$

2. QED

IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c)(\lambda x. e')$:

1. $e \rightarrow_{F-D} E^\bullet[e'[x \leftarrow v_1]]$
by $v_0 v_1 \triangleright_{D-1} e'[x \leftarrow v_1]$

2. QED

IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c)(\lambda(x:\tau_x). e')$

$\wedge \mathcal{X}(\tau_x, v_1) = v'_1$:

1. $e \rightarrow_{F-D} E^\bullet[\text{stat } \tau_c(\text{chk } \tau_c e'[x \leftarrow v'_1])]$
by $v_0 v_1 \triangleright_{D-1} \text{stat } \tau_c(\text{chk } \tau_c e'[x \leftarrow v'_1])$

2. QED

IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c)(\lambda(x:\tau_x). e')$

$\wedge \mathcal{X}(\tau_x, v_1) = \text{BndryErr}$:

1. $e \rightarrow_{F-D} \text{BndryErr}$
by $v_0 v_1 \triangleright_{D-1} \text{BndryErr}$

2. QED

IF $v_0 = \lambda(x:\tau_x). e'$:

1. Contradiction by $\vdash_F e$

ELSE $v_0 = i$

$\vee v_0 = \langle v, v' \rangle$

$\vee v_0 = \text{mon } \tau_0 \times \tau_1 v'$:

1. $e \rightarrow_{F-D} \text{TagErr}$
by $(v_0 v_1) \triangleright_{D-1} \text{TagErr}$

2. QED

CASE $e = E^\bullet[op^1 v]$:

IF $v = \text{mon } \tau_0 \times \tau_1 \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{fst}$

$\wedge \mathcal{X}(\tau_0, v_0) = v'_0$:

1. $e \rightarrow_{F-D} E^\bullet[v'_0]$
by $op^1 v \triangleright_{D-1} v'_0$

2. QED

IF $v = \text{mon } \tau_0 \times \tau_1 \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{fst}$

$\wedge \mathcal{X}(\tau_0, v_0) = \text{BndryErr}$:

1. $e \rightarrow_{F-D} \text{BndryErr}$
by $op^1 v \triangleright_{D-1} \text{BndryErr}$

2. QED

IF $v = \text{mon } \tau_0 \times \tau_1 \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{snd}$

$\wedge \mathcal{X}(\tau_1, v_1) = v'_1$:

1. $e \rightarrow_{F-D} E^\bullet[v'_1]$

11771	1. $e \rightarrow_{F-D} E^\bullet[v_1']$	a. QED $e \rightarrow_{F-S} e'$	11826
11772	by $op^1 v \triangleright_{D-1} v_1'$	IF $e' \rightarrow_{F-S} e''$:	11827
11773	2. QED	a. QED $e \rightarrow_{F-S} E[\text{stat } \tau' e'']$	11828
11774	IF $v = \text{mon } \tau_0 \times \tau_1 \langle v_0, v_1 \rangle$	IF $e' \rightarrow_{F-S} \text{BndryErr}$:	11829
11775	$\wedge op^1 = \text{snd}$	a. QED $e \rightarrow_{F-S} E[\text{stat } \tau' \text{BndryErr}]$	11830
11776	$\wedge X(\tau_1, v_1) = \text{BndryErr}$:	ELSE $e' = E''[\text{dyn } \tau'' E'''[e'']]$ and $e'' \triangleright_{D-1} \text{TagErr}$	11831
11777	1. $e \rightarrow_{F-D} \text{BndryErr}$:	11832
11778	by $op^1 v \triangleright_{D-1} \text{BndryErr}$	a. Contradiction by e' is boundary-free	11833
11779	2. QED	CASE $e = E[\text{Err}]$:	11834
11780	IF $\delta(op^1, v) = e'$:	1. QED $e \rightarrow_{F-D} \text{Err}$	11835
11781	1. $(op^1 v) \triangleright_{D-1} e'$	□	11836
11782	2. QED by $e \rightarrow_{F-D} E^\bullet[e']$	Lemma 6.10 : HF <i>static preservation</i>	11837
11783	ELSE $\delta(op^1, v)$ is undefined :	IF $\vdash_F e : \tau$ and $e \rightarrow_{F-S} e'$ then $\vdash_F e' : \tau$	11838
11784	1. $e \rightarrow_{F-D} \text{TagErr}$	<i>Proof</i> :	11839
11785	by $(op^1 v) \triangleright_{D-1} \text{TagErr}$	By the <i>boundary factoring</i> lemma there are eight cases.	11840
11786	2. QED	CASE e is a value :	11841
11787	CASE $e = E^\bullet[op^2 v_0 v_1]$:	1. Contradiction by $e \rightarrow_{F-S} e'$	11842
11788	IF $\delta(op^2, v_0, v_1) = e''$:	CASE $e = E^\bullet[v_0 v_1]$:	11843
11789	1. $op^2 v_0 v_1 \triangleright_{D-1} e''$	IF $v_0 = \lambda(x:\tau_x). e'$	11844
11790	2. QED	$\wedge e \rightarrow_{F-S} e'[x \leftarrow v_1]$:	11845
11791	ELSE $\delta(op^2, v_0, v_1)$ is undefined :	1. $\vdash_F v_0 v_1 : \tau'$	11846
11792	1. $e \rightarrow_{F-D} \text{TagErr}$	by <i>static hole typing</i>	11847
11793	by $op^2 v_0 v_1 \triangleright_{D-1} \text{TagErr}$	2. $\vdash_F v_0 : \tau_d \Rightarrow \tau_c$	11848
11794	2. QED	$\wedge \vdash_F v_1 : \tau_d$	11849
11795	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	$\wedge \tau_c \leq \tau'$	11850
11796	1. e' is a value	by <i>inversion</i>	11851
11797	$\vee e' \in \text{Err}$	3. $(x:\tau_x) \vdash_F e' : \tau_c$	11852
11798	$\vee e' \rightarrow_{F-D} e''$	by <i>inversion</i> (2)	11853
11799	$\vee e' \rightarrow_{F-D} \text{BndryErr}$	4. $\tau_d \leq \tau_x$	11854
11800	$\vee e' = E^\bullet[e'']$ and $e'' \triangleright_{D-1} \text{TagErr}$	by <i>canonical forms</i> (2)	11855
11801	by <i>dynamic progress</i>	5. $\vdash_F v_1 : \tau_x$	11856
11802	2. IF e' is a value :	by (2, 4)	11857
11803	a. QED $e \rightarrow_{F-D} E[\mathcal{D}_F(\tau', e')]$	6. $\vdash_F e'[x \leftarrow v_1] : \tau_c$	11858
11804	IF $e' \in \text{Err}$:	by <i>substitution</i> (3, 5)	11859
11805	a. QED $e \rightarrow_{F-D} e'$	7. $\vdash_F e'[x \leftarrow v_1] : \tau'$	11860
11806	IF $e' \rightarrow_{F-D} e''$:	by (2, 6)	11861
11807	a. QED $e \rightarrow_{F-S} E[\text{dyn } \tau' e'']$	8. QED by <i>hole substitution</i>	11862
11808	IF $e' \rightarrow_{F-D} \text{BndryErr}$:	IF $v_0 = \text{mon } \tau_d \Rightarrow \tau_c \lambda x. e'$	11863
11809	a. QED $e \rightarrow_{F-D} E[\text{dyn } \tau' \text{BndryErr}]$	$\wedge e \rightarrow_{F-S} E^\bullet[\text{dyn } \tau_c ((\lambda x. e') (X(\tau_d, v_1)))]$:	11864
11810	ELSE $e' = E[e'']$ and $e'' \triangleright_{D-1} \text{TagErr}$:	1. $\vdash_F v_0 v_1 : \tau'$	11865
11811	a. $E \in E^\bullet$	by <i>static hole typing</i>	11866
11812	by e' is boundary-free	2. $\vdash_F v_0 : \tau'_d \Rightarrow \tau'_c$	11867
11813	b. QED	$\wedge \tau'_c \leq \tau'$	11868
11814	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	by <i>inversion</i>	11869
11815	1. e' is a value	3. $\tau_d \Rightarrow \tau_c \leq \tau'_d \Rightarrow \tau'_c$	11870
11816	$\vee e' \in \text{Err}$	by <i>canonical forms</i> (2)	11871
11817	$\vee e' \rightarrow_{F-S} e''$	4. $\vdash_F \lambda x. e'$	11872
11818	$\vee e' \rightarrow_{F-S} \text{BndryErr}$	by <i>inversion</i> (2)	11873
11819	$\vee e' = E''[\text{dyn } \tau'' E'''[e'']]$ and $e'' \triangleright_{D-1} \text{TagErr}$	5. $\tau'_d \leq \tau_d$	11874
11820	by <i>static progress</i>	$\wedge \tau_c \leq \tau'_c$	11875
11821	2. IF e' is a value :	by (3)	11876
11822	a. QED $e \rightarrow_{F-S} E[\mathcal{S}_F(\tau', e')]$	6. $\vdash_F X(\tau_d, v_1)$	11877
11823	IF $e' \in \text{Err}$:	by <i>X soundness</i>	11878
11824			11879
11825			11880

11881	7. $\vdash_{\mathbb{F}} (\lambda x. e') \mathcal{X}(\tau_d, v_1)$	2. $\vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	11936
11882	by (4, 6)	$\wedge \tau_1 \leq: \tau'$	11937
11883	8. $\vdash_{\mathbb{F}} \text{dyn } \tau_c ((\lambda x. e') \mathcal{X}(\tau_d, v_1)) : \tau_c$	by <i>inversion</i>	11938
11884	by (7)	3. $\vdash_{\mathbb{F}} v_1 : \tau_1$	11939
11885	9. $\vdash_{\mathbb{F}} \text{dyn } \tau_c ((\lambda x. e') \mathcal{X}(\tau_d, v_1)) : \tau'$	by <i>inversion</i>	11940
11886	by (2, 5, 8)	4. $\vdash_{\mathbb{F}} v_1 : \tau'$	11941
11887	10. QED by <i>hole substitution</i>	by (2)	11942
11888	ELSE $v_0 = \text{mon } \tau_d \Rightarrow \tau_c (\lambda(x : \tau_x). e')$	5. QED by <i>hole substitution</i>	11943
11889	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[\text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x : \tau_x). e') \mathcal{X}(\tau_x, v_1)))]$	IF $v = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	11944
11890	:	$\wedge \text{op}^1 = \text{fst}$	11945
11891	1. $\vdash_{\mathbb{F}} v_0 v_1 : \tau'$	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[\mathcal{X}(\tau_0, v_0)] :$	11946
11892	by <i>static hole typing</i>	1. $\vdash_{\mathbb{F}} \text{fst } v : \tau'$	11947
11893	2. $\vdash_{\mathbb{F}} v_0 : \tau'_d \Rightarrow \tau'_c$	by <i>static hole typing</i>	11948
11894	$\wedge \vdash_{\mathbb{F}} v_1 : \tau'_d$	2. $\vdash_{\mathbb{F}} v : \tau'_0 \times \tau'_1$	11949
11895	$\wedge \tau'_c \leq: \tau'$	$\wedge \tau'_0 <: \tau'$	11950
11896	by <i>inversion</i>	by <i>inversion</i> (1)	11951
11897	3. $\vdash_{\mathbb{F}} \lambda(x : \tau_x). e' : \tau_x \Rightarrow \tau'_x$	3. $\tau_0 \leq: \tau'_0$	11952
11898	by <i>inversion</i>	by <i>canonical forms</i> (2)	11953
11899	4. $\tau_d \Rightarrow \tau_c \leq: \tau'_d \Rightarrow \tau'_c$	4. $\vdash_{\mathbb{F}} \langle v_0, v_1 \rangle$	11954
11900	by <i>canonical forms</i> (2)	$\vee \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau''$	11955
11901	5. $\tau_c \leq: \tau'_c$	by <i>inversion</i> (2)	11956
11902	by (4)	5. $\vdash_{\mathbb{F}} v_0$	11957
11903	6. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_x, v_1) : \tau_x$	$\vee \vdash_{\mathbb{F}} v_0 : \tau'''$	11958
11904	by <i>X soundness</i>	by <i>inversion</i> (4)	11959
11905	7. $\vdash_{\mathbb{F}} (\lambda(x : \tau_x). e') \mathcal{X}(\tau_x, v_1) : \tau'_x$	6. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_0, v_0) : \tau_0$	11960
11906	by (3, 6)	by <i>X soundness</i> (5)	11961
11907	8. $\vdash_{\mathbb{F}} \text{chk } \tau_c ((\lambda(x : \tau_x). e') \mathcal{X}(\tau_x, v_1)) : \tau_c$	7. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_0, v_0) : \tau'$	11962
11908	by (7)	by (2, 3, 6)	11963
11909	9. $\vdash_{\mathbb{F}} \text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x : \tau_x). e') \mathcal{X}(\tau_x, v_1))) : \tau_c$	8. QED by <i>hole substitution</i>	11964
11910	by (8)	ELSE $v = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	11965
11911	10. $\vdash_{\mathbb{F}} \text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x : \tau_x). e') \mathcal{X}(\tau_x, v_1))) : \tau'$	$\wedge \text{op}^1 = \text{snd}$	11966
11912	by (2, 5, 9)	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[\mathcal{X}(\tau_1, v_1)] :$	11967
11913	11. QED by <i>hole substitution</i>	1. $\vdash_{\mathbb{F}} \text{snd } v : \tau'$	11968
11914	CASE $e = E^*[\text{op}^1 v] :$	by <i>static hole typing</i>	11969
11915	IF $v = \langle v_0, v_1 \rangle$	2. $\vdash_{\mathbb{F}} v : \tau'_0 \times \tau'_1$	11970
11916	$\wedge \text{op}^1 = \text{fst}$	$\wedge \tau'_1 <: \tau'$	11971
11917	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[v_0] :$	by <i>inversion</i> (1)	11972
11918	1. $\vdash_{\mathbb{F}} \text{fst } \langle v_0, v_1 \rangle : \tau'$	3. $\tau_1 \leq: \tau'_1$	11973
11919	by <i>static hole typing</i>	by <i>canonical forms</i> (2)	11974
11920	2. $\vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	4. $\vdash_{\mathbb{F}} \langle v_0, v_1 \rangle$	11975
11921	$\wedge \tau_0 \leq: \tau'$	$\vee \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau''$	11976
11922	by <i>inversion</i>	by <i>inversion</i> (2)	11977
11923	3. $\vdash_{\mathbb{F}} v_0 : \tau_0$	5. $\vdash_{\mathbb{F}} v_1$	11978
11924	by <i>inversion</i>	$\vee \vdash_{\mathbb{F}} v_1 : \tau'''$	11979
11925	4. $\vdash_{\mathbb{F}} v_0 : \tau'$	by <i>inversion</i> (4)	11980
11926	by (2)	6. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_1, v_1) : \tau_1$	11981
11927	5. QED by <i>hole substitution</i>	by <i>X soundness</i> (5)	11982
11928	IF $v = \langle v_0, v_1 \rangle$	7. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_1, v_1) : \tau'$	11983
11929	$\wedge \text{op}^1 = \text{snd}$	by (2, 3, 6)	11984
11930	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[v_1] :$	8. QED by <i>hole substitution</i>	11985
11931	1. $\vdash_{\mathbb{F}} \text{snd } \langle v_0, v_1 \rangle : \tau'$	CASE $e = E^*[\text{op}^2 v_0 v_1]$	11986
11932	by <i>static hole typing</i>	$\wedge \delta(\text{op}^2, v_0, v_1) = v$	11987
11933		$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[v] :$	11988
11934			11989
11935			11990

11991	1. $\vdash_{\mathbb{F}} op^2 v_0 v_1 : \tau'$	6. QED by <i>hole substitution</i> (5)	12046
11992	by <i>static hole typing</i>	CASE $e = E[\text{Err}] :$	12047
11993	2. $\vdash_{\mathbb{F}} v_0 : \tau_0$	1. $e \rightarrow_{\mathbb{F}\text{-S}} \text{Err}$	12048
11994	$\wedge \vdash_{\mathbb{F}} v_1 : \tau_1$	2. QED by $\vdash_{\mathbb{F}} \text{Err} : \tau$	12049
11995	$\wedge \Delta(op^2, \tau_0, \tau_1) = \tau''$	CASE $e = E^\bullet[\text{chk } \tau v] :$	12050
11996	$\wedge \tau'' \leq \tau'$	1. $\vdash_{\mathbb{F}} \text{chk } \tau v : \tau$	12051
11997	by <i>inversion</i>	by <i>static hole typing</i>	12052
11998	3. $\vdash_{\mathbb{F}} v : \tau''$	2. $\vdash_{\mathbb{F}} v : \tau'$	12053
11999	by Δ <i>type soundness</i> (2)	by <i>inversion</i> (1)	12054
12000	4. $\vdash_{\mathbb{F}} v : \tau'$	3. $\vdash_{\mathbb{F}} \mathcal{X}(\tau, v') : \tau$	12055
12001	by (2, 3)	by \mathcal{X} <i>soundness</i> (2)	12056
12002	5. QED by <i>hole substitution</i> (4)	4. QED by <i>hole substitution</i> (3)	12057
12003	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	□	12058
12004	IF e' is a value :	Lemma 6.11 : HF <i>dynamic preservation</i>	12059
12005	1. $e \rightarrow_{\mathbb{F}\text{-S}} E[\mathcal{D}_{\mathbb{F}}(\tau', e')]$	■ If $\vdash_{\mathbb{F}} e$ and $e \rightarrow_{\mathbb{F}\text{-D}} e'$ then $\vdash_{\mathbb{F}} e'$	12060
12006	2. $\vdash_{\mathbb{F}} \text{dyn } \tau' e' : \tau'$	<i>Proof</i> :	12061
12007	by <i>boundary hole typing</i>	By the <i>boundary factoring</i> lemma, there are seven cases.	12062
12008	3. $\vdash_{\mathbb{F}} e'$	CASE e is a value :	12063
12009	by <i>inversion</i> (2)	1. Contradiction by $e \rightarrow_{\mathbb{F}\text{-D}} e'$	12064
12010	4. $\vdash_{\mathbb{F}} \mathcal{D}_{\mathbb{F}}(\tau', e') : \tau'$	CASE $e = E^\bullet[v_0 v_1] :$	12065
12011	by $\mathcal{D}_{\mathbb{F}}$ <i>soundness</i> (3)	IF $v_0 = \lambda x. e'$	12066
12012	5. QED by <i>hole substitution</i> (4)	$\wedge e \rightarrow_{\mathbb{F}\text{-D}} E^\bullet[e'[x \leftarrow v_1]] :$	12067
12013	ELSE $e' \rightarrow_{\mathbb{F}\text{-D}} e'' :$	1. $\vdash_{\mathbb{F}} v_0 v_1$	12068
12014	1. $e \rightarrow_{\mathbb{F}\text{-S}} E[\text{dyn } \tau' e'']$	by <i>dynamic hole typing</i>	12069
12015	2. $\vdash_{\mathbb{F}} \text{dyn } \tau' e' : \tau'$	2. $\vdash_{\mathbb{F}} v_0$	12070
12016	by <i>boundary hole typing</i>	$\wedge \vdash_{\mathbb{F}} v_1$	12071
12017	3. $\vdash_{\mathbb{F}} e'$	by <i>inversion</i> (1)	12072
12018	by <i>inversion</i> (2)	3. $x \vdash_{\mathbb{F}} e'$	12073
12019	4. $\vdash_{\mathbb{F}} e''$	by <i>inversion</i> (2)	12074
12020	by <i>dynamic preservation</i> (3)	4. $\vdash_{\mathbb{F}} e'[x \leftarrow v_1]$	12075
12021	5. $\vdash_{\mathbb{F}} \text{dyn } \tau' e'' : \tau'$	by <i>substitution</i> (2, 3)	12076
12022	by (4)	5. QED <i>hole substitution</i> (4)	12077
12023	6. QED by <i>hole substitution</i> (5)	IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) \lambda x. e'$	12078
12024	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	$\wedge e \rightarrow_{\mathbb{F}\text{-D}} E^\bullet[(\lambda x. e') v_1] :$	12079
12025	IF e' is a value :	1. $\vdash_{\mathbb{F}} v_0 v_1$	12080
12026	1. $e \rightarrow_{\mathbb{F}\text{-S}} E[\mathcal{S}_{\mathbb{F}}(\tau', e')]$	by <i>dynamic hole typing</i>	12081
12027	2. $\vdash_{\mathbb{F}} \text{stat } \tau' e'$	2. $\vdash_{\mathbb{F}} v_0$	12082
12028	by <i>boundary hole typing</i>	$\wedge \vdash_{\mathbb{F}} v_1$	12083
12029	3. $\vdash_{\mathbb{F}} e' : \tau'$	by <i>inversion</i> (1)	12084
12030	by <i>inversion</i> (2)	3. $\vdash_{\mathbb{F}} (\lambda x. e') v_1$	12085
12031	4. $\vdash_{\mathbb{F}} \mathcal{S}_{\mathbb{F}}(\tau', e')$	by (2)	12086
12032	by $\mathcal{S}_{\mathbb{F}}$ <i>soundness</i> (3)	4. QED <i>hole substitution</i> (5)	12087
12033	5. QED by <i>hole substitution</i> (4)	ELSE $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) \lambda(x : \tau_x). e'$	12088
12034	ELSE $e' \rightarrow_{\mathbb{F}\text{-S}} e'' :$	$\wedge e \rightarrow_{\mathbb{F}\text{-D}} E^\bullet[\text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x : \tau_x). e') \mathcal{X}(\tau_x, v_1)))]$	12089
12035	1. $e \rightarrow_{\mathbb{F}\text{-S}} E[\text{stat } \tau' e'']$:	12090
12036	2. $\vdash_{\mathbb{F}} \text{stat } \tau' e'$	1. $\vdash_{\mathbb{F}} v_0 v_1$	12091
12037	by <i>boundary hole typing</i>	by <i>dynamic hole typing</i>	12092
12038	3. $\vdash_{\mathbb{F}} e' : \tau'$	2. $\vdash_{\mathbb{F}} v_0$	12093
12039	by <i>inversion</i> (2)	$\wedge \vdash_{\mathbb{F}} v_1$	12094
12040	4. $\vdash_{\mathbb{F}} e'' : \tau'$	by <i>inversion</i>	12095
12041	by <i>static preservation</i> (3)	3. $\vdash_{\mathbb{F}} \lambda(x : \tau_x). e' : \tau_x \Rightarrow \tau'_x$	12096
12042	5. $\vdash_{\mathbb{F}} \text{stat } \tau' e''$	by <i>inversion</i> (2)	12097
12043	by (4)		12098
12044			12099
12045			12100

12101	4. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_x, v_1) : \tau_x$	4. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_1, v_1)$	12154
12102	by \mathcal{X} soundness (2)	by \mathcal{X} soundness (3)	12157
12103	5. $\vdash_{\mathbb{F}} ((\lambda(x:\tau_x). e') \mathcal{X}(\tau_x, v_1)) : \tau'_x$	5. QED by <i>hole substitution</i>	12158
12104	by (3, 4)	CASE $e = E^{\bullet}[op^2 v_0 v_1]$	12159
12105	6. $\vdash_{\mathbb{F}} \text{chk } \tau_c ((\lambda(x:\tau_x). e') \mathcal{X}(\tau_x, v_1)) : \tau_c$	$\wedge \delta(op^2, v_0, v_1) = v$	12160
12106	by (5)	$\wedge e \rightarrow_{\mathbb{F}\text{-D}} E^{\bullet}[v]$	12161
12107	7. $\vdash_{\mathbb{F}} \text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x:\tau_x). e') \mathcal{X}(\tau_x, v_1)))$	1. $\vdash_{\mathbb{F}} op^2 v_0 v_1$	12162
12108	by (6)	by <i>dynamic hole typing</i>	12163
12109	8. QED <i>hole substitution</i>	2. $\vdash_{\mathbb{F}} v_0$	12164
12110	CASE $e = E^{\bullet}[op^1 v]$	$\wedge \vdash_{\mathbb{F}} v_1$	12165
12111	IF $v = \langle v_0, v_1 \rangle$	by <i>inversion</i> (1)	12166
12112	$\wedge op^1 = \text{fst}$	3. $\vdash_{\mathbb{F}} v$	12167
12113	$\wedge e \rightarrow_{\mathbb{F}\text{-D}} E^{\bullet}[v_0]$	by δ <i>preservation</i> (2)	12168
12114	1. $\vdash_{\mathbb{F}} op^1 v$	4. QED by <i>hole substitution</i> (3)	12169
12115	by <i>dynamic hole typing</i>	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	12170
12116	2. $\vdash_{\mathbb{F}} v$	IF e' is a value :	12171
12117	by <i>inversion</i> (1)	1. $e \rightarrow_{\mathbb{F}\text{-D}} E[\mathcal{D}_{\mathbb{F}}(\tau', e')]$	12172
12118	3. $\vdash_{\mathbb{F}} v_0$	2. $\vdash_{\mathbb{F}} \text{dyn } \tau' e' : \tau'$	12173
12119	by <i>inversion</i> (2)	by <i>boundary hole typing</i>	12174
12120	4. QED by <i>hole substitution</i>	3. $\vdash_{\mathbb{F}} e'$	12175
12121	IF $v = \langle v_0, v_1 \rangle$	by <i>inversion</i> (2)	12176
12122	$\wedge op^1 = \text{snd}$	4. $\vdash_{\mathbb{F}} \mathcal{D}_{\mathbb{F}}(\tau', e') : \tau'$	12177
12123	$\wedge e \rightarrow_{\mathbb{F}\text{-D}} E^{\bullet}[v_1]$	by $\mathcal{D}_{\mathbb{F}}$ <i>soundness</i> (3)	12178
12124	1. $\vdash_{\mathbb{F}} op^1 v$	5. QED by <i>hole substitution</i> (4)	12179
12125	by <i>dynamic hole typing</i>	ELSE $e' \rightarrow_{\mathbb{F}\text{-D}} e''$:	12180
12126	2. $\vdash_{\mathbb{F}} v$	1. $e \rightarrow_{\mathbb{F}\text{-D}} E[\text{dyn } \tau' e'']$	12181
12127	by <i>inversion</i> (1)	2. $\vdash_{\mathbb{F}} \text{dyn } \tau' e' : \tau'$	12182
12128	3. $\vdash_{\mathbb{F}} v_1$	by <i>boundary hole typing</i>	12183
12129	by <i>inversion</i> (2)	3. $\vdash_{\mathbb{F}} e'$	12184
12130	4. QED by <i>hole substitution</i>	$\wedge \tau' \leq: \tau''$	12185
12131	IF $v = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	by <i>inversion</i> (2)	12186
12132	$\wedge op^1 = \text{fst}$	4. $\vdash_{\mathbb{F}} e''$	12187
12133	$\wedge e \rightarrow_{\mathbb{F}\text{-D}} E^{\bullet}[\mathcal{X}(\tau_0, v_0)]$	by <i>dynamic preservation</i> (3)	12188
12134	1. $\vdash_{\mathbb{F}} op^1 v$	5. $\vdash_{\mathbb{F}} \text{dyn } \tau' e'' : \tau'$	12189
12135	by <i>dynamic hole typing</i>	by (4)	12190
12136	2. $\vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	6. QED by <i>hole substitution</i> (5)	12191
12137	by <i>inversion</i> (1)	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	12192
12138	3. $\vdash_{\mathbb{F}} v_0$	IF $e' \in v$:	12193
12139	$\vee \vdash_{\mathbb{F}} v_0 : \tau'_0$	1. $e \rightarrow_{\mathbb{F}\text{-D}} E[\mathcal{S}_{\mathbb{F}}(\tau', e')]$	12194
12140	by <i>inversion</i> (2)	2. $\vdash_{\mathbb{F}} \text{stat } \tau' e'$	12195
12141	4. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_0, v_0)$	by <i>boundary hole typing</i>	12196
12142	by \mathcal{X} soundness (3)	3. $\vdash_{\mathbb{F}} e' : \tau'$	12197
12143	5. QED by <i>hole substitution</i>	by <i>inversion</i> (2)	12198
12144	ELSE $v = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	4. $\vdash_{\mathbb{F}} \mathcal{S}_{\mathbb{F}}(\tau', e')$	12199
12145	$\wedge op^1 = \text{snd}$	by $\mathcal{S}_{\mathbb{F}}$ <i>soundness</i> (3)	12200
12146	$\wedge e \rightarrow_{\mathbb{F}\text{-D}} E^{\bullet}[\mathcal{X}(\tau_1, v_1)]$	5. QED by <i>hole substitution</i> (5)	12201
12147	1. $\vdash_{\mathbb{F}} op^1 v$	ELSE $e' \rightarrow_{\mathbb{F}\text{-S}} e''$:	12202
12148	by <i>dynamic hole typing</i>	1. $e \rightarrow_{\mathbb{F}\text{-D}} E[\text{stat } \tau' e'']$	12203
12149	2. $\vdash_{\mathbb{F}} \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	2. $\vdash_{\mathbb{F}} \text{stat } \tau' e'$	12204
12150	by <i>inversion</i> (1)	by <i>boundary hole typing</i>	12205
12151	3. $\vdash_{\mathbb{F}} v_1$	3. $\vdash_{\mathbb{F}} e' : \tau'$	12206
12152	$\vee \vdash_{\mathbb{F}} v_1 : \tau'_1$	by <i>inversion</i> (2)	12207
12153	by <i>inversion</i> (2)	4. $\vdash_{\mathbb{F}} e'' : \tau'$	12208
12154		by <i>static preservation</i> (3)	12209
12155			12210

12211 5. $\vdash_{\mathbb{F}} \text{stat } \tau' e''$
 12212 by (4)
 12213 6. QED by *hole substitution* (5)
 12214 **CASE** $e = E[\text{Err}]$:
 12215 1. $e \rightarrow_{\mathbb{F}\text{-D}} \text{Err}$
 12216 2. QED $\vdash_{\mathbb{F}} \text{Err}$
 12217 \square
 12218 **Lemma 6.12** : HF *static boundary factoring*
 12219 If $\vdash_{\mathbb{F}} e : \tau$ then one of the following holds:
 12220 • e is a value
 12221 • $e = E^{\bullet}[v_0 v_1]$
 12222 • $e = E^{\bullet}[\text{op}^1 v]$
 12223 • $e = E^{\bullet}[\text{op}^2 v_0 v_1]$
 12224 • $e = E^{\bullet}[\text{chk } \tau v]$
 12225 • $e = E[\text{dyn } \tau e']$ where e' is boundary-free
 12226 • $e = E[\text{stat } \tau e']$ where e' is boundary-free
 12227 • $e = E[\text{Err}]$

12228 *Proof*:

12229 By the *unique static evaluation contexts* lemma, there are
 12230 eight cases.

12231 **CASE** e is a value :
 12232 1. QED
 12233 **CASE** $e = E[v_0 v_1]$:
 12234 1. $E = E^{\bullet}$
 12235 $\vee E = E'[\text{dyn } \tau E^{\bullet}]$
 12236 $\vee E = E'[\text{stat } \tau E^{\bullet}]$
 12237 by *inner boundary*
 12238 2. **IF** $E = E^{\bullet}$:
 12239 a. QED $e = E^{\bullet}[v_0 v_1]$
 12240 **IF** $E = E'[\text{dyn } \tau E^{\bullet}]$:
 12241 a. QED $e = E'[\text{dyn } \tau E^{\bullet}[v_0 v_1]]$
 12242 **ELSE** $E = E'[\text{stat } \tau E^{\bullet}]$:
 12243 a. QED $e = E'[\text{stat } \tau E^{\bullet}[v_0 v_1]]$
 12244 **CASE** $e = E[\text{op}^1 v]$:
 12245 1. $E = E^{\bullet}$
 12246 $\vee E = E'[\text{dyn } \tau E^{\bullet}]$
 12247 $\vee E = E'[\text{stat } \tau E^{\bullet}]$
 12248 by *inner boundary*
 12249 2. **IF** $E = E^{\bullet}$:
 12250 a. QED $e = E^{\bullet}[\text{op}^1 v]$
 12251 **IF** $E = E'[\text{dyn } \tau E^{\bullet}]$:
 12252 a. QED $e = E'[\text{dyn } \tau E^{\bullet}[\text{op}^1 v]]$
 12253 **ELSE** $E = E'[\text{stat } \tau E^{\bullet}]$:
 12254 a. QED $e = E'[\text{stat } \tau E^{\bullet}[\text{op}^1 v]]$
 12255 **CASE** $e = E[\text{op}^2 v_0 v_1]$:
 12256 1. $E = E^{\bullet}$
 12257 $\vee E = E'[\text{dyn } \tau E^{\bullet}]$
 12258 $\vee E = E'[\text{stat } \tau E^{\bullet}]$
 12259 by *inner boundary*
 12260 2. **IF** $E = E^{\bullet}$:
 12261 a. QED $e = E^{\bullet}[\text{op}^2 v_0 v_1]$
 12262 **IF** $E = E'[\text{dyn } \tau E^{\bullet}]$:
 12263 a. QED $e = E'[\text{dyn } \tau E^{\bullet}[\text{op}^2 v_0 v_1]]$
 12264 **ELSE** $E = E'[\text{stat } \tau E^{\bullet}]$:

12265

a. QED $e = E'[\text{stat } \tau E^{\bullet}[\text{op}^2 v_0 v_1]]$ 12266
CASE $e = E[\text{chk } \tau v]$: 12267
 1. $E = E^{\bullet}$ 12268
 $\vee E = E'[\text{dyn } \tau E^{\bullet}]$ 12269
 $\vee E = E'[\text{stat } \tau E^{\bullet}]$ 12270
 by *inner boundary* 12271
 2. **IF** $E = E^{\bullet}$: 12272
 a. QED $e = E^{\bullet}[\text{chk } \tau v]$ 12273
IF $E = E'[\text{dyn } \tau E^{\bullet}]$: 12274
 a. Contradiction by $\vdash_{\mathbb{F}} e : \tau$ 12275
ELSE $E = E'[\text{stat } \tau E^{\bullet}]$: 12276
 a. QED $e = E'[\text{stat } \tau E^{\bullet}[\text{chk } \tau v]]$ 12277
CASE $e = E[\text{dyn } \tau v]$: 12278
 1. QED v is boundary-free 12279
CASE $e = E[\text{stat } \tau v]$: 12280
 1. QED v is boundary-free 12281
CASE $e = E[\text{Err}]$: 12282
 1. QED 12283
 \square 12284

12285 **Lemma 6.13** : HF *unique static evaluation contexts*

12286 If $\vdash_{\mathbb{F}} e : \tau$ then one of the following holds:

12287 • e is a value
 12288 • $e = E[v_0 v_1]$
 12289 • $e = E[\text{op}^1 v]$
 12290 • $e = E[\text{op}^2 v_0 v_1]$
 12291 • $e = E[\text{chk } \tau v]$
 12292 • $e = E[\text{dyn } \tau v]$
 12293 • $e = E[\text{stat } \tau v]$
 12294 • $e = E[\text{Err}]$

12295 *Proof*:

