Analysis of Recursively Parallel Programs
Ahmed Bouajjani, Michael Emmi

To cite this version:
Ahmed Bouajjani, Michael Emmi. Analysis of Recursively Parallel Programs. 2011. <hal-00639351v2>

HAL Id: hal-00639351
https://hal.archives-ouvertes.fr/hal-00639351v2
Submitted on 14 Nov 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Analysis of Recursively Parallel Programs

Ahmed Bouajjani
LIAFA, Université Paris Diderot, France
abou@liafa.jussieu.fr

Michael Emmi
LIAFA, Université Paris Diderot, France
mje@liafa.jussieu.fr

Abstract

We propose a general formal model of isolated hierarchical parallel computations, and identify several fragments to match the concurrency constructs present in real-world programming languages such as Cilk and X10. By associating fundamental formal models (vector addition systems with recursive transitions) to each fragment, we provide a common platform for exposing the relative difficulties of algorithmic reasoning. For each case we measure the complexity of deciding state-reachability for finite-data recursive programs, and propose algorithms for the decidable cases. The complexities which include PTIME, NP, EXPSPACE, and 2EXPSPACE contrast with undecidable state-reachability for recursive multi-threaded programs.

1. Introduction

Despite the ever-increasing importance of concurrent software (e.g., for designing reactive applications, or parallelizing computation across multiple processor cores), concurrent programming and concurrent program analysis remain challenging endeavors. The most widely available facility for designing concurrent applications is multithreading, where concurrently executing sequential threads nondeterministically interleave their accesses to shared memory. Such nondeterminism leads to rarely occurring “Heisenbugs” which are notoriously difficult to reproduce and repair. To prevent such bugs programmers are faced with the difficult task of preventing undesirable interleavings, e.g., by employing lock-based synchronization, without preventing benign interleavings—otherwise the desired reactivity or parallelism is forfeited.

The complexity of multi-threaded program analysis seems to comply with the perceived difficulty of multi-threaded programming. The state-reachability problem for multi-threaded programs is PSPACE-complete \[ \text{PSPACE-complete} \] with a finite number of finite-state threads, and undecidable \[ \text{undecidable} \] with recursive threads. Current analysis approaches either explore an underapproximate concurrent semantics by considering relatively few interleavings \[ \text{underapproximate} \] or explore a coarse overapproximate semantics via abstraction \[ \text{coarse overapproximate} \].

Explicitly-parallel programming languages have been advocated to avoid the intricate interleavings implicit in program syntax \[ \text{syntax} \], and several such industrial-strength languages have been developed \[ \text{developed} \]. Such systems introduce various mechanisms for creating (e.g., fork, spawn, post) and consuming \[ \text{creating} \] concurrent computations, and either encourage (through recommended programming practices) or ensure (through static analyses or runtime systems) that parallel computations execute in isolation without interference from others, through data-partitioning \[ \text{data-partitioning} \], data-replication \[ \text{data-replication} \], functional programming \[ \text{functional programming} \], message passing \[ \text{message passing} \], or version-based memory access models \[ \text{version-based memory access models} \].

perhaps falling back on transactional mechanisms \[ \text{transactional mechanisms} \] when complete isolation is impractical. Although few of these systems behave deterministically, consuming one concurrent computation at a time, many are sensitive to the order in which multiple isolated computations are consumed. Furthermore, some allow computations creating an unbounded number of sub-computations, returning to their superiors an unbounded number of handles to unfinished computations. Even without multithreaded interleaving, nondeterminism in the order in which an unbounded number of computations are consumed has the potential to make program reasoning complex.

In this work we investigate key questions on the analysis of interleaving-free programming models. Specifically, we ask to what extent such models simplify program reasoning, how those models compare with each other, and how to design appropriate analysis algorithms. We attempt to answer these questions as follows:

- We introduce a general interleaving-free parallel programming model on which to express the features found in popular parallel programming languages (Section 2).
- We discover a surprisingly-complex feature of some existing languages: even simple classes of programs with the ability to pass unfinished computations both to and from subordinate computations have undecidable state-reachability problems (Section 2.4).
- We show that the concurrency features present in many real-world programming languages such as Cilk, X10, and Multilisp are captured precisely (modulo the possibility of interleaving) by various fragments of our model (Sections 3 and 6).
- For fragments corresponding to real-world language features, we measure the complexity of computing state-reachability for finite-data programs, and provide, in most cases, asymptotically optimal state-reachability algorithms (Sections 5 and 7).

Our focus on finite-data programs without interleaving is a means to measuring complexity for the sake of comparison, required since state-reachability for infinite-data or multi-threaded programs is generally undecidable. Applying our algorithms in practice may rely on data abstraction \[ \text{data abstraction} \], and separately ensuring isolation \[ \text{isolation} \], or approximating possible interleavings \[ \text{approximating} \] still, our handling of computation-order non-determinism is precise.

The major distinguishing language features are whether a single or an arbitrary number of subordinate computations are waited for at once, and whether the scope of subordinate computations is confined. Generally speaking, reasoning for the “single-wait” case of Section 4 is less difficult than for the “multi-wait” case of Section 5, and we demonstrate a range of complexities \[ \text{complexities} \] from PTIME, NP, EXPSPACE, and 2EXPSPACE for various scope restrictions in Sections 5 and 7.

Despite these worst-case complexities, a promising line of work has

---

* Partially supported by the project ANR-09-SEGI-016 Veridyc.
† Supported by a post-doctoral fellowship from the Fondation Sciences Mathématiques de Paris.
0 Proofs to technical results are contained in the appendices.
1 In order to isolate concurrent complexity from the exponential factor in the number of program variables, we consider a fixed number of variables in each procedure frame; this allows us a PTIME point-of-reference for state-reachability in recursive sequential programs [23].
We consider a simple concurrent programming model where computation is hierarchically divided into isolated parallelly executing tasks. Each task executes sequentially while maintaining a set of region identifiers, which highlight the sources of concurrent complexity resulting from the inter-procedural statement blocks executing until some task whose handle is stored in region \( r \) completes, at which point its return-value handler is executed. Similarly, the await \( r \) statement blocks execution until all tasks whose handles are stored in region \( r \) complete, at which point all of their return-value handlers are executed, in some order. We refer to the call, return, post, await and await as inter-procedural statements, and the others as intra-procedural statements, and insist that return-value handlers are comprised only of intra-procedural statements. The assume \( e \) statement proceeds only when \( e \) evaluates to true—we use this statement in subsequent sections to block undesired executions in our encodings of other parallel programming models.

Example 1. The Fibonacci function can be implemented as a single-region recursively parallel program as follows.

\[
\begin{align*}
\text{proc } fib \ (\text{var } n : \mathbb{N}) \\
\text{var } \text{sum} : \mathbb{N} \\
\text{if } n < 2 \text{ then } \\
\text{return } 1 \\
\text{else } \\
\text{post } r \leftarrow fib (n-1) \in (\lambda v. \text{sum} := \text{sum} + v); \\
\text{post } r \leftarrow fib (n-2) \in (\lambda v. \text{sum} := \text{sum} + v); \\
\text{await } r; \\
\text{return } \text{sum}
\end{align*}
\]

Alternate implementations are possible, e.g., by replacing the await statement by two await statements, or storing the handles to the recursive calls in separate regions. Note that in this implementation task-handles are not passed to child tasks (\( e \) specifies the empty region sequence) nor to parent tasks (all handles are consumed by the await statement before returning).

The programming language we consider is simple yet expressive, since the syntax of types and expressions is left free, and we lose no generality by considering only a single variable per procedure.

2.2 Parallel Semantics with Task-Passing

Unlike recursive sequential programs, whose semantics is defined over stacks of procedure frames, the semantics of recursively parallel programs is defined over trees of procedure frames. Intuitively, the frame of each posted task becomes a child of the posting task’s frame. Each step of execution proceeds either by making a single intra-procedural statement or by invoking a child frame by posting a task, or removing a frame by consuming a completed task; the only sub-task frames of a completed task are added as children to the completed task’s parent.

A task \( \ell, t, d \) is a valuation \( \ell \in \text{Vals} \) to the procedure-local variable \( \ell \), along with a statement \( s \) to be executed, and a return-value handler \( d \in \text{Rets} \). (Here \( s \) describes the entire body of a procedure \( p \) that remains to be evaluated, and is initially set to \( \text{post} \)’s top-level statement \( s_p \).) A tree configuration \( c \) is a finite unordered tree of task-labeled vertices and region-labeled edges, and the set of configurations is denoted \( \text{Configs} \). Let \( \mathbb{M}[\text{Configs}] \) denote the set of configuration multisets, which are represented inductively, writing \( (t, m, \ell) \) for the tree with \( \ell \)-labeled root whose child subtrees are given by a region valuation \( m : \text{Rets} \rightarrow \mathbb{M}[\text{Configs}] \). The collection of sub-trees connected to the root of \( (t, m) \) by an \( r \)-edge. The initial region valuation \( m_\emptyset \) is defined by \( m_\emptyset (r) \equiv \emptyset \) for all \( r \in \text{Regs} \). The singleton region valuation \( (r \mapsto \{ c \}) \) maps \( r \) to \( \{ c \} \), and \( \{ r \} \in \text{Regs} \setminus \{ r \} \rightarrow \emptyset \), and the union \( m_1 \cup m_2 \) of region valuations is
defined by the multiset union of each valuation: \((m_1 \cup m_2) | r \) \(= m_1 | r \cup m_2 | r \) for all \( r \in \text{Regs} \). The projection \( m \mid r \) of a region valuation \( m \) to a region sequence \( r \) is defined by \( m \mid r \) = \( m | r' \) when \( r' \) occurs in \( m \), and \( m | r \) = \( \emptyset \) otherwise.

For expressions without program variables, we assume the existence of an evaluation function \( \text{Eval} \) such that \( \text{Eval}(\text{Vals}) \) is a valuation \( \ell \) is reachable in \( P \) from \( i \) when there exists an execution of \( P \) from some \( c_0 \) to \( c_f \), where \( c_0 \) is \( i \)-initial and \( c_f \) is \( \ell \)-final.

**Problem 1 (State-Reachability).** The state-reachability problem is to determine, given an initial condition \( i \) of a program \( P \) and a valuation \( \ell \), whether \( \ell \) is reachable in \( P \) from \( i \).

### 2.3 Sequential Semantics with Task-Passing

Since tasks only exchange values at creation and completion-time, the order in which concurrently-executing tasks make execution steps does not affect computed program values. In this section we leverage this fact and focus on a particular execution order in which at any moment only a single task is enabled. When the currently enabled task encounters an \text{await}/\text{await} statement, suspending execution to wait for a subordinate task \( t \), becomes the currently-enabled task; when \( t \) completes, control returns to its waiting parent. At any moment only the tasks along one path \( \rho \) in the configuration tree have ever been enabled, and all but the last task in \( \rho \) are waiting for their child in \( \rho \) to complete. We encode this execution order into an equivalent stack-based operational semantics, which essentially transforms recursively parallel programs into sequential programs with an unbounded auxiliary storage device used to store subordinate tasks. We interpret the \text{await} and \text{await} statements as procedure calls which compute the values returned by previously-posted tasks.

We define a \textit{frame} to be a configuration in the sense of the tree-based semantics of Section 2.2, i.e., a finite unordered tree of task-labeled vertices and region-labeled edges. (Here all non-root nodes in the tree are posted tasks that have yet to take a single step of execution.) In our stack-based semantics, a \textit{stack configuration} \( c \) is a sequence of frames, representing a procedure activation stack.

Figure 3 and Figure 4 define the sequential transition relation \( \text{vrpp} / P \) of recursively parallel programs as a set of operational steps on configurations. The inter-procedural transitions of Figure 3 which implicitly include a transition \( C([t_1, m_1]) \text{vrpp} / P \rightarrow C([t_2, m_1]) \) whenever \( t_1 \rightarrow t_0 \) to \( t_2 \). The \text{POST-T} rule creates a procedure frame to execute in parallel, and links it to the current frame by the given region, passing ownership of tasks in the specified region sequence to the newly-created frame. The \text{WAIT-T} rule consumes the result of a single child frame in the given region, and applies the return-value handler to update the parent frame’s local valuation. Similarly, the \text{WAIT-NEXT-T} and \text{WAIT-DONE-T} rules consume the results of every child frame in the given region, applying their return handlers in the order they are consumed. The semantics of \text{call} statements reduces to that of \text{POST} and \text{await}: supposing an unused region identifier \( r_{call} \), we translate each statement \text{call} \( 1 \colon p \in \ell \) into the sequence

\begin{align*}
\text{post } r_{call} & \leftarrow p \in \ell \in \text{dcall}; \\
\text{await } r_{call},
\end{align*}

where \( \text{dcall}(v) \)

The parallel execution of a program \( P \) from \( c_0 \) to \( c_f \) is a configuration sequence \( c_0; c_1; \ldots; c_j \) where \( c_0 \text{vrpp} / P c_{i+1} \) for \( 0 \leq i < j \). An initial condition \( t = (p_0, \ell_0) \) is a procedure \( p_0 \in \text{Procs} \) along with a value \( \ell_0 \in \text{Vals} \). A configuration \( \langle \ell_0, s, d, m_0 \rangle \) is called \( \langle \ell_0, s, d, m_0 \rangle \)-initial when \( s \) is the top-level statement of \( p_0 \). A configuration \( c_f \) is called \( \ell_f \)-final when there exists a context \( C \) such that \( c_f \in C([t, m]) \) and \( \ell(t) = \ell_f \). We say
This capability makes the state-reachability problem undecidable—

Definition 1

unbounded chains of pending tasks can be used to simulate an arbi-

to the most-recently created task. We can then show that such

tasks, it becomes possible to construct and manipulate unbounded

task-chains by keeping a handle to most-recently created task, after

Figures 2 and 5 implicitly include

Lemma 1. The parallel semantics and the sequential semantics

are indistinguishable w.r.t. state reachability, i.e., for all initial

conditions $i$ of a program $P$, the valuation $i$ is reachable in $P$ from

$i$ by a parallel execution if and only if $i$ is reachable in $P$ from $i$ by

a sequential execution.

