BIGFOOT: Static Check Placement for Dynamic Race Detection

Williams College Technical Report CSTR201702, March 14, 2017

Dustin Rhodes  Cormac Flanagan
University of California, Santa Cruz, USA

Stephen N. Freund
Williams College, USA

Abstract
Precise dynamic data race detectors provide strong correctness guarantees but have high overheads because they generally keep analysis state in a separate shadow location for each heap memory location, and they check (and potentially update) the corresponding shadow location on each heap access. The BIGFOOT dynamic data race detector uses a combination of static and dynamic analysis techniques to coalesce checks and compress shadow locations. With BIGFOOT, multiple accesses to an object or array often induce a single coalesced check that manipulates a single compressed shadow location, resulting in a performance improvement over FASTTRACK of 61%.

CCS Concepts • Theory of computation → Program analysis; • Software and its engineering → Concurrent programming languages; Software defect analysis

Keywords Data race conditions, concurrency, static analysis, dynamic analysis

1. Introduction
Data race conditions are a notorious problem in multithreaded software, often resulting in erroneous outputs and violations of expected correctness properties such as sequential consistency and atomicity. Much prior work has focused on static [1, 2, 4, 10, 18, 21, 31, 37, 53] and dynamic [15, 38, 40, 44, 45, 51, 59] data race detection.

Static analyses are able to reason about all executions of a program, but they generate false alarms or miss actual data races due to their necessarily conservative approximations of program behavior. In contrast, precise dynamic analyses offer a stronger guarantee of reporting a race condition if and only if a race occurs in the observed trace. The main limitation of precise dynamic detection is performance. The most efficient precise detectors, such as DJIT+ [40] and FASTTRACK [23] have overheads close to an order of magnitude or more, which is too high for many applications.

In general, precise dynamic race detectors work by keeping, for each shared memory location in the target program, a corresponding shadow location that records information about the access history for that memory location. For example, in DJIT+ each shadow location records the time of the last read and write to that location by each thread [40]. FASTTRACK refines this representation to store only the most recent read and write among all threads when possible [23].

The primary sources of overhead in dynamic race detectors are: the space overhead of maintaining a shadow location for each memory location in the target, and the time overhead of updating shadow locations for each memory access of the target. Dynamic analyses may sacrifice precision for reduced overhead, but only at the cost of introducing undesirable false alarms or missed races. In this paper, we present an optimized precise dynamic data race detection algorithm, BIGFOOT, that mitigates these overheads as follows:

1. Rather than keeping a distinct shadow location for each field in an object, or each entry in an array, BIGFOOT employs compressed representations using fewer shadow locations per object/array.

2. Rather than checking and updating shadow location metadata at each memory access of the target program, BIGFOOT uses a sophisticated static analysis to optimize check placement in the target code. In particular, it statically eliminates redundant checks where possible and statically combines multiple checks into a single coalesced check covering multiple fields or array indices.

Figure 1 compares BIGFOOT’s static check placement algorithm to the standard approach of performing a check at each access. In the move method, a typical race detector would instrument each of the six accesses with a check verifying that the access is race free. In contrast, BIGFOOT determines that the read check in each read-modify-write sequence is redundant with the check on the subsequent write, in the sense that the read will be involved in a data-race only if the write is also in a race. Thus, the read checks are not necessary to validate whether a trace is race free.

Furthermore, BIGFOOT combines the three write checks into a single coalesced check CheckWrite(this.x/y/z)
covering all three fields. Coalescing field checks in this manner is particularly helpful because it enables static shadow location compression for objects. In particular, suppose that all checks on Point objects are coalesced checks of the form CheckWrite(p.x/y/z) or CheckRead(p.x/y/z). BigFoot can then safely combine the shadow locations for the three fields into a single shadow location, and the coalesced checks then perform a single check-and-update operation on that shadow location, in contrast to the six checks on three shadow locations required by the traditional approach.

BigFoot optimizes array checks similarly, as shown in the method movePts in Figure 1. That code iterates over all array indices in a from lo to hi and moves each corresponding Point. In contrast to a standard dynamic race detector, which separately checks each array read, BigFoot coalesces these checks into the single check CheckRead(a[lo..hi]) after the loop. Here, lo..hi denotes the closed-open interval lo,lo + 1,...,hi − 2,hi − 1.

To efficiently handle such coalesced checks, BigFoot again employs a compressed representation for array shadow locations. In contrast to objects however, this compressed representation is chosen and adaptively refined at run time. Specifically, an array like a is initially represented as a "coarse-grained" single shadow location covering all array elements. A call such as movePts(a,0,a.length) generates a coalesced check CheckRead(a[0..a.length]) covering all array elements, which is processed at run time by checking and updating that array's single shadow location. If a subsequent call movePts(a, 0, a.length/2) generates a check CheckRead(a[0..a.length/2]) covering just half the array elements, the BigFoot run time would refine the shadow state for a to be two shadow locations, each covering half of a. That check is then handled by appropriately updating the first of these two shadow locations.

BigFoot's adaptive mechanism for arrays, modeled after SlimState [55], enables compressed array representations under a variety of common access patterns including block-based and strided accesses. If those patterns are not followed, BigFoot reverts to the "fine-grained" representation of a shadow location for each array element.

Imprecisions in BigFoot's static analysis may lead to sub-optimal check placement, as in the following example:

```java
def static int predicate() { return false; }
for(int i = 0; i < a.length; i++) {
  a[i].move(1, 1, 1);
  if(predicate()) {
    CheckRead(a[i]);
  }
}
```

BigFoot's method-local analysis will not statically coalesce the array checks because it cannot statically determine which elements are accessed. At run time, suppose a has a single shadow location when this code runs. If predicate() always returns true, then all indices in a are accessed, and we'd like to preserve the coarse-grained representation to save both space and time. To do so, BigFoot's run time defers checks on arrays, and instead dynamically records a per-thread footprint of which indices have "pending" checks. BigFoot


“commits” the footprint for a thread and checks the corresponding shadow locations for races when the thread next performs a synchronization operation. This dynamic footprinting technique allows BIGFOOT to keep a single shadow location for the array \(a\), even in the presence of a scenario like the above that is not amenable to static coalescing.

Figure 2 compares BIGFOOT to several prior precise race detection algorithms: FASTTRACK, REDCARD (which statically eliminates some redundant checks and compresses shadow state), SLIMSTATE (which dynamically compresses array shadow state), and SLIMCARD (which combines the REDCARD and SLIMSTATE analyses, as described in Section 5). All were implemented in the ROADRUNNER framework for Java [24]. The key innovations of BIGFOOT, namely static check motion and coalescing, provide substantial performance improvements, particularly when combined with existing static and dynamic shadow compression techniques.

Detection Precision A data race detector is trace-precise if it correctly determines whether a given trace has a race condition or not. A trace-precise race detector is additionally address-precise if it can also determine all addresses that have race conditions. Using this terminology, FASTTRACK and SLIMSTATE are address-precise. Our BIGFOOT core algorithm is also address-precise, as we discuss in Section 3. Our BIGFOOT implementation, however, uses additional check placement optimizations for which one data race may prevent the detection of a subsequent race. Consequently, our implementation is trace-precise but not address-precise, as described in Section 5. In practice, the BIGFOOT implementation was address-precise in all our experiments.

We also note that since BIGFOOT defers checking until after accesses occur, a data race may be detected only after it has happened. This introduces several subtleties related to precision. First, we currently assume for simplicity that all loops terminate and consider all unchecked exceptions to be programming errors. Thus, a race preventing a loop from terminating or causing an unchecked exception may be missed since the deferred check is never reached. However, we did not see this occur in practice, and we discuss analysis extensions to cover these items in Sections 3 and 5. In addition, if a data race can corrupt the race detector’s analysis state, it may similarly go undetected [5], but for type-safe languages like Java, this cannot happen.

Contributions The primary contributions of this paper are:

- We define a theory of precise check placement for dynamic race detection and describe a core static analysis to optimize check placement (Sections 2 and 3).
- We integrate static field proxy compression and dynamic array shadow compression techniques to further reduce run-time overhead (Section 4).
- We present our BIGFOOT prototype for Java (Section 5).
- We show that BIGFOOT’s static analysis scales well (requiring on average less than 0.2s per method processed) and reduces run-time overhead from 7.3\(x\) (for FASTTRACK) to 2.5\(x\), an improvement of 61\% (Section 6).

2. Theory of Check Placement

A key design goal of the core BIGFOOT algorithm is that the checks inserted into a target program enable address-precise data race detection. That is, BIGFOOT must insert checks that are sufficient to detect all data races but that never report false alarms. Reasoning about this requirement can be subtle. For example, the code in Figure 3 contains a single check that enables precise data race detection for all three accesses, but it may not be immediately apparent why this is the case.

<table>
<thead>
<tr>
<th>Race Detector</th>
<th>Check Motion and Coalescing</th>
<th>Red. Check Elimination</th>
<th>Metadata Compression</th>
<th>Run-Time Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>FASTTRACK [23]</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>7.3x</td>
</tr>
<tr>
<td>REDCARD [25]</td>
<td>no</td>
<td>no</td>
<td>static proxy</td>
<td>6.0x</td>
</tr>
<tr>
<td>SLIMSTATE [55]</td>
<td>no</td>
<td>dynamic</td>
<td>static proxy, global</td>
<td>6.0x</td>
</tr>
<tr>
<td>SLIMCARD</td>
<td>no</td>
<td>dynamic</td>
<td>static proxy</td>
<td>5.1x</td>
</tr>
<tr>
<td>BIGFOOT</td>
<td>static</td>
<td>static + dynamic</td>
<td>static proxy</td>
<td>2.5x</td>
</tr>
</tbody>
</table>

Figure 2. Comparison to prior precise dynamic race detectors, and SLIMCARD (which combines REDCARD and SLIMSTATE).

<table>
<thead>
<tr>
<th>RACK</th>
<th>Detector</th>
<th>Check Motion and Coalescing</th>
<th>Red. Check Elimination</th>
<th>Metadata Compression</th>
<th>Run-Time Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>FASTTRACK [23]</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>7.3x</td>
</tr>
<tr>
<td>REDCARD [25]</td>
<td>no</td>
<td>no</td>
<td>static</td>
<td>static proxy</td>
<td>6.0x</td>
</tr>
<tr>
<td>SLIMSTATE [55]</td>
<td>no</td>
<td>dynamic</td>
<td>no</td>
<td>dynamic</td>
<td>6.0x</td>
</tr>
<tr>
<td>SLIMCARD</td>
<td>no</td>
<td>dynamic</td>
<td>static</td>
<td>dynamic</td>
<td>5.1x</td>
</tr>
<tr>
<td>BIGFOOT</td>
<td>static</td>
<td>static + dynamic</td>
<td>static, better</td>
<td>static proxy</td>
<td>2.5x</td>
</tr>
</tbody>
</table>

Figure 3. A code fragment with precise checks, and the corresponding BIGFOOT analysis contexts from Section 3.

(All variables are thread-local, and objects thread-shared.)

1 REDCARD and SLIMCARD exhibit similar precision properties for the same reasons.
In this section, we develop a theory of check placement to characterize exactly where checks must be performed to avoid false negatives and false positives. To simplify our exposition, we initially do not distinguish between read and write accesses (although our implementation extends these ideas to do so, as described in Section 5).

Given an execution trace of a program, we say the trace has a data race if it has two accesses to the same memory location that are not ordered by the happens-before relation, which is defined in the usual fashion \[33, 40\]. Similarly, a trace has a check race if it has two checks to the same memory location that are not ordered by happens-before. A precise check placement algorithm must ensure that any execution trace of the target program has a data race if and only if it has a check race.

Figure 4(a) illustrates where checks must be performed in a trace to guarantee all data races are detected. The trace shown has a data race because the happens-before edges (shown as solid arrows) generated by synchronization operations do not order the two accesses to \(y.f\), as indicated by the dashed edge. Any check performed by Thread 1 in the Covering Check Range will trigger a check race corresponding to that data race. However, checks outside that range will not, resulting in a false negative because the access race would have no corresponding check race.

With this intuition, we say that a check covers an access to the same location by the same thread if the check either:

- precedes the access with no intervening release, or
- succeeds the access with no intervening acquire.

Note that we treat acquire and released differently, as they serve as sources and sinks for synchronization edges in the happens-before graph, respectively. Returning to Figure 4(a), the single check thus covers all three accesses in any trace generated by this code. We show in the supplementary appendix that if each access in a program has a covering check, then any trace with a data race also has a check race. That is, access coverage guarantees no missed races.

Figure 4(b) illustrates where checks may be performed in a trace to guarantee all check races indicate data races. This trace has no data race because the three accesses to \(y.f\) are ordered by happens-before edges. Similarly, the checks inside the critical section of Thread 1 (marked Legitimate Check Range) produce no check races. However, a check outside this range produces a check race, which would be a false alarm since there is no corresponding data race.

We say that a check is legitimate for an access to the same location by the same thread if the check either:

- precedes the access with no intervening acquire, or
- succeeds the access with no intervening release.

For example, in Figure 3, the check is legitimate for the second access, but not the first or third.

With these notions of legitimacy and coverage, we say a trace has precise checks if each access is covered by some check (no missed races) and each check is legitimate for some access (no false alarms). A program has precise checks if all possible execution traces have precise checks.

3. Optimizing Check Placement

We next describe our static analysis for optimizing the placement of precise checks.

3.1 BFJ Language and Semantics

We formalize our ideas in terms of the idealized language BFJ (BigFoot Java) shown in Figure 5. A program \(P\) contains a sequence of class definitions \(D\) and a collection of concurrent threads \(s_1 || ... || s_n\). Each class definition \(D\) contains field and method declarations. Each field declaration is simply a field name \(f\). Each method declaration \(m(\overline{x})\{s; \text{ return } z\}\) includes a unique method \(m\), formal parameters \(\overline{x}\), and a body \(s\) followed by a return of the local variable \(z\). We omit static
The B\textsubscript{F} path of the form $\{ f \}$ describes an object field, and path of the form $b..e$ to abbreviate singleton ("$b..e$" describes properties of the form $b..e:k$). To illustrate how B\textsubscript{F} uses context information to place checks, we examine the analysis contexts in Figure 5. As in all BFJ code, the variables in this snippet are local and cannot be changed by other threads, although they may point to shared objects.

BigFOOT adds a past access $p^\perp$ to the history whenever the code accesses $p$, and before an acquire it inserts a check for any past access $p^\perp$ with no past covering check $p^\vee$, as at line 5. Since the acquire signifies the end of that past access’s covering check range, placing the check any later would introduce the potential for missed data races.

At each release, BigFOOT removes each past access $p^\perp$ from the history. The release signifies the end of the legitimate check range for those accesses, and placing checks for them any later would introduce the potential for false alarms. “Forgetting” a past access $p^\perp$ like this typically requires BigFOOT to place a covering check before the release, but there are two situations when no check is needed: (1) a covering check has already occurred ($p^\vee$ is in the history), as at line 8; or (2) we anticipate a later access to the same location, as at line 3. The anticipated later access (and hence its covering check) will occur before leaving the original access’s covering check range at the next acquire. Each check $p^\vee$ must also be forgotten at a release because that check does not cover any subsequent access to $p$.

Anticipated access information flows backwards, and anticipated accesses in an acquire’s post-history must be removed from its pre-history because checks covering those future accesses will not cover accesses prior to the acquire.

