

A Memory-Bounded, Deterministic and Terminating Semantics for the Synchronous Programming Language CÉU

Anonymous Author(s)

Abstract

CÉU is a synchronous programming language for embedded soft real-time systems. It focus on control-flow safety features, such as safe shared-memory concurrency and safe abortion of lines of execution, while enforcing memory-bounded, deterministic, and terminating reactions to the environment. In this work, we present a small-step structural operational semantics for CÉU and a proof that reactions have the properties enumerated above: that for a given arbitrary timeline of input events, multiple executions of the same program always react in bounded time and arrive at the same final finite memory state.

CCS Concepts • Theory of computation → Operational semantics; • Software and its engineering → Concurrent programming languages; • Computer systems organization → Embedded software;

Keywords Operational semantics, CÉU, Synchronous languages

ACM Reference Format:

Anonymous Author(s). 1997. A Memory-Bounded, Deterministic and Terminating Semantics for the Synchronous Programming Language CÉU. In *Proceedings of ACM Woodstock conference (WOODSTOCK'97)*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.475/123_4

1 Introduction

CÉU [16, 18] is a Esterel-based [8] programming language for embedded soft real-time systems that aims to offer a concurrent, safe, and expressive alternative to C with the characteristics that follow:

Reactive: code only executes in reactions to events.

Structured: programs use structured control mechanisms, such as `await` (to suspend a line of execution), and `par` (to combine multiple lines of execution).

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).

WOODSTOCK'97, July 1997, El Paso, Texas USA

© 2016 Copyright held by the owner/author(s).

ACM ISBN 123-4567-24-567/08/06...\$15.00

https://doi.org/10.475/123_4

Synchronous: reactions run atomically and to completion on each line of execution, i.e., there's no implicit preemption or real parallelism.

Structured reactive programming lets developers write code in direct style, recovering from the inversion of control imposed by event-driven execution [1, 13, 15]. Synchronous languages offer a simple run-to-completion execution model that enables deterministic execution and make formal reasoning tractable. For this reason, it has been successfully adopted in safety-critical real-time embedded systems [3].

Previous work in the context of embedded sensor networks evaluates the expressiveness of CÉU in comparison to event-driven code in C and attests a reduction in source code size (around 25%) with a small increase in memory usage (around 5–10% for *text* and *data*) [18]. CÉU has also been used in the context of multimedia systems [19] and games [17].

CÉU inherits the synchronous and imperative mindset of Esterel but adopts a simpler semantics with fine-grained execution control [16]. The list that follows summarizes the semantic peculiarities of CÉU:

- Fine-grained, intra-reaction deterministic execution, which makes CÉU fully deterministic.
- Stack-based execution for internal events, which provides a limited but memory-bounded form of subroutines.
- Finalization mechanism for lines of execution, which makes abortion safe with regards to external resources.

In this work, we present a formal small-step structural operational semantics for CÉU and proofs that it enforces memory-bounded, deterministic, and terminating reactions to the environment, i.e., that for a given arbitrary timeline of input events, multiple executions of the same program always react in bounded time and arrive at the same final finite memory state.

2 CÉU

CÉU is a synchronous reactive language in which programs advance in a sequence of discrete reactions to external events. It is designed for control-intensive applications, supporting concurrent lines of execution, known as *trails*, and instantaneous broadcast communication through events. Computations within a reaction (such as expressions, assignments, and system calls) are also instantaneous considering the synchronous hypothesis [9]. CÉU provides an `await` statement

that blocks the current running trail allowing the program to advance its other trails; when all trails are blocked, the reaction terminates and control returns to the environment.

In C  U, every execution path within loops must contain at least one `await` statement to an external input event [6, 18]. This restriction, which is statically checked by the compiler, ensures that every reaction runs in bounded time, eventually terminating with all trails blocked in `await` statements. C  U has an additional restriction, which it shares with Esterel and synchronous languages in general [4]: computations that take a non-negligible time to run (e.g., cryptography or image processing algorithms) violate the zero-delay hypothesis, and thus cannot be directly implemented.

Listing 1 shows a compact reference of C  U:

```

// Declarations
input <type> <id>;           // declares an external input event
event <type> <id>;           // declares an internal event
var <type> <id>;             // declares a variable

// Event handling
<id> = await <id>;           // awaits an event and assigns the received value
emit <id>(<exp>);            // emits an event passing a value

// Control flow
<stmt> ; <stmt>               // sequence
if <exp> then <stmts> else <stmts> end // conditional
loop do <stmts> end           // repetition
every <id> in <id> do <stmts> end // event iteration
finalize [<stmts>] with <stmts> end // finalization

// Logical parallelism
par/or do <stmts> with <stmts> end // aborts when any side ends
par/and do <stmts> with <stmts> end // terminates when all sides ends
par do <stmts> with <stmts> end // never terminates

// Assignment & Integration with C
<id> = <exp>;                 // assigns a value to a variable
_(<id>)(<exps>)                // calls a C function (id starts with '_')
```

Listing 1. The concrete syntax of C  U.

Listing 2 shows a complete example in C  U that toggles a LED whenever a radio packet is received, terminating with a button press always with the LED off. The implementation first declares the `BUTTON` and `RADIO_RECV` as input events (ln. 1–2). Then, it uses a `par/or` composition to run two activities in parallel: a single statement that waits for a button press before terminating (ln. 4), and an endless loop that toggles the LED on and off on radio receives (ln. 9–14). The `finalize` clause (ln. 6–8) ensures that, no matter how its enclosing trail terminates, the LED will be unconditionally turned off (ln. 7).

The `par/or` composition, which stands for a *parallel-or*, provides an orthogonal abortion mechanism [4] in which its composed trails do not know when and how they are aborted (i.e., abortion is external to them). The finalization mechanism extends orthogonal abortion to also work with activities that use stateful resources from the environment

(such as files and network handlers), as we discuss in Section 2.3.

```

1 input void BUTTON;
2 input void RADIO_RECV;
3 par/or do
4   await BUTTON;
5 with
6   finalize with
7     _led(0);
8   end
9   loop do
10    _led(1);
11    await RADIO_RECV;
12    _led(0);
13    await RADIO_RECV;
14  end
15 end
```

Listing 2. A program in C  U that toggles a LED on every radio receive, terminating on a button press in a consistent state.

In C  U, any identifier prefixed with an underscore (e.g., `_led`) is passed unchanged to the underlying C compiler. Therefore, access to C is straightforward and syntactically traceable. To ensure that programs operate under the synchronous hypothesis, the compiler environment should only provide access to C operations that can be assumed to be instantaneous, such as non-blocking I/O and simple accesses to data structures.

2.1 External and Internal Events

C  U defines time as a discrete sequence of reactions to unique external input events. External input events are received from the environment, and each delimits a new logical unit of time that triggers an associated reaction. The life-cycle of a program in C  U can be summarized as follows [18]:

- i The program initiates a “boot reaction” in a single trail (parallel constructs may create new trails).
- ii Active trails execute until they await or terminate, one after another. This step is called a *reaction chain*, and always runs in bounded time.
- iii When all trails are blocked, the program goes idle and the environment takes control.
- iv On the occurrence of a new external input event, the environment awakes *all* trails awaiting that event, and the program goes back to step (ii).

A program must react to an event completely before handling the next one. By the synchronous hypothesis, the time the program spends in step (ii) is conceptually zero (in practice, negligible). Hence, from the point of view of the environment, the program is always idle on step (iii). In practice, if a new external input event occurs while a reaction executes, the event is saved on a queue, which effectively schedules it to be processed in a subsequent reaction.

External events and discrete time

The sequential processing of external input events induces a discrete notion of time in C  u, as illustrated in Figure 1. The continuous timeline shows an absolute reference clock with “physical timestamps” for the event occurrences (e.g., event C occurs at 17ms521us). The discrete timeline shows how the same occurring events fit in the logical notion of time of C  u. The boot reaction boot-0 happens before any input, at program startup. Event A “physically” occurs during boot-0 but, because time is discrete, its corresponding reaction only executes afterwards, at logical instant A-1. Similarly, event B occurs during A-1 and its reaction is postponed to execute at B-2. Event C also occurs during A-1 but its reaction must also wait for B-2 to execute and so it is postponed to execute at C-3. Finally, event D occurs during an idle period and can start immediately at D-4.

Unique input events imply mutually exclusive reactions, which execute atomically and never overlap. Automatic mutual exclusion is a prerequisite for deterministic reactions as we discuss in Section 3.

In practice, the synchronous hypothesis for C  u holds if reactions execute faster than the rate of incoming input events. Otherwise, the program would continuously accumulate delays between physical occurrences and actual reactions for the input events. Considering the context soft real-time systems, such delays and postponed reactions might be tolerated as long as they are infrequent and the application does not take too long to catch up with real time. Note that the synchronous semantics is the norm in typical event-driven systems, such as event dispatching in UI toolkits, game loops in game engines, and clock ticks in embedded systems.