2.4 Undecidability of State-Reachability with Task-Passing

Recursively parallel programs allow pending tasks to be passed bidi-

rectionally: both from completed tasks and to newly-created tasks.

This capability makes the state-reachability problem undecidable—
even for the very simple cases recursive programs with at least one
region, and for non-recursive programs with at least two regions.

Essentially, when pending tasks can be passed to newly-created

tasks, it becomes possible to construct and manipulate unbounded

task-chains by keeping a handle to most-recently created task, after

having passed the handle of the previously-most-recently created
task to the most-recently created task. We can then show that such

unbounded chains of pending tasks can be used to simulate an arbi-

tary unbounded and ordered storage device.

Definition 1 (Task passing). A program which contains a statement

$\text{post } r \leftarrow p e \vec{r} d$, such that $|\vec{r}| > 0$ is called task-passing.

The task-depth of a program $P$ is the maximum length of a

sequence $p_1 \ldots p_i$ of procedures in $P$ such that each $p_j$ contains a

statement $\text{post } r \leftarrow p_{i+j} e \vec{r} d$, for $0 < j < i$, and some $r \in \text{Regs}$,

$\in \text{Exprs}$, $\in \text{Regs}^*$, and $d \in \text{Rets}$. Programs with unbounded

task-depth are recursive, and are otherwise non-recursive.

Theorem 1. The state-reachability problem for $n$-region finite-

value task-passing parallel programs is undecidable for

(a) non-recursive programs with $n > 1$, and

(b) recursive programs with $n > 0$.

The proof of Theorem 1 is given by two separate reductions from the emptiness problem for Turing machines to “single-wait”
programs, i.e., those using $\text{await}$ statements but not $\text{await}$ statements. In essence, as each task-handle can point to an unbounded
chain of task-handles, we can construct an unbounded Turing ma-
tine tape by using one task-chain to store the contents of cells to
the left of the tape head, and another chain to store the contents
of cells to the right of the tape head. If only one region is granted
but recursion is allowed (i.e., as in (b)), we can still construct the

tape using the task-chain for the cells right of the tape head, while

using the (unbounded) procedure-stack to store the cells left of
the head. When only one region is granted and recursion is not allowed,

neither of these reductions work. Without recursion we can bound
the procedure stack, and then we can show that single-stack machine

suffices to encode the single unbounded chain of tasks.

3. Programs without Task-Passing

Due to the undecidability result of Theorem 1 and our desire to
compare the analysis complexities of parallel programming mod-
els, we consider, henceforth, unless otherwise specified, only non-
task-passing programs, simplifying program syntax by writing

post $r \leftarrow p e \vec{r} d$. When task-passing is not allowed, region valu-

ations need not store an entire configuration for each newly-posted

Task, since the posted task’s initial region valuation is empty. As

this represents a significant simplification on which our subsequent

analysis results rely, we redefine here a few key notions.

3.1 Sequential Semantics without Task-Passing

A region valuation is a (non-nested) mapping $m : \text{Regs} \rightarrow \mathbb{N} [\text{Tasks}]$ from regions to multiset of tasks, a frame $(t, m)$ is a task

$t \in \text{Tasks} \text{ paired with a region valuation } m$, and a configuration $c$

is a sequence of frames representing a procedure activation stack.

The transition relation $\rightarrow_{\text{seq}}$ of Figures 2 and 5 implicitly include a transition $(t_1, m) \rightarrow_{\text{seq}} (t_2, m)$ whenever $t_1 \rightarrow_{\text{seq}} t_2$. The definitions of sequential execution, initial, and reachable are nearly identical to their task-passing parallel and sequential counterparts. Since pending tasks need not store initial region-valuations in non-
task-passing programs, this simpler semantics is equivalent to the

previous stack-based semantics.

Lemma 2. For all initial conditions $i$ non-task-passing programs

$P$, the valuation $i$ is reachable in $P$ from $i$ by a sequential execution

local valuation. The definitions of sequential execution, initial, and

reachable are nearly identical to their parallel counterparts.

Lemma 1. The parallel semantics and the sequential semantics

are indistinguishable w.r.t. state reachability, i.e., for all initial

conditions $i$ of a program $P$, the valuation $i$ is reachable in $P$ from

$i$ by a parallel execution if and only if $i$ is reachable in $P$ from $i$ by

a sequential execution.
with task-passing if and only if \( \ell \) is reachable in \( P \) from \( \ell \) by a sequential execution without task-passing.

Even with this simplification, we do not presently know whether the state-reachability problem for (finite-value) recursively parallel programs is decidable in general. In the following sections, we identify several decidable, and in some cases tractable, restrictions to the program model which correspond to the concurrency mechanisms found in real-world parallel programming languages.

### 3.2 Recursive Vector Addition Systems with Zero-Test Edges

Fix \( k \in \mathbb{N} \). A recursive vector addition system (RVASS) \( A = (Q, \delta) \) of dimension \( k \) is a finite set \( Q \) of states, along with a finite set \( \delta = \delta_1 \cup \delta_2 \cup \delta_3 \) of transitions partitioned into additive transitions \( \delta_1 \subseteq Q \times \mathbb{N}^k \times \mathbb{N}^k \times Q \), recursive transitions \( \delta_2 \subseteq Q \times Q \times Q \times Q \), and zero-test transitions \( \delta_3 \subseteq \mathbb{N}^k \times Q \times Q \). We write

\[
\begin{align*}
q_1, q_2 \rightarrow q' & \quad \text{when } (q, q_1, q_2, q') \in \delta_1, \quad \\
q_1, q_2 \rightarrow q' & \quad \text{when } (q, q_1, q_2, q') \in \delta_2, \quad \\
q \rightarrow q' & \quad \text{when } (q, q') \in \delta_3.
\end{align*}
\]

A (non-recursive) vector addition system (with states) (VASS) is a recursive vector addition system \((Q, \delta)\) such that \( \delta \) contains only additive transitions.

An (RVASS) frame \( \langle q, \vec{n} \rangle \) is a state \( q \in Q \) along with a vector \( \vec{n} \in \mathbb{N}^k \), and an (RVASS) configuration \( c \in (Q \times \mathbb{N}^k)^+ \) is a non-empty sequence of frames representing a stack of non-recursive sub-computations. The transition relation \( \rightarrow_{\text{rvass}} \) for recursive vector addition systems is defined in Frames 3. The ADDITIVE rule updates the top frame \( \langle q, \vec{n} \rangle \) by subtracting the vector \( \vec{n}_1 \) from \( \vec{n} \), adding the vector \( \vec{n}_2 \) to the result, and updating the control state to \( q' \). The CALL rule pushes on the frame-stack a new frame \( \langle q_1, 0 \rangle \) from which the RETURN rule will eventually pop at some point when the control state is \( q_2 \); when this happens, the vector \( \vec{n}_1 \) of the popped frame is added to the vector \( \vec{n}_2 \) of the frame below. We describe an application of the CALL (resp., RETURN) rule as a call (resp., return) transition. Finally, the ZERO rule proceeds only when the top-most frame’s vector equals \( \vec{0} \).

An execution of a RVASS \( A \) (from \( c_0 \) to \( c_j \)) is a configuration sequence \( c_0, c_1, \ldots, c_j \) where \( c_i \rightarrow_{\text{rvass}} c_{i+1} \) for \( 0 \leq i < j \). A configuration \( \langle q, \vec{n} \rangle \) is called \( q_0\text{-initial} \) when \( q = q_0 \) and \( \vec{n} = \vec{0} \), and a configuration \( c_j \) is called \( q_j\text{-final} \) when there exists a configuration \( \vec{n} \in \mathbb{N}^k \) and \( q \in Q \) such that \( c_j = \langle q, \vec{n} \rangle \). We say a state \( q_j \) is reachable in \( A \) from \( q_0 \) when there exists an execution of \( A \) from some \( q_0\text{-initial} \) configuration \( c_0 \) to some \( q_j\text{-final} \) configuration \( c_j \). The state-reachability problem for recursive vector addition systems is to determine whether a given state \( q \) is reachable from some \( q_0 \).

Recently Demri et al. [8] have proved that state-reachability in branching vector addition systems (BVASS)—a very similar formal model to which RVASS reduces—is in \( 2\text{EXPTIME} \). This immediately gives us an upper-bound on computing state-reachability in RVASS without zero-test edges. Though state-reachability in non-recursive systems is \( \text{EXPSPACE}\)-complete [26, 29], for the moment, we do not know matching upper and lower bounds for RVASS.

**Lemma 3.** The state-reachability problem for recursive (resp., non-recursive) vector addition systems without zero-test edges is \( \text{EXPSPACE}\)-hard, and in \( 2\text{EXPTIME} \) (resp., \( \text{EXPSPACE} \)).

### 3.3 Encoding Recursively Parallel Programs as RVASSs

When the value set \( \text{Vals} \) of a given program \( P \) is taken to be finite, the set \( \text{Tasks} \) also becomes finite since there are finitely many statements and return-value handlers occurring in \( P \). As finite-domain multisets are equivalently encoded with a finite number of counters (i.e., one counter per element), we can encode each region valuation \( m \in \text{Regs} \rightarrow \mathbb{M}[\text{Tasks}] \) by a vector \( \vec{n} \in \mathbb{N}^k \) of counters, where \( k = |\text{Regs} \times \text{Tasks}| \). To clarify the correspondence, we fix an enumeration \( c_n : \text{Regs} \times \text{Tasks} \rightarrow \{1, \ldots, k\} \), and associate each region valuation \( m \) with a vector \( \vec{n} \) such that for all \( r \in \text{Regs} \) and \( t \in \text{Tasks} \), \( m(r)(t) = \vec{n}(c_n(r, t)) \). Let \( \vec{n}_i \) denote the unit vector of dimension \( i \), i.e., \( \vec{n}_i(t) = 1 \) and \( \vec{n}_i(j) = 0 \) for \( j \neq i \).

Given a finite-data recursively parallel program \( P \) without task-passing, we associate a corresponding recursive vector addition system \( A_P = (Q, \delta) \). We define \( Q \equiv \text{Tasks} \cup \text{Tasks}^* \), and define \( \delta \) formally in Figure 7. Intra-procedural transitions translate directly to additive transitions. The CALL statements are handled by recursive transitions between entry and exit points \( t_0 \) and \( t_j \) of the called procedure. The POST statements are handled by additive transitions that increment the counter corresponding to a region-task pair. The EWAIT statements are handled in two steps: first an additive transition decrements the counter corresponding to region-task pair \( (r, t_0) \), and then a recursive transition between entry and exit points \( t_0 \) and \( t_j \) of the corresponding procedure is made, applying the return-value handler of \( t_j \) upon the return. (Here we use an intermediate state \( T[\text{skip}] \), \( t_0, t_j \in Q \) to connect the two transitions, in order to differentiate the intermediate steps of other EWAIT transitions.)

The POST statements are handled similarly, except the EWAIT statement must be repeated again upon the return. Finally, a zero-test transition allows \( A_P \) to eventually step past each EWAIT statement. Notice that ignoring intermediate states \( \{t_1, t_2, t_3\} \subseteq Q \), the frames \( (\ell, \vec{n}) \) of \( A_P \) correspond directly to frames \( (\ell, m) \) of the given program \( P \), given the correspondence between vectors and region valuations. This correspondence between frames indeed extents to configurations, and ultimately to the state-reachability problems between \( A_P \) and \( P \).

**Lemma 4.** For all programs \( P \) without task-passing, procedures \( p_0 \in \text{Procs} \), and values \( \ell_0, \ell \in \text{Vals} \), \( \ell \) is reachable from \( \ell_0, p_0 \) in \( P \) if and only if there exist \( s \in \text{Stmts} \) and \( d_0 \in \text{Rets} \) such that \( (\ell, s, d) \) is reachable from \( (\ell_0, s_0, d_0) \) in \( A_P \).

Our analysis algorithms in the following sections use Lemma 4 to compute state-reachability of a program \( P \) without task-passing by computing state-reachability on the corresponding RVASS \( A_P \).
Figure 6. The transition relation for recursive vector addition systems. To simplify presentation, we assume that there is at most one recursive transition originating from each state, i.e., for all \( q \in Q \), \(|\delta_2 \cap (\{q\} \times Q^3)| \leq 1\). We denote by 0 the vector \( \langle 0, 0, \ldots, 0 \rangle \), and by \( \oplus \) and \( \ominus \) the usual vector addition and subtraction operators.

![Transition Relation](image)

Figure 7. The transitions of the RVASS \( A_P \) encoding the behavior of a finite-data recursively parallel program \( P \).

In general, our algorithms compute sets of region valuation vectors

\[
\text{sms}(t_0, t_f, P) \overset{\text{def}}{=} \{ \vec{n} : (t_0, 0) \xrightarrow{\text{rvvas}} (t_f, \vec{n}) \},
\]

summarizing the execution of a procedure between an entry point \( t_0 \) and exit point \( t_f \), where we write \( \rightarrow_{\text{rvvas}} \) * to denote zero or more applications of \( \rightarrow_{\text{rvvas}} \). Given an effective way to compute such a function, we could systematically replace inter-procedural program steps (i.e., of the \( \text{call} \), \( \text{await} \), and \( \text{wait} \) statements) with intra-procedural edges performing their net effect. Note however that even if the set of tasks is finite, the set \( \text{sms}(t_0, t_f, A_P) \) of summaries between \( t_0 \) and \( t_f \) need not be finite; the ability to compute this set is thus the key to our summarization-based algorithms in the following sections.

