

Data Race Detection by Digest-Driven Abstract Interpretation (Extended Version)

Michael Schwarz¹  and Julian Erhard^{2,3} 

¹ National University of Singapore, Singapore
m.schwarz@nus.edu.sg

² Technische Universität München, Garching, Germany
³ Ludwig-Maximilians-Universität München, Munich, Germany
julian.erhard@tum.de



Abstract. Sound static analysis can prove the absence of data races by establishing that no two conflicting memory accesses can occur at the same time. We repurpose the concept of *digests* — summaries of computational histories originally introduced to bring tunable concurrency-sensitivity to thread-modular value analysis by abstract interpretation, extending this idea to race detection: We use digests to capture the conditions under which conflicting accesses may not happen in parallel. To formalize this, we give a definition of data races in the thread-modular local trace semantics and show how exclusion criteria for potential conflicts can be expressed as digests. We report on our implementation of digest-driven data race detection in the static analyzer GOBLINT, and evaluate it on the Sv-COMP benchmark suite. Combining the lockset digest with digests reasoning on thread *ids* and thread joins increases the number of correctly solved tasks by more than a factor of five compared to lockset reasoning alone.

Keywords: data races, concurrency, static program analysis, software verification, abstract interpretation

1 Introduction

Data races happen when the same data is accessed by two different threads, the accesses are unordered, and at least one access is a write. As data races and any bugs they may trigger do not manifest deterministically, finding them by testing is exceedingly difficult. For this reason, many dynamic [19, 32, 37, 39, 41, 48] and static [18, 20, 26, 30, 38, 49] analyses have been proposed, with some of the latter [12, 13, 16, 28, 34, 50] building on abstract interpretation [14].

Showing data race freedom amounts to proving at least one of two properties for each pair of accesses where at least one is a write. Either

- (a) a separation in space (accesses go to different data); or
- (b) a separation in time (accesses are not concurrent)

```

1   main:
2     init(a);
3     g = 0;
4     create(t1);
5     lock(a);
6     g = 5;
7     unlock(a);
8   t1:
9     lock(a);
10    g = 12;
11    unlock(a);

```

Fig. 1. Multi-threaded program with thread prototypes `main` and `t1`.

is to be established. Here, we propose a novel framework for property (b) and a principled way of designing new abstractions of it.

Example 1. Consider the program in Figure 2 with thread prototypes `main` and `t1`. It uses the mutex `a` for synchronization. The mutex is first initialized by `main`. Later, `main` creates a thread from prototype `t1`. There are two write-accesses to the global variable `g` in `main`, and one in `t1`. While the access to `g` in line 3 is unprotected, i.e., `a` is not held, it occurs before `t1` is created. Thus, the program is still single-threaded at that time and the access does not race with any other access. The accesses in lines 6 and 10 do not race as both are protected by `a`. \square

Example 1 illustrates that one has to rely on different forms of reasoning to establish race freedom. Sometimes, the program is still in single-threaded mode for an access, sometimes the set of mutexes overlaps. In other cases, two writes from the same thread prototype can be shown to not race because only one unique instance of that thread prototype is created. Here, we introduce a framework that captures all these different types of arguments. Conceptually,

- (a) we associate with each access an abstraction of the execution history leading up to the access from some set \mathcal{A} of *digests*. Locksets, thread *ids*, and whether the program is single-threaded all are (rather coarse) history abstractions.
- (b) we introduce, for each global `g`, a predicate $(||_g^?) : \mathcal{A} \rightarrow \mathcal{A} \rightarrow \{\text{false}, \top\}$ which checks whether two accesses with respective digests may happen in parallel. While `false` indicates that the accesses may definitely not happen in parallel, \top indicates that either such accesses may happen in parallel, or that the analyzer cannot exclude that they may based on digests alone. Whenever the definition does not depend on `g`, we write $||^?$ — omitting the index.

Example 2. For a digest tracking locksets, one can, irrespective of the global, set

$$A_a ||^? A_b = \begin{cases} \text{false} & \text{if } A_a \cap A_b \neq \emptyset \\ \top & \text{otherwise} \end{cases}$$

to capture that accesses with overlapping locksets do not happen in parallel. \square

As a semantic foundation for our framework, we build on the *local trace semantics* [21, 43, 45, 46] which is a concrete semantics which, for each thread, tracks only *relevant* history information. While commonly some sort of interleaving semantics [29] is used to characterize multi-threaded programs, the local trace semantics as an equivalent, but thread-modular concrete semantics, is

better-suited to our approach, as digests also take a thread-modular view of the execution history.

Previous work [46] introduced the notion of *digests* as a way to track relevant history information in a thread-modular way to make value analyses by abstract interpretation more precise. In this way, one obtains *families* of abstract interpretations parametrized by digests which offer a configurable degree of what was later dubbed *concurrency-sensitivity* [43]. However, neither of these works addresses data races. We take on this gap and repurpose digests for data race detection. The existing digest-driven abstract interpretation framework provides a notion of *admissibility* for instances of digests from which the soundness of analyses refined by such an instance directly follows. Here, we enhance this framework with a predicate $\parallel_g^?$ as discussed above and show how a first definition of such a predicate can automatically be derived from an admissible digest.

Our proposed framework does not only drastically simplify reasoning about race freedom by decoupling the base analysis from the admissibility of the digests, but also provides the conceptual foundation for our existing implementation of data race detection in the successful static analyzer GOBLINT.

The rest of the paper is structured as follows: Section 2 recalls the local trace semantics and its abstract interpretation, whereas Section 3 recalls digests and introduces the notion of *access stability*. Section 4 proposes two definitions of data races, one closely aligned with intuition and one more directly amenable to abstraction, and establishes their equivalence. Section 5 formally introduces the predicate $\parallel_g^?$ and its soundness requirements, before showing how a definition can automatically be derived and how bespoke definitions can sometimes be more precise. Section 6 presents our digest-driven race detection algorithm, whereas Section 7 reports on experiments within the static analyzer GOBLINT. Section 8 outlines related work, with Section 9 describing future work and concluding.

2 Local Trace Semantics and Its Abstract Interpretation

Thread-modular abstract interpretation scales as it avoids considering all possible interleavings. Traditional concrete semantics, on the other hand, distinguish all interleavings. This disconnect renders soundness proofs of thread-modular analyses cumbersome. The local trace semantics [21, 43, 45, 46], which has been shown equivalent to the interleaving semantics w.r.t. safety properties [21], embraces thread-modularity already at the level of the concrete semantics:

- Instead of considering interleavings and hence total orders, the local trace semantics considers a *partial order* of actions. Other than actions within one thread, only relevant actions are ordered, namely those where information flows between threads as is, e.g., the case for locking and unlocking mutexes.
- A local trace corresponds to the *local perspective* of one thread. It only contains those parts of the computational history that the thread can have knowledge about: This includes its own past as well as those parts of the past of other threads that it has learned about by communicating. Such

communication happens via pairs of *observable* and *observing actions*, such as unlocking and locking some specific mutex.