We now examine the `if` statement in Figure 5(a). The merged context $\{ b.f^\perp \}$ after the `if` describes properties holding after both branches, and it omits past accesses occurring only on one branch. BigFOOT must ensure a covering check exists for any such “forgotten” past access. That necessitates checking $b.g$ in the “then” branch, after which it is permissible to simultaneously forget both the past access and past check on $b.g$ when leaving the `if`. In contrast, $x.f$ is anticipated at the end of the “else” branch, and we skip checking it at that point because the later access will have a check covering both accesses.

3.3 Check Placement Algorithm Overview

The BigFOOT check placement algorithm defers checks as long as possible and only inserts them into the program code when they cannot be further deferred without risking false alarms or missed data races; thus checks are only placed before synchronization operations and control flow merge points, and at the ends of methods and threads.

To illustrate how BigFOOT uses context information to place checks, we examine the analysis contexts in Figure 5. As in all BFJ code, the variables in this snippet are local and cannot be changed by other threads, although they may point to shared objects.

BigFOOT adds a past access $p^\perp$ to the history whenever the code accesses $p$, and before an acquire it inserts a check for any past access $p^\perp$ with no past covering check $p^\vee$, as at line 5. Since the acquire signifies the end of that past access’s covering check range, placing the check any later would introduce the potential for missed data races.

At each release, BigFOOT removes each past access $p^\perp$ from the history. The release signifies the end of the legitimate check range for those accesses, and placing checks for them any later would introduce the potential for false alarms. “Forgetting” a past access $p^\perp$ like this typically requires BigFOOT to place a covering check before the release, but there are two situations when no check is needed: (1) a covering check has already occurred ($p^\vee$ is in the history), as at line 8; or (2) we anticipate a later access to the same location, as at line 3. The anticipated later access (and hence its covering check) will occur before leaving the original access’s covering check range at the next acquire. Each check $p^\vee$ must also be forgotten at a release because that check does not cover any subsequent access to $p$.

Anticipated access information flows backwards, and anticipated accesses in an acquire’s post-history must be removed from its pre-history because checks covering those future accesses will not cover accesses prior to the acquire.

We now examine the `if` statement in Figure 5(a). The merged context $\{ b.f^\perp \}$ after the `if` describes properties holding after both branches, and it omits past accesses occurring only on one branch. BigFOOT must ensure a covering check exists for any such “forgotten” past access. That necessitates checking $b.g$ in the “then” branch, after which it is permissible to simultaneously forget both the past access and past check on $b.g$ when leaving the `if`. In contrast, $x.f$ is anticipated at the end of the “else” branch, and we skip checking it at that point because the later access will have a check covering both accesses.
if (i<0) {
  \{ i < 0 \} \{ \text{bf}^\circ, \text{bg}^\circ \}
  y = \text{bg};
  \{ i < 0, \text{bg}^\circ \} \{ \text{bf}^\circ \}
  \text{check}(\text{bg});
  \{ i < 0, \text{bg}^\circ, \text{bg}^\prime \} \{ \text{bf}^\circ \}
} else {
  \{ i \geq 0 \} \{ \text{bf}^\circ \}
  x = \text{bf};
  \{ i \geq 0, \text{bf}^\circ \} \{ \text{bf}^\circ \}
} \{ \text{bf}^\circ, \text{bf}^\prime \} \{ \emptyset \}
\text{check}(\text{bf});
\{ \text{bf}^\circ, \text{bf}^\prime \} \{ \emptyset \}

1: i = 0;
2: loop {
  \{ i = 0 \} \{ \text{bf}^\circ, a[i]^\circ \}
  \{ a[0..i]^\circ \} \{ a[i]^\circ, \text{bf}^\circ \}
  t = \text{bf};
  \{ a[0..i]^\circ, \text{bf}^\circ \} \{ a[i]^\circ \}
  i' = i + 1;
  \{ i = i' + 1 \} \{ a[0..i']^\circ, a[i']^\circ, \text{bf}^\circ \} \{ \emptyset \}
  \text{if} (...) \text{break};
  \{ i = i' + 1, a[0..i']^\circ, a[i']^\circ, \text{bf}^\circ \} \{ \text{bf}^\circ, a[i]^\circ \}
} \{ i = i' + 1, a[0..i']^\circ, a[i']^\circ, \text{bf}^\circ \} \{ \emptyset \}
9: \text{check}(a[0..i], \text{bf});

Figure 6. Analysis contexts and check placements for BFJ method bodies containing (a) an if statement and (b) a loop.

Checks deferred until after a loop may never be executed if the loop diverges. We currently assume all loops terminate but could alternatively include a termination analysis and treat potentially non-terminating loops specially by, for example, periodically committing deferred checks inside the loop.

3.4 Check Placement Rules

We formalize BigFOOT’s check placement algorithm as the judgment \( \vdash s : H \bullet A \rightarrow H' \bullet A' \) defined in Figure 7. The contexts \( H \bullet A \) and \( H' \bullet A' \) are the pre- and post-contexts of \( s \). The analysis is a combined forward/backward analysis; history properties flow forward from pre-history \( H \) to post-history \( H' \), while anticipated properties flow backwards from post-anticipated \( A' \) to pre-anticipated \( A \).

For conciseness, we do not express check placement as a rewriting transformation on program syntax. Instead, we assume that a pre-transformation has already inserted a check \( \text{check}(C) \) wherever one may be required. The goal of the check placement algorithm is then to resolve each path set variable \( C \) into the appropriate set of paths to be checked at that point. The rules for \( \vdash s : H \bullet A \rightarrow H' \bullet A' \) include antecedents constraining each \( C \) appropriately.

Context Entailment and Ordering. Our rules use the notation \( h \in H \) for the usual syntactic notion of set membership for history properties. In addition, we introduce a richer notion of history entailment \( (H \vdash h) \) that accounts for other information in \( H \). For example, if \( H = \{ z[i]^\circ, i = j \} \) then we can safely infer that \( H \) entails \( z[j]^\circ \), written \( H \vdash z[j]^\circ \). Similarly, we introduce anticipated entailment \((H \bullet A \vdash a)\), as in \( \{ i < 10 \} \{ x[0..10]^\circ \} \vdash x[0..9]^\circ \). Our implementation uses Z3 [16] to reason about entailment.

While history and anticipated sets could be ordered by the subset relation \( (\subseteq) \), we employ a stronger ordering \( (\sqsubseteq) \) based on entailment to achieve greater precision:

\[
H_1 \sqsubseteq H_2 \iff \forall h \in H_1, H_2 \vdash h
\]
\[
H \vdash A_1 \sqsubseteq A_2 \iff \forall a \in A_1, H \bullet A_2 \vdash a
\]
These orderings generate corresponding meet operators, where the meet on anticipated sets additionally takes history sets to reason about entailment.

\[ H_1 \cap H_2 = \{ h \in H_1 \cup H_2 : H_1 \vdash a, H_2 \vdash a \} \]
\[ H_1 \cdot A_1 \cap H_2 \cdot A_2 = \{ a \in A_1 \cup A_2 : H_1 \cdot A_1 \vdash a, H_2 \cdot A_2 \vdash a \} \]

**Analysis Rules** The analysis rules are somewhat complex due to their bidirectional nature and the subtle properties being captured. We present the technical details of our core rules below, but subsequent paper sections do not assume an in-depth understanding of all their details.

**[Rel]**: Since past accesses need to be checked before a release, this rule targets the syntax `check(C); rel(x)` and uses the function

\[ \text{Checks}(H, A) = \{ p : p^\ll H, H \not\vdash p^\ll, H \cdot A \not\vdash p^\ll \} \]

(We assume \( x \not\in \text{Vars}(H) \) in the rules modifying \( x \): [Assign], [Rename], [New], [Read], [A-New], [A-Read], and [Call].)
as the assignment would otherwise invalidate that history information. The \textbf{[Read]} rule adds past access \( y.f^\mathcal{C} \) to the post-history. The pre-anticipated paths become \( A \setminus x \cup \{ y.f^\mathcal{C} \} \), where \( A \setminus x \) removes all properties mentioning \( x \) from \( A \).

\textbf{[Rename]}: As mentioned above, assignments can only target “fresh” variables not in \( H \), but in some cases, e.g. before a loop back edge, we may need to modify an existing non-fresh variable \( y \). We cannot simply remove \( y \) from the history, as that might remove past accesses with pending checks, such as \( y.f^\mathcal{C} \). Instead, the renaming operation \( x \leftarrow y \) copies the value of \( y \) into a fresh variable \( x \), and replaces all mentions of \( y \) in the history \( H \) by \( x \), with the result that \( y \) is now “fresh” (not mentioned in the history) and can be an assignment target. To illustrate this rule, consider the renaming \( i \leftarrow i' \) on line 5 in Figure 6(b). The history prior to the renaming contains \( a_\{0..i\}^\mathcal{C} \) and \( a_\{i\}^\mathcal{C} \). After renaming, we have \( a_\{0..i\}'^\mathcal{C} \) and \( a_\{i\}'^\mathcal{C} \), enabling us to continue deferring the checks for those accesses.

\textbf{[Write]}: This rule for \( y.f = x \) adds the access \( y.f^\mathcal{C} \) to the pre-history, and \( y.f^\mathcal{O} \) to the pre-anticipated set.

\textbf{[Assign]}: This rule for the assignment \( x = e \) adds the boolean expression \( x = e \) to the post-history. We require \( x \not\in \text{Vars}(e) \) to ensure the post-history does not refer to the pre-value of \( x \). The pre-anticipated set is computed from the \( A \) via the substitution \( A[x := e] \), which replaces all occurrences of \( x \) with \( e \) in each \( p^\mathcal{O} \in A \). Since anticipated paths are not closed under this substitution, we remove from the result any syntactically ill-formed anticipated paths.

\textbf{[If]}: Conditionals may require checks to be placed at the end of each branch, and so this rule targets the syntax \( \text{if } be \{ s_1; \text{check}(C_1) \} \{ s_2; \text{check}(C_2) \} \). This rule first computes the post-histories \( H'_1 \) and \( H'_2 \) and pre-anticipated sets \( A_1 \) and \( A_2 \) for \( s_1 \) and \( s_2 \). The merged history \( H'_1 \cap H'_2 \) describes properties holding after both branches but may leave out accesses that occurred only on one branch. We introduce the following variant of the \textbf{Checks} function to compute the unanticipated unchecked past accesses in \( H \) that must be checked when \( H \) is approximated by \( H' \):

\[
\text{Checks}(H, H', A) = \\
\{ p : p^\mathcal{C} \in H, H' \not\vdash p^\mathcal{C}, H \not\vdash p^\mathcal{O}, H \circ A \not\vdash p^\mathcal{O} \}
\]

Thus, \( C_1 = \text{Checks}(H'_1, H'_1 \cap H'_2, A_{out}) \) are those paths that must be checked at the end of the “then” branch, and similarly for \( C_2 \) on the “else” branch. The contexts at the end of the branches are then \( H_1 \cup C_1^\mathcal{O} \) and \( H_2 \cup C_2^\mathcal{O} \), and these are merged via \( \cap \) to yield the final history \( H_{out} \). The anticipated pre-context \( A_{in} \) is computed by merging together the anticipated contexts preceding \( s_1 \) and \( s_2 \).

\textbf{[Loop]}: Loops similarly require checks on the two paths meeting at the loop head, and this rule targets the form:

\[
\text{check}(C_{in}); \text{loop } \{ \text{if be break } \}; \text{check}(C_{back})
\]

In this rule, \( H_{in} \) and \( H_{back} \) are the pre-histories of \( \text{check}(C_{in}) \) and \( \text{check}(C_{back}) \), respectively, and \( H_{inv} \) is the loop-invariant history at the loop head. As in \cite{11}, the \textbf{Checks} function uses these sets and \( A_{in} \), the anticipated set at the loop head, to compute \( C_{in} \) and \( C_{back} \). The side conditions \( H_{in} \cup C_{in}^\mathcal{O} \supseteq H_{inv} \) and \( H_{back} \cup C_{back}^\mathcal{O} \supseteq H_{inv} \) ensure that properties in \( H_{inv} \) are true on all paths into the loop head.

Note that \( H_{inv} \), \( H_{in} \), and \( H_{back} \) are defined via mutual recursion; they are computed as part of a greatest fixed point computation over a method body. The computation is seeded with an initial conjecture for \( H_{inv} \) that is then refined via a form of predicate abstraction. (See Section 5.) An analogous anticipated set \( A_{inv} \) characterizing what is anticipated prior to the loop exit test is used in the computation of \( A_{in} \).

\textbf{[Call]}: A method call may require checks prior to the call if the callee performs synchronization (either directly or indirectly via a nested method call). Thus we match syntax of the form \( \text{check}(C); x = y.m(\tau) \). The function \textbf{KillSetHistory}(m) denotes the set of history properties killed by the side effects of method \( m \), and contains:

\[
\{ -_C \} \quad \text{if } m \text{ acquires a lock} \\
\{ -_C, -_V \} \quad \text{if } m \text{ releases a lock}
\]

The function \textbf{KillSetAnticipated}(m) describes anticipated accesses killed by \( m \). It is \( \{ -_C \} \) if \( m \) acquires a lock and \( \emptyset \) otherwise. Our implementation pre-computes \textbf{KillSetHistory}(m) and \textbf{KillSetAnticipated}(m) using a separate whole program analysis. Checks are added before the call for any unchecked accesses \( C \) that are killed by the call, and the post-history \( H' \) is derived from the pre-history \( H \) and \( C \) by removing all such killed properties.

\textbf{Correctness Sketch} The Appendix contains a detailed proof showing that the BigFoot algorithm described so far is correct in that it is address-precise. We present a short outline of our argument below.

We first formalize an operational semantics for BFJ that evaluates program \( P = D; s_1; \ldots; s_n \) via a sequence of states \( \Sigma_0 \rightarrow a_1^\Sigma \rightarrow a_2^\Sigma \cdots \rightarrow a_n^\Sigma \Sigma_n \), where \( \Sigma_0 \) is an initial state for \( P \) and \( \Sigma_n \) is a final terminating state. This evaluation sequence yields a trace \( \alpha = a_1.a_2 \ldots a_n \) describing the memory accesses, race checks, and synchronization operations performed by \( P \).

We also define a judgement \( D; \alpha \vdash \Sigma \) describing when a run-time state has correct checks in the context of an execution history \( \alpha \). This judgement most notably ensures that, for each thread \( t \), the context \( H \circ A \) for thread \( t \)’s current program point is consistent with \( \Sigma \) and \( \alpha \). This judgement entails the following:

1) Each expression \( be \in H \) is true when evaluated at \( t \) in the current state \( \Sigma \).
2) If \( p^\mathcal{O} \in H \) and \( p \) denotes a memory \( l \), there is an access to \( l \) in \( t \) \( \alpha \) with no later release. (Each \( p^\mathcal{O} \in H \) must have similar check.)
3) Each check by \( t \) in \( \alpha \) is legitimate for a preceding access.
4) Each access to a location \( l \) by \( t \) in \( \alpha \) is either covered by a check, or \( t \) is still in that access’s covering check range and
there is some path \( p \) denoting \( l \) such that either \( p^< \) is in \( H \) or \( p^\circ \) is in \( A \).