12296 By induction on the structure of e .

12297 **CASE** $e = x$ 12297
 $\vee e = \lambda x. e'$ 12298
 $\vee e = \text{stat } \tau e'$: 12299
 1. Contradiction by $\vdash_{\mathbb{F}} e : \tau$ 12300
CASE $e = i$ 12301
 $\vee e = \lambda(x:\tau_d). e'$ 12302
 $\vee e = \text{mon}(\tau_d \Rightarrow \tau_c) v$: 12303
 1. QED e is a value 12304
CASE $e = \langle e_0, e_1 \rangle$: 12305
IF $e_0 \notin v$: 12306
 1. $\vdash_{\mathbb{F}} e_0 : \tau_0$ 12307
 by *inversion* 12308
 2. $e_0 = E_0[e'_0]$ 12309
 by the induction hypothesis (1) 12310
 3. $E = \langle E_0, e_1 \rangle$ 12311
 4. QED $e = E[e'_0]$ 12312
IF $e_0 \in v$ 12313
 $\wedge e_1 \notin v$: 12314
 1. $\vdash_{\mathbb{F}} e_1 : \tau_1$ 12315
 by *inversion* 12316
 2. $e_1 = E_1[e'_1]$ 12317
 by the induction hypothesis (1) 12318
 3. $E = \langle e_0, E_1 \rangle$ 12319

12320

12321	4. QED $e = E[e'_1]$	1. $E = []$	12376
12322	ELSE $e_0 \in v$	2. QED $e = E[op^2 e_0 e_1]$	12377
12323	$\wedge e_1 \in v :$	CASE $e = \text{chk } \tau e_0 :$	12378
12324	1. $E = []$	IF $e_0 \notin v :$	12379
12325	2. QED e is a value	1. $\vdash_{\mathbb{F}} e_0 : \tau_0$	12380
12326	CASE $e = e_0 e_1 :$	by <i>inversion</i>	12381
12327	IF $e_0 \notin v :$	2. $e_0 = E_0[e'_0]$	12382
12328	1. $\vdash_{\mathbb{F}} e_0 : \tau_0$	by the induction hypothesis (1)	12383
12329	by <i>inversion</i>	3. $E = \text{chk } \tau E_0$	12384
12330	2. $e_0 = E_0[e'_0]$	4. QED $e = E[e'_0]$	12385
12331	by the induction hypothesis (1)	ELSE $e_0 \in v :$	12386
12332	3. $E = E_0 e_1$	1. $E = []$	12387
12333	4. QED $e = E[e'_0]$	2. QED $e = E[\text{chk } \tau e_0]$	12388
12334	IF $e_0 \in v$	CASE $e = \text{dyn } \tau e_0 :$	12389
12335	$\wedge e_1 \notin v :$	IF $e_0 \notin v :$	12390
12336	1. $\vdash_{\mathbb{F}} e_1 : \tau_1$	1. $\vdash_{\mathbb{F}} e_0$	12391
12337	by <i>inversion</i>	by <i>inversion</i>	12392
12338	2. $e_1 = E_1[e'_1]$	2. $e_0 = E_0[e'_0]$	12393
12339	by the induction hypothesis (1)	by <i>unique dynamic evaluation contexts</i> (1)	12394
12340	3. $E = e_0 E_1$	3. $E = \text{dyn } \tau E_0$	12395
12341	4. QED $e = E[e'_1]$	4. QED $e = E[e'_0]$	12396
12342	ELSE $e_0 \in v$	ELSE $e_0 \in v :$	12397
12343	$\wedge e_1 \in v :$	1. $E = []$	12398
12344	1. $E = []$	2. QED $e = E[\text{dyn } \tau e_0]$	12399
12345	2. QED $e = E[e_0 e_1]$	CASE $e = \text{Err} :$	12400
12346	CASE $e = op^1 e_0 :$	1. $E = []$	12401
12347	IF $e_0 \notin v :$	2. QED $e = E[\text{Err}]$	12402
12348	1. $\vdash_{\mathbb{F}} e_0 : \tau_0$	□	12403
12349	by <i>inversion</i>	Lemma 6.14 : HF <i>inner boundary</i>	12404
12350	2. $e_0 = E_0[e'_0]$	For all contexts E , one of the following holds:	12405
12351	by the induction hypothesis (1)	• $E = E^\bullet$	12406
12352	3. $E = op^1 E_0$	• $E = E'[\text{dyn } \tau E^\bullet]$	12407
12353	4. QED $e = E[e'_0]$	• $E = E'[\text{stat } \tau E^\bullet]$	12408
12354	ELSE $e_0 \in v :$	<i>Proof</i> :	12409
12355	1. $E = []$	By induction on the structure of E .	12410
12356	2. QED $e = E[op^1 e_0]$	CASE $E = E^\bullet :$	12411
12357	CASE $e = op^2 e_0 e_1 :$	1. QED	12412
12358	IF $e_0 \notin v :$	CASE $E = E_0 e_1 :$	12413
12359	1. $\vdash_{\mathbb{F}} e_0 : \tau_0$	1. $E_0 = E^\bullet$	12414
12360	by <i>inversion</i>	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	12415
12361	2. $e_0 = E_0[e'_0]$	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	12416
12362	by the induction hypothesis (1)	by the induction hypothesis	12417
12363	3. $E = op^2 E_0 e_1$	2. IF $E_0 = E^\bullet :$	12418
12364	4. QED $e = E[e'_0]$	a. QED E is boundary-free	12419
12365	IF $e_0 \in v$	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet] :$	12420
12366	$\wedge e_1 \notin v :$	a. $E' = E'_0 e_1$	12421
12367	1. $\vdash_{\mathbb{F}} e_1 : \tau_1$	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	12422
12368	by <i>inversion</i>	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet] :$	12423
12369	2. $e_1 = E_1[e'_1]$	a. $E' = E'_0 e_1$	12424
12370	by the induction hypothesis (1)	b. QED $E = E'[\text{stat } \tau E^\bullet]$	12425
12371	3. $E = op^2 e_0 E_1$	CASE $E = v_0 E_1 :$	12426
12372	4. QED $e = E[e'_1]$	1. $E_1 = E^\bullet$	12427
12373	ELSE $e_0 \in v$	$\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$	12428
12374	$\wedge e_1 \in v :$		12429
12375			12430

12431	$\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	12486
12432	by the induction hypothesis	by the induction hypothesis	12487
12433	2. IF $E_1 = E^\bullet$:	2. IF $E_0 = E^\bullet$:	12488
12434	a. QED E is boundary-free	a. QED E is boundary-free	12489
12435	IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:	12490
12436	a. $E' = v_0 E'_1$	a. $E' = op^2 E'_0 e_1$	12491
12437	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	12492
12438	ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:	12493
12439	a. $E' = v_0 E'_1$	a. $E' = op^2 E'_0 e_1$	12494
12440	b. QED $E = E'[\text{stat } \tau E^\bullet]$	b. QED $E = E'[\text{stat } \tau E^\bullet]$	12495
12441	CASE $E = \langle E_0, e_1 \rangle$:	CASE $E = op^2 v_0 E_1$:	12496
12442	1. $E_0 = E^\bullet$	1. $E_1 = E^\bullet$	12497
12443	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	$\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$	12498
12444	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	$\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$	12499
12445	by the induction hypothesis	by the induction hypothesis	12500
12446	2. IF $E_0 = E^\bullet$:	2. IF $E_1 = E^\bullet$:	12501
12447	a. QED E is boundary-free	a. QED E is boundary-free	12502
12448	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:	IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:	12503
12449	a. $E' = \langle E'_0, e_1 \rangle$	a. $E' = op^2 v_0 E'_1$	12504
12450	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	12505
12451	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:	ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:	12506
12452	a. $E' = \langle E'_0, e_1 \rangle$	a. $E' = op^2 v_0 E'_1$	12507
12453	b. QED $E = E'[\text{stat } \tau E^\bullet]$	b. QED $E = E'[\text{stat } \tau E^\bullet]$	12508
12454	CASE $E = \langle v_0, E_1 \rangle$:	CASE $E = \text{chk } \tau E_0$:	12509
12455	1. $E_1 = E^\bullet$	1. $E_0 = E^\bullet$	12510
12456	$\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	12511
12457	$\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	12512
12458	by the induction hypothesis	by the induction hypothesis	12513
12459	2. IF $E_1 = E^\bullet$:	2. IF $E_0 = E^\bullet$:	12514
12460	a. QED E is boundary-free	a. QED E is boundary-free	12515
12461	IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:	12516
12462	a. $E' = \langle v_0, E'_1 \rangle$	a. $E' = \text{chk } \tau E'_0$	12517
12463	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	12518
12464	ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:	12519
12465	a. $E' = \langle v_0, E'_1 \rangle$	a. $E' = \text{chk } \tau E'_0$	12520
12466	b. QED $E = E'[\text{stat } \tau E^\bullet]$	b. QED $E = E'[\text{stat } \tau E^\bullet]$	12521
12467	CASE $E = op^1 E_0$:	CASE $E = \text{dyn } \tau E_0$:	12522
12468	1. $E_0 = E^\bullet$	1. $E_0 = E^\bullet$	12523
12469	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	$\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$	12524
12470	$\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$	$\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$	12525
12471	by the induction hypothesis	by the induction hypothesis	12526
12472	2. IF $E_0 = E^\bullet$:	2. IF $E_0 = E^\bullet$:	12527
12473	a. QED E is boundary-free	a. QED	12528
12474	IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:	IF $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:	12529
12475	a. $E' = op^1 E'_0$	a. $E' = \text{dyn } \tau E'_0$	12530
12476	b. QED $E = E'[\text{dyn } \tau E^\bullet]$	b. QED $E = E'[\text{dyn } \tau' E^\bullet]$	12531
12477	ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:	ELSE $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:	12532
12478	a. $E' = op^1 E'_0$	a. $E' = \text{dyn } \tau E'_0$	12533
12479	b. QED $E = E'[\text{stat } \tau E^\bullet]$	b. QED $E = E'[\text{stat } \tau' E^\bullet]$	12534
12480	CASE $E = op^2 E_0 e_1$:	CASE $E = \text{stat } \tau E_0$:	12535
12481	1. $E_0 = E^\bullet$	1. $E_0 = E^\bullet$	12536
12482	$\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$	$\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$	12537
12483			12538
12484			12539
12485			12540

12541 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 12542 by the induction hypothesis
 12543 2. **IF** $E_0 = E^\bullet$:
 12544 a. QED
 12545 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 12546 a. $E' = \text{stat } \tau E'_0$
 12547 b. QED $E = E'[\text{dyn } \tau' E^\bullet]$
 12548 **ELSE** $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 12549 a. $E' = \text{stat } \tau E'_0$
 12550 b. QED $E = E'[\text{stat } \tau' E^\bullet]$

□

12552 **Lemma 6.15** : HF *dynamic boundary factoring*

12553 If $\vdash_{\mathbb{F}} e$ then one of the following holds:

- 12554 • e is a value
- 12555 • $e = E^\bullet[v_0 v_1]$
- 12556 • $e = E^\bullet[op^1 v]$
- 12557 • $e = E^\bullet[op^2 v_0 v_1]$
- 12558 • $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- 12559 • $e = E[\text{stat } \tau e']$ where e' is boundary-free
- 12560 • $e = E[\text{Err}]$

12561 *Proof*:

12562 By the *unique dynamic evaluation contexts* lemma, there
 12563 are eight cases.

12564 **CASE** e is a value :

12565 1. QED

12566 **CASE** $e = E[v_0 v_1]$:

12567 1. $E = E^\bullet$

12568 $\vee E = E'[\text{dyn } \tau E^\bullet]$

12569 $\vee E = E'[\text{stat } \tau E^\bullet]$

12570 by *inner boundary*

12571 2. **IF** $E = E^\bullet$:

12572 a. QED $e = E^\bullet[v_0 v_1]$

12573 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:

12574 a. QED $e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$

12575 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:

12576 a. QED $e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$

12577 **CASE** $e = E[op^1 v]$:

12578 1. $E = E^\bullet$

12579 $\vee E = E'[\text{dyn } \tau E^\bullet]$

12580 $\vee E = E'[\text{stat } \tau E^\bullet]$

12581 by *inner boundary*

12582 2. **IF** $E = E^\bullet$:

12583 a. QED $e = E^\bullet[op^1 v]$

12584 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:

12585 a. QED $e = E'[\text{dyn } \tau E^\bullet[op^1 v]]$

12586 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:

12587 a. QED $e = E'[\text{stat } \tau E^\bullet[op^1 v]]$

12588 **CASE** $e = E[op^2 v_0 v_1]$:

12589 1. $E = E^\bullet$

12590 $\vee E = E'[\text{dyn } \tau E^\bullet]$

12591 $\vee E = E'[\text{stat } \tau E^\bullet]$

12592 by *inner boundary*

12593 2. **IF** $E = E^\bullet$:

12594 a. QED $e = E^\bullet[op^2 v_0 v_1]$

12595

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. QED $e = E'[\text{dyn } \tau E^\bullet[op^2 v_0 v_1]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. QED $e = E'[\text{stat } \tau E^\bullet[op^2 v_0 v_1]]$

CASE $e = E[\text{chk } \tau' v]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. Contradiction by $\vdash_{\mathbb{F}} e$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. Contradiction by $\vdash_{\mathbb{F}} e$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. QED $e = E'[\text{stat } \tau E^\bullet[\text{chk } \tau' v]]$

CASE $e = E[\text{dyn } \tau v]$:

1. QED v is boundary-free

CASE $e = E[\text{stat } \tau v]$:

1. QED v is boundary-free

CASE $e = E[\text{Err}]$:

1. QED

□

Lemma 6.16 : HF *unique dynamic evaluation contexts*

If $\vdash_{\mathbb{F}} e$ then one of the following holds:

- e is a value
- $e = E[v_0 v_1]$
- $e = E[op^1 v]$
- $e = E[op^2 v_0 v_1]$
- $e = E[\text{chk } \tau v]$
- $e = E[\text{dyn } \tau v]$
- $e = E[\text{stat } \tau v]$
- $e = E[\text{Err}]$

Proof:

By induction on the structure of e .

CASE $e = x$

$\vee e = \lambda(x:\tau). e'$

$\vee e = \text{dyn } \tau e'$:

1. Contradiction by $\vdash_{\mathbb{F}} e$

CASE $e = i$

$\vee e = \lambda x. e'$

$\vee e = \text{mon}(\tau_d \Rightarrow \tau_c) v$:

1. QED e is a value

CASE $e = \text{Err}$:

1. $E = []$

2. QED $e = E[\text{Err}]$

CASE $e = \langle e_0, e_1 \rangle$:

IF $e_0 \notin v$:

1. $\vdash_{\mathbb{F}} e_0$

by *inversion*

2. $e_0 = E_0[e'_0]$

by the induction hypothesis (1)

3. $E = \langle E_0, e_1 \rangle$

4. QED $e = E[e'_0]$

12651	IF $e_0 \in v$	1. $\vdash_{\mathbb{F}} e_1$	12706
12652	$\wedge e_1 \notin v :$	by <i>inversion</i>	12707
12653	1. $\vdash_{\mathbb{F}} e_1$	2. $e_1 = E_1[e'_1]$	12708
12654	by <i>inversion</i>	by the induction hypothesis (1)	12709
12655	2. $e_1 = E_1[e'_1]$	3. $E = op^2 e_0 E_1$	12710
12656	by the induction hypothesis (1)	4. QED $e = E[e'_1]$	12711
12657	3. $E = \langle e_0, E_1 \rangle$	ELSE $e_0 \in v$	12712
12658	4. QED $e = E[e'_1]$	$\wedge e_1 \in v :$	12713
12659	ELSE $e_0 \in v$	1. $E = []$	12714
12660	$\wedge e_1 \in v :$	2. QED $e = E[op^2 e_0 e_1]$	12715
12661	1. $E = []$	CASE $e = \text{chk } \tau e_0 :$	12716
12662	2. QED e is a value	Contradiction by $\vdash_{\mathbb{F}} e$	12717
12663	CASE $e = e_0 e_1 :$	CASE $e = \text{stat } \tau e_0 :$	12718
12664	IF $e_0 \notin v :$	IF $e_0 \notin v :$	12719
12665	1. $\vdash_{\mathbb{F}} e_0$	1. $\vdash_{\mathbb{F}} e_0$	12720
12666	by <i>inversion</i>	by <i>inversion</i>	12721
12667	2. $e_0 = E_0[e'_0]$	2. $e_0 = E_0[e'_0]$	12722
12668	by the induction hypothesis (1)	by <i>unique static evaluation contexts</i> (1)	12723
12669	3. $E = E_0 e_1$	3. $E = \text{stat } \tau E_0$	12724
12670	4. QED $e = E[e'_0]$	4. QED $e = E[e'_0]$	12725
12671	IF $e_0 \in v$	ELSE $e_0 \in v :$	12726
12672	$\wedge e_1 \notin v :$	1. $E = []$	12727
12673	1. $\vdash_{\mathbb{F}} e_1$	2. QED $e = E[\text{stat } \tau e_0]$	12728
12674	by <i>inversion</i>	□	12729
12675	2. $e_1 = E_1[e'_1]$	Lemma 6.17 : HF <i>static hole typing</i>	12730
12676	by the induction hypothesis (1)	▮ If $\vdash_{\mathbb{F}} E^*[e] : \tau$ then the derivation contains a sub-term $\vdash_{\mathbb{F}} e : \tau'$	12731
12677	3. $E = e_0 E_1$	<i>Proof</i> :	12732
12678	4. QED $e = E[e'_1]$	By induction on the structure of E^* .	12733
12679	ELSE $e_0 \in v$	CASE $E^* = [] :$	12734
12680	$\wedge e_1 \in v :$	1. QED $E^*[e] = e$	12735
12681	1. $E = []$	CASE $E^* = E^*_0 e_1 :$	12736
12682	2. QED $e = E[e_0 e_1]$	1. $E^*[e] = E^*_0[e] e_1$	12737
12683	CASE $e = op^1 e_0 :$	2. $\vdash_{\mathbb{F}} E^*_0[e] : \tau_d \Rightarrow \tau_c$	12738
12684	IF $e_0 \notin v :$	by <i>inversion</i>	12739
12685	1. $\vdash_{\mathbb{F}} e_0$	3. QED by the induction hypothesis (2)	12740
12686	by <i>inversion</i>	CASE $E^* = v_0 E^*_1 :$	12741
12687	2. $e_0 = E_0[e'_0]$	1. $E^*[e] = v_0 E^*_1[e]$	12742
12688	by the induction hypothesis (1)	2. $\vdash_{\mathbb{F}} E^*_1[e] : \tau_d$	12743
12689	3. $E = op^1 E_0$	by <i>inversion</i>	12744
12690	4. QED $e = E[e'_0]$	3. QED by the induction hypothesis (2)	12745
12691	ELSE $e_0 \in v :$	CASE $E^* = \langle E^*_0, e_1 \rangle :$	12746
12692	1. $E = []$	1. $E^*[e] = \langle E^*_0[e], e_1 \rangle$	12747
12693	2. QED $e = E[op^1 e_0]$	2. $\vdash_{\mathbb{F}} E^*_0[e] : \tau_0$	12748
12694	CASE $e = op^2 e_0 e_1 :$	by <i>inversion</i>	12749
12695	IF $e_0 \notin v :$	3. QED by the induction hypothesis (2)	12750
12696	1. $\vdash_{\mathbb{F}} e_0$	CASE $E^* = \langle v_0, E^*_1 \rangle :$	12751
12697	by <i>inversion</i>	1. $E^*[e] = \langle v_0, E^*_1[e] \rangle$	12752
12698	2. $e_0 = E_0[e'_0]$	2. $\vdash_{\mathbb{F}} E^*_1[e] : \tau_1$	12753
12699	by the induction hypothesis (1)	by <i>inversion</i>	12754
12700	3. $E = op^2 E_0 e_1$	3. QED by the induction hypothesis (2)	12755
12701	4. QED $e = E[e'_0]$	CASE $E^* = op^1 E^*_0 :$	12756
12702	IF $e_0 \in v$	1. $E^*[e] = op^1 E^*_0[e]$	12757
12703	$\wedge e_1 \notin v :$		12758
12704			12759
12705			12760

12761 2. $\vdash_{\mathbb{F}} E^{\bullet}_0[e] : \tau_0$
 12762 by *inversion*
 12763 3. QED by the induction hypothesis (2)
 12764 **CASE** $E^{\bullet} = op^2 E^{\bullet}_0 e_1 :$
 12765 1. $E^{\bullet}[e] = op^2 E^{\bullet}_0[e] e_1$
 12766 2. $\vdash_{\mathbb{F}} E^{\bullet}_0[e] : \tau_0$
 12767 by *inversion*
 12768 3. QED by the induction hypothesis (2)
 12769 **CASE** $E^{\bullet} = op^2 v_0 E^{\bullet}_1 :$
 12770 1. $E^{\bullet}[e] = op^2 v_0 E^{\bullet}_1[e]$
 12771 2. $\vdash_{\mathbb{F}} E^{\bullet}_1[e] : \tau_1$
 12772 by *inversion*
 12773 3. QED by the induction hypothesis (2)
 12774 **CASE** $E^{\bullet} = chk \tau E^{\bullet}_0 :$
 12775 1. $E^{\bullet}[e] = chk \tau E^{\bullet}_0[e]$
 12776 2. $\vdash_{\mathbb{F}} E^{\bullet}_0[e] : \tau_0$
 12777 by *inversion*
 12778 3. QED by the induction hypothesis (2)
 12779 \square

12780 **Lemma 6.18** : HF *dynamic hole typing*

12781 If $\vdash_{\mathbb{F}} E^{\bullet}[e]$ then the derivation contains a sub-term $\vdash_{\mathbb{F}} e$

12782 *Proof*:

12783 By induction on the structure of E^{\bullet} .

12784 **CASE** $E^{\bullet} = [] :$

12785 1. QED $E^{\bullet}[e] = e$

12786 **CASE** $E^{\bullet} = E^{\bullet}_0 e_1 :$

12787 1. $E^{\bullet}[e] = E^{\bullet}_0[e] e_1$

12788 2. $\vdash_{\mathbb{F}} E^{\bullet}_0[e]$

12789 by *inversion*

12790 3. QED by the induction hypothesis (2)

12791 **CASE** $E^{\bullet} = v_0 E^{\bullet}_1 :$

12792 1. $E^{\bullet}[e] = v_0 E^{\bullet}_1[e]$

12793 2. $\vdash_{\mathbb{F}} E^{\bullet}_1[e]$

12794 by *inversion*

12795 3. QED by the induction hypothesis (2)

12796 **CASE** $E^{\bullet} = \langle E^{\bullet}_0, e_1 \rangle :$

12797 1. $E^{\bullet}[e] = \langle E^{\bullet}_0[e], e_1 \rangle$

12798 2. $\vdash_{\mathbb{F}} E^{\bullet}_0[e]$

12799 by *inversion*

12800 3. QED by the induction hypothesis (2)

12801 **CASE** $E^{\bullet} = \langle v_0, E^{\bullet}_1 \rangle :$

12802 1. $E^{\bullet}[e] = \langle v_0, E^{\bullet}_1[e] \rangle$

12803 2. $\vdash_{\mathbb{F}} E^{\bullet}_1[e]$

12804 by *inversion*

12805 3. QED by the induction hypothesis (2)

12806 **CASE** $E^{\bullet} = op^1 E^{\bullet}_0 :$

12807 1. $E^{\bullet}[e] = op^1 E^{\bullet}_0[e]$

12808 2. $\vdash_{\mathbb{F}} E^{\bullet}_0[e]$

12809 by *inversion*

12810 3. QED by the induction hypothesis (2)

12811 **CASE** $E^{\bullet} = op^2 E^{\bullet}_0 e_1 :$

12812 1. $E^{\bullet}[e] = op^2 E^{\bullet}_0[e] e_1$

12813
12814
12815

2. $\vdash_{\mathbb{F}} E^{\bullet}_0[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E^{\bullet} = op^2 v_0 E^{\bullet}_1 :$
 1. $E^{\bullet}[e] = op^2 v_0 E^{\bullet}_1[e]$
 2. $\vdash_{\mathbb{F}} E^{\bullet}_1[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)

\square

Lemma 6.19 : HF *boundary hole typing*

- If $\vdash_{\mathbb{F}} E[\text{dyn } \tau e] : \tau'$ then the derivation contains a sub-term $\vdash_{\mathbb{F}} \text{dyn } \tau e : \tau$
- If $\vdash_{\mathbb{F}} E[\text{dyn } \tau e]$ then the derivation contains a sub-term $\vdash_{\mathbb{F}} \text{dyn } \tau e : \tau$
- If $\vdash_{\mathbb{F}} E[\text{stat } \tau e] : \tau'$ then the derivation contains a sub-term $\vdash_{\mathbb{F}} \text{stat } \tau e$
- If $\vdash_{\mathbb{F}} E[\text{stat } \tau e]$ then the derivation contains a sub-term $\vdash_{\mathbb{F}} \text{stat } \tau e$

Proof:

By the following four lemmas: *static dyn hole typing*, *dynamic dyn hole typing*, *static stat hole typing*, and *dynamic stat hole typing*.

\square

Lemma 6.20 : HF *static dyn hole typing*

If $\vdash_{\mathbb{F}} E[\text{dyn } \tau e] : \tau'$ then the derivation contains a sub-term $\vdash_{\mathbb{F}} \text{dyn } \tau e : \tau$.

Proof:

By induction on the structure of E .

CASE $E \in E^{\bullet} :$

1. $\vdash_{\mathbb{F}} \text{dyn } \tau e : \tau''$

by *static hole typing*

2. $\vdash_{\mathbb{F}} \text{dyn } \tau e : \tau$

by *inversion* (1)

3. QED

CASE $E = E_0 e_1 :$

1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$

2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e] : \tau_0$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = v_0 E_1 :$

1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$

2. $\vdash_{\mathbb{F}} E_1[\text{dyn } \tau e] : \tau_1$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle :$

1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$

2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e] : \tau_0$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle v_0, E_1 \rangle :$

1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$

2. $\vdash_{\mathbb{F}} E_1[\text{dyn } \tau e] : \tau_1$

by *inversion*

12871 3. QED by the induction hypothesis (2)
 12872 **CASE** $E = op^1 E_0$:
 12873 1. $E[\text{dyn } \tau e] = op^1 E_0[\text{dyn } \tau e]$
 12874 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e] : \tau_0$
 12875 by *inversion*
 12876 3. QED by the induction hypothesis (2)
 12877 **CASE** $E = op^2 E_0 e_1$:
 12878 1. $E[\text{dyn } \tau e] = op^2 E_0[\text{dyn } \tau e] e_1$
 12879 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e] : \tau_0$
 12880 by *inversion*
 12881 3. QED by the induction hypothesis (2)
 12882 **CASE** $E = op^2 v_0 E_1$:
 12883 1. $E[\text{dyn } \tau e] = op^2 v_0 E_1[\text{dyn } \tau e]$
 12884 2. $\vdash_{\mathbb{F}} E_1[\text{dyn } \tau e] : \tau_1$
 12885 by *inversion*
 12886 3. QED by the induction hypothesis (2)
 12887 **CASE** $E = \text{chk } \tau'' E_0$:
 12888 1. $E[\text{dyn } \tau e] = \text{chk } \tau'' E_0[\text{dyn } \tau e]$
 12889 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e] : \tau_0$
 12890 by *inversion*
 12891 3. QED by the induction hypothesis (2)
 12892 **CASE** $E = \text{dyn } \tau_0 E_0$:
 12893 1. $E[\text{dyn } \tau e] = \text{dyn } \tau_0 E_0[\text{dyn } \tau e]$
 12894 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e]$
 12895 by *inversion*
 12896 3. QED by *dynamic dyn hole typing* (2)
 12897 **CASE** $E = \text{stat } \tau_0 E_0$:
 12898 1. Contradiction by $\vdash_{\mathbb{F}} E[\text{dyn } \tau e] : \tau'$
 12899 \square
 12900 **Lemma 6.21** : HF *dynamic dyn hole typing*
 12901 If $\vdash_{\mathbb{F}} E[\text{dyn } \tau e]$ then the derivation contains a sub-term
 12902 $\vdash_{\mathbb{F}} \text{dyn } \tau e : \tau$.
 12903 *Proof*:
 12904 By induction on the structure of E .
 12905 **CASE** $E \in E^*$:
 12906 1. Contradiction by $\vdash_{\mathbb{F}} E[\text{dyn } \tau e]$
 12907 **CASE** $E = E_0 e_1$:
 12908 1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
 12909 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e]$
 12910 by *inversion*
 12911 3. QED by the induction hypothesis (2)
 12912 **CASE** $E = v_0 E_1$:
 12913 1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
 12914 2. $\vdash_{\mathbb{F}} E_1[\text{dyn } \tau e]$
 12915 by *inversion*
 12916 3. QED by the induction hypothesis (2)
 12917 **CASE** $E = \langle E_0, e_1 \rangle$:
 12918 1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$
 12919 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e]$
 12920 by *inversion*
 12921 3. QED by the induction hypothesis (2)
 12922 **CASE** $E = \langle v_0, E_1 \rangle$:
 12923 1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$
 12924
 12925

2. $\vdash_{\mathbb{F}} E_1[\text{dyn } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^1 E_0$:
 1. $E[\text{dyn } \tau e] = op^1 E_0[\text{dyn } \tau e]$
 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 E_0 e_1$:
 1. $E[\text{dyn } \tau e] = op^2 E_0[\text{dyn } \tau e] e_1$
 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 v_0 E_1$:
 1. $E[\text{dyn } \tau e] = op^2 v_0 E_1[\text{dyn } \tau e]$
 2. $\vdash_{\mathbb{F}} E_1[\text{dyn } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{chk } \tau'' E_0$:
 1. Contradiction by $\vdash_{\mathbb{F}} E[\text{dyn } \tau e]$
 \square
CASE $E = \text{dyn } \tau E_0$:
 1. Contradiction by $\vdash_{\mathbb{F}} E[\text{dyn } \tau e]$
CASE $E = \text{stat } \tau_0 E_0$:
 1. $E[\text{dyn } \tau e] = \text{stat } \tau_0 E_0[\text{dyn } \tau e]$
 2. $\vdash_{\mathbb{F}} E_0[\text{dyn } \tau e] : \tau_0$
 by *inversion*
 3. QED by *static dyn hole typing* (2)
 }
Lemma 6.22 : HF *static stat hole typing*
 If $\vdash_{\mathbb{F}} E[\text{stat } \tau e] : \tau'$ then the derivation contains a sub-term
 $\vdash_{\mathbb{F}} \text{stat } \tau e$.
Proof:
 By induction on the structure of E .
CASE $E \in E^*$:
 1. Contradiction by $\vdash_{\mathbb{F}} E[\text{stat } \tau e] : \tau'$
CASE $E = E_0 e_1$:
 1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$
 2. $\vdash_{\mathbb{F}} E_0[\text{stat } \tau e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = v_0 E_1$:
 1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$
 2. $\vdash_{\mathbb{F}} E_1[\text{stat } \tau e] : \tau_1$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle E_0, e_1 \rangle$:
 1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$
 2. $\vdash_{\mathbb{F}} E_0[\text{stat } \tau e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle v_0, E_1 \rangle$:
 1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$
 12926
 12927
 12928
 12929
 12930
 12931
 12932
 12933
 12934
 12935
 12936
 12937
 12938
 12939
 12940
 12941
 12942
 12943
 12944
 12945
 12946
 12947
 12948
 12949
 12950
 12951
 12952
 12953
 12954
 12955
 12956
 12957
 12958
 12959
 12960
 12961
 12962
 12963
 12964
 12965
 12966
 12967
 12968
 12969
 12970
 12971
 12972
 12973
 12974
 12975
 12976
 12977
 12978
 12979
 12980

12981 2. $\vdash_F E_1[\text{stat } \tau e] : \tau_1$
 12982 by *inversion*
 12983 3. QED by the induction hypothesis (2)
 12984 **CASE** $E = \text{op}^1 E_0$:
 12985 1. $E[\text{stat } \tau e] = \text{op}^1 E_0[\text{stat } \tau e]$
 12986 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 12987 by *inversion*
 12988 3. QED by the induction hypothesis (2)
 12989 **CASE** $E = \text{op}^2 E_0 e_1$:
 12990 1. $E[\text{stat } \tau e] = \text{op}^2 E_0[\text{stat } \tau e] e_1$
 12991 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 12992 by *inversion*
 12993 3. QED by the induction hypothesis (2)
 12994 **CASE** $E = \text{op}^2 v_0 E_1$:
 12995 1. $E[\text{stat } \tau e] = \text{op}^2 v_0 E_1[\text{stat } \tau e]$
 12996 2. $\vdash_F E_1[\text{stat } \tau e] : \tau_1$
 12997 by *inversion*
 12998 3. QED by the induction hypothesis (2)
 12999 **CASE** $E = \text{chk } \tau'' E_0$:
 13000 1. $E[\text{stat } \tau e] = \text{chk } \tau'' E_0[\text{stat } \tau e]$
 13001 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 13002 by *inversion*
 13003 3. QED by the induction hypothesis (2)
 13004 **CASE** $E = \text{dyn } \tau_0 E_0$:
 13005 1. $E[\text{stat } \tau e] = \text{dyn } \tau_0 E_0[\text{stat } \tau e]$
 13006 2. $\vdash_F E_0[\text{stat } \tau e]$
 13007 by *inversion*
 13008 3. QED by *dynamic stat hole typing* (2)
 13009 **CASE** $E = \text{stat } \tau_0 E_0$:
 13010 1. Contradiction by $\vdash_F E[\text{stat } \tau e] : \tau'$
 13011 \square
 13012 **Lemma 6.23** : HF *dynamic stat hole typing*
 13013 If $\vdash_F E[\text{stat } \tau e]$ then the derivation contains a sub-term \vdash_F
 13014 $\text{stat } \tau e$.
 13015 *Proof*:
 13016 By induction on the structure of E .
 13017 **CASE** $E \in E^\bullet$:
 13018 1. QED by *dynamic hole typing*
 13019 **CASE** $E = E_0 e_1$:
 13020 1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$
 13021 2. $\vdash_F E_0[\text{stat } \tau e]$
 13022 by *inversion*
 13023 3. QED by the induction hypothesis (2)
 13024 **CASE** $E = v_0 E_1$:
 13025 1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$
 13026 2. $\vdash_F E_1[\text{stat } \tau e]$
 13027 by *inversion*
 13028 3. QED by the induction hypothesis (2)
 13029 **CASE** $E = \langle E_0, e_1 \rangle$:
 13030 1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$
 13031 2. $\vdash_F E_0[\text{stat } \tau e]$
 13032 by *inversion*
 13033 3. QED by the induction hypothesis (2)
 13034 **CASE** $E = \langle v_0, E_1 \rangle$:

1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$
 2. $\vdash_F E_1[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{op}^1 E_0$:
 1. $E[\text{stat } \tau e] = \text{op}^1 E_0[\text{stat } \tau e]$
 2. $\vdash_F E_0[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{op}^2 E_0 e_1$:
 1. $E[\text{stat } \tau e] = \text{op}^2 E_0[\text{stat } \tau e] e_1$
 2. $\vdash_F E_0[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{op}^2 v_0 E_1$:
 1. $E[\text{stat } \tau e] = \text{op}^2 v_0 E_1[\text{stat } \tau e]$
 2. $\vdash_F E_1[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{chk } \tau'' E_0$:
 1. Contradiction by $\vdash_F E[\text{stat } \tau e]$
CASE $E = \text{dyn } \tau E_0$:
 1. Contradiction by $\vdash_F E[\text{stat } \tau e]$
CASE $E = \text{stat } \tau_0 E_0$:
 1. $E[\text{stat } \tau e] = \text{stat } \tau_0 E_0[\text{stat } \tau e]$
 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 by *inversion*
 3. QED by *static stat hole typing* (2)

 \square **Lemma 6.24** : HF *static boundary-free hole substitution*

If $\vdash_F E^\bullet[e] : \tau$ and the derivation contains a sub-term $\vdash_F e : \tau'$
 and $\vdash_F e' : \tau'$ then $\vdash_F E^\bullet[e'] : \tau$.