Internal events as subroutines

In C  u, queue-based processing of events applies only to external input events, i.e., events submitted to the program by the environment. Internal events, which are events generated internally by the program via `emit` statements, are processed in a stack-based manner. Internal events provide a fine-grained execution control, and, because of their stack-based processing, can be used to implement a limited form of subroutines, as illustrated in Listing 3:

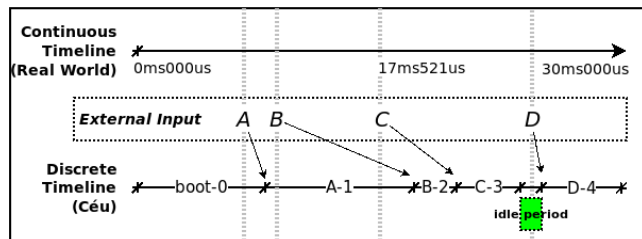


Figure 1. The discrete notion of time in C  u.

```

1 event int* inc;           // declares subroutine "inc"
2 par/or do
3   var int* p;
4   every p in inc do       // implements "inc" through an event iterator
5     *p = *p + 1;
6   end
7 with
8   var int v = 1;
9   emit inc(&v);           // calls "inc"
10  emit inc(&v);           // calls "inc"
11  _assert(v==3);          // asserts result after the two returns
12 end

```

Listing 3. A C  u program with a “subroutine”.

In the example, the “subroutine” `inc` is defined as an event iterator (ln. 4–6) that continuously awaits its identifying event (ln. 4), and increments the value passed by reference (ln. 5). A trail in parallel (ln. 8–11) invokes the subroutine through two consecutive `emit` statements (ln. 9–10). Given the stack-based execution for internal events, as the first `emit` executes, the calling trail pauses (ln. 9), the subroutine awakes (ln. 4), runs its body (yielding `v=2`), iterates, and awaits the next “call” (ln. 4, again). Only after this sequence does the calling trail resumes (ln. 9), makes a new invocation (ln. 10), and passes the assertion test (ln. 11).

C  u also supports nested `emit` invocations, e.g., the body of the subroutine `inc` (ln. 5) could `emit` an event targeting another subroutine, creating a new level in the stack. We can think of the stack as a record of the nested, fine-grained internal reactions that happen inside the same outer reaction to a single external event.

This form of subroutines has a significant limitation though: it cannot express recursion, since an `emit` to itself is always ignored as a running trail cannot be waiting on itself. That being said, it is this very limitation that brings important safety properties to subroutines. First, they are guaranteed to react in bounded time. Second, memory for locals is also bounded, not requiring data stacks.

At first sight, event iteration such as in “every `e` do <...> end” seems to be equivalent to “loop do await `e`; <...> end”. However, the loop variation would not compile because it does not contain a path to an external input await (`e` is an internal event). However, event iterators enforce syntactic restrictions and cannot contain `await` or `break` statements. The absence of `break` guarantees that an iterator never terminates from itself, essentially behaving as a safe blocking point in the program. For this reason, the restriction that execution paths within loops must contain at least one external `await` is extended to alternatively contain an `every` statement.

2.2 Shared-Memory Concurrency

Embedded applications make extensive use of global memory and shared resources, such as through memory-mapped

registers and system calls to device drivers. Hence, an important goal of C  U is to ensure a reliable behavior for programs with concurrent lines of execution sharing memory and interacting with the environment.

input void A;	1	input void A;	
input void B;	2	// (empty line)	
var int x = 1;	3	var int y = 1;	
par/and do	4	par/and do	
await A;	5	await A;	
x = x + 1;	6	y = y + 1;	
with	7	with	
await B;	8	await A;	
x = x * 2;	9	y = y * 2;	
end	10	end	
[a] Accesses to x are never concurrent.		[b] Accesses to y are concurrent but deterministic.	

Figure 2. Shared-memory concurrency in C  U: example [a] is safe because the trails access x atomically in different reactions; example [b] is unsafe because both trails access y in the same reaction.

In C  U, when multiple trails are active during the same reaction, they are scheduled in lexical order, i.e., in the order they appear in the program source code. For instance, consider the two examples in Figure 2, both defining shared variables (ln. 3), and assigning to them in parallel trails (ln. 6, 9).

In the example [a], the two assignments to x can only execute in reactions to different events A and B, which cannot occur simultaneously by definition (Section 2.1). Hence, for the sequence of events A→B, x becomes 4 ((1+1)*2), while for B→A, x becomes 3 ((1*2)+1).

In the example [b], the two assignments to y are simultaneous because they execute in reaction to the same event A. Since C  U employs lexical order for intra-reaction statements, the execution is still deterministic, and y always becomes 4 ((1+1)*2). However, note that an apparently innocuous change in the order of trails modifies the behavior of the program. To mitigate this threat, C  U performs concurrency checks at compile time to detect conflicting accesses to shared variables: if a variable is written in a trail segment, then a concurrent trail segment cannot read or write to that variable [18]. Nonetheless, the static checks are optional and are not a prerequisite for the deterministic semantics of the language.

2.3 Abortion and Finalization

The par/or of C  U is an orthogonal abortion mechanism because the two sides in the composition need not be tweaked with synchronization primitives or state variables in order to affect each other. In addition, abortion is *immediate* in the sense that it executes atomically in the current micro reaction.

par/or do	1	par/or do	386
var _msg_t msg;	2	var _FILE* f;	387
<...> // prepare msg	3	finalize	388
finalize	4	f = _fopen(...);	389
_send(&msg);	5	with	390
_cancel(&msg);	6	_fclose(f);	391
end	7	end	392
await SEND_ACK;	8	_fwrite(..., f);	393
with	9	await A;	394
<...>	10	_fwrite(..., f);	395
end	11	with	396
//	12	<...>	397
	13	end	398
[a] Local resource finalization		[b] External resource finalization	

Figure 3. C  U enforces the use of finalization to prevent *dangling pointers* for local resources and *memory leaks* for external resources.

Immediate orthogonal abortion is a distinctive feature of synchronous languages and cannot be expressed effectively in traditional (asynchronous) multi-threaded languages [4, 14].

However, aborting lines of execution that deal with external resources may lead to inconsistencies. For this reason, C  U provides a *finalize* construct to unconditionally execute a series of statements even if the enclosing block is externally aborted.

C  U also enforces the use of *finalize* for system calls that deal with pointers representing resources, as illustrated in the two examples of Figure 3:

- If C  U **passes** a pointer to a system call (ln. [a]:5), the pointer represents a **local** resource (ln. [a]:2) that requires finalization (ln. [a]:7).
- If C  U **receives** a pointer from a system call return (ln. [b]:4), the pointer represents an **external** resource (ln. [b]:2) that requires finalization (ln. [b]:6).

C  U tracks the interaction of system calls with pointers and requires finalization clauses to accompany them. In the example in Figure 3.a, the local variable msg (ln. 2) is an internal resource passed as a pointer to _send (ln. 5), which is an asynchronous call that transmits the buffer in the background. If the block aborts (ln. 11) before receiving an acknowledge from the environment (ln. 9), the local msg goes out of scope and the external transmission now holds a *dangling pointer*. The finalization ensures that the transmission also aborts (ln. 7). In the example in Figure 3.b, the call to _fopen (ln. 4) returns an external file resource as a pointer. If the block aborts (ln. 12) during the await A (ln. 9), the file remains open as a *memory leak*. The finalization ensures that the

file closes properly (ln. 6). In both cases, the code does not compile without the `finalize` construct.¹

The finalization mechanism of Céu is fundamental to preserve the orthogonality of the `par/or` construct since the clean up code is encapsulated in the aborted trail itself.

3 Formal Semantics

In this section, we introduce a reduced syntax for Céu and propose an operational semantics to formally describe the behavior of its programs. We describe a small synchronous kernel highlighting the peculiarities of Céu, in particular, the stack-based execution for internal events. For the sake of simplicity, we focus on the control aspects of the language, leaving out side-effects and system calls (which behave like in conventional imperative languages).

3.1 Abstract Syntax

The grammar below defines the syntax of a subset of Céu that is sufficient to describe all semantic peculiarities of the language.

$p ::= \text{mem}(id)$	<i>any memory access to “id”</i>
$\text{await}_{\text{ext}}(id)$	<i>await external event “id”</i>
$\text{await}_{\text{int}}(id)$	<i>await internal event “id”</i>
$\text{emit}_{\text{int}}(id)$	<i>emit internal event “id”</i>
break	<i>loop escape</i>
$\text{if } b \text{ then } p_1 \text{ else } p_2$	<i>conditional</i>
$p_1; p_2$	<i>sequence</i>
$\text{loop } p_1$	<i>repetition</i>
$\text{every } id \ p_1$	<i>event iteration</i>
$p_1 \text{ and } p_2$	<i>par/and</i>
$p_2 \text{ or } p_2$	<i>par/or</i>
$\text{fin } p$	<i>finalization</i>
$p_1 @ \text{loop } p_2$	<i>unwinded loop</i>
$p_1 @ \text{and } p_2$	<i>unwinded par/and</i>
$p_1 @ \text{or } p_2$	<i>unwinded par/or</i>
$@ \text{canrun}(n)$	<i>can run on stack level n</i>
$@ \text{nop}$	<i>terminated program</i>

The $\text{mem}(id)$ primitive represents all accesses, assignments, and system calls that affect a memory location identified by id . According to the synchronous hypothesis of Céu, mem expressions are considered to be atomic and instantaneous. As the challenging parts of Céu reside on its control structures, we are not concerned here with a precise semantics for side effects, but only with their occurrences in programs.

We assume that mem , $\text{await}_{\text{ext}}$, $\text{await}_{\text{int}}$ and emit_{int} expressions do not share identifiers: any identifier is either a variable, an external event, or an internal event.