The first two requirements show that the history context soundly approximates program behavior. The third and fourth guarantee that each check performed by \( t \) is legitimate and that each access by \( t \) has either been covered by a check or will be covered by deferred check performed later in the trace.

Provided \( \vdash P \), the initial state satisfies the criteria for well-formed states (i.e., \( \mathcal{D}; e \models \Sigma_0 \)), and we show via a preservation argument that it holds for each subsequent state, including the last, i.e., \( \mathcal{D}; \alpha \models \Sigma_n \). Since each thread in \( \Sigma_n \) has terminated and will perform no subsequent checks or accesses, the rules for (\( \models \)) imply that \( \alpha \) has precise checks. Consequently, the checks in \( P \) are address-precise. That is, if \( \vdash P \) and \( P \) generates a trace \( \alpha \), then for any address \( l \), \( \alpha \) has a data race on \( l \) if and only if it has a check race on \( l \).

4. Check Coalescing & Shadow Compression

Post-Analysis Path Coalescing

In preparation for our shadow compression algorithms, we perform one last coalescing step on each set of checks added to the program. Specifically, for each check \( \text{check}(C) \) statement, we divide the paths in \( C \) into equivalence classes based on the path designator: that is, \( d_1.f_1 \) and \( d_2.f_2 \) are in the same class if \( d_1 \) and \( d_2 \) refer to the same object in the check’s pre-history written \( H_\vdash d_1 = d_2 \), and similarly for array paths.

We then coalesce each group \( d_1.f_1, d_2.f_2, \ldots, d_n.f_n \) sharing equivalent designators to the coalesced field path \( d_1.f_1/f_2/\cdots/f_n \). We also coalesce each group of paths \( d_1[b_1..c_1:k_1], \ldots, d_n[b_n..e_n:k_n] \) to one array path \( d_1[b..e:k] \) such that the strided range “\( b..e : k \)” captures the exact same set of indices as the \( n \) original strided ranges. This step necessitates solving a collection of integer constraints over program expressions, but those constraints have a form that cannot be handled by, e.g., Omega [41] or effectively solved directly via Z3. Thus, to find a suitable \( b, e, \) and \( k \), our implementation tries various combinations of the bounds and step sizes from the original strided ranges. This combinatorial approach can be expensive if there are a large number of strided ranges, but we have found it effective in practice. If a coalesced path cannot be found, we simply keep the original set of paths. We could alternatively try to divide the set into two or more coalescible subsets, but this provided little benefit in practice.

Shadow Compression

A precise dynamic race detector typically maintains a distinct shadow location for each object field or array element. Thus, an object \( pt \) with three fields requires three shadow locations and \( \text{check}(pt.x/y/z) \) performs three shadow-location operations. Similarly, an array \( a \) of \( n \) elements requires \( n \) shadow locations, and \( \text{check}(a[0..n]) \) performs \( n \) shadow-location operations.

However, check coalescing enables us to identify groups of shadow locations that can be compressed into a single shadow location at run time with no loss in precision. More-over, a coalesced check covering a compressible group only requires a single shadow-location operation, yielding substantial performance benefits. Compressible locations can be identified statically or dynamically. We have found the combination of static compression for object fields and dynamic compression for array elements yields the best performance.

Static Field Compression

We identify fields of a class that are compressible via a static shadow proxy analysis [25]. Given a class with fields \( x \) and \( y \), field \( x \) is a proxy for \( y \) if every check \( \text{check}(p..x/y/\cdots) \) also checks \( p..x \). Thus, any trace exhibiting a race on \( p.y \) will also have a race on \( p.x \). Hence, we can compress the shadow locations for \( x \) and \( y \) into a single location while still being able to distinguish race-free executions from those with races. Identifying field proxies requires a single pass over all checks.

Dynamic Array Compression

We could express similar proxy relationships for array elements. For example, \( \text{a}[0] \) could be a proxy for all array entries \( \text{a}[0..n] \) if all checks on the array all have the form \( \text{check}(\text{a}[0..n]) \). Similarly, \( \text{a}[1,2] \) could be the proxy for each \( \text{a}[1] \) if all checks have the form \( \text{check}(\text{a}[0..n:2]) \) or \( \text{check}(\text{a}[1..n:2]) \). REDCARD [25] used this approach, but its static array proxy analysis failed to scale and was too imprecise to capture many proxy relationships, as we demonstrate in Section 6.

BIGFOOT instead makes array shadow compression choices dynamically using an extension of the approach introduced in the SLIMSTATE checker [55]. Specifically, BIGFOOT augments static array check coalescing with a complementary dynamic coalescing technique based on array footprints. For each array \( a \), the BIGFOOT run time maintains a per-thread footprint of which indices must be checked prior to that thread’s next synchronization operation. When a thread \( t \) performs \( \text{check}(\text{a}[b..e:k]) \), BIGFOOT adds the strided range \( b..e:k \) to \( t \)’s footprint for \( a \). In this way, many individual check operations that were not coalesced statically may be coalesced dynamically into a single, large footprint. At thread \( t \)’s next synchronization point, its footprint for \( a \) is “committed” and the necessary shadow-location operations are performed to verify race freedom.

BIGFOOT initially compresses the shadow state for the entire array into a single shadow location. It then adaptively refines that representation whenever it must commit a footprint that is not consistent with the array’s current representation. As in SLIMSTATE, BIGFOOT supports compression modes matching common patterns of array accesses, including block-based and stride-based patterns. SLIMSTATE processes every individual array access at run time to build its dynamic footprints. By statically coalescing checks, BIGFOOT eliminates much of that overhead.

2 While this optimization guarantees that we precisely identify race-free traces, we may not identify all memory locations with races since a race on \( x \) may or may not imply a race on \( y \). This subtlety goes away if we consider only symmetric proxy relations, e.g., when \( y \) is also a proxy for \( x \).
5. Implementation

We have implemented our analysis in the BigFoot checker for Java. BigFoot consists of a static component (StaticBF) and a dynamic component (DynamicBF). StaticBF reads in a bytecode program and a list of classes and methods to transform, and it outputs a version of the program with explicit race checks for all object and array accesses in the specified methods. DynamicBF is the complementary dynamic race detector that reads in the instrumented program, runs it, and reports any races observed.

Extending the BFJ analysis to the full Java language is straightforward, and we describe the most important aspects of StaticBF below. BigFoot handles all basic synchronization operations present in Java, including locks, volatile variables, fork/join, and wait/notify, as described in [23].

**Alias Expressions and Precision** StaticBF augments BFJ’s set of boolean expression be with heap alias expressions of the form \( x = y.f \) and \( x = y[z] \), which enable us to reason about aliasing when deciding entailment. Those expressions are added to the history on field/array reads and are retained as long as they are valid under the assumption that the target is race free. If an alias expression is invalidated by a data race at run time, we may miss reporting some subsequent data races (because race checks were not placed in the necessary positions), but we will always detect the initial race.

For example, consider the code fragment to the right, which includes the alias expressions recorded by StaticBF.

```java
acq(lock); x = a.f; // x = a.f
s = x.g; y = a.f; // y = a.f
t = y.g;
check(a.f, x.g);
rel(lock);
```

While utilizing local alias expressions enables StaticBF to better optimize check placement, it means that, in theory, BigFoot is trace precise but not address precise. In practice, however, BigFoot was address-precise for all of our benchmark runs, which we verified via an additional dynamic analysis that checks that each observed execution trace performs precise checks (in the sense of Section 2).

5.1 StaticBF

StaticBF is built on top of the WALA analysis framework [54]. WALA represents methods as CFGs over SSA instructions and analyzes all methods in a call graph constructed using a 0-CFA analysis. To ensure method CFGs are amenable to our analysis, StaticBF performs an initial pass over the target to (1) rewrite each loop as an if statement containing a do-while loop matching BFJ's syntax, and (2) eliminate all critical edges from the CFGs (see, e.g., [3]). We use Soot [50] for this pass. We also precompute KillSetHistory and KillSetAnticipated via a simple inter-procedural dataflow analysis. StaticBF then inserts checks into each method using a method-local dataflow analysis.

The initial context for each program point is \( \{ h : h \in \text{History} \} \cdot \{ a : a \in \text{Anticipated} \} \), and the analysis computes the greatest fixed point solution for those contexts according to the rules in Figure 7. To simplify the implementation, we compute context properties via separate passes for (1) boolean and alias expressions, (2) past accesses, (3) anticipated accesses, and finally (4) past checks and the set \( C \) for each \( \text{check} (C) \). All passes are forward analyses, except for the anticipated accesses pass.

StaticBF handles SSA \( \phi \)-functions as they were handled in RedCard [25]. Also as in RedCard, StaticBF tracks extended paths containing multiple field/array accesses (as in \( a[1].f \) or \( b.f.g \)), which are necessary for maintaining precision when merging contexts encoding equivalent aliasing facts via different local variables. We implement the entailment relations via the Z3 SMT Solver [16].

After applying the final coalescing step and static field proxy analysis described in Section 4, StaticBF generates a new version of the target code with the necessary checks inserted. These checks take the form of method calls into the DynamicBF run time. Paths in check statements refer to SSA variables and variables introduced via the [rename] rule, and not the stack slots and locals present in the original bytecode. Thus, StaticBF inserts additional locals and load/store instructions to reify them in the instrumented target. Our relatively naive algorithm may introduce extraneous memory loads/stores, and we apply the Soot optimizer in a post-transformation pass to eliminate them.

**Distinguishing Reads and Writes** Up to this point, we have not distinguished reads and writes. However, StaticBF must do so because precise dynamic race detectors treat them differently. In particular, two concurrent accesses are considered conflicting only when at least one is a write.

To account for this, we extend our notions of legitimate and covering checks. A write check is only legitimate for a write access, but a read check is legitimate for both write and read accesses. A write check can cover write or read accesses, but a read check can only cover read accesses. In addition, contexts record whether each \( p^x \) and \( p^y \) is a read or write access, and whether each \( p^v \) is a read or write check. The analysis rules and coalescing operations are also extended appropriately.

**Loop Invariants** StaticBF infers the loop invariant \( H_{inv} \) for rule [loop] via a form of Cartesian predicate abstraction [26] [30]. Specifically, StaticBF identifies the loop’s linear induction variables and trip count [28] [50] and then builds an initial set \( H_{heuristic} \) of boolean constraints and past accesses consistent with that information. Since this algorithm does not reason precisely about synchronization, function
calls, and various other bytecode features, it may produce some incorrect properties. Thus, STATICBF repeatedly analyzes the loop body to infer the maximal $H_{inv} \subseteq H_{heuristic}$ that is valid loop invariant as part of its dataflow analysis passes. STATICBF similarly infers the anticipated invariant $A_{inv}$ by constructing an initial $A_{heuristic}$ and computing the maximal valid $A_{inv} \subseteq A_{heuristic}$. If no induction variables can be identified, then $A_{heuristic}$ is the empty set, and no loop invariant are inferred. Irreducible loops and complex computations may be problematic for our algorithm, but it is quite effective in practice.

**Static Fields** In the JVM, a thread’s first access to a static field may synchronize with the declaring class’s static initializer to ensure proper behavior [34]. STATICBF provides a command line flag to treat static field accesses as potential synchronization so that checks will not be deferred across them. We use this flag for several benchmarks where this matters. (Other instructions that may synchronize with static initializers, *e.g.* type casts, are handled similarly.)

**Exceptions** STATICBF reasons about control paths for checked exceptions [29], but assumes unchecked exceptions, such as NullPointerExceptions, are errors in the target program and guarantees precision only for error-free traces. This is an artifact of our current implementation and not a fundamental limitation. Unchecked exceptions could be fully handled via a more sophisticated code translation scheme inside STATICBF, but given the complexity of the resulting code, a better approach would be to integrate parts of the analysis into the JVM’s exception mechanism. Our current treatment of exceptions did not lead to missed race checks in any of our benchmark experiments.

5.2 **DYNAMICBF**

We built our complementary DYNAMICBF dynamic analysis in the ROADRUNNER framework [24]. Dynamic footprinting and array shadow compression are implemented as in the earlier SLIMSTATE checker and we use FastTrack’s adaptive epoch representation [24] for shadow locations. BigFoot follows ROADRUNNER’s standard treatment of libraries: fields of Java’s core library classes are not checked for races, and synchronization operations internal to those libraries are assumed not to be used to protect any of the target’s data and are ignored. However, several key library methods from java.lang.Object and java.lang.Thread, such as Object.notify and Thread.start, are treated specially as synchronizing operations. These assumptions are shared by all checkers we evaluate, and also included in STATICBF. Their violation may impact precision.

6. **Validation**

We validate BigFoot’s performance by comparing it to FastTrack [23], SLIMSTATE [55], RedCARD [25], and SLIMCARD (Section 6.2) on the JavaGrande [32] and DaCapo [6] benchmark suites. To facilitate comparison the detectors share as much common implementation as possible.

We configured the JavaGrande programs to use their largest data sizes and 16 worker threads. We also fixed racy barrier implementations in several of them. We configured the DaCapo benchmarks to use their default sizes, but we exclude tradebeans and eclipse because of incompatibilities with our underlying framework and other known issues [55]. We additionally exclude several specific methods from the other programs that ROADRUNNER cannot properly instrument because the resulting code would exceed a JVM limit on method size. Several DaCapo programs use reflection heavily. To facilitate building the call graph for those programs in STATICBF and RedCARD, we used a modified version of Tamiflex [7] to eliminate reflection.

Since ROADRUNNER does not support the specialized class loading features used by the DaCapo test harness, we implemented a simplified version of that harness. It runs a target’s workload several times in a warm up phase and then measures the running time for 10 iterations of the workload. We used that harness for the JavaGrande programs as well. We report the means of ten such trials.

We verified all race detection tools examined reported the same races (modulo variations due scheduling) manually. All experiments were performed on a 2.4GHz 16-core AMD Opteron processor with 64GB running Ubuntu Linux and Oracle’s Java HotSpot 64-bit Server VM version 1.8.

6.1 **STATICBF**

BigFoot took 0.16 seconds per method on average to process the benchmark programs, as shown in Table [4]. With careful caching of SMT solver results, only about 10% of this time was spent solving Z3 queries. Together, call graph construction for computing method kill sets and reasoning about heap and boolean constraints accounted for more than half of the running time in most cases. We have focused on implementation simplicity and high precision. More careful tuning would likely lead to significant improvements.

6.2 **DYNAMICBF Time Overhead**

Figure [8] shows, for each program, how many race checks on shadow locations FastTrack (left graph) and BigFoot (middle graph) perform relative to the number of heap accesses. FastTrack performs a check on each access, meaning its check ratio ($\frac{\text{Checks}}{\text{Accesses}}$) is always 1. For BigFoot, the average check ratio is 0.43, and much smaller for some programs, particularly those in which traversals over large arrays are covered by a single coalesced check. BigFoot’s check ratio is also substantially lower than that of RedCARD (0.73), SLIMSTATE (1.0), and SLIMCARD (0.76).

Table [9] shows the base running time for each program and the overhead of each checker. Overhead is the additional time beyond the base time necessary to check a program:

$$\text{CheckerOverhead} = \text{CheckerTime} - \text{BaseTime}$$
Comparison to FastTrack  
BigFoot is significantly faster than the other detectors. As shown in the last column of Table [1] BigFoot incurs only 39% of the overhead of FastTrack. The right-most graph in Figure 8 shows this improvement visually. BigFoot is most effective on programs exhibiting highly-structured access patterns to large data sets, and thus low check ratios, such as crypt, moldyn, montecarlo, and sunflow. Moving checks out of loops and coalescing them accounts for much of this improvement. BigFoot is also effective on programs with many redundant checks that can be eliminated altogether, such as sparse.