At an observing action (e.g., locking a mutex), the observed local trace (e.g., one ending in an unlock of the same mutex) is incorporated into the local trace of the observing thread and the result prolonged to record the observing action having taken place. At this step, only *compatible* local traces can be incorporated. Abstract interpretations of the local trace semantics track values for program points and for observable actions and thus share the rough structure with the concrete semantics [45, 46] allowing for scalable analyses that enjoy modular soundness proofs. Abstractions of the aforementioned compatibility of local traces are a key ingredient for making thread-modular abstract interpretation and, as we show in this paper, data race detection more precise.

Local Traces. More concretely, a local trace consists of several swimlanes, one for each thread appearing in the trace, which records a sequence of thread-local configurations attained by this thread. Such thread-local configurations record, e.g., the values of *local* variables and the current program point of the thread, but crucially no information about the global state, such as values of global variables. The order of configurations within one swimlane is the program order of the corresponding thread. Additionally, some dependencies between thread-local configurations are recorded. Such dependencies may, e.g., be between the action creating a thread⁴ and the first configuration of the resulting thread, or between unlock and lock operations of the same mutex. We call the union of all such dependencies and the program orders the causality order, and demand that it is acyclic and has a unique maximal element. This unique maximal configuration belongs to one thread —the *ego thread*— whose perspective is taken.

Example 3. Consider the program in Figure 2, for now ignoring any annotations. Figure 3 shows an example local trace for this program, with the last appearing configuration of the ego thread highlighted by a thicker border. □

The program in Figure 2 is a variant of the one from Figure 1 where all accesses to the global variable g are surrounded by an additional mutex m_g , its so-called *atomicity mutex*. In fact, this is how the local trace semantics enforces a sequential-consistency-like property for accesses to global variables. Let \mathcal{G} the set of global variables. Then, any access χ to a global $g \in \mathcal{G}$ (we allow accesses of the form $x = g$ and $g = x$ to copy the value of a global g from/to a local variable x), is immediately preceded by locking the atomicity mutex for g and immediately followed by unlocking it, i.e., it occurs as the sequence $\text{lock}(m_g); \chi; \text{unlock}(m_g)$. This allows conveniently treating accesses to global variables as local actions — with all communication happening via locking and unlocking atomicity mutexes. We will outline in Section 4 how this assumption interacts with the goal of detecting data races.

⁴ For technical reasons relating to the use of creation histories as concrete thread *ids* in prior work, the dependency is from the last configuration of the creating thread before the create action to the first configuration of the created thread.

	MT-dig.	Lockset-dig.		MT-dig.	Lockset-dig.
1 main :	ST _{main}	∅	13 t1 :	MT	∅
2 init(a) ;	ST _{main}	∅	14 lock(a) ;	MT	{a}
3 init(m_g) ;	ST _{main}	∅	15 lock(m_g) ;	MT	{a, m_g }
4 lock(m_g) ;	ST _{main}	{ m_g }	16 g = 12 ;	MT	{a, m_g }
5 g = 0 ;	ST _{main}	{ m_g }	17 unlock(m_g) ;	MT	{a}
6 unlock(m_g) ;	ST _{main}	∅	18 unlock(a) ;	MT	∅
7 create(t1) ;	MT _{main}	∅			
8 lock(a) ;	MT _{main}	{a}			
9 lock(m_g) ;	MT _{main}	{a, m_g }			
10 g = 5 ;	MT _{main}	{a, m_g }			
11 unlock(m_g) ;	MT _{main}	{a}			
12 unlock(a) ;	MT _{main}	∅			

Fig. 2. Multi-threaded program from Figure 1 enhanced with the atomicity mutex m_g required by the local trace semantics. All program locations are annotated using the MT-digest (see Figure 4) and the lockset-digest (see Figure 6).

More formally, let \mathcal{N} denote the set of all program points. We consider disjoint, uniquely labeled, control flow graphs where each control flow graph corresponds to the prototype of a thread. Control flow graphs consist of nodes corresponding to program points and edges $(u, \text{act}, v) \in \mathcal{E}$ where $u, v \in \mathcal{N}$ and act is from some set $\mathcal{A}ct$ of actions. This set of actions is given as the disjoint union of the sets of observing, observable, local, and creating actions. Each control-flow graph has exactly one start node which has no incoming edges. We identify the label of a control flow graph with its start node. One of the control-flow graphs is labeled **main**. It represents the main thread with which execution starts.

Let us call the set of all local traces \mathcal{T} . Within \mathcal{T} , there is a subset $\text{init} \subset \mathcal{T}$ of local traces consisting only of an initial configuration of the main thread at its initial program point u_0 .

An instantiation of the local trace semantics to some set of actions then provides for each edge (u, act, v) a function $\llbracket(u, \text{act}, v)\rrbracket$ prolonging a local trace with the corresponding action, where possible. For non-observing actions, $\llbracket(u, \text{act}, v)\rrbracket$ has type $\mathcal{T} \rightarrow 2^{\mathcal{T}}$ where the returned set is either a singleton or empty.⁵ This corresponds to extending the local trace with the action act when possible. For example, extending a local trace t along an edge originating at some program point u is only possible if t ends in u . For an observing action act , $\llbracket(u, \text{act}, v)\rrbracket$ has type $\mathcal{T} \rightarrow \mathcal{T} \rightarrow 2^{\mathcal{T}}$, where the returned set is again either empty or a singleton. When $\llbracket(u, \text{act}, v)\rrbracket t_0 t_1$ returns a non-empty set, the local traces t_0 and t_1 are said to be *compatible* w.r.t. the edge (u, act, v) and each other. In particular, to be compatible, t_1 must end in an observable action whose type matches the ones observed by act . Depending on the type of observing action, additional requirements have to be fulfilled. For instance, the operations corresponding to locking

⁵ This is purely for technical reasons. Constructs such as non-deterministic assignment remain possible, as CFGs can have several outgoing edges per node.