Most expressions in the abstract language are mapped to their counterparts in the concrete language. The exceptions are the finalization block $\text{fin } p$ and the $@$ -expressions,

¹ The compiler only forces the programmer to write the finalization clause, but cannot check if it actually handles the resource properly.

which are internal expressions that result from the expansion of awaits, emits, and loops by the transition rules to be discussed.

Regarding other mismatches between the concrete and abstract languages, the concrete `await` and `emit` primitives support communication of values between them, e.g., an “`emit a(10)`” awakes a “`v=await a`” setting variable v to 10. To reproduce this functionality in the formal semantics, we can use a shared variable to hold the value of an emit_{int} and access it after the corresponding $\text{await}_{\text{int}}$. Also, a “`finalize A with B end; C`” in the concrete language is equivalent to “`A; ((fin B) or C)`” in the abstract language. In the concrete language, A and C execute in sequence, and the finalization code B is implicitly suspended waiting for C termination. In the abstract language, “`fin B`” suspends forever when reached (it is an awaiting expression that never awakes). Hence, we need an explicit `or` to execute C in parallel, whose termination aborts “`fin B`”, which finally causes B to execute (by the semantic rules to be discussed).

3.2 Operational Semantics

The core of our semantics describes how a program reacts to a single external input event, i.e., starting from an input event, how the program behaves and becomes idle again to proceed to a subsequent reaction. We use a set of small-step operational rules, which are built in such a way that at most one transition is possible at any time, resulting in deterministic reactions. The transition rules map a triple with a program p , a stack level n , and an emitted event e to a modified triple as follows:

$$\langle p, n, e \rangle \longrightarrow \langle p', n', e' \rangle,$$

where

Rodrigo: Na BNF o p não deveria ser P (maiúsculo) tbm?

$p, p' \in P$ are abstract-language programs, $n, n' \in \mathbb{N}$ are nonnegative integers representing the current stack level, and

Rodrigo: Checar: Acho que o conjunto E não foi previamente definido em lugar nenhum

$e, e' \in E \cup \{\varepsilon\}$ are the events emitted before and after the transition (both being possibly the empty event ε).

We will refer to the triples on the left-hand and right-hand sides of symbol \rightarrow as *descriptions* (denoted δ). The triple on the left-hand side of symbol \rightarrow is called the *input description*, and the triple on its right-hand side is called the *output description*.

At the beginning of a reaction to an input event id , the input description is initialized with stack level 0 ($n = 0$) and with the emitted event ($e = id$). At the end of a reaction, after an arbitrary but finite number of transitions, the last output description will block with a (possibly) modified program p' , at stack level 0, and with no event emitted (ε):

$$\langle p, 0, e \rangle \xrightarrow{*} \langle p', 0, \varepsilon \rangle.$$

We distinguish between two types of transition rules: *outermost transitions* \xrightarrow{out} and *nested transitions* \xrightarrow{nst} .

Outermost transitions

The \xrightarrow{out} rules **push** and **pop** are non-recursive definitions that only apply to the program as a whole and manipulate the stack level:

$$\begin{array}{l} \frac{e \neq \varepsilon}{\langle p, n, e \rangle \xrightarrow{out} \langle bcast(p, e), n + 1, \varepsilon \rangle} \quad (\text{push}) \\ \frac{n > 0 \quad p = @nop \vee isblocked(p, n)}{\langle p, n, \varepsilon \rangle \xrightarrow{out} \langle p, n - 1, \varepsilon \rangle} \quad (\text{pop}) \end{array}$$

Rule **push** matches whenever there is an emitted event in the input description, and instantly broadcasts the event to the program, which means (a) awaking active $await_{ext}$ or $await_{int}$ expressions altogether (see function *bcast* in Figure 4), (b) creating a nested reaction by increasing the stack level, and, at the same time, (c) consuming the event (e becomes ε). Rule **push** is the only rule in the semantics that matches an emitted event and also immediately consumes it.

Rule **pop** only decreases the stack level, not affecting the program, and only applies if the program is blocked (see function *isblocked* in Figure 4). This condition ensures that an $emit_{int}$ only resumes after its internal reaction completes and blocks, as discussed in Section 2.1.

At the beginning of the reaction, an external event is emitted, which will trigger rule **push**, which will immediately raise the stack level to 1. At the end of the reaction, the program will block or terminate and successive applications of rule **pop** will eventually lead to a description containing this same program at stack level 0. (Rule **pop** is the only rule that decreases the stack level.)

Nested transitions

The \xrightarrow{nst} rules are recursive definitions with the following general format:

$$\langle p, n, \varepsilon \rangle \xrightarrow{nst} \langle p', n, \varepsilon \rangle.$$

Nested transitions do not affect the stack level and never have an emitted event as a precondition. The distinction between \xrightarrow{out} and \xrightarrow{nst} prevents rules **push** and **pop** from matching and, consequently, from inadvertently modifying the current stack level before the nested reaction is complete.

A complete reaction consists of the following series of transitions:

$$\langle p, 0, e_{ext} \rangle \xrightarrow{push_{out}} \langle p_1, 1, \varepsilon \rangle \left[\xrightarrow{nst} \xrightarrow{out} \right]^* \xrightarrow{nst} \xrightarrow{pop_{out}} \langle p', 0, \varepsilon \rangle.$$

First, a $\xrightarrow{push_{out}}$ starts a nested reaction at level 1. Then, a series of alternations between zero or more \xrightarrow{nst} transitions (nested reactions) and a single \xrightarrow{out} transition (stack operation) takes place. Finally, a last $\xrightarrow{pop_{out}}$ transition decrements the stack level to 0 and terminates the reaction.

The \xrightarrow{nst} transition rules for atomic expressions are defined as follows:

$$\begin{array}{l} \langle mem(id), n, \varepsilon \rangle \xrightarrow{nst} \langle @nop, n, \varepsilon \rangle \quad (\text{mem}) \\ \langle emit_{int}(id), n, \varepsilon \rangle \xrightarrow{nst} \langle @canrun(n), n, id \rangle \quad (\text{emit-int}) \\ \langle @canrun(n), n, \varepsilon \rangle \xrightarrow{nst} \langle @nop, n, \varepsilon \rangle \quad (\text{can-run}) \end{array}$$

A mem operation becomes a @nop which indicates the memory access (rule **mem**). An $emit_{int}(id)$ generates an event id and transits to a $@canrun(n)$ which can only resume at level n (rule **emit-int**). Since all \xrightarrow{nst} rules can only transit with $e = \varepsilon$, an $emit_{int}$ causes rule **push** to execute at the outer level, creating a new level $n + 1$ on the stack. Also, with the new stack level, the resulting $@canrun(n)$ itself cannot transit (rule **can-run**), providing the desired stack-based semantics for internal events.

Proceeding to compound expressions, the rules for conditionals and sequences are straightforward:

$$\begin{array}{l} \frac{eval(mem(id))}{\langle if\ mem(id)\ then\ p\ else\ q, n, \varepsilon \rangle \xrightarrow{nst} \langle p, n, \varepsilon \rangle} \quad (\text{if-true}) \\ \frac{\neg eval(mem(id))}{\langle if\ mem(id)\ then\ p\ else\ q, n, \varepsilon \rangle \xrightarrow{nst} \langle q, n, \varepsilon \rangle} \quad (\text{if-false}) \\ \frac{\langle p, n, \varepsilon \rangle \xrightarrow{nst} \langle p', n, \varepsilon \rangle}{\langle p; q, n, \varepsilon \rangle \xrightarrow{nst} \langle p'; q, n, \varepsilon \rangle} \quad (\text{seq-adv}) \\ \langle @nop; q, n, \varepsilon \rangle \xrightarrow{nst} \langle q, n, \varepsilon \rangle \quad (\text{seq-nop}) \\ \langle break; q, n, \varepsilon \rangle \xrightarrow{nst} \langle break, n, \varepsilon \rangle \quad (\text{seq-brk}) \end{array}$$

Given that our semantics focuses on control, rules **if-true** and **if-false** are the only to query mem expressions. Function *eval* evaluates a given mem expression.

The rules for loops are analogous to sequences, but use “@” as separators to properly bind breaks to their enclosing loops:

$$\begin{array}{l} \langle loop\ p, n, \varepsilon \rangle \xrightarrow{nst} \langle p\ @loop\ p, n, \varepsilon \rangle \quad (\text{loop-expd}) \\ \frac{\langle q, n, \varepsilon \rangle \xrightarrow{nst} \langle q', n, \varepsilon \rangle}{\langle q\ @loop\ p, n, \varepsilon \rangle \xrightarrow{nst} \langle q'\ @loop\ p, n, \varepsilon \rangle} \quad (\text{loop-adv}) \\ \langle @nop\ @loop\ p, n, \varepsilon \rangle \xrightarrow{nst} \langle loop\ p, n, \varepsilon \rangle \quad (\text{loop-nop}) \\ \langle break\ @loop\ p, n, \varepsilon \rangle \xrightarrow{nst} \langle @nop, n, \varepsilon \rangle \quad (\text{loop-brk}) \end{array}$$

When a program encounters a loop, it first expands its body in sequence with itself (rule **loop-expd**). Rules **loop-adv** and **loop-nop** are similar to rules **seq-adv** and **seq-nop**, advancing the loop until a @nop is reached. However, what follows the loop is the loop itself (rule **loop-nop**). Note that if we used “;” as a separator in loops, rules **loop-brk** and **seq-brk** would conflict. Rule **loop-brk** escapes the enclosing loop, transforming everything into a @nop.