It is interesting to note that several programs do not follow the expected trend. For series, the FastTrack overhead of only 1% is mostly due to internal ROADRUNNER bookkeeping, which leaves little opportunity for improvement. The lufact benchmark performs a triangular array computation whose array accesses are readily coalesced by BigFoot, resulting in a small check ratio. However, that triangular pattern is not amenable to our online array state compression algorithm, meaning that the array’s shadow representation becomes fine-grained and each coalesced check reduces many shadow location operations.

In other benchmarks, such as h2 and avrora, bookkeeping for synchronization operations accounts for a greater fraction of checking overhead, diminishing the benefit of optimizing memory operations with BigFoot. The degraded performance for tomcat appears to be caused by higher contention on interal ROADRUNNER data structures when using BigFoot.

Field compression via proxies accounted for about 5% of the savings in general, but over 50% of the savings in raytracer and sunflow.

Comparison to RedCard  
RedCard eliminates one form of redundant check [25], namely checks on accesses where the current thread has already accessed (and checked) that location within the same release-free span. The BigFoot check placement algorithm is able to eliminate other forms of redundancy by both reasoning about anticipated accesses and moving checks. For example, BigFoot can eliminate more redundant checks and move checks out of loops, as shown in Figure 6.

RedCard also performs static proxy analysis, but the array component crucially depends upon globally-computed allocation-site points-to information. As such, RedCard’s static analysis fails to terminate within four hours on many benchmarks, as indicated by the † symbol in Table 1. We use RedCard’s redundancy analysis without proxies for those programs. Moreover, imprecisions in the proxy analysis limit its effectiveness even on small programs.

Overall, the check ratio and overhead reduction for RedCard were 0.73 and 17%, respectively. In contrast, the check ratio and overhead reduction for BigFoot were 0.43 and 61%. BigFoot’s ability to move checks out of loops is key to achieving this improvement, particularly when coupled with dynamic array shadow compression.

Comparison to SlimState  
SlimState introduced the dynamic array compression scheme we use in BigFoot, but its check ratio is 1 because it processes every access at run time. BigFoot offers two crucial improvements: 1) BigFoot eliminates many redundant checks. 2) While SlimState must process every individual array access at run time to build its footprints, BigFoot statically coalesces array checks where possible, thereby reducing the amount of run-time footprint processing and eliminating much of SlimState’s dynamic footprint construction overhead. BigFoot’s overhead is less than half of SlimState’s as a result. Field compression, and moving field checks out of loops, contributes to the performance savings as well.
While we have focused primarily on running time, we also report the target program’s memory requirements, as well as the overheads for each checker in Table 2. Following the methodology of earlier work [55], we measure memory as the smallest heap permitting successful execution of the target program, which we find by iteratively shrinking the JVM’s maximum heap until the program crashes or fails to terminate within thrice the time to run with a 64 GB heap.

**Comparison to SLIMSTATE**  SLIMSTATE’s dynamic array state compression. We did not include static proxy analysis for arrays in SLIMSTATE because integrating the run-time bookkeeping necessary to support static array proxies [25] into SLIMSTATE’s analysis led to worse performance. As a result, SLIMSTATE has an overall check ratio of 76%, which is a few percent higher than REDCARD’s ratio (73%).

As expected, the combined analysis improves upon SLIMSTATE by eliminating many redundant checks and incurs only 70% of FASTTRACK’s overhead. However, SLIMSTATE still experiences the same overheads related to the construction of footprints at run time as SLIMSTATE. Moreover, it cannot move checks out of loops and coalesce them, which are crucial for achieving BigFoot’s much better performance. SLIMSTATE’s memory overhead did not differ significantly from SLIMSTATE’s or BigFoot’s.

### 6.3 DynamicBF Memory Overhead

While we have focused primarily on running time, we also report the target program’s memory requirements, as well as the overheads for each checker in Table 2. Following the methodology of earlier work [55], we measure memory as the smallest heap permitting successful execution of the target program, which we find by iteratively shrinking the JVM’s maximum heap until the program crashes or fails to terminate within thrice the time to run with a 64 GB heap.

**BigFoot, SLIMSTATE, and SLIMSTATE** reduce space overhead by about 26–28% when compared to FASTTRACK. These three tools utilize the same dynamic array compression scheme. SLIMSTATE and BigFoot additionally uses field compression, but while field compression improved time, it did not lead to sizable space reductions. Inspection of the programs for which field compression made the greatest speed difference revealed that there were never sufficiently many objects with compressed fields alive at the same time to sizably impact overall space needs.

The limited impact of static compression on space can also be seen by comparing the space overhead of REDCARD to FASTTRACK. The only fundamental space difference is due to REDCARD’s use of compression for field and array proxies, but again, there is little overall impact.

### 7. Other Related Work

In addition to REDCARD and SLIMSTATE, described earlier, much work has focused on improving the performance of dynamic race detection. Many precise tools, such as...
Many static analyses for identifying races have also been explored, including type-based systems [1, 2, 31], model checking [12, 36, 51], and dataflow analyses [21], as well as whole-program analyses [37, 53]. Many of the mentioned static analyses are unsound by design or unsound in their implementations to reduce the number of spurious warnings (see, e.g., [11, 21]). Their focus on identifying race-free accesses rather than redundant checks also lead to different design choices in terms of precision and scalability.

Gross et al. present a global static analysis to improve the precision and performance of a LockSet-based detector [52]. It is primarily designed to identify objects on which no races can occur and requires global aliasing information, as well as a static approximation of the happens-before graph for the whole program. Moreover, their reliance on an imprecise race detector leads their system to both miss races and report spurious warnings. They also do not support arrays. Choi et al. present a different global analysis for removing runtime race checks for accesses guaranteed to be race-free [14]. Their analysis eliminates some redundant checks via a simple intra-procedural forward analysis.

Properties related to accesses or checks within release-free spans have been used in other settings. For example, the IFRit race detector uses similar insights in its notion of interference-free regions [20], which were originally designed to facilitate compiler optimizations for race-free programs [19]. The IFRit race detector monitors execution and reports a data race when multiple concurrently executing interference-free regions access the same variable. IFRit prioritizes performance over precision, and so may possibly miss races (but nicely guarantees no false alarms). IFRit uses a static analysis to insert and minimize monitor start/stop calls, which is analogous to BigFoot’s check insertion algorithm. BigFoot’s approach necessitates a more complex static analysis to ensure sufficient precision to perform check motion, and so is at a different point in the design space.

Another approach for reducing overheads is to use sampling [8, 20, 22], again with some loss of soundness. Eraser verifies race-freedom for data that is thread-local, read-shared, or lock protected [44], and has been extended to produce fewer false alarms [11, 21, 59, 47, 57].

Several dynamic checkers defer the processing of accesses. RecPlay [43] records all locations accessed within each synchronization-free region and then verifies that concurrent regions access disjoint locations during replay. DRD [17] and ThreadSanitizer [46] similarly buffer accesses but do not infer patterns or compress shadow state. Similar buffering is also common in transactional memory systems [48]. Other work [49] uses a single shadow location for contiguous memory locations accessed within the same critical sections. However, only the first two critical sections accessing a location are considered, resulting in potential false alarms if later accesses are not correlated.

### Table 2. Checker space overhead relative to FASTTrack.

<table>
<thead>
<tr>
<th>Program</th>
<th>Base Mem (MB)</th>
<th>Geo Mean</th>
<th>FT Base</th>
<th>RC FT</th>
<th>SS FT</th>
<th>SC FT</th>
<th>BF FT</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypt</td>
<td>193.76</td>
<td>6.84</td>
<td>(0.97)</td>
<td>(0.04)</td>
<td>(0.04)</td>
<td>(0.04)</td>
<td></td>
</tr>
<tr>
<td>series</td>
<td>22.01</td>
<td></td>
<td>4.45</td>
<td>(1.02)</td>
<td>(0.58)</td>
<td>(0.59)</td>
<td>(0.57)</td>
</tr>
<tr>
<td>lufact</td>
<td>32.15</td>
<td></td>
<td>10.16</td>
<td>(1.00)</td>
<td>(1.10)</td>
<td>(1.10)</td>
<td>(1.11)</td>
</tr>
<tr>
<td>moldyn</td>
<td>16.20</td>
<td></td>
<td>5.44</td>
<td>(0.82)</td>
<td>(0.91)</td>
<td>(0.80)</td>
<td>(0.82)</td>
</tr>
<tr>
<td>montecarlo</td>
<td>622.83</td>
<td></td>
<td>3.67</td>
<td>(1.00)</td>
<td>(0.30)</td>
<td>(0.30)</td>
<td>(0.30)</td>
</tr>
<tr>
<td>sparse</td>
<td>98.11</td>
<td></td>
<td>5.64</td>
<td>(1.01)</td>
<td>(1.44)</td>
<td>(1.05)</td>
<td>(0.79)</td>
</tr>
<tr>
<td>sor</td>
<td>32.12</td>
<td></td>
<td>5.11</td>
<td>(1.00)</td>
<td>(1.40)</td>
<td>(1.40)</td>
<td>(2.48)</td>
</tr>
<tr>
<td>batak</td>
<td>44.74</td>
<td></td>
<td>3.78</td>
<td>(0.99)</td>
<td>(0.75)</td>
<td>(0.95)</td>
<td>(1.00)</td>
</tr>
<tr>
<td>raytracer</td>
<td>16.42</td>
<td></td>
<td>3.67</td>
<td>(0.96)</td>
<td>(0.60)</td>
<td>(0.57)</td>
<td>(0.60)</td>
</tr>
<tr>
<td>tomcat</td>
<td>19.59</td>
<td></td>
<td>4.81</td>
<td>(0.99)</td>
<td>(0.98)</td>
<td>(0.99)</td>
<td>(1.14)</td>
</tr>
<tr>
<td>sunflow</td>
<td>10.42</td>
<td></td>
<td>9.50</td>
<td>(0.91)</td>
<td>(0.93)</td>
<td>(0.88)</td>
<td>(0.86)</td>
</tr>
<tr>
<td>luindex</td>
<td>6.15</td>
<td></td>
<td>16.3</td>
<td>(0.98)</td>
<td>(0.96)</td>
<td>(0.96)</td>
<td>(0.52)</td>
</tr>
<tr>
<td>pmd</td>
<td>30.24</td>
<td></td>
<td>6.02</td>
<td>(1.05)</td>
<td>(1.02)</td>
<td>(1.03)</td>
<td>(1.09)</td>
</tr>
<tr>
<td>flop</td>
<td>28.07</td>
<td></td>
<td>6.35</td>
<td>(1.00)</td>
<td>(0.98)</td>
<td>(0.97)</td>
<td>(0.99)</td>
</tr>
<tr>
<td>lusearch</td>
<td>12.04</td>
<td></td>
<td>7.00</td>
<td>(1.00)</td>
<td>(0.57)</td>
<td>(0.57)</td>
<td>(0.57)</td>
</tr>
<tr>
<td>avrora</td>
<td>2.09</td>
<td></td>
<td>15.22</td>
<td>(1.01)</td>
<td>(1.01)</td>
<td>(1.01)</td>
<td>(1.01)</td>
</tr>
<tr>
<td>jython</td>
<td>24.06</td>
<td></td>
<td>5.97</td>
<td>(1.03)</td>
<td>(0.96)</td>
<td>(0.96)</td>
<td>(1.02)</td>
</tr>
<tr>
<td>xalan</td>
<td>8.20</td>
<td></td>
<td>11.00</td>
<td>(1.00)</td>
<td>(0.84)</td>
<td>(0.84)</td>
<td>(0.82)</td>
</tr>
<tr>
<td>h2</td>
<td>259.71</td>
<td></td>
<td>3.90</td>
<td>(1.06)</td>
<td>(1.10)</td>
<td>(1.10)</td>
<td>(0.72)</td>
</tr>
</tbody>
</table>

DJIT+ [40] use vector clocks [35], which are expensive. FASTTrack introduced epochs [25] to reduce these overheads. A common approach for further reducing overhead is to use a single shadow location for whole arrays and objects [9, 13, 23, 39, 40, 51], although this may generate false alarms, motivating additional technology to see if a reported warning reflects a real race [11, 21].

Another approach for reducing overheads is to use sampling [8, 20, 22], again with some loss of soundness. Eraser verifies race-freedom for data that is thread-local, read-shared, or lock protected [44], and has been extended to produce fewer false alarms [11, 21, 59, 47, 57].

8. Summary

BigFoot leverages our theory of precise check placement to substantially improve the efficiency of dynamic data race detection. This work may enable more wide-spread use of data race detectors, and it opens the door for further studies on statically optimizing dynamic concurrency analyses.

One interesting direction is to extend our techniques to compress memory locations across multiple arrays or objects, which could yield further time and space savings. Another important avenue for future work is to improve StaticCBF’s performance by adapting it to be modular or incremental and by tailoring its data structures and decision procedures to the most common cases encountered in practice.

Acknowledgment

We thank our shepherd Michael Pradel, the anonymous reviewers, Shaz Qadeer, and James Wilcox for their feedback. This work was supported, in part, by NSF Grants 1337278, 1421051, 1421016, and 1439042.
References


We next prove that the check placement algorithm is correct. In particular it inserts checks so that any generated trace has precise checks, and so has a data race if and only if there is a check race detected by DYNAMICBF.

- Appendix A formalizes the operational semantics of BFJ.
- Appendix B shows that a trace with precise checks has a data race if and only if it has a check race.
- Appendix C formalizes a GOODCHECKS judgment that satisfies preservation.
- Appendix D shows that the CHECKPLACEMENT algorithm inserts checks satisfying GOODCHECKS.
- Appendix E shows that the programs satisfying the GOODCHECKS judgment generate traces with precise checks.
- Appendix F shows that correctness of BIGFOOT.
A. Semantics

We specify the operational semantics of BFJ in Figure 9. This semantics evaluates a program by stepping through a sequence of states. Each state $\Sigma$ consists of two components: a heap $S$ and a collection of threads $T$. The heap maps locations to values, where each location $\rho.f$ or $\rho[i]$ combines an address $\rho$ with a field name $f$ or array index $i$. The heap also maps each object address $\rho$ to the thread identifier (or Tid) of the thread holding the object’s lock (or $\bot$ if it is not held). The thread set $T$ maps each thread identifier $t \in Tid$ to a thread state $\langle \sigma, s \rangle$ that combines a statement $s$ with a (thread-local) store $\sigma$ mapping variables in $s$ to values.

In the context of a set of definitions $\overline{D}$, the relation

$$\overline{D} \vdash S \cdot \langle \sigma, s \rangle \longrightarrow^a S' \cdot \langle \sigma', s' \rangle$$

models the effect of a single step by thread $\langle \sigma, s \rangle$ on the heap $S$ and the thread’s local state. The Action $a$ captures the heap operation performed by the step. For example, if thread $t$ accesses location $\rho.f$, $a$ would be $t: acc(\rho.f)$. The special action $t:\epsilon$ indicates that a step has no heap effect.