4. Single-Wait Programs

Definition 2 (Single wait). A single-wait program is a program which does not contain the \( \text{await} \) statement.

Single-wait programs can wait only for a single pending task at any program point. Many parallel programming constructs can be modeled as single-wait programs.

4.1 Parallel Programming with Futures

The future annotation of Multilisp [17] has become a widely adopted parallel programming construct, included, for example, in X10 [6] and in Leijen et al. [25]’s task parallel library. Flanagan and Fellesien [12] provide a principled description of its semantics. The future construct leverages the procedural program structure for parallelism, essentially adding a “lazy” procedure call which immediately returns control to the caller with a placeholder for a value that may not yet have been computed, along with an operation for ensuring that a given placeholder has been filled in with a computed value. Syntactically, futures add two statements,

\[
\text{future } x := p e \quad \text{touch } x,
\]

where \( x \) ranges over program variables, \( p \in \text{Procs} \), and \( e \in \text{Exprs} \). Though it is not necessarily present in the syntax of a source language with futures, we assume every use of a variable assigned by a future statement is explicitly preceded by a touch statement. Semantically, the future statement creates a new process in which to execute the given procedure, which proceeds to execute in parallel with the caller—and all other processes created in this way. The touch statement on a variable \( x \) blocks execution of the current procedure until the future procedure call which assigned to \( x \) completes, returning a value with which is copied into \( x \). Even though each procedure can only spawn a bounded number of parallel processes—i.e., one per program variable—there is in general no bound on the total number of parallelly-executing processes, since procedure calls—even parallel ones—are recursive.

Example 2. The Fibonacci function can be implemented as a parallel algorithm using futures as follows.

\[
\text{proc } \text{fib} \text{ (var } n : \text{ N) }
\]

\[
\begin{align*}
\text{var } x, y : \text{ N} \\
&\text{if } n < 2 \text{ then} \\
&\quad \text{return } 1 \\
&\text{else} \\
&\quad \text{future } x := \text{fib} (n-1); \\
&\quad \text{future } y := \text{fib} (n-2); \\
&\quad \text{touch } x; \\
&\quad \text{touch } y; \\
&\quad \text{return } x + y
\end{align*}
\]

As opposed to the usual (naïve) sequential implementation operating in time \( O(n^2) \), this parallel implementation runs in time \( O(n) \).

The semantics of futures is readily expressed with task-passing programs using the post and await statements. Assuming a region identifier \( r_x \) and return handler \( d_x \) for each program variable \( x \), we encode

\[
\begin{align*}
\text{future } x := p e & \quad \text{as post } r_x \leftarrow p e \not{x} d_x \\
\text{touch } x & \quad \text{as await } r_x
\end{align*}
\]

where \( d_x (v) \overset{\text{def}}{=} x := v \) simply assigns the return value \( v \) to the variable \( x \), and the vector \( \not{x} \) contains each \( r_y \) such that the variable \( y \) appears in \( e \).

4.2 Parallel Programming with Revisions

Burckhardt et al. [5]’s revisions model of concurrent programming proposes a mechanism analogous to (software) version control systems such as CVS and subversion, which promises to naturally and easily parallize sequential code in order to take advantage of multiple computing cores. There, each sequentially executing process is referred to as a revision. A revision can branch into two revisions; each continuing to execute in parallel on their own separate copies of data, or merge a previously-created revision, provided a programmer-defined merge function to mitigate the updates to data which each have performed. Syntactically, revisions add two statements,

\[
x := \text{rfork } s \quad \text{join } x,
\]
where \( x \) ranges over program variables, and \( s \in \text{Stmts} \). Semantically, the \text{rfork} statement creates a new process to execute the given statement, which proceeds to execute in parallel with the invoker—and all other processes created in this way. The assignment stores a \text{handle} to the newly-created revision in a \text{revision variable} \( x \). The \text{join} statement on a revision variable \( x \) blocks execution of the current revision until the revision whose handle is stored in \( x \) completes; at that point the current revision’s data is updated according to a programmer-supplied merge function \( m : \langle \text{Val} \times \text{Val} \times \text{Val} \rangle \rightarrow \text{Val} \): when \( v_0, v_1 \) are, resp., the initial and final data values of the merged revision, and \( v_2 \) is the current data value of the current revision, the current revisions data value is updated to \( m(v_0, v_1, v_2) \).

The semantics of revisions is readily expressed with task-passing programs using the \text{post} and \text{await} statements. Assuming a region identifier \( r \) for each program variable \( x \), and a programmer-supplied merge function \( m \), we encode

\[
x := \text{rfork} s \quad \text{as} \quad \text{post} \quad r_x \leftarrow p_s \ 1 \ \vec{r} \ d
\]

\[
\text{join} \quad x \quad \text{as} \quad \text{await} \quad r_x
\]

where \( p_s \) is a procedure declared as

\[
\text{proc} \quad p_s \ (\text{var} \ 1 : T) \\
\text{var} \quad l_0 := 1 \\
\text{var} \quad s; \\
\text{return} \quad (l_0, 1)
\]

and \( d((v_0, v_1)) \equiv 1 := m(v_0, l, v_1) \) updates the current local valuation based on the joined revision’s initial and final valuations \( v_0, v_1 \in \text{Val} \), and the joining revision’s current local valuation stored in \( l \). The vector \( \vec{r} \) contains each \( r_x \) for which the revision variable \( y \) is accessed in \( s \).

4.3 Programming with Asynchronous Procedures

Asynchronous programs \cite{14, 19, 34} are becoming widely-used to build reactive systems, such as device drivers, web servers, and graphical user interfaces, with low-latency requirements. Essentially, a program is made up of a collection of short-lived tasks running one-by-one and accessing a global store, which post other tasks to be run at some later time. Tasks are initially posted by an initial procedure, and may also be generated by external system events. An \text{event loop} repeatedly chooses a pending task from its collection to execute to completion, adding the tasks it posts back to the task collection. Syntactically, asynchronous programs add two statements,

\[
\text{async} \quad p \ e \quad \text{eventloop}
\]

such that \text{eventloop} is invoked only once as the last statement of the initial procedure. Semantically, the \text{async} statement initializes a procedure call and returns control immediately, without waiting for the call to return. The \text{eventloop} statement repeatedly dispatches pending—i.e., called but not yet returned—procedures, and executing them to completion; each procedure executes atomically making both synchronous calls, as well as an unbounded number of additional asynchronous procedure calls. The order in which procedure calls are dispatched is chosen non-deterministically.

We encode asynchronous programs as (non-deterministic) recursively parallel programs using the \text{post} and \text{await} statements. Assuming a single region identifier \( r_0 \), we encode

\[
\text{async} \quad p \ e \quad \text{as} \quad \text{post} \quad r_0 \leftarrow p \ e \ d
\]

\[
\text{eventloop} \quad \text{as} \quad \text{while} \quad \text{true} \quad \text{do} \quad \text{await} \quad r_0.
\]

Supposing \( p \) has top-level statement \( s \) accessing a shared global variable \( g \) (besides the procedure parameter \( l \)), we declare \( p’ \) as

\[
\text{proc} \quad p’ \ (\text{var} \ 1 : T) \\
\text{var} \quad g_0 := * s \\
\text{var} \quad g := g_0 s; \\
\text{return} \quad (g_0, g).
\]

Finally \( d((v_0, v_1)) \equiv 1 = v_0; 1 := v_1 \) models the atomic update \( p \) performs from an initial (guessed) shared global valuation \( v_0 \). Guessing allows us to simulate the communication of a shared global state \( g \), which is later ensured to have begun with \( v_0 \), which the previously-executed asynchronous task had written.

5. Single-Wait Analysis

The absence of \text{await} edges in a program \( P \) implies the absence of zero-test transitions in the corresponding recursive vector addition system \( \mathcal{A}_P \). To compute state-reachability in \( P \) via procedure summarization, we must summarize the recursive transitions of \( \mathcal{A}_P \) by additive transitions (in a non-recursive system) accounting for the left-over pending tasks returned by reach procedure. This is not trivial in general, since the space of possibly returned region valuations is infinite. In increasing difficulty, we isolate three special cases of single-wait programs, whose analysis problems are simpler than the general case. In the simplest “non-aliasing” case where the number of tasks stored in each region of a procedure frame is limited to one, the execution of \text{await} statements are deterministic. When the number of tasks stored in each region is not limited to one, non-determinism arises from the choice of which completed task to pick at each \text{await} statement (see the \text{await} rule of Figure 5). This added power makes the state-reachability problem at least as hard as state-reachability in vector addition systems—i.e., EXPSPACE-hard, though the precise complexity depends on the scope of pending tasks. After examining the PTIME-complete non-aliasing case, we examine two EXPSPACE-complete cases by restricting the scope of task handles, before moving to the general case.

5.1 Single-Wait Analysis without Aliasing

Many parallel programming languages consume only the computations of precisely-addressed tasks. In futures, for example, the \text{touch} \( x \) statement applies to the return value of a particular procedure—the last one whose future result was assigned to \( x \). Similarly, in revisions, the \text{join} \( x \) statement applies to the last revision whose handle was stored in \( x \). Indeed in the single-wait program semantics of each case, we are guaranteed that the corresponding region, \( r_x \), contains at most one task handle. Thus the non-determinism arising (from choosing between tasks in a given region) in the \text{await} rule of Figure 5 disappears. Though both futures and revisions allow task-passing, the following results apply to futures- and revisions-based programs which only pass pending tasks from child to parent.

Definition 3 (Non-aliasing). We say a region \( r \in \text{Regs} \) is \text{aliased} in a region valuation \( m : \text{Regs} \rightarrow \mathbb{M}[\text{Tasks}] \) when \( |m(r)| > 1 \).

We say \( r \) is \text{aliasing} in a program \( P \) if there exists a reachable configuration \( C[(t, m)] \) of \( P \) in which \( r \) is aliased in \( m \). A \text{non-aliasing program} is a program in which no region is aliasing.

Note that the set of non-aliasing region valuations is finite when the number of program values is. The non-aliasing restriction thus allows us immediately to reduce the state-reachability problem for single-wait programs to reachability in a recursive finite-data sequential program. To compute state-reachability we consider a sequence \( \mathcal{A}_0, \mathcal{A}_1, \ldots \) of finite-state systems iteratively under-approximating the recursive system \( \mathcal{A}_P \) given from a single-wait program \( P \). Initially, \( \mathcal{A}_0 \) has only the transitions of \( \mathcal{A}_P \) corresponding to intra-procedural and \text{post} transitions of \( P \). At each step \( i > 0 \), we add to \( \mathcal{A}_i \) an

\footnote{Actually \( \vec{r} \) must in general be chosen non-deterministically, as each revision handle may be joined either by the parent revision or its branch.}
additive edge summarizing an \( \text{ewait} \) transition

\[ T[\text{ewait} \, r] \xrightarrow{\vec{n}} T[s], \]

for some \( t_0, t_f \in \text{Tasks} \) such that \( j = \text{cn}(r, t_0), s \in \text{rvh}(t_f), \) and \( \vec{n} \) is reachable at \( t_f \) from \( t_0 \) in \( \mathcal{A}_{t_f} \), i.e., \( \vec{n} \in \text{sms}(t_0, t_f, \mathcal{A}_{t_f}). \) This \( \mathcal{A}_0, \mathcal{A}_1, \ldots \) sequence is guaranteed to reach a fixed-point \( \mathcal{A}_k \), since the set of non-aliasing region valuation systems, and thus the number of possibly added edges, is finite. Furthermore, as each \( \mathcal{A}_i \) is finite-state, only finite-state reachability queries are needed to determine the reachable states of \( \mathcal{A}_i \), which are precisely the same reachable states of \( \mathcal{A}_P \). Note that the number of region valuations grows exponentially in the number of regions.

**Theorem 2.** The state-reachability problem for non-aliasing single-wait finite-value programs is PTIME-complete for a fixed number of regions, and EXPSPACE-complete in the number of regions.

5.2 Local-Scope Single-Wait Analysis

**Definition 4** (Local scope). A local-scope program is a program in which tasks only return with empty region valuations; i.e., for all \( \text{Tasks} \) arising from a program \( P \), the ordering on vectors of integers is a well quasi-ordering (WQO), such that \( \vec{v} \) is less or equal than \( \vec{w} \).

To solve state-reachability in local-scope single-wait programs, we compute a sequence \( \mathcal{A}_0, \mathcal{A}_1, \ldots \) of non-recursive vector addition systems iteratively under-approximating the recursive system \( \mathcal{A}_P \), arising from a program \( P \). The initial system \( \mathcal{A}_0 \) has only the transitions of \( \mathcal{A}_P \) corresponding to intra-procedural and post transitions of \( P \). At each step \( i > 0 \), we add to \( \mathcal{A}_i \) an additive edge summarizing an \( \text{ewait} \) transition

\[ T[\text{ewait} \, r] \xrightarrow{\vec{n}, \vec{o}} T[s], \]

for some \( t_0, t_f \in \text{Tasks} \) such that \( j = \text{cn}(r, t_0), s \in \text{rvh}(t_f), \) and \( \vec{n} \in \text{sms}(t_0, t_f, \mathcal{A}_{t_f}). \) Since the number of possibly added edges is polynomial in \( P \), the \( \mathcal{A}_0, \mathcal{A}_1, \ldots \) sequence is guaranteed to reach in a polynomial number of steps a fixed-point \( \mathcal{A}_k \) whose reachable states are exactly those of \( \mathcal{A}_P \). The entire procedure is EXPSPACE-complete, since each procedure-summarization reachability query is equivalent to computing state-reachability in vector addition systems.