The semantic rules for and and or compositions force transitions on their left branches p to occur before their

right branches q :

$$\langle p \text{ and } q, n, \epsilon \rangle \xrightarrow{nst} \langle p \text{ @and } (@\text{canrun}(n); q), n, \epsilon \rangle \quad (\text{and-expd})$$

$$\frac{\langle p, n, \epsilon \rangle \xrightarrow{nst} \langle p', n, \epsilon \rangle}{\langle p \text{ @and } q, n, \epsilon \rangle \xrightarrow{nst} \langle p' \text{ @and } q, n, \epsilon \rangle} \quad (\text{and-adv1})$$

$$\frac{\text{isblocked}(p, n) \quad \langle q, n, \epsilon \rangle \xrightarrow{nst} \langle q', n, \epsilon \rangle}{\langle p \text{ @and } q, n, \epsilon \rangle \xrightarrow{nst} \langle p \text{ @and } q', n, \epsilon \rangle} \quad (\text{and-adv2})$$

$$\langle p \text{ or } q, n, \epsilon \rangle \xrightarrow{nst} \langle p \text{ @or } (@\text{canrun}(n); q), n, \epsilon \rangle \quad (\text{or-expd})$$

$$\frac{\langle p, n, \epsilon \rangle \xrightarrow{nst} \langle p', n, \epsilon \rangle}{\langle p \text{ @or } q, n, \epsilon \rangle \xrightarrow{nst} \langle p' \text{ @or } q, n, \epsilon \rangle} \quad (\text{or-adv1})$$

$$\frac{\text{isblocked}(p, n) \quad \langle q, n, \epsilon \rangle \xrightarrow{nst} \langle q', n, \epsilon \rangle}{\langle p \text{ @or } q, n, \epsilon \rangle \xrightarrow{nst} \langle p \text{ @or } q', n, \epsilon \rangle} \quad (\text{or-adv2})$$

Rules **and-expd** and **or-expd** insert a $@\text{canrun}(n)$ at the beginning of the right branch. This ensures that any emit_{int} on the left branch, which transits to a $@\text{canrun}(n)$, still resumes before the right branch starts. The deterministic behavior of the semantics relies on the *isblocked* predicate (see Figure 4) which appears in rules **and-adv2** and **or-adv2**. These rules require the left branch p to be blocked for the right branch to transition from q to q' .

In a parallel $@\text{and}$, if one of the sides terminates, the composition is simply substituted by the other side (rules **and-nop1** and **and-nop2** below). In a parallel $@\text{or}$, however, if one of the sides terminates, the whole composition terminates and function *clear* is used to properly finalize the aborted side (rules **or-nop1** and **or-nop2**).

$$\langle @\text{nop} \text{ @and } q, n, \epsilon \rangle \xrightarrow{nst} \langle q, n, \epsilon \rangle \quad (\text{and-nop1})$$

$$\frac{\text{isblocked}(p, n)}{\langle p \text{ @and } @\text{nop}, n, \epsilon \rangle \xrightarrow{nst} \langle p, n, \epsilon \rangle} \quad (\text{and-nop2})$$

$$\langle @\text{nop} \text{ @or } q, n, \epsilon \rangle \xrightarrow{nst} \langle \text{clear}(q), n, \epsilon \rangle \quad (\text{or-nop1})$$

$$\frac{\text{isblocked}(p, n)}{\langle p \text{ @or } @\text{nop}, n, \epsilon \rangle \xrightarrow{nst} \langle \text{clear}(p), n, \epsilon \rangle} \quad (\text{or-nop2})$$

The *clear* function (see Figure 4) concatenates all active *fin* bodies of the side being aborted, so that they execute before the composition rejoins. Note that there are no transition rules for *fin* expressions. This is because once reached, a *fin* expression halts and will only execute when it is aborted by a parallel trail and is expanded by the *clear* function. Note also that there is a syntactic restriction that postulates that *fin* bodies cannot contain awaiting expressions (*await_{ext}*, *await_{int}*, *every*, or *fin*), i.e., the result of a *clear* call is guaranteed to execute entirely within a reaction.

Finally, a break in one of the sides in parallel escapes the closest enclosing loop, properly aborting the other side by

applying the *clear* function:

$$\langle \text{break} \text{ @and } q, n, \epsilon \rangle \xrightarrow{nst} \langle \text{clear}(q); \text{break}, n, \epsilon \rangle \quad (\text{and-brk1})$$

$$\frac{\text{isblocked}(p, n)}{\langle p \text{ @and } \text{break}, n, \epsilon \rangle \xrightarrow{nst} \langle \text{clear}(p); \text{break}, n, \epsilon \rangle} \quad (\text{and-brk2})$$

$$\langle \text{break} \text{ @or } q, n, \epsilon \rangle \xrightarrow{nst} \langle \text{clear}(q); \text{break}, n, \epsilon \rangle \quad (\text{or-brk1})$$

$$\frac{\text{isblocked}(p, n)}{\langle p \text{ @or } \text{break}, n, \epsilon \rangle \xrightarrow{nst} \langle \text{clear}(p); \text{break}, n, \epsilon \rangle} \quad (\text{or-brk2})$$

A reaction eventually blocks in *await_{ext}*, *await_{int}*, *every*, *fin*, and $@\text{canrun}$ expressions in parallel trails. Then, if none of the trails is blocked in $@\text{canrun}$ expressions, it means that the program cannot advance in the current reaction. However, $@\text{canrun}$ expressions can still resume in lower stack indexes and will eventually resume in the current reaction (see rule **pop**).

3.3 Determinism, Termination, and Memory Bounds

- informal discussion

Determinism

The proof for determinism relies on the fact all semantic rules are mutually exclusive, i.e., their preconditions are unique in the set of rules. This can be verified by direct inspection of rules.

Rule **push** is the only one with $e \neq \epsilon$ as a precondition, and is trivially mutually exclusive with all other rules.

Rule **pop** either has $p = @\text{nop}$ or *isblocked*(p, n) as preconditions. Note that rule **pop** only applies syntactically to top-level transitions. For instance, it can never match \xrightarrow{nst} rules for subprograms as in rule **seq-adv**. Hence, for the first case, rule **pop** only applies, and is the only one to apply, to *nop* as the whole program (i.e., a *nop* not surrounded by other expressions, such as in rule **seq-nop**). For the second case, we need to show that given $\langle p, n, \epsilon \rangle$, no \xrightarrow{nst} transitions apply with *isblocked*(p, n) and vice versa. Except for $@\text{canrun}$, there are no \xrightarrow{nst} transitions for the other blocking expressions (*await_{Ext}*, *await_{Int}*, *every*, and *fin*). However, considering the precondition $\langle p, n, \epsilon \rangle$, *isblocked*($@\text{canrun}(n), n$) is false. Hence, given the preconditions for rule **pop**, no \xrightarrow{nst} transitions can occur. Conversely, if a \xrightarrow{nst} transition is possible, then *isblocked*(p, n) must be false. Again, except for $@\text{canrun}$, all other transitions do not involve blocking expressions, hence, for these transitions, *isblocked*(p, n) must be false. For rule **can-run**, a transition can only occur if the current stack level matches $@\text{canrun}(n)$. In this case, *isblocked*($@\text{canrun}(n), n$) is false.

Finally, we need to show that \xrightarrow{nst} transitions are mutually exclusive among themselves. Note that most rules have

```

771      (i) Function bcast:
772      bcast(awaitext(e), e) = @nop
773      bcast(awaitint(e), e) = @nop
774      bcast(every e p, e) = p; every e p
775      bcast(@canrun(n), e) = @canrun(n)
776      bcast(fin p, e) = fin p
777      bcast(p; q) = bcast(p, e); q
778      bcast(p @loop q, e) = bcast(p, e) @loop q
779      bcast(p @and q, e) = bcast(p, e) and bcast(q, e)
780      bcast(p @or q, e) = bcast(p, e) @or bcast(q, e)
781      bcast(_, e) = ⊥ (mem, emitint, break,
782      if then else, loop, and, or, @nop)
783
784      (ii) Predicate isblocked:
785      isblocked(awaitext(e), n) = true
786      isblocked(awaitint(e), n) = true
787      isblocked(every e p, n) = true
788      isblocked(@canrun(m), n) = (n > m)
789      isblocked(fin p, n) = true
790      isblocked(p; q, n) = isblocked(p, n)
791      isblocked(p @loop q, n) = isblocked(p, n)
792      isblocked(p @and q, n) = isblocked(p, n) ∧ isblocked(q, n)
793      isblocked(p @or q, n) = isblocked(p, n) ∧ isblocked(q, n)
794      isblocked(_, n) = false (mem, emitint, break,
795      if then else, loop, and, or, @nop)
796
797      (iii) Function clear:
798      clear(awaitext(e)) = @nop
799      clear(awaitint(e)) = @nop
800      clear(every e p) = @nop
801      clear(@canrun(n)) = @nop
802      clear(fin p) = p
803      clear(p; q) = clear(p)
804      clear(p @loop q) = clear(p)
805      clear(p @and q) = clear(p); clear(q)
806      clear(p @or q) = clear(p); clear(q)
807      clear(_) = ⊥ (mem, emitint, break,
808      if then else, loop, and, or, @nop)

```

Figure 4. (i) Function *bcast* awakes awaiting trails matching the event by converting await_{ext} and await_{int} to @nop expressions, and by unwinding every expressions. (ii) Predicate *isblocked* is true only if all branches in parallel are blocked waiting for events, for finalization clauses, or for certain stack levels. (iii) Function *clear* extracts fin expressions in parallel and put their bodies in sequence.

unique syntactic prefixes, e.g., (@nop @and *q*) (rule **and-nop1**) is trivially mutually exclusive with (@nop @loop *p*) (rule **or-nop1**). The only exceptions are rules **and-adv1** vs. **and-adv2**, and **or-adv1** vs. **or-adv2**. In both cases, we need to show that if the left branch can advance, then it cannot be blocked and vice-versa, i.e., that $\langle p, n, \epsilon \rangle \xrightarrow{nst} \langle p', n, e \rangle$ and *isblocked*(*p*, *n*) are mutually exclusive, which is exactly the same reasoning for rule **pop** above.