Proof:By induction on the structure of E^\bullet **CASE** $E^\bullet = []$:1. $E^\bullet[e] = e$ $\wedge E^\bullet[e'] = e'$ 2. $\vdash_F e : \tau$

by (1)

3. $\tau' = \tau$ 4. $\vdash_F e' : \tau$

5. QED by (1, 4)

CASE $E^\bullet = E^\bullet_0 e_1$:1. $E^\bullet[e] = E^\bullet_0[e] e_1$ $\wedge E^\bullet[e'] = E^\bullet_0[e'] e_1$ 2. $\vdash_F E^\bullet_0[e] e_1 : \tau$ 3. $\vdash_F E^\bullet_0[e] : \tau_0$ $\wedge \vdash_F e_1 : \tau_1$ by *inversion*4. $\vdash_F E^\bullet_0[e'] : \tau_0$

by the induction hypothesis (3)

5. $\vdash_F E^\bullet_0[e'] e_1 : \tau$

by (2, 3, 4)

13091	6. QED by (1, 5)	3. $\vdash_F E^\bullet_0[e] : \tau_0$	13146
13092	CASE $E^\bullet = v_0 E^\bullet_1 :$	$\wedge \vdash_F e_1 : \tau_1$	13147
13093	1. $E^\bullet[e] = v_0 E^\bullet_1[e]$	by <i>inversion</i>	13148
13094	$\wedge E^\bullet[e'] = v_0 E^\bullet_1[e']$	4. $\vdash_F E^\bullet_0[e'] : \tau_0$	13149
13095	2. $\vdash_F v_0 E^\bullet_1[e] : \tau$	by the induction hypothesis (3)	13150
13096	3. $\vdash_F v_0 : \tau_0$	5. $\vdash_F op^2 E^\bullet_0[e'] e_1 : \tau$	13151
13097	$\wedge \vdash_F E^\bullet_1[e] : \tau_1$	by (2, 3, 4)	13152
13098	by <i>inversion</i>	6. QED by (1, 5)	13153
13099	4. $\vdash_F E^\bullet_1[e'] : \tau_1$	CASE $E^\bullet = op^2 v_0 E^\bullet_1 :$	13154
13100	by the induction hypothesis (3)	1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$	13155
13101	5. $\vdash_F v_0 E^\bullet_1[e'] : \tau$	$\wedge E^\bullet[e'] = op^2 v_0 E^\bullet_1[e']$	13156
13102	by (2, 3, 4)	2. $\vdash_F op^2 v_0 E^\bullet_1[e] : \tau$	13157
13103	6. QED by (1, 5)	3. $\vdash_F v_0 : \tau_0$	13158
13104	CASE $E^\bullet = op^1 E^\bullet_0 :$	$\wedge \vdash_F E^\bullet_1[e] : \tau_1$	13159
13105	1. $E^\bullet[e] = op^1 E^\bullet_0[e]$	by <i>inversion</i>	13160
13106	$\wedge E^\bullet[e'] = op^1 E^\bullet_0[e']$	4. $\vdash_F E^\bullet_1[e'] : \tau_1$	13161
13107	2. $\vdash_F op^1 E^\bullet_0[e] : \tau$	by the induction hypothesis (3)	13162
13108	3. $\vdash_F E^\bullet_0[e] : \tau_0$	5. $\vdash_F op^2 v_0 E^\bullet_1[e'] : \tau$	13163
13109	by <i>inversion</i>	by (2, 3, 4)	13164
13110	4. $\vdash_F E^\bullet_0[e'] : \tau_0$	6. QED by (1, 5)	13165
13111	by the induction hypothesis (3)	CASE $E^\bullet = chk \tau'' E^\bullet_0 :$	13166
13112	5. $\vdash_F op^1 E^\bullet_0[e'] : \tau$	1. $E^\bullet[e] = chk \tau'' E^\bullet_0[e]$	13167
13113	by (2, 3, 4)	$\wedge E^\bullet[e'] = chk \tau'' E^\bullet_0[e']$	13168
13114	6. QED by (1, 5)	2. $\vdash_F chk \tau'' E^\bullet_0[e] : \tau$	13169
13115	CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$	3. $\vdash_F E^\bullet_0[e] : \tau_0$	13170
13116	1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$	by <i>inversion</i>	13171
13117	$\wedge E^\bullet[e'] = \langle E^\bullet_0[e'], e_1 \rangle$	4. $\vdash_F E^\bullet_0[e'] : \tau_0$	13172
13118	2. $\vdash_F \langle E^\bullet_0[e], e_1 \rangle : \tau$	by the induction hypothesis (3)	13173
13119	3. $\vdash_F E^\bullet_0[e] : \tau_0$	5. $\vdash_F chk \tau'' E^\bullet_0[e'] : \tau$	13174
13120	$\wedge \vdash_F e_1 : \tau_1$	by (2, 3, 4)	13175
13121	by <i>inversion</i>	6. QED by (1, 5)	13176
13122	4. $\vdash_F E^\bullet_0[e'] : \tau_0$	□	13177
13123	by the induction hypothesis (3)	Lemma 6.25 : HF <i>dynamic hole substitution</i>	13178
13124	5. $\vdash_F \langle E^\bullet_0[e'], e_1 \rangle : \tau$	■ If $\vdash_F E^\bullet[e]$ and $\vdash_F e'$ then $\vdash_F E^\bullet[e']$	13179
13125	by (2, 3, 4)	<i>Proof</i> :	13180
13126	6. QED by (1, 5)	By induction on the structure of E^\bullet	13181
13127	CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$	CASE $E^\bullet = [] :$	13182
13128	1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$	1. QED $E^\bullet[e'] = e'$	13183
13129	$\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$	CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$	13184
13130	2. $\vdash_F \langle v_0, E^\bullet_1[e] \rangle : \tau$	1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$	13185
13131	3. $\vdash_F v_0 : \tau_0$	$\wedge E^\bullet[e'] = \langle E^\bullet_0[e'], e_1 \rangle$	13186
13132	$\wedge \vdash_F E^\bullet_1[e] : \tau_1$	2. $\vdash_F \langle E^\bullet_0[e], e_1 \rangle$	13187
13133	by <i>inversion</i>	3. $\vdash_F E^\bullet_0[e]$	13188
13134	4. $\vdash_F E^\bullet_1[e'] : \tau_1$	$\wedge \vdash_F e_1$	13189
13135	by the induction hypothesis (3)	by <i>inversion</i>	13190
13136	5. $\vdash_F \langle v_0, E^\bullet_1[e'] \rangle : \tau$	4. $\vdash_F E^\bullet_0[e']$	13191
13137	by (2, 3, 4)	by the induction hypothesis (3)	13192
13138	6. QED by (1, 5)	5. $\vdash_F \langle E^\bullet_0[e'], e_1 \rangle$	13193
13139	CASE $E^\bullet = op^2 E^\bullet_0 e_1 :$	by (3, 4)	13194
13140	1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$	6. QED by (1, 5)	13195
13141	$\wedge E^\bullet[e'] = op^2 E^\bullet_0[e'] e_1$	CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$	13196
13142	2. $\vdash_F op^2 E^\bullet_0[e] e_1 : \tau$	1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$	13197
13143		$\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$	13198
13144			13199
13145			13200

13201	2. $\vdash_{\mathbb{F}} \langle v_0, E^{\bullet}_1[e] \rangle$	5. $\vdash_{\mathbb{F}} op^2 E^{\bullet}_0[e'] e_1$	13256
13202	3. $\vdash_{\mathbb{F}} v_0$	by (3, 4)	13257
13203	$\wedge \vdash_{\mathbb{F}} E^{\bullet}_1[e]$	6. QED by (1, 5)	13258
13204	by <i>inversion</i>	CASE $E^{\bullet} = op^2 v_0 E^{\bullet}_1 :$	13259
13205	4. $\vdash_{\mathbb{F}} E^{\bullet}_1[e']$	1. $E^{\bullet}[e] = op^2 v_0 E^{\bullet}_1[e]$	13260
13206	by the induction hypothesis (3)	$\wedge E^{\bullet}[e'] = op^2 v_0 E^{\bullet}_1[e']$	13261
13207	5. $\vdash_{\mathbb{F}} \langle v_0, E^{\bullet}_1[e'] \rangle$	2. $\vdash_{\mathbb{F}} op^2 v_0 E^{\bullet}_1[e']$	13262
13208	by (3, 4)	3. $\vdash_{\mathbb{F}} v_0$	13263
13209	6. QED by (1, 5)	$\wedge \vdash_{\mathbb{F}} E^{\bullet}_1[e]$	13264
13210	CASE $E^{\bullet} = E^{\bullet}_0 e_1 :$	by <i>inversion</i>	13265
13211	1. $E^{\bullet}[e] = E^{\bullet}_0[e] e_1$	4. $\vdash_{\mathbb{F}} E^{\bullet}_1[e']$	13266
13212	$\wedge E^{\bullet}[e'] = E^{\bullet}_0[e'] e_1$	by the induction hypothesis (3)	13267
13213	2. $\vdash_{\mathbb{F}} E^{\bullet}_0[e] e_1$	5. $\vdash_{\mathbb{F}} op^2 v_0 E^{\bullet}_1[e']$	13268
13214	3. $\vdash_{\mathbb{F}} E^{\bullet}_0[e]$	by (3, 4)	13269
13215	$\wedge \vdash_{\mathbb{F}} e_1$	6. QED by (1, 5)	13270
13216	by <i>inversion</i>	CASE $E^{\bullet} = chk \tau_0 E^{\bullet}_0 :$	13271
13217	4. $\vdash_{\mathbb{F}} E^{\bullet}_0[e']$	1. Contradiction by $\vdash_{\mathbb{F}} E^{\bullet}[e]$	13272
13218	by the induction hypothesis (3)	□	13273
13219	5. $\vdash_{\mathbb{F}} E^{\bullet}_0[e'] e_1$		13274
13220	by (3, 4)	Lemma 6.26 : HF <i>hole substitution</i>	13275
13221	6. QED by (1, 5)	• If $\vdash_{\mathbb{F}} E[e]$ and the derivation contains a sub-term $\vdash_{\mathbb{F}} e : \tau'$	13276
13222	CASE $E^{\bullet} = v_0 E^{\bullet}_1 :$	and $\vdash_{\mathbb{F}} e' : \tau'$ then $\vdash_{\mathbb{F}} E[e']$.	13277
13223	1. $E^{\bullet}[e] = v_0 E^{\bullet}_1[e]$	• If $\vdash_{\mathbb{F}} E[e]$ and the derivation contains a sub-term $\vdash_{\mathbb{F}} e$ and	13278
13224	$\wedge E^{\bullet}[e'] = v_0 E^{\bullet}_1[e']$	$\vdash_{\mathbb{F}} e'$ then $\vdash_{\mathbb{F}} E[e']$.	13279
13225	2. $\vdash_{\mathbb{F}} v_0 E^{\bullet}_1[e]$	• If $\vdash_{\mathbb{F}} E[e] : \tau$ and the derivation contains a sub-term $\vdash_{\mathbb{F}} e : \tau'$	13280
13226	3. $\vdash_{\mathbb{F}} v_0$	and $\vdash_{\mathbb{F}} e' : \tau'$ then $\vdash_{\mathbb{F}} E[e'] : \tau$.	13281
13227	$\wedge \vdash_{\mathbb{F}} E^{\bullet}_1[e]$	• If $\vdash_{\mathbb{F}} E[e] : \tau$ and the derivation contains a sub-term $\vdash_{\mathbb{F}} e$	13282
13228	by <i>inversion</i>	and $\vdash_{\mathbb{F}} e'$ then $\vdash_{\mathbb{F}} E[e'] : \tau$.	13283
13229	4. $\vdash_{\mathbb{F}} E^{\bullet}_1[e']$	<i>Proof</i> :	13284
13230	by the induction hypothesis (3)	By the following four lemmas: <i>dynamic context static hole</i>	13285
13231	5. $\vdash_{\mathbb{F}} v_0 E^{\bullet}_1[e']$	<i>substitution</i> , <i>dynamic context dynamic hole substitution</i> ,	13286
13232	by (3, 4)	<i>static context static hole substitution</i> , and <i>static context</i>	13287
13233	6. QED by (1, 5)	<i>dynamic hole substitution</i> .	13288
13234	CASE $E^{\bullet} = op^1 E^{\bullet}_0 :$	□	13289
13235	1. $E^{\bullet}[e] = op^1 E^{\bullet}_0[e]$	Lemma 6.27 : HF <i>dynamic context static hole substitution</i>	13290
13236	$\wedge E^{\bullet}[e'] = op^1 E^{\bullet}_0[e']$	If $\vdash_{\mathbb{F}} E[e]$ and contains $\vdash_{\mathbb{F}} e : \tau'$, and furthermore $\vdash_{\mathbb{F}} e' : \tau'$,	13291
13237	2. $\vdash_{\mathbb{F}} op^1 E^{\bullet}_0[e]$	then $\vdash_{\mathbb{F}} E[e']$	13292
13238	3. $\vdash_{\mathbb{F}} E^{\bullet}_0[e]$	<i>Proof</i> :	13293
13239	by <i>inversion</i>	By induction on the structure of E .	13294
13240	4. $\vdash_{\mathbb{F}} E^{\bullet}_0[e']$	CASE $E \in E^{\bullet} :$	13295
13241	by the induction hypothesis (3)	1. Contradiction by $\vdash_{\mathbb{F}} E[e]$	13296
13242	5. $\vdash_{\mathbb{F}} op^1 E^{\bullet}_0[e']$	CASE $E = E_0 e_1 :$	13297
13243	by (4)	1. $E[e] = E_0[e] e_1$	13298
13244	6. QED by (1, 5)	2. $\vdash_{\mathbb{F}} E_0[e]$	13299
13245	CASE $E^{\bullet} = op^2 E^{\bullet}_0 e_1 :$	by <i>inversion</i>	13300
13246	1. $E^{\bullet}[e] = op^2 E^{\bullet}_0[e] e_1$	3. QED by the induction hypothesis (2)	13301
13247	$\wedge E^{\bullet}[e'] = op^2 E^{\bullet}_0[e'] e_1$	CASE $E = v_0 E_1 :$	13302
13248	2. $\vdash_{\mathbb{F}} op^2 E^{\bullet}_0[e] e_1$	1. $E[e] = v_0 E_1[e]$	13303
13249	3. $\vdash_{\mathbb{F}} E^{\bullet}_0[e]$	2. $\vdash_{\mathbb{F}} E_1[e]$	13304
13250	$\wedge \vdash_{\mathbb{F}} e_1$	by <i>inversion</i>	13305
13251	by <i>inversion</i>	3. QED by the induction hypothesis (2)	13306
13252	4. $\vdash_{\mathbb{F}} E^{\bullet}_0[e']$	CASE $E = \langle E_0, e_1 \rangle :$	13307
13253	by the induction hypothesis (3)	1. $E[e] = \langle E_0[e], e_1 \rangle$	13308
13254			13309
13255			13310

13311 2. $\vdash_{\mathbb{F}} E_0[e]$
 13312 by *inversion*
 13313 3. QED by the induction hypothesis (2)
 13314 **CASE** $E = \langle v_0, E_1 \rangle :$
 13315 1. $E[e] = \langle v_0, E_1[e] \rangle$
 13316 2. $\vdash_{\mathbb{F}} E_1[e]$
 13317 by *inversion*
 13318 3. QED by the induction hypothesis (2)
 13319 **CASE** $E = op^1 E_0 :$
 13320 1. $E[e] = op^1 E_0[e]$
 13321 2. $\vdash_{\mathbb{F}} E_0[e]$
 13322 by *inversion*
 13323 3. QED by the induction hypothesis (2)
 13324 **CASE** $E = op^2 E_0 e_1 :$
 13325 1. $E[e] = op^2 E_0[e] e_1$
 13326 2. $\vdash_{\mathbb{F}} E_0[e]$
 13327 by *inversion*
 13328 3. QED by the induction hypothesis (2)
 13329 **CASE** $E = op^2 v_0 E_1 :$
 13330 1. $E[e] = op^2 v_0 E_1[e]$
 13331 2. $\vdash_{\mathbb{F}} E_1[e]$
 13332 by *inversion*
 13333 3. QED by the induction hypothesis (2)
 13334 **CASE** $E = \text{chk } \tau'' E_0 :$
 13335 1. $E[e] = \text{chk } \tau'' E_0[e]$
 13336 2. $\vdash_{\mathbb{F}} E_0[e]$
 13337 by *inversion*
 13338 3. QED by the induction hypothesis (2)
 13339 **CASE** $E = \text{dyn } \tau'' E_0 :$
 13340 1. Contradiction by $\vdash_{\mathbb{F}} E[e]$
 13341 **CASE** $E = \text{stat } \tau_0 E_0 :$
 13342 1. $E[e] = \text{stat } \tau_0 E_0[e]$
 13343 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 13344 by *inversion*
 13345 3. QED by *static context static hole substitution* (2)
 13346 \square
 13347 **Lemma 6.28** : HF *dynamic context dynamic hole substitution*
 13348 If $\vdash_{\mathbb{F}} E[e]$ and contains $\vdash_{\mathbb{F}} e$, and furthermore $\vdash_{\mathbb{F}} e'$, then $\vdash_{\mathbb{F}} E[e']$
 13349 *Proof*:
 13350 By induction on the structure of E .
 13351 **CASE** $E \in E^* :$
 13352 1. QED by *dynamic boundary-free hole substitution*
 13353 **CASE** $E = E_0 e_1 :$
 13354 1. $E[e] = E_0[e] e_1$
 13355 2. $\vdash_{\mathbb{F}} E_0[e]$
 13356 by *inversion*
 13357 3. QED by the induction hypothesis (2)
 13358 **CASE** $E = v_0 E_1 :$
 13359 1. $E[e] = v_0 E_1[e]$
 13360 2. $\vdash_{\mathbb{F}} E_1[e]$
 13361 by *inversion*
 13362 3. QED by the induction hypothesis (2)
 13363 **CASE** $E = \langle E_0, e_1 \rangle :$
 13364
 13365

1. $E[e] = \langle E_0[e], e_1 \rangle$
 2. $\vdash_{\mathbb{F}} E_0[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle v_0, E_1 \rangle :$
 1. $E[e] = \langle v_0, E_1[e] \rangle$
 2. $\vdash_{\mathbb{F}} E_1[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^1 E_0 :$
 1. $E[e] = op^1 E_0[e]$
 2. $\vdash_{\mathbb{F}} E_0[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 E_0 e_1 :$
 1. $E[e] = op^2 E_0[e] e_1$
 2. $\vdash_{\mathbb{F}} E_0[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 v_0 E_1 :$
 1. $E[e] = op^2 v_0 E_1[e]$
 2. $\vdash_{\mathbb{F}} E_1[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{chk } \tau'' E_0 :$
 1. Contradiction by $\vdash_{\mathbb{F}} E[e]$
CASE $E = \text{dyn } \tau'' E_0 :$
 1. Contradiction by $\vdash_{\mathbb{F}} E[e]$
CASE $E = \text{stat } \tau_0 E_0 :$
 1. $E[e] = \text{stat } \tau_0 E_0[e]$
 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 by *inversion*
 3. QED by *static context dynamic hole substitution* (2)
 \square
Lemma 6.29 : HF *static context static hole substitution*
 If $\vdash_{\mathbb{F}} E[e] : \tau$ and contains $\vdash_{\mathbb{F}} e : \tau'$, and furthermore $\vdash_{\mathbb{F}} e' : \tau'$,
 then $\vdash_{\mathbb{F}} E[e'] : \tau$
Proof:
 By induction on the structure of E .
CASE $E \in E^* :$
 1. QED by *static boundary-free hole substitution*
CASE $E = E_0 e_1 :$
 1. $E[e] = E_0[e] e_1$
 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = v_0 E_1 :$
 1. $E[e] = v_0 E_1[e]$
 2. $\vdash_{\mathbb{F}} E_1[e] : \tau_1$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle E_0, e_1 \rangle :$
 1. $E[e] = \langle E_0[e], e_1 \rangle$

13421 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 13422 by *inversion*
 13423 3. QED by the induction hypothesis (2)
 13424 **CASE** $E = \langle v_0, E_1 \rangle :$
 13425 1. $E[e] = \langle v_0, E_1[e] \rangle$
 13426 2. $\vdash_{\mathbb{F}} E_1[e] : \tau_1$
 13427 by *inversion*
 13428 3. QED by the induction hypothesis (2)
 13429 **CASE** $E = op^1 E_0 :$
 13430 1. $E[e] = op^1 E_0[e]$
 13431 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 13432 by *inversion*
 13433 3. QED by the induction hypothesis (2)
 13434 **CASE** $E = op^2 E_0 e_1 :$
 13435 1. $E[e] = op^2 E_0[e] e_1$
 13436 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 13437 by *inversion*
 13438 3. QED by the induction hypothesis (2)
 13439 **CASE** $E = op^2 v_0 E_1 :$
 13440 1. $E[e] = op^2 v_0 E_1[e]$
 13441 2. $\vdash_{\mathbb{F}} E_1[e] : \tau_1$
 13442 by *inversion*
 13443 3. QED by the induction hypothesis (2)
 13444 **CASE** $E = \text{chk } \tau'' E_0 :$
 13445 1. $E[e] = \text{chk } \tau'' E_0[e]$
 13446 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 13447 by *inversion*
 13448 3. QED by the induction hypothesis (2)
 13449 **CASE** $E = \text{dyn } \tau_0 E_0 :$
 13450 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 13451 2. $\vdash_{\mathbb{F}} E_0[e]$
 13452 by *inversion*
 13453 3. QED by *static dyn hole typing* (2)
 13454 **CASE** $E = \text{stat } \tau_0 E_0 :$
 13455 1. Contradiction by $\vdash_{\mathbb{F}} E[e] : \tau$
 13456 \square
 13457 **Lemma 6.30** : HF *static context dynamic hole substitution*
 13458 If $\vdash_{\mathbb{F}} E[e] : \tau$ and contains $\vdash_{\mathbb{F}} e$, and furthermore $\vdash_{\mathbb{F}} e'$, then
 13459 $\vdash_{\mathbb{F}} E[e'] : \tau$
 13460 *Proof*:
 13461 By induction on the structure of E .
 13462 **CASE** $E \in E^* :$
 13463 1. Contradiction by $\vdash_{\mathbb{F}} E[e] : \tau$
 13464 **CASE** $E = E_0 e_1 :$
 13465 1. $E[e] = E_0[e] e_1$
 13466 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 13467 by *inversion*
 13468 3. QED by the induction hypothesis (2)
 13469 **CASE** $E = v_0 E_1 :$
 13470 1. $E[e] = v_0 E_1[e]$
 13471 2. $\vdash_{\mathbb{F}} E_1[e] : \tau_1$
 13472 by *inversion*
 13473 3. QED by the induction hypothesis (2)
 13474
 13475

CASE $E = \langle E_0, e_1 \rangle :$
 1. $E[e] = \langle E_0[e], e_1 \rangle$
 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle v_0, E_1 \rangle :$
 1. $E[e] = \langle v_0, E_1[e] \rangle$
 2. $\vdash_{\mathbb{F}} E_1[e] : \tau_1$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^1 E_0 :$
 1. $E[e] = op^1 E_0[e]$
 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^1 E_0[e] :$
 1. $E[e] = op^1 E_0[e]$
 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 E_0 e_1 :$
 1. $E[e] = op^2 E_0[e] e_1$
 2. $\vdash_{\mathbb{F}} E_0[e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 v_0 E_1 :$
 1. $E[e] = op^2 v_0 E_1[e]$
 2. $\vdash_{\mathbb{F}} E_1[e] : \tau_1$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{chk } \tau'' E_0 :$
 1. Contradiction by $\vdash_{\mathbb{F}} E[e] : \tau$
CASE $E = \text{dyn } \tau_0 E_0 :$
 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 2. $\vdash_{\mathbb{F}} E_0[e]$
 by *inversion*
 3. QED by *dynamic stat hole typing* (2)
CASE $E = \text{stat } \tau_0 E_0 :$
 1. Contradiction by $\vdash_{\mathbb{F}} E[e] : \tau$
 \square

Lemma 6.31 : $\vdash_{\mathbb{F}}$ *static inversion*

- 13531 • If $\Gamma \vdash_F x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$
- 13532 • If $\Gamma \vdash_F \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash_F e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$
- 13533
- 13534 • If $\Gamma \vdash_F \langle e_0, e_1 \rangle : \tau_0 \times \tau_1$ then $\Gamma \vdash_F e_0 : \tau'_0$ and $\Gamma \vdash_F e_1 : \tau'_1$ and $\tau'_0 \leq \tau_0$ and $\tau'_1 \leq \tau_1$
- 13535
- 13536 • If $\Gamma \vdash_F e_0 e_1 : \tau_c$ then $\Gamma \vdash_F e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash_F e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$
- 13537
- 13538 • If $\Gamma \vdash_F \text{fst } e : \tau$ then $\Gamma \vdash_F e : \tau_0 \times \tau_1$ and $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$
- 13539
- 13540 • If $\Gamma \vdash_F \text{snd } e : \tau$ then $\Gamma \vdash_F e : \tau_0 \times \tau_1$ and $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$
- 13541
- 13542 • If $\Gamma \vdash_F \text{op}^2 e_0 e_1 : \tau$ then $\Gamma \vdash_F e_0 : \tau_0$ and $\Gamma \vdash_F e_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$
- 13543
- 13544 • If $\Gamma \vdash_F \text{mon } \tau'_0 \times \tau'_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$ then either:
- 13545 – $\Gamma \vdash_F \langle v_0, v_1 \rangle$
- 13546 – or $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau$
- 13547 • If $\Gamma \vdash_F \text{mon } \tau'_d \Rightarrow \tau'_c \lambda x. e : \tau_d \Rightarrow \tau_c$ then $\Gamma \vdash_F \lambda x. e$ and $\tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- 13548
- 13549 • If $\Gamma \vdash_F \text{mon } \tau'_d \Rightarrow \tau'_c \lambda(x : \tau'_d). e : \tau_d \Rightarrow \tau_c$ then $\Gamma \vdash_F \lambda(x : \tau_x). e : \tau'_d \Rightarrow \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- 13550
- 13551 • If $\Gamma \vdash_F \text{dyn } \tau' e' : \tau$ then $\Gamma \vdash_F e'$ and $\tau' \leq \tau$
- 13552 • If $\Gamma \vdash_F \text{chk } \tau e' : \tau$ then $\Gamma \vdash_F e' : \tau'$

Proof:

QED by the definition of $\Gamma \vdash_F e : \tau$

□

Lemma 6.32 : \vdash_F *dynamic inversion*

- 13556 • If $\Gamma \vdash_F x$ then $x \in \Gamma$
- 13557
- 13558 • If $\Gamma \vdash_F \lambda x. e'$ then $x, \Gamma \vdash_F e'$
- 13559
- 13560 • If $\Gamma \vdash_F \langle e_0, e_1 \rangle$ then $\Gamma \vdash_F e_0$ and $\Gamma \vdash_F e_1$
- 13561
- 13562 • If $\Gamma \vdash_F \text{op}^1 e_0$ then $\Gamma \vdash_F e_0$
- 13563
- 13564 • If $\Gamma \vdash_F \text{op}^2 e_0 e_1$ then $\Gamma \vdash_F e_0$ and $\Gamma \vdash_F e_1$
- 13565
- 13566 • If $\Gamma \vdash_F \text{mon } (\tau_d \Rightarrow \tau_c) \lambda x. e$ then $\Gamma \vdash_F \lambda x. e$
- 13567
- 13568 • If $\Gamma \vdash_F \text{mon } (\tau_d \Rightarrow \tau_c) \lambda(x : \tau_x). e$ then $\Gamma \vdash_F \lambda(x : \tau_x). e : \tau_x \Rightarrow \tau'_c$
- 13569
- 13570 • If $\Gamma \vdash_F \text{mon } (\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$ then either:
- 13571 – $\Gamma \vdash_F \langle v_0, v_1 \rangle$
- 13572 – or $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau'$
- 13573
- 13574 • If $\Gamma \vdash_F \text{stat } \tau' e'$ then $\Gamma \vdash_F e' : \tau'$

Proof:

QED by the definition of $\Gamma \vdash_F e$

□

Lemma 6.33 : HF *canonical forms*

13573
13574
13575
13576
13577
13578
13579
13580
13581
13582
13583
13584
13585

- 13586 • If $\vdash_F v : \tau_0 \times \tau_1$ then either:
- 13587 – $v = \langle v_0, v_1 \rangle$
- 13588 – or $v = \text{mon } \tau'_0 \times \tau'_1 \langle v_0, v_1 \rangle$
- 13589 $\wedge \tau'_0 \times \tau'_1 \leq \tau_0 \times \tau_1$
- 13590 • If $\vdash_F v : \tau_d \Rightarrow \tau_c$ then either:
- 13591 – $v = \lambda(x : \tau_x). e'$
- 13592 $\wedge \tau_d \leq \tau_x$
- 13593 – or $v = \text{mon } (\tau'_d \Rightarrow \tau'_c) (\lambda x. e)$
- 13594 $\wedge \tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- 13595 – or $v = \text{mon } (\tau'_d \Rightarrow \tau'_c) \lambda(x : \tau_x). e$
- 13596 $\wedge \tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- 13597 • If $\vdash_F v : \text{Int}$ then $v = i$
- 13598 • If $\vdash_F v : \text{Nat}$ then $v = i$ and $v \in \mathbb{N}$

Proof:

QED by definition of $\vdash_F \cdot : \tau$

□

Lemma 6.34 : Δ *type soundness*

If $\vdash_F v_0 : \tau_0$ and $\vdash_F v_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau$ then one of the following holds:

- 13603 • $\delta(\text{op}^2, v_0, v_1) = v$ and $\vdash_F v : \tau$, or
- 13604
- 13605 • $\delta(\text{op}^2, v_0, v_1) = \text{BndryErr}$
- 13606

Proof (sketch): Similar to the proof for the higher-order Δ *type soundness* lemma. □

Lemma 6.35 : δ *preservation*

- 13607 • If $\vdash_F v$ and $\delta(\text{op}^1, v) = v'$ then $\vdash_F v'$
- 13608
- 13609 • If $\vdash_F v_0$ and $\vdash_F v_1$ and $\delta(\text{op}^2, v_0, v_1) = v'$ then $\vdash_F v'$
- 13610

Proof:

Similar to the proof for the higher-order δ *preservation* lemma.

□

Lemma 6.36 : HF *substitution*

- 13611 • If $(x : \tau_x), \Gamma \vdash_F e$ and $\vdash_F v : \tau_x$ then $\Gamma \vdash_F e[x \leftarrow v]$
- 13612
- 13613 • If $x, \Gamma \vdash_F e$ and $\vdash_F v$ then $\Gamma \vdash_F e[x \leftarrow v]$
- 13614
- 13615 • If $(x : \tau_x), \Gamma \vdash_F e : \tau$ and $\vdash_F v : \tau_x$ then $\Gamma \vdash_F e[x \leftarrow v] : \tau$
- 13616
- 13617 • If $x, \Gamma \vdash_F e : \tau$ and $\vdash_F v$ then $\Gamma \vdash_F e[x \leftarrow v] : \tau$
- 13618

Proof:

Similar to the proof for the higher-order *substitution* lemma.