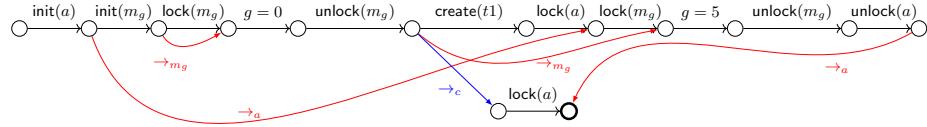


Fig. 3. Stylized local trace of the program in Figure 2, where the ego thread is the single instance of $t1$, which completes its first action `lock(a)`. The black arrows indicate the order of configurations within a thread. The red arrows indicate an ordering between two configurations that is mediated via a `unlock/init` and `lock` of a certain mutex. The blue arrow indicates the order between a configuration of a thread creating another thread and the first configuration of the newly created thread.

and unlocking some mutex a need to be totally ordered. For edges corresponding to the creation of new threads, which are of the form $(u_1, \text{create } u', u_2)$, we additionally require a function $\text{new} : \mathcal{T} \rightarrow \mathcal{N} \rightarrow \mathcal{N} \rightarrow 2^{\mathcal{T}}$; $\text{new } t \ u_1 \ u'$ computes from a local trace t ending in u_1 the local trace of the newly created thread starting its execution at u' , provided such a thread creation is possible at this edge.

Instantiation. While we avoid fixing the set of observable, observing, and local actions to remain general, we will fix subsets to give examples. We then have, in addition to thread creates as described above, the following actions:

- The observing action `lock(a)`, and the observable actions `unlock(a)` and `init(a)`, for each mutex a from the set of mutexes \mathcal{S} . We require $\{m_g \mid g \in \mathcal{G}\} \subseteq \mathcal{S}$, i.e., atomicity mutexes for all global variables are included in the set of mutexes.
- As local actions, we have at least $x = g$ and $g = x$ to copy values between local variables and globals. We call either an *access* to g .

Consider again the local trace in Figure 3 which originates from the program in Figure 2. This local trace belongs to thread $t1$ as evidenced by the maximal element being a configuration of that thread. Of particular interest are the locking orders \rightarrow_a and \rightarrow_{m_g} for mutexes a and m_g , which illustrate additional conditions that need to hold in local traces: In the lock order \rightarrow_a for each mutex a , every lock must be preceded by exactly one unlock of a or be the first lock of a in which case it is preceded by `init(a)`. Each unlock and init operation of a must be directly followed by at most one lock operation. Some further requirements on these orders are detailed in previous work [42].

Fixpoint Formulation. While the set \mathcal{T} of local traces can be characterized as the least fixpoint obtained when, starting from `init`, applying the functions $[\cdot]$ and `new` to all (pairs of) local traces and taking the union with `init`, a different—but equivalent [42, 43]—view is more conducive to static analysis: Here, one considers the least solution of a constraint system with several constraint system variables,

called *unknowns*. One such unknown is introduced for each program point, and for each observable action. An unknown $[u]$ associated with a program point u collects all local traces ending in u . For each observable action act an unknown $[\text{act}]$ collects all local traces ending with this action. When lifting $\llbracket \cdot \rrbracket$ and new point-wise to sets, the resulting constraint system takes the following form:

$$[u_0] \supseteq \text{init} \quad (1)$$

$$[u'] \supseteq \text{new}([u_1], u_1, u'), \text{ for } (u_1, \text{create } u', u_2) \in \mathcal{E} \quad (2)$$

$$[u_2] \supseteq \llbracket (u_1, \text{act}, u_2) \rrbracket ([u_1]), \text{ for } (u_1, \text{act}, u_2) \in \mathcal{E}, \text{ act not observing} \quad (3)$$

$$[\text{act}] \supseteq \llbracket (u_1, \text{act}, u_2) \rrbracket ([u_1]), \text{ for } (u_1, \text{act}, u_2) \in \mathcal{E}, \text{ act observable} \quad (4)$$

$$[u_2] \supseteq \llbracket (u_1, \text{act}, u_2) \rrbracket ([u_1], [\text{act}']), \text{ for } (u_1, \text{act}, u_2) \in \mathcal{E}, \text{ act observing, } \text{act}' \text{ observed by act} \quad (5)$$

For edges labelled with an observable action, there are two constraints: Constraints (3) propagate sets of resulting local traces to the unknown corresponding to the control-flow successor, whereas constraints (4) ensure that the resulting local traces are recorded at the unknown corresponding to the observable action.

Abstract Interpretation. To set up an abstract interpretation, it suffices to let unknowns range over values from a suitable abstract domain \mathcal{D} instead of over $2^{\mathcal{T}}$ and replace functions $\llbracket \cdot \rrbracket$, init , and new with suitable abstract counterparts $\llbracket \cdot \rrbracket^\sharp$, init^\sharp , and new^\sharp . Adapting constraints (1) to (5) in this way, one obtains the abstract constraint system. For simplicity, we assume that \mathcal{D} is a complete lattice with least element \perp (denoting unreachability), greatest element \top , and that \sqcup is used to denote the join (binary least-upper-bound). Furthermore, we require a monotonic concretization function $\gamma_{\mathcal{D}} : \mathcal{D} \rightarrow 2^{\mathcal{T}}$. An analysis is *sound* when $\llbracket \cdot \rrbracket^\sharp$, init^\sharp , and new^\sharp are sound abstractions (w.r.t. $\gamma_{\mathcal{D}}$) of their concrete counterparts. Our considerations in this paper are generic in the base analysis and abstract domain. We assume that it is sound but do not provide details.

3 Digests as Concurrency-Sensitivity

Digests [42, 43, 46] are a way to refine abstract interpretations of multi-threaded programs to yield more precise results. Unknowns are split according to an abstraction of the computational past (the *digest*). Then, the abstract value at each unknown only describes those local traces that agree w.r.t. the digest. This approach can be understood as a generalization of trace partitioning [25, 33, 35, 40] to a multi-threaded setting. It offers a convenient way to specify which aspects of the computational history to consider and what to abstract away.

Digests exploit that, when at observing actions different views about the computational past are combined, some views are known to be incompatible already after considering their abstraction as given in the digest alone. These combinations then do not need to be considered by the analysis. Technically, digests

overapproximate the concrete trace compatibility: If two digests are *incompatible*, so are all traces they represent. However, the reverse does not necessarily hold: digests may be compatible when the corresponding traces are, in fact, not.