Termination

- there is always a possible transition until *n*=0
every cannot restart itself - break disallowed - emit ignored

Memory Bounds

- program is finite - lexical scope - no heap allocation - no code reentrancy - reexecution only due to loops - loop reuse nested vars -

4 Related Work

CÉU follows the lineage of imperative synchronous languages initiated by Esterel [8]. These languages typically define time as a discrete sequence of logical “ticks” in which multiple simultaneous input events can be active [16]. The presence of multiple inputs requires careful static analysis to detect and reject programs with *causality cycles* and *schizophrenia problems* [5]. In contrast, CÉU defines time as a discrete sequence of reactions to unique input events, which is a prerequisite for the concurrency checks that enable safe shared-memory concurrency.

Also, in most synchronous languages, the behavior of internal and external events is equivalent. In CÉU, internal events introduce stack-based micro reactions within external reactions, providing more fine-grained control for intra-reaction execution. This allows for memory-bounded sub-routines that execute multiple times in the same external reaction. The synchronous languages Statecharts [20] and Statemate [11] also distinguish internal from external events. In the former, “*reactions to external and internal events (...) can be sensed only after completion of the step*”. In the latter, “*the receiving state (of the internal event) acts here as a function*”. Although the descriptions suggest a stack-based semantics, we are not aware of formalizations for these ideas for a deeper comparison with CÉU.

Like CÉU, many synchronous languages [2, 7, 10, 12, 21] also rely on lexical scheduling to preserve determinism. In contrast, in Esterel, the execution order for operations within a reaction is non-deterministic: “*if there is no control dependency, as in (call f1() || call f2()), the order is unspecified and it would be an error to rely on it*” [6]. For this reason, Esterel, does not support shared-memory concurrency: “*if a variable is written by some thread, then it can neither be read nor be written by concurrent threads*” [6].

Regarding the integration with the C language-based environment, CÉU supports a finalization mechanism for external resources. In addition, CÉU also tracks pointers representing resources that cross C boundaries and forces the programmer to provide associated finalizers.

5 Conclusion

Francisco: TODO

References

- [1] A. Adya et al. 2002. Cooperative Task Management Without Manual Stack Management. In *Proceedings of ATEC'02*. USENIX Association, 289–302.
- [2] Sidharta Andalam, Partha Roop, and Alain Girault. 2010. Predictable multithreading of embedded applications using PRET-C. In *Proceeding of MEMOCODE'10*. IEEE, 159–168.
- [3] Albert Benveniste, Paul Caspi, Stephen A. Edwards, Nicolas Halbwachs, Paul Le Guernic, and Robert De Simone. 2003. The synchronous languages twelve years later. In *Proceedings of the IEEE*, Vol. 91. 64–83.
- [4] Gérard Berry. 1993. Preemption in Concurrent Systems.. In *FSTTCS (LNCS)*, Vol. 761. Springer, 72–93.
- [5] Gérard Berry. 1999. *The Constructive Semantics of Pure Esterel (draft version 3)*. Ecole des Mines de Paris and INRIA.
- [6] Gérard Berry. 2000. *The Esterel-V5 Language Primer*. CMA and Inria, Sophia-Antipolis, France. Version 5.10, Release 2.0.
- [7] Frédéric Boussinot. 1991. Reactive C: An extension of C to program reactive systems. *Software: Practice and Experience* 21, 4 (1991), 401–428.
- [8] Frédéric Boussinot and Robert De Simone. 1991. The Esterel language. *Proc. IEEE* 79, 9 (Sep 1991), 1293–1304.
- [9] Robert de Simone, Jean-Pierre Talpin, and Dumitru Potop-Butucaru. 2005. The Synchronous Hypothesis and Synchronous Languages. In *Embedded Systems Handbook*, R. Zurawski (Ed.).
- [10] Adam Dunkels, Oliver Schmidt, Thiemo Voigt, and Muneeb Ali. 2006. Protothreads: simplifying event-driven programming of memory-constrained embedded systems. In *Proceedings of SenSys'06*. ACM, 29–42.
- [11] David Harel and Amnon Naamad. 1996. The STATEMATE semantics of statecharts. *ACM Transactions on Software Engineering and Methodology* 5, 4 (1996), 293–333.
- [12] Marcin Karpinski and Vinny Cahill. 2007. High-Level Application Development is Realistic for Wireless Sensor Networks. In *Proceedings of SECON'07*. 610–619.
- [13] Ingo Maier, Tiark Rompf, and Martin Odersky. 2010. *Deprecating the observer pattern*. Technical Report.
- [14] ORACLE. 2011. Java Thread Primitive Deprecation. <http://docs.oracle.com/javase/6/docs/technotes/guides/concurrency/threadPrimitiveDeprecation.html> (accessed in Aug-2014). (2011).
- [15] Guido Salvaneschi et al. 2014. REScala: Bridging between object-oriented and functional style in reactive applications. In *Proceedings of Modularity'13*. ACM, 25–36.
- [16] Francisco Sant'anna, Roberto Ierusalimsky, Noemi Rodriguez, Silvana Rossetto, and Adriano Branco. 2017. The Design and Implementation of the Synchronous Language Céu. *ACM Trans. Embed. Comput. Syst.* 16, 4, Article 98 (July 2017), 26 pages. <https://doi.org/10.1145/3035544>
- [17] Francisco Sant'Anna, Noemi Rodriguez, and Roberto Ierusalimsky. 2015. Structured Synchronous Reactive Programming with Céu. In *Proceedings of Modularity'15*.
- [18] Francisco Sant'Anna, Noemi Rodriguez, Roberto Ierusalimsky, Olaf Landsiedel, and Philippas Tsigas. 2013. Safe System-level Concurrency on Resource-Constrained Nodes. In *Proceedings of SenSys'13*. ACM.
- [19] Rodrigo Santos, Guilherme Lima, Francisco Sant'Anna, and Noemi Rodriguez. 2016. Céu-Media: Local Inter-Media Synchronization Using Céu. In *Proceedings of WebMedia'16*. ACM, New York, NY, USA, 143–150. <https://doi.org/10.1145/2976796.2976856>
- [20] Michael von der Beeck. 1994. A comparison of statecharts variants. In *Proceedings of FTRIFT'94*. Springer, 128–148.
- [21] Reinhard von Hanxleden. 2009. SyncCharts in C: a proposal for light-weight, deterministic concurrency. In *Proceedings EMSOFT'09*. ACM, 225–234.

A Proofs

Determinism

Lemma A.1. *If $\delta \xrightarrow{\text{out}} \delta_1$ and $\delta \xrightarrow{\text{out}} \delta_2$ then $\delta_1 = \delta_2$.*

Proof. The lemma is vacuously true if δ cannot be advanced by $\xrightarrow{\text{out}}$ transitions. Suppose that is not the case and let $\delta = \langle p, n, e \rangle$, $\delta_1 = \langle p_1, n_1, e_1 \rangle$ and $\delta_2 = \langle p_2, n_2, e_2 \rangle$. Then, there are two possibilities.

Case 1. $e \neq \varepsilon$. Both transitions are applications of **push**. Hence $p_1 = p_2 = \text{bcast}(p, e)$, $n_1 = n_2 = n + 1$, and $e_1 = e_2 = \varepsilon$.

Case 2. $e = \varepsilon$. Both transitions are applications of **pop**. Hence $p_1 = p_2 = p$, $n_1 = n_2 = n - 1$, and $e_1 = e_2 = \varepsilon$. \square

Theorem A.2. *If $\delta \xrightarrow{n} \delta_1$ and $\delta \xrightarrow{n} \delta_2$ then $\delta_1 = \delta_2$.*

Proof. By induction on n . The theorem is trivially true for $n = 0$ and follows directly from Lemma A.1 for $n = 1$. (The theorem is vacuously true for $\xrightarrow{\text{push}_{\text{out}}}$ transitions if $n > 1$ since, by definition, $\xrightarrow{\text{push}_{\text{out}}}$ transitions cannot be applied more than once in a row and cannot occur after a $\xrightarrow{\text{pop}_{\text{out}}}$ transition.) Suppose $\delta \xrightarrow{1}_{\text{out}} \delta'_1 \xrightarrow{n-1}_{\text{out}} \delta_1$ and $\delta \xrightarrow{1}_{\text{out}} \delta'_2 \xrightarrow{n-1}_{\text{out}} \delta_2$, for some $n > 1$ and $\delta'_1, \delta'_2 \in \Delta$. By Lemma A.1, $\delta'_1 = \delta'_2$. By the induction hypothesis, $\delta_1 = \delta_2$. \square

Lemma A.3. *If $\delta \xrightarrow{nst} \delta_1$ and $\delta \xrightarrow{nst} \delta_2$ then $\delta_1 = \delta_2$.*

Proof. By induction on the structure of \xrightarrow{nst} derivations. The lemma is vacuously true if δ cannot be advanced by \xrightarrow{nst} transitions. Suppose that is not the case and let $\delta = \langle p, n, e \rangle$, $\delta_1 = \langle p_1, n_1, e_1 \rangle$ and $\delta_2 = \langle p_2, n_2, e_2 \rangle$. Then, by the hypothesis of the lemma, there are derivations π_1 and π_2 such that

$$\pi_1 \Vdash \langle p, n, e \rangle \xrightarrow{nst} \langle p_1, n_1, e_1 \rangle$$

$$\pi_2 \Vdash \langle p, n, e \rangle \xrightarrow{nst} \langle p_2, n_2, e_2 \rangle$$

i.e., the conclusion of π_1 is $\langle p, n, e \rangle \xrightarrow{nst} \langle p_1, n_1, e_1 \rangle$ and the conclusion of π_2 is $\langle p, n, e \rangle \xrightarrow{nst} \langle p_2, n_2, e_2 \rangle$.