□

Lemma 6.37 : *weakening*

- 13619 • If $\Gamma \vdash_F e$ then $x, \Gamma \vdash_F e$
- 13620
- 13621 • If $\Gamma \vdash_F e : \tau$ then $(x : \tau'), \Gamma \vdash_F e : \tau$
- 13622

Proof:

QED because e is closed under Γ

□

13586
13587
13588
13589
13590
13591
13592
13593
13594
13595
13596
13597
13598
13599
13600
13601
13602
13603
13604
13605
13606
13607
13608
13609
13610
13611
13612
13613
13614
13615
13616
13617
13618
13619
13620
13621
13622
13623
13624
13625
13626
13627
13628
13629
13630
13631
13632
13633
13634
13635
13636
13637
13638
13639
13640

13641	E.7 Embeddings Summary	13696
13642	The paragraphs in this section summarize the five embed-	13697
13643	dings with four slogans. Each slogan pertains to one aspect	13698
13644	of the embedding:	13699
13645	1. What kinds of checks does the embedding perform	13700
13646	when a value reaches a type boundary?	13701
13647	2. When, if ever, does the embedding wrap a value in a	13702
13648	monitor?	13703
13649	3. If an ill-typed value reaches a type boundary, when	13704
13650	does the embedding signal an error?	13705
13651	4. How do types affect behavior?	13706
13652	These embeddings are ordered on a speculative scale from	13707
13653	"most guarantees" to "least guarantees".	13708
13654		13709
13655	Higher-Order embedding	13710
13656	1. recursively check read-only values;	13711
13657	2. monitor functional and mutable values;	13712
13658	3. detect boundary errors as early as possible;	13713
13659	4. types globally constrain behavior.	13714
13660		13715
13661	Co-Natural embedding	13716
13662	1. tag-check all values;	13717
13663	2. monitor all data structures and functions;	13718
13664	3. detect boundary errors as late as possible;	13719
13665	4. types globally constrain behavior	13720
13666		13721
13667	Forgetful embedding	13722
13668	1. tag-check all values;	13723
13669	2. apply at most one monitor to each value;	13724
13670	3. detect boundary errors as late as possible;	13725
13671	4. types (of values) locally constrain behavior.	13726
13672		13727
13673	First-Order embedding	13728
13674	1. tag-check all values;	13729
13675	2. never allocate a monitor;	13730
13676	3. detect boundary errors as late as possible;	13731
13677	4. types (of contexts) locally constrain behavior.	13732
13678		13733
13679	Erasure embedding	13734
13680	1. never check values;	13735
13681	2. never allocate a monitor;	13736
13682	3. never detect a type boundary error;	13737
13683	4. types do not affect behavior	13738
13684		13739
13685		13740
13686		13741
13687		13742
13688		13743
13689		13744
13690		13745
13691		13746
13692		13747
13693		13748
13694		13749
13695		13750

E.8 Simulation Lemmas

E.8.1 Definitions

Combined Language

$e = x \mid v \mid \langle e, e \rangle \mid ee \mid op^1 e \mid op^2 ee \mid$
 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err} \mid \text{chk } K e \mid \text{dyn } e \mid \text{stat } e$
 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e \mid \text{mon}(\tau \Rightarrow \tau) v$
 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet \mid \text{chk } K E^\bullet$
 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E$
 $\text{chk } K E \mid \text{dyn } E \mid \text{stat } E$

$e \text{ } 1 \lesssim_E e$

$$\frac{}{\text{Err } 1 \lesssim_E e^E} \quad \frac{e^1 \text{ } 1 \lesssim_E e^E}{\text{chk } K e^1 \text{ } 1 \lesssim_E e^E} \quad \frac{e^1 \text{ } 1 \lesssim_E e^E}{\text{dyn } e^1 \text{ } 1 \lesssim_E e^E}$$

$$\frac{e^1 \text{ } 1 \lesssim_E e^E}{\text{stat } e^1 \text{ } 1 \lesssim_E e^E} \quad \frac{}{x \text{ } 1 \lesssim_E x} \quad \frac{}{i \text{ } 1 \lesssim_E i} \quad \frac{e^1 \text{ } 1 \lesssim_E e^E}{\lambda x. e^1 \text{ } 1 \lesssim_E \lambda x. e^E}$$

$$\frac{e^1 \text{ } 1 \lesssim_E e^E}{\lambda(x:\tau). e^1 \text{ } 1 \lesssim_E \lambda(x:\tau). e^E} \quad \frac{e_0^1 \text{ } 1 \lesssim_E e_0^E \quad e_1^1 \text{ } 1 \lesssim_E e_1^E}{e_0^1 e_1^1 \text{ } 1 \lesssim_E e_0^E e_1^E}$$

$$\frac{e_0^1 \text{ } 1 \lesssim_E e_0^E \quad e_1^1 \text{ } 1 \lesssim_E e_1^E}{\langle e_0^1, e_1^1 \rangle \text{ } 1 \lesssim_E \langle e_0^E, e_1^E \rangle} \quad \frac{e_0^1 \text{ } 1 \lesssim_E e_0^E}{op^1 e_0^1 \text{ } 1 \lesssim_E op^1 e_0^E}$$

$$\frac{e_0^1 \text{ } 1 \lesssim_E e_0^E \quad e_1^1 \text{ } 1 \lesssim_E e_1^E}{op^2 e_0^1 e_1^1 \text{ } 1 \lesssim_E op^2 e_0^E e_1^E} \quad \frac{e_0^1 \text{ } 1 \lesssim_E e_0^E}{\text{dyn } \tau e_0^1 \text{ } 1 \lesssim_E \text{dyn } \tau e_0^E}$$

$$\frac{e_0^1 \text{ } 1 \lesssim_E e_0^E}{\text{stat } \tau e_0^1 \text{ } 1 \lesssim_E \text{stat } \tau e_0^E} \quad \frac{}{\text{Err } 1 \lesssim_E \text{Err}}$$

$E \text{ } 1 \lesssim_E E$

$$\frac{}{[] \text{ } 1 \lesssim_E []} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E}{\text{chk } K E^1 \text{ } 1 \lesssim_E E^E} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E}{\text{dyn } E^1 \text{ } 1 \lesssim_E E^E}$$

$$\frac{E^1 \text{ } 1 \lesssim_E E^E}{\text{stat } E^1 \text{ } 1 \lesssim_E E^E} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E \quad e^1 \text{ } 1 \lesssim_E e^E}{E^1 e^1 \text{ } 1 \lesssim_E E^E e^E}$$

$$\frac{v^1 \text{ } 1 \lesssim_E v^E \quad E^1 \text{ } 1 \lesssim_E E^E}{v^1 E^1 \text{ } 1 \lesssim_E v^E E^E} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E \quad e^1 \text{ } 1 \lesssim_E e^E}{\langle E^1, e^1 \rangle \text{ } 1 \lesssim_E \langle E^E, e^E \rangle}$$

$$\frac{v^1 \text{ } 1 \lesssim_E v^E \quad E^1 \text{ } 1 \lesssim_E E^E}{\langle v^1, E^1 \rangle \text{ } 1 \lesssim_E \langle v^E, E^E \rangle} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E}{op^1 E^1 \text{ } 1 \lesssim_E op^1 E^E}$$

$$\frac{E^1 \text{ } 1 \lesssim_E E^E \quad e^1 \text{ } 1 \lesssim_E e^E}{op^2 E^1 e^1 \text{ } 1 \lesssim_E op^2 E^E e^E} \quad \frac{v^1 \text{ } 1 \lesssim_E v^E \quad E^1 \text{ } 1 \lesssim_E E^E}{op^2 v^1 E^1 \text{ } 1 \lesssim_E op^2 v^E E^E}$$

$$\frac{E^1 \text{ } 1 \lesssim_E E^E}{\text{dyn } \tau E^1 \text{ } 1 \lesssim_E \text{dyn } \tau E^E} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E}{\text{stat } \tau E^1 \text{ } 1 \lesssim_E \text{stat } \tau E^E}$$

13861	$\boxed{e \text{H}_{\lesssim 1} e}$	13916
13862	$\frac{e^H \text{H}_{\lesssim 1} e^1}{e^H \text{H}_{\lesssim 1} \text{chk } K e^1}$	13917
13863	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\text{Err}_{\text{H}_{\lesssim 1} e^1}}$	13918
13864	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\text{dyn } \tau e^H \text{H}_{\lesssim 1} \text{dyn } \tau e^1}$	13919
13865		13920
13866	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\text{dyn } \tau e^H \text{H}_{\lesssim 1} \text{dyn } e^1}$	13921
13867	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\text{dyn } \tau_0 (\text{stat } \tau_1 e^H) \text{H}_{\lesssim 1} e^1}$	13922
13868		13923
13869	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\text{stat } \tau e^H \text{H}_{\lesssim 1} \text{stat } \tau e^1}$	13924
13870	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\text{stat } \tau e^H \text{H}_{\lesssim 1} \text{stat } e^1}$	13925
13871		13926
13872	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\text{stat } \tau_0 (\text{dyn } \tau_1 e^H) \text{H}_{\lesssim 1} e^1}$	13927
13873	$\frac{e_0^H \text{H}_{\lesssim 1} e_0^1 \quad e_1^H \text{H}_{\lesssim 1} e_1^1}{e_0^H e_1^H \text{H}_{\lesssim 1} e_0^1 e_1^1}$	13928
13874		13929
13875		13930
13876	$\frac{e_0^H \text{H}_{\lesssim 1} e_0^1 \quad e_1^H \text{H}_{\lesssim 1} e_1^1}{\langle e_0^H, e_1^H \rangle \text{H}_{\lesssim 1} \langle e_0^1, e_1^1 \rangle}$	13931
13877	$\frac{e^H \text{H}_{\lesssim 1} e^1}{op^1 e^H \text{H}_{\lesssim 1} op^1 e^1}$	13932
13878		13933
13879	$\frac{e_0^H \text{H}_{\lesssim 1} e_0^1 \quad e_1^H \text{H}_{\lesssim 1} e_1^1}{op^2 e_0^H e_1^H \text{H}_{\lesssim 1} op^2 e_0^1 e_1^1}$	13934
13880	$\frac{e^H \text{H}_{\lesssim 1} e^1}{x \text{H}_{\lesssim 1} x \quad i \text{H}_{\lesssim 1} i}$	13935
13881		13936
13882		13937
13883	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\lambda x. e^H \text{H}_{\lesssim 1} \lambda x. e^1}$	13938
13884	$\frac{e^H \text{H}_{\lesssim 1} e^1}{\lambda(x:\tau). e^H \text{H}_{\lesssim 1} \lambda(x:\tau). e^1}$	13939
13885		13940
13886		13941
13887	$\frac{v^H \text{H}_{\lesssim 1} v^1}{\text{mon } \tau v^H \text{H}_{\lesssim 1} v^1}$	13942
13888	$\frac{v^H \text{H}_{\lesssim 1} v^1}{\text{Err}_{\text{H}_{\lesssim 1} v^1}}$	13943
13889	$\boxed{E \text{H}_{\lesssim 1} E}$	13944
13890	$\frac{E^H \text{H}_{\lesssim 1} E^1}{E^H \text{H}_{\lesssim 1} \text{chk } K E^1}$	13945
13891	$\frac{E^H \text{H}_{\lesssim 1} E^1 \quad e^H \text{H}_{\lesssim 1} e^1}{E^H e^H \text{H}_{\lesssim 1} E^1 e^1}$	13946
13892	$\frac{v^H \text{H}_{\lesssim 1} v^1 \quad E^H \text{H}_{\lesssim 1} E^1}{v^H E^H \text{H}_{\lesssim 1} v^1 E^1}$	13947
13893	$\frac{E^H \text{H}_{\lesssim 1} E^1 \quad e^H \text{H}_{\lesssim 1} e^1}{\langle E^H, e^H \rangle \text{H}_{\lesssim 1} \langle E^1, e^1 \rangle}$	13948
13894	$\frac{v^H \text{H}_{\lesssim 1} v^1 \quad E^H \text{H}_{\lesssim 1} E^1}{\langle v^H, E^H \rangle \text{H}_{\lesssim 1} \langle v^1, E^1 \rangle}$	13949
13895	$\frac{E^H \text{H}_{\lesssim 1} E^1}{op^1 E^H \text{H}_{\lesssim 1} op^1 E^1}$	13950
13896		13951
13897	$\frac{E^H \text{H}_{\lesssim 1} E^1 \quad e^H \text{H}_{\lesssim 1} e^1}{op^2 E^H e^H \text{H}_{\lesssim 1} op^2 E^1 e^1}$	13952
13898	$\frac{v^H \text{H}_{\lesssim 1} v^1 \quad E^H \text{H}_{\lesssim 1} E^1}{op^2 v^H E^H \text{H}_{\lesssim 1} op^2 v^1 E^1}$	13953
13899		13954
13900		13955
13901	$\frac{E^H \text{H}_{\lesssim 1} E^1}{\text{dyn } \tau E^H \text{H}_{\lesssim 1} \text{dyn } \tau E^1}$	13956
13902	$\frac{E^H \text{H}_{\lesssim 1} E^1}{\text{dyn } \tau E^H \text{H}_{\lesssim 1} \text{dyn } E^1}$	13957
13903		13958
13904	$\frac{E^H \text{H}_{\lesssim 1} E^1}{\text{dyn } \tau_0 (\text{stat } \tau_1 E^H) \text{H}_{\lesssim 1} E^1}$	13959
13905	$\frac{E^H \text{H}_{\lesssim 1} E^1}{\text{stat } \tau E^H \text{H}_{\lesssim 1} \text{stat } \tau E^1}$	13960
13906		13961
13907	$\frac{E^H \text{H}_{\lesssim 1} E^1}{\text{stat } \tau E^H \text{H}_{\lesssim 1} \text{stat } E^1}$	13962
13908	$\frac{E^H \text{H}_{\lesssim 1} E^1}{\text{stat } \tau_0 (\text{dyn } \tau_1 E^H) \text{H}_{\lesssim 1} E^1}$	13963
13909		13964
13910		13965
13911	$\frac{E^H \text{H}_{\lesssim 1} E^1}{\text{stat } \tau E^H \text{H}_{\lesssim 1} \text{stat } E^1}$	13966
13912	$\frac{E^H \text{H}_{\lesssim 1} E^1}{\text{stat } \tau_0 (\text{dyn } \tau_1 E^H) \text{H}_{\lesssim 1} E^1}$	13967
13913		13968
13914		13969
13915		13970

E.8.2 Theorems
Theorem 8.0 : Err approximation

If $e \in e_S$ and $\vdash e : \tau$ then the following statements hold:

- if $e \rightarrow_{E-S}^* \text{Err}$ then $e \rightarrow_{1-S}^* \text{Err}$
- if $e \rightarrow_{1-S}^* \text{Err}$ then $e \rightarrow_{H-S}^* \text{Err}$

Proof:

QED by *1-E approximation* and *H-1 approximation*.

□

E.8.3 Lemmas
Lemma 8.1 : 1-E approximation

If $e \in e_S$ and $\vdash e : \tau$ and $e \rightarrow_{E-S}^* \text{Err}$ then:

- $\vdash_1 e : \lfloor \tau \rfloor \rightsquigarrow e''$
- $e'' \rightarrow_{1-S}^* \text{Err}$

Proof:

- $e'' \mathrel{1\lesssim_E} e$
by *1-E static reflexivity*
- QED by *1-E simulation*

□

Lemma 8.2 : 1-E static reflexivity

If $\Gamma \vdash e : \tau$ and $\Gamma \vdash e : \tau \rightsquigarrow e''$ then $e'' \mathrel{1\lesssim_E} e$.

Proof:

By structural induction on the $\Gamma \vdash e : \tau \rightsquigarrow e''$ judgment.

CASE $\frac{}{\Gamma \vdash i : \text{Nat} \rightsquigarrow i}$:

1. QED $i \mathrel{1\lesssim_E} i$

CASE $\frac{}{\Gamma \vdash i : \text{Int} \rightsquigarrow i}$:

1. QED $i \mathrel{1\lesssim_E} i$

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1 \rightsquigarrow \langle e'_0, e'_1 \rangle}$:

1. $e'_0 \mathrel{1\lesssim_E} e_0$
 $\wedge e'_1 \mathrel{1\lesssim_E} e_1$
by the induction hypothesis

2. QED

CASE $\frac{(x:\tau_d), \Gamma \vdash e : \tau_c \rightsquigarrow e'}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c \rightsquigarrow \lambda(x:\tau_d). e'}$:

1. $e' \mathrel{1\lesssim_E} e$
by the induction hypothesis
2. QED

CASE $\frac{}{\Gamma \vdash x : \tau \rightsquigarrow x}$:

1. QED $x \mathrel{1\lesssim_E} x$

CASE $\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_d \rightsquigarrow e'_1 \quad \lfloor \tau_c \rfloor = K}{\Gamma \vdash e_0 e_1 : \tau_c \rightsquigarrow \text{chk } K (e'_0 e'_1)}$

1. $e'_0 \mathrel{1\lesssim_E} e_0$
 $\wedge e'_1 \mathrel{1\lesssim_E} e_1$
by the induction hypothesis

2. $e'_0 e'_1 \mathrel{1\lesssim_E} e_0 e_1$
3. QED $\text{chk } K e'_0 e'_1 \mathrel{1\lesssim_E} e_0 e_1$

CASE $\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad \lfloor \tau_0 \rfloor = K}{\Gamma \vdash \text{fst } e : \tau_0 \rightsquigarrow \text{chk } K (\text{fst } e')}$:

1. $e' \mathrel{1\lesssim_E} e$
by the induction hypothesis
2. $\text{fst } e' \mathrel{1\lesssim_E} \text{fst } e$
3. QED $\text{chk } K \text{fst } e' \mathrel{1\lesssim_E} \text{fst } e$

14081 **CASE**
$$\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad [\tau_1] = K}{\Gamma \vdash \text{snd } e : \tau_1 \rightsquigarrow \text{chk } K (\text{snd } e')}$$
 :

- 14082 1. $e' \underset{1}{\rightsquigarrow}_E e$
- 14083 by the induction hypothesis
- 14084 2. $\text{snd } e' \underset{1}{\rightsquigarrow}_E \text{snd } e$
- 14085 3. QED $\text{chk } K \text{ snd } e' \underset{1}{\rightsquigarrow}_E \text{snd } e$

14088 **CASE**
$$\frac{\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau \rightsquigarrow \text{op}^2 e'_0 e'_1}$$
 :

- 14089 1. $e'_0 \underset{1}{\rightsquigarrow}_E e_0$
- 14090 $\wedge e'_1 \underset{1}{\rightsquigarrow}_E e_1$
- 14091 by the induction hypothesis
- 14092 2. QED

14093 **CASE**
$$\frac{\Gamma \vdash e : \tau' \rightsquigarrow e' \quad \tau' \leq \tau}{\Gamma \vdash e : \tau \rightsquigarrow e'}$$
 :

- 14094 1. QED by the induction hypothesis

14095 **CASE**
$$\frac{}{\Gamma \vdash \text{Err} : \tau \rightsquigarrow \text{Err}}$$
 :

- 14096 1. QED $\text{Err} \underset{1}{\rightsquigarrow}_E \text{Err}$

14097 **CASE**
$$\frac{\Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash \text{dyn } \tau e : \tau \rightsquigarrow \text{dyn } \tau e'}$$
 :

- 14098 1. $e' \underset{1}{\rightsquigarrow}_E e$
- 14099 by the induction hypothesis
- 14100 2. QED

14101 \square

14102 **Lemma 8.3 : 1-E dynamic reflexivity**

14103 If $\Gamma \vdash e$ and $\Gamma \vdash e \rightsquigarrow e''$ then $e'' \underset{1}{\rightsquigarrow}_E e$.

14104 *Proof:*

14105 By structural induction on the $\Gamma \vdash e \rightsquigarrow e''$ judgment.

14106 **CASE**
$$\frac{}{\Gamma \vdash i \rightsquigarrow i}$$
 :

- 14107 1. QED $i \underset{1}{\rightsquigarrow}_E i$

14108 **CASE**
$$\frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash \langle e_0, e_1 \rangle \rightsquigarrow \langle e'_0, e'_1 \rangle}$$
 :

- 14109 1. $e'_0 \underset{1}{\rightsquigarrow}_E e_0$
- 14110 $\wedge e'_1 \underset{1}{\rightsquigarrow}_E e_1$
- 14111 by the induction hypothesis
- 14112 2. QED

14113 **CASE**
$$\frac{x, \Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash \lambda x. e \rightsquigarrow \lambda x. e'}$$
 :

- 14114 1. $e' \underset{1}{\rightsquigarrow}_E e$
- 14115 by the induction hypothesis
- 14116 2. QED

14117 **CASE**
$$\frac{}{\Gamma \vdash x \rightsquigarrow x}$$
 :

14118

14119

14120

14121

14122

14123

14124

14125

14126

14127

1. QED $x \underset{1}{\rightsquigarrow}_E x$

14128 **CASE**
$$\frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash e_0 e_1 \rightsquigarrow e'_0 e'_1}$$
 :

- 14129 1. $e'_0 \underset{1}{\rightsquigarrow}_E e_0$
- 14130 $\wedge e'_1 \underset{1}{\rightsquigarrow}_E e_1$
- 14131 by the induction hypothesis

14132 2. QED

14133 **CASE**
$$\frac{\Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash \text{op}^1 e \rightsquigarrow \text{op}^1 e'}$$
 :

- 14134 1. $e' \underset{1}{\rightsquigarrow}_E e$
- 14135 by the induction hypothesis
- 14136 2. QED

14137 **CASE**
$$\frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash \text{op}^2 e_0 e_1 \rightsquigarrow \text{op}^2 e'_0 e'_1}$$
 :

- 14138 1. $e'_0 \underset{1}{\rightsquigarrow}_E e_0$
- 14139 $\wedge e'_1 \underset{1}{\rightsquigarrow}_E e_1$
- 14140 by the induction hypothesis

- 14141 2. QED

14142 **CASE**
$$\frac{}{\Gamma \vdash \text{Err} \rightsquigarrow \text{Err}}$$
 :

- 14143 1. QED $\text{Err} \underset{1}{\rightsquigarrow}_E \text{Err}$

14144 **CASE**
$$\frac{\Gamma \vdash e : \tau \rightsquigarrow e'}{\Gamma \vdash \text{stat } \tau e \rightsquigarrow \text{stat } \tau e'}$$
 :

- 14145 1. $e' \underset{1}{\rightsquigarrow}_E e$
- 14146 by 1-E static reflexivity
- 14147 2. QED

14148 \square

14149 **Lemma 8.4 : 1-E simulation**

14150 If $E^1[e_0^1] \underset{1}{\rightsquigarrow}_E E^E[e_0^E]$ and $E^E[e_0^E] \rightarrow_{E-S} E^E[e_1^E]$

14151 then $E^1[e_0^1] \rightarrow_{1-S}^* E^1[e_1^1]$ and $E^1[e_1^1] \underset{1}{\rightsquigarrow}_E E^E[e_1^E]$

14152 *Proof:*

14153 By case analysis on $e_0^E \triangleright_{E-S} e_1^E$.

14154 **CASE** $\text{dyn } \tau_0 v_0^E \triangleright_{E-S} v_0^E$:

- 14155 1. $e_0^1 = \text{dyn } \tau_0 e_0^1$
- 14156 by definition $\underset{1}{\rightsquigarrow}_E$
- 14157 2. $e_0^1 \underset{1}{\rightsquigarrow}_E v_0^E$
- 14158 by (1)
- 14159 3. $\tau_1 e_0^1$
- 14160 by 1 inversion
- 14161 4. $e_0^1 \rightarrow_{1-D}^* v_0^1$ and $v_0^1 \underset{1}{\rightsquigarrow}_E v_0^E$
- 14162 $\vee e_0^1 \rightarrow_{1-D}^* \text{BndryErr}$
- 14163 by 1-E dynamic value stutter
- 14164 5. **IF** $e_0^1 \rightarrow_{1-D}^* \text{BndryErr}$:
- 14165 a. $e_0^1 \rightarrow_{1-S}^* \text{BndryErr}$
- 14166 b. $E^1[\text{BndryErr}] \underset{1}{\rightsquigarrow}_E E^E[e_1^E]$
- 14167 by 1-E hole substitution
- 14168 c. QED

14191	ELSE $e_{0'}^1 \rightarrow_{1-D}^* v_0^1 :$	b. $\vdash_1 v_{0'}^1, v_{1'}^1 : K_0$	14246
14192	a. $e_0^1 \rightarrow_{1-S}^* v_0^1$	by 1 static preservation	14247
14193	b. $E^1[v_0^1] \text{ i}_{\lesssim E} E^E[v_0^E]$	c. Contradiction by (a, b)	14248
14194	by 1-E hole substitution	CASE $v_0^E v_1^E \triangleright_{E-S} \text{TagErr}$	14249
14195	c. QED	$\wedge \vdash_1 e_0^1 :$	14250
14196	CASE $\text{stat } \tau_0 v_0^E \triangleright_{E-S} v_0^E :$	1. $e_0^1 = e_{0'}^1 e_{1'}^1$	14251
14197	1. $e_0^1 = \text{stat } \tau_0 e_{0'}^1$	by $e_0^1 \text{ i}_{\lesssim E} e_0^E$	14252
14198	by definition $\text{ i}_{\lesssim E}$	2. $e_{0'}^1 \rightarrow_{1-D}^* v_{0'}^1$ and $v_{0'}^1 \text{ i}_{\lesssim E} v_0^E$	14253
14199	2. $e_{0'}^1 \text{ i}_{\lesssim E} v_0^E$	$\vee e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	14254
14200	by (1)	by 1-E dynamic value stutter	14255
14201	3. $\vdash_1 e_{0'}^1 : [\tau_0]$	3. IF $e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr} :$	14256
14202	by 1 inversion	a. $e^1 \rightarrow_{1-D}^* \text{BndryErr}$	14257
14203	4. $e_{0'}^1 \rightarrow_{1-S}^* v_0^1$ and $v_0^1 \text{ i}_{\lesssim E} v_0^E$	b. QED $E^1[\text{BndryErr}] \text{ i}_{\lesssim E} E^E[\text{TagErr}]$	14258
14204	$\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$	4. $e_{1'}^1 \rightarrow_{1-D}^* v_{1'}^1$ and $v_{1'}^1 \text{ i}_{\lesssim E} v_1^E$	14259
14205	by 1-E dynamic value stutter	$\vee e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	14260
14206	5. IF $e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr} :$	by 1-E static value stutter	14261
14207	a. $e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	5. IF $e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr} :$	14262
14208	b. $E^1[\text{BndryErr}] \text{ i}_{\lesssim E} E^E[e_{1'}^E]$	a. $e^1 \rightarrow_{1-D}^* \text{BndryErr}$	14263
14209	by 1-E hole substitution	b. QED $E^1[\text{BndryErr}] \text{ i}_{\lesssim E} E^E[\text{TagErr}]$	14264
14210	c. QED	6. $v_0^E \in \mathbb{Z}$	14265
14211	ELSE $e_{0'}^1 \rightarrow_{1-S}^* v_0^1 :$	$\vee v_0^E \in \langle v, v' \rangle$	14266
14212	a. $e_0^1 \rightarrow_{1-D}^* v_0^1$	by definition \triangleright_{E-S}	14267
14213	b. $E^1[v_0^1] \text{ i}_{\lesssim E} E^E[v_0^E]$	7. $v_{0'}^1 \in \mathbb{Z}$	14268
14214	by 1-E hole substitution	$\vee v_{0'}^1 \in \langle v, v' \rangle$	14269
14215	c. QED	by (2)	14270
14216	CASE $v_0^E v_1^E \triangleright_{E-S} \text{TagErr}$	8. $e^1 \rightarrow_{1-D}^* \text{TagErr}$	14271
14217	$\wedge \vdash_1 e_0^1 : K_0 :$	9. QED $E^1[\text{TagErr}] \text{ i}_{\lesssim E} E^E[\text{TagErr}]$	14272
14218	1. $e_0^1 = e_{0'}^1 e_{1'}^1$	CASE $(\lambda x. e^E) v_1^E \triangleright_{E-S} e^E[x \leftarrow v_1^E] :$	14273
14219	by $e_0^1 \text{ i}_{\lesssim E} e_0^E$	1. $e_0^1 = e_{0'}^1 e_{1'}^1$	14274
14220	2. $e_{0'}^1 \rightarrow_{1-S}^* v_{0'}^1$ and $v_{0'}^1 \text{ i}_{\lesssim E} v_0^E$	by $e_0^1 \text{ i}_{\lesssim E} e_0^E$	14275
14221	$\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$	2. $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$ and $v_0^1 \text{ i}_{\lesssim E} v_0^E$	14276
14222	by 1-E static value stutter	$\vee e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	14277
14223	3. IF $e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr} :$	by 1-E dynamic value stutter	14278
14224	a. $e^1 \rightarrow_{1-S}^* \text{BndryErr}$	3. IF $e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr} :$	14279
14225	b. QED $E^1[\text{BndryErr}] \text{ i}_{\lesssim E} E^E[\text{TagErr}]$	a. $e^1 \rightarrow_{1-D}^* \text{BndryErr}$	14280
14226	4. $e_{1'}^1 \rightarrow_{1-S}^* v_{1'}^1$ and $v_{1'}^1 \text{ i}_{\lesssim E} v_1^E$	b. QED $E^1[\text{BndryErr}] \text{ i}_{\lesssim E} E^E[\text{TagErr}]$	14281
14227	$\vee e_{1'}^1 \rightarrow_{1-S}^* \text{BndryErr}$	4. $e_{1'}^1 \rightarrow_{1-D}^* v_{1'}^1$ and $v_{1'}^1 \text{ i}_{\lesssim E} v_1^E$	14282
14228	by 1-E static value stutter	$\vee e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	14283
14229	5. IF $e_{1'}^1 \rightarrow_{1-S}^* \text{BndryErr} :$	by 1-E static value stutter	14284
14230	a. $e^1 \rightarrow_{1-S}^* \text{BndryErr}$	5. IF $e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr} :$	14285
14231	b. QED $E^1[\text{BndryErr}] \text{ i}_{\lesssim E} E^E[\text{TagErr}]$	a. $e^1 \rightarrow_{1-D}^* \text{BndryErr}$	14286
14232	6. $v_0^E \in \mathbb{Z}$	b. QED $E^1[\text{BndryErr}] \text{ i}_{\lesssim E} E^E[\text{TagErr}]$	14287
14233	$\vee v_0^E \in \langle v, v' \rangle$	6. $v_0^1 = \lambda x. e^1$ and $e^1 \text{ i}_{\lesssim E} e^E$	14288
14234	by definition \triangleright_{E-S}	by (2)	14289
14235	7. IF $v_0^E \in \mathbb{Z} :$	7. $v_0^1 v_1^1 \triangleright_{1-D} e^1[x \leftarrow v_1^1]$	14290
14236	a. $v_{0'}^1 \in \mathbb{Z}$	$\vee v_0^1 v_1^1 \triangleright_{1-S} e^1[x \leftarrow v_1^1]$	14291
14237	by (2)	8. $e^1[x \leftarrow v_1^1] \text{ i}_{\lesssim E} e^E[x \leftarrow v_1^E]$	14292
14238	b. $\vdash_1 v_{0'}^1, v_{1'}^1 : K_0$	by 1-E substitution	14293
14239	by 1 static preservation	9. $E^1[e^1[x \leftarrow v_1^1]] \text{ i}_{\lesssim E} E^E[e^E[x \leftarrow v_1^E]]$	14294
14240	c. Contradiction by (a, b)	by 1-E hole substitution	14295
14241	ELSE $v_0^E \in \langle v, v' \rangle :$	10. QED	14296
14242	a. $v_{0'}^1 \in \langle v, v' \rangle$	CASE $(\lambda(x:\tau). e_0^E) v_1^E \triangleright_{E-S} e_0^E[x \leftarrow v_1^E] :$	14297
14243	by (2)		14298
14244			14299
14245			14300

14301	1. $e_0^1 = e_{0'}^1 e_{1'}^1$	b. $v_0^1 \notin \langle v, v \rangle$	14356
14302	by $e_0^1 \underset{1 \lesssim_E}{\sim} e_0^E$	by $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	14357
14303	2. $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$ and $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	c. $op^1 v_0^1 \triangleright_{1-D} \text{TagErr}$	14358
14304	$\vee e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	by definition \triangleright_{1-D}	14359
14305	by 1-E dynamic value stutter	d. $\text{QED } E^1[\text{TagErr}] \underset{1 \lesssim_E}{\sim} E^E[\text{TagErr}]$	14360
14306	3. IF $e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$:	ELSE $e_{0'}^1 \rightarrow_{1-S}^* v_0^1$:	14361
14307	a. $e^1 \rightarrow_{1-D}^* \text{BndryErr}$	a. $\vdash_1 op^1 e_{0'}^1 : K_0$	14362
14308	b. $\text{QED } E^1[\text{BndryErr}] \underset{1 \lesssim_E}{\sim} E^E[\text{TagErr}]$	b. $\vdash_1 op^1 v_0^1 : K_0$	14363
14309	4. $e_{1'}^1 \rightarrow_{1-D}^* v_1^1$ and $v_1^1 \underset{1 \lesssim_E}{\sim} v_1^E$	by 1 static preservation	14364
14310	$\vee e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	c. $v_0^E \notin \langle v, v \rangle$	14365
14311	by 1-E static value stutter	by definition \triangleright_{E-S}	14366
14312	5. IF $e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr}$:	d. $v_0^1 \notin \langle v, v \rangle$	14367
14313	a. $e^1 \rightarrow_{1-D}^* \text{BndryErr}$	by $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	14368
14314	b. $\text{QED } E^1[\text{BndryErr}] \underset{1 \lesssim_E}{\sim} E^E[\text{TagErr}]$	e. Contradiction by (b)	14369
14315	6. $v_0^1 = \lambda(x:\tau). e^1$ and $e^1 \underset{1 \lesssim_E}{\sim} e^E$	CASE $op^1 v_0^E \triangleright_{E-S} \delta(op^1, v_0^E)$:	14370
14316	by (2)	1. $e_0^1 = op^1 e_{0'}^1$	14371
14317	7. $v_0^1 v_1^1 \triangleright_{1-D} e^1[x \leftarrow v_1^1]$	by $e_0^1 \underset{1 \lesssim_E}{\sim} e_0^E$	14372
14318	$\vee v_0^1 v_1^1 \triangleright_{1-S} \text{BndryErr}$ and $\mathcal{X}(\lfloor \tau \rfloor, v_1^1) = \text{BndryErr}$	2. $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$ and $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	14373
14319	$\vee v_0^1 v_1^1 \triangleright_{1-S} e^1[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v_1^1)]$	$\vee e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	14374
14320	8. IF $v_0^1 v_1^1 \triangleright_{1-D} e^1[x \leftarrow v_1^1]$:	$\vee e_{0'}^1 \rightarrow_{1-S}^* v_0^1$ and $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	14375
14321	a. $e^1[x \leftarrow v_1^1] \underset{1 \lesssim_E}{\sim} e^E[x \leftarrow v_1^E]$	$\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$	14376
14322	by 1-E substitution	by 1-E dynamic value stutter or 1-E static value	14377
14323	b. $E^1[e^1[x \leftarrow v_1^1]] \underset{1 \lesssim_E}{\sim} E^E[e^E[x \leftarrow v_1^E]]$	stutter	14378
14324	by 1-E hole substitution	3. IF $e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	14379
14325	c. QED	$\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$:	14380
14326	IF $v_0^1 v_1^1 \triangleright_{1-S} \text{BndryErr}$:	a. $\text{QED } E^1[\text{BndryErr}] \underset{1 \lesssim_E}{\sim} E^E[\text{TagErr}]$	14381
14327	a. $e^1 \rightarrow_{1-S}^* \text{BndryErr}$	IF $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$:	14382
14328	b. $\text{QED } E^1[\text{BndryErr}] \underset{1 \lesssim_E}{\sim} E^E[\text{BndryErr}]$	a. $v_0^E \in \langle v, v \rangle$	14383
14329	ELSE $v_0^1 v_1^1 \triangleright_{1-S} e^1[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v_1^1)]$:	by definition \triangleright_{E-S}	14384
14330	a. $\mathcal{X}(\lfloor \tau \rfloor, v_1^1) = v_1^1$	b. $v_0^1 \in \langle v, v \rangle$	14385
14331	b. $e^1[x \leftarrow v_1^1] \underset{1 \lesssim_E}{\sim} e^E[x \leftarrow v_1^E]$	by $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	14386
14332	by 1-E substitution	c. $op^1 v_0^1 \triangleright_{1-D} \delta(op^1, v_0^1)$	14387
14333	c. $E^1[e^1[x \leftarrow v_1^1]] \underset{1 \lesssim_E}{\sim} E^E[e^E[x \leftarrow v_1^E]]$	by definition \triangleright_{1-D}	14388
14334	by 1-E hole substitution	d. $\delta(op^1, v_0^1) \underset{1 \lesssim_E}{\sim} \delta(op^1, v_0^E)$	14389
14335	d. QED	by 1-E delta	14390
14336	CASE $op^1 v_0^E \triangleright_{E-S} \text{TagErr}$:	e. $\text{QED } E^1[\delta(op^1, v_0^1)] \underset{1 \lesssim_E}{\sim} E^E[\delta(op^1, v_0^E)]$	14391
14337	1. $e_0^1 = op^1 e_{0'}^1$	ELSE $e_{0'}^1 \rightarrow_{1-S}^* v_0^1$:	14392
14338	by $e_0^1 \underset{1 \lesssim_E}{\sim} e_0^E$	a. $v_0^E \in \langle v, v \rangle$	14393
14339	2. $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$ and $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	by definition \triangleright_{E-S}	14394
14340	$\vee e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	b. $v_0^1 \in \langle v, v \rangle$	14395
14341	$\vee e_{0'}^1 \rightarrow_{1-S}^* v_0^1$ and $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	by $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	14396
14342	$\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$	c. $op^1 v_0^1 \triangleright_{1-S} \delta(op^1, v_0^1)$	14397
14343	by 1-E dynamic value stutter or 1-E static value	by definition \triangleright_{1-S}	14398
14344	stutter	d. $\delta(op^1, v_0^1) \underset{1 \lesssim_E}{\sim} \delta(op^1, v_0^E)$	14399
14345	3. IF $e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	by 1-E delta	14400
14346	$\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$:	e. $\text{QED } E^1[\delta(op^1, v_0^1)] \underset{1 \lesssim_E}{\sim} E^E[\delta(op^1, v_0^E)]$	14401
14347	a. $e^1 \rightarrow_{1-D}^* \text{BndryErr}$	CASE $op^2 v_0^E v_1^E \triangleright_{E-S} \text{TagErr}$:	14402
14348	b. $\text{QED } E^1[\text{BndryErr}] \underset{1 \lesssim_E}{\sim} E^E[\text{TagErr}]$	1. $e_0^1 = op^2 e_{0'}^1 e_{1'}^1$	14403
14349	IF $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$:	by $e_0^1 \underset{1 \lesssim_E}{\sim} e_0^E$	14404
14350	a. $v_0^E \notin \langle v, v \rangle$	2. $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$ and $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	14405
14351	by definition \triangleright_{E-S}	$\vee e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$	14406
14352	b. $v_0^1 \in \langle v, v \rangle$	$\vee e_{0'}^1 \rightarrow_{1-S}^* v_0^1$ and $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$	14407
14353	by $v_0^1 \underset{1 \lesssim_E}{\sim} v_0^E$		14408
14354	c. $op^1 v_0^1 \triangleright_{1-S} \delta(op^1, v_0^1)$		14409
14355	by definition \triangleright_{1-S}		14410