Figure 9 defines the evaluation rules for each statement. In these rules, the heap $S[\rho.f := v]$ is identical to $S$ except that it maps the location $\rho.f$ to the value $v$. Similar update operations are used on the other state components. For example, $S[\rho := t]$ updates $S$ to indicate that the lock for the object at location $\rho$ is held by $t$. The term $\sigma(e)$ evaluates an expression $e$ using local store $\sigma$ for the values of variables.

The rule [E-CHKSET] unrolls a check on a set of paths to separate checks on each path. The rule [E-CHKINDEX] checks a strided range of array indices by explicitly checking the first index and generating a new check for the remainder of the strided range. Rule [E-CHKEMPY] handles empty strided array indices.

To invoke a method $x = y.m(\tau)$, we first look up the method $m$ in the program definitions. We then construct a substitution $\theta$ that maps 1) $m$’s local variables, which are the free variables of $s$, other than the return result variable $r$, to fresh names, 2) the parameters $\tau'$ to the arguments $\tau$, 3) the self-reference $\text{this}$ to $y$, and 4) the return variable $r$ to $x$. If $s$ is the method body of $m$, $\theta(s)$ may be inserted into the evaluation context surrounding the call without variable capture. Moreover, the result of the call is placed in $x$, as expected.

The relation $\overline{D} \vdash \Sigma \longrightarrow^a \Sigma'$ describes a single step of multithreaded program execution. That rule selects an arbitrary thread $t$ to take a step and updates the global state $\Sigma$ accordingly. As above, $a$ captures the memory or synchronization operation performed by the step. We use the notation $t:,_\Sigma$ to represent an arbitrary action by thread $t$.

The relation $\overline{D} \vdash \Sigma \longrightarrow^\alpha \Sigma'$ denotes the reflexive-transitive closure of $\longrightarrow^a$, where the trace $\alpha$ is a sequence of actions $a_1.a_2\ldots a_n$. Given this definition, $\overline{D} \vdash \Sigma \longrightarrow^\alpha \Sigma'$ models the arbitrary interleaving of the various threads of a multithreaded program $\overline{D}$.

For a program $\overline{D} s_1 || \ldots || s_n$, its initial state is $\Sigma_0 = S_0 \cdot T_0$, where

- $S_0$ maps all locations to null and all addresses to $\bot$; and
- $T_0$ maps each thread $t \in 1..n$ to $\langle \sigma, s_t \rangle$, where $\sigma$ assigns a distinct global address to each free variable in $s_{1..n}$. Thus, free variables in $s_{1..n}$ implicitly denote potentially thread-shared objects.
$\Sigma \in \text{State} ::= S \cdot T$

$S \in \text{Store} = (\text{Location} \to \text{Value}) \cup (\text{Address} \to \text{Tid}_\perp)$

$\rho \in \text{Address}$

$t \in \text{Location} ::= \rho.f \mid \rho[i]$

$t, t \in \text{Tid} ::= 1 \mid 2 \mid \ldots$

$T \in \text{Threads} ::= \text{Tid} \to \langle \sigma, s \rangle$

$\sigma \in \text{Store} = \text{Var} \to \text{Value}$

$v \in \text{Value} ::= \rho \mid \text{true} \mid \text{false} \mid \text{null} \mid i \mid \ldots$

$i \in \text{Nat}$

$\alpha, \beta \in \text{Trace} ::= \overline{\pi}$

$a, b, c, d \in \text{Action} ::= t:\text{acc}(l) \mid t:\text{check}(l) \mid t:\text{acq}(\rho) \mid t:\text{rel}(\rho) \mid t:\varepsilon$

$\overline{D} \vdash \Sigma \rightarrow^a \Sigma'$

$\overline{D} \vdash S \cdot T[t := \langle \sigma, s \rangle] \rightarrow^a S \cdot T[t := \langle \sigma', s' \rangle]$ if $\overline{D} \vdash S \cdot \langle \sigma, s \rangle \rightarrow^a S' \cdot \langle \sigma', s' \rangle$ and $a = t:_-$

$\overline{D} \vdash S \cdot \langle \sigma, \text{check}\{x.f\} \rangle$ if $\sigma(x) = \rho$

$\overline{D} \vdash S \cdot \langle \sigma, \text{check}\{p_1, \ldots, p_n\} \rangle$ if $\sigma(e_1) \geq \sigma(e_2)$

$\overline{D} \vdash S \cdot \langle \sigma, \text{check}\{e_1.e_2.e_3\} \rangle$ if $\rho = \sigma(x), i = \sigma(e_1), i < \sigma(e_2)$

$\overline{D} \vdash S \cdot \langle \sigma, \text{skip}\{s_1.s_2\} \rangle$ if $\sigma(\text{be}) = \text{true}$

$\overline{D} \vdash S \cdot \langle \sigma, \text{if be s}_1 s_2 \rangle$ if $\sigma(\text{be}) = \text{false}$

$\overline{D} \vdash S \cdot \langle \sigma, \text{if be s}_1 s_2 \rangle$ if $\sigma(\text{be}) = \text{true}$

$\overline{D} \vdash S \cdot \langle \sigma, \text{L} \rangle$ if $\sigma(\text{be}) = \text{false}$

$\overline{D} \vdash S \cdot \langle \sigma, \text{x} = y.f \rangle$ if $\sigma(y) = \rho$ and $S(\rho.f) = v$

$\overline{D} \vdash S \cdot \langle \sigma, \text{x} = x \rangle$ if $\sigma(y) = \rho$ and $S(\rho) = v$

$\overline{D} \vdash S \cdot \langle \sigma, \text{acq}(\rho) \rangle$ if $\sigma(y) = \rho$ and $S(\rho) = v$

$\overline{D} \vdash S \cdot \langle \sigma, \text{rel}(\rho) \rangle$ if $\sigma(y) = \rho$ and $S(\rho) = v$

$\overline{D} \vdash S \cdot \langle \sigma, \text{rel}(\rho) \rangle$ if $\sigma(y) = \rho$ and $S(\rho) = v$

$\overline{D} \vdash S \cdot \langle \sigma, \text{x} = \text{new c} \rangle$ if $\rho$ is fresh

$\overline{D} \vdash S \cdot \langle \sigma, \text{x} = \text{new_array z} \rangle$ if $\rho$ is fresh

$\overline{D} \vdash S \cdot \langle \sigma, \text{x} = z \rangle$ if $\sigma(e) = v$

$\overline{D} \vdash S \cdot \langle \sigma, \text{x} = y \rangle$ if $\sigma(e) = v$

$\overline{D} \vdash S \cdot \langle \sigma, \text{x} = y.m(z) \rangle$ if $\sigma(e) = v$

if $m(\overline{z}) \{ s; \text{return } r \} \in \overline{D}$

and $\theta$ maps $\text{TV}(s) \setminus \{ r \}$ to fresh names

and $\theta$ maps $\overline{z}$, this, $r$ to $\overline{z}$, $y$, $x$, respectively.

Figure 9. Semantics and Runtime Values for BFJ.
B. Data Races and Check Races

The *happens-before relation* \(<_\alpha\)* for a trace \(\alpha\) is the smallest transitive-closed relation over the operations in \(\alpha\) such that the relation \(a <_\alpha b\) holds whenever \(a\) occurs before \(b\) in \(\alpha\) and one of the following holds:

- Program order: The two operations performed by the same thread.
- Locking: The two operations acquire or release the same lock.

We introduce the following definitions:

- Two operations are *concurrent* if they are not ordered by happens before.
- Two accesses *conflict* if they access the same location.
- Two checks *conflict* if they check the same location.
- A trace has a *data race* on a location \(l\) if it has a pair of conflicting concurrent accesses to \(l\).
- A trace has a *check race* on a location \(l\) if it has a pair of conflicting concurrent checks on \(l\).

A check \(c = t:\check(l)\) *covers* an access \(a = t:\acc(l)\) if:
- \(c\) precedes \(a\) with no intervening \(t:\rel(l)\).
- \(c\) succeeds \(a\) with no intervening \(t:\acq(l)\).

A check \(c = t:\check(l)\) is *legitimate* for an access \(a = t:\acc(l)\) if:
- \(c\) precedes \(a\) with no intervening \(t:\acq(l)\).
- \(c\) succeeds \(a\) with no intervening \(t:\rel(l)\).

A trace \(\alpha\) has *precise* checks if each access has a covering check and each check is legitimate for some access.

We start with two technical lemmas that show how the notions of covering and legitimate checks constrain the happens-before relation for a trace.

**Lemma 1.** If a trace \(\alpha\) has an access \(a\) with a covering check \(c\) then for any action \(d\) by a different thread in \(\alpha\) we have that:

1. \(c <_\alpha d \Rightarrow a <_\alpha d\)
2. \(d <_\alpha c \Rightarrow d <_\alpha a\)

**Proof.** The check \(c\) can become either before or after the access in \(\alpha\).

- Case Before:
  \(\alpha = \alpha_1.c_\alpha.a_\alpha.\alpha_3\), where \(\alpha_2\) has no releases by thread \(t\) since check \(c\) covers \(a\).
  Program order then shows that \(d <_\alpha c \Rightarrow d <_\alpha a\).
  Since \(\alpha_2\) does not contain a release by thread \(t\), \(c <_\alpha d \Rightarrow a <_\alpha d\).

- Case After:
  \(\alpha = \alpha_1.a_\alpha.\alpha_2.c_\alpha.\alpha_3\), where \(\alpha_2\) has no acquires by \(t\) since check \(c\) covers \(a\)
  By program order \(c <_\alpha d \Rightarrow a <_\alpha d\).
  Since \(\alpha_2\) does not contain an acquire by thread \(t\), \(d <_\alpha c \Rightarrow d <_\alpha a\).

**Lemma 2.** If a trace \(\alpha\) has a check \(c\) that is legitimate for an access \(a\) then for any action \(d\) by a different thread in \(\alpha\) we have:

1. \(a <_\alpha d \Rightarrow c <_\alpha d\)
2. \(d <_\alpha a \Rightarrow d <_\alpha c\)

**Proof.** The proof is similar to the above lemma.

We next show that the notion of covering checks guarantees no missed races (false negatives), and the notion of legitimate checks guarantees no false alarms (false positives).
**Lemma 3.** Let \( l \) be a location and suppose each access to \( l \) in \( \alpha \) has a covering check. If \( \alpha \) has no check race on \( l \) then \( \alpha \) has no data race on \( l \).

**Proof.** Let \( t : \text{acc}(l) \) and \( u : \text{acc}(l) \) be two accesses in \( \alpha \) whose covering checks are not racy. Without loss of generality we assume \( t : \text{check}(l) <_\alpha u : \text{check}(l) \). By Lemma 1(1), \( t : \text{acc}(l) <_\alpha u : \text{check}(l), \) and hence by Lemma 1(2) \( t : \text{acc}(l) <_\alpha u : \text{acc}(l), \) so the accesses are race-free.

**Lemma 4.** Let \( l \) be a location and suppose each check in \( \alpha \) on \( l \) is legitimate for some access. If \( \alpha \) has a check race on \( l \) then \( \alpha \) has a data race on \( l \).

**Proof.** Suppose \( \alpha \) has two race-free accesses \( t : \text{acc}(l) \) and \( u : \text{acc}(l), \) where \( t : \text{acc}(l) <_\alpha u : \text{acc}(l). \) Each access has a covering check \( t : \text{check}(l) \) and \( u : \text{check}(l) \). By Lemma 2(1), \( t : \text{check}(l) <_\alpha u : \text{check}(l) \). By Lemma 2(2), \( t : \text{check}(l) <_\alpha u : \text{check}(l) \).

By combining these ideas of covering and legitimate checks, we prove that a trace with precise checks has a check race if and only if the trace has a data race (and therefore running a dynamic race detector with these checks will report a race if and only if there is a data race).

**Theorem B.1.** Suppose \( \alpha \) has precise checks. Then for all locations \( l, \) \( \alpha \) has a check race on \( l \) if and only if \( \alpha \) has a data race on \( l \).

**Proof.** By the application of Lemma 3 and 4.
C. **GOODCHECKS Judgment**

Studies of type systems typically separate the problems of type inference and type checking. In our setting, we also separate the problems of inferring where to place checks and verifying that check placement is precise. BigFoot’s check placement judgment shown in Figure 7 performs the former; the “good checks” judgment presented in this section performs the latter. We refer to those judgments as **CHECKPLACEMENT** and **GOODCHECKS**, respectively.

The **GOODCHECKS** rules shown in Figure 10 include a subsumption rule [CC-SUB], and so it is not a syntax-directed algorithm like **CHECKPLACEMENT**; instead it is a mathematical definition designed to satisfy the usual preservation property plus other correctness properties discussed below regarding precise race detection.

The **CHECKPLACEMENT** algorithm uses both a history context \( H \) and anticipated context \( A \) to represent the forwards and backwards analysis. **GOODCHECKS** combines these two to form a single context \( \Pi = H \cup A \). We define the entailment relation \( \Pi \vdash h \) from a context \( \Pi = H \cup A \) as simply \( H \vdash h \). The **GOODCHECKS** rules are defined as follows:

- [CC-Skip], [CC-New], and [CC-ANew] do not change the context and always succeed.
- [CC-Assign] adds a new constraint representing the assignment to the post-context.
- [CC-Chk] adds the checked paths \( (C^\vee) \) to the post context. It only succeeds if each path \( p \) to check has already been accessed. This condition prevents false positives by preventing checking locations which have not yet been accessed. We always delay checks and never bring them forward so a location must have been accessed in order to be checked.
- [CC-Read] removes any anticipated accesses to \( y.f \) and adds an access to \( y.f \). Removing the anticipated access is safe because we are adding in an access to the same location.
- [CC-Write] also removes any anticipated accesses to \( y.f \) and adds an access to \( y.f \).
- [CC-ARead] and [CC-AWrite] are similar to the above.
- [CC-Seq] allows for the chaining of two statements with the post-context of the first becoming the pre-context of the second.
- [CC-If] checks both the then and the else branches using the pre-context along with the information gained about \( be \). The resulting post-contexts must match and are used for the post-context of the whole expression. Rule [CC-SUB] below can be used to bring the two post-contexts into alignment.
- [CC-Loop] enters the loop with a context of \( \Pi_{inv} \). Statement \( s_1 \) is checked with this context and produces a new context \( \Pi_1 \cup \{\neg be\} \). Statement \( s_2 \) is then checked with \( \Pi_1 \cup \{\neg be\} \) and produces the post context \( \Pi_{inv} \) which can safely check \( s_1 \). Upon exiting the loop \( s_1 \) has run and the \( be \) is true so the resulting post-context is \( \Pi_1 \cup \{be\} \).
- [CC-AcQ] does not change the context. However, it does check that all accesses in the context have already been checked (as checking them after acquiring the lock may cause a false negative). It also checks that there are no anticipated accesses in the context as in the backward analysis the anticipated accesses can not be safely moved before an acquire.
- [CC-Rel] removes all history information from the context except boolean expressions. We must remove accesses and checks as the checks made so far are only valid while the lock about to be released is held. For every variable that has been accessed but not checked yet there must be an anticipated access in the post context. This constraint allows the delaying of checks outside of critical sections but only when a later access can be guaranteed.
- [CC-Call] does not modify the context and requires that it not contain any items in the kill set of that method. All accesses which may be killed in the method must be checked before the call. We can use [CC-SUB], shown below, to remove checked access that may be killed but we can not use subsumtion to remove unchecked accesses so the analysis remains sound.
- [CC-Sub] allows us to conservatively approximate contexts according to the following context ordering:

\[
(H_1 \cup A_1) \preceq (H_2 \cup A_2) \quad \text{iff} \quad \begin{cases} 
H_1 \supseteq H_2 \\
H_1 \vdash A_1 \subseteq A_2 \\
\forall p^\alpha \in H_1. (H_2 \vdash p^\alpha) \lor (H_1 \vdash p^\vee) \lor (H_2 \bullet A_2 \vdash p^\diamond)
\end{cases}
\]