More formally, let \mathcal{A} be a set and $\alpha_{\mathcal{A}} : \mathcal{T} \rightarrow \mathcal{A}$ a function to extract such information from a local trace t , we refer to $\alpha_{\mathcal{A}} t$ as its *digest*. We require that for each observable action $\text{act} \in \mathcal{A}_{\text{act}}$, there is a function $[\![\text{act}]\!]_{\mathcal{A}}^{\sharp} : \mathcal{A} \rightarrow \mathcal{A} \rightarrow 2^{\mathcal{A}}$ overapproximating the set of resulting digests of traces obtained by executing act . Similarly, for non-observable actions act and functions $[\![\text{act}]\!]_{\mathcal{A}}^{\sharp} : \mathcal{A} \rightarrow 2^{\mathcal{A}}$. More formally, for an edge $e = (u, \text{act}, v)$ we require

$$\begin{aligned} \forall t_0, t_1 \in \mathcal{T} : \alpha_{\mathcal{A}}([\![e]\!](t_0, t_1)) &\subseteq [\![\text{act}]\!]_{\mathcal{A}}^{\sharp}(\alpha_{\mathcal{A}} t_0, \alpha_{\mathcal{A}} t_1) & (\text{act observable}) \\ \forall t_0 \in \mathcal{T} : \alpha_{\mathcal{A}}([\![e]\!](t_0)) &\subseteq [\![\text{act}]\!]_{\mathcal{A}}^{\sharp}(\alpha_{\mathcal{A}} t_0) & (\text{act non-observable}) \end{aligned} \quad (6)$$

where $\alpha_{\mathcal{A}}$ is lifted element-wise to sets. Intuitively, this corresponds to $[\![\cdot]\!]_{\mathcal{A}}^{\sharp}$ soundly overapproximating $[\![\cdot]\!]$. Additionally, we require $[\![\text{act}]\!]_{\mathcal{A}}^{\sharp}$ to be deterministic, i.e., to either yield an empty set of digests or a singleton set:⁶

$$\begin{aligned} \forall A_0, A_1 \in \mathcal{A} : |[\![\text{act}]\!]_{\mathcal{A}}^{\sharp}(A_0, A_1)| &\leq 1 & (\text{act observable}) \\ \forall A_0 \in \mathcal{A} : |[\![\text{act}]\!]_{\mathcal{A}}^{\sharp}(A_0)| &\leq 1 & (\text{act non-observable}) \end{aligned} \quad (7)$$

As an abstract counterpart for `new`, we require a function $\text{new}_{\mathcal{A}}^{\sharp} : \mathcal{A} \rightarrow \mathcal{N} \rightarrow 2^{\mathcal{A}}$ that returns for a thread starting execution at program point u_1 the digest of this new trace. We once again require determinism in the sense discussed above.

$$\forall t_0 \in \mathcal{T} : \alpha_{\mathcal{A}}(\text{new } t_0 u u_1) \subseteq \text{new}_{\mathcal{A}}^{\sharp}(\alpha_{\mathcal{A}} t_0) u_1 \quad \forall A_0 \in \mathcal{A} : |\text{new}_{\mathcal{A}}^{\sharp} A_0 u_1| \leq 1 \quad (8)$$

Furthermore, we require that whenever there is a successor digest for the edge corresponding to creating a new thread, there is also an appropriate digest for the newly created thread, i.e.,

$$[\![\text{create}(u_1)]!]_{\mathcal{A}}^{\sharp}(A_0) \neq \emptyset \implies \text{new}_{\mathcal{A}}^{\sharp} A_0 u_1 \neq \emptyset \quad (9)$$

For the initial digest at program start, we define:

$$\text{init}_{\mathcal{A}}^{\sharp} = \{\alpha_{\mathcal{A}} t \mid t \in \text{init}\} \quad (10)$$

Deviating from earlier work, we here additionally require a property called *access stability*, which intuitively states that executing an access sequence of the form $\text{lock}(m_g); x = g; \text{unlock}(m_g)$ or $\text{lock}(m_g); g = x; \text{unlock}(m_g)$ does not affect the digest, whenever it is defined. More formally, consider a sequence $\bar{\chi}$ consisting of an access χ (read or write) to a global g and locking and unlocking the atomicity mutex m_g . For such *access sequences* of the form $(v_0^i, \text{lock}(m_g), v_1^i) \cdot (v_1^i, \chi, v_2^i) \cdot (v_2^i, \text{unlock}(m_g), v_3^i)$, we define the effect on the digest by

$$[\![\bar{\chi}]\!]_{\mathcal{A}}^{\sharp}(A_0, A_1) = \left([\![\text{unlock}(m_g)]!]_{\mathcal{A}}^{\sharp} \circ [\![\chi]\!]_{\mathcal{A}}^{\sharp} \circ [\![\text{lock}(m_g)]!]_{\mathcal{A}}^{\sharp} \right)(A_0, A_1).$$

⁶ This assumption simplifies reasoning about digests. To lift this restriction, one can instead consider *abstract digests* [43] where digests come from (complete) lattices. As (normal) digests are already quite expressive, we stick with them here for simplicity.

Here, composition is lifted to return \emptyset when an intermediate computation does so, and we identify singleton sets of resulting digests with their members. We call a digest *access stable*, if for all access sequences $\bar{\chi}$ we have

$$\forall A_0 \in \mathcal{A} : \bigcup_{A_1 \in \mathcal{A}} \llbracket \bar{\chi} \rrbracket_{\mathcal{A}}^{\sharp} (A_0, A_1) \subseteq \{A_0\}. \quad (11)$$

Definition 1. A set \mathcal{A} together with functions $\llbracket \text{act} \rrbracket_{\mathcal{A}}^{\sharp}$, $\text{new}_{\mathcal{A}}^{\sharp}$, and $\text{init}_{\mathcal{A}}^{\sharp}$ is called *digest*. If properties (6) - (10) hold for a digest, it is called *admissible*. If property (11) also holds, the digest is also called *access stable*.

We remark that the question of admissibility is independent of the used analysis and the abstract domain, and is tied to the concrete semantics only. We take the freedom to refer to both the structure such as in Definition 1 as well as to an element of its set \mathcal{A} as a *digest*, as the meaning is clear from the context.

A digest then gives rise to a refined abstract constraint system where each of the unknowns is split into several unknowns, corresponding to the different digests associated with the reaching traces: Each unknown $[u]$ for a program point u is replaced with unknowns $[u, A]$ for $A \in \mathcal{A}$, and each unknown $[\text{act}]$ for an observable action act is replaced with unknowns $[\text{act}, A]$ for $A \in \mathcal{A}$.