**Theorem 3.** The state-reachability problem for local-scope single-wait finite-value programs is EXPSPACE-complete.

5.3 Global-Scope Single-Wait Analysis

Another relatively simple case of interest is when pending tasks are allowed to leave the scope in which they are posted, but can only be consumed by a particular, statically declared, task in an enclosing scope. This is the case, for example, in asynchronous programs [14], although here we allow for slightly more generality, since tasks can be posted to multiple regions, and arbitrary control in the initial procedure frame is allowed.

**Definition 5** (Global scope). A global-scope program is a program in which the \( \text{ewait} \) (and \( \text{await} \)) statements are used only in the initial procedure frame.

Since each non-initial procedure \( p \) of a global-scope program cannot consume tasks, the set of tasks posted by \( p \) and recursively-called procedures along any execution from \( t_0 \) to \( t_f \) is a semi-linear set, described by the Parikh-image of a context-free language. Following Ganty and Majumdar [14]’s approach, for each \( t_0, t_f \in \text{Tasks} \) we construct a polynomial-sized vector addition system \( \mathcal{A}(t_0, t_f) \) characterizing this semi-linear set of tasks (recursively) posted between \( t_0 \) and \( t_f \). Then, we use each \( \mathcal{A}(t_0, t_f) \) as a component of a non-recursive vector addition system \( \mathcal{A}_P \) representing execution of the initial frame. In particular, \( \mathcal{A}_P \) contains transitions to and from the component \( \mathcal{A}(t_0, t_f) \) for each \( t_0, t_f \in \text{Tasks} \),

\[ T[\text{ewait} \, r] \xrightarrow{\vec{n}, \vec{o}} \langle q_0, T[\text{skip}] \rangle \quad \langle q_f, T[\text{skip}] \rangle \xrightarrow{00} T[s], \]

for all \( r \in \text{Regs} \) such that \( j = \text{cn}(r, t_0), s \in \text{rvh}(t_f), \) and \( q_0 \) and \( q_f \) are the initial and final states of \( \mathcal{A}(t_0, t_f). \) We assume each \( \mathcal{A}(t_0, t_f) \) has unique initial and final states, distinct from the states of other components \( \mathcal{A}(t_i', t_f') \). In order to transition to the correct state \( T[s] \) upon completion, \( \mathcal{A}(t_0, t_f) \) carries an auxiliary state-component \( T[\text{skip}] \). In this way, for each task \( t_i' \) posted to region \( r' \) in an execution between \( t_0 \) and \( t_f \), the component \( \mathcal{A}(t_0, t_f) \) does the incrementing of the \( \text{cn}(r', t') \)-component of the region-valuation vector. Since each of the polynomially-many components \( \mathcal{A}(t_0, t_f) \) are constructed in polynomial time [14], this method constructs \( \mathcal{A}_P \) in polynomial time. Thus state-reachability in \( P \) is computed by state-reachability in the non-recursive vector addition system \( \mathcal{A}_P \), in exponential space. The complexity is asymptotically optimal since global-scope single-wait programs are powerful enough to capture state-reachability in vector addition systems.

**Theorem 4.** The state-reachability problem for global-scope single-wait finite-value programs is EXPSPACE-complete.

5.4 The General Case of Single-Wait Analysis

In general, the state-reachability problem for finite-value single-wait programs is as hard as state-reachability in recursive vector addition systems without zero-test edges.

**Theorem 5.** The state-reachability problem for single-wait finite-value programs is EXPSPACE-hard, and in 2EXPTIME.
We must solve several state-reachability queries on a sequence of (in a given region) at any program point. Many parallel programming

Examples 3. The Fibonacci function can be implemented as a parallel algorithm using Cilk as follows.

As opposed to the usual (naive) sequential implementation operating in time $O(n^2)$, this parallel implementation runs in time $O(n)$.

The semantics of Cilk is ready expressed with recursively parallel programs using the post and await statements. Assuming a region identifier $r_0$, we encode

where $s$ ranges over program statements. Semantically, the async statement creates a new process to execute the given statement, which proceeds to execute in parallel with the invoker—and all other processes created in this way. The finish statement executes
the given statement $s$, then blocks execution until every process
created within $s$ has completed.

Example 4. The Fibonacci function can be implemented as a
parallel algorithm using asynchronous statements as follows.

```plaintext
proc fib (var n: N)
var x, y: N
if n < 2 then
  return 1
else
  finish
  async call x := fib(n-1);
  async call y := fib(n-2);
  return x + y
end
```

As opposed to the usual (naive) sequential implementation operating
in time $O(n^2)$, this parallel implementation runs in time $O(n)$.

Asynchronous statements are readily expressed with (non-
deterministic) recursively parallel programs using the post and
await statements. Let $N$ be the maximum depth of nested finish
statements. Assuming region identifiers $r_1, \ldots, r_N$, we encode

```plaintext
async s as post $r_i$ ← $p_s \ast d$
finish s as await $r_i$
```

where $i - 1$ is number of enclosing finish statements, and $p_s$ is a
procedure declared as

```plaintext
proc $p_s$ (var $l$: T)
var $l_0 := l$
$s$;
return ($l_0$, $l$)
```

and $d((v_0, v_1)) \equiv \{assume l = v_0; l := v_1 models the up-
date $p$ performs from an initial (guessed) local valuation $v_0$. Using
the same trick we have used to model asynchronous programs in Sec-
tion 6.3, we model the sequencing of asynchronous tasks by initially
guessing the value $v_0$ which the previously-executed asynchronous
tasks had written, and validating that value when the return-value
handler of a given task is finally run. Note that although X10 allows,
in general, asynchronous tasks to interleave their memory accesses,
our model captures only non-interfering tasks, by assuming either
data-parallelism (i.e., disjoint accesses to data), or by assuming tasks
are properly synchronized to ensure atomicity.

6.3 Structured Parallel Programming

So-called structured parallel constructs are becoming a standard
parallel programming feature, adopted, for instance, in X10 [6] and
in Leijen et al. [25]'s task parallel library. These constructs leverage
normally sequential control structures to express parallelism.
A typical syntactic instance of this is the parallel for-each loop:

```plaintext
foreach $x$ in $e$ do $s$
```

where $x$ ranges over program variables, $e$ over expressions,
and $s$ over statements. Semantically, the foreach statement creates a
collection of new processes in which to execute the given statement—
one for each valuation of the loop variable. After creating these
processes, the foreach statement then block execution, waiting for each
holding.

The semantics of the for-each loop is readily expressed with
recursively parallel programs using the post and await statements.
With a region identifier $r_0$, we encode foreach $x$ in $e$ do $s$ as

```plaintext
for $x$ in $e$ do post $r_0$ ← $p_s (x,*) d$;
await $r_0$
```

and given that both $x$ and $l$ are free variables in $s$, $p_s$ is a procedure declared as

```plaintext
proc $p_s$ (var $x$: T, $l$: T)
var $l_0 := l$
$s$;
return ($l_0$, $l$)
```

and $d((v_0, v_1)) \equiv \{assume l = v_0; l := v_1 models the up-
date $p$ performs from an initial (guessed) local valuation $v_0$.

7. Multi-Wait Analysis

The presence of await edges implies the presence of zero-test
transitions in the recursive vector addition system $A_P$ corresponding
to a multi-wait program $P$. As we have done for single-wait
programs, we first examine the easier sub-case of local-scoped
programs, which in the multi-wait setting corresponds concurrency
in the Cilk [31] language (modulo task interleaving), as well as
structured parallel programming constructs such as the foreach
parallel loop in X10 [6] and in Leijen et al. [25]'s task parallel library
(see Section 6.3). The asymptotic behavior of the asynchronous
statements (Section 6.2) in X10 [6] does not satisfy the local-
scope restriction, since async statements can include recursive
procedure calls which are nested without interpolating finish
statements. These computing state-reachability is equivalent to
determining whether a particular vector is reachable in a non-
recursive vector addition system—a decidable problem which is
known to be EXPSPACE-hard, but for which the only known
algorithms are non-primitive recursive. Since all multi-wait parallel
languages we have encountered use only a single-region, we restrict
our attention at present to single-region multi-wait programs.

7.1 Local-Scope Single-Region Multi-Wait Analysis

With the local-scoping restriction, executions of each procedure
$p \in$ Procs between entry point $t_0 \in$ Tasks and exit point $t_f \in$ Tasks
are completely summarized by a Boolean indicating whether
or not $t_f$ is reachable from $t_0$. However, as executions of $p$ may
encounter await statements, modeled by zero-test edges in the
recursive vector addition system $A_P$, computing this Boolean
requires determining the reachable program valuations between each
pair of consecutive “synchronization points” (i.e., occurrences of
the await statement), which in principle requires deciding whether
the vector 0 is reachable in a vector addition system describing
execution from the program point just after the first await statement
to the point just after the second; i.e., when $T_1[\text{await } r]$ and
$T_2[\text{await } r]$ are consecutively-occurring synchronization points,
we must determine whether $\{T_1[\text{skip}] \cdot 0\}$ can reach $\{T_2[\text{skip}] \cdot 0\}$.

A careful analysis of our reachability problem reveals it does not
have the EXPSPACE-hard complexity of determining vector-
reachability in general, due to the special structure of our reachability
query. We notice that between two synchronization points $t_1$ and $t_2$
of $p$, execution proceeds in two phases. In the first, post statements
made by $p$ only increment the vector valuations. In the second
phase, starting when the second await statement is encountered, the
await statement repeatedly consumes tasks, only decrementing the
vector valuations—the vector valuations can not be re-incremented
again because of the local-scoped restriction: each consumed task is
forbidden from returning addition tasks. Due to this special structure,
deciding reachability between $t_1$ and $t_2$ reduces to deciding if a
particular integer linear program $I(t_1, t_2)$ has a solution.

Since consuming tasks in the await-loop requires using the
summaries computed for other procedures, we consider a sequence
$A_0, A_1, \ldots$ of non-recursive vector addition systems iteratively under-
approximating the recursive system $A_P$. Initially $A_0$ has only
the transitions of $A_P$ corresponding to intra-procedural and post
transitions of $P$. At each step $i > 0$, we add to $A_i$ one of two edges
types. One type is an additive procedure-summary edge, used to
describe a single task-consumption step of an await transition,
\[ T[\text{await } r] \overset{\delta_f^0}{\longrightarrow} T[s; \text{ await } r], \]
for some \( t_0, t_f \in \text{Tasks} \) such that \( j = cn(r, t_0), s = rhv(t_f) \), and \( sms(t_0, t_f, A_{i-1}) \neq \emptyset \). The second possibility is an additive synchronization-point summary edge, summarizing an entire sequence of program transitions between two synchronization points,
\[ T_1[\text{skip}] \overset{00}{\longrightarrow} T_2[\text{skip}], \]
where \( T_1[\text{await } r], T_2[\text{await } r] \in \text{Tasks} \) are consecutive synchronization points occurring \( P \), and \( 0 \in sms(T_1[\text{skip}], T_2[\text{skip}], A_P) \).

The procedure-summary edges are computed using only finite-state reachability between program states, using the synchronization-point summary edges, while the synchronization-point summary edges are computed by reduction to integer linear programming. As the number of possible edges is bounded polynomially in the program size, the \( A_0A_i \) sequence is guaranteed to reach a fixed-point \( A_k \) in a polynomial number of steps, though each step may take nondeterministic-polynomial time, in the worst case, to compute solutions to integer linear programs. The reachable states of \( A_k \) are precisely the same reachable states of \( A_P \).

**Theorem 6.** The state-reachability problem for local-scope multi-wait single-region finite-value programs is NP-complete.

### 7.2 Single-Region Multi-Wait Analysis

Without the local-scoping restriction, each execution of each procedure \( p \in \text{Procs} \) between entry point \( t_0 \in \text{Tasks} \) and exit point \( t_f \in \text{Tasks} \) is summarized by the tasks posted between the last-encountered await statement, at a “synchronization point” \( t_s \in \text{Tasks} \) (note that \( t_s = t_0 \) if no await statements are encoun-
tered), and a return statement, at the exit point \( t_f \). Since \( P \) can make recursive procedure calls between \( t_s \) and \( t_f \), and each called procedure can again return pending tasks, the possible sets of pending tasks upon \( p \)'s return at \( t_f \) is described by the Parikh-image of a context-free language \( L(t_0, t_f) \). It turns out we can describe this image as the set of vectors computed by a polynomially-sized vector addition system \( A^k(t_0, t_f) \) without recursion and zero-test edges [14]. We use thus computations of \( A^k(t_0, t_f) \) to summarize the set of possible region-valuations reached in an execution from \( t_0 \) to \( t_f \). However, computing \( A^k(t_0, t_f) \) is not immediate, since between \( t_0 \) and the last-encountered synchronization point \( t_s \), execution of the given procedure \( p \) may encounter await statements (necessarily so when \( t_0 \neq t_s \)). Since we use zero-test edges to express await statements, we also need to summarize execution between synchronization points (i.e., between the procedure entry point and among await statements) using only additive edges. To further complicate matters, each such summarization requires, in turn, the summaries \( A_i^k(t_i', t_i') \) computed for other procedures!