**Run-Time States** We introduce the rules shown in Figure 11 to extend the **GOODCHECKS** relation to run-time states. The judgment \( \sigma; \alpha \vdash h \) determines when a history property \( h \) holds in a given thread-local store \( \sigma \) of thread \( t \). The execution history \( \alpha \) is used to validate past checks and accesses in \( h \). The judgment \( \sigma; \alpha \vdash \Pi \) extends the previous judgment to contexts, and ensures (via C1) each check in \( \alpha \) has a legitimizing previous access in \( \alpha \), and also each access in \( \alpha \) either 1) has a covering check in \( \alpha \) (via A1 or A2) or 2) the context \( \Pi \) records a corresponding past or anticipated access (via A3).
We assume $x \notin \text{Vars}(\Pi)$ in [CC-New], [CC-Assign], [CC-Read], [CC-ARead], [CC-ANew], [CC-Rename], [CC-Call].

$$\models s : \Pi \rightarrow \Pi'$$

[CC-Skip]
$$\Pi' = \Pi \cup \{x = e\} \quad \models \text{skip} : \Pi \rightarrow \Pi'$$

[CC-Assign]
$$\Pi' = H \cup A \models x = e \text{ : } \Pi \rightarrow \Pi'$$

[CC-Rename]
$$\Pi' = H \cup A \models x := y \rightarrow \Pi'$$

[CC-Chk]
$$\forall p \in C. \Pi \models p^c \models \text{check}(C) : \Pi \rightarrow \Pi \cup C^\vee$$

[CC-New]
$$\models x = \text{new} c : \Pi \rightarrow \Pi$$

[CC-Read]
$$\Pi' = \Pi \setminus \{y.f^\circ \cup \{y.f^c\}\} \models x = y.f : \Pi \rightarrow \Pi'$$

[CC-Write]
$$\Pi' = \Pi \setminus \{y.f^\circ \cup \{y.f^c\}\} \models y.f = x : \Pi \rightarrow \Pi'$$

[CC-ARead]
$$\Pi' = \Pi \setminus \{y.z^\circ \cup \{y.z^c\}\} \models x = y.z : \Pi \rightarrow \Pi'$$

[CC-AWrite]
$$\Pi' = \Pi \setminus \{y.z^\circ \cup \{y.z^c\}\} \models y.z = x : \Pi \rightarrow \Pi'$$

[CC-Seq]
$$\models s_1 : \Pi \rightarrow \Pi_1 \quad \models s_2 : \Pi_1 \rightarrow \Pi_2 \quad \models s_1; s_2 : \Pi \rightarrow \Pi_2$$

[CC-If]
$$\models s_1 : \Pi \cup \{\text{be}\} \rightarrow \Pi' \quad \models s_2 : \Pi \cup \{\neg \text{be}\} \rightarrow \Pi' \quad \models \text{if be} s_1 s_2 : \Pi \rightarrow \Pi'$$

[CC-Loop]
$$\models s_1 : \Pi_{\text{inv}} \rightarrow \Pi_1 \quad \models s_2 : \Pi_1 \cup \{\neg \text{be}\} \rightarrow \Pi_{\text{inv}} \quad \models \text{loop}\{s_1; \text{if be break}; s_2\} : \Pi_{\text{inv}} \rightarrow \Pi_1 \cup \{\text{be}\}$$

[CC-Acq]
$$\forall p. p^\circ \notin \Pi \quad \models \text{acq}(x) : \Pi \rightarrow \Pi$$

[CC-Rel]
$$\forall p. p^\circ \notin \Pi \text{ and } p^\circ \notin \Pi \quad \models \text{rel}(x) : \Pi \rightarrow \Pi$$

[CC-Call]
$$\Pi \cap \text{KillSetHistory}(m) = \emptyset \quad \Pi \cap \text{KillSetAnticipated}(m) = \emptyset \quad \models x = y.m.(\pi) : \Pi \rightarrow \Pi$$

[CC-Sub]
$$\models s : \Pi_1 \rightarrow \Pi_2 \quad \Pi_1 \sqsubseteq \Pi_3 \quad \Pi_3 \sqsubseteq \Pi_2 \quad \models s : \Pi_1 \rightarrow \Pi_2$$

[CC-Method]
$$\models \text{meth}$$

[CC-Program]
$$\forall D \in \overline{D}. \models D \models \text{class} c\{\overline{\text{meth}}\}$$

[CC-Decl]
$$\models s \text{ : } \emptyset \rightarrow \emptyset \quad \models \text{class} c\{\overline{\text{meth}}\}$$

[CC-Method]
$$\forall \text{meth} \in \text{meth}. \models \text{meth}$$

[CC-State]
$$\forall i. \models s_i$$

Figure 10. GoodChecks Rules.

We extend the store $\sigma$ to map paths (used by the static analysis) to sets of locations (used by the dynamic semantics) as follows:

$$\sigma(x.f) = \{\sigma(x).f\}$$
$$\sigma(x[e_1..e_2:e_3]) = \{p[j] : \begin{array}{l} p = \sigma(x), j = \sigma(e_1) + i \sigma(e_3), \\
\sigma(e_1) \leq j < \sigma(e_2) \end{array}\}$$

The rules [CC-Thread] and [CC-State] then extend this well-formedness criteria to threads and states, respectively. Note that [CC-State] does not constraint the heap $S$ in any way, since we do not reason about heap contents statically. If we were to, for example, include alias assumptions in our core analysis, then we would need to ensure that all of our alias assumptions are true for $S$.  

23 2017/0/12
Each $t:\text{check}(l)$ in $\alpha$ is preceded by $t:\text{acc}(l)$ with no intervening $t:\text{rel}(\_)$

Each $t:\text{acc}(l)$ in $\alpha$ is
\begin{align*}
\begin{cases}
\text{preceded by } t:\text{check}(l) \text{ with no intervening } t:\text{rel}(\_)& \quad (A1) \\
\text{followed by } t:\text{check}(l) \text{ with no intervening } t:\text{acq}(\_)& \quad (A2) \\
\text{not followed by } t:\text{acq}(\_) \text{ and } \exists p. (l \in \sigma(p) \text{ and } (p^{\text{c}} \in \Pi \text{ or } p^{\text{c}} \in \Pi))& \quad (A3)
\end{cases}
\end{align*}

$\sigma;\alpha \vdash t \Pi$

\[\forall h \in \Pi. \sigma;\alpha \vdash t h\]

$\sigma;\alpha \vdash t h$

\[\forall l \in \sigma(p). \left( \sigma = \alpha_1.t: \text{acc}(l).\alpha_2 \text{ does not contain } t: \text{rel}(\rho) \right.\]

$\sigma;\alpha \vdash t \rho^{\text{c}}$

\[\sigma;\alpha \vdash t \rho^{\text{p}}\]

\[\sigma;\alpha \vdash t \rho^{\text{c}}\]

\[\sigma;\alpha \vdash t \rho^{\text{p}}\]

\begin{figure}[h]
\centering
\begin{tabular}{|c|c|}
\hline
$\sigma;\alpha \vdash \Sigma$ & $\sigma;\alpha \vdash \langle \sigma, s \rangle$ \\
\hline
\hline
$\forall D \in \mathcal{D}. D \vdash D$ & $\sigma;\alpha \vdash \Pi$ \\
\hline
$\forall t \in \text{Tid}. \mathcal{D};\alpha \vdash_t T(t)$ & $\vdash s : \Pi \rightarrow \emptyset$ \\
\hline
$\mathcal{D};\alpha \vdash \mathcal{S} \cdot \mathcal{T}$ & $\mathcal{D};\alpha \vdash \langle \sigma, s \rangle$ \\
\hline
\end{tabular}
\caption{GOODCHECKS rules for Runtime States.}
\end{figure}
D. Correctness of CHECKPLACEMENT

Any program satisfying the CHECKPLACEMENT judgment will satisfy the GOODCHECKS judgment.

Lemma 5. If $\vdash D s_1 \ldots s_n$ then $\models D s_1 \ldots s_n$.

Proof. Follows from Lemma 6.

Lemma 6. If $\vdash s$ then $\models s$.

Proof. If $\vdash s$ then $s = s'$; check($C$) where $\vdash s' : \emptyset \rightarrow H \bullet \emptyset$ and $C =$ Check($H, \emptyset$) from [STMT]. Hence $\vdash s' : A \rightarrow H$ by Lemma 7, so $\models s : A \rightarrow H \cup C \checkmark$ by [CC-SEQ], and so by [CC-SUB] $\models s : \emptyset \rightarrow \emptyset$, and hence $\models s$.

Lemma 7. If $\vdash s : H \bullet A' \rightarrow H' \bullet A$ then $(\models s : H \cup A' \rightarrow H' \cup A)$.

Proof. By induction on the derivation of $(\vdash s : H \bullet A' \rightarrow H' \bullet A)$ and case analysis on the rule concluding that derivation.

- [Assign] where $s = (x = e)$: In this case we have
  
  $\vdash x = e : H \bullet A[x := e] \rightarrow H \cup \{x = e\} \bullet A$

  where $x \notin \text{Vars}(e, H)$. Rule [CC-ASSIGN] gives us
  
  $\models x = e : H \cup A[x := e] \rightarrow H \cup \{x = e\} \cup A[x := e]$

  Finally, $H \cup A[x := e] \cup \{x = e\} \leq H \cup \{x = e\} \cup A$ by our assumption about entailment, so by [CC-SUB]
  
  $\models x = e : H \cup A[x := e] \rightarrow H \cup \{x = e\} \cup A$

  as required.

- [Rename] where $s = (x \leftarrow y)$: In this case we have
  
  $\vdash x \leftarrow y : H \bullet A[x := y] \rightarrow H[y := x] \bullet A$

  where $x \notin \text{Vars}(H)$. Rule [CC-ASSIGN] gives us the desired
  
  $\models x \leftarrow y : H \cup A[x := y] \rightarrow H[y := x] \cup A$

- [Write] where $s = (y.f = x)$: In this case we have
  
  $\vdash y.f = x : H \bullet A \cup \{y.f\} \rightarrow H \cup \{y.f\} \bullet A$

  Rule [CC-WRITE] gives us
  
  $\models y.f = x : H \cup A \cup \{y.f\} \rightarrow H \cup A \cup \{y.f\}$

- [Read] where $s = (x = y.f)$: In this case we have
  
  $\vdash x = y.f : H \bullet A \searrow x \cup \{y.f\} \rightarrow H \cup \{y.f\} \bullet A$

  Rule [CC-READ] gives us
  
  $\models x = y.f : H \cup A \searrow x \cup \{y.f\} \rightarrow H \cup \{y.f\} \cup A \searrow y.f$

  Finally, $H \cup \{y.f\} \cup A \searrow y.f \leq H \cup \{y.f\} \cup A$ so by [CC-SUB] we reach our desired
  
  $\models x = y.f : H \cup A \searrow x \cup \{y.f\} \rightarrow H \cup \{y.f\} \cup A$
• [SKIP] where \( s = \text{skip} \): Skip does not modify or place restrictions on the context in either GOODCHECKS or CHECKPLACEMENT and so is trivial.

• [NEW] where \( s = (x = \text{new } c) \): In this case we have

\[
\vdash x = \text{new } c : H \cdot A \ x \rightarrow H \cdot A
\]

where \( x \notin \text{Vars}(H) \). Rule [CC-NEW] gives us

\[
\models \vdash x = \text{new } c : H \cup A \ x \rightarrow H \cup A \ x
\]

Finally, \( H \cup A \ x \subseteq H \cup A \) so by [CC-SUB]

\[
\models \vdash x = \text{new } c : H \cup A \ x \rightarrow H \cup A
\]

• [A-NEW], [A-WRITE], and [A-READ] follow the same proofs as [NEW], [WRITE], and [READ].

• [ACQ] where \( s = \text{check}(C) \cdot \text{acq}(x) \): In this case we have

\[
\vdash \text{check}(C) \cdot \text{acq}(x) : H \cdot \emptyset \rightarrow H \cup C^\triangleright \cdot A
\]

where \( C = \text{Checks}(H, \emptyset) \). Rule [CC-CHK] gives us

\[
\models \vdash \text{check}(C) : H \rightarrow H \cup C^\triangleright
\]

and requires that \( \forall p \in C. H \vdash p^\triangleleft \) which holds by the construction of \( C \). Next [CC-Acq] gives us

\[
\models \vdash \text{acq}(x) : H \cup C^\triangleright \rightarrow H \cup C^\triangleright
\]

and requires that \( \forall p, p^\triangleright \notin H \cup C^\triangleright \), which is trivially true, and \( \forall p, p^\triangleleft \in H \cup C^\triangleright \Rightarrow H \cup C^\triangleright \vdash p^\triangleright \) which is true by the construction of \( C \). Finally, \( H \cup C^\triangleright \subseteq H \cup C^\triangleright \cup A \) and so by [CC-SUB] and [CC-SEQ] we have the desired

\[
\models \vdash \text{check}(C) \cdot \text{acq}(x) : H \rightarrow H \cup C^\triangleright \cup A
\]

• [REL] where \( s = \text{check}(C) \cdot \text{rel}(x) \): In this case we have

\[
\vdash \text{check}(C) \cdot \text{rel}(x) : H \cdot A \rightarrow H \setminus \{\_^\triangleright, \_^\triangleleft\} \cdot A
\]

where \( C = \text{Checks}(H, A) \). GOODCHECKS gives us

\[
\models \vdash \text{check}(C) : H \cup A \rightarrow H \cup A \cup C^\triangleright
\]

and requires that \( \forall p \in C. H \vdash p^\triangleleft \) which it does by the construction of \( C \).