The refined constraint system then takes the following form:

$$\begin{aligned} [u_0, A_0] &\sqsupseteq \text{init}_{\mathcal{A}}^{\sharp} && (\text{for } A_0 \in \text{init}_{\mathcal{A}}^{\sharp}) \\ [u_2, A'] &\sqsupseteq \llbracket (u_1, \text{act}, u_2) \rrbracket_{\mathcal{A}}^{\sharp} ([u_1, A_0]) && (\text{for } (u_1, \text{act}, u_2) \in \mathcal{E}, \text{act not observing,} \\ &&& A' \in \llbracket \text{act} \rrbracket_{\mathcal{A}}^{\sharp} A_0) \\ [\text{act}, A'] &\sqsupseteq \llbracket (u_1, \text{act}, u_2) \rrbracket_{\mathcal{A}}^{\sharp} ([u_1, A_0]) && (\text{for } (u_1, \text{act}, u_2) \in \mathcal{E}, \text{act observable,} \\ &&& A' \in \llbracket \text{act} \rrbracket_{\mathcal{A}}^{\sharp} A_0) \\ [u_2, A'] &\sqsupseteq \llbracket (u_1, \text{act}, u_2) \rrbracket_{\mathcal{A}}^{\sharp} ([u_1, A_0], [\text{act}', A_1]) && (\text{for } (u_1, \text{act}, u_2) \in \mathcal{E}, \\ &&& \text{act observing, act' observed by act, } A' \in \llbracket \text{act} \rrbracket_{\mathcal{A}}^{\sharp} (A_0, A_1)) \\ [u', A'] &\sqsupseteq \text{new}_{\mathcal{A}}^{\sharp} ([u_1, A_0], u_1, u') && (\text{for } (u_1, \text{create } u', u_2) \in \mathcal{E}, A' \in \text{new}_{\mathcal{A}}^{\sharp} A_0 u'). \end{aligned}$$

We quickly state the main soundness theorem for such refined analyses:

Proposition 1. Refining a sound analysis with an admissible digest yields a sound refined analysis.

Proof (Sketch). The proof proceeds by first proving a refined version of the concrete semantics sound w.r.t. the original semantics and then showing that the refined analysis is sound w.r.t. the refined semantics, provided the original analysis is sound w.r.t. the original semantics (see [42, Chapter 2.3] and [43]). \square

Consider the local trace semantics with the actions described in the previous section. We provide a first example digest for this setting.

Example 4. A lightweight thread *id* digest may track for each thread whether

$$\begin{aligned}
\mathcal{A} &= \{\text{ST}_{\text{main}}, \text{MT}_{\text{main}}, \text{MT}\} \\
\text{init}_{\mathcal{A}}^{\sharp} &= \{\text{ST}_{\text{main}}\} & \llbracket \text{create } u_0 \rrbracket_{\mathcal{A}}^{\sharp} M &= \begin{cases} \{\text{MT}\} & \text{if } M = \text{MT} \\ \{\text{MT}_{\text{main}}\} & \text{otherwise} \end{cases} \\
\text{new}_{\mathcal{A}}^{\sharp} M u_1 &= \{\text{MT}\} & \llbracket \text{act} \rrbracket_{\mathcal{A}}^{\sharp} M &= \{M\} & (\text{other non-observing}) \\
&& \llbracket \text{lock}(a) \rrbracket_{\mathcal{A}}^{\sharp} (M_0, M_1) &= \begin{cases} \emptyset & \text{if } M_0 = \text{ST}_{\text{main}} \wedge M_1 \neq \text{ST}_{\text{main}} \\ \{M_0\} & \text{otherwise} \end{cases}
\end{aligned}$$

Fig. 4. Digest for lightweight thread *ids*.

- it is the main thread and has not started any other threads (ST_{main}), or
- it is the main thread and has started other threads (MT_{main}), or
- it is some other thread (MT).

The corresponding definitions are given in Figure 4. $\llbracket \text{lock}(a) \rrbracket_{\mathcal{A}}^{\sharp}$ exploits that if the digest for the ego thread is ST_{main} , i.e., the ego thread is the main thread and has not created other threads yet, it cannot acquire a mutex from another thread (with the MT digest) or from itself already having created threads (with the MT_{main} digest). Thus, in these cases, it yields \emptyset . However, the result of $\llbracket \text{lock}(a) \rrbracket_{\mathcal{A}}^{\sharp} (\text{MT}_{\text{main}}, \text{ST}_{\text{main}})$ cannot be set to \emptyset , as the last unlock of the mutex a can in fact have happened while the main thread was single-threaded, even if further threads were created in the meantime. This digest is *access stable*. \square

Example 5. Consider the program in Figure 2. The MT-digests reachable after each statement is executed are annotated. Here, for each program point only one digest is reachable. Reasoning about data races using digests, we will later be able to conclude that line 5 does not race with either of the other accesses. \square

Remark 1. By setting $\mathcal{D} = \{\bullet\}$ with $\gamma_{\mathcal{D}}(\bullet) = \mathcal{T}$, one obtains a trivially sound analysis. In this way, one can analyze a program using only digests for reasoning.

4 Races in Terms of Local Traces

To arrive at techniques for checking data races that are based on a thread-modular abstract interpretation of the local trace semantics, we first precisely define what exactly constitutes a race in the context of the local trace semantics.

We first make the following observation about the atomicity mutexes we have introduced: In race-free programs, any two conflicting accesses are ordered w.r.t. each other. Thus, the extra edges and dependencies introduced in the local trace semantics for atomicity mutexes only serve to make transitive dependencies between conflicting accesses in race-free executions explicit. Additionally, an ordering between read operations is introduced. However, as both orderings of these reads are considered, and executions only differing in the order in which such reads are performed are indistinguishable, all executions are still captured. In fact, by virtue of having atomicity mutexes, the local trace semantics assigns

a meaning even to executions which would not traditionally have one, as they contain races.

To detect whether two accesses are racy, it thus suffices to check whether these appear in any local trace such that they are unordered but for their special atomicity mutex, leading to the following definition:

Definition 2 (Racy Accesses). *Let g be a global variable and χ_a and χ_b be two accesses to g . Accesses χ_a and χ_b are racy if at least one is a write and there exists a local trace in which these accesses are unordered w.r.t. each other when not considering the order provided by the m_g mutex.*

A local trace containing a racy access to g is visualized in Figure 5.

While this definition corresponds closely to the intuition, it does not directly lend itself to abstraction. We thus provide an alternative definition that can be given in terms of the functions $\llbracket \cdot \rrbracket$ of the local trace semantics, which is better amenable to abstraction, and prove them equivalent.

The latter definition builds on the following observation: When accesses are unordered when ignoring the m_g mutexes, one can, from a local trace containing both accesses and ending in one of them, construct a local trace where the order of these accesses is flipped.