We break the circular dependence between procedure summaries and synchronization-point summaries by iteratively computing both. In particular, we compute a sequence \( A^k_0, A^k_1, \ldots \) of procedure summary vector addition systems along with a sequence \( A_0, A_1, \ldots \) of vector addition systems such that each \( A^k_i \), for \( i > 0 \), is computed using the transitions of \( A_{i-1} \), and \( A_i \), for \( i \geq 0 \) is computed using the procedure summaries of \( A^k_i \). Initially, \( A^k_0 \) contains only the pending-task sets reachable without taking await transitions, and \( A_0 \) contains only the transitions of \( A_P \) corresponding to intra-procedural and post transitions of \( P \), along with transitions to components \( A^k_i \). For \( i > 0, A_i \) contains transitions to and from the components \( A^k_i(t_i, t_f) \)
\[ T[\text{await } r] \overset{\delta_f^0}{\longrightarrow} (q_0, T[\text{skip}]) \quad \langle q_f, T[\text{skip}] \rangle \overset{00}{\longrightarrow} T[s; \text{ await } r] \]
for each \( t_0, t_f \in \text{Tasks} \) such that \( j = cn(r, t_0), s = rhv(t_f) \), and \( q_0 \) and \( q_f \) are the unique initial and final states of \( A^k_i(t_i, t_f) \). (We assume each component \( A^k_i(t_0, t_f) \) has unique initial and final states, distinct from the states of other components. Additionally, we equip each \( A^k_i(t_0, t_f) \) with auxiliary state to carry the identity \( T[\text{skip}] \) of the invoking task to ensure the proper return of control when \( A^k_i(t_0, t_f) \) completes.) At each step \( i > 0 \), we add to \( A_i \) an additive edge summarizing the execution between two synchronization points \( T_1[\text{await } r] \) and \( T_2[\text{await } r] \) occurring in \( P \):
\[ T_1[\text{skip}] \overset{00}{\longrightarrow} T_2[\text{skip}], \]
such that \( T_2[\text{skip}] \) is reachable in \( A_{i-1} \) from \( T_1[\text{skip}] \), i.e., \( 0 \in sms(T_1[\text{skip}], T_2[\text{skip}], A_{i-1}) \). Note that when \( T[\text{await } r] \) is a synchronization point occurring in \( P \), \( T[\text{skip}] \) refers to the program point immediately after the await statement. Since there are only polynomially-many such edges that can possibly be added, we are guaranteed to reach a fixed-point \( A_k \) of \( A_0, A_1 \ldots \) in a polynomial number of steps. Furthermore, the reachable states of \( A_k \) are precisely the same reachable states of \( A_P \). However, computing \( 0 \in sms(t_1, t_2, A_{i-1}) \) at each step is difficult due to the zero-test edge in the await statement immediately preceding \( t_2 \); this is computationally equivalent to computing reachability of a particular vector in non-recursive vector addition systems.

**Theorem 7.** The state-reachability problem for multi-wait single-region finite-value programs is decidable.

Since practical algorithms to compute vector-reachability is a difficult open problem, we remark that it is possible to obtain algorithms to approximate our state-reachability problem. Consider, for instance, the over-approximate semantics given by transforming each await \( r \) statement into while + do await \( r \). Though many more behaviors are present in the resulting program, since not every task is necessarily consumed during the while loop, practical algorithmic solutions are more probable (see Section 5.4).

### 8. Related Work

Formal modeling and verification of multi-threaded programs has been heavily studied, including but not limited to identifying decidable sub-classes [20], and effective over-approximate [13] and under-approximate [9] analyses.

To our knowledge little work has been done in formal modeling and verification of programs written in explicitly-parallel languages which are free of thread interleaving. Sen and Viswanathan [13]'s asynchronous programs, which falls out as a special case of our single-wait programs, is perhaps most similar to our work in this regard. Practical verification algorithms by combining iterative over- and under-approximation [19], and in-depth complexity analysis [14] of asynchronous programs have been studied.

Though decidability results of abstract parallel models have been reported [4] [10] (Bouajjani and Espanza [8] survey this line of work), these works target abstract computation models, and do not identify precise complexities and optimal algorithms for real-world parallel programming languages, nor do they handle the case where procedures can return unbounded sets of unfinished computations to their callers.

### 9. Conclusion

We have proposed a general model of recursively parallel programs which captures the concurrency constructs in a variety of popular programming languages. By isolating the fragments corresponding to various language features, we are able to associate corresponding formal models, measure the complexity of state-reachability, and provide precise analysis algorithms. We hope our complexity measurements may be used to guide the design and choice of con-
We greatly appreciate formative discussions with Arnaud Sangnier References the anonymous POPL reviewers.

Acknowledgments

current programming languages and program analyses. Figure 8 summarizes our results.

Acknowledgments

We greatly appreciate formative discussions with Arnaud Sangnier and Peter Habermehl, and the feedback of Pierre Ganty, Giorgio Delzanno, Rupak Majumdar, Tom Ball, Sebastian Burckhardt, and the anonymous POPL reviewers.

References


Comparing current programming languages and program analyses. Figure 8 summarizes our results.

Acknowledgments

We greatly appreciate formative discussions with Arnaud Sangnier and Peter Habermehl, and the feedback of Pierre Ganty, Giorgio Delzanno, Rupak Majumdar, Tom Ball, Sebastian Burckhardt, and the anonymous POPL reviewers.

References


A. Proofs of Theorems

To begin with we introduce notation and simplifying assumptions in order to simplify the proof arguments in the following subsections.

Notation and Simplifying Assumptions

**Words & Languages** A \( \Sigma \)-word is a finite sequence \( w \in \Sigma^* \) of symbols from an alphabet \( \Sigma \); the symbol \( \epsilon \) denotes the empty word, and a language \( L \subseteq \Sigma^* \) is a set of words. The Parikh-image \( \Pi(w) \) of a word \( w \in \Sigma^* \) is the multiset \( m \in \mathbb{N}[\Sigma] \) (equivalently, the vector \( \vec{n} \in \mathbb{N}[\Sigma] \) such that for each \( a \in \Sigma \), \( m(a) = \#a \)). The number of occurrences of \( a \) in \( w \); the Parikh-image of a language \( L \subseteq \Sigma^* \) is the set of Parikh-images of each constituent word: \( \Pi(L) = \{ \Pi(w) : w \in L \} \). Two languages \( L_1 \) and \( L_2 \) are Parikh-equivalent whenever \( \Pi(L_1) = \Pi(L_2) \).

**Finite-State Automata** A finite-state automaton (FSA) \( A = (Q, \Sigma, \rightarrow) \) over an alphabet \( \Sigma \) is a finite set \( Q \) of states, along with a set \( \rightarrow \subseteq Q \times \Sigma \times Q \) of transitions. Given initial and accepting states \( q_0, q_f \in Q \), the language \( A(q_0, q_f) \) is the set of \( \Sigma \)-words labeling runs of \( A \) which begin in the initial state \( q_0 \) and terminate in the accepting state \( q_f \). The language-emptiness problem for finite-state automata is to decide, given an automaton \( A \) and states \( q_0, q_f \in Q \), whether \( A(q_0, q_f) = \emptyset \).

**Context-Free Grammars** A context-free grammar (CFG) \( \mathcal{G} = (V, \Sigma, S, \rightarrow) \) over an alphabet \( \Sigma \) is a finite set \( V \) of variables, along with a finite set \( \rightarrow \subseteq V \times (V \cup \Sigma)^* \) of productions. Given an initial variable \( S_0 \in V \), the language \( \mathcal{G}(S_0) \) is the set of \( \Sigma \)-words derived by \( \mathcal{G} \) from the initial variable \( S_0 \).

**Pushdown Automata** A pushdown automaton (PDA) \( A = (Q, \Sigma, \Gamma, \rightarrow) \) over an alphabet \( \Sigma \) is a finite set \( Q \) of states, along with a stack alphabet \( \Gamma \), and a finite set \( \rightarrow \subseteq Q \times \Sigma \times \Gamma^* \times Q \) of transitions. A configuration \( q \omega \) is a state \( q \in Q \) paired with a stack-symbol sequence \( \omega \). Given initial and accepting states \( q_0, q_f \in Q \), the language \( A(q_0, q_f) \) is the set of \( \Sigma \)-words labeling runs of \( A \) which begin in the initial configuration \( q_0 \epsilon \) and terminate in an accepting configuration \( q_f \omega \), for some \( \omega \in \Gamma^* \). The language-emptiness problem for pushdown automata is to decide, given an automaton \( A \) and states \( q_0, q_f \in Q \), whether \( A(q_0, q_f) = \emptyset \).

**Vector Addition Systems** A vector addition system (VAS) \( A = (Q, \rightarrow) \) of dimension \( \mathbb{N} \) is a finite set \( Q \) of states, along with a finite set \( \rightarrow \subseteq Q \times \mathbb{N}^k \times \mathbb{N}^k \times Q \) of transitions. A configuration \( q \vec{n} \) is a state \( q \in Q \) paired with a vector \( \vec{n} \in \mathbb{N}^k \). Given initial and accepting states \( q_0, q_f \in Q \), the language \( A(q_0, q_f) \) is the set of vectors \( N_f \subseteq \mathbb{N}^k \) such that \( A \) has a run which begins in \( q_0 \vec{0} \) and terminates in \( q_f \vec{n}_f \), for some \( \vec{n}_f \in N_f \). The state-reachability problem (resp., the configuration-reachability problem) for vector addition systems is to decide, given a system \( A \) and states \( q_0, q_f \in Q \) (resp., and a vector \( \vec{n}_f \in \mathbb{N}^k \)), whether \( A(q_0, q_f) \neq \emptyset \) (resp., whether \( \vec{n}_f \in A(q_0, q_f) \)).

**Turing Machines** A Turing machine (TM) \( A = (Q, \Sigma, \rightarrow) \) over an alphabet \( \Sigma \) is a finite set \( Q \) of states, along with a finite set \( \rightarrow \subseteq Q \times \Sigma \times \{L, R\} \times \Sigma \times Q \) of transitions. A configuration \( q \omega \) is a state \( q \in Q \) along with two words \( \omega, \omega' \in \Sigma^* \). Given initial and accepting states \( q_0, q_f \in Q \), the language \( A(q_0, q_f) \) is the set of \( \Sigma \)-words \( w \) such that \( A \) has a run which begins in an initial configuration \( q_0 \epsilon \omega \) and terminates in an accepting configuration \( q_f \omega' \), for some \( \omega, \omega' \in \Sigma^* \). The language-emptiness problem for Turing machines is to decide, given a machine \( A \) and states \( q_0, q_f \in Q \), whether \( A(q_0, q_f) = \emptyset \).

A.1 Proof of Theorem 1

**Theorem 1** The state-reachability problem for \( n \)-region finite-value task-passing parallel programs is undecidable for

(a) non-recursive programs with \( n > 1 \), and
(b) recursive programs with \( n > 0 \).

We prove (a) and (b) separately, both by reduction from the language emptiness problem for Turing machines.

**Proof (a).** By reduction from the language emptiness problem for Turing machines, let \( A = (Q, \Sigma, \rightarrow) \) be a Turing machine with \( \rightarrow = \{d_i \rightarrow d_j\} \), and let \( q_0, q_f \in Q \). We assume, without loss of generality, that upon entering the accepting state \( q_f \), \( A \) performs a sequence of left-moves until reaching the end of the tape; i.e., \( (q_f, a, L, a, q_f) \in \rightarrow \) for all \( a \in \Sigma \). We define a task-passing program \( P_A \) with two regions \( P_{L} \) and \( P_R \), and one return-value handler \( d \), along with an initial procedure given by

```plaintext
proc main ()
var state: Q
var sym: \Sigma
var done: \text{\texttt{B}} = \text{false}
while * do post rR \leftarrow p * d;
post rR \leftarrow p w(k) d;
post rR \leftarrow p w(k-1) d;
......
p post rR \leftarrow p w(2) d;
state := q_0;
sym := w(1);
while * do
if * then s_1
else if * then s_2
......
else if * then s_j
// check: is state = q_f reachable here?
done := true;
return
```

and an auxiliary non-recursive procedure \( p \) given by

```plaintext
proc p (var sym: \Sigma)
return sym
```

where each transition \( d_i \in \rightarrow \) gives rise to a corresponding statement \( s_i \) defined as follows. For right-moving transitions \( d_i = a/b, R \), we define \( s_i \) as
assume state = q;
assume sym = a;
post rl ← p b d;
state := q’;
await rr // overwrites sym

For left-moving transitions \( d_i = q \xrightarrow{a/b,L} q’ \), we define \( s_i \) as

\[
\begin{align*}
\text{assume state} & = q; \\
\text{assume sym} & = a; \\
\text{post} \; rl & ← p \; b \; d; \\
\text{state} & := q’; \\
\text{await} \; rr & // \text{overwrites sym}
\end{align*}
\]

where the return-value handler \( d(a) \triangleq \text{sym} := a \) assigns \( a \) to \( \text{sym} \).

By connecting the configurations of \( ⟨q, w_1, w_2⟩ \) of \( A \) to the chain of tasks in region \( r_L \)—corresponding to the cells of \( w_1 \)—and the chain of tasks in region \( r_R \)—corresponding to the cells of \( w_2 \)—it is routine to show that \( P_A \) faithfully simulates precisely the runs of \( A \). As we assume \( A \) moves to the left upon encountering the accepting state \( q_f \), we need only check reachability of a valuation \( q_f \) to state \( q \) at the end of the main procedure to know whether or not \( A \) has an accepting run.

**Proposition A.1.I.** \( A(q_0, q_f) \neq \emptyset \) if and only if state = \( q_f \) and done = true is reachable in \( P_A \).

Thus state-reachability in \( P_A \) solves language emptiness for \( A \). \( \square \)

Using only a single region, it will not be possible to create two independent, unbounded task chains. However, if the program is allowed to be recursive, we can leverage the unbounded procedure stack as an additional, independent, unbounded data structure.