14411 $\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$
 14412 by 1-E *dynamic value stutter* or 1-E *static value*
 14413 *stutter*
 14414 3. $e_{1'}^1 \rightarrow_{1-D}^* v_1^1$ and $v_1^1 \mathrel{1 \lesssim_E} v_1^E$
 14415 $\vee e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr}$
 14416 $\vee e_{1'}^1 \rightarrow_{1-S}^* v_1^1$ and $v_1^1 \mathrel{1 \lesssim_E} v_1^E$
 14417 $\vee e_{1'}^1 \rightarrow_{1-S}^* \text{BndryErr}$
 14418 by 1-E *dynamic value stutter* or 1-E *static value*
 14419 *stutter*
 14420 4. **IF** $e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$
 14421 $\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$
 14422 $\vee e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr}$
 14423 $\vee e_{1'}^1 \rightarrow_{1-S}^* \text{BndryErr}$:
 14424 a. QED $E^1[\text{BndryErr}] \mathrel{1 \lesssim_E} E^E[\text{TagErr}]$
 14425 **IF** $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$
 14426 $\wedge e_{1'}^1 \rightarrow_{1-D}^* v_1^1$:
 14427 a. $v_0^E \notin \mathbb{Z}$
 14428 $\vee v_1^E \notin \mathbb{Z}$
 14429 by definition \triangleright_{E-S}
 14430 b. $v_0^1 \notin \mathbb{Z}$
 14431 $\vee v_1^1 \notin \mathbb{Z}$
 14432 by (a)
 14433 c. $op^2 v_0^1 v_1^1 \triangleright_{1-D} \text{TagErr}$
 14434 by definition \triangleright_{1-D}
 14435 d. QED $E^1[\text{TagErr}] \mathrel{1 \lesssim_E} E^E[\text{TagErr}]$
 14436 **ELSE** $e_{0'}^1 \rightarrow_{1-S}^* v_0^1$
 14437 $\wedge e_{1'}^1 \rightarrow_{1-S}^* v_1^1$:
 14438 a. $\vdash_1 op^2 e_{0'}^1 e_{1'}^1 : K_0$
 14439 b. $\vdash_1 op^2 v_0^1 v_1^1 : K_0$
 14440 by 1 *static preservation*
 14441 c. $v_0^E \notin \mathbb{Z}$
 14442 $\vee v_1^E \notin \mathbb{Z}$
 14443 by definition \triangleright_{E-S}
 14444 d. $v_0^1 \notin \mathbb{Z}$
 14445 $\vee v_1^1 \notin \mathbb{Z}$
 14446 by (c)
 14447 e. Contradiction by (b)
 14448 **CASE** $op^2 v_0^E v_1^E \triangleright_{E-S} \delta(op^2, v_0^E, v_1^E)$:
 14449 1. $e_0^1 = op^2 e_{0'}^1 e_{1'}^1$
 14450 by $e_0^1 \mathrel{1 \lesssim_E} e_0^E$
 14451 2. $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$ and $v_0^1 \mathrel{1 \lesssim_E} v_0^E$
 14452 $\vee e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$
 14453 $\vee e_{0'}^1 \rightarrow_{1-S}^* v_0^1$ and $v_0^1 \mathrel{1 \lesssim_E} v_0^E$
 14454 $\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$
 14455 by 1-E *dynamic value stutter* or 1-E *static value*
 14456 *stutter*
 14457 3. $e_{1'}^1 \rightarrow_{1-D}^* v_1^1$ and $v_1^1 \mathrel{1 \lesssim_E} v_1^E$
 14458 $\vee e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr}$
 14459 $\vee e_{1'}^1 \rightarrow_{1-S}^* v_1^1$ and $v_1^1 \mathrel{1 \lesssim_E} v_1^E$
 14460 $\vee e_{1'}^1 \rightarrow_{1-S}^* \text{BndryErr}$
 14461 by 1-E *dynamic value stutter* or 1-E *static value*
 14462 *stutter*
 14463
 14464
 14465

4. **IF** $e_{0'}^1 \rightarrow_{1-D}^* \text{BndryErr}$ 14466
 $\vee e_{0'}^1 \rightarrow_{1-S}^* \text{BndryErr}$ 14467
 $\vee e_{1'}^1 \rightarrow_{1-D}^* \text{BndryErr}$ 14468
 $\vee e_{1'}^1 \rightarrow_{1-S}^* \text{BndryErr}$: 14469
 a. QED $E^1[\text{BndryErr}] \mathrel{1 \lesssim_E} E^E[\text{TagErr}]$ 14470
IF $e_{0'}^1 \rightarrow_{1-D}^* v_0^1$ 14471
 $\wedge e_{1'}^1 \rightarrow_{1-D}^* v_1^1$: 14472
 a. $v_0^E \in \mathbb{Z}$ 14473
 $\wedge v_1^E \in \mathbb{Z}$ 14474
 by definition \triangleright_{E-S} 14475
 b. $v_0^1 \in \mathbb{Z}$ 14476
 by $v_0^1 \mathrel{1 \lesssim_E} v_0^E$ 14477
 c. $v_1^1 \in \mathbb{Z}$ 14478
 by $v_1^1 \mathrel{1 \lesssim_E} v_1^E$ 14479
 d. $op^2 v_0^1 v_1^1 \triangleright_{1-D} \delta(op^2, v_0^1, v_1^1)$ 14480
 by definition \triangleright_{1-D} 14481
 e. $\delta(op^2, v_0^1, v_1^1) \mathrel{1 \lesssim_E} \delta(op^2, v_0^E, v_1^E)$ 14482
 by 1-E *delta* 14483
 f. QED $E^1[\delta(op^2, v_0^1, v_1^1)] \mathrel{1 \lesssim_E} E^E[\delta(op^2, v_0^E, v_1^E)]$ 14484
ELSE $e_{0'}^1 \rightarrow_{1-S}^* v_0^1$ 14485
 $\wedge e_{1'}^1 \rightarrow_{1-S}^* v_1^1$: 14486
 a. $v_0^E \in \mathbb{Z}$ 14487
 $\wedge v_1^E \in \mathbb{Z}$ 14488
 by definition \triangleright_{E-S} 14489
 b. $v_0^1 \in \mathbb{Z}$ 14490
 by $v_0^1 \mathrel{1 \lesssim_E} v_0^E$ 14491
 c. $v_1^1 \in \mathbb{Z}$ 14492
 by $v_1^1 \mathrel{1 \lesssim_E} v_1^E$ 14493
 d. $op^2 v_0^1 v_1^1 \triangleright_{1-S} \delta(op^2, v_0^1, v_1^1)$ 14494
 by definition \triangleright_{1-S} 14495
 e. $\delta(op^2, v_0^1, v_1^1) \mathrel{1 \lesssim_E} \delta(op^2, v_0^E, v_1^E)$ 14496
 by 1-E *delta* 14497
 f. QED $E^1[\delta(op^2, v_0^1, v_1^1)] \mathrel{1 \lesssim_E} E^E[\delta(op^2, v_0^E, v_1^E)]$ 14498
 14499
 14500

□

Lemma 8.5 : 1-E static value stutter

If $e^1 \mathrel{1 \lesssim_E} v^E$ and $\vdash_1 e^1 : K$ then one of the following holds:

- $e^1 \rightarrow_{1-S}^* v^1$ and $v^1 \mathrel{1 \lesssim_E} v^E$
- $e^1 \rightarrow_{1-S}^* \text{BndryErr}$

Proof:

By induction on the structure of e^1 , and case analysis on $e^1 \mathrel{1 \lesssim_E} v^E$.

CASE e^1 is a value :

1. QED

CASE $e^1 = \text{chk } K e_0^1$:

1. $e_0^1 \mathrel{1 \lesssim_E} v^E$

by definition $1 \lesssim_E$

2. $\vdash_1 e_0^1$: Any

3. $e_0^1 \rightarrow_{1-S}^* v_0^1$ and $v_0^1 \mathrel{1 \lesssim_E} v^E$

$\vee e_0^1 \rightarrow_{1-S}^* \text{BndryErr}$

by the induction hypothesis

4. **IF** $e_0^1 \rightarrow_{1-S}^* \text{BndryErr}$:

a. QED $e^1 \rightarrow_{1-S}^* \text{BndryErr}$

14521 **IF** $e_0^1 \rightarrow_{1-S}^* v_0^1$
 14522 $\wedge X(K, e_0^1) = \text{BndryErr}$:
 14523 a. QED $e^1 \rightarrow_{1-S}^* \text{BndryErr}$
 14524 **ELSE** $e_0^1 \rightarrow_{1-S}^* v_0^1$
 14525 $\wedge X(K, e_0^1) = v_0^1$:
 14526 a. QED $e^1 \rightarrow_{1-S}^* v_0^1$
 14527 **CASE** $e^1 = \text{dyn } e_0^1$:
 14528 1. $e_0^1 \mathrel{\vDash}_E v^E$
 14529 by definition $\mathrel{\vDash}_E$
 14530 2. $\vdash_1 e_0^1$
 14531 3. $e_0^1 \rightarrow_{1-D}^* v_0^1$ and $v_0^1 \mathrel{\vDash}_E v^E$
 14532 $\vee e_0^1 \rightarrow_{1-D}^* \text{BndryErr}$
 14533 by **1-E dynamic value stutter**
 14534 4. **IF** $e_0^1 \rightarrow_{1-D}^* \text{BndryErr}$:
 14535 a. QED $e^1 \rightarrow_{1-S}^* \text{BndryErr}$
 14536 **ELSE** :
 14537 a. QED $e^1 \rightarrow_{1-S}^* v_0^1$
 14538 **CASE** $e^1 = \text{stat } v_0^1$:
 14539 1. Contradiction by $\vdash_1 e^1 : K$
 14540 \square

Lemma 8.6 : 1-E dynamic value stutter

If $e^1 \mathrel{\vDash}_E v^E$ and $\vdash_1 e^1$ then one of the following holds:

- $e^1 \rightarrow_{1-D}^* v^1$ and $v^1 \mathrel{\vDash}_E v^E$
- $e^1 \rightarrow_{1-D}^* \text{BndryErr}$

Proof:

By induction on the structure of e^1 , and case analysis on $e^1 \mathrel{\vDash}_E v^E$.

14547 **CASE** e^1 is a value :
 14548 1. QED
 14549 **CASE** $e^1 = \text{chk } K e_0^1$:
 14550 1. Contradiction by $\vdash_1 e^1$
 14551 **CASE** $e^1 = \text{dyn } e_0^1$:
 14552 1. Contradiction by $\vdash_1 e^1$
 14553 **CASE** $e^1 = \text{stat } v_0^1$:
 14554 1. $e_0^1 \mathrel{\vDash}_E v^E$
 14555 by definition $\mathrel{\vDash}_E$
 14556 2. $\vdash_1 e_0^1$: Any
 14557 3. $e_0^1 \rightarrow_{1-S}^* v_0^1$ and $v_0^1 \mathrel{\vDash}_E v^E$
 14558 $\vee e_0^1 \rightarrow_{1-S}^* \text{BndryErr}$
 14559 by **1-E static value stutter**
 14560 4. **IF** $e_0^1 \rightarrow_{1-S}^* \text{BndryErr}$:
 14561 a. QED $e^1 \rightarrow_{1-D}^* \text{BndryErr}$
 14562 **ELSE** :
 14563 a. QED $e^1 \rightarrow_{1-D}^* v_0^1$
 14564 \square

Lemma 8.7 : 1-E hole substitution

If $e^1 \mathrel{\vDash}_E e^E$ and $E^1 \mathrel{\vDash}_E E^E$ then $E^1[e^1] \mathrel{\vDash}_E E^E[e^E]$

Proof:

By induction on the structure of E^1 .

14567 **CASE** $E^1 = []$:
 14568 1. $e^E = []$
 14569 14570

2. $E^1[e^1] = e^1$
 $\wedge E^E[e^E] = e^E$
 3. QED
CASE $E^1 = E_0^1 e_1^1$:
 1. $E^E = E_0^E e_1^E$
 $\wedge E_0^1 \mathrel{\vDash}_E E_0^E$
 $\wedge e_1^1 \mathrel{\vDash}_E e_1^E$
 by definition $\mathrel{\vDash}_E$
 2. $E_0^1[e^1] \mathrel{\vDash}_E E_0^E[e^E]$
 by the induction hypothesis
 3. $E^1[e^1] = E_0^1[e^1] e_1^1$
 4. $E^E[e^E] = E_0^E[e^E] e_1^E$
 5. QED by (1, 2)
CASE $E^1 = v_0^1 E_1^1$:
 1. $E^E = e_0^E E_1^E$
 $\wedge e_0^1 \mathrel{\vDash}_E e_0^E$
 $\wedge E_1^1 \mathrel{\vDash}_E E_1^E$
 by definition $\mathrel{\vDash}_E$
 2. $E_1^1[e^1] \mathrel{\vDash}_E E_1^E[e^E]$
 by the induction hypothesis
 3. $E^1[e^1] = e_0^1 E_1^1[e^1]$
 4. $E^E[e^E] = e_0^E E_1^E[e^E]$
 5. QED by (1, 2)
CASE $E^1 = \langle E_0^1, e_1^1 \rangle$:
 1. $E^E = \langle E_0^E, e_1^E \rangle$
 $\wedge E_0^1 \mathrel{\vDash}_E E_0^E$
 $\wedge e_1^1 \mathrel{\vDash}_E e_1^E$
 by definition $\mathrel{\vDash}_E$
 2. $E_0^1[e^1] \mathrel{\vDash}_E E_0^E[e^E]$
 by the induction hypothesis
 3. $E^1[e^1] = \langle E_0^1[e^1], e_1^1 \rangle$
 4. $E^E[e^E] = \langle E_0^E[e^E], e_1^E \rangle$
 5. QED by (1, 2)
CASE $E^1 = \langle v_0^1, E_1^1 \rangle$:
 1. $E^E = \langle e_0^E, E_1^E \rangle$
 $\wedge e_0^1 \mathrel{\vDash}_E e_0^E$
 $\wedge E_1^1 \mathrel{\vDash}_E E_1^E$
 by definition $\mathrel{\vDash}_E$
 2. $E_1^1[e^1] \mathrel{\vDash}_E E_1^E[e^E]$
 by the induction hypothesis
 3. $E^1[e^1] = \langle e_0^1, E_1^1[e^1] \rangle$
 4. $E^E[e^E] = \langle e_0^E, E_1^E[e^E] \rangle$
 5. QED by (1, 2)
CASE $E^1 = \text{op}^1 E_0^1$:
 1. $E^E = \text{op}^1 E_0^E$
 $\wedge E_0^1 \mathrel{\vDash}_E E_0^E$
 by definition $\mathrel{\vDash}_E$
 2. $E_0^1[e^1] \mathrel{\vDash}_E E_0^E[e^E]$
 by the induction hypothesis
 3. $E^1[e^1] = \text{op}^1 E_0^1[e^1]$
 4. $E^E[e^E] = \text{op}^1 E_0^E[e^E]$
 5. QED by (1, 2)
CASE $E^1 = \text{op}^2 E_0^1 e_1^1$:
 14571 14572 14573 14574 14575

14631	1. $E^E = op^2 E_0^E e_1^E$	3. $E^1[e^1] = \text{stat } E_0^1[e^1]$	14686
14632	$\wedge E_0^1 \text{ } 1 \lesssim_E E_0^E$	4. QED (2)	14687
14633	$\wedge e_1^1 \text{ } 1 \lesssim_E e_1^E$	□	14688
14634	by definition $1 \lesssim_E$	Lemma 8.8 : 1-E substitution	14689
14635	2. $E_0^1[e^1] \text{ } 1 \lesssim_E E_0^E[e^E]$	If $e^1 \text{ } 1 \lesssim_E e^E$ and $v^1 \text{ } 1 \lesssim_E v^E$ then $e^1[x \leftarrow v^1] \text{ } 1 \lesssim_E e^E[x \leftarrow v^E]$	14690
14636	by the induction hypothesis	<i>Proof</i> :	14691
14637	3. $E^1[e^1] = op^2 E_0^1[e_0^1] e_1^1$	By induction on the structure of e^1 .	14692
14638	4. $E^E[e^E] = op^2 E_0^E[e_0^E] e_1^E$	CASE $e^1 = x$:	14693
14639	5. QED by (1, 2)	1. $e^E = x$	14694
14640	CASE $E^1 = op^2 v_0^1 E_1^1$:	by $e^1 \text{ } 1 \lesssim_E e^E$	14695
14641	1. $E^E = op^2 e_0^E E_1^E$	2. $e^1[x \leftarrow v^1] = v^1$	14696
14642	$\wedge e_0^1 \text{ } 1 \lesssim_E e_0^E$	$\wedge e^E[x \leftarrow v^E] = v^E$	14697
14643	$\wedge E_1^1 \text{ } 1 \lesssim_E E_1^E$	3. QED	14698
14644	by definition $1 \lesssim_E$	CASE $e^1 = y$:	14699
14645	2. $E_1^1[e^1] \text{ } 1 \lesssim_E E_1^E[e^E]$	1. $e^E = y$	14700
14646	by the induction hypothesis	by $e^1 \text{ } 1 \lesssim_E e^E$	14701
14647	3. $E^1[e^1] = op^2 e_0^1 E_1^1[e_0^1]$	2. $e^1[x \leftarrow v^1] = y$	14702
14648	4. $E^E[e^E] = op^2 e_0^E E_1^E[e_0^E]$	$\wedge e^E[x \leftarrow v^E] = y$	14703
14649	5. QED by (1, 2)	3. QED (1)	14704
14650	CASE $E^1 = \text{dyn } \tau E_0^1$:	CASE $e^1 = i$:	14705
14651	1. $E^E = \text{dyn } \tau E_0^E$	1. $e^E = i$	14706
14652	$\wedge E_0^1 \text{ } 1 \lesssim_E E_0^E$	by definition $1 \lesssim_E$	14707
14653	by definition $1 \lesssim_E$	2. $e^1[x \leftarrow v^1] = i$	14708
14654	2. $E_0^1[e^1] \text{ } 1 \lesssim_E E_0^E[e^E]$	$\wedge e^E[x \leftarrow v^E] = i$	14709
14655	by the induction hypothesis	3. QED	14710
14656	3. $E^1[e^1] = \text{dyn } \tau E_0^1[e_0^1]$	CASE $e^1 = \lambda x. e_0^1$:	14711
14657	4. $E^E[e^E] = \text{dyn } \tau E_0^E[e_0^E]$	1. $e^E = \lambda x. e_0^E$	14712
14658	5. QED by (1, 2)	$\wedge e_0^1 \text{ } 1 \lesssim_E e_0^E$	14713
14659	CASE $E^1 = \text{stat } \tau E_0^1$:	by definition $1 \lesssim_E$	14714
14660	1. $E^E = \text{stat } \tau E_0^E$	2. $e^1[x \leftarrow v^1] = \lambda x. e_0^1$	14715
14661	$\wedge E_0^1 \text{ } 1 \lesssim_E E_0^E$	$\wedge e^E[x \leftarrow v^E] = \lambda x. e_0^E$	14716
14662	by definition $1 \lesssim_E$	3. QED	14717
14663	2. $E_0^1[e^1] \text{ } 1 \lesssim_E E_0^E[e^E]$	CASE $e^1 = \lambda(x:\tau). e_0^1$:	14718
14664	by the induction hypothesis	1. $e^E = \lambda(x:\tau). e_0^E$	14719
14665	3. $E^1[e^1] = \text{stat } \tau E_0^1[e_0^1]$	$\wedge e_0^1 \text{ } 1 \lesssim_E e_0^E$	14720
14666	4. $E^E[e^E] = \text{stat } \tau E_0^E[e_0^E]$	by definition $1 \lesssim_E$	14721
14667	5. QED by (1, 2)	2. $e^1[x \leftarrow v^1] = \lambda(x:\tau). e_0^1$	14722
14668	CASE $E^1 = \text{chk } K E_0^1$:	$\wedge e^E[x \leftarrow v^E] = \lambda(x:\tau). e_0^E$	14723
14669	1. $E_0^1 \text{ } 1 \lesssim_E E^E$	3. QED	14724
14670	2. $E_0^1[e^1] \text{ } 1 \lesssim_E E^E[e^E]$	CASE $e^1 = \lambda y. e_0^1$:	14725
14671	by the induction hypothesis (1)	1. $e^E = \lambda y. e_0^E$	14726
14672	3. $E^1[e^1] = \text{chk } K E_0^1[e^1]$	$\wedge e_0^1 \text{ } 1 \lesssim_E e_0^E$	14727
14673	4. QED (2)	by definition $1 \lesssim_E$	14728
14674	CASE $E^1 = \text{dyn } E_0^1$:	2. $e_0^1[x \leftarrow v^1] \text{ } 1 \lesssim_E e_0^E[x \leftarrow v^E]$	14729
14675	1. $E_0^1 \text{ } 1 \lesssim_E E^E$	by the induction hypothesis (1)	14730
14676	2. $E_0^1[e^1] \text{ } 1 \lesssim_E E^E[e^E]$	3. $e^1[x \leftarrow v^1] = \lambda y. e_0^1[x \leftarrow v^E]$	14731
14677	by the induction hypothesis (1)	$\wedge e^E[x \leftarrow v^E] = \lambda y. e_0^E[x \leftarrow v^E]$	14732
14678	3. $E^1[e^1] = \text{dyn } E_0^1[e^1]$	4. QED (2, 3)	14733
14679	4. QED (2)	CASE $e^1 = \lambda(y:\tau). e_0^1$:	14734
14680	CASE $E^1 = \text{stat } E_0^1$:	1. $e^E = \lambda(y:\tau). e_0^E$	14735
14681	1. $E_0^1 \text{ } 1 \lesssim_E E^E$	$\wedge e_0^1 \text{ } 1 \lesssim_E e_0^E$	14736
14682	2. $E_0^1[e^1] \text{ } 1 \lesssim_E E^E[e^E]$	by definition $1 \lesssim_E$	14737
14683	by the induction hypothesis (1)		14738
14684			14739
14685			14740

14741 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_0^E[x \leftarrow v^E]$
 14742 by the induction hypothesis (1)
 14743 3. $e^1[x \leftarrow v^1] = \lambda(y:\tau). e_0^1[x \leftarrow v^E]$
 14744 $\wedge e^E[x \leftarrow v^E] = \lambda(y:\tau). e_0^E[x \leftarrow v^E]$
 14745 4. QED (2, 3)
 14746 **CASE** $e^1 = \text{mon } \tau v_0^1$:
 14747 1. Contradiction by $e^1 \underset{1}{\lesssim_E} e^E$
 14748 **CASE** $e^1 = \langle e_0^1, e_1^1 \rangle$:
 14749 1. $e^E = \langle e_0^E, e_1^E \rangle$
 14750 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_0^E[x \leftarrow v^E]$
 14751 $\wedge e_1^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_1^E[x \leftarrow v^E]$
 14752 by the induction hypothesis
 14753 3. $e^1[x \leftarrow v^1] = \langle e_0^1[x \leftarrow v^1], e_1^1[x \leftarrow v^1] \rangle$
 14754 $\wedge e^E[x \leftarrow v^E] = \langle e_0^E[x \leftarrow v^E], e_1^E[x \leftarrow v^E] \rangle$
 14755 4. QED (2, 3)
 14756 **CASE** $e^1 = e_0^1 e_1^1$:
 14757 1. $e^E = e_0^E e_1^E$
 14758 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_0^E[x \leftarrow v^E]$
 14759 $\wedge e_1^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_1^E[x \leftarrow v^E]$
 14760 by the induction hypothesis
 14761 3. $e^1[x \leftarrow v^1] = e_0^1[x \leftarrow v^1] e_1^1[x \leftarrow v^1]$
 14762 $\wedge e^E[x \leftarrow v^E] = e_0^E[x \leftarrow v^E] e_1^E[x \leftarrow v^E]$
 14763 4. QED (2, 3)
 14764 **CASE** $e^1 = \text{op}^1 e_0^1$:
 14765 1. $e^E = \text{op}^1 e_0^E$
 14766 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_0^E[x \leftarrow v^E]$
 14767 by the induction hypothesis
 14768 3. $e^1[x \leftarrow v^1] = \text{op}^1 e_0^1[x \leftarrow v^1]$
 14769 $\wedge e^E[x \leftarrow v^E] = \text{op}^1 e_0^E[x \leftarrow v^E]$
 14770 4. QED (2, 3)
 14771 **CASE** $e^1 = \text{op}^2 e_0^1 e_1^1$:
 14772 1. $e^E = \text{op}^2 e_0^E e_1^E$
 14773 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_0^E[x \leftarrow v^E]$
 14774 $\wedge e_1^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_1^E[x \leftarrow v^E]$
 14775 by the induction hypothesis
 14776 3. $e^1[x \leftarrow v^1] = \text{op}^2 e_0^1[x \leftarrow v^1] e_1^1[x \leftarrow v^1]$
 14777 $\wedge e^E[x \leftarrow v^E] = \text{op}^2 e_0^E[x \leftarrow v^E] e_1^E[x \leftarrow v^E]$
 14778 4. QED (2, 3)
 14779 **CASE** $e^1 = \text{dyn } \tau e_0^1$:
 14780 1. $e^E = \text{dyn } \tau e_0^E$
 14781 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_0^E[x \leftarrow v^E]$
 14782 by the induction hypothesis
 14783 3. $e^1[x \leftarrow v^1] = \text{dyn } \tau e_0^1[x \leftarrow v^1]$
 14784 $\wedge e^E[x \leftarrow v^E] = \text{dyn } \tau e_0^E[x \leftarrow v^E]$
 14785 4. QED (2, 3)
 14786 **CASE** $e^1 = \text{stat } \tau e_0^1$:
 14787 1. $e^E = \text{stat } \tau e_0^E$
 14788 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e_0^E[x \leftarrow v^E]$
 14789 by the induction hypothesis
 14790 3. $e^1[x \leftarrow v^1] = \text{stat } \tau e_0^1[x \leftarrow v^1]$
 14791 $\wedge e^E[x \leftarrow v^E] = \text{stat } \tau e_0^E[x \leftarrow v^E]$
 14792 4. QED (2, 3)
 14793
 14794
 14795

CASE $e^1 = \text{Err}$:
 14796 1. QED $e^1[x \leftarrow v^1] = \text{Err}$ 14797
CASE $e^1 = \text{chk } K e_0^1$:
 14798 1. $e_0^1 \underset{1}{\lesssim_E} e^E$ 14799
 14800 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e^E[x \leftarrow v^E]$ 14800
 14801 by the induction hypothesis 14801
 14802 3. $e^1[x \leftarrow v^1] = \text{chk } K e_0^1[x \leftarrow v^1]$ 14802
 14803 4. QED (2, 3) 14803
CASE $e^1 = \text{dyn } e_0^1$:
 14804 1. $e_0^1 \underset{1}{\lesssim_E} e^E$ 14805
 14806 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e^E[x \leftarrow v^E]$ 14806
 14807 by the induction hypothesis 14807
 14808 3. $e^1[x \leftarrow v^1] = \text{dyn } e_0^1[x \leftarrow v^1]$ 14808
 14809 4. QED (2, 3) 14809
CASE $e^1 = \text{stat } e_0^1$:
 14810 1. $e_0^1 \underset{1}{\lesssim_E} e^E$ 14811
 14812 2. $e_0^1[x \leftarrow v^1] \underset{1}{\lesssim_E} e^E[x \leftarrow v^E]$ 14812
 14813 by the induction hypothesis 14813
 14814 3. $e^1[x \leftarrow v^1] = \text{stat } e_0^1[x \leftarrow v^1]$ 14814
 14815 4. QED (2, 3) 14815
 14816 \square 14816

Lemma 8.9 : 1-E δ -preservation

- If $v^1 \underset{1}{\lesssim_E} v^E$ and $\delta(\text{op}^1, v^1)$ is defined then $\delta(\text{op}^1, v^1) \underset{1}{\lesssim_E} \delta(\text{op}^1, v^E)$ 14817
- If $v_0^1 \underset{1}{\lesssim_E} v_0^E$ and $v_1^1 \underset{1}{\lesssim_E} v_1^E$ and $\delta(\text{op}^2, v_0^1, v_1^1)$ is defined then $\delta(\text{op}^2, v_0^1, v_1^1) \underset{1}{\lesssim_E} \delta(\text{op}^2, v_0^E, v_1^E)$ 14818

Proof:

CASE $\text{op}^1 = \text{fst}$:
 14819 1. $v^1 = \langle v_0^1, v_1^1 \rangle$ 14819
 14820 by $\delta(\text{fst}, v^1)$ is defined 14820
 14821 2. $v^E = \langle v_0^E, v_1^E \rangle$ 14821
 14822 $\wedge v_0^1 \underset{1}{\lesssim_E} v_0^E$ and $v_1^1 \underset{1}{\lesssim_E} v_1^E$ 14822
 14823 by $\underset{1}{\lesssim_E}$ 14823
 14824 3. $\delta(\text{fst}, v^1) = v_0^1$ 14824
 14825 $\wedge \delta(\text{fst}, v^E) = v_0^E$ 14825
 14826 4. QED (2) 14826
CASE $\text{op}^1 = \text{snd}$:
 14827 1. $v^1 = \langle v_0^1, v_1^1 \rangle$ 14827
 14828 by $\delta(\text{snd}, v^1)$ is defined 14828
 14829 2. $v^E = \langle v_0^E, v_1^E \rangle$ 14829
 14830 $\wedge v_0^1 \underset{1}{\lesssim_E} v_0^E$ and $v_1^1 \underset{1}{\lesssim_E} v_1^E$ 14830
 14831 by $\underset{1}{\lesssim_E}$ 14831
 14832 3. $\delta(\text{snd}, v^1) = v_1^1$ 14832
 14833 $\wedge \delta(\text{snd}, v^E) = v_1^E$ 14833
 14834 4. QED (2) 14834
CASE $\text{op}^2 = \text{sum}$:
 14835 1. $v_0^1 \in \mathbb{Z}$ 14835
 14836 $\wedge v_1^1 \in \mathbb{Z}$ 14836
 14837 by $\delta(\text{op}^2, v_0^1, v_1^1)$ is defined 14837
 14838 2. $v_0^1 = v_0^E$ 14838
 14839 $\wedge v_1^1 = v_1^E$ 14839
 14840 by $\underset{1}{\lesssim_E}$ 14840
 14841 3. QED 14841

14851 **CASE** $op^2 = \text{quotient}$:
 14852 1. $v_0^1 \in \mathbb{Z}$
 14853 $\wedge v_1^1 \in \mathbb{Z}$
 14854 by $\delta(op^2, v_0^1, v_1^1)$ is defined
 14855 2. $v_0^1 = v_0^E$
 14856 $\wedge v_1^1 = v_1^E$
 14857 by $1 \lesssim_E$
 14858 3. QED
 14859 \square

14860
 14861
 14862
 14863
 14864
 14865
 14866
 14867
 14868
 14869
 14870
 14871
 14872
 14873
 14874
 14875
 14876
 14877
 14878
 14879
 14880
 14881
 14882
 14883
 14884
 14885
 14886
 14887
 14888
 14889
 14890
 14891
 14892
 14893
 14894
 14895
 14896
 14897
 14898
 14899
 14900
 14901
 14902
 14903
 14904
 14905

Lemma 8.10 : H-1 approximation

If $e \in e_S$ and $\vdash e : \tau$ and $\vdash_1 e : [\tau] \rightsquigarrow e''$ and $e'' \rightarrow_{1-S}^* \text{Err}$
 then $e \rightarrow_{H-S}^* \text{Err}$

Proof:

- $e \text{ H}\lesssim_1 e''$
by H-1 static reflexivity
- QED by H-1 simulation

\square

Lemma 8.11 : H-1 static reflexivity

If $\Gamma \vdash e : \tau$
 $\wedge \Gamma \vdash_1 e : [\tau] \rightsquigarrow e''$
 then $e \text{ H}\lesssim_1 e''$.

Proof:

By structural induction on the $\Gamma \vdash_1 e : [\tau] \rightsquigarrow e''$ judgment.