We first introduce some helpful notation: Consider once again an access sequence $\bar{\chi} \equiv (v_0, \text{lock}(m_g), v_1) \cdot (v_1, \chi, v_2) \cdot (v_2, \text{unlock}(m_g), v_3)$ where χ is an access to the global g (either read or write). We, akin to the definition of $\llbracket \bar{\chi} \rrbracket_A^\sharp$, denote by $\llbracket \bar{\chi} \rrbracket(t_0, t_1)$ the function $(\llbracket (v_2, \text{unlock}(m_g), v_3) \rrbracket \circ \llbracket (v_1, \chi, v_2) \rrbracket \circ \llbracket (v_0, \text{lock}(m_g), v_1) \rrbracket)(t_0, t_1)$ with composition lifted to return \emptyset when an intermediate computation does so.

Definition 3 (Bidirectional Compatibility). *We call two access sequences $\bar{\chi}_a$ and $\bar{\chi}_b$ for a global g bidirectionally (trace) compatible if*

$$\exists t_a, t_b, t_l \in \mathcal{T} : (\llbracket \bar{\chi}_b \rrbracket(t_b, \llbracket \bar{\chi}_a \rrbracket(t_a, t_l)) \neq \emptyset) \wedge (\llbracket \bar{\chi}_a \rrbracket(t_a, \llbracket \bar{\chi}_b \rrbracket(t_b, t_l)) \neq \emptyset),$$

i.e., both orders of accesses are possible.

Here, t_l corresponds to the local trace ending in the last unlock of m_g before the pair of considered accesses (or the initialization if no accesses have happened yet), whereas t_a corresponds to the local trace ending in the last action of the thread performing $\bar{\chi}_a$ before the pair of considered accesses, and conversely for t_b and $\bar{\chi}_b$. It thus remains to relate the two definitions:

Theorem 1. *Two access sequences for a global variable g — at least one of which corresponds to a write — are bidirectionally compatible if and only if the accesses are racy.*

Proof. We consider the two directions separately:

- (\Rightarrow) Consider two bidirectionally compatible access sequences $\bar{\chi}_a$ and $\bar{\chi}_b$, with at least one a write. Then, $\exists t_a, t_b, t_l \in \mathcal{T} : \llbracket \bar{\chi}_b \rrbracket(t_b, \llbracket \bar{\chi}_a \rrbracket(t_a, t_l)) \neq \emptyset$. Let us call the trace in this set t' . By the construction of the actions for locking atomicity

mutexes, the two accesses in t' are unordered safe for the m_g mutexes and any program order edges (as these are the only edges introduced). For the accesses to be ordered by program order edges, both access would have to belong to the same thread, as program order edges are thread-local. However, in this case we would have $\llbracket \bar{\chi}_a \rrbracket(t_a, \llbracket \bar{\chi}_b \rrbracket(t_b, t_l)) = \emptyset$, as the access $\bar{\chi}_a$ would already appear in t_b . Thus, the accesses are unordered safe for m_g mutexes and thus racy.

- (\Leftarrow) Consider two racy accesses χ_a and χ_b of g . At least one is a write and there exists a local trace t in which these accesses are unordered safe for the m_g mutexes. Consider the subtrace ending in the second access. The accesses in this subtrace remain unordered safe for the m_g mutexes. We prolong this trace by appending the unlock operation of m_g . This yields another trace, say t' , in which the accesses remain unordered safe for the m_g mutexes. t' now contains sequences $\bar{\chi}_a, \bar{\chi}_b$ corresponding to accesses to g and locking and unlocking m_g .

Then, let the subtrace of t' ending in the last program point preceding the access sequence of the thread performing the first access be called t_a and conversely for t_b and the second access. Furthermore, let t_l denote the subtrace ending in the last $\text{unlock}(m_g)$ before either of these access sequences or in $\text{init}(m_g)$ if no such unlock exists. Then, $\llbracket \bar{\chi}_b \rrbracket(t_b, \llbracket \bar{\chi}_a \rrbracket(t_a, t_l)) = t'$ and $\llbracket \bar{\chi}_a \rrbracket(t_a, \llbracket \bar{\chi}_b \rrbracket(t_b, t_l))$ also yields a local trace, as both t_a and t_b originate from the same computation, $\llbracket \bar{\chi}_b \rrbracket(t_b, t_l)$ ends in $\text{unlock}(m_g)$, and there are no requirements enforcing a particular order of $\bar{\chi}_a$ and $\bar{\chi}_b$. Thus, $\bar{\chi}_b$ and $\bar{\chi}_a$ are bidirectionally compatible. \square

Thus, both definitions coincide.

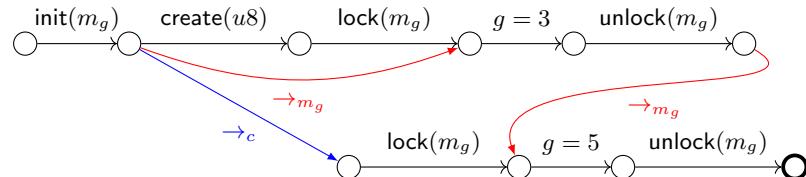


Fig. 5. An example local trace of a racy program.

Remark 2. Unlike in many other definitions, the local trace semantics assigns meaning even to executions past their first racy access, assuming sequential consistency. Thus, the local trace semantics has a notion of traces containing multiple races. However, our notion of how program execution continues *after the first race* need not coincide with other notions: For instance, *garbled* writes are not considered in the local trace semantics. A semantics that allows for such garbled writes may then disagree with the local trace semantics on races that happen after the first race.

5 Races in Terms of Digests

With the previous section having established bidirectional trace compatibility as a key ingredient to a formal definition of data races in the local trace semantics, we now turn to the question of designing sound abstractions of bidirectional trace compatibility that can be used in practical analyses. To this end, we introduce for each digest a family of new (commutative) predicates

$$(\parallel_g^?) : \mathcal{A} \rightarrow \mathcal{A} \rightarrow \{\text{false}, \top\}$$

which is meant to express whether two accesses to global g associated with the respective digests can happen in parallel. Here, `false` means that two accesses with these digests can definitely not happen in parallel, whereas \top means that this cannot be excluded.⁷

We tie this definition directly to the definition of bidirectional trace compatibility (Definition 3). We call $\parallel_g^?$ *sound* if for all traces t_a, t_b, t_l and sequences $\bar{\chi}_a$ and $\bar{\chi}_b$ of accesses to some global g as above, the following implication holds:

$$\begin{aligned} \emptyset \neq [\bar{\chi}_b](t_b, [\bar{\chi}_a](t_a, t_l)) \wedge \emptyset \neq [\bar{\chi}_a](t_a, [\bar{\chi}_b](t_b, t_l)) \\ \implies (\alpha_{\mathcal{A}} t_a) \parallel_g^? (\alpha_{\mathcal{A}} t_b) = \top \end{aligned} \quad (12)$$