**Proof (b).** By reduction from the language emptiness problem for Turing machines, let \( A = ⟨Q, \Sigma, \xrightarrow{→}⟩ \) be a Turing machine with \( \xrightarrow{→} = \{d_1, \ldots, d_j\} \), and let \( q_0, q_f ∈ Q \). We assume, without loss of generality, that upon entering the accepting state \( q_f \), \( A \) performs a sequence of left-moves until reaching the end of the tape; i.e., \( ⟨q_f, a, L, a, q_f⟩ ∈ \xrightarrow{→} \) for all \( a ∈ \Sigma \). We define a single-region task-passing program \( P_A \) with a single return-value handler \( d \), along with an initial procedure given by

```plaintext
proc main ()
var q_cur, q_R: Q
var sym_R: Γ
var done: B = false

while * do post r ← p * d;
post r ← p w(k) d;
post r ← p w(k-1) d;
...;
post r ← p w(1) d;
await r;
assume q_R = q_0;

// check: is q_cur = q_f reachable here?
done := true;
return
```

and an auxiliary recursive procedure \( p \) given by

```plaintext
proc p (var sym: Γ)
var q_cur, q_init, q_R: Q
var sym_R: Γ
q_init := *;
```

where each transition \( d_i ∈ δ \) gives rise to a corresponding statement \( s_i \) defined as follows. For the right-moving transitions \( d_i = a/b,r \), we define \( s_i \) as

\[
\begin{align*}
\text{assume q_cur} & = q; \\
\text{assume sym} & = a; \\
\text{sym} & := b; \\
\text{await} \; r; \\
// At this point q_R, q_cur, and sym_R \\
// have been overwritten by the initial- \\
// and current-state valuations, and the \\
// symbol stored in the right-neighbor \\
// who has just moved left. \\
\text{assume q_R} & = q’; \\
\text{post} \; r & ← p \; \text{sym}_R \; d
\end{align*}
\]

Our program thus simulates right moves by awaiting a pending task representing the right neighbor of the current task. For left-moving transitions \( d_i = a/b,L \), we define \( s_i \) as

\[
\begin{align*}
\text{assume q_cur} & = q; \\
\text{assume sym} & = a; \\
\text{sym} & := b;
\end{align*}
\]

Our program thus simulates left moves by returning to the awaiting task, who promptly recreates its right-neighbor by posting a new task to replace it.

By connecting the configurations of \( ⟨q, w_1, w_2⟩ \) of \( A \) to the chain of awaiting tasks—corresponding to the cells of \( w_1 \)—and the chain of posted tasks—corresponding to the cells of \( w_2 \)—it is routine to show that \( P_A \) faithfully simulates precisely the runs of \( A \). As we assume \( A \) moves to the left upon encountering the accepting state \( q_f \), we need only check reachability of a valuation \( q_f \) to \( q \) at the end of the main procedure to know whether or not \( A \) has an accepting run.

**Proposition A.1.II.** \( A(q_0, q_f) \neq \emptyset \) if and only if \( q \_cur = q_f \) and \( \text{done} = \text{true} \) is reachable in \( P_A \).

Thus state-reachability of \( P_A \) solves language emptiness for \( A \). \( \square \)

**Theorem A.1.1.** The state-reachability problem for single-region non-recursive finite-value task-passing parallel programs is PTIME-complete for fixed task-depth, and EXPTIME in the task-depth.

**Proof.** Let \( P \) be a non-aliasing single-wait finite-value single-region non-recursive task-passing parallel program with finite sets of procedures \( \text{Procs} \), values \( \text{Vals} \), regions \( \text{Regs} \), and return-value handlers \( \text{Rets} \), and let \( ℓ ∈ \text{Vals} \) be a target reachable value. Furthermore, we assume \( P \) is non-recursive, which implies there is a maximum task-depth \( N ∈ \mathbb{N} \)—i.e., \( N \) is the maximum length of a sequence \( p_0 p_1 \ldots \in \text{Procs}^* \) such that each \( p_i \) contains a post to \( p_{i+1} \). Without loss of generality, suppose \( ℓ \) is only reachable in procedure frames where the current statement is \( s_f \).

We construct a pushdown automaton \( A_P = ⟨Q, Σ, Γ, \xrightarrow{→}⟩ \) along with initial and accepting states \( q_0, q_f ∈ Q \). We define the states of \( A_P \) to be \( N \)-bounded sequences of tasks

\[
Q \equiv \text{Tasks}^{≤N}
\]
In this way a state \( t_0 t_1 \ldots t_i \in Q \) represents a computation of \( P \) in which each \( t_{j-1} (0 < j \leq i) \) is a task posted by \( t_j \). Note that this finite representation is only possible since we know the task-depth is bounded by \( N \). Given this state-representation, we define the transition relation \( \rightarrow \) of \( A_P \) as follows:

**Intra-task transitions** For each intra-task transition \( t_1 \rightarrow t_2 \) of Figure 2 we add the transition

\[
t_1 \cdot \vec{t} \rightarrow t_2 \cdot \vec{t}.
\]

**POST** For each statement \( \textit{post} \ r \leftarrow p e d \) occurring in \( P \), we add a transition which transfers control directly to procedure \( p \),

\[
T[\textit{post} \ r \leftarrow p e d] \rightarrow t \cdot T[\text{skip}],
\]

where \( t = (v, s_p, d) \), for each \( v \in e(T) \).

**\( \triangleright \text{wait} \)** For each statement \( \textit{wait} \ r \) occurring in \( P \), we add a transition which simply pops the pair \((v, d)\) from the top of the pushdown stack, and applies the return-value handler,

\[
T[\textit{wait} \ r] \cdot \vec{t} \stackrel{\text{pop}(v,d)}{\longrightarrow} T[s] \cdot \vec{t},
\]

where \( s \in d(v) \).

**\( \textit{return} \)** For each statement \( \textit{return} \ e \) occurring in \( P \), we add a transition which pushes the return value and return-value handler for the current task onto the pushdown stack, to be later consumed by a subsequent \( \textit{wait} \) statement,

\[
\ell, s[\textit{return} \ e], d) \cdot t_0 \cdot \vec{t} \rightarrow \ell \cdot \text{push}(v,d) \cdot t_0 \cdot \vec{t},
\]

where \( v \in e(\ell) \).

Finally, given an initial condition \( s = (p_0, \ell_0) \) and target value \( \ell_f \) of \( P \), we let \( q_0 = (\ell_0, s_{p_0}, d) \), and \( q_f = (\ell_f, s_f, d) \), for some \( d \in \text{Rets} \). (See above for the definition of \( \text{Rets} \).

**Proposition A.1.III.** \( A_P(q_0, q_f) \neq \emptyset \) if and only if \( \ell \) is reachable in \( P \) from \( \iota \).

As \( |Q| \) is \( O((1, |\text{Locs}| \cdot |\text{Rets}|)^N) \) and \( |\Gamma| \) is \( O(|\text{Vals}| \cdot |\text{Rets}|) \), the size of \( A_P \) is polynomial in \( P \). Since language emptiness is decidable in polynomial time for pushdown automata, our procedure gives a polynomial-time algorithm for state-reachability when \( N \) is fixed, though exponential in \( N \).

\begin{proof}

A.2 Proof of Theorem

**Theorem 2** The state-reachability problem for non-aliasing single-wait finite-value programs is PTIME-complete for a fixed number of regions, and EXPSPACE-complete in the number of regions.

Though our proof only handles local-scope programs, the extension to generally-scoped programs is possibly by allowing the values of the region-container variables \( \text{rg} \) below to be returned to waiting procedures.

**Proof.** Let \( P \) be a non-aliasing local-scope single-wait finite-value program with regions \( r_1, \ldots, r_n \). We define a sequential finite-value program \( P_0 \) by a code-to-code translation of \( P \). We extend each procedure declaration \( \text{proc} \ p \ (\text{var} \ 1: \ T) \ s \) with additional procedure-local variables \( \text{rg}, \text{rg}' \), and \( \text{rv} \).

\[
\text{proc} \ p \ (\text{var} \ 1: \ T)
\]

\[
\text{var} \ \text{rg}[1]: R := [\perp; \ldots; \perp]
\]

\[
\text{var} \ \text{rg}'[1]: R
\]

\[
\text{var} \ \text{rv}: T
\]

\[
s
\]

where \( R \) is a type containing \( \perp \), and values of the record type

\[
\{ \text{prc: Procs, arg: Vals, rh: Rets} \}.
\]

Note that \( R \) is a finite-type since \( \text{Procs}, \text{Vals}, \) and \( \text{Rets} \) are finite sets. We translate each statement \( \text{return} \ e \) into \( \text{return} \ (\text{rg}, e) \), each statement \( \text{post} \ r \leftarrow p e d \) into the assignment

\[
\text{rg}[1] := \{ \text{prc} = p, \text{arg} = e, \text{rh} = d \}
\]

and each statement \( \text{wait} \ r_i \) into the statement

\[
\text{assume} \ \text{rg}[1] \neq \perp;
\]

\[
\text{call} (\text{rg}', e) := \{ \text{rg}[1].\text{prc} = \text{rg}[1].\text{arg} \}; \ l := \text{rg}[1].\text{rh}; \ \text{rg}[1] := \perp;
\]

\[
\text{for} \ j := 1 \text{ to } n \text{ do}
\]

\[
\text{if} \ \text{rg}'[j] \neq \perp \text{ then} \ \text{rg}[j] := \text{rg}'[j]
\]

where we assume each \( d \in \text{Rets} \) is given by an expression in which \( e \) is a free variable. Note that for local-scope programs, the \( \text{rg}' \) array will always be equal to \( [\perp; \ldots; \perp] \) and can be safely omitted from the translation.

Since regions do not alias, it is not hard to show that the state-reachability problem for the resulting sequential program \( P_0 \) is equivalent to the state-reachability problem for \( P \). (Though technically we must check for reachability for a complete local valuation in \( P_0 \), including \( l, \text{rg}, \text{rg}' \), and \( e \), we may assume without loss of generality reachability to certain values, by adding

\[
\text{if} * \text{ then } \text{rg} := *; \ \text{rg}' := *; \ e := *;
\]

\[
\text{assume false}
\]

between every statement of \( P_0 \). Since the \( \text{assume false} \) statement cannot continue execution, this extra conditional statement has no effect on program behavior, besides making any valuation with \( l = \ell \) reachable, if there is some reachable valuation with \( l = \ell \).)

**Proposition A.2.1.** The value \( l \) is reachable in \( P \) from \( i \) if and only if \( l \) is reachable in \( P \) from \( i \).

The size of \( P_0 \) is polynomial in \( P \), while the number of variables in \( P_0 \) increases by \( n \). Thus our state-reachability problem is PTIME-complete for fixed \( n \) since the state-reachability for sequential programs is \( \emptyset \). When the number \( n \) of regions is not fixed, this state-reachability problem becomes EXPSPACE-complete, due to the logarithmic encoding of the program values into the \( n \) extra variables.

**A.3 Proof of Theorem**

**Theorem 3** The state-reachability problem for local-scope single-wait finite-value programs is EXPSPACE-complete.

We show an equivalence between the state-reachability problems of local-scope single-wait recursively parallel programs and vector addition systems (VASS)—i.e., we show the problems are polynomial-time reducible to each other. EXPSPACE-completeness follows since state-reachability in VASS is known to be EXPSPACE-complete.

**Lemma A.3.1**. The state-reachability problem for local-scope single-wait finite-value programs is polynomial-time reducible to the state-reachability problem for vector addition systems (VASS).

**Proof sketch.** To solve state-reachability in local-scope single-wait programs, we compute a sequence \( A_0, A_1, \ldots \) of non-recursive vector addition systems iteratively under-approximating the recursive system \( A \) arising from a program \( P \). The initial system \( A_0 \) has only the transitions of \( A \) corresponding to intra-procedural and \( \text{post} \) transitions of \( P \). At each step \( i > 0 \), we add to \( A_i \) an additive edge summarizing an \( \text{wait} \) transition

\[
T[\text{wait} \ r] \rightarrow T[r].
\]

...
for some \( t_0, t_f \in \text{Tasks} \) such that \( j = \text{cn}(r, t_0), s = \text{rvh}(t_f) \), and \( n \in \text{sms}(t_0, t_f, A_{n-1}) \); since \( P \) is local-scope, every such \( n \) must equal \( 0 \). Since the number of possibly added edges is polynomial in \( P \), the \( A_{n}A_{i} \) sequence is guaranteed to reach in a polynomial number of steps a fixed-point \( A_{\ell} \) whose reachable states are exactly those of \( A_{\ell} \). Thus by solving a polynomial-sized sequence of state-reachability queries in polynomial-sized VASSs, we compute state-reachability in local-scope single-wait programs.

Lemma A.3.11. The state-reachability problem for vector addition systems (VASS) is polynomial-time reducible to the state-reachability problem for local-scope single-wait finite-value programs.

Proof. Let \( k \in \mathbb{N} \), and let \( A = (Q, \rightarrow) \) be a \( k \)-dimension VASS, and let \( q_0, q_f \in Q \). We construct a single-wait program \( P_A \) with an initial condition \( \ell \) and target valuation \( \ell_f \) such that \( A(q_0, q_f) \neq \emptyset \) if and only if \( \ell_f \) is reachable in \( P_A \) from \( \ell \).

The program \( P_A \) contains only two procedures: an initial procedure \( \text{main} \) and a dummy procedure \( p \) which will be posted (resp., awaited) for each addition (resp., subtraction) performed in \( A \). Accordingly, the region-set \( \text{Regs} = \{r_1, \ldots, r_k\} \) of \( P_A \) contains a region \( r_i \) per vector component. The program’s local variable \( \ell \) is used to store the control-state of \( A \), and we set \( \text{Vals} = Q \).

Finally, let \( \text{Rets} = \{d_{\text{const}}\} \), where \( d_{\text{const}}(v) \equiv 1 \); i.e., \( d_{\text{const}} \) is the return-value handler which ignores the return value, keeping the local valuation intact.