By definition of \xrightarrow{nst} , we have that $e = \varepsilon$ and $n_1 = n_2 = n$. It remains to be shown that $p_1 = p_2$ and $e_1 = e_2$.

Depending on the structure of program p , the following 11 cases are possible. (Note that p cannot be an $\text{await}_{\text{ext}}$, $\text{await}_{\text{int}}$, break , every , fin , or @nop expression as there are no \xrightarrow{nst} rules to transition such programs.)

Case 1. $p = \text{mem}(id)$. Then derivations π_1 and π_2 are instances of rule **mem**, i.e., their conclusions are obtained by an application of this rule. Hence $p_1 = p_2 = \text{@nop}$ and $e_1 = e_2 = \varepsilon$.

Case 2. $p = \text{emit}_{\text{int}}(e')$. Then π_1 and π_2 are instances of **emit-int**. Hence $p_1 = p_2 = \text{@canrun}(n)$ and $e_1 = e_2 = e'$.

Case 3. $p = \text{@canrun}(n)$. Then π_1 and π_2 are instances of **can-run**. Hence $p_1 = p_2 = \text{@nop}$ and $e_1 = e_2 = \varepsilon$.

Case 4. $p = \text{if mem}(id) \text{ then } p' \text{ else } p''$. There are two sub-cases.

Case 4.1. $\text{eval}(\text{mem}(id))$ is true. Then π_1 and π_2 are instances of **if-true**. Hence $p_1 = p_2 = p'$ and $e_1 = e_2 = \varepsilon$.

Case 4.2. $eval(mem(id))$ is false. Then π_1 and π_2 are instances of **if-false**. Hence $p_1 = p_2 = p''$ and $e_1 = e_2 = \varepsilon$.

Case 5. $p = p'; p''$. There are three subcases.

Case 5.1. $p' = @nop$. Then π_1 and π_2 are instances of **seq-nop**. Hence $p_1 = p_2 = p''$ and $e_1 = e_2 = \varepsilon$.

Case 5.2. $p' = break$. Then π_1 and π_2 are instances of **seq-brk**. Hence $p_1 = p_2 = break$ and $e_1 = e_2 = \varepsilon$.

Case 5.3. $p' \neq @nop, break$. Then π_1 and π_2 are instances of **seq-adv**. Thus there are derivations π'_1 and π'_2 such that

$$\pi'_1 \Vdash \langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1, n, e'_1 \rangle$$

$$\pi'_2 \Vdash \langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_2, n, e'_2 \rangle$$

for some $p'_1, p'_2 \in P$ and $e'_1, e'_2 \in E$. By the induction hypothesis, $p'_1 = p'_2$ and $e'_1 = e'_2$. Hence $p_1 = p'_1; p'' = p'_2; p'' = p_2$ and $e_1 = e'_1 = e'_2 = e_2$.

Case 6. $p = loop p'$. Then π_1 and π_2 are instances of **loop-expd**. Hence $p_1 = p_2 = p' @loop p''$ and $e_1 = e_2 = \varepsilon$.

Case 7. $p = p' @loop p''$. There are three subcases.

Case 7.1. $p' = @nop$. Then π_1 and π_2 are instances of **loop-nop**. Hence $p_1 = p_2 = loop p''$ and $e_1 = e_2 = \varepsilon$.

Case 7.2. $p' = break$. Then π_1 and π_2 are instances of **loop-break**. Hence $p_1 = p_2 = @nop$ and $e_1 = e_2 = \varepsilon$.

Case 7.3. $p' \neq @nop, break$. Then π_1 and π_2 are instances of **loop-adv**. Thus there are derivations π'_1 and π'_2 such that

$$\pi'_1 \Vdash \langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1, n, e'_1 \rangle$$

$$\pi'_2 \Vdash \langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_2, n, e'_2 \rangle$$

for some $p'_1, p'_2 \in P$ and $e'_1, e'_2 \in E$. By the induction hypothesis, $p'_1 = p'_2$ and $e'_1 = e'_2$. Hence $p_1 = p'_1 @loop p'' = p'_2 @loop p'' = p_2$ and $e_1 = e'_1 = e'_2 = e_2$.

Case 8. $p = p'$ and p'' . Then π_1 and π_2 are instances of **and-expd**. Hence $p_1 = p_2 = p' @and (@canrun(n); p'')$ and $e_1 = e_2 = \varepsilon$.

Case 9. $p = p' @and p''$. There are two subcases.

Case 9.1. $isblocked(p', n)$ is false. There are three subcases.

Case 9.1.1. $p' = @nop$. Then π_1 and π_2 are instances of **and-nop1**. Hence $p_1 = p_2 = p''$ and $e_1 = e_2 = \varepsilon$.

Case 9.1.2. $p' = break$. Then π_1 and π_2 are instances of **and-brk1**. Hence $p_1 = p_2 = clear(p'')$; break and $e_1 = e_2 = \varepsilon$.

Case 9.1.3. $p' \neq @nop, break$. Then π_1 and π_2 are instances of **and-adv1**. Thus there are derivations π'_1 and π'_2 such that

$$\pi'_1 \Vdash \langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1, n, e'_1 \rangle$$

$$\pi'_2 \Vdash \langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_2, n, e'_2 \rangle$$

for some $p'_1, p'_2 \in P$ and $e'_1, e'_2 \in E$. By the induction hypothesis, $p'_1 = p'_2$ and $e'_1 = e'_2$. Hence $p_1 = p'_1$ and $p'' = p'_2$ and $p'' = p_2$ and $e_1 = e'_1 = e'_2 = e_2$.

Case 9.2. $isblocked(p', n)$ is true. There are three subcases.

Case 9.2.1. $p'' = @nop$. Then π_1 and π_2 are instances of **and-nop2**. Hence $p_1 = p_2 = p'$ and $e_1 = e_2 = \varepsilon$.

Case 9.2.2. $p'' = break$. Then π_1 and π_2 are instances of **and-brk2**. Hence $p_1 = p_2 = clear(p')$; break and $e_1 = e_2 = \varepsilon$.

Case 9.2.3. $p'' \neq @nop, break$. Then π_1 and π_2 are instances of **and-adv2**. Thus there are derivations π''_1 and π''_2 such that

$$\pi''_1 \Vdash \langle p'', n, \varepsilon \rangle \xrightarrow{nst} \langle p''_1, n, e''_1 \rangle$$

$$\pi''_2 \Vdash \langle p'', n, \varepsilon \rangle \xrightarrow{nst} \langle p''_2, n, e''_2 \rangle$$

for some $p''_1, p''_2 \in P$ and $e''_1, e''_2 \in E$. By the induction hypothesis, $p''_1 = p''_2$ and $e''_1 = e''_2$. Hence $p_1 = p'$ and $p'_1 = p'$ and $p'_2 = p_2$ and $e_1 = e''_1 = e''_2 = e_2$.

Case 10. $p = p'$ or p'' . Then π_1 and π_2 are instances of **or-expd**. Hence $p_1 = p_2 = p' @or (@canrun(n); p'')$ and $e_1 = e_2 = \varepsilon$.

Case 11. $p = p' @or p''$. There are two subcases.

Case 11.1. $isblocked(p', n)$ is false. There are three subcases.

Case 11.1.1. $p' = @nop$. Then π_1 and π_2 are instances of **or-nop1**. Hence $p_1 = p_2 = clear(p'')$ and $e_1 = e_2 = \varepsilon$.

Case 11.1.2. $p' = break$. Similar to Case 9.1.2.

Case 11.1.3. $p' \neq @nop, break$. Similar to Case 9.1.3.

Case 11.2. $isblocked(p', n)$ is true. There are three subcases.

Case 11.2.1. $p'' = @nop$. Then π_1 and π_2 are instances of **or-nop1**. Hence $p_1 = p_2 = clear(p')$ and $e_1 = e_2 = \varepsilon$.

Case 11.2.2. $p'' = break$. Similar to Case 9.2.2.

Case 11.2.3. $p'' \neq @nop, break$. Similar to Case 9.2.3. \square

Theorem A.4. If $\delta \xrightarrow{nst} \delta_1$ and $\delta \xrightarrow{nst} \delta_2$ then $\delta_1 = \delta_2$.