CASE $\frac{}{\Gamma \vdash i : \text{Nat} \rightsquigarrow i}$:

1. QED $i \text{ H}\lesssim_1 i$

CASE $\frac{}{\Gamma \vdash i : \text{Int} \rightsquigarrow i}$:

1. QED $i \text{ H}\lesssim_1 i$

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1 \rightsquigarrow \langle e'_0, e'_1 \rangle}$:

1. $e'_0 \text{ H}\lesssim_1 e_0$
 $\wedge e'_1 \text{ H}\lesssim_1 e_1$
by the induction hypothesis
2. QED

CASE $\frac{(x:\tau_d), \Gamma \vdash e : \tau_c \rightsquigarrow e'}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c \rightsquigarrow \lambda(x:\tau_d). e'}$:

1. $e' \text{ H}\lesssim_1 e$
by the induction hypothesis
2. QED

CASE $\frac{}{\Gamma \vdash x : \tau \rightsquigarrow x}$:

1. QED $x \text{ H}\lesssim_1 x$

CASE $\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_d \rightsquigarrow e'_1 \quad [\tau_c] = K}{\Gamma \vdash e_0 e_1 : \tau_c \rightsquigarrow \text{chk } K (e'_0 e'_1)}$

1. $e'_0 \text{ H}\lesssim_1 e_0$
 $\wedge e'_1 \text{ H}\lesssim_1 e_1$
by the induction hypothesis
2. $e'_0 e'_1 \text{ H}\lesssim_1 e_0 e_1$
3. QED $\text{chk } K e'_0 e'_1 \text{ H}\lesssim_1 e_0 e_1$

CASE $\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad [\tau_0] = K}{\Gamma \vdash \text{fst } e : \tau_0 \rightsquigarrow \text{chk } K (\text{fst } e')}$:

1. $e' \text{ H}\lesssim_1 e$
by the induction hypothesis
2. $\text{fst } e' \text{ H}\lesssim_1 \text{fst } e$
3. QED $\text{chk } K \text{fst } e' \text{ H}\lesssim_1 \text{fst } e$

14906
 14907
 14908
 14909
 14910
 14911
 14912
 14913
 14914
 14915
 14916
 14917
 14918
 14919
 14920
 14921
 14922
 14923
 14924
 14925
 14926
 14927
 14928
 14929
 14930
 14931
 14932
 14933
 14934
 14935
 14936
 14937
 14938
 14939
 14940
 14941
 14942
 14943
 14944
 14945
 14946
 14947
 14948
 14949
 14950
 14951
 14952
 14953
 14954
 14955
 14956
 14957
 14958
 14959
 14960

14961 **CASE**
$$\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad [\tau_1] = K}{\Gamma \vdash \text{snd } e : \tau_1 \rightsquigarrow \text{chk } K (\text{snd } e')}$$
 :

1. $e' \text{H}\lesssim_1 e$
by the induction hypothesis
2. $\text{snd } e' \text{H}\lesssim_1 \text{snd } e$
3. QED $\text{chk } K \text{snd } e' \text{H}\lesssim_1 \text{snd } e$

14968 **CASE**
$$\frac{\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau \rightsquigarrow \text{op}^2 e'_0 e'_1}$$
 :

1. $e'_0 \text{H}\lesssim_1 e_0$
 $\wedge e'_1 \text{H}\lesssim_1 e_1$
by the induction hypothesis
2. QED

14976 **CASE**
$$\frac{\Gamma \vdash e : \tau' \rightsquigarrow e' \quad \tau' \leq \tau}{\Gamma \vdash e : \tau \rightsquigarrow e'}$$
 :

1. QED by the induction hypothesis

14980 **CASE**
$$\frac{}{\Gamma \vdash \text{Err} : \tau \rightsquigarrow \text{Err}}$$
 :

1. QED $\text{Err} \text{H}\lesssim_1 \text{Err}$

14984 **CASE**
$$\frac{\Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash \text{dyn } \tau e : \tau \rightsquigarrow \text{dyn } \tau e'}$$
 :

1. $e' \text{H}\lesssim_1 e$
by the induction hypothesis
2. QED

□

Lemma 8.12 : H-1 dynamic reflexivity

If $\Gamma \vdash e$
 $\wedge \Gamma \vdash_1 e \rightsquigarrow e''$
then $e \text{H}\lesssim_1 e''$.

Proof:

By structural induction on the $\Gamma \vdash_1 e \rightsquigarrow e''$ judgment.

14997 **CASE**
$$\frac{}{\Gamma \vdash i \rightsquigarrow i}$$
 :

1. QED $i \text{H}\lesssim_1 i$

15000 **CASE**
$$\frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash \langle e_0, e_1 \rangle \rightsquigarrow \langle e'_0, e'_1 \rangle}$$
 :

1. $e'_0 \text{H}\lesssim_1 e_0$
 $\wedge e'_1 \text{H}\lesssim_1 e_1$
by the induction hypothesis
2. QED

15008 **CASE**
$$\frac{x, \Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash \lambda x. e \rightsquigarrow \lambda x. e'}$$
 :

1. $e' \text{H}\lesssim_1 e$
by the induction hypothesis
2. QED

15016 **CASE**
$$\frac{}{\Gamma \vdash x \rightsquigarrow x}$$
 :

1. QED $x \text{H}\lesssim_1 x$

15020 **CASE**
$$\frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash e_0 e_1 \rightsquigarrow e'_0 e'_1}$$
 :

1. $e'_0 \text{H}\lesssim_1 e_0$
 $\wedge e'_1 \text{H}\lesssim_1 e_1$
by the induction hypothesis
2. QED

15027 **CASE**
$$\frac{\Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash \text{op}^1 e \rightsquigarrow \text{op}^1 e'}$$
 :

1. $e' \text{H}\lesssim_1 e$
by the induction hypothesis
2. QED

15033 **CASE**
$$\frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash \text{op}^2 e_0 e_1 \rightsquigarrow \text{op}^2 e'_0 e'_1}$$
 :

1. $e'_0 \text{H}\lesssim_1 e_0$
 $\wedge e'_1 \text{H}\lesssim_1 e_1$
by the induction hypothesis
2. QED

15041 **CASE**
$$\frac{}{\Gamma \vdash \text{Err} \rightsquigarrow \text{Err}}$$
 :

1. QED $\text{Err} \text{H}\lesssim_1 \text{Err}$

15044 **CASE**
$$\frac{\Gamma \vdash e : \tau \rightsquigarrow e'}{\Gamma \vdash \text{stat } \tau e \rightsquigarrow \text{stat } \tau e'}$$
 :

1. $e' \text{H}\lesssim_1 e$
by 1-E static reflexivity
2. QED

□

Lemma 8.13 : H-1 simulation

If $\vdash_H E^H[e_0^H] : \tau$
 $\wedge \vdash_1 E^1[e_0^1] : [\tau]$
 $\wedge E^H[e_0^H] \text{H}\lesssim_1 E^1[e_0^1]$
 $\wedge E^1[e_0^1] \rightarrow_{1-S} E^1[e_1^1]$
then $E^H[e_0^H] \rightarrow_{H-S}^* E^H[e_n^H]$ and $E^H[e_n^H] \text{H}\lesssim_1 E^1[e_1^1]$

Proof:

By case analysis on $E^1[e_0^1] \rightarrow_{1-S} E^1[e_1^1]$ **CASE** $E^1[\text{dyn } v_0^1] \rightarrow_{1-S} E^1[v_0^1]$:

1. $e_0^H = \text{dyn } \tau_0 e_{0'}^H$
 $\wedge e_{0'}^H \text{H}\lesssim_1 v_0^1$
by $\text{H}\lesssim_1$
2. $\vdash_H e_{0'}^H$
by $\vdash_H E^H[e_0^H] : \tau$
3. $e_{0'}^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$
 $\vee e_{0'}^H \rightarrow_{H-S}^* \text{BndryErr}$
by H-1 static value stutter (1, 2)
4. **IF** $e_{0'}^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$:

15071	a. $\vdash_H v_0^H$	3. $e_{0'}^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	15126
15072	by H static preservation	$\vee e_{0'}^H \rightarrow_{H-S}^* \text{BndryErr}$	15127
15073	b. $\text{dyn } \tau_0 v_0^H \rightarrow_{H-S}^* e_{1'}^H$	by H-1 static value stutter (1, 2)	15128
15074	$\wedge e_{1'}^H \text{H}\lesssim_1 v_0^1$	4. IF $e_{0'}^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$:	15129
15075	$\wedge e_{1'}^H \in v$ or $e_{1'}^H = \text{BndryErr}$	a. $\vdash_H v_0^H$	15130
15076	by H-1 boundary checking	by H static preservation	15131
15077	c. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* E^H[e_1^H]$	b. $\text{dyn } \tau_0 v_0^H \rightarrow_{H-S}^* e_{1'}^H$	15132
15078	ELSE $e_{0'}^H \rightarrow_{H-S}^* \text{BndryErr}$:	$\wedge e_{1'}^H \text{H}\lesssim_1 v_0^1$	15133
15079	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	$\wedge e_{1'}^H \in v$ or $e_{1'}^H = \text{BndryErr}$	15134
15080	CASE $E^1[\text{stat } v_0^1] \rightarrow_{1-S} E^1[v_0^1]$:	by H-1 boundary checking	15135
15081	1. $e_0^H = \text{stat } \tau_0 e_{0'}^H$	c. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* E^H[e_1^H]$	15136
15082	$\wedge e_{0'}^H \text{H}\lesssim_1 v_0^1$	ELSE $e_{0'}^H \rightarrow_{H-S}^* \text{BndryErr}$:	15137
15083	by $\text{H}\lesssim_1$	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	15138
15084	2. $\vdash_H e_{0'}^H : \tau_0$	CASE $E^1[\text{stat } \tau_0 v_0^1] \rightarrow_{1-S} E^1[v_0^1]$:	15139
15085	by $\vdash_H E^H[e_0^H] : \tau$	1. $e_0^H = \text{stat } \tau_0 e_{0'}^H$	15140
15086	3. $e_{0'}^H \rightarrow_{H-D} v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	$\wedge e_{0'}^H \text{H}\lesssim_1 v_0^1$	15141
15087	$\vee e_{0'}^H \rightarrow_{H-D} \text{BndryErr}$	by $\text{H}\lesssim_1$	15142
15088	by H-1 dynamic value stutter (1, 2)	2. $\vdash_H e_{0'}^H : \tau_0$	15143
15089	4. IF $e_{0'}^H \rightarrow_{H-D} v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$:	by $\vdash_H E^H[e_0^H] : \tau$	15144
15090	a. $\vdash_H v_0^H : \tau_0$	3. $e_{0'}^H \rightarrow_{H-D} v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	15145
15091	by H dynamic preservation	$\vee e_{0'}^H \rightarrow_{H-D} \text{BndryErr}$	15146
15092	b. $\text{stat } \tau_0 v_0^H \rightarrow_{H-D} e_{1'}^H$	by H-1 dynamic value stutter (1, 2)	15147
15093	$\wedge e_{1'}^H \text{H}\lesssim_1 v_0^1$	4. IF $e_{0'}^H \rightarrow_{H-D} v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$:	15148
15094	$\wedge e_{1'}^H \in v$ or $e_{1'}^H = \text{BndryErr}$	a. $\vdash_H v_0^H : \tau_0$	15149
15095	by H-1 boundary checking	by H dynamic preservation	15150
15096	c. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* E^H[e_1^H]$	b. $\text{stat } \tau_0 v_0^H \rightarrow_{H-D} e_{1'}^H$	15151
15097	ELSE $e_{0'}^H \rightarrow_{H-D} \text{BndryErr}$:	$\wedge e_{1'}^H \text{H}\lesssim_1 v_0^1$	15152
15098	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	$\wedge e_{1'}^H \in v$ or $e_{1'}^H = \text{BndryErr}$	15153
15099	CASE $E^1[\text{dyn } \tau_0 v_0^1] \rightarrow_{1-S} E^1[\text{BndryErr}]$:	by H-1 boundary checking	15154
15100	1. $e_0^H = \text{dyn } \tau_0 e_{0'}^H$	c. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* E^H[e_1^H]$	15155
15101	$\wedge e_{0'}^H \text{H}\lesssim_1 v_0^1$	ELSE $e_{0'}^H \rightarrow_{H-D} \text{BndryErr}$:	15156
15102	by $\text{H}\lesssim_1$	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	15157
15103	2. $\vdash_H e_{0'}^H$	CASE $E^1[\text{chk } K_0 v_0^1] \rightarrow_{1-S} E^1[\text{BndryErr}]$:	15158
15104	by $\vdash_H E^H[e_0^H] : \tau$	1. $\vdash_1 \text{chk } K_0 v_0^1 : K_0$	15159
15105	3. $e_{0'}^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	by $\vdash_1 E^1[e_0^1] : K$	15160
15106	$\vee e_{0'}^H \rightarrow_{H-S}^* \text{BndryErr}$	2. $\vdash_H e_{0'}^H : \tau_0$	15161
15107	by H-1 static value stutter (1, 2)	by H-1 static hole typing	15162
15108	4. IF $e_{0'}^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$:	3. $e_0^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	15163
15109	a. $\mathcal{X}([\tau_0], v_0^1) = \text{BndryErr}$	$\vee e_0^H \rightarrow_{H-S}^* \text{BndryErr}$	15164
15110	by $E^1[\text{dyn } \tau_0 v_0^1] \rightarrow_{1-S} E^1[\text{BndryErr}]$	by H-1 static value stutter (2)	15165
15111	b. $\mathcal{D}_H(\tau_0, v_0^H) = \text{BndryErr}$	4. IF $e_0^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$:	15166
15112	by X inversion	a. $\vdash_1 v_0^1 : [\tau_0]$	15167
15113	c. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	by H-1 value inversion (2, 3)	15168
15114	ELSE $e_{0'}^H \rightarrow_{H-S}^* \text{BndryErr}$:	b. $[\tau_0] = K_0$	15169
15115	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	by chk inversion, H-1 static reflexivity, H static preservation, and 1 static preservation	15170
15116	CASE $E^1[\text{dyn } \tau_0 v_0^1] \rightarrow_{1-S} E^1[v_0^1]$:	c. $\text{chk } K_0 v_0^1 \triangleright_{1-S} v_0^1$	15171
15117	1. $e_0^H = \text{dyn } \tau_0 e_{0'}^H$	by definition \triangleright_{1-S}	15172
15118	$\wedge e_{0'}^H \text{H}\lesssim_1 v_0^1$	d. Contradiction by $E^1[\text{chk } K_0 v_0^1] \rightarrow_{1-S} E^1[\text{BndryErr}]$	15173
15119	by $\text{H}\lesssim_1$	(b)	15174
15120	2. $\vdash_H e_{0'}^H$	ELSE $e_0^H \rightarrow_{H-S}^* \text{BndryErr}$:	15175
15121	by $\vdash_H E^H[e_0^H] : \tau$	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	15176
15122			15177
15123			15178
15124			15179
15125			15180

15181	CASE $E^1[\text{chk } K_0 v_0^1] \rightarrow_{1-S} E^1[v_0^1]$:	IF $e_0^H \rightarrow_{H-D}^* \text{BndryErr}$:	15236
15182	1. $\vdash_1 \text{chk } K_0 v_0^1 : K_0$	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	15237
15183	by $\vdash_1 E^1[e_0^1] : K$	ELSE $e_{1'}^H \rightarrow_{H-D}^* \text{BndryErr}$:	15238
15184	2. $\vdash_H e_0^H : \tau_0$	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	15239
15185	by H-1 static hole typing	CASE $E^1[\text{op}^1 v_0^1] \rightarrow_{1-S} E^1[\delta(\text{op}^1, v_0^1)]$	15240
15186	3. $e_0^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	$\wedge \vdash_1 \text{op}^1 v_0^1 : K_0$:	15241
15187	$\vee e_0^H \rightarrow_{H-S}^* \text{BndryErr}$	1. $\vdash_H e_0^H : \tau_0$	15242
15188	by H-1 static value stutter (2)	by H-1 static hole typing	15243
15189	4. IF $e_0^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$:	2. $e_0^H = \text{op}^1 e_0^H$	15244
15190	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* v_0^H$	by $\text{H}\lesssim_1$	15245
15191	ELSE $e_0^H \rightarrow_{H-S}^* \text{BndryErr}$:	3. $\vdash_H e_0^H : \tau_0$	15246
15192	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	by H inversion (1, 2)	15247
15193	CASE $E^1[v_0^1 v_1^1] \rightarrow_{1-S} E^1[e_2^1]$	4. $e_0^H \text{H}\lesssim_1 v_0^1$	15248
15194	$\wedge \vdash_1 v_0^1 v_1^1 : K'$:	by $\text{H}\lesssim_1$	15249
15195	1. $\vdash_H e_0^H : \tau_0$	5. $e_0^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	15250
15196	by H-1 static hole typing	$\vee e_0^H \rightarrow_{H-S}^* \text{BndryErr}$	15251
15197	2. $e_0^H = e_0^H e_1^H$	by H-1 static value stutter	15252
15198	by $\text{H}\lesssim_1$	6. IF $e_0^H \rightarrow_{H-S}^* v_0^H$:	15253
15199	3. $e_0^H \rightarrow_{H-S}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	a. $\text{op}^1 v_0^H \triangleright_{H-S} \delta(\text{op}^1, v_0^H)$	15254
15200	$\vee e_0^H \rightarrow_{H-S}^* \text{BndryErr}$	by \triangleright_{H-S}	15255
15201	by H-1 static value stutter (1, 2)	b. $\delta(\text{op}^1, v_0^H) \text{H}\lesssim_1 \delta(\text{op}^1, v_0^1)$	15256
15202	4. $e_1^H \rightarrow_{H-S}^* v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$	by H-1 δ-preservation	15257
15203	$\vee e_1^H \rightarrow_{H-S}^* \text{BndryErr}$	c. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* E^H[\delta(\text{op}^1, v_0^H)]$	15258
15204	by H-1 static value stutter (1, 2)	ELSE $e_0^H \rightarrow_{H-S}^* \text{BndryErr}$:	15259
15205	5. IF $e_0^H \rightarrow_{H-S}^* v_0^H$	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	15260
15206	$\wedge e_1^H \rightarrow_{H-S}^* v_1^H$:	CASE $E^1[\text{op}^1 v_0^1] \rightarrow_{1-S} E^1[\delta(\text{op}^1, v_0^1)]$	15261
15207	a. $v_0^H v_1^H \rightarrow_{H-S}^* e_2^H$	$\wedge \vdash_1 \text{op}^1 v_0^1$:	15262
15208	$\wedge e_2^H \text{H}\lesssim_1 e_2^1$	1. $\vdash_H e_0^H$	15263
15209	by H-1 static application (1)	by H-1 dynamic hole typing	15264
15210	b. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* E^H[e_2^H]$	2. $e_0^H = \text{op}^1 e_0^H$	15265
15211	IF $e_0^H \rightarrow_{H-S}^* \text{BndryErr}$:	by $\text{H}\lesssim_1$	15266
15212	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	3. $\vdash_H e_0^H : \tau_0$	15267
15213	ELSE $e_1^H \rightarrow_{H-S}^* \text{BndryErr}$:	by H inversion (1, 2)	15268
15214	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	4. $e_0^H \text{H}\lesssim_1 v_0^1$	15269
15215	CASE $E^1[v_0^1 v_1^1] \rightarrow_{1-S} E^1[e_2^1]$	by $\text{H}\lesssim_1$	15270
15216	$\wedge \vdash_1 v_0^1 v_1^1$:	5. $e_0^H \rightarrow_{H-D}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	15271
15217	1. $\vdash_H e_0^H$	$\vee e_0^H \rightarrow_{H-D}^* \text{BndryErr}$	15272
15218	by H-1 static hole typing	by H-1 dynamic value stutter	15273
15219	2. $e_0^H = e_0^H e_1^H$	6. IF $e_0^H \rightarrow_{H-D}^* v_0^H$:	15274
15220	by $\text{H}\lesssim_1$	a. $\text{op}^1 v_0^H \triangleright_{H-D} \delta(\text{op}^1, v_0^H)$	15275
15221	3. $e_0^H \rightarrow_{H-D}^* v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	by \triangleright_{H-D}	15276
15222	$\vee e_0^H \rightarrow_{H-D}^* \text{BndryErr}$	b. $\delta(\text{op}^1, v_0^H) \text{H}\lesssim_1 \delta(\text{op}^1, v_0^1)$	15277
15223	by H-1 dynamic value stutter (1, 2)	by H-1 δ-preservation	15278
15224	4. $e_1^H \rightarrow_{H-D}^* v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$	c. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* E^H[\delta(\text{op}^1, v_0^H)]$	15279
15225	$\vee e_1^H \rightarrow_{H-D}^* \text{BndryErr}$	ELSE $e_0^H \rightarrow_{H-D}^* \text{BndryErr}$:	15280
15226	by H-1 dynamic value stutter (1, 2)	a. $\text{QED } E^H[e_0^H] \rightarrow_{H-S}^* \text{BndryErr}$	15281
15227	5. IF $e_0^H \rightarrow_{H-D}^* v_0^H$	CASE $E^1[\text{op}^1 v_0^1] \rightarrow_{1-S} E^1[\text{TagErr}]$:	15282
15228	$\wedge e_1^H \rightarrow_{H-D}^* v_1^H$:	1. $\vdash_1 \text{op}^1 v_0^1$	15283
15229	a. $v_0^H v_1^H \rightarrow_{H-D}^* e_2^H$	by definition \rightarrow_{1-S}	15284
15230	$\wedge e_2^H \text{H}\lesssim_1 e_2^1$	2. $\vdash_H e_0^H$	15285
15231	by H-1 dynamic application (1)	by H-1 dynamic hole typing (1)	15286
15232	b. $\text{QED } E^H[e_0^H] \rightarrow_{H-D}^* E^H[e_2^H]$		15287
15233			15288
15234			15289
15235			15290

15291	3. $e_0^H = op^1 e_{0'}^H$	2. $e_0^H = op^2 e_{0'}^H e_{1'}^H$	15346
15292	by $H \lesssim_1$	by $H \lesssim_1$	15347
15293	4. $\vdash_H e_{0'}^H : \tau_0$	3. $\vdash_H e_{0'}^H$	15348
15294	by H inversion (2, 3)	$\wedge \vdash_H e_{1'}^H$	15349
15295	5. $e_{0'}^H \xrightarrow{H \lesssim_1} v_0^1$	by H inversion (1, 2)	15350
15296	by $H \lesssim_1$	4. $e_{0'}^H \xrightarrow{H \lesssim_1} v_0^1$	15351
15297	6. $e_{0'}^H \xrightarrow{*}_{H-D} v_0^H$ and $v_0^H \xrightarrow{H \lesssim_1} v_0^1$	$\wedge e_{1'}^H \xrightarrow{H \lesssim_1} v_1^1$	15352
15298	$\vee e_{0'}^H \xrightarrow{*}_{H-D} \text{BndryErr}$	by $H \lesssim_1$	15353
15299	by H-1 dynamic value stutter	5. $e_{0'}^H \xrightarrow{*}_{H-D} v_0^H$ and $v_0^H \xrightarrow{H \lesssim_1} v_0^1$	15354
15300	7. IF $e_{0'}^H \xrightarrow{*}_{H-D} v_0^H$:	$\vee e_{0'}^H \xrightarrow{*}_{H-D} \text{BndryErr}$	15355
15301	a. $\delta(op^1, v_0^1)$ is undefined	by H-1 dynamic value stutter	15356
15302	by definition \triangleright_{H-D}	6. $e_{1'}^H \xrightarrow{*}_{H-D} v_1^H$ and $v_1^H \xrightarrow{H \lesssim_1} v_1^1$	15357
15303	b. $v_0^1 \notin \langle v, v \rangle$	$\vee e_{1'}^H \xrightarrow{*}_{H-D} \text{BndryErr}$	15358
15304	by (a)	by H-1 dynamic value stutter	15359
15305	c. $v_0^H \notin \langle v, v \rangle$	7. IF $e_{0'}^H \xrightarrow{*}_{H-D} v_0^H$	15360
15306	by $v_0^H \xrightarrow{H \lesssim_1} v_0^1$	$\wedge e_{1'}^H \xrightarrow{*}_{H-D} v_1^H$:	15361
15307	d. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} \text{TagErr}$	a. $op^2 v_0^H v_1^H \triangleright_{H-D} \delta(op^2, v_0^H, v_1^H)$	15362
15308	ELSE $e_{0'}^H \xrightarrow{*}_{H-D} \text{BndryErr}$:	by \triangleright_{H-D}	15363
15309	a. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} \text{BndryErr}$	b. $\delta(op^2, v_0^H, v_1^H) \xrightarrow{H \lesssim_1} \delta(op^2, v_0^1, v_1^1)$	15364
15310	CASE $E^1[op^2 v_0^1 v_1^1] \rightarrow_{1-S} E^1[\delta(op^2, v_0^1, v_1^1)]$	by H-1 δ-preservation	15365
15311	$\wedge \vdash_1 op^2 v_0^1 v_1^1 : K_0$:	c. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} E^H[\delta(op^2, v_0^H, v_1^H)]$	15366
15312	1. $\vdash_H e_0^H : \tau_0$	IF $e_{0'}^H \xrightarrow{*}_{H-D} \text{BndryErr}$:	15367
15313	by H-1 static hole typing	a. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} \text{BndryErr}$	15368
15314	2. $e_0^H = op^2 e_{0'}^H e_{1'}^H$	ELSE $e_{1'}^H \xrightarrow{*}_{H-D} \text{BndryErr}$:	15369
15315	by $H \lesssim_1$	a. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} \text{BndryErr}$	15370
15316	3. $\vdash_H e_{0'}^H : \tau_0$	CASE $E^1[op^2 v_0^1 v_1^1] \rightarrow_{1-S} E^1[\text{TagErr}]$:	15371
15317	$\wedge \vdash_H e_{1'}^H : \tau_1$	1. $\vdash_1 op^2 v_0^1 v_1^1$	15372
15318	by H inversion (1, 2)	by definition \rightarrow_{1-S}	15373
15319	4. $e_{0'}^H \xrightarrow{H \lesssim_1} v_0^1$	2. $\vdash_H e_0^H$	15374
15320	$\wedge e_{1'}^H \xrightarrow{H \lesssim_1} v_1^1$	by H-1 dynamic hole typing (1)	15375
15321	by $H \lesssim_1$	3. $e_0^H = op^2 e_{0'}^H e_{1'}^H$	15376
15322	5. $e_{0'}^H \xrightarrow{*}_{H-S} v_0^H$ and $v_0^H \xrightarrow{H \lesssim_1} v_0^1$	by $H \lesssim_1$	15377
15323	$\vee e_{0'}^H \xrightarrow{*}_{H-S} \text{BndryErr}$	4. $\vdash_H e_{0'}^H : \tau_0$	15378
15324	by H-1 static value stutter	$\wedge \vdash_H e_{1'}^H : \tau_1$	15379
15325	6. $e_{1'}^H \xrightarrow{*}_{H-S} v_1^H$ and $v_1^H \xrightarrow{H \lesssim_1} v_1^1$	by H inversion (2, 3)	15380
15326	$\vee e_{1'}^H \xrightarrow{*}_{H-S} \text{BndryErr}$	5. $e_{0'}^H \xrightarrow{H \lesssim_1} v_0^1$	15381
15327	by H-1 static value stutter	$\wedge e_{1'}^H \xrightarrow{H \lesssim_1} v_1^1$	15382
15328	7. IF $e_{0'}^H \xrightarrow{*}_{H-S} v_0^H$	by $H \lesssim_1$	15383
15329	$\wedge e_{1'}^H \xrightarrow{*}_{H-S} v_1^H$:	6. $e_{0'}^H \xrightarrow{*}_{H-D} v_0^H$ and $v_0^H \xrightarrow{H \lesssim_1} v_0^1$	15384
15330	a. $op^2 v_0^H v_1^H \triangleright_{H-S} \delta(op^2, v_0^H, v_1^H)$	$\vee e_{0'}^H \xrightarrow{*}_{H-D} \text{BndryErr}$	15385
15331	by \triangleright_{H-D}	by H-1 dynamic value stutter	15386
15332	b. $\delta(op^2, v_0^H, v_1^H) \xrightarrow{H \lesssim_1} \delta(op^2, v_0^1, v_1^1)$	7. $e_{1'}^H \xrightarrow{*}_{H-D} v_1^H$ and $v_1^H \xrightarrow{H \lesssim_1} v_1^1$	15387
15333	by H-1 δ-preservation	$\vee e_{1'}^H \xrightarrow{*}_{H-D} \text{BndryErr}$	15388
15334	c. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} E^H[\delta(op^2, v_0^H, v_1^H)]$	by H-1 dynamic value stutter	15389
15335	IF $e_{0'}^H \xrightarrow{*}_{H-S} \text{BndryErr}$:	8. IF $e_{0'}^H \xrightarrow{*}_{H-D} v_0^H$	15390
15336	a. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} \text{BndryErr}$	$\wedge e_{1'}^H \xrightarrow{*}_{H-D} v_1^H$:	15391
15337	ELSE $e_{1'}^H \xrightarrow{*}_{H-S} \text{BndryErr}$:	a. $\delta(op^2, v_0^1, v_1^1)$ is undefined	15392
15338	a. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} \text{BndryErr}$	by definition \triangleright_{H-D}	15393
15339	ELSE $e_{1'}^H \xrightarrow{*}_{H-S} \text{BndryErr}$:	b. $v_0^1 \notin \mathbb{Z}$	15394
15340	a. $\text{QED } E^H[e_0^H] \xrightarrow{*}_{H-S} \text{BndryErr}$	$\wedge v_1^1 \notin \mathbb{Z}$	15395
15341	CASE $E^1[op^2 v_0^1 v_1^1] \rightarrow_{1-S} E^1[\delta(op^2, v_0^1, v_1^1)]$	by (a)	15396
15342	$\wedge \vdash_1 op^2 v_0^1 v_1^1$:		15397
15343	1. $\vdash_H e_0^H$		15398
15344	by H-1 static hole typing		15399
15345			15400

- 15401 c. $v_0^H \notin \mathbb{Z}$
 15402 by $v_0^H \text{H}\lesssim_1 v_0^1$
 15403 d. $v_1^H \notin \mathbb{Z}$
 15404 by $v_1^H \text{H}\lesssim_1 v_1^1$
 15405 e. QED $E^H[e_0^H] \rightarrow_{\text{H-S}}^* \text{TagErr}$
 15406 **IF** $e_{0'}^H \rightarrow_{\text{H-D}}^* \text{BndryErr}$:
 15407 a. QED $E^H[e_0^H] \rightarrow_{\text{H-S}}^* \text{BndryErr}$
 15408 **ELSE** $e_{1'}^H \rightarrow_{\text{H-D}}^* \text{BndryErr}$:
 15409 a. QED $E^H[e_0^H] \rightarrow_{\text{H-S}}^* \text{BndryErr}$
 15410 \square

Lemma 8.14 : H-1 static application

15412 **If** $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15413 $\wedge \text{H} v_0^H v_1^H : \tau$
 15414 $\wedge \text{H} v_0^1 v_1^1 : \text{Any}$
 15415 $\wedge v_0^1 v_1^1 \rightarrow_{1-S} e_2^1$ then $v_0^H v_1^H \rightarrow_{\text{H-S}}^* e_2^H$ and $e_2^H \text{H}\lesssim_1 e_2^1$
 15416 **Proof**:

15417 By induction on the number of monitors in v_0^H , proceed-
 15418 ing by case analysis on $v_0^1 v_1^1 \rightarrow_{1-S} e_2^1$.