We simulate the transitions of \( A \) by awaiting a task from each region \( r_i \) once per decrement to the \( i \)th vector component, and subsequently posting a task to each region \( r_i \) once per increment to the \( i \)th vector component. Thus for each transition \( d_j = q \rightarrow q' \), we define the statement \( s_j \) given by

\[
\begin{align*}
\text{assume} & \quad \ell = q \\
\text{ewait} & \quad r_1; \ldots; \text{ewait} r_1; \ldots; \text{ewait} r_k; \ldots; \text{ewait} r_k; \\
\text{post} & \quad r_1 \leftarrow p \times d_{\text{const}}; \ldots; \text{post} r_1 \leftarrow p \times d_{\text{const}}; \\
\text{post} & \quad r_k \leftarrow p \times d_{\text{const}}; \ldots; \text{post} r_k \leftarrow p \times d_{\text{const}};
\end{align*}
\]

Finally, the initial procedure is given by

\[
\begin{align*}
\text{proc} & \quad \text{main}() \\
\ell & \quad := q_0; \\
\text{while} & \quad * \text{ do} \\
& \quad \text{if} * \text{ then} s_1 \\
& \quad \text{else if} * \text{ then} s_2 \\
& \quad \ldots \\
& \quad \text{else if} * \text{ then} s_{|A|}.
\end{align*}
\]

Note the correspondence between configurations of \( A \) and \( P_A \). Each configuration \( \langle q, n, \ell \rangle \) of \( A \) maps directly to a configuration \( \langle \langle q, s, \text{Val} \rangle, m \rangle \) of \( P_A \), where \( s \) is the loop statement of the initial procedure, and \( |m(r_i)| = n_i \). Given this correspondence, it follows easily that the state \( q_f \) is reachable in \( A \) from \( q_0 \) if and only if the valuation \( \ell_f \) is reachable in \( P_A \) from \( \ell = (\ell_{\text{main}}, q_0) \). As there are \( O(|A|^2) \) statements in \( P_A \) per transition of \( A \), the size of \( P_A \) is \( O(|A|^3) \).

A.4 Proof of Theorem 4

Theorem 4. The state-reachability problem for global-scope single-wait finite-value programs is EXPSPACE-complete.

To proceed we show an equivalence between the state-reachability problems of global-scope single-wait recursively parallel programs and vector addition systems (VASS)—i.e., we show the problems are polynomial-time reducible to each other. EXPSPACE-completeness follows since state-reachability in VASS is known to be EXPSPACE-complete.

Lemma A.4.1. The state-reachability problem for global-scope single-wait finite-value programs is polynomial-time reducible to the state-reachability problem for vector addition systems (VASS).

Proof sketch. Since each non-initial procedure \( p \) of a global-scope program cannot consume tasks, the set of tasks posted by \( p \) and recursively-called procedures along any execution from \( t_0 \) to \( t_f \) is a semi-linear set, described by the Parikh-image of a context-free language. Following Ganty and Majumdar [13]’s approach, for each \( t_0, t_f \in \text{Tasks} \) we construct a polynomial-sized vector addition system \( A(t_0, t_f) \) characterizing this semi-linear set of tasks (recursively) posted between \( t_0 \) and \( t_f \).

Proposition A.4.1 ([13]). For every pair \( t_0, t_f \in \text{Tasks}, \text{region valuation} m, \) and \( p \in \text{Procs} \), there exists an execution of \( p \) from \( \langle t_0, m_0 \rangle \) to \( \langle t_f, m \rangle \) if and only if there exists \( n \in \mathbb{N}^k \) such that \( n \in A_P(t_0, t_f) \), and \( m \) and \( n \) represent the same Parikh-image.

We use each \( A(t_0, t_f) \) as a component of a non-recursive vector addition system \( A_P \) representing execution of the initial frame. In particular, \( A_P \) contains transitions to and from the component \( A(t_0, t_f) \) for each \( t_0, t_f \in \text{Tasks} \).

\[
T|\text{ewait} \quad r_1 \rightarrow \langle q_0, T[\text{skip}] \rangle \quad \langle q_f, T[\text{skip}] \rangle \rightarrow T[s],
\]

for all \( r \in \text{Regs} \) such that \( j = \text{cn}(r, t_0), s = \text{rvh}(t_f) \), and \( q_0 \) and \( q_f \) are the initial and final states of \( A(t_0, t_f) \). We assume each \( A(t_0, t_f) \) has unique initial and final states, distinct from the states of other components \( A(t_0', t_f') \). In order to transition to the correct state \( T[s] \) upon completion, \( A(t_0, t_f) \) carries an auxiliary state-component \( T[\text{skip}] \). In this way, for each task \( t \) posted to region \( r \), an execution between \( t_0 \) and \( t_f \), the component \( A(t_0, t_f) \) does the incrementing of the \( \text{cn}(r', t') \)-component of the region-valuation vector. As each of the polynomially-many components \( A(t_0, t_f) \) are constructed in polynomial time [13], this method constructs \( A_P \), in polynomial time, reducing state-reachability in \( P \) to state-reachability in the VASS \( A_P \).

Lemma A.4.11. The state-reachability problem for vector addition systems (VASS) is polynomial-time reducible to the state-reachability problem for global-scope single-wait finite-value programs.

Proof. As the program \( P_A \) constructed in Lemma A.3.11 from a given VASS \( A \) only uses the \text{ewait} statement in the initial procedure, \( P_A \) is also a global-scope program.

A.5 Proof of Theorem 5

Theorem 5. The state-reachability problem for single-wait finite-value programs is EXPSPACE-hard, and in 2EXPSPACE.

To proceed we show an equivalence between the state-reachability problems of single-wait recursively parallel programs and recursive vector addition systems without zero-test edges—i.e., we show the problems are polynomial-time reducible to each other. EXPSPACE-hardness follows from that of non-recursive vector addition systems, and membership in 2EXPSPACE follows from Demri et al. [8]’s result on branching vector addition systems (BVAS).
We simulate the additive transitions by awaiting a task from each value handler which ignores the return value, keeping the local valuation intact.

\[ \delta = \delta_1 \cup \delta_2 \]

Note the correspondence between configurations of \( A \) and \( P_A \). Each frame \( \langle q, \vec{n} \rangle \) of \( A \) maps directly to a frame \( \langle q, s, \delta_{\text{const}} \rangle, m \) of \( P_A \), where \( s \) is the top-level statement of some procedure \( p_q \), and \( |m(r_i)| = \vec{n}(i) \) for all \( i \in \{1, \ldots, k\} \); this correspondence extends directly to the configurations of \( A \) and \( P_A \). It follows that the state \( q_f \) is reachable in \( A \) and only if the valuation \( q_f \) is reachable in \( P_A \). As there are \( O(|Q|) \) statements in \( P_A \) per transition of \( A \), the size of \( P_A \) is \( O(|A|^2) \), \( P_A \).

### A.6 Proof of Theorem 6

#### Theorem 6

The state-reachability problem for local-scope multi-wait single-region finite-value programs is NP-complete.

We show NP-hardness in Lemma A.6.1 by a reduction from circuit satisfiability [27], and membership in NP in Lemma A.6.2 by a procedure which solves a polynomial number of polynomial-sized integer linear programs.

#### A.6.1. The circuit satisfiability problem [27]

The circuit satisfiability problem is polynomial-time reducible to the state-reachability problem for local-scope multi-wait single-region finite-value programs.

Proof. Let \( C \) be a Boolean circuit with wires \( W \), gates \( G \), inputs \( I \), and an output wire \( w_0 \in W \). Without loss of generality, assume that each gate \( g \in G \) is connected to exactly two input wires and two output wires, and that each input \( h \in I \) is connected to exactly two wires. The circuit satisfiability problem asks if there exists a valuation to the inputs \( I \) which makes the value of wire \( w_0 \) true.

We construct a multi-wait single-region finite-value program \( P_C \) as follows. Let \( Wire \) be the type defined as

\[
\text{type Wire} = \{ \text{id: } \mathbb{B}, \text{active: } \mathbb{B}, \text{val: } \mathbb{B} \}
\]

and define a procedure for writing a value to a wire,

\[
\text{proc set (var id: W, val: B) }
\]

\[
\text{var fst, snd: Wire}
\]

\[
\text{if * then}
\]

\[
\text{fst.id := id;}
\]

\[
\text{fst.val := val;}
\]

\[
\text{fst.active := true;}
\]

\[
\text{else}
\]

\[
\text{snd.id := id;}
\]

\[
\text{snd.val := val;}
\]

\[
\text{snd.active := true;}
\]

\[
\text{return (fst, snd)}
\]

which takes a value to be written and returns two output wires (one of which is written to), and a procedure for reading the value of a wire,

\[
\text{proc get (var id: W, fst, snd: Wire) }
\]

\[
\text{var val: B}
\]

\[
\text{if * then}
\]

\[
\text{assume fst.active and fst.id = id;}
\]

\[
\text{val := fst.val;}
\]

\[
\text{fst.active := false;}
\]

\[
\text{else}
\]

\[
\text{assume snd.active and snd.id = id;}
\]

\[
\text{val := snd.val;}
\]

\[
\text{snd.active := false;}
\]

\[
\text{return (val, fst, snd)}.
\]

which takes two wires \( fst \) and \( snd \), reads a value from one of them, and returns the same (but mutated) wires, along with the value read. For each gate \( g \in G \) connected to input wires \( w_1, w_2 \), output wires \( w_3, w_4 \), and computing a function \( f : \mathbb{B} \rightarrow \mathbb{B} \), we declare a procedure.
We can block executions by allowing return handlers to be partial functions.

Finally, the initial procedure posts two instances of set per input $h \in I$, and two instances of set per gate $g \in G$, along with one instance of $p_g$, then waits until every task is consumed in some sequence.

**Lemma A.6.II.** The state-reachability problem for local-scope multi-wait single-region finite-value programs $P$ over values $\mathcal{V}$s and return-value handlers $\mathcal{R}$s is reducible to solving a $O(|P|^3 \cdot |\mathcal{V}|^3 \cdot |\mathcal{R}|)$-length series of integer linear programs, each of size $O(|P|^5 \cdot |\mathcal{V}|^5 \cdot |\mathcal{R}|)$.

**Proof.** Let $P$ be a program with finite sets of procedures $\mathcal{P}$, values $\mathcal{V}$, and return-value handlers $\mathcal{R}$, and let $f \in \mathcal{V}$ be a target reachable value from an initial condition $i = (p_0, e_0)$. We construct two sequences $A_1$, $A_2$,... and $A_1$, $A_2$,... of finite-state automata. Intuitively, each $A_i$ will be a sync-point summary automaton, characterizing pairs of program states reachable between two consecutive await statements; each $A_i$ will be a task-summary automaton, characterizing pairs of program states reachable between the entry and the exit of each task’s procedure.

Let $Q \triangleq \mathcal{P}$. We model task-posting by labeling the transitions of the automata by tasks, and define the alphabet $\Sigma \triangleq \text{Tasks} \cup \{\varepsilon\}$. The initial task-summary automaton is $A_0 = \langle Q, \{\varepsilon\}, \emptyset \rangle$ with states $Q$, alphabet $\{\varepsilon\}$, and the empty set $\emptyset$ of transitions.

**Construction of $A_i$.** For $i > 0$, we define the $i$th sync-point summary automaton, characterizing state-reachability between sync-point pairs, as $A_i = \langle Q \cup \bar{Q}, \Sigma, \delta_i \rangle$, where the states $Q$ and $\bar{Q} \triangleq \{q : q \in Q\}$ correspond, resp., to control locations of the first (task-posting) and second (task-consuming) phases, and the transitions $\delta_i = \delta^+ \cup \delta^- \cup \delta^\varepsilon$ are partitioned into first-phase transitions $\delta^+ \subseteq Q \times \Sigma \times Q$, phase-change transitions $\delta^- = \{(q, e, \bar{q}) : q \in Q\}$, and second-phase transitions $\delta^\varepsilon \subseteq \bar{Q} \times \Sigma \times \bar{Q}$.

The relation $\delta^+ \subseteq Q \times \Sigma \times Q$ is given directly by the sequential and task-posting transitions of the input program. The relation $\delta^- \subseteq \bar{Q} \times \Sigma \times \bar{Q}$ contains a transition $[T[\text{await} r], t_0, T[\text{await} r]]$ summarizing the computation of the task $t_0$ if and only if there exists $t_f \in \text{Tasks}$ such that $A_{i-1}[t_0, t_f]$ is non-empty, and $s \in \text{rvh}(t_f)$. In other words, $(q, t, \bar{q})$ summarizes the effect of consuming task $t$, based on $A_{i-1}$’s summarization of $t$, including the local-variable update due to its return-value handler. In this way, the possible behaviors between sync-points are computed using the thus-far computed (entire) behaviors of each posted task.

Note that not every word of $A_i(q_0, \bar{q}_f)$ represents a valid computation between two consecutive sync points $q_0$ and $q_f$, since $A_i$ cannot ensure that each task posted in the first phase is consumed in the second. For $q_0, q_f \in Q$, we say a word $w_1w_2 \in A_i(q_0, \bar{q}_f)$ is balanced if and only if $\Pi(w_1) = \Pi(w_2)$ and there exists $q \in Q$ such that $w_1 \in A_i(q_0, q)$ and $w_2 \in A_i(q, q_f)$. We say $A_i(q_0, \bar{q}_f)$ has a balanced run if some word of $A_i(q_0, \bar{q}_f)$ is balanced. For each sync-point pair $(q_0, q_f)$, we can decide whether $A_i(q_0, q_f)$ has a balanced run by integer linear programming. In particular, given $A_i$ and $(q_0, q_f)$, we construct a integer linear program $\Phi_i(q_0, \bar{q}_f)$ which has a positive integer solution exactly when $A_i(q_0, q_f)$ has a balanced run.