5.1 Bidirectional Digest Compatibility

A natural question arises: Can we soundly derive a predicate $\parallel_g^?$ for any admissible, access stable digest? To this end, we first define the notion of *bidirectional digest compatibility*:

Definition 4. Sequences $\bar{\chi}_a$ and $\bar{\chi}_b$ corresponding to accesses to a global g are called *bidirectionally digest compatible* if

$$\begin{aligned} \exists A_a, A_b, A_l \in \mathcal{A} : \\ \left([\bar{\chi}_b]_{\mathcal{A}}^\#(A_b, [\bar{\chi}_a]_{\mathcal{A}}^\#(A_a, A_l)) \neq \emptyset \right) \wedge \left([\bar{\chi}_a]_{\mathcal{A}}^\#(A_a, [\bar{\chi}_b]_{\mathcal{A}}^\#(A_b, A_l)) \neq \emptyset \right). \end{aligned} \quad (13)$$

Theorem 2. *Bidirectional trace compatibility implies bidirectional digest compatibility.*

Proof. By repeated application of the properties of digests (Eqs. (6) and (7)), and $\alpha_{\mathcal{A}}$ being total. \square

We remark that the opposite direction does not hold: (13) holding for two sequences $\bar{\chi}_a$ and $\bar{\chi}_b$ does not imply that these sequences are in fact bidirectionally trace compatible, as the digests (by design) introduce an overapproximation.

With this insight, we can now give a definition of the predicate $\parallel_g^?$ for admissible and *access stable* digests.

⁷ As the digests are an overapproximation, they do not generally carry enough information to determine that two accesses can definitely happen in parallel.

$$\begin{array}{ll}
\mathcal{A} = 2^S & \llbracket \text{lock}(a) \rrbracket_{\mathcal{A}}^{\sharp} (S_0, S_1) = \begin{cases} \emptyset & \text{if } a \in S_0 \\ \{S_0 \cup \{a\}\} & \text{otherwise} \end{cases} \\
\text{init}_{\mathcal{A}}^{\sharp} = \{\emptyset\} & \\
\text{new}_{\mathcal{A}}^{\sharp} S u_1 = \{\emptyset\} & \\
\llbracket \text{act} \rrbracket_{\mathcal{A}}^{\sharp} S = \{S\} \text{ (other non-observing)} & \llbracket \text{unlock}(a) \rrbracket_{\mathcal{A}}^{\sharp} S = \begin{cases} \emptyset & \text{if } a \notin S \\ \{S \setminus \{a\}\} & \text{otherwise} \end{cases} \\
\llbracket \text{act} \rrbracket_{\mathcal{A}}^{\sharp} (S_0, S_1) = \{S_0\} \text{ (other observing)} &
\end{array}$$

Fig. 6. Right-hand sides for lockset digest [43].

Proposition 2. *For an access stable and admissible digest \mathcal{A} , the definition*

$$A_a \parallel_g^? A_b = \begin{cases} \text{false} & \text{if } \llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp} (A_a, A_b) = \emptyset \vee \llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp} (A_b, A_a) = \emptyset \\ \top & \text{otherwise} \end{cases}$$

is sound.

Proof. This amounts to showing Eq. (12). Consider two bidirectionally compatible access sequences $\bar{\chi}_a$ and $\bar{\chi}_b$ and traces t_a , t_b , and t_l such that

$$(\llbracket \bar{\chi}_b \rrbracket(t_b, \llbracket \bar{\chi}_a \rrbracket(t_a, t_l)) \neq \emptyset) \wedge (\llbracket \bar{\chi}_a \rrbracket(t_a, \llbracket \bar{\chi}_b \rrbracket(t_b, t_l)) \neq \emptyset).$$

Let $A_a = \alpha_{\mathcal{A}} t_a$, $A_b = \alpha_{\mathcal{A}} t_b$, and $A_l = \alpha_{\mathcal{A}} t_l$. By the properties of digests (Eqs. (6) and (7)), also

$$\emptyset \neq \llbracket \bar{\chi}_b \rrbracket_{\mathcal{A}}^{\sharp} (A_b, \llbracket \bar{\chi}_a \rrbracket_{\mathcal{A}}^{\sharp} (A_a, A_l)) \wedge \emptyset \neq \llbracket \bar{\chi}_a \rrbracket_{\mathcal{A}}^{\sharp} (A_a, \llbracket \bar{\chi}_b \rrbracket_{\mathcal{A}}^{\sharp} (A_b, A_l)).$$

As the digest is *access stable* (Eq. (11)), this implies $\emptyset \neq \llbracket \bar{\chi}_b \rrbracket_{\mathcal{A}}^{\sharp} (A_b, A_a) \wedge \emptyset \neq \llbracket \bar{\chi}_a \rrbracket_{\mathcal{A}}^{\sharp} (A_a, A_b)$ which in turn implies $\emptyset \neq \llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp} (A_b, A_a) \wedge \emptyset \neq \llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp} (A_a, A_b)$, and thus $A_a \parallel_g^? A_b = \top$. \square

Example 6. Consider again the program in Figure 2, which is annotated using the digest for lightweight thread *ids* (Figure 4). For the two access sequences starting after line 3 and line 14, with associated digests ST_{main} and MT , it can be excluded that these two accesses race with each other: While $\llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp} (\text{MT}, \text{ST}_{\text{main}}) = \{\text{MT}\} \neq \emptyset$, $\llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp} (\text{ST}_{\text{main}}, \text{MT}) = \emptyset$ and the respective sequences thus are known to not be bidirectionally compatible. \square

This definition in Proposition 2 is sound and generic — but can be overly conservative:

Example 7. Consider the lockset digest [43] (see Figure 6) which associates with each program point the set of locks held when it is reached. The program in Figure 2 is annotated with this information. The digests for lines 8 and line 14, right before the following access sequences, are given by $\{a\}$. $\llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp} (\{a\}, \{a\})$ yields $\{\{a, m_g\}\}$, i.e., a non-empty set of digests, and thus $\{a\} \parallel_g^? \{a\} = \top$. Using the generic definition of $\parallel_g^?$ from Proposition 2, we cannot exclude that the accesses in line 10 and line 16 race, despite both happening while holding the mutex *a*. \square

Remark 3. Setting $\llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp}(S_a, S_b) = \emptyset$ when $S_a \cap S_b \neq \emptyset$ renders the digest inadmissible: Consider a program where all accesses to a global g are protected by some mutex a . Then, any unlock of m_g happens while holding a , as does any lock of m_g . Setting $\llbracket \text{lock}(m_g) \rrbracket_{\mathcal{A}}^{\sharp}(\{a\}, \{a\}) = \emptyset$ thus violates (Eq. (6)).