Proof. Similar to the proof of Theorem A.2. \square

Termination

Definition A.5. A description $\delta = \langle p, n, e \rangle$ is *nested-irreducible* iff $e \neq \varepsilon$ or $p = @nop, break$ or $isblocked(p, n)$ is true. Nested-irreducible descriptions serve as normal forms for \xrightarrow{nst} transitions: they embody the result of an exhaustive number of \xrightarrow{nst} applications. We will write $\delta_{\#nst}$ to indicate that description δ is nested-irreducible.

The next lemma justifies the use of qualifier “irreducible” in Definition A.5.

Lemma A.6. *If $\delta \xrightarrow{nst} \delta'_{\#nst}$ then, for all $i \neq n$, there is no $\delta''_{\#nst}$ such that $\delta \xrightarrow{i} \delta''_{\#nst}$.*

Proof. By contradiction on the hypothesis that there is such i . Let $\delta \xrightarrow{n} \delta'_{\#nst}$, for some $n \geq 0$. There are two cases.

Case 1. Suppose there are $i > n$ and $\delta''_{\#nst}$ such that $\delta \xrightarrow{i} \delta''$. Then, by definition of \xrightarrow{i} ,

$$\delta \xrightarrow{n} \delta' \xrightarrow{n+1} \delta'_1 \xrightarrow{n+2} \dots \xrightarrow{i} \delta'' \quad (1)$$

Since $\delta' = \langle p', n, e' \rangle$ is nested-irreducible, $e' = \varepsilon$ or $p = @nop$, break or *isblocked*(p', n). In any of these cases, by the definition of \xrightarrow{nst} , there is no δ'_1 such that $\delta' \xrightarrow{1} \delta'_1$, which contradicts (1). Therefore, no such i can exist.

Case 2. Suppose there are $i < n$ and $\delta''_{\#nst}$ such that $\delta \xrightarrow{i} \delta''$. Then, since $n > i$, by Case 1, δ' cannot exist, which is absurd. Therefore, the assumption that there is such i is false. \square

The next lemma establishes some basic properties of sequences of \xrightarrow{nst} transitions.

Lemma A.7. *If $\langle p_1, n, e \rangle \xrightarrow{nst} \langle p'_1, n, e' \rangle$ then, for any p_2 :*

- (a) $\langle p_1; p_2, n, e \rangle \xrightarrow{nst} \langle p'_1; p_2, n, e' \rangle$;
- (b) $\langle p_1 @loop p_2, n, e \rangle \xrightarrow{nst} \langle p'_1 @loop p_2, n, e' \rangle$;
- (c) $\langle p_1 @and p_2, n, e \rangle \xrightarrow{nst} \langle p'_1 @and p_2, n, e' \rangle$;
- (d) $\langle p_1 @or p_2, n, e \rangle \xrightarrow{nst} \langle p'_1 @or p_2, n, e' \rangle$.

*If $\langle p_2, n, e \rangle \xrightarrow{nst} \langle p'_2, n, e' \rangle$, for any p_1 such that *isblocked*(p_1, n):*

- (e) $\langle p_1 @and p_2, n, e \rangle \xrightarrow{nst} \langle p_1 @and p'_2, n, e' \rangle$;
- (f) $\langle p_1 @or p_2, n, e \rangle \xrightarrow{nst} \langle p_1 @or p'_2, n, e' \rangle$.

Proof. By induction on n .

(a) The lemma is trivially true for $n = 0$, as $p_1 = p'_1$, and follows directly from **seq-adv** for $n = 1$. Suppose

$$\langle p_1, n, e \rangle \xrightarrow{1} \langle p'_1, n, e'' \rangle \xrightarrow{n-1} \langle p'_1, n, e' \rangle, \quad (2)$$

for some $n > 1$. Then $\langle p'_1, n, e'' \rangle$ is not nested-irreducible, i.e., $e = \varepsilon$ and $p \neq @nop$, break and *isblocked*(p'_1, n) is false. By (2) and by **seq-adv**,

$$\langle p_1; p_2, n, e \rangle \xrightarrow{1} \langle p'_1; p_2, n, e'' \rangle. \quad (3)$$

From (2), by the induction hypothesis,

$$\langle p'_1; p_2, n, e'' \rangle \xrightarrow{n-1} \langle p'_1; p_2, n, e' \rangle. \quad (4)$$

From (3) and (4),

$$\langle p_1; p_2, n, e \rangle \xrightarrow{n} \langle p'_1; p_2, n, e' \rangle.$$

- (b) Similar to Case (a).
- (c) Similar to Case (a).
- (d) Similar to Case (a).

(e) The lemma is trivially true for $n = 0$, as $p_2 = p'_2$, and follows directly from **and-adv2** for $n = 1$. Suppose

$$\langle p_2, n, e \rangle \xrightarrow{1} \langle p'_2, n, e'' \rangle \xrightarrow{n-1} \langle p'_2, n, e' \rangle, \quad (5)$$

for some $n > 1$. Then $\langle p'_2, n, e'' \rangle$ is not nested-irreducible. By (5) and by **and-adv2**,

$$\langle p_1 @and p_2, n, e \rangle \xrightarrow{1} \langle p_1 @and p'_2, n, e'' \rangle. \quad (6)$$

From (5), by the induction hypothesis,

$$\langle p_1 @and p'_2, n, e'' \rangle \xrightarrow{n-1} \langle p_1 @or p'_2, n, e' \rangle. \quad (7)$$

From (6) and (7),

$$\langle p_1 @and p_2, n, e \rangle \xrightarrow{n} \langle p_1 @and p'_2, n, e' \rangle.$$

(f) Similar to Case (e). \square

The syntactic restrictions discussed in Section ??, regarding the body of *fin* and *loop* expressions, are formalized by the following assumptions.

Assumption A.8. If $\delta = \langle clear(p), n, \varepsilon \rangle$ then there is a description $\delta' = \langle @nop, n, \varepsilon \rangle$ such that $\delta \xrightarrow{*} \delta'$.

Assumption A.9. If $\delta = \langle loop p, n, \varepsilon \rangle$ then there is a description $\delta' = \langle p', n, e \rangle$ such that $\delta \xrightarrow{*} \delta'$ where either $p' = break @loop p$ or *isblocked*_{ext}(p', n).

Theorem A.10. For any δ there is a $\delta'_{\#nst}$ such that $\delta \xrightarrow{*} \delta'_{\#nst}$.

Proof. By induction on the structure of programs. Let $\delta = \langle p, n, \varepsilon \rangle$. The theorem is trivially true if δ is nested-irreducible, as by definition $\delta \xrightarrow{0} \delta_{\#nst}$. Suppose that is not the case. Then, depending on the structure of p , there are 11 possibilities. In each one of them, we show that such $\delta'_{\#nst}$ indeed exists.

Case 1. $p = mem(id)$. Then, by **mem**,

$$\langle mem(id), n, \varepsilon \rangle \xrightarrow{1} \langle @nop, n, \varepsilon \rangle_{\#nst}.$$

Case 2. $p = emit_{int}(e)$. Then, by **emit-int**,

$$\langle emit_{int}(e), n, \varepsilon \rangle \xrightarrow{1} \langle @canrun(n), n, e \rangle_{\#nst}.$$

Case 3. $p = @canrun(n)$. Then, by **can-run**,

$$\langle @canrun(n), n, \varepsilon \rangle \xrightarrow{1} \langle @nop, n, \varepsilon \rangle_{\#nst}.$$

Case 4. $p = if mem(id) then p' else p''$. There are two subcases.

Case 4.1. *eval*(*mem*(*id*)) is true. Then, by **if-true** and by the induction hypothesis, there is a δ' such that

$$\langle if mem(id) then p' else p'', n, \varepsilon \rangle \xrightarrow{1} \langle p', n, e \rangle \xrightarrow{*} \delta'_{\#nst}.$$

Case 4.2. *eval*(*mem*(*id*)) is false. Then, by **if-false** and by the induction hypothesis, there is a δ' such that

$$\langle if mem(id) then p' else p'', n, \varepsilon \rangle \xrightarrow{1} \langle p'', n, e \rangle \xrightarrow{*} \delta'_{\#nst}.$$

Case 5. $p = p'; p''$. There are three subcases.

Case 5.1. $p' = \text{@nop}$. Then, by **seq-nop** and by the induction hypothesis, there is a δ' such that

$$\langle \text{@nop}; p'', n, \varepsilon \rangle \xrightarrow{nst} \langle p'', n, e \rangle \xrightarrow{nst} \delta'_{\#nst}.$$

Case 5.2. $p' = \text{break}$. Then, by **seq-brk**,

$$\langle \text{break}; p'', n, \varepsilon \rangle \xrightarrow{nst} \langle \text{break}, n, \varepsilon \rangle_{\#nst}.$$

Case 5.3. $p' \neq \text{@nop}, \text{break}$. Then, by the induction hypothesis, there are p'_1 and e such that

$$\langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1, n, e \rangle_{\#nst}.$$

By item (a) of Lemma A.7,

$$\langle p'; p'', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1; p'', n, e \rangle. \quad (8)$$

It remains to be shown that $\langle p'_1; p'', n, e \rangle$ is nested-irreducible. There are four possibilities following from the fact that the simpler $\langle p'_1, n, e \rangle$ is nested-irreducible.