15419 **CASE** $(\lambda(x:\tau_0). e_0^1) v_1^1 \rightarrow_{1-S} \text{BndryErr}$
 15420 $\wedge v_0^H = \lambda(x:\tau_0). e_0^H$:

- 15421 1. $\mathcal{X}([\tau_0], v_1^1) = \text{BndryErr}$
 15422 by definition \triangleright_{1-S}
 15423 2. $\text{H} v_1^H : \tau_1$
 15424 $\wedge \tau_1 \leq \tau_0$
 15425 by **H inversion**
 15426 3. $v_1^H \text{H}\lesssim_1 v_1^1$
 15427 by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15428 4. $\text{H} v_1^1 : [\tau_1]$
 15429 by **H-1 value inversion** (3)
 15430 5. $\text{H} v_1^1 : [\tau_0]$
 15431 by **subtyping preservation** (2)
 15432 6. $\mathcal{X}([\tau_0], v_1^1) = v_1^1$
 15433 by (5)
 15434 7. Contradiction by (1, 6)

15435 **CASE** $(\lambda(x:\tau_0). e_0^1) v_1^1 \rightarrow_{1-S} \text{BndryErr}$
 15436 $\wedge v_0^H = \text{mon}(\tau_d \Rightarrow \tau_c) v_{0'}^H$:

- 15437 1. $v_{0'}^H \text{H}\lesssim_1 v_0^1$
 15438 $\wedge v_1^H \text{H}\lesssim_1 v_1^1$
 15439 by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15440 2. $v_0^H v_1^H \triangleright_{\text{H-S}} \text{dyn } \tau_c (v_{0'}^H (\text{stat } \tau_d v_1^H))$
 15441 by definition $\triangleright_{\text{H-S}}$
 15442 3. $\text{H} \text{stat } \tau_d v_1^H$
 15443 by **H static preservation**
 15444 4. $\text{stat } \tau_d v_1^H \rightarrow_{\text{H-D}}^* v_{1'}^H$ and $v_{1'}^H \text{H}\lesssim_1 v_1^1$
 15445 by **H-1 boundary checking** (1, 3)
 15446 5. $v_{0'}^H = \text{mon}(\tau_d' \Rightarrow \tau_c') v_{0''}^H$ and $v_{0''}^H \text{H}\lesssim_1 v_0^1$
 15447 $\vee v_{0'}^H = \lambda(x:\tau_0). e^H$ and $e^H \text{H}\lesssim_1 e_0^1$
 15448 by (1)
 15449 6. **IF** $v_{0'}^H = \lambda(x:\tau_0). e^H$:
 15450 a. Contradiction by $\text{H} v_0^H v_1^H : \tau$
 15451 7. $v_{0'}^H v_{1'}^H \triangleright_{\text{H-D}} \text{stat } \tau_c' (v_{0''}^H (\text{dyn } \tau_d' v_{1'}^H))$

- 15452 8. $\text{dyn } \tau_d' v_{1'}^H \rightarrow_{\text{H-S}}^* v_{1''}^H$ and $v_{1''}^H \text{H}\lesssim_1 v_1^1$
 15453 $\vee \text{dyn } \tau_d' v_{1'}^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$
 15454 by **H-1 boundary checking**
 15455 9. **IF** $\text{dyn } \tau_d' v_{1'}^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$:
 15456 a. QED $v_0^H v_1^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$
 15457 10. $\text{dyn } \tau_c (\text{stat } \tau_c' []) \text{H}\lesssim_1 []$
 15458 by definition $\text{H}\lesssim_1$
 15459 11. $v_{0''}^H v_{1''}^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15460 12. $\text{H} v_{0''}^H v_{1''}^H : \tau_c'$
 15461 by **H static preservation**
 15462 13. $v_{0''}^H v_{1''}^H \rightarrow_{\text{H-S}}^* e_2^H$
 15463 $\wedge e_2^H \text{H}\lesssim_1 \text{BndryErr}$
 15464 by the induction hypothesis
 15465 14. QED $v_0^H v_1^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$
 15466 **CASE** $(\lambda(x:\tau_0). e_0^1) v_1^1 \rightarrow_{1-S} e_0^1[x \leftarrow \mathcal{X}([\tau_0], v_1^1)]$
 15467 $\wedge v_0^H = \lambda(x:\tau_0). e_0^H$:
 15468 1. $\mathcal{X}([\tau_0], v_1^1) = v_1^1$
 15469 by definition \triangleright_{1-S}
 15470 2. $\text{H} v_1^H : \tau_1$
 15471 $\wedge \tau_1 \leq \tau_0$
 15472 by **H inversion**
 15473 3. $v_1^H \text{H}\lesssim_1 v_1^1$
 15474 $\wedge e_0^H \text{H}\lesssim_1 e_0^1$
 15475 by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15476 4. $(\lambda(x:\tau_0). e_0^H) v_1^H \triangleright_{\text{H-S}} e_0^H[x \leftarrow v_1^H]$
 15477 5. $e_0^H[x \leftarrow v_1^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v_1^1]$
 15478 by **H-1 substitution**
 15479 6. QED $v_0^H v_1^H \rightarrow_{\text{H-S}}^* e_0^H[x \leftarrow v_1^H]$
 15480 **CASE** $(\lambda(x:\tau_0). e_0^1) v_1^1 \rightarrow_{1-S} e_0^1[x \leftarrow \mathcal{X}([\tau_0], v_1^1)]$
 15481 $\wedge v_0^H = \text{mon}(\tau_d \Rightarrow \tau_c) v_{0'}^H$:
 15482 1. $v_{0'}^H \text{H}\lesssim_1 v_0^1$
 15483 $\wedge v_1^H \text{H}\lesssim_1 v_1^1$
 15484 by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15485 2. $v_0^H v_1^H \triangleright_{\text{H-S}} \text{dyn } \tau_c (v_{0'}^H (\text{stat } \tau_d v_1^H))$
 15486 by definition $\triangleright_{\text{H-S}}$
 15487 3. $\text{H} \text{stat } \tau_d v_1^H$
 15488 by **H static preservation**
 15489 4. $\text{stat } \tau_d v_1^H \rightarrow_{\text{H-D}}^* v_{1'}^H$ and $v_{1'}^H \text{H}\lesssim_1 v_1^1$
 15490 by **H-1 boundary checking** (1, 3)
 15491 5. $v_{0'}^H = \text{mon}(\tau_d' \Rightarrow \tau_c') v_{0''}^H$ and $v_{0''}^H \text{H}\lesssim_1 v_0^1$
 15492 $\vee v_{0'}^H = \lambda(x:\tau_0). e^H$ and $e^H \text{H}\lesssim_1 e_0^1$
 15493 by (1)
 15494 6. **IF** $v_{0'}^H = \lambda(x:\tau_0). e^H$:
 15495 a. $\text{H} \text{mon}(\tau_d \Rightarrow \tau_c) v_{0'}^H : \tau_d \Rightarrow \tau_c$
 15496 by $\text{H} v_0^H v_1^H : \tau$
 15497 b. $\text{H} v_{0''}^H$
 15498 by **H inversion** (a)
 15499 c. Contradiction by $\text{H} \lambda(x:\tau_0). e^H$
 15500 7. $v_{0''}^H v_{1'}^H \triangleright_{\text{H-D}} \text{stat } \tau_c' (v_{0''}^H (\text{dyn } \tau_d' v_{1'}^H))$
 15501 8. $\text{H} \text{dyn } \tau_d' v_{1'}^H : \tau_d'$
 15502 by **H dynamic preservation**

15511	9. $\text{dyn } \tau'_d v_1^H \xrightarrow{*}_{\text{H-S}} v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$	2. $v_0^H \in \mathbb{Z}$	15566
15512	$\vee \text{dyn } \tau'_d v_1^H \xrightarrow{*}_{\text{H-S}} \text{BndryErr}$	$\vee v_0^H \in \langle v, v \rangle$	15567
15513	by H-1 boundary checking	by $v_0^H \text{H}\lesssim_1 v_0^1$	15568
15514	10. IF $\text{dyn } \tau'_d v_1^H \xrightarrow{*}_{\text{H-S}} \text{BndryErr}$:	3. QED $v_0^H v_1^H \triangleright_{\text{H-D}} \text{TagErr}$	15569
15515	a. QED $v_0^H v_1^H \xrightarrow{*}_{\text{H-S}} \text{BndryErr}$	CASE $(\lambda(x:\tau_0). e_0^1) v_1^1 \rightarrow_{1\text{-D}} \text{BndryErr}$	15570
15516	11. $\text{dyn } \tau_c (\text{stat } \tau'_c []) \text{H}\lesssim_1 []$	$\wedge v_0^H = \lambda(x:\tau_0). e_0^H :$	15571
15517	by definition $\text{H}\lesssim_1$	1. Contradiction by $\text{H}_H v_0^H v_1^H$	15572
15518	12. $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$	CASE $(\lambda(x:\tau_0). e_0^1) v_1^1 \rightarrow_{1\text{-D}} \text{BndryErr}$	15573
15519	13. $\text{H}_H v_0^H v_1^H : \tau'_c$	$\wedge v_0^H = \text{mon}(\tau_d \Rightarrow \tau_c) v_0^H :$	15574
15520	by H static preservation	1. $v_0^H \text{H}\lesssim_1 v_0^1$	15575
15521	14. $v_0^H v_1^H \xrightarrow{*}_{\text{H-S}} e_2^H$	$\wedge v_1^H \text{H}\lesssim_1 v_1^1$	15576
15522	$\wedge e_2^H \text{H}\lesssim_1 e_2^1$	by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$	15577
15523	by the induction hypothesis	2. $v_0^H v_1^H \triangleright_{\text{H-D}} \text{stat } \tau_c (v_0^H (\text{dyn } \tau_d v_1^H))$	15578
15524	15. QED $v_0^H v_1^H \xrightarrow{*}_{\text{H-S}} \text{dyn } \tau_c (\text{stat } \tau'_c e_2^H)$	by definition $\triangleright_{\text{H-D}}$	15579
15525	CASE $(\lambda x. e_0^1) v_1^1 \rightarrow_{1\text{-S}} \text{dyn } e_0^1[x \leftarrow v_1^1]$	3. $\text{H}_H \text{dyn } \tau_d v_1^H : \tau_d$	15580
15526	$\wedge v_0^H = \lambda x. e_0^H :$	by H dynamic preservation	15581
15527	1. Contradiction by $\text{H}_H v_0^H v_1^H : \tau$	4. $\text{dyn } \tau_d v_1^H \xrightarrow{*}_{\text{H-S}} v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$	15582
15528	CASE $(\lambda x. e_0^1) v_1^1 \rightarrow_{1\text{-S}} \text{dyn } e_0^1[x \leftarrow v_1^1]$	$\vee \text{dyn } \tau_d v_1^H \xrightarrow{*}_{\text{H-S}} \text{BndryErr}$	15583
15529	$\wedge v_0^H = \text{mon}(\tau_d \Rightarrow \tau_c) v_0^H :$	by H-1 boundary checking (1, 3)	15584
15530	1. $v_0^H \text{H}\lesssim_1 (\lambda x. e_0^1)$	5. IF $\text{dyn } \tau_d v_1^H \xrightarrow{*}_{\text{H-S}} \text{BndryErr}$:	15585
15531	$\wedge v_1^H \text{H}\lesssim_1 v_1^1$	a. QED $v_0^H v_1^H \xrightarrow{*}_{\text{H-D}} \text{BndryErr}$	15586
15532	by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$	6. $v_0^H = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$	15587
15533	2. $v_0^H v_1^H \triangleright_{\text{H-S}} \text{dyn } \tau_c (v_0^H (\text{stat } \tau_d v_1^H))$	$\vee v_0^H = \lambda(x:\tau_0). e^H$ and $e^H \text{H}\lesssim_1 e_0^1$	15588
15534	by definition $\triangleright_{\text{H-S}}$	by (1)	15589
15535	3. $\text{H}_H \text{stat } \tau_d v_1^H$	7. IF $v_0^H = \lambda(x:\tau_0). e^H :$	15590
15536	by H static preservation	a. $\mathcal{X}(\lfloor \tau_0 \rfloor, v_1^1) = \text{BndryErr}$	15591
15537	4. $\text{stat } \tau_d v_1^H \xrightarrow{*}_{\text{H-D}} v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$	by definition $\triangleright_{1\text{-D}}$	15592
15538	by H-1 boundary checking	b. $\text{H}_H v_1^H : \tau_1$	15593
15539	5. $\text{dyn } \tau_c [] \text{H}\lesssim_1 \text{dyn } []$	$\wedge \tau_1 \leq \tau_0$	15594
15540	by definition $\text{H}\lesssim_1$	by H inversion	15595
15541	6. $\text{H}_H v_0^H v_1^H$	c. $\text{H}_1 v_1^1 : \lfloor \tau_1 \rfloor$	15596
15542	by H static preservation (2, 3)	by H-1 value inversion (3)	15597
15543	7. $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$	d. $\text{H}_1 v_1^1 : \lfloor \tau_0 \rfloor$	15598
15544	8. $v_0^H v_1^H \xrightarrow{*}_{\text{H-D}} e_2^H$	by subtyping preservation (c)	15599
15545	$\wedge e_2^H \text{H}\lesssim_1 e_2^1$	e. $\mathcal{X}(\lfloor \tau_0 \rfloor, v_1^1) = v_1^1$	15600
15546	by H-1 dynamic application (6, 7)	by (d)	15601
15547	9. QED $v_0^H v_1^H \xrightarrow{*}_{\text{H-S}} \text{dyn } \tau_c e_2^H$	f. Contradiction by (a)	15602
15548	$\wedge \text{dyn } \tau_c e_2^H \text{H}\lesssim_1 \text{dyn } e_2^1$	8. $v_0^H v_1^H \triangleright_{\text{H-S}} \text{dyn } \tau'_c (v_0^H (\text{stat } \tau'_d v_1^H))$	15603
15549	\square	9. $\text{H}_H \text{stat } \tau'_d v_1^H$	15604
15550		by H static preservation	15605
15551	Lemma 8.15 : H-1 dynamic application	10. $\text{stat } \tau'_d v_1^H \xrightarrow{*}_{\text{H-D}} v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$	15606
15552	If $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$	by H-1 boundary checking	15607
15553	$\wedge \text{H}_H v_0^H v_1^H$	11. $\text{stat } \tau_c (\text{dyn } \tau'_c []) \text{H}\lesssim_1 []$	15608
15554	$\wedge \text{H}_1 v_0^1 v_1^1$	by definition $\text{H}\lesssim_1$	15609
15555	$\wedge v_0^1 v_1^1 \rightarrow_{1\text{-D}} e_2^1$ then $v_0^H v_1^H \xrightarrow{*}_{\text{H-D}} e_2^H$ and $e_2^H \text{H}\lesssim_1 e_2^1$	12. $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$	15610
15556	Proof :	13. $\text{H}_H v_0^H v_1^H$	15611
15557	By induction on the number of monitors in v_0^H , proceed-	by H dynamic preservation	15612
15558	ing by case analysis on $v_0^1 v_1^1 \rightarrow_{1\text{-D}} e_2^1$.	14. $v_0^H v_1^H \xrightarrow{*}_{\text{H-D}} e_2^H$	15613
15559	CASE $v_0^1 v_1^1 \triangleright_{1\text{-D}} \text{TagErr}$:	$\wedge e_2^H \text{H}\lesssim_1 \text{BndryErr}$	15614
15560	1. $v_0^1 \in \mathbb{Z}$	by the induction hypothesis	15615
15561	$\vee v_0^1 \in \langle v, v \rangle$	15. QED $v_0^H v_1^H \xrightarrow{*}_{\text{H-D}} \text{BndryErr}$	15616
15562	by definition $\triangleright_{1\text{-D}}$		15617
15563			15618
15564			15619
15565			15620

15621 **CASE** $(\lambda(x:\tau_0).e_0^1) v_1^1 \rightarrow_{1-D} \text{stat } e_0^1[x \leftarrow \mathcal{X}(\lfloor \tau_0 \rfloor, v_1^1)]$
 15622 $\wedge v_0^H = \lambda(x:\tau_0).e_0^H :$
 15623 1. $\vdash_H v_0^H$
 15624 by **H inversion**
 15625 2. Contradiction by $\vdash_H \lambda(x:\tau_0).e_0^H$
 15626 **CASE** $(\lambda(x:\tau_0).e_0^1) v_1^1 \rightarrow_{1-D} \text{stat } e_0^1[x \leftarrow \mathcal{X}(\lfloor \tau_0 \rfloor, v_1^1)]$
 15627 $\wedge v_0^H = \text{mon}(\tau_d \Rightarrow \tau_c) v_0^H :$
 15628 1. $v_0^H \text{H}\lesssim_1 v_1^1$
 15629 $\wedge v_1^H \text{H}\lesssim_1 v_1^1$
 15630 by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15631 2. $v_0^H v_1^H \triangleright_{H-D} \text{stat } \tau_c (v_0^H (\text{dyn } \tau_d v_1^H))$
 15632 by definition \triangleright_{H-D}
 15633 3. $\vdash_H \text{dyn } \tau_d v_1^H : \tau_d$
 15634 by **H dynamic preservation**
 15635 4. $\text{dyn } \tau_d v_1^H \rightarrow_{H-S}^* v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$
 15636 $\vee \text{dyn } \tau_d v_1^H \rightarrow_{H-S}^* \text{BndryErr}$
 15637 by **H-1 boundary checking** (1, 3)
 15638 5. **IF** $\text{dyn } \tau_d v_1^H \rightarrow_{H-S}^* \text{BndryErr} :$
 15639 a. **QED** $v_0^H v_1^H \rightarrow_{H-D}^* \text{BndryErr}$
 15640 6. $\text{stat } \tau_c [] \text{H}\lesssim_1 \text{stat } []$
 15641 by definition of $\text{H}\lesssim_1$
 15642 7. $\vdash_H v_0^H v_1^H : \tau_c$
 15643 by **H dynamic preservation**
 15644 8. $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15645 9. $v_0^H v_1^H \rightarrow_{H-S}^* e_2^H$
 15646 $\wedge e_2^H \text{H}\lesssim_1 e_2^1$
 15647 by **H-1 static application** (7, 8)
 15648 10. **QED** $v_0^H v_1^H \rightarrow_{H-D}^* \text{stat } \tau_c e_2^H$
 15649 $\wedge \text{stat } \tau_c e_2^H \text{H}\lesssim_1 \text{stat } e_2^1$
 15650 **CASE** $(\lambda x. e_0^1) v_1^1 \rightarrow_{1-S} e_0^1[x \leftarrow v_1^1]$
 15651 $\wedge v_0^H = \lambda x. e_0^H :$
 15652 1. $e_0^H \text{H}\lesssim_1 e_0^1$
 15653 $\wedge v_1^H \text{H}\lesssim_1 v_1^1$
 15654 by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15655 2. $v_0^H v_1^H \triangleright_{H-D} e_0^H[x \leftarrow v_1^1]$
 15656 by definition \triangleright_{H-D}
 15657 3. $e_0^H[x \leftarrow v_1^1] \text{H}\lesssim_1 e_0^1[x \leftarrow v_1^1]$
 15658 by **H-1 substitution**
 15659 4. **QED**
 15660 **CASE** $(\lambda x. e_0^1) v_1^1 \rightarrow_{1-D} e_0^1[x \leftarrow v_1^1]$
 15661 $\wedge v_0^H = \text{mon}(\tau_d \Rightarrow \tau_c) v_0^H :$
 15662 1. $v_0^H \text{H}\lesssim_1 (\lambda x. e_0^1) v_1^1 \text{H}\lesssim_1 v_1^1$
 15663 by $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 15664 2. $v_0^H v_1^H \triangleright_{H-D} \text{stat } \tau_c (v_0^H (\text{dyn } \tau_d v_1^H))$
 15665 by definition \triangleright_{H-D}
 15666 3. $\vdash_H \text{dyn } \tau_d v_1^H : \tau_d$
 15667 by **H dynamic preservation**
 15668 4. $\text{dyn } \tau_d v_1^H \rightarrow_{H-D}^* v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$
 15669 $\vee \text{dyn } \tau_d v_1^H \rightarrow_{H-D}^* \text{BndryErr}$
 15670 by **H-1 boundary checking** (1, 3)
 15671 5. **IF** $\text{dyn } \tau_d v_1^H \rightarrow_{H-D}^* \text{BndryErr} :$
 15672 a. **QED** $v_0^H v_1^H \rightarrow_{H-D}^* \text{BndryErr}$
 15673
 15674
 15675

6. $v_0^H = \text{mon}(\tau_d' \Rightarrow \tau_c') v_0^H$ and $v_0^H \text{H}\lesssim_1 v_0^1$
 $\vee v_0^H = \lambda x. e^H$ and $e^H \text{H}\lesssim_1 e_0^1$
 by (1)
 7. **IF** $v_0^H = \lambda x. e^H :$
 a. $\vdash_H v_0^H : \tau_0$
 $\wedge \tau_0 \leq \tau_d \Rightarrow \tau_c$
 by **H inversion**
 b. Contradiction by $\vdash_H \lambda x. e^H : \tau_0$
 8. $v_0^H v_1^H \triangleright_{H-S} \text{dyn } \tau_c' (\text{stat } \tau_d' v_1^H)$
 by definition \triangleright_{H-S}
 9. $\vdash_H \text{stat } \tau_d' v_1^H : \tau_d'$
 by **H static preservation**
 10. $\text{stat } \tau_d' v_1^H \rightarrow_{H-S}^* v_1^H$ and $v_1^H \text{H}\lesssim_1 v_1^1$
 by **H-1 boundary checking**
 11. $\text{stat } \tau_c (\text{dyn } \tau_c' []) \text{H}\lesssim_1 []$
 by definition $\text{H}\lesssim_1$
 12. $v_0^H v_1^H \text{H}\lesssim_1 v_0^1 v_1^1$
 13. $\vdash_H v_0^H v_1^H$
 by **H dynamic preservation**
 14. $v_0^H v_1^H \rightarrow_{H-D}^* e_2^H$
 $\wedge e_2^H \text{H}\lesssim_1 e_2^1$
 by the induction hypothesis
 15. **QED** $v_0^H v_1^H \rightarrow_{H-S}^* \text{stat } \tau_c (\text{dyn } \tau_c' e_2^H)$
 □

Lemma 8.16 : \mathcal{X} inversion

If $\mathcal{X}(\lfloor \tau \rfloor, v^1) = \text{BndryErr}$ and $v^H \text{H}\lesssim_1 v^1$ then $\mathcal{D}_H(\tau, v^H) = \text{BndryErr}$

Proof:

By case analysis on τ .

CASE $\tau = \text{Nat} :$

1. $v^1 \notin \mathbb{N}$
by $\mathcal{X}(\lfloor \tau \rfloor, v^1) = \text{BndryErr}$
2. $v^H \notin \mathbb{N}$
by (1)
3. $\mathcal{D}_H(\tau, v^H) = \text{BndryErr}$
by (2)
4. **QED**

CASE $\tau = \text{Int} :$

1. $v^1 \notin \mathbb{Z}$
by $\mathcal{X}(\lfloor \tau \rfloor, v^1) = \text{BndryErr}$
2. $v^H \notin \mathbb{Z}$
by (1)
3. $\mathcal{D}_H(\tau, v^H) = \text{BndryErr}$
by (2)
4. **QED**

CASE $\tau = \tau_0 \times \tau_1 :$

1. $v^1 \notin \langle v, v \rangle$
by $\mathcal{X}(\lfloor \tau \rfloor, v^1) = \text{BndryErr}$
2. $v^H \notin \langle v, v \rangle$
by (1)
3. $\mathcal{D}_H(\tau, v^H) = \text{BndryErr}$
by (2)
4. **QED**

15676
15677
15678
15679
15680
15681
15682
15683
15684
15685
15686
15687
15688
15689
15690
15691
15692
15693
15694
15695
15696
15697
15698
15699
15700
15701
15702
15703
15704
15705
15706
15707
15708
15709
15710
15711
15712
15713
15714
15715
15716
15717
15718
15719
15720
15721
15722
15723
15724
15725
15726
15727
15728
15729
15730

15731 **CASE** $\tau = \tau_d \Rightarrow \tau_c$:
 15732 1. $v^1 \in \mathbb{Z}$
 15733 $\vee v^1 \in \langle v, v \rangle$
 15734 by $\mathcal{X}(\lfloor \tau \rfloor, v^1) = \text{BndryErr}$
 15735 2. $v^H \in \mathbb{Z}$
 15736 $\vee v^H \in \langle v, v \rangle$
 15737 by (1)
 15738 3. $\mathcal{D}_H(\tau, v^H) = \text{BndryErr}$
 15739 by (2)
 15740 4. QED
 15741 \square

15742 **Lemma 8.17** : H-1 static value stutter

15743 If $e^H \text{H}\lesssim_1 v^1$ and $\vdash_H e^H : \tau$ then one of the following holds:

- 15744 • $e^H \rightarrow_{\text{H-S}}^* v^H$ and $v^H \text{H}\lesssim_1 v^1$
- 15745 • $e^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$

15746 *Proof*:

15747 By induction on the number of boundary terms in e^H ,
 15748 and case analysis on $e^H \text{H}\lesssim_1 v^1$.

15749 **CASE** e^H is a value :

15750 1. QED

15751 **CASE** $e^H = \text{dyn } \tau \text{ (stat } \tau' e_2^H)$:

- 15752 1. $e_2^H \text{H}\lesssim_1 v^1$
 15753 by $\text{H}\lesssim_1$
- 15754 2. $\vdash_H \text{stat } \tau' e_2^H$
 15755 $\wedge \vdash_H e_2^H : \tau'$
 15756 by **H inversion** and **H inversion**
- 15757 3. $e_2^H \rightarrow_{\text{H-S}}^* v_2^H$
 15758 $\wedge v_2^H \text{H}\lesssim_1 v^1$
 15759 by the induction hypothesis (1, 2)
- 15760 4. $\vdash_H \text{stat } \tau' v_2^H$
 15761 by **H static preservation** (2, 3)
- 15762 5. $\text{stat } \tau' v_2^H \rightarrow_{\text{H-S}}^* v_3^H$ and $v_3^H \text{H}\lesssim_1 v^1$
 15763 $\vee \text{stat } \tau' v_2^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$
 15764 by **H-1 boundary checking** (4)
- 15765 6. **IF** $\text{stat } \tau' v_2^H \rightarrow_{\text{H-S}}^* v_3^H$:
 15766 a. $\vdash_H \text{dyn } \tau v_3^H : \tau$
 15767 by **H static preservation** (5)
 15768 b. $\text{dyn } \tau v_3^H \rightarrow_{\text{H-S}}^* v_4^H$ and $v_4^H \text{H}\lesssim_1 v^1$
 15769 $\vee \text{dyn } \tau v_3^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$
 15770 by **H-1 boundary checking** (a)
 15771 c. QED (b)
- 15772 **ELSE** $\text{stat } \tau' v_2^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$:
 15773 a. QED $\text{dyn } \tau \text{ (stat } \tau' e_2^H) \rightarrow_{\text{H-S}}^* \text{BndryErr}$
- 15774 **CASE** $e^H = \text{stat } \tau \text{ (dyn } \tau' e_2^H)$:
 15775 1. Contradiction by $\vdash_H e^H : \tau$

15776 \square

15777 **Lemma 8.18** : H-1 dynamic value stutter

15778 If $e^H \text{H}\lesssim_1 v^1$ and $\vdash_H e^H$ then one of the following holds:

- 15779 • $e^H \rightarrow_{\text{H-D}}^* v^H$ and $v^H \text{H}\lesssim_1 v^1$
- 15780 • $e^H \rightarrow_{\text{H-D}}^* \text{BndryErr}$

15781 *Proof*:

15782

15783

15784

15785

By induction on the number of boundary terms in e^H ,
 and case analysis on $e^H \text{H}\lesssim_1 v^1$.

CASE e^H is a value :

1. QED

CASE $e^H = \text{dyn } \tau \text{ (stat } \tau' e_2^H)$:

1. Contradiction by $\vdash_H e^H : \tau$

CASE $e^H = \text{stat } \tau \text{ (dyn } \tau' e_2^H)$:

1. $e_2^H \text{H}\lesssim_1 v^1$

by $\text{H}\lesssim_1$

2. $\vdash_H \text{dyn } \tau' e_2^H : \tau'$

$\wedge \vdash_H e_2^H$

by **H inversion** and **H inversion**

3. $e_2^H \rightarrow_{\text{H-D}}^* v_2^H$

$\wedge v_2^H \text{H}\lesssim_1 v^1$

by the induction hypothesis (1, 2)

4. $\vdash_H \text{dyn } \tau' v_2^H$

by **H static preservation** (2, 3)

5. $\text{dyn } \tau' v_2^H \rightarrow_{\text{H-S}}^* v_3^H$ and $v_3^H \text{H}\lesssim_1 v^1$

$\vee \text{dyn } \tau' v_2^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$

by **H-1 boundary checking** (4)

6. **IF** $\text{dyn } \tau' v_2^H \rightarrow_{\text{H-S}}^* v_3^H$:

a. $\vdash_H \text{stat } \tau v_3^H : \tau$

by **H static preservation** (5)

b. $\text{stat } \tau v_3^H \rightarrow_{\text{H-S}}^* v_4^H$ and $v_4^H \text{H}\lesssim_1 v^1$

$\vee \text{stat } \tau v_3^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$

by **H-1 boundary checking** (a)

c. QED (b)

ELSE $\text{dyn } \tau' v_2^H \rightarrow_{\text{H-S}}^* \text{BndryErr}$:

a. QED $\text{stat } \tau \text{ (dyn } \tau' e_2^H) \rightarrow_{\text{H-S}}^* \text{BndryErr}$

\square

Lemma 8.19 : H-1 static hole typing

If $\vdash_H E^H[e^H] : \tau$

$\wedge \vdash_1 E^1[e^1] : K$

$\wedge E^H[e^H] \text{H}\lesssim_1 E^1[e^1]$

then one of the following holds:

- $\vdash_H e^H : \tau'$
- $\wedge \vdash_1 e^1 : K'$
- $\vdash_H e^H$
- $\wedge \vdash_1 e^1$

Proof:

By induction on the structure of $E^H[e^H] \text{H}\lesssim_1 E^1[e^1]$
 judgment.

CASE $[\] \text{H}\lesssim_1 [\]$:

1. $E^H[e^H] = e^H$

2. $E^1[e^1] = e^1$

3. QED

CASE $E^H \text{H}\lesssim_1 \text{chk } K E_0^1$:

1. $E^1[e^1] = \text{chk } K E_0^1[e^1]$

2. $\vdash_1 E_0^1[e^1] : \text{Any}$

by **1 inversion**

3. $E^H[e^H] \text{H}\lesssim_1 E_0^1[e^1]$

4. QED by the induction hypothesis

CASE $E_0^H e_1^H \text{H}\lesssim_1 E_0^1 e_1^1$:

15841	1. $E^H[e^H] = E_0^H[e^H] e_1^H$	4. $E_1^H[e^H]_{H \lesssim 1} E_1^1[e^1]$	15896
15842	$\wedge E^1[e^1] = E_0^1[e^1] e_1^1$	5. QED by the induction hypothesis	15897
15843	2. $\vdash_H E_0^H[e^H] : \tau_d \Rightarrow \tau_c$	CASE $\text{dyn } \tau_0 E_0^H_{H \lesssim 1} \text{dyn } \tau_0 E_0^1 :$	15898
15844	by H inversion	1. $E^H[e^H] = \text{dyn } \tau_0 E_0^H[e^H]$	15899
15845	3. $\vdash_1 E_0^1[e^1] : \text{Fun}$	$\wedge E^1[e^1] = \text{dyn } \tau_0 E_0^1[e^1]$	15900
15846	4. $E_0^H[e^H]_{H \lesssim 1} E_0^1[e^1]$	2. $\vdash_H E_0^H[e^H]$	15901
15847	5. QED by the induction hypothesis	$\wedge \vdash_1 E_0^1[e^1]$	15902
15848	CASE $v_0^H E_1^H_{H \lesssim 1} v_0^1 E_1^1 :$	3. $E_0^H[e^H]_{H \lesssim 1} E_0^1[e^1]$	15903
15849	1. $E^H[e^H] = v_0^H E_1^H[e^H]$	4. QED H-1 dynamic hole typing	15904
15850	$\wedge E^1[e^1] = v_0^1 E_1^1[e^1]$	CASE $\text{dyn } \tau_0 E_0^H_{H \lesssim 1} \text{dyn } E_0^1 :$	15905
15851	2. $\vdash_H E_1^H[e^H] : \tau_d$	1. $E^H[e^H] = \text{dyn } \tau_0 E_0^H[e^H]$	15906
15852	by H inversion	$\wedge E^1[e^1] = \text{dyn } E_0^1[e^1]$	15907
15853	3. $\vdash_1 E_1^1[e^1] : \text{Any}$	2. $\vdash_H E_0^H[e^H]$	15908
15854	4. $E_1^H[e^H]_{H \lesssim 1} E_1^1[e^1]$	$\wedge \vdash_1 E_0^1[e^1]$	15909
15855	5. QED by the induction hypothesis	3. $E_0^H[e^H]_{H \lesssim 1} E_0^1[e^1]$	15910
15856	CASE $\langle E_0^H, e_1^H \rangle_{H \lesssim 1} \langle E_0^1, e_1^1 \rangle :$	4. QED H-1 dynamic hole typing	15911
15857	1. $E^H[e^H] = \langle E_0^H[e^H], e_1^H \rangle$	CASE $\text{dyn } \tau_0 (\text{stat } \tau_1 E_0^H)_{H \lesssim 1} E_0^1 :$	15912
15858	$\wedge E^1[e^1] = \langle E_0^1[e^1], e_1^1 \rangle$	1. $E^H[e^H] = \text{dyn } \tau_0 (\text{stat } \tau_1 E_0^H[e^H])$	15913
15859	2. $\vdash_H E_0^H[e^H] : \tau_0$	2. $\vdash_H \text{stat } \tau_1 E_0^H[e^H]$	15914
15860	by H inversion	3. $\vdash_H E_0^H[e^H] : \tau_1$	15915
15861	3. $\vdash_1 E_0^1[e^1] : \text{Any}$	4. $E_0^H[e^H]_{H \lesssim 1} E^1[e^1]$	15916
15862	4. $E_0^H[e^H]_{H \lesssim 1} E_0^1[e^1]$	5. QED by the induction hypothesis	15917
15863	5. QED by the induction hypothesis	CASE $\text{stat } \tau_0 E_0^H_{H \lesssim 1} \text{stat } \tau_0 E_0^1 :$	15918
15864	CASE $\langle v_0^H, E_1^H \rangle_{H \lesssim 1} \langle v_0^1, E_1^1 \rangle :$	1. Contradiction by $\vdash_H E^H[e^H] : \tau_0$	15919
15865	1. $E^H[e^H] = \langle v_0^H, E_1^H[e^H] \rangle$	CASE $\text{stat } \tau_0 E_0^H_{H \lesssim 1} \text{stat } E_0^1 :$	15920
15866	$\wedge E^1[e^1] = \langle v_0^1, E_1^1[e^1] \rangle$	1. Contradiction by $\vdash_H E^H[e^H] : \tau_0$	15921
15867	2. $\vdash_H E_1^H[e^H] : \tau_1$	CASE $\text{stat } \tau_0 (\text{dyn } \tau_1 E_0^H)_{H \lesssim 1} E_0^1 :$	15922
15868	by H inversion	1. Contradiction by $\vdash_H E^H[e^H] : \tau$	15923
15869	3. $\vdash_1 E_1^1[e^1] : \text{Any}$		15924
15870	4. $E_1^H[e^H]_{H \lesssim 1} E_1^1[e^1]$	□	15925
15871	5. QED by the induction hypothesis	Lemma 8.20 : H-1 dynamic hole typing	15926
15872	CASE $op^1 E_0^H_{H \lesssim 1} op^1 E_0^1 :$	If $\vdash_H E^H[e^H]$	15927
15873	1. $E^H[e^H] = op^1 E_0^H[e^H]$	$\wedge \vdash_1 E^1[e^1]$	15928
15874	$\wedge E^1[e^1] = op^1 E_0^1[e^1]$	$\wedge E^H[e^H]_{H \lesssim 1} E^1[e^1]$	15929
15875	2. $\vdash_H E_0^H[e^H] : \tau_0 \times \tau_1$	then one of the following holds:	15930
15876	by H inversion	• $\vdash_H e^H : \tau'$	15931
15877	3. $\vdash_1 E_0^1[e^1] : \text{Pair}$	$\wedge \vdash_1 e^1 : K$	15932
15878	4. $E_0^H[e^H]_{H \lesssim 1} E_0^1[e^1]$	• $\vdash_H e^H$	15933
15879	5. QED by the induction hypothesis	$\wedge \vdash_1 e^1$	15934
15880	CASE $op^2 E_0^H e_1^H_{H \lesssim 1} op^2 E_0^1 e_1^1 :$	<i>Proof:</i>	15935
15881	1. $E^H[e^H] = op^2 E_0^H[e^H] e_1^H$	By induction on the structure of the $E^H[e^H]_{H \lesssim 1} E^1[e^1]$	15936
15882	$\wedge E^1[e^1] = op^2 E_0^1[e^1] e_1^1$	judgment.	15937
15883	2. $\vdash_H E_0^H[e^H] : \tau_0$	CASE $[\]_{H \lesssim 1} [\] :$	15938
15884	by H inversion	1. $E^H[e^H] = e^H$	15939
15885	3. $\vdash_1 E_0^1[e^1] : K_0$	2. $E^1[e^1] = e^1$	15940
15886	4. $E_0^H[e^H]_{H \lesssim 1} E_0^1[e^1]$	3. QED	15941
15887	5. QED by the induction hypothesis	CASE $E^H_{H \lesssim 1} \text{chk } K E_0^1 :$	15942
15888	CASE $op^2 v_0^H E_1^H_{H \lesssim 1} op^2 v_0^1 E_1^1 :$	1. Contradiction by $\vdash_1 E^1[e^1]$	15943
15889	1. $E^H[e^H] = op^2 v_0^H E_1^H[e^H]$	CASE $E_0^H e_1^H_{H \lesssim 1} E_0^1 e_1^1 :$	15944
15890	$\wedge E^1[e^1] = op^2 v_0^1 E_1^1[e^1]$	1. $E^H[e^H] = E_0^H[e^H] e_1^H$	15945
15891	2. $\vdash_H E_1^H[e^H] : \tau_1$	$\wedge E^1[e^1] = E_0^1[e^1] e_1^1$	15946
15892	by H inversion	2. $\vdash_H E_0^H[e^H]$	15947
15893	3. $\vdash_1 E_1^1[e^1] : K_1$	by H inversion	15948
15894			15949
15895			15950