\( H \cup A \cup C^\triangleright \subseteq H \setminus \{\_^\triangleright, \_^\triangleleft\} \cup A \) because we will never remove an access \( p^\triangleleft \) where \( p^\triangleright \notin H \cup C^\triangleright \). Thus by [CC-SUB] we have that

\[
\models \vdash \text{check}(C) : H \cup A \rightarrow H \setminus \{\_^\triangleright, \_^\triangleleft\} \cup A
\]

and by [CC-REL] and the fact that \( \forall p, p^\triangleleft \notin H \setminus \{\_^\triangleright, \_^\triangleleft\} \) and \( p^\triangleright \notin H \setminus \{\_^\triangleright, \_^\triangleleft\} \) we have

\[
\models \vdash \text{rel}(x) : H \setminus \{\_^\triangleright, \_^\triangleleft\} \cup A \rightarrow H \setminus \{\_^\triangleright, \_^\triangleleft\} \cup A
\]

Finally, by [CC-SEQ] we have the desired

\[
\models \vdash \text{check}(C) \cdot \text{rel}(x) : H \cup A \rightarrow H \setminus \{\_^\triangleright, \_^\triangleleft\} \cup A
\]
• [Ir] where $s = \text{if be } (s_1; \text{check}(C_1)) (s_2; \text{check}(C_2))$: In this case we have

\[
\vdash \text{if be } (s_1; \text{check}(C_1)) (s_2; \text{check}(C_2)) : H_{in} \bullet A_{in} \rightarrow H_{out} \bullet A_{out}
\]

\[
\vdash s_1 : H_{in} \cup \{be\} \bullet A_{in} \rightarrow H_{1}' \bullet A_{out}
\]

\[
\vdash s_2 : H_{in} \cup \{\neg be\} \bullet A_{in} \rightarrow H_{2}' \bullet A_{out}
\]

\[
C_1 = \text{Checks}(H_{1}', H_{1}' \cap H_{2}', A_{out})
\]

\[
C_2 = \text{Checks}(H_{2}', H_{2}' \cap H_{1}', A_{out})
\]

\[
A_{in} = H_1 \bullet A_1 \cap H_2 \bullet A_2
\]

\[
H_{out} = (H_{1}' \cup C_1') \cap (H_{2}' \cup C_2')
\]

In order to conclude

\[
\vdash \text{if be } (s_1; \text{check}(C_1)) (s_2; \text{check}(C_2)) : H_{in} \cup A_{in} \rightarrow H_{out} \cup A_{out}
\]

We need to show that

\[
\vdash s_1; \text{check}(C_1) : H_{in} \cup A_{in} \cup \{be\} \rightarrow H_{out} \cup A_{out}
\]

\[
\vdash s_2; \text{check}(C_2) : H_{in} \cup A_{in} \cup \{\neg be\} \rightarrow H_{out} \cup A_{out}
\]

By induction, [CC-Chk], and [CC-Seq] we have

\[
\vdash s_1; \text{check}(C_1) : H_{in} \cup A_{in} \cup \{be\} \rightarrow H_{1}' \cup C_1' \cup A_{out}
\]

\[
\vdash s_2; \text{check}(C_2) : H_{in} \cup A_{in} \cup \{\neg be\} \rightarrow H_{2}' \cup C_2' \cup A_{out}
\]

Finally by [CC-Sub]

\[
\vdash s_1; \text{check}(C_1) : H_{in} \cup A_{in} \cup \{be\} \rightarrow H_{out} \cup A_{out}
\]

\[
\vdash s_2; \text{check}(C_2) : H_{in} \cup A_{in} \cup \{\neg be\} \rightarrow H_{out} \cup A_{out}
\]

• [Seq] where $s = s_1; s_2$: This case holds trivial by induction.

• [Call] where $s = (\text{check}(C); x = y.m(\tau))$: In this case we have

\[
\vdash \text{check}(C); x = y.m(\tau) : H \bullet A \rightarrow H' \bullet A'
\]

such that

\[
C = \text{Checks}(H, H \setminus \text{KillSetHistory}(m), A)
\]

\[
= \{p : p^\triangleleft \in H, H \setminus \text{KillSetHistory}(m) \nvdash p^\downarrow, H \bullet A \nvdash p^\triangledown\}
\]

\[
H' = (H \cup C^\triangledown) \setminus \text{KillSetHistory}(m)
\]

\[
A = A' \setminus x \setminus \text{KillSetAnticipated}(m)
\]

By [CC-Check]

\[
\vdash \text{check}(C) : H \cup A \rightarrow H \cup C^\triangledown \cup A
\]

By [CC-Call]

\[
\vdash x = y.m(\tau) : H' \cup A \rightarrow H' \cup A
\]

Also $H' \cup A \preceq H' \cup A'$.

Finally, we need to show

\[
H \cup C^\triangledown \cup A \preceq H' \cup A = (H \cup C^\triangledown) \setminus \text{KillSetHistory}(m) \cup A
\]

and in particular that

\[
\forall p^\triangleleft \in H. H' \vdash p^\downarrow \text{ or } H' \bullet A \vdash p^\triangledown
\]
If \( C^\top \not\vdash p^\top \) then \( H \setminus \text{KillSetHistory}(m) \vdash p^\top \) or \( H \cup C^\top \vdash p^\top \) or \( H^\top A \vdash p^\top \) and so the desired context ordering follows. Hence

\[
\begin{align*}
&\vdash \text{check}(C) : H \cup A \rightarrow H \cup C^\top \cup A \\
&H \cup C^\top \cup A \preceq H^\top A \\
&\vdash x = y.m(z) : H^\top A \rightarrow H^\top A
\end{align*}
\]

and so the desired context ordering follows.

Hence

\[
\models \text{check}(C) : H \cup A \rightarrow H \cup C^\top \cup A
\]

\[
H \cup C^\top \cup A \preceq H^\top A
\]

\[
\vdash x = y.m(z) : H^\top A \rightarrow H^\top A
\]

also, by \([CC-C\text{-}CHK}\),

\[
\models \text{check}(C_{\text{back}}) : H_{\text{back}} \cup A_{\text{inv}} \rightarrow H_{\text{back}} \cup A_{\text{inv}} \cup C_{\text{back}}^\top
\]

Also, \( H_{\text{back}} \cup A_{\text{inv}} \cup C_{\text{back}}^\top \preceq H_{\text{inv}} \cup A_{\text{in}} \). Hence by \([CC-\text{LOOP}]\)

\[
\models \text{check}(C_{\text{in}}); \text{loop\{ s_1; \ if \ break \} ; \text{check}(C_{\text{back}}) \} : H_{\text{inv}} \cup A_{\text{in}} \rightarrow H_{\text{out}} \cup A_{\text{inv}}
\]

this case concludes via \([CC-\text{SEQ}]\) and \([CC-\text{SUB}]\) based on:

\[
\begin{align*}
H_{\text{out}} \cup A_{\text{inv}} &\preceq H_{\text{out}} \cup A_{\text{out}} \\
\models \text{check}(C_{\text{in}}) : H_{\text{in}} \cup A_{\text{in}} \rightarrow H_{\text{in}} \cup A_{\text{in}} \cup C_{\text{in}}^\top \\
H_{\text{in}} \cup A_{\text{in}} \cup C_{\text{in}}^\top &\preceq H_{\text{inv}} \cup A_{\text{in}}
\end{align*}
\]

Assumption 1 (Entailment Assumptions). We rely on the following assumptions about the entailment relationship.

1. \( H \cdot A \vdash p^\top \) is monotonic in \( H \) and \( A \).
2. \( H \vdash h \) is monotonic in \( H \).
3. \( \{ x = e \} \cdot \{ p^\top \} \vdash p[x := e]^\top \)
4. \( \{ x = e \} \cdot \{ p[x := e]^\top \} \vdash p^\top \)
5. \( \{ h \} \vdash h \)
6. \( H \cdot A \vdash p^\top \) only depends on boolean expressions in \( H \)
7. \( \{ x[e_1]^\top, x[(e_1 + e_3) \ldots e_2 : e_3]^\top \} \vdash x[e_1 \ldots e_2 : e_3]^\top \)
E. Correctness of GOODCHECKS

We now show that if a program has passed GOODCHECKS then the program generates traces that have precise checks.

Definition E.1. A state $\Sigma$ is terminated if all threads are $\texttt{skip}$.

Theorem E.1 (Correctness of GOODCHECKS). If $\bar{D};\epsilon \models \Sigma_0$ and $\bar{D} \models \Sigma_0 \rightarrow^\alpha \Sigma'$ and $\Sigma'$ is terminated then $\alpha$ has precise checks.

Proof. By the Preservation Theorem, we have that $\bar{D};\alpha \models \Sigma'$ where $\Sigma' = S \cdot T$. Pick any thread $t$, and let $\langle \sigma, \texttt{skip} \rangle = T(t)$. By $[\text{CC-STATE}]$ and $[\text{CC-THREAD}]$, $\bar{D}; \alpha \models_i \langle \sigma, \texttt{skip} \rangle$ where $\sigma; \alpha \models_i \Pi$ and $\models_i \texttt{skip} : \Pi \rightarrow \emptyset$ for some $\Pi \leq \emptyset$. Hence $[\text{CC-CONTEXT}]$ implies that (from C1) each check by $t$ has a preceding legitimizing access. Moreover, since $\Pi \leq \emptyset$, from the definition of $\leq$ we know that $\Pi$ has no anticipated access, and $\forall p^\exists \in \Pi$ we have that $\Pi \models p^\forall$.

Consider any access $t;\texttt{acc(l)}$ in $\alpha$, which must satisfy one of the antecedents A1, A2, A3 in $[\text{CC-CONTEXT}]$. If the access satisfies A1 or A2, then it clearly has a covering check. If the access satisfies A3, then, since $\Pi$ has no anticipated accesses, $\exists p, \sigma(p) = l$ and $p^\exists \in \Pi$. Then, from above, $\Pi \models p^\forall$, and so by $[\text{CC-PASTCHECK}]$ $\alpha$ contains a check covering the access. Hence, $\alpha$ has precise checks. □

In order to prove the above induction we must prove that evaluation preserves well-formed states.

Theorem E.2 (Preservation). If $\bar{D};\alpha \models \Sigma$ and $\Sigma \rightarrow^\alpha \Sigma'$ then $\bar{D}; (\alpha.a) \models \Sigma'$.

Proof. Suppose the action $a$ is performed by thread $t$. From the rule $[\text{CC-STATE}]$ and the definition of our transition relation, we have:

$$\models D \quad \forall D \in \bar{D}
\bar{D}; \alpha \models_i T(i) \quad \forall i \in \text{Tid}
\Sigma = S \cdot T[i := \langle \sigma, s \rangle]
\Sigma' = S' \cdot T[t := \langle \sigma', s' \rangle]
\bar{D} \models S \cdot (\sigma, s) \rightarrow^a S' \cdot (\sigma', s')$$

In addition, for any thread $T(i) = \langle \sigma_i, s_i \rangle$, rule $[\text{CC-THREAD}]$ requires that there is a $\Pi_i$ such that:

$$\sigma_i; \alpha \models_i \Pi_i
\models_i s_i : \Pi_i \rightarrow \emptyset$$

If $i \neq t$, then an inspection of $[\text{CC-CONTEXT}]$ shows that $\sigma_i; \alpha.a \models_i \Pi_i$, and hence $\bar{D}; (\alpha.a) \models_i T(i)$. For thread $t$, from Lemma 8 below we have that there exists $\Pi_3$ such that

$$\models_i s' : \Pi_3 \rightarrow \emptyset$$
$$\sigma'; \alpha.a \models_i \Pi_3$$

Hence $\bar{D}; (\alpha.a) \models_i \langle \sigma', s' \rangle$. Finally, $\bar{D}; (\alpha.a) \models \Sigma'$ then follows by rule $[\text{CC-STATE}]$. □

To prove the above we must prove preservation for an individual thread step. Given a well formed thread state, if we take one step of evaluation the thread state remains well-formed.

Lemma 8 (Preservation for Statements). If $\forall D \in \bar{D}. \models D$ and $a$ is an action by thread $t$ and

$$\models s : \Pi_1 \rightarrow \Pi_2
\sigma; \alpha \models_t \Pi_1$$
$$\bar{D} \models S \cdot (\sigma, s) \rightarrow^a S' \cdot (\sigma', s')$$

then there exist $\Pi_3$ such that:

$$\models s' : \Pi_3 \rightarrow \Pi_2$$
$$\sigma'; (\alpha.a) \models_t \Pi_3$$

Proof. By induction on the derivation of $\models s : \Pi_1 \rightarrow \Pi_2$ and case analysis on the rule used to conclude that derivation.

- $[\text{CC-IF}]$ where $s = \text{if } \langle s_1, s_2 \rangle$: There are two cases:
  - if $\sigma(\text{be}) = \text{true}$:
    $$s' = s_1, \sigma' = \sigma, a = t: \epsilon$$
    Via Evaluation
    Let $\Pi_3 = \Pi_1 \cup \{\text{be}\}$
    $\sigma; \alpha \models_t \Pi_1$
    Given
    Need to show $\sigma; \alpha \models_t \Pi_1 \cup \{\text{be}\}$ as $\sigma(\text{be}) = \text{true}$
    Need to show $\models s_1 : \Pi_1 \cup \{\text{be}\} \rightarrow \Pi_2$ Shown via $[\text{CC-IF}]$
We must show \( \sigma \).

There are four evaluation rules for \( s \).

- **[CC-Skip]** \( s = \text{rel}(x) \): In this case, 
  \[
  \Pi_2 = \Pi_1 \\
  \forall p. p^\sigma \not\in \Pi_1, p^{\sigma'} \not\in \Pi_1 \\
  s' = \text{skip} \\
  a = t: \text{rel}(p) \\
  \sigma' = \sigma
  \]
  Let \( \Pi_3 = \Pi_1 \). We have \( \vdash s': \Pi_1 \rightarrow \Pi_1 \) via [CC-Skip].

  Since \( \Pi_1 \) does not contain prior accesses or checks, it only contains boolean expressions, and so \( \forall h \in \Pi_1 \) from \( \sigma; \alpha. a \vdash h \) we can conclude \( \sigma; \alpha.a \vdash h \). Also, properties C1, A1, A2, A3 are not invalidated by adding \( a \) to \( \sigma \) so we conclude \( \sigma; \alpha.a \vdash h \) as required.

- **[CC-Acq]** \( s = \text{acq}(x) \): In this case, 
  \[
  \Pi_2 = \Pi_1 \quad \text{Via [CC-Acq]} \\
  \forall p. p^\sigma \not\in \Pi_1 \\
  \forall p. p^\sigma \in \Pi_1 \Rightarrow \Pi_1 \vdash p^{\sigma'} \quad \text{Via [CC-Acq]} \\
  a = t: \text{acq}(p) \\
  s' = \text{skip}, \sigma' = \sigma \quad \text{Via Evaluation} \\
  \]
  Let \( \Pi_3 = \Pi_2 \)
  \[
  \vdash s': \Pi_2 \rightarrow \Pi_2 
  \]
  Shown via [CC-Skip]

  We must show \( \sigma; (\alpha.a) \vdash h, \Pi_1 \).

  For all \( h \in \Pi_2 \), we have \( \sigma; (\alpha) \vdash h \) and hence \( \sigma; (\alpha.a) \vdash h \) as \( a \) is not a release.

  Since \( \Pi_1 \) does not contain any anticipated access, the requirements C1, A2, A2, A3 on \( \alpha \) also hold for \( \alpha.a \). Hence \( \sigma; (\alpha.a) \vdash h, \Pi_1 \).

- **[CC-Chk]** \( s = \text{check}(C) \)

  There are four evaluation rules for \( s \).

  - **[E-ChkField]** \( s = \text{check}(\{x.f\}) \).
    
    In this case, 
    \[
    s' = \text{skip}, \sigma' = \sigma \quad \text{Via Evaluation} \\
    a = t: \text{check}(\sigma(x).f) \quad \text{Via Evaluation} \\
    \Pi_1 \vdash x.f^\sigma \quad \text{Via [CC-Chk]} \\
    \Pi_2 = \Pi_1 \cup \{x.f^\nu\} \quad \text{Via [CC-Chk]} \\
    \]
    Let \( \Pi_3 = \Pi_2 \)
    \[
    \vdash s': \Pi_2 \rightarrow \Pi_2 \quad \text{Via [CC-Skip]} 
    \]
    It remains to show \( \sigma; \alpha.a \vdash h, \Pi_2 \).