Case 5.3.1. $e \neq \varepsilon$. Then, by the definition of $\#nst$, description $\langle p'_1; p'', n, e \rangle$ is nested-irreducible.

Case 5.3.2. $p'_1 = \text{@nop}$. From (8),

$$\langle p'; p'', n, \varepsilon \rangle \xrightarrow{nst} \langle \text{@nop}; p'', n, e \rangle.$$

From this point on, this case is similar to Case 5.1.

Case 5.3.3. $p'_1 = \text{break}$. From (8),

$$\langle p'; p'', n, \varepsilon \rangle \xrightarrow{nst} \langle \text{break}; p'', n, e \rangle.$$

From this point on, this case is similar to Case 5.2.

Case 5.3.4. $\text{isblocked}(p'_1, n)$ is true. Then, by definition, $\text{isblocked}(p'_1; p'', n) = \text{isblocked}(p'_1, n) = \text{true}$.

Hence, from (8) and by the definition $\#nst$, description $\langle p'_1; p'', n, e \rangle$ is nested-irreducible.

Case 6. $p = \text{loop } p'$. Then, by Assumption A.9,

$$\langle \text{loop } p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1, n, e \rangle, \quad (9)$$

for some e and p'_1 such that either $p'_1 = \text{break @loop } p'$ or $\text{isblocked}_{\text{ext}}(p'_1, n)$.

Case 6.1. $p'_1 = \text{break @loop } p'$. From (9), by **loop-brk**,

$$\langle \text{loop } p', n, \varepsilon \rangle \xrightarrow{nst} \langle \text{break @loop } p', n, e \rangle \xrightarrow{nst} \langle \text{@nop}, n, e \rangle_{\#nst}.$$

Case 6.2. $\text{isblocked}_{\text{ext}}(p'_1, n)$ is true. Then, by definition, $\text{isblocked}_{\text{ext}}(p'_1, n)$ implies $\text{isblocked}(p'_1, n)$. Hence, from (9) and by the definition of $\#nst$, $\langle p'_1, n, e \rangle_{\#nst}$.

Case 7. $p = p' @ \text{loop } p''$. There are three subcases.

Case 7.1. $p' = \text{@nop}$. Then, by **loop-nop**,

$$\langle \text{@nop @loop } p'', n, \varepsilon \rangle \xrightarrow{nst} \langle \text{loop } p'', n, \varepsilon \rangle.$$

From this point on, this case is similar to Case 6.

Case 7.2. $p' = \text{break}$. Then, by **loop-brk**,

$$\langle \text{break @loop } p'', n, \varepsilon \rangle \xrightarrow{nst} \langle \text{@nop}, n, \varepsilon \rangle_{\#nst}.$$

Case 7.3. $p' \neq \text{@nop}, \text{break}$. Then, by the induction hypothesis, there are p'_1 and e such that

$$\langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1, n, e \rangle_{\#nst}.$$

By item (b) of Lemma A.7,

$$\langle p' @ \text{loop } p'', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1 @ \text{loop } p'', n, e \rangle.$$

It remains to be show that $\langle p'_1 @ \text{loop } p'', n, e \rangle$ is nested-irreducible. The rest of this proof is similar to that of Case 5.3.

Case 8. $p = p'$ and p'' . Then, by **and-expd**,

$$\langle p' \text{ and } p'', n, \varepsilon \rangle \xrightarrow{nst} \langle p' @ \text{and} (\text{canrun}(n); p''), n, \varepsilon \rangle.$$

From this point on, this case is similar to Case 9.

Case 9. $p = p' @ \text{and } p''$. There are two subcases.

Case 9.1. $\text{isblocked}(p', n)$ is false. There are three subcases.

Case 9.1.1. $p' = \text{@nop}$. Then, by **and-nop1** and by the induction hypothesis, there is a δ' such that

$$\langle \text{@nop @and } p'', n, \varepsilon \rangle \xrightarrow{nst} \langle p'', n, \varepsilon \rangle \xrightarrow{nst} \delta'_{\#nst}.$$

Case 9.1.2. $p' = \text{break}$. Then, by **and-brk1**,

$$\langle \text{break @and } p'', n, \varepsilon \rangle \xrightarrow{nst} \langle \text{clear}(p''); \text{break}, n, \varepsilon \rangle. \quad (10)$$

From (10), by Assumption A.8 and **seq-nop**,

$$\langle \text{clear}(p''); \text{break}, n, \varepsilon \rangle \xrightarrow{nst} \langle \text{@nop}; \text{break}, n, \varepsilon \rangle \xrightarrow{nst} \langle \text{break}, n, \varepsilon \rangle_{\#nst}.$$

Case 9.1.3. $p' \neq \text{@nop}, \text{break}$. Then, by the induction hypothesis, there are p'_1 and e such that

$$\langle p', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1, n, e \rangle_{\#nst}.$$

By item (c) of Lemma A.7,

$$\langle p' @ \text{and } p'', n, \varepsilon \rangle \xrightarrow{nst} \langle p'_1 @ \text{and } p'', n, e \rangle.$$

It remains to be show that $\langle p'_1 @ \text{and } p'', n, e \rangle$ leads to an nested-irreducible description. There are four possibilities following from the fact that the simpler $\langle p'_1, n, e \rangle$ is nested-irreducible.

1. If $e \neq \varepsilon$ then, by definition, $\langle p'_1 @ \text{and } p'', n, e \rangle_{\#nst}$.
2. If $p'_1 = \text{@nop}$, this case is similar to Case 9.1.1.
3. If $p'_1 = \text{break}$, this case is similar to Case 9.1.2.
4. If $\text{isblocked}(p'_1, n)$, this case is similar to Case 9.2.

Case 9.2. $\text{isblocked}(p', n)$ is true. There are three subcases.

Case 9.2.1. $p'' = \text{@nop}$. Then, by **and-nop2**,

$$\langle p' @ \text{and} @ \text{nop}, n, \varepsilon \rangle \xrightarrow{nst} \langle p', n, \varepsilon \rangle_{\#nst}.$$

Case 9.2.2. $p'' = \text{break}$. Then, by **and-brk2**,

$$\langle p' @ \text{and } \text{break}, n, \varepsilon \rangle \xrightarrow{nst} \langle \text{clear}(p'); \text{break}, n, \varepsilon \rangle.$$

From this point on, this case is similar to Case 9.1.2.

Case 9.2.3. $p'' \neq \text{@nop}$, break. Then, by the induction hypothesis, there are p_1'' and e such that

$$\langle p'', n, \varepsilon \rangle \xrightarrow[nst]{*} \langle p_1'', n, e \rangle_{\#nst}.$$

By item (e) of Lemma A.7,

$$\langle p' \text{@and } p'', n, \varepsilon \rangle \xrightarrow[nst]{*} \langle p' \text{@and } p_1'', n, e \rangle.$$

It remains to be show that $\langle p' \text{@and } p_1'', n, e \rangle$ leads to an nested-irreducible description. There are four possibilities following from the fact that the simpler $\langle p_1'', n, e \rangle$ is nested-irreducible.

1. If $e \neq \varepsilon$ then, by definition, $\langle p' \text{@and } p_1'', n, e \rangle_{\#nst}$.
2. If $p_1'' = \text{@nop}$, this case is similar to Case 9.2.1.
3. If $p_1'' = \text{break}$, this case is similar to Case 9.2.2.
4. If $\text{isblocked}(p_1'', n)$ then, as both sides are blocked, by definition, $\langle p' \text{@and } p_1'', n, e \rangle_{\#nst}$.

Case 10. $p = p'$ or p'' . Then, by **or-expd**,

$$\langle p' \text{ or } p'', n, \varepsilon \rangle \xrightarrow[nst]{1} \langle p' \text{@or } (\text{@canrun}(n); p''), n, \varepsilon \rangle.$$

From this point on, this case is similar to Case 11.

Case 11. $p = p' \text{@or } p''$. There are two subcases.

Case 11.1. $\text{isblocked}(p', n)$ is false. There are three subcases.

Case 11.1.1. $p' = \text{@nop}$. Then, by **or-nop1**,

$$\langle \text{@nop @or } p'', n, \varepsilon \rangle \xrightarrow[nst]{1} \langle \text{clear}(p''), n, \varepsilon \rangle. \quad (11)$$

From (11), by Assumption A.8,

$$\langle \text{clear}(p''), n, \varepsilon \rangle \xrightarrow[nst]{*} \langle \text{@nop}, n, \varepsilon \rangle_{\#nst}.$$

Case 11.1.2. $p' = \text{break}$. Similar to Case 9.1.2.

Case 11.1.3. $p' \neq \text{@nop}$, break. Similar to Case 9.1.3.

Case 11.2. $\text{isblocked}(p', n)$ is true. There are three subcases.

Case 11.2.1. $p'' = \text{@nop}$. Then, by **or-nop2**,

$$\langle p' \text{@or } \text{@nop}, n, \varepsilon \rangle \xrightarrow[nst]{1} \langle \text{clear}(p'), n, \varepsilon \rangle. \quad (12)$$

From (12), by Assumption A.8,

$$\langle \text{clear}(p'), n, \varepsilon \rangle \xrightarrow[nst]{*} \langle \text{@nop}, n, \varepsilon \rangle_{\#nst}.$$

Case 11.2.2. $p'' = \text{break}$. Similar to Case 9.2.2.

Case 11.2.3. $p'' \neq \text{@nop}$, break. Similar to Case 9.2.3.

□