15951	3. $\vdash E_0^1[e^1]$	CASE $\text{dyn } \tau_0 E_0^H \text{ H}\lesssim_1 \text{dyn } \tau_0 E_0^1 :$	16006
15952	4. $E_0^H[e^H] \text{ H}\lesssim_1 E_0^1[e^1]$	1. Contradiction by $\vdash_H E^H[e^H]$	16007
15953	5. QED by the induction hypothesis	CASE $\text{dyn } \tau_0 E_0^H \text{ H}\lesssim_1 \text{dyn } E_0^1 :$	16008
15954	CASE $v_0^H E_1^H \text{ H}\lesssim_1 v_0^1 E_1^1 :$	1. Contradiction by $\vdash_H E^H[e^H]$	16009
15955	1. $E^H[e^H] = v_0^H E_1^H[e^H]$	CASE $\text{dyn } \tau_0 (\text{stat } \tau_1 E_0^H) \text{ H}\lesssim_1 E_0^1 :$	16010
15956	$\wedge E^1[e^1] = v_0^1 E_1^1[e^1]$	1. Contradiction by $\vdash_H E^H[e^H]$	16011
15957	2. $\vdash_H E_1^H[e^H]$	CASE $\text{stat } \tau_0 E_0^H \text{ H}\lesssim_1 \text{stat } \tau_0 E_0^1 :$	16012
15958	by H inversion	1. $E^H[e^H] = \text{stat } \tau_0 E_0^H[e^H]$	16013
15959	3. $\vdash E_1^1[e^1]$	$\wedge E^1[e^1] = \text{stat } \tau_0 E_0^1[e^1]$	16014
15960	4. $E_1^H[e^H] \text{ H}\lesssim_1 E_1^1[e^1]$	2. $\vdash_H E_0^H[e^H] : \tau_0$	16015
15961	5. QED by the induction hypothesis	$\wedge \vdash E_0^1[e^1] : \lfloor \tau_0 \rfloor$	16016
15962	CASE $\langle E_0^H, e_1^H \rangle \text{ H}\lesssim_1 \langle E_0^1, e_1^1 \rangle :$	3. $E_0^H[e^H] \text{ H}\lesssim_1 E_0^1[e^1]$	16017
15963	1. $E^H[e^H] = \langle E_0^H[e^H], e_1^H \rangle$	4. QED H-1 static hole typing	16018
15964	$\wedge E^1[e^1] = \langle E_0^1[e^1], e_1^1 \rangle$	CASE $\text{stat } \tau_0 E_0^H \text{ H}\lesssim_1 \text{stat } E_0^1 :$	16019
15965	2. $\vdash_H E_0^H[e^H]$	1. $E^H[e^H] = \text{stat } \tau_0 E_0^H[e^H]$	16020
15966	by H inversion	$\wedge E^1[e^1] = \text{stat } E_0^1[e^1]$	16021
15967	3. $\vdash E_0^1[e^1]$	2. $\vdash_H E_0^H[e^H] : \tau_0$	16022
15968	4. $E_0^H[e^H] \text{ H}\lesssim_1 E_0^1[e^1]$	$\wedge \vdash E_0^1[e^1]$	16023
15969	5. QED by the induction hypothesis	3. $E_0^H[e^H] \text{ H}\lesssim_1 E_0^1[e^1]$	16024
15970	CASE $\langle v_0^H, E_1^H \rangle \text{ H}\lesssim_1 \langle v_0^1, E_1^1 \rangle :$	4. QED H-1 static hole typing	16025
15971	1. $E^H[e^H] = \langle v_0^H, E_1^H[e^H] \rangle$	CASE $\text{stat } \tau_0 (\text{dyn } \tau_1 E_0^H) \text{ H}\lesssim_1 E_0^1 :$	16026
15972	$\wedge E^1[e^1] = \langle v_0^1, E_1^1[e^1] \rangle$	1. $E^H[e^H] = \text{stat } \tau_0 (\text{dyn } \tau_1 E_0^H[e^H])$	16027
15973	2. $\vdash_H E_1^H[e^H]$	2. $\vdash_H \text{dyn } \tau_1 E_0^H[e^H] : \tau_1$	16028
15974	by H inversion	3. $\vdash_H E_0^H[e^H]$	16029
15975	3. $\vdash E_1^1[e^1]$	4. $E_0^H[e^H] \text{ H}\lesssim_1 E^1[e^1]$	16030
15976	4. $E_1^H[e^H] \text{ H}\lesssim_1 E_1^1[e^1]$	5. QED by the induction hypothesis	16031
15977	5. QED by the induction hypothesis	□	16032
15978	CASE $op^1 E_0^H \text{ H}\lesssim_1 op^1 E_0^1 :$	Lemma 8.21 : H-1 value inversion	16033
15979	1. $E^H[e^H] = op^1 E_0^H[e^H]$	If $\vdash_H v^H : \tau$	16034
15980	$\wedge E^1[e^1] = op^1 E_0^1[e^1]$	$\wedge v^H \text{ H}\lesssim_1 v^1$	16035
15981	2. $\vdash_H E_0^H[e^H]$	then $\vdash v^1 : \lfloor \tau \rfloor$	16036
15982	by H inversion	<i>Proof</i> :	16037
15983	3. $\vdash E_0^1[e^1]$	By induction on the structure of the $v^H \text{ H}\lesssim_1 v^1$ judgment.	16038
15984	4. $E_0^H[e^H] \text{ H}\lesssim_1 E_0^1[e^1]$	CASE $\langle v_0^H, v_1^H \rangle \text{ H}\lesssim_1 \langle v_0^1, v_1^1 \rangle :$	16039
15985	5. QED by the induction hypothesis	1. $\tau = \tau_0 \times \tau_1$	16040
15986	CASE $op^2 E_0^H e_1^H \text{ H}\lesssim_1 op^2 E_0^1 e_1^1 :$	by H inversion	16041
15987	1. $E^H[e^H] = op^2 E_0^H[e^H] e_1^H$	2. $\lfloor \tau \rfloor = \text{Pair}$	16042
15988	$\wedge E^1[e^1] = op^2 E_0^1[e^1] e_1^1$	3. QED $\vdash \langle v_0^1, v_1^1 \rangle : \text{Pair}$	16043
15989	2. $\vdash_H E_0^H[e^H]$	$i \text{ H}\lesssim_1 i$	16044
15990	by H inversion	by IF $\tau = \text{Nat} :$	16045
15991	3. $\vdash E_0^1[e^1]$	1. $i \in \mathbb{N}$	16046
15992	4. $E_0^H[e^H] \text{ H}\lesssim_1 E_0^1[e^1]$	by H inversion	16047
15993	5. QED by the induction hypothesis	2. QED $\vdash i \text{Nat}$	16048
15994	CASE $op^2 v_0^H E_1^H \text{ H}\lesssim_1 op^2 v_0^1 E_1^1 :$	ELSE $\tau = \text{Int} :$	16049
15995	1. $E^H[e^H] = op^2 v_0^H E_1^H[e^H]$	1. QED $\vdash i : \text{Int}$	16050
15996	$\wedge E^1[e^1] = op^2 v_0^1 E_1^1[e^1]$	$\lambda x. e^H \text{ H}\lesssim_1 \lambda x. e^1$	16051
15997	2. $\vdash_H E_1^H[e^H]$	by Contradiction by $\vdash_H \lambda x. e^1 : \tau$	16052
15998	by H inversion	$\lambda(x:\tau). e^H \text{ H}\lesssim_1 \lambda(x:\tau). e^1$	16053
15999	3. $\vdash e_0^1$	by $\tau = \tau_d \Rightarrow \tau_c$	16054
16000	$\wedge \vdash E_1^1[e^1]$	by H inversion $\lfloor \tau \rfloor = \text{FunQED } \vdash \lambda(x:\tau). e^1 : \text{Fun}$	16055
16001	4. $E_1^H[e^H] \text{ H}\lesssim_1 E_1^1[e^1]$		16056
16002	5. QED by the induction hypothesis		16057
16003			16058
16004			16059
16005			16060

16061 $\text{mon } \tau v^H \text{ }_{H \lesssim 1} v^1$
 16062 by $v^H \text{ }_{H \lesssim 1} v^1 \text{ QED}$ by the induction hypothesis
 16063 \square

Lemma 8.22 : H-1 boundary checking

16065 • If $\vdash_H \text{stat } \tau v^H$ and $v^H \text{ }_{H \lesssim 1} v^1$ then $\text{stat } \tau v^H \rightarrow_{1-D}^* v_1^H$
 16066 $\wedge v_1^H \text{ }_{H \lesssim 1} v^1$
 16067 • If $\vdash_H \text{dyn } \tau v^H : \tau$ and $v^H \text{ }_{H \lesssim 1} v^1$ then one of the following
 16068 holds:
 16069 – $\text{dyn } \tau v^H \rightarrow_{1-S}^* \text{BndryErr}$
 16070 – $\text{dyn } \tau v^H \rightarrow_{1-S}^* v_1^H$
 16071 $\wedge v_1^H \text{ }_{H \lesssim 1} v^1$

Proof:

16073 By the following two lemmas: **H-1 stat checking** and
 16074 **H-1 dyn checking**.
 16075 \square

Lemma 8.23 : H-1 stat checking

16077 If $\vdash_H \text{stat } \tau v^H$
 16078 $\wedge v^H \text{ }_{H \lesssim 1} v^1$
 16079 then $\text{stat } \tau v^H \rightarrow_{1-D}^* v_1^H$
 16080 $\wedge v_1^H \text{ }_{H \lesssim 1} v^1$

Proof:

16082 By induction on the structure of τ .

CASE $\tau = \text{Nat}$:

16084 1. $\text{stat } \tau v^H \triangleright_{H-D} v^H$
 16085 by definition \triangleright_{H-D}
 16086 2. QED

CASE $\tau = \text{Int}$:

16088 1. $\text{stat } \tau v^H \triangleright_{H-D} v^H$
 16089 by definition \triangleright_{H-D}
 16090 2. QED

CASE $\tau = \tau_0 \times \tau_1$:

16092 1. $v^H = \langle v_0^H, v_1^H \rangle$
 16093 by **H inversion** and **canonical forms**
 16094 2. $v^1 = \langle v_0^1, v_1^1 \rangle$
 16095 $\wedge v_0^H \text{ }_{H \lesssim 1} v_0^1$
 16096 $\wedge v_1^H \text{ }_{H \lesssim 1} v_1^1$
 16097 by $H \lesssim 1$
 16098 3. $\text{stat } \tau v^H \triangleright_{H-D} \langle \text{stat } \tau_0 v_0^H, \text{stat } \tau_1 v_1^H \rangle$
 16099 by definition \triangleright_{H-D}
 16100 4. $\vdash_H \text{stat } \tau_0 v_0^H$
 16101 $\wedge \vdash_H \text{stat } \tau_1 v_1^H$
 16102 by **H static preservation** and **H inversion**
 16103 5. $\text{stat } \tau_0 v_0^H \rightarrow_{1-D}^* v_0^H$
 16104 $\wedge v_0^H \text{ }_{H \lesssim 1} v_0^1$
 16105 $\wedge \text{stat } \tau_1 v_1^H \rightarrow_{1-D}^* v_1^H$
 16106 $\wedge v_1^H \text{ }_{H \lesssim 1} v_1^1$
 16107 by the induction hypothesis (2, 4)
 16108 6. $\text{stat } \tau v^H \rightarrow_{H-D}^* \langle v_0^H, v_1^H \rangle$
 16109 $\wedge \langle v_0^H, v_1^H \rangle \text{ }_{H \lesssim 1} v^1$
 16110 by (5)
 16111 7. QED

CASE $\tau = \tau_d \Rightarrow \tau_c$:

16114

16115

1. $\text{stat } \tau v^H \triangleright_{H-D} \text{mon } \tau v^H$
 2. $\text{mon } \tau v^H \text{ }_{H \lesssim 1} v^1$
 by $v^H \text{ }_{H \lesssim 1} v^1$
 3. QED

 \square **Lemma 8.24** : H-1 dyn checking

16116 If $\vdash_H \text{dyn } \tau v^H : \tau$
 16117 $\wedge v^H \text{ }_{H \lesssim 1} v^1$
 16118 then one of the following holds:
 16119 • $\text{dyn } \tau v^H \rightarrow_{1-S}^* \text{BndryErr}$
 16120 • $\text{dyn } \tau v^H \rightarrow_{1-S}^* v_1^H$
 16121 $\wedge v_1^H \text{ }_{H \lesssim 1} v^1$

Proof:

16122 By induction on the structure of τ .

CASE $\tau = \text{Nat}$:**IF** $v^H \in \mathfrak{h}$:

1. $\text{dyn } \tau v^H \triangleright_{H-S} v^H$
 by definition \triangleright_{H-S}

2. QED

ELSE $v^H \notin \mathfrak{h}$:1. $\text{dyn } \tau v^H \triangleright_{H-S} \text{BndryErr}$

2. QED

CASE $\tau = \text{Int}$:**IF** $v^H \in \mathbb{Z}$:

1. $\text{dyn } \tau v^H \triangleright_{H-S} v^H$
 by definition \triangleright_{H-S}

2. QED

ELSE $v^H \notin \mathbb{Z}$:1. $\text{dyn } \tau v^H \triangleright_{H-S} \text{BndryErr}$

2. QED

CASE $\tau = \tau_0 \times \tau_1$:**IF** $v^H = \langle v_0^H, v_1^H \rangle$:1. $v^1 = \langle v_0^1, v_1^1 \rangle$ $\wedge v_0^H \text{ }_{H \lesssim 1} v_0^1$ $\wedge v_1^H \text{ }_{H \lesssim 1} v_1^1$ by $H \lesssim 1$ 2. $\text{dyn } \tau v^H \triangleright_{H-S} \langle \text{dyn } \tau_0 v_0^H, \text{dyn } \tau_1 v_1^H \rangle$ by definition \triangleright_{H-S} 3. $\vdash_H \text{dyn } \tau_0 v_0^H : \tau_0$ $\wedge \vdash_H \text{dyn } \tau_1 v_1^H : \tau_1$ by **H static preservation** and **H inversion**4. $\text{dyn } \tau_0 v_0^H \rightarrow_{1-D}^* e_0^H$ $\wedge e_0^H \text{ }_{H \lesssim 1} v_0^1$ $\wedge e_0^H = v_0^H$ or $e_0^H = \text{BndryErr}$ $\wedge \text{dyn } \tau_1 v_1^H \rightarrow_{1-D}^* e_1^H$ $\wedge e_1^H \text{ }_{H \lesssim 1} v_1^1$ or $e_1^H = \text{BndryErr}$

by the induction hypothesis (2, 4)

5. $\text{dyn } \tau v^H \rightarrow_{H-S}^* \text{BndryErr}$ $\vee \text{dyn } \tau v^H \rightarrow_{H-S}^* \langle v_0^H, v_1^H \rangle$ and $\langle v_0^H, v_1^H \rangle \text{ }_{H \lesssim 1}$ v^1

by (5)

6. QED

ELSE $v^H \notin \langle v, v \rangle$:

16171 1. $\text{dyn } \tau v^H \triangleright_{H-S} \text{BndryErr}$
 16172 2. QED
 16173 **CASE** $\tau = \tau_d \Rightarrow \tau_c$:
 16174 **IF** $v^H = \lambda x. e^H$:
 16175 1. $\text{dyn } \tau v^H \triangleright_{H-S} \text{mon } \tau v^H$
 16176 2. $\text{mon } \tau v^H \underset{H \lesssim_1}{\sim} v^1$
 16177 by $v^H \underset{H \lesssim_1}{\sim} v^1$
 16178 3. QED
 16179 **IF** $v^H = \text{mon } \tau_0 v_0^H$:
 16180 1. $\text{dyn } \tau v^H \triangleright_{H-S} \text{mon } \tau v^H$
 16181 2. $\text{mon } \tau v^H \underset{H \lesssim_1}{\sim} v^1$
 16182 by $v^H \underset{H \lesssim_1}{\sim} v^1$
 16183 3. QED
 16184 **ELSE** $v^H \in i \vee v^H \in \langle v, v \rangle$:
 16185 1. $\text{dyn } \tau v^H \triangleright_{H-S} \text{BndryErr}$
 16186 2. QED

□

Lemma 8.25 : H-1 hole substitution

16189 If $E^H \underset{H \lesssim_1}{\sim} E^1$
 16190 $\wedge e^H \underset{H \lesssim_1}{\sim} e^1$
 16191 then $E^H[e^H] \underset{H \lesssim_1}{\sim} E^1[e^1]$

Proof:

16193 By induction on the structure of the $E^H \underset{H \lesssim_1}{\sim} E^1$ judgment.

16194 **CASE** $[\] \underset{H \lesssim_1}{\sim} [\]$:

16195 1. $E^H[e^H] = e^H$
 16196 2. $E^1[e^1] = e^1$
 16197 3. QED

16198 **CASE** $E^H \underset{H \lesssim_1}{\sim} \text{chk } K E_0^1$:

16199 1. $E^H \underset{H \lesssim_1}{\sim} E_0^1$
 16200 2. QED by the induction hypothesis

16201 **CASE** $E_0^H e_1^H \underset{H \lesssim_1}{\sim} E_0^1 e_1^1$:

16202 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$
 16203 2. QED by the induction hypothesis

16204 **CASE** $v_0^H E_1^H \underset{H \lesssim_1}{\sim} v_0^1 E_1^1$:

16205 1. $E_1^H \underset{H \lesssim_1}{\sim} E_1^1$
 16206 2. QED by the induction hypothesis

16207 **CASE** $\langle E_0^H, e_1^H \rangle \underset{H \lesssim_1}{\sim} \langle E_0^1, e_1^1 \rangle$:

16208 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$
 16209 2. QED by the induction hypothesis

16210 **CASE** $\langle v_0^H, E_1^H \rangle \underset{H \lesssim_1}{\sim} \langle v_0^1, E_1^1 \rangle$:

16211 1. $E_1^H \underset{H \lesssim_1}{\sim} E_1^1$
 16212 2. QED by the induction hypothesis

16213 **CASE** $op^1 E_0^H \underset{H \lesssim_1}{\sim} op^1 E_0^1$:

16214 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$
 16215 2. QED by the induction hypothesis

16216 **CASE** $op^2 E_0^H e_1^H \underset{H \lesssim_1}{\sim} op^2 E_0^1 e_1^1$:

16217 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$
 16218 2. QED by the induction hypothesis

16219 **CASE** $op^2 v_0^H E_1^H \underset{H \lesssim_1}{\sim} op^2 v_0^1 E_1^1$:

16220 1. $E_1^H \underset{H \lesssim_1}{\sim} E_1^1$
 16221 2. QED by the induction hypothesis

16222 **CASE** $\text{dyn } \tau_0 E_0^H \underset{H \lesssim_1}{\sim} \text{dyn } \tau_0 E_0^1$:

16223 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$

16224 2. QED by the induction hypothesis

16225 3. $\text{dyn } \tau_0 E_0^H \underset{H \lesssim_1}{\sim} \text{dyn } \tau_0 E_0^1$

16226 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$

16227 2. QED by the induction hypothesis

16228 **CASE** $\text{dyn } \tau_0 E_0^H \underset{H \lesssim_1}{\sim} \text{dyn } E_0^1$:

16229 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$

16230 2. QED by the induction hypothesis

16231 **CASE** $\text{dyn } \tau_0 (\text{stat } \tau_1 E_0^H) \underset{H \lesssim_1}{\sim} E_0^1$:

16232 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$

16233 2. QED by the induction hypothesis

16234 **CASE** $\text{stat } \tau_0 E_0^H \underset{H \lesssim_1}{\sim} \text{stat } \tau_0 E_0^1$:

16235 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$

16236 2. QED by the induction hypothesis

16237 **CASE** $\text{stat } \tau_0 E_0^H \underset{H \lesssim_1}{\sim} \text{stat } E_0^1$:

16238 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$

16239 2. QED by the induction hypothesis

16240 **CASE** $\text{stat } \tau_0 (\text{dyn } \tau_1 E_0^H) \underset{H \lesssim_1}{\sim} E_0^1$:

16241 1. $E_0^H \underset{H \lesssim_1}{\sim} E_0^1$

16242 2. QED by the induction hypothesis

□

Lemma 8.26 : H-1 substitution

16243 If $e^H \underset{H \lesssim_1}{\sim} e^1$ and $v^H \underset{1 \lesssim_E}{\sim} v^1$ then $e^H[x \leftarrow v^H] \underset{H \lesssim_1}{\sim} e^1[x \leftarrow v^1]$

Proof:

16244 By induction on the structure of the $e^H \underset{H \lesssim_1}{\sim} e^1$ judgment.

16245 **CASE** $e^H \underset{H \lesssim_1}{\sim} \text{chk } K_0 e_0^1$:

16246 1. $e^H \underset{H \lesssim_1}{\sim} e_0^1$

16247 2. $e^H[x \leftarrow v^H] \underset{H \lesssim_1}{\sim} e_0^1[x \leftarrow v^1]$

16248 by the induction hypothesis

16249 3. $\text{chk } K_0 e_0^1[x \leftarrow v^1] = \text{chk } K_0 e_0^1[x \leftarrow v^1]$

16250 4. QED

16251 **CASE** $\text{Err } \underset{H \lesssim_1}{\sim} e^1$:

16252 1. $\text{Err}[x \leftarrow v^H] = \text{Err}$

16253 2. QED $\text{Err } \underset{H \lesssim_1}{\sim} e^1[x \leftarrow v^1]$

16254 **CASE** $\text{dyn } \tau_0 e_0^H \underset{H \lesssim_1}{\sim} \text{dyn } \tau_0 e_0^1$:

16255 1. $e_0^H \underset{H \lesssim_1}{\sim} e_0^1$

16256 2. $e_0^H[x \leftarrow v^H] \underset{H \lesssim_1}{\sim} e_0^1[x \leftarrow v^1]$

16257 by the induction hypothesis

16258 3. $\text{dyn } \tau_0 e_0^H[x \leftarrow v^H] = \text{dyn } \tau_0 e_0^H[x \leftarrow v^H]$

16259 4. $\text{dyn } \tau_0 e_0^1[x \leftarrow v^1] = \text{dyn } \tau_0 e_0^1[x \leftarrow v^1]$

16260 5. QED

16261 **CASE** $\text{dyn } \tau_0 e_0^H \underset{H \lesssim_1}{\sim} \text{dyn } e_0^1$:

16262 1. $e_0^H \underset{H \lesssim_1}{\sim} e_0^1$

16263 2. $e_0^H[x \leftarrow v^H] \underset{H \lesssim_1}{\sim} e_0^1[x \leftarrow v^1]$

16264 by the induction hypothesis

16265 3. $\text{dyn } \tau_0 e_0^H[x \leftarrow v^H] = \text{dyn } \tau_0 e_0^H[x \leftarrow v^H]$

16266 4. $\text{dyn } e_0^1[x \leftarrow v^1] = \text{dyn } e_0^1[x \leftarrow v^1]$

16267 5. QED

16268 **CASE** $\text{dyn } \tau_0 (\text{stat } \tau_1 e_0^H) \underset{H \lesssim_1}{\sim} e^1$:

16269 1. $e_0^H \underset{H \lesssim_1}{\sim} e^1$

16270 2. $e_0^H[x \leftarrow v^H] \underset{H \lesssim_1}{\sim} e^1[x \leftarrow v^1]$

16271 by the induction hypothesis

16272 3. $\text{dyn } \tau_0 (\text{stat } \tau_1 e_0^H)[x \leftarrow v^H] = \text{dyn } \tau_0 (\text{stat } \tau_1 e_0^H[x \leftarrow v^H])$

16273 4. QED

16274 **CASE** $\text{stat } \tau_0 E_0^H \underset{H \lesssim_1}{\sim} \text{stat } \tau_0 E_0^1$:

16281	1. $e_0^H \text{H}\lesssim_1 e_0^1$	5. QED	16336
16282	2. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v^1]$	CASE $x_0 \text{H}\lesssim_1 x_0 :$	16337
16283	by the induction hypothesis	IF $x_0 = x :$	16338
16284	3. $\text{stat } \tau_0 e_0^H[x \leftarrow v^H] = \text{stat } \tau_0 e_0^H[x \leftarrow v^H]$	1. QED $x_0[x \leftarrow v^H] = v^H$	16339
16285	4. QED	$\wedge x_0[x \leftarrow v^1] = v^1$	16340
16286	CASE $\text{stat } \tau_0 e_0^H \text{H}\lesssim_1 \text{stat } e_0^1 :$	ELSE $x_0 \neq x :$	16341
16287	1. $e_0^H \text{H}\lesssim_1 e_0^1$	1. QED $x_0[x \leftarrow v^H] = x_0$	16342
16288	2. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v^1]$	$\wedge x_0[x \leftarrow v^1] = x_0$	16343
16289	by the induction hypothesis	CASE $i \text{H}\lesssim_1 i :$	16344
16290	3. $\text{stat } \tau_0 e_0^H[x \leftarrow v^H] = \text{stat } \tau_0 e_0^H[x \leftarrow v^H]$	1. QED $i[x \leftarrow v^H] = i$	16345
16291	4. $\text{stat } e_0^1[x \leftarrow v^1] = \text{stat } e_0^1[x \leftarrow v^1]$	$\wedge i[x \leftarrow v^1] = i$	16346
16292	5. QED	CASE $\lambda x_0. e_0^H \text{H}\lesssim_1 \lambda x_0. e_0^1 :$	16347
16293	CASE $\text{stat } \tau_0 (\text{dyn } \tau_1 e_0^H) \text{H}\lesssim_1 e^1 :$	1. IF $x_0 = x :$	16348
16294	1. $e_0^H \text{H}\lesssim_1 e^1$	a. QED $\lambda x_0. e_0^H[x \leftarrow v^H] = \lambda x_0. e_0^H$	16349
16295	2. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e^1[x \leftarrow v^1]$	$\wedge \lambda x_0. e_0^1[x \leftarrow v^1] = \lambda x_0. e_0^1$	16350
16296	by the induction hypothesis	2. ELSE $x_0 \neq x :$	16351
16297	3. $\text{stat } \tau_0 (\text{dyn } \tau_1 e_0^H)[x \leftarrow v^H] = \text{stat } \tau_0 (\text{dyn } \tau_1 e_0^H[x \leftarrow v^H])$	a. $e_0^H \text{H}\lesssim_1 e_0^1$	16352
16298	4. QED	b. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v^1]$	16353
16299	CASE $e_0^H e_1^H \text{H}\lesssim_1 e_0^1 e_1^1 :$	by the induction hypothesis	16354
16300	1. $e_0^H \text{H}\lesssim_1 e_0^1$	c. $\lambda x_0. e_0^H[x \leftarrow v^H] = \lambda x_0. e_0^H[x \leftarrow v^H]$	16355
16301	$\wedge e_1^H \text{H}\lesssim_1 e_1^1$	$\wedge \lambda x_0. e_0^1[x \leftarrow v^1] = \lambda x_0. e_0^1[x \leftarrow v^1]$	16356
16302	2. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v^1]$	d. QED	16357
16303	$\wedge e_1^H[x \leftarrow v^H] \text{H}\lesssim_1 e_1^1[x \leftarrow v^1]$	CASE $\lambda(x_0 : \tau_0). e_0^H \text{H}\lesssim_1 \lambda(x_0 : \tau_0). e_0^1 :$	16358
16304	by the induction hypothesis	1. IF $x_0 = x :$	16359
16305	3. $e_0^H e_1^H[x \leftarrow v^H] = e_0^H[x \leftarrow v^H] e_1^H[x \leftarrow v^H]$	a. QED $\lambda(x_0 : \tau_0). e_0^H[x \leftarrow v^H] = \lambda(x_0 : \tau_0). e_0^H$	16360
16306	4. $e_0^1 e_1^1[x \leftarrow v^1] = e_0^1[x \leftarrow v^1] e_1^1[x \leftarrow v^1]$	$\wedge \lambda(x_0 : \tau_0). e_0^1[x \leftarrow v^1] = \lambda(x_0 : \tau_0). e_0^1$	16361
16307	5. QED	2. ELSE $x_0 \neq x :$	16362
16308	CASE $\langle e_0^H, e_1^H \rangle \text{H}\lesssim_1 \langle e_0^1, e_1^1 \rangle :$	a. $e_0^H \text{H}\lesssim_1 e_0^1$	16363
16309	1. $e_0^H \text{H}\lesssim_1 e_0^1$	b. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v^1]$	16364
16310	$\wedge e_1^H \text{H}\lesssim_1 e_1^1$	by the induction hypothesis	16365
16311	2. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v^1]$	c. $\lambda(x_0 : \tau_0). e_0^H[x \leftarrow v^H] = \lambda(x_0 : \tau_0). e_0^H[x \leftarrow v^H]$	16366
16312	$\wedge e_1^H[x \leftarrow v^H] \text{H}\lesssim_1 e_1^1[x \leftarrow v^1]$	$\wedge \lambda(x_0 : \tau_0). e_0^1[x \leftarrow v^1] = \lambda(x_0 : \tau_0). e_0^1[x \leftarrow v^1]$	16367
16313	by the induction hypothesis	d. QED	16368
16314	3. $\langle e_0^H, e_1^H \rangle[x \leftarrow v^H] = \langle e_0^H[x \leftarrow v^H], e_1^H[x \leftarrow v^H] \rangle$	CASE $\text{mon } \tau_0 v_0^H \text{H}\lesssim_1 v_0^1 :$	16370
16315	4. $\langle e_0^1, e_1^1 \rangle[x \leftarrow v^1] = \langle e_0^1[x \leftarrow v^1], e_1^1[x \leftarrow v^1] \rangle$	1. $v_0^H \text{H}\lesssim_1 v_0^1$	16371
16316	5. QED	2. $v_0^H[x \leftarrow v^H] \text{H}\lesssim_1 v_0^1[x \leftarrow v^1]$	16372
16317	CASE $op^1 e_0^H \text{H}\lesssim_1 op^1 e_0^1 :$	by the induction hypothesis	16373
16318	1. $e_0^H \text{H}\lesssim_1 e_0^1$	3. $\text{mon } \tau_0 v_0^H[x \leftarrow v^H] = \text{mon } \tau_0 v_0^H[x \leftarrow v^H]$	16374
16319	$\wedge e_1^H \text{H}\lesssim_1 e_1^1$	4. QED	16375
16320	2. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v^1]$	CASE $\text{Err} \text{H}\lesssim_1 \text{Err} :$	16376
16321	by the induction hypothesis	1. QED $\text{Err}[x \leftarrow v^H] = \text{Err}$	16377
16322	3. $op^1 e_0^H[x \leftarrow v^H] = op^1 e_0^H[x \leftarrow v^H]$	\square	16378
16323	4. $op^1 e_0^1[x \leftarrow v^1] = op^1 e_0^1[x \leftarrow v^1]$	Lemma 8.27 : <i>chk inversion</i>	16379
16324	5. QED	■ If $\Gamma \vdash_1 \text{chk } K e' : K$ and $\Gamma \vdash e : \tau \rightsquigarrow \text{chk } K e'$ then $K = \lfloor \tau \rfloor$.	16380
16325	CASE $op^2 e_0^H e_1^H \text{H}\lesssim_1 op^2 e_0^1 e_1^1 :$	<i>Proof</i> :	16381
16326	1. $e_0^H \text{H}\lesssim_1 e_0^1$	By case analysis on \rightsquigarrow .	16382
16327	$\wedge e_1^H \text{H}\lesssim_1 e_1^1$	CASE $\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_d \rightsquigarrow e'_1 \quad \lfloor \tau_c \rfloor = K}{\Gamma \vdash e_0 e_1 : \tau_c \rightsquigarrow \text{chk } K (e'_0 e'_1)}$	16383
16328	2. $e_0^H[x \leftarrow v^H] \text{H}\lesssim_1 e_0^1[x \leftarrow v^1]$		16384
16329	$\wedge e_1^H[x \leftarrow v^H] \text{H}\lesssim_1 e_1^1[x \leftarrow v^1]$		16385
16330	by the induction hypothesis		16386
16331	3. $op^2 e_0^H e_1^H[x \leftarrow v^H] = op^2 e_0^H[x \leftarrow v^H] e_1^H[x \leftarrow v^H]$		16387
16332	4. $op^2 e_0^1 e_1^1[x \leftarrow v^1] = op^2 e_0^1[x \leftarrow v^1] e_1^1[x \leftarrow v^1]$	1. QED	16388
16333			16389
16334			16390
16335			16390

16391 **CASE** $\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad \lfloor \tau_0 \rfloor = K}{\Gamma \vdash \text{fst } e : \tau_0 \rightsquigarrow \text{chk } K (\text{fst } e')}$: 16446
 16392 16447
 16393 16448

16394 1. QED 16449

16395 **CASE** $\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad \lfloor \tau_1 \rfloor = K}{\Gamma \vdash \text{snd } e : \tau_1 \rightsquigarrow \text{chk } K (\text{snd } e')}$: 16450
 16396 16451
 16397 16452

16398 1. QED 16453
 16399 □ 16454

Lemma 8.28 : H-1 δ -preservation

- If $v^H \text{H}\lesssim_1 v^1$ and $\delta(\text{op}^1, v^H)$ is defined then $\delta(\text{op}^1, v^H) \text{H}\lesssim_1 \delta(\text{op}^1, v^1)$
- If $v_0^H \text{H}\lesssim_1 v_0^1$ and $v_1^H \text{H}\lesssim_1 v_1^1$ and $\delta(\text{op}^2, v_0^H, v_1^H)$ is defined then $\delta(\text{op}^2, v_0^H, v_1^H) \text{H}\lesssim_1 \delta(\text{op}^2, v_0^1, v_1^1)$

Proof:

16405 **CASE** $\text{op}^1 = \text{fst}$: 16460

16406 1. $v^H = \langle v_0^H, v_1^H \rangle$ 16461

16407 by $\delta(\text{fst}, v^H)$ is defined 16462

16408 2. $v^1 = \langle v_0^1, v_1^1 \rangle$ 16463

16409 $\wedge v_0^H \text{H}\lesssim_1 v_0^1$ and $v_1^H \text{H}\lesssim_1 v_1^1$ 16464

16410 by $\text{H}\lesssim_1$ 16465

16411 3. $\delta(\text{fst}, v^H) = v_0^H$ 16466

16412 $\wedge \delta(\text{fst}, v^1) = v_0^1$ 16467

16413 4. QED (2) 16468

16414 16469

16415 **CASE** $\text{op}^1 = \text{snd}$: 16470

16416 1. $v^H = \langle v_0^H, v_1^H \rangle$ 16471

16417 by $\delta(\text{snd}, v^H)$ is defined 16472

16418 2. $v^1 = \langle v_0^1, v_1^1 \rangle$ 16473

16419 $\wedge v_0^H \text{H}\lesssim_1 v_0^1$ and $v_1^H \text{H}\lesssim_1 v_1^1$ 16474

16420 by $\text{H}\lesssim_1$ 16475

16421 3. $\delta(\text{snd}, v^H) = v_1^H$ 16476

16422 $\wedge \delta(\text{snd}, v^1) = v_1^1$ 16477

16423 4. QED (2) 16478

16424 **CASE** $\text{op}^2 = \text{sum}$: 16479

16425 1. $v_0^H \in \mathbb{Z}$ 16480

16426 $\wedge v_1^H \in \mathbb{Z}$ 16481

16427 by $\delta(\text{op}^2, v_0^H, v_1^H)$ is defined 16482

16428 2. $v_0^H = v_0^1$ 16483

16429 $\wedge v_1^H = v_1^1$ 16484

16430 by $\text{H}\lesssim_1$ 16485

16431 3. QED 16486

16432 **CASE** $\text{op}^2 = \text{quotient}$: 16487

16433 1. $v_0^H \in \mathbb{Z}$ 16488

16434 $\wedge v_1^H \in \mathbb{Z}$ 16489

16435 by $\delta(\text{op}^2, v_0^H, v_1^H)$ is defined 16490

16436 2. $v_0^H = v_0^1$ 16491

16437 $\wedge v_1^H = v_1^1$ 16492

16438 by $\text{H}\lesssim_1$ 16493

16439 3. QED 16494

16440 □ 16495

16441 16496

16442 16497

16443 16498

16444 16499

16445 16500