    Clearly \( \sigma; \alpha.a \vdash x.f^\nu \) and \( \sigma; \alpha.a \vdash h \).

    Since we are adding \( t: \text{check}(\sigma(x).f) \) to \( \alpha \), we need to show by C1 there was a \( t: \text{acq}(\sigma(x).f) \) in \( \alpha \) with no later release, which is already guaranteed by \( \sigma; \alpha \vdash x.f^\sigma \).

    Hence we conclude \( \sigma; \alpha.a \vdash h, \Pi_2 \).

  - **[E-ChkSet]** \( C = \{p_1, \ldots, p_n\} \).
    
    In this case, 
    \[
    s' = \text{check}(\{p_1\}) \ldots \text{check}(\{p_n\}) \quad \text{Via Evaluation} \\
    \sigma' = \sigma \quad \text{Via Evaluation} \\
    a = t; \epsilon \quad \text{Via Evaluation} \\
    \]
    Let \( \Pi_3 = \Pi_1 \)
    
    From \( \vdash \vdash s': \Pi_1 \rightarrow \Pi_2 \) we clearly have \( \vdash s': \Pi_1 \rightarrow \Pi_2 \) and \( \sigma; \alpha.a \vdash h, \Pi_1 \).

  - **[E-ChkEmpty]** \( C = x[e_1 \ldots e_2; e_3] \) and \( \sigma(e_1) \geq \sigma(e_2) \).

    We have
\( s' = \text{skip} \quad \text{Via Evaluation} \)
\( \sigma' = \sigma \quad \text{Via Evaluation} \)
\( a = t: \epsilon \quad \text{Via Evaluation} \)
\( \Pi_2 = \Pi_1 \cup \{x[e_1..e_2]!v\} \quad \text{Via [CC-CHECK]} \)

Let \( \Pi_3 = \Pi_2 \)
\( \vdash s' : \Pi_2 \rightarrow \Pi_2 \quad \text{Via [CC-Skip]} \)

We need to show \( \sigma; a.a \vdash \Pi_2 \), which reduces to showing \( \sigma; a.a \vdash x[e_1..e_2]!v \), which holds via [CC-PASTCHECK] as \( \sigma(x[e_1..e_2]!v) \) is empty.

• [E-CHECKINDEX] where \( C = \{x[e_1..e_2]!v\} \).

We have
\( \rho = \sigma(x) \quad \text{Via Evaluation} \)
\( i = \sigma(e_1) \quad \text{Via Evaluation} \)
\( i < \sigma(e_2) \quad \text{Via Evaluation} \)
\( s' = \text{check}(\{x[(e_1 + e_3)..e_2!v]\}) \quad \text{Via Evaluation} \)
\( \sigma' = \sigma \quad \text{Via Evaluation} \)
\( a = t:\text{check}(\rho[i]) \quad \text{Via Evaluation} \)
\( \Pi_2 = \Pi_1 \cup \{x[e_1..e_2]!v\} \quad \text{Via [CC-CHECK]} \)

Let \( \Pi_3 = \Pi_1 \cup \{x[e_1]!v\} \)

Clearly \( \sigma; a.a \vdash x[e_1]!v \).

Since we are adding check \( a \) to the trace, we need to show by C1 there was a corresponding access \( t:\text{acc}(\rho[i]) \) in \( \alpha \) with no later release, which is already guaranteed by \( \sigma; a.\alpha \vdash x[e_1..e_2]!v \).

Hence we conclude \( \sigma; a.a \vdash x[e_1..e_2]!v \).

Also, we have \( \vdash s' : \Pi_1 \cup \{x[e_1]!v\} \rightarrow \Pi_1 \cup \{x[e_1]!v\} \cup \{x[e_1 + e_3..e_2]!v\} \) via [CC-CHECK], which via [CC-SUB] gives \( \vdash s' : \Pi_3 \rightarrow \Pi_2 \) as required.

• [CC-CALL] where \( s = (x = y.m(\bar{x})) \): In this case,
\( \overline{D} \vdash m(\overline{x})\{s_m; \text{return } r\} \quad \text{Via [CC-CALL]} \)
\( x \notin \text{Vars}(\Pi_1, e) \quad \text{Via Evaluation} \)
\( s' = \theta(s_m) \quad \text{Via Evaluation} \)
\( \theta = \{x' = z, \text{this} = y, r = x\} \quad \text{Via [CC-CALL]} \)
\( \Pi \cap \text{KillSetHistory}(m) = \emptyset \quad \text{Via [CC-CALL]} \)
\( \Pi \cap \text{KillSetAnticipated}(m) = \emptyset \quad \text{Via [CC-CALL]} \)
\( \sigma' = \sigma, a = t: \epsilon \quad \text{Via Evaluation} \)

Let \( \Pi_3 = \Pi_1 = \Pi_2 = \Pi \)

Need to show \( \sigma; a.a \vdash \Pi \)

Need to show \( \vdash s_m : \Pi \rightarrow \Pi \)
\( \vdash \theta(s_m) : \emptyset \rightarrow \emptyset \quad \text{Via Lemma 10} \)
\( \vdash s_m : \emptyset \cup \Pi \rightarrow \emptyset \cup \Pi \quad \text{Via Lemma 9} \)

• [CC-LOOP] where \( s = L \):
\( L = \text{loop}\{s_1; \{\text{if } b \text{ break } \}; s_2\} \)
\( s' = s_1; \text{if } b \text{ break } \{s_2; L\} \quad \text{Via Evaluation} \)
\( \sigma' = \sigma, a = t: \epsilon \quad \text{Via Evaluation} \)
\( \Pi' = \Pi_2 \setminus \{b\} \quad \text{Via Evaluation} \)
\( \vdash s_1 : \Pi_1 \rightarrow \Pi' \quad \text{Via [CC-LOOP]} \)
\( \vdash s_2 : \Pi' \cup \{\neg b\} \rightarrow \Pi_1 \quad \text{Via [CC-LOOP]} \)

Let \( \Pi_3 = \Pi_1 \)

Need to show \( \sigma; a.a \vdash \Pi_1 \)

\( \Pi_2 = \Pi_1 \cup \{b\} \quad \text{Via [CC-LOOP]} \)

Need to show \( \vdash s' : \Pi_1 \rightarrow \Pi' \cup \{b\} \)
\( \vdash L : \Pi_1 \rightarrow \Pi' \cup \{b\} \quad \text{Given} \)
\( \vdash s_2 : L : \Pi' \cup \{\neg b\} \rightarrow \Pi' \cup \{b\} \quad \text{Via [CC-SEQ]} \)
\( \vdash \text{skip} : \Pi' \cup \{b\} \rightarrow \Pi' \cup \{b\} \quad \text{Via [CC-Skip]} \)
\( \vdash \text{if be skip} (s_2; L) : \Pi' \rightarrow \Pi' \cup \{\neg b\} \quad \text{Via [CC-SEQ] and [CC-SUB]} \)
\( \vdash s' : \Pi_1 \rightarrow \Pi' \cup \{b\} \quad \text{Via [CC-SEQ]} \)
• [CC-Seq] where $s = s_1; s_2$: There are two cases:
  
  - If $s_1 = \text{skip}$:
    
    $S' = s_2, \sigma' = \sigma, a = t: e$ \hspace{1cm} Via Evaluation
  
    Let $\Pi_3 = \Pi_1$
  
    Need to show $\vdash s_2 : \Pi_1 \rightarrow \Pi_2$ \hspace{1cm} Shown via [CC-SEQ]
  
    Need to show $\sigma; \alpha \vdash t \Pi_1$ \hspace{1cm} Given
  
  - If $s_1 \neq \text{skip}$:
    
    $D \vdash S \cdot \langle \sigma, s_1 \rangle \rightarrow^a S' \cdot \langle \sigma', s_1' \rangle$ \hspace{1cm} Via Evaluation
  
    $\vdash s_1 : \Pi_1 \rightarrow \Pi'$ \hspace{1cm} Via [CC-SEQ]
  
    $\vdash s_2 : \Pi' \rightarrow \Pi_2$ \hspace{1cm} Via [CC-SEQ]
  
    $\sigma; \alpha \vdash t \Pi_1$ \hspace{1cm} Given
  
    $\vdash s_1' : \Pi_4 \rightarrow \Pi'$ \hspace{1cm} Via inductive hypothesis
  
    $\vdash \sigma; \alpha.a \vdash t \Pi_4$ \hspace{1cm} Via inductive hypothesis
  
    Let $\Pi_3 = \Pi_4$
  
    Need to show $\sigma; \alpha.a \vdash t \Pi_4$ \hspace{1cm} Shown via induction above
  
    Need to show $\vdash s_1'; s_2 : \Pi_3 \rightarrow \Pi_2$ \hspace{1cm} Shown via application of [CC-SEQ]

• [CC-Read] where $s = (x = y.f)$:
  
  $\Pi_2 = (\Pi_1 \setminus \{y.f^\triangleright\}) \cup \{y.f^\triangleright\}$ \hspace{1cm} Via [CC-Read]
  
  $x \not\in \text{Vars}(\Pi_1,e)$
  
  $s' = \text{skip}, \sigma' = \sigma[x := v], v = S(\sigma(y.f))$ \hspace{1cm} Via Evaluation
  
  Let $\Pi_3 = \Pi_2$
  
  Need to show $\vdash s' : \Pi_2 \rightarrow \Pi_2$ \hspace{1cm} Shown via [CC-Skip]
  
  $a = t: \text{acc}(y.f)$ \hspace{1cm} Via Evaluation
  
  Need to show $\sigma'; (\alpha.a) \vdash t \Pi_3$ \hspace{1cm} Shown via application of [CC-SEQ]

All actions in $\alpha$ proved by $A3$ are still proved because we have removed $y.f^\triangleright$ but added in $y.f^\triangleright$. Clearly $\sigma; \alpha.a \vdash t y.f^\triangleright$. $\alpha$ is proved by $A3$ because $y.f^\triangleright \in \Pi_3$. All history properties in $\Pi_1$ remain proved in $\sigma'$ as $x \not\in \text{Vars}(\Pi_1)$.

• [CC-Write] where $s = (y.f = x)$:
  
  $\Pi_2 = \Pi_1 \setminus \{f, y.f^\triangleright\} \cup \{x, y.f\}$ \hspace{1cm} Via [CC-Write]
  
  $s' = \text{skip}, \sigma' = \sigma$ \hspace{1cm} Via Evaluation
  
  Let $\Pi_3 = \Pi_2$
  
  Need to show $\vdash s' : \Pi_2 \rightarrow \Pi_2$ \hspace{1cm} Shown via [CC-Skip]
  
  $a = t: \text{acc}(y.f)$ \hspace{1cm} Via Evaluation
  
  Need to show $\sigma'; (\alpha.a) \vdash t \Pi_2$ \hspace{1cm} Shown via application of [CC-SEQ]

All actions in $\alpha$ proved by $A3$ are still proved because we have removed $y.f^\triangleright$ but added in $y.f^\triangleright$. Those proved by $A1$, $A2$, and $C1$ do not change because we have not changed $\alpha$. Clearly $\sigma; \alpha.a \vdash t y.f^\triangleright$. $a$ is proved by $A3$ because $y.f^\triangleright \in \Pi_3$.

• [CC-Assign] where $s = (y[z] = x)$: The proof is similar to above.

• [CC-New] where $s = (x = \text{new } c)$:
  
  $\Pi_2 = \Pi_1$ \hspace{1cm} [CC-New]
  
  $x \not\in \text{Vars}(\Pi_1,e)$
  
  $\sigma' = \sigma[x := \rho]$ \hspace{1cm} Via Evaluation
  
  $s' = \text{skip}, a = t: e$ \hspace{1cm} Via Evaluation
  
  Let $\Pi_3 = \Pi_2$
  
  Need to show $\vdash s' : \Pi_2 \rightarrow \Pi_2$ \hspace{1cm} Shown via [CC-Skip]
  
  Need to show $\sigma'; \alpha \vdash t \Pi_1$ \hspace{1cm} Given

• [CC-ANew]: The proof is similar to above.

• [CC-Assgn] where $s = (x = e)$:
  
  $s' = \text{skip}, \sigma' = \sigma[x := v], a = t: e, v = \sigma(e)$ \hspace{1cm} Via Evaluation
  
  $x \not\in \text{Vars}(\Pi_1,e)$
  
  $\Pi_2 = \Pi_1 \cup \{x = e\}$ \hspace{1cm} Via [CC-Assgn]
  
  Let $\Pi_3 = \Pi_2$
  
  Need to show $\vdash s' : \Pi_2 \rightarrow \Pi_2$ \hspace{1cm} Shown via [CC-Skip]
  
  Need to show $\sigma'; \alpha \vdash t \Pi_1 \cup \{x = e\}$ \hspace{1cm} Shown via what is given and the new constraint is true based on $\sigma'$
Theorem F.1. Proof. By induction on the derivation of \( \Pi \). Let \( \Pi = \Pi_2 \)

Need to show \( \Pi' \). Shown via \( \Pi \) and case analysis on the rule used to conclude that derivation.

- \( \Pi' \) : Var

- \( \Pi' \) : Var

A release kills past checks and acquires, so \( \forall \Pi \) and \( \forall \Pi' \) as required.

- \( \Pi' \) : Var

- \( \Pi' \) : Var

A requirement involving subterms are proved by induction. The only remaining requirements are proved because \( \Pi_1 \) is a permutation on variables, then \( \Pi \) and case analysis on the rule used to conclude that derivation.

- \( \Pi' \) : Var

- \( \Pi' \) : Var

Lemma 9 (Extension). If \( \Pi \) : \( \Pi_1 \rightarrow \Pi_2 \) and \( \Pi' \) : \( \Pi \setminus \text{KillSetHistory}(s) \setminus \text{KillSetAnticipated}(s) \) then \( \Pi \) : \( \Pi_1 \rightarrow \Pi_2 \).

Proof. Proof is by induction on the derivation of \( \Pi \). By Theorem E.1, the rule still holds as the resulting \( \Pi_f \) is greater than the original.

Lemma 10 (Substitution). If \( \Pi \) : \( \Pi_1 \rightarrow \Pi_2 \) and \( \theta : \text{Var} \rightarrow \text{Var} \) is a permutation on variables, then \( \Pi \) : \( \Pi_1 \rightarrow \Pi_2 \).

Proof. Proof is by induction on the derivation of \( \Pi \). By Theorem E.1, the rule still holds as the resulting \( \Pi_f \) is greater than the original.
Proof. By definition, \( T_0 \) maps each \( t \in 1..n \) to \( \langle \sigma, s_t \rangle \), where \( \text{Dom}(\sigma) = FV(s_1) \cup \ldots \cup FV(s_n) \). Since \( \vdash P \) can only be derived via [CC-PROG], it must be that \( \forall D \in \overline{D}. \vdash D \). Also, we have that \( \sigma; \epsilon \vdash t \emptyset \) via [CC-CTX]. Consider any \( t \). Since \( \vdash P \), we know that \( \vdash s_t \) via [PROGRAM], which implies that \( \vdash s_t \) via Lemma. This is only derivable via rule [CC-STM], which means that \( \vdash s : \emptyset \rightarrow \emptyset \). From the above, rule [CC-THREAD] allows us to conclude that \( D; \epsilon \vdash t \langle \sigma, s_t \rangle \). It then follows from rule [CC-STATE] that \( D; \epsilon \vdash \Sigma \).

\( \square \)