**Construction of $\Phi_i$.** Given the sync-point summary automaton $A_i$ and sync-point pair $q_0, q_f \in Q$, we construct an ILP, denoted $\Phi_i(q_0, q_f)$. Fix (finite) enumerations $q_0, q_1, \ldots, q_n$ of the states, symbols, and transitions, resp., of $A_i$; i.e., $Q = \{q_1, q_2, \ldots, \Sigma = \{a_1, a_2, \ldots, \delta = \{d_1, d_2, \ldots, \}$. Additionally, assume that $d_1 = (q_1, e, \bar{q}) \in \delta^\varepsilon$ for each $q_1 \in Q$.

We define $\Phi_i(q_0, q_f)$ as an integer linear program with $|\delta|$ transition occurrence variables, one $d_j$ for each transition $d_j \in \delta^\varepsilon$, and

---

4 We can block executions by allowing return handlers to be partial functions.
For $d$ would set the variables $arbitrary tasks. As the set of possible added transitions is bounded
exists a fixed-point $A$.

Construction of $A$. A synchronization point
ensures each state in the first phase is exited once per entry (except $q_0$, which is exited one extra time); for each $q_k \in Q$,

$$
\left( d_k + \sum_{d_j \in \delta^+(q_k, \ldots)} d_j - \sum_{d_j \in \delta^+(\ldots q_k)} d_j \right) = \begin{cases} 0 & \text{when } q_k \neq q_0 \\ 1 & \text{when } q_k = q_0 
\end{cases}
$$

ensures each state in the second phase is exited once per entry (except $q_f$, which is entered one extra time);

$$
\left( \sum_{d_j \in \delta^'} d_j \right) = 1
$$
esures a single inter-phase transition is taken; and for each $a_k \in \Sigma$,

$$
\left( \sum_{d_j \in \delta^+(\ldots a_k)} d_j \right) = a_k = \left( \sum_{d_j \in \delta^+(\ldots a_k)} d_j \right)
$$
eures that the number of occurrences of each $a_k$ in the first phase is equal to the number of occurrence in the second phase. (Note that the $a_i$ variables are not strictly necessary; they are added only for clarity.) Supposing $d_1, d_2, \ldots$, is a connected sequence of transitions through $A^i$, a corresponding solution to the given set of constraints would set the variables $d_1, d_2, \ldots$ to positive (non-zero) values corresponding to the number of times each transition is taken in $A^i$. However, supposing there are loops in $A^i$ which are not connected to any of the selected transitions, the given constraints do not prohibit solutions which take each transition of these loops an arbitrary number of times. This is a standard issue with encoding automaton traces which can be addressed by adding a polynomial number of constraints to $\Phi_i(q_0, q_f)$.

**Proposition A.6.I.** $A^i(q_0, q_f)$ has a balanced run if and only if $\Phi_i(q_0, q_f)$ has a positive integer solution.

Note that $|\Phi_i|$ is bounded by $O(|P|^3 \cdot |\text{Vals}|^3 \cdot |\text{Rets}|)$, since each of $O(|Q|^2)$ many programs $|\Phi_i(q, q')|$ contains $O(|\delta_i|) = O(|Q|^2)$ $|\Sigma|$ variables and $O(|Q + |\Sigma|)$ constraints, where $O(|Q|) = O(|P| \cdot |\text{Vals}|)$ and $O(|\Sigma|) = O(|P| \cdot |\text{Vals}| \cdot |\text{Rets}|)$.

**Construction of $A^i$.** For $i > 0$ we define the $i^{th}$ task-summary automaton, characterizing state-reachability among synchronization points, as

$$
A^i = (Q, \{e\}, \delta^i)
$$
such that $(q, e, q') \in \delta^i$ if and only if $(q, q')$ is a sync-point pair, and $A^i(q, q')$ has a balanced run.

Note that there are only finitely-many transitions which can be added over the entire $A^0$ and $A^i$ sequence. It follows that there exists a fixed-point $m \in \mathbb{N}$ of this sequence, and it is not hard to see that $A^m$ and $A^o$ capture every behavior of the input program $P$.

**Proposition A.6.II.** A synchronization point $q_f$ of the initial task is reachable from an initial control location $q_0$ if and only if $A^i(q_0, q_f)$ is non-empty.

Though we consider here only state-reachability to a synchronization point contained in the initial task for simplicity, Proposition A.6.II can indeed be extended to arbitrary control locations of arbitrary tasks. As the set of possible added transitions is bounded by $O(|Q|^2 \cdot |\Sigma|) = O(|P|^3 \cdot |\text{Vals}|^3 \cdot |\text{Rets}|)$, our procedure is guaranteed to terminate in polynomial-time. $\square$

**A.7 Proof of Theorem**

**Theorem.** The state-reachability problem for multi-wait finite-value programs is polynomial-time equivalent to the configuration-reachability problem for vector addition systems.

We demonstrate this equivalence by a polynomial-time reduction in each direction. Though VASS configuration-reachability has been shown decidable [29], only non-primitive recursive algorithms are known; VASS state-reachability gives an EXPTIME upper-bound.

**Lemma A.7.1.** The state-reachability problem for multi-wait finite-value programs is reducible to the configuration-reachability problem for vector addition systems.

**Proof sketch.** Without the local-scoping restriction, each execution of each procedure $p \in \text{Proc}$ between entry point $t_0 \in \text{Tasks}$ and exit point $t_f \in \text{Tasks}$ is summarized by the tasks posted between the last-encountered await statement, at a “synchronization point” $t_s \in \text{Tasks}$ (note that $t_s \neq t_f$ if no await statements are encountered), and a return statement, at the exit point $t_f$. Since $p$ can make recursive procedure calls between $t_s$ and $t_f$, and each called procedure can again return pending tasks, the possible sets of pending tasks upon $p$’s return at $t_f$ is described by the Parikh-image of a context-free language $L(t_0, t_f)$. It turns out we can describe this image as the set of vectors computed by a polynomially-sized vector addition system $A^i(t_0, t_f)$ without recursion and zero-test edges [4]. We use thus computations of $A^i(t_0, t_f)$ to summarize the set of possible region-valuations reached in an execution from $t_0$ to $t_f$. However, computing $A^i(t_0, t_f)$ is not immediate, since between $t_0$ and the last-encountered synchronization point $t_s$, execution of the given procedure $p$ may encounter await statements (necessarily so when $t_0 \neq t_f$). Since we use zero-test edges to express await statements, we also need to summarize execution between synchronization points (i.e., between the procedure entry point and among await statements) using only additive edges. To further complicate matters, each such summarization requires, in turn, the summaries $A^i(t_0, t_f)$ computed for other procedures!

We break the circular dependence between procedure summaries and synchronization-point summaries by iteratively computing both. In particular, we compute a sequence $A^0, A^1, \ldots$, of procedure summary vector addition systems along with a sequence $A_0, A_1, \ldots$ of vector addition systems such that each $A_i$, for $i > 0$, is computed using the transitions of $A_{i-1}$, and $A_i$ returns $0$ is computed using the procedure summaries of $A_{i-1}$. Initially $A_0$ contains only the pending-task sets reachable without taking await transitions, and $A_i$ contains only the transitions of $A_{i-1}$ corresponding to intra-procedural and post transitions of $P$, along with transitions to components $A_{i-1}$. For $i > 0$, $A_i$ contains transitions to and from the components $A_{i-1}^i(t_0, t_f)$ with auxiliary state to carry the identity $T[\text{skip}]$ of the invoking task to ensure the proper return of control when $A_{i-1}^i(t_0, t_f)$ completes.

At each step $i > 0$, we add to $A_i$ an additive edge summarizing the execution between two synchronization points $T_1[\text{await}]$ and $T_2[\text{await}]$ occurring in $P$:

$$
T_1[\text{skip}] \xrightarrow{0} T_2[\text{skip}]
$$
such that $T_2[\text{skip}]$ is reachable in $A_{i-1}$ from $T_i[\text{skip}]$, i.e., $0 \in \text{sms}(T_i[\text{skip}], T_2[\text{skip}], A_{i-1})$. Note that when $T[\text{await } r]$ is a synchronization point occurring in $P$, $T[\text{skip}]$ refers to the program point immediately after the await statement. Since there are only polynomially-many such edges that can possibly be added, we are guaranteed to reach a fixed-point $A_{\infty}$ of $A_0, A_1, \ldots$ in a polynomial number of steps. Furthermore, the reachable states of $A_{\infty}$ are precisely the same reachable states of $A_\infty$. However, computing $0 \in \text{sms}(t_1, t_2, A_{i-1})$ at each step is difficult due to the zero-test edge in the await statement immediately preceding $t_2$; this is computationally equivalent to computing configuration reachability in non-recursive vector addition systems. 

**Lemma A.7.11.** The configuration-reachability problem for vector addition systems is reducible to the state-reachability problem for multi-wait finite-value programs.

**Proof.** Let $A = \langle Q, \rightarrow \rangle$ be a $k$-dimension vector addition system with $\rightarrow = \{d_1, \ldots, d_n\}$, and let $q_0, q_f \in Q$. Instead of checking reachability of a vector $\vec{n}_i$ from $0$ in $A$, we will instead solve an equally-hard problem of checking whether $0$ is reachable from an initial vector $\vec{n}_0$. To do this we construct a multi-wait program $P_A$ and a local valuation $\ell$ which is reachable in $P_A$ if and only if the configuration $q0$ is reachable from $q_0\ell_0$ in $A$.

We will construct $P_A$ such that the number of pending tasks in a configuration is equal to the sum of vector components in a corresponding configuration of $A$. We then simulate each step of $A$, which subtracts $\vec{n}_1 \in \mathbb{N}^k$ and adds $\vec{n}_2 \in \mathbb{N}^k$, by consuming $\sum \vec{n}_1(i)$ tasks and posting $\sum \vec{n}_2(i)$ tasks, while ensuring each task consumed (resp., posted) corresponds to a subtraction (resp., addition) to the correct vector-component.

For each transition $d_i = \langle q, \vec{n}_1, \vec{n}_2, q \rangle$ we define the sequence $\sigma_i \in [1, k]^* \cup \sigma_i \in [1, k]^*$ of counter decrements as

$$\sigma_i = \begin{cases} 11 \ldots 11 22 \ldots 22 \ldots k \ldots k & \text{if } \vec{n}_1 = \vec{n}_2 \\
1 \ldots 1 & \text{otherwise} 
\end{cases}$$

We assume, without loss of generality, that each transition has a non-zero decrement vector, i.e., $\vec{n}_1 \neq 0$ and thus $|\sigma_i| > 0$. We will use return-value handlers to ensure that a $|\sigma_i|$-length sequence of consecutively-consumed tasks corresponds to the decrement of transition $d_i$. For each $j \in \{1, \ldots, |\sigma_i|\}$, let $d_{i,j}(v)$ be the return-value handler defined by

- assume $\text{cur\_tx} = i$;
- assume $\text{cur\_pos} = j$;
- if $\text{cur\_pos} = |\sigma_i|$ then
  - assume $v = \text{true}$;
  - $\text{cur\_tx} := i$;
  - $\text{cur\_pos} := 1$;
- else
  - assume $v = \text{false}$;
  - $\text{cur\_pos} := \text{cur\_pos} + 1$,

which checks that consuming a given task corresponds to a decrement (by one) of the $\sigma_i(j)$th component of the decrement vector of $d_i \in \delta$. For each increment vector $\vec{n}$ (i.e., $(q, \vec{n}_1, \vec{n}, q) \in \delta$ for some $\vec{n}_1 \in \mathbb{N}^k$), or initial vector $\vec{n} = \vec{n}_0$, we declare the procedure

**Procedure inc**

- for var $\text{idx} := 1$ to $k$
  - for var $\text{cnt} := 1$ to $\vec{n}(\text{idx})$
    - let $\text{tx} = *$
    - and $\text{pos} = *$
    - assume $\sigma_{\text{tx}}(\text{pos}) = \text{idx}$
    - post $r \leftarrow \text{p}_{\text{tx}} \ast d_{\text{tx}} \ast \text{pos}$

which posts $\vec{n}(m)$ tasks for each $m \in \{1, \ldots, k\}$, to be consumed later by arbitrary positions $j$ of the decrement sequences $\sigma_i$ (since $\text{pos}$ is assigned $\ast$) of arbitrary transitions $d_i$ (since $\text{tx}$ is assigned $\ast$) such that $\sigma_i(j) = m$—this ensures that the subsequent consumption of a task with handler $d_{i,j}$ corresponds to decrementing the $m$th component of $\vec{n}$. To perform the increment of transition $d_i \in \delta$ by vector $\vec{n}_2$, we declare the procedure $\text{p}_i$, which non-deterministically calls $\text{inc}_{\vec{n}_2}$, as

**Procedure main**

- var $\text{cur\_tx} := *$;
- var $\text{cur\_pos} = 1$;
- var $\text{empty} := \text{false}$;
- call inc$\vec{n}_0$ $()$
- await $r$
- // check: is this point reachable?
- $\text{empty} := \text{true}$;
- return.

Checking that $P_A$ faithfully simulates $A$ is easily done by noticing the correspondence between configurations $q_i\ell$ of $A$ and configurations of $P_A$ with $\sum_i \vec{n}$ pending tasks. Since $\text{empty} = \text{true}$ is only reachable when there are no pending tasks, reachability to $\text{empty} = \text{true}$ implies $0$ is reachable in $A$. Furthermore, if $0$ is reachable in $A$, a run of $P_A$ will eventually pass the await statement without pending tasks, setting $\text{empty} = \text{true}$.

**Proposition A.7.1.** The configuration $q0$ is reachable in $A$ from $q_i\ell_0$ if and only if $\text{empty} = \text{true}$ is reachable in $P_A$.

Since the size of $P_A$ is polynomial in $A$, we have a polynomial-time reduction for deciding configuration-reachability in $A$. 

\[\square\]