Nevertheless, two accesses where a common program mutex is held cannot race. In fact, synchronization via mutexes is a common way to prevent races. Thus, this first definition in terms of bidirectional digest compatibility — while sound and generic — does not sufficiently capture the property for all digests.

5.2 Bespoke Definitions

While the definition in Proposition 2 allows using information computed by any access stable digest to exclude races, often better definitions of $\parallel_g^?$ are possible.

Example 8. Consider again the definition of $\parallel^?$ for the lockset digest provided in Example 2.

$$S_a \parallel_g^? S_b = \begin{cases} \text{false} & \text{if } S_a \cap S_b \neq \emptyset \\ \top & \text{otherwise} \end{cases}$$

This definition is more precise than the definition in terms of bidirectional digest compatibility and captures the intent behind mutex-based synchronization. \square

Proposition 3. *The definition of $\parallel^?$ for the lockset digest given above is sound.*

Proof Sketch 1 While immediately believable, we still sketch a proof. It is by contraposition: Consider sequences $\bar{\chi}_a$ and $\bar{\chi}_b$ of accesses to a global g and local traces t_a , t_b and t_l where at the end of t_a and t_b , both threads hold some mutex m . Then, $m \in (\alpha_{\mathcal{A}} t_a) \cap (\alpha_{\mathcal{A}} t_b)$ and thus $(\alpha_{\mathcal{A}} t_a) \parallel^? (\alpha_{\mathcal{A}} t_b) = \text{false}$. We show that then the left-hand side of implication (12) is false, i.e., the accesses are not bidirectionally compatible. If both accesses are performed by the same thread, these sequences are not bidirectionally compatible as the program order orders one sequence before the other. Consider the case where the accesses are performed by different threads: Neither $\bar{\chi}_a$ nor $\bar{\chi}_b$ unlocks m , and both t_a and t_b contain operations that lock m . As locks of m are totally ordered, one of the sequences must have happened before the other thread acquired m . Thus, trace compatibility holds at most in one direction. For an in-depth proof, see Appendix A. \square

Later, we will usually not flesh out soundness arguments where they are intuitive.

Example 9. For a further example, consider again the digest from Figure 4. The definition in terms of bidirectional digest compatibility already serves to exclude races where one access happens in single-threaded mode whereas the other one happens in multi-threaded mode. However, two accesses performed by the main thread can also not race as the main thread is unique, and such accesses are totally ordered by the program order. To exploit this, we can set:

$$M_a \parallel^? M_b = \begin{cases} \text{false} & \text{if } (M_a = \text{ST}_{\text{main}} \vee M_b = \text{ST}_{\text{main}}) \vee (M_a = M_b = \text{MT}_{\text{main}}) \\ \top & \text{otherwise.} \end{cases}$$

Appendix B provides a definition for general thread *ids*. \square

```

1 # From program, digest, and RHS of abstract interpretation, construct constr. sys. (Sect. 3)
2 constraintSystem = constructConSys(program, digest, ([·]#, new#, init#, D));
3
4 # Add helper unknowns and constraints (Eq. (14)) and solve using fixpoint engine
5 hConstraintSystem = addHelperConstraints(constraintSystem);
6 solution = solve(hConstraintSystem);
7
8 # Postprocessing
9 for g in globals:
10     accesses = solution[RG]; # Get set of accesses to g
11
12     # For each pair of accesses, check whether they may race and at least one is a write
13     for (u0, τ0, A0) in accesses:
14         for (u1, τ1, A1) in accesses:
15             if (τ0 == W or τ1 == W) and (A0 ||?g A1 == ⊤):
16                 report_race(u0, u1);

```

Fig. 7. Pseudocode of the digest-driven algorithm for data race detection.

5.3 Combination of Digests

Several admissible digests can be combined into an admissible product digest [43] with all operations given pointwise. If all digests are access stable, so is the product digest. To leverage such a product digest for race detection, we consider the range of answers $\{\text{false}, \top\}$ of the predicate $\|_g^?$ as a lattice, with false as the least element. The predicate $\|_g^?$ for a product $(\prod_{j=0}^{n-1} \mathcal{A}_j)$ of n active digests then is defined as the component-wise meet of predicates $\|_{g,j}^?$ for individual digests

$$(A_0^0, \dots, A_{n-1}^0) \|_g^? (A_0^1, \dots, A_{n-1}^1) = \prod_{j=0}^{n-1} (A_j^0 \|_{g,j}^? A_j^1)$$

As all $\|_{g,j}^?$ soundly overapproximate bidirectional compatibility, so does the meet.

Example 10. Consider again the program in Figure 2 where the main thread first initializes a global g and then starts two threads which each write to g , with only the latter accesses synchronized via some mutex. Neither the lockset digest (Example 8) nor the lightweight thread id digest (Example 9) on their own suffice to show the absence of all data races, but their combination does. \square

Alternatively, one can define a custom predicate for the product digest to jointly exploit information from all digests — at the expense of providing a dedicated soundness argument. Such a custom predicate resembles the *reduced* product construction as proposed by Cousot and Cousot [15], while the definition via the component-wise meet is more in the spirit of the *direct* product.

6 The Digest-Driven Race Detection Algorithm

The predicate $\|_g^?$ as a convenient yet expressive overapproximation of bidirectional trace compatibility can serve as a cornerstone of a race detection algorithm

for a static analyzer. Such an algorithm works in two phases: During the analysis, for each global g the digest associated with each access and the access type is recorded. In a post-processing phase, the predicate $\parallel_g^?$ is then used to check whether there are any accesses that may race.

The algorithm is shown in Figure 7. In line 2 a refined abstract constraint system is constructed that is parameterized by the program, the abstract domain and the digest, which we require to be admissible and access stable. This constraint system is extended with constraints that enforce that for each global variable information about each access to it is accumulated (line 5). For each global g , a dedicated unknown $[\mathcal{R}_g]$ is introduced, with values ranging over $2^{(\mathcal{N} \times \{W,R\} \times (\Pi_i \mathcal{A}_i))}$ where each tuple corresponds to an access. It consists of the location of access, its type (W(rite) or R(ead)), and digest information from all active digests. This is achieved by introducing for each constraint of the form

$$[\text{unlock}(m_g), A'] \sqsupseteq \llbracket (u_1, \text{unlock}(m_g), u_2) \rrbracket^\# [u_1, A_0]$$

an additional constraint

$$[\mathcal{R}_g] \sqsupseteq \left(\lambda x \rightarrow \begin{cases} \{(u_1, \tau u_1, A')\} & \text{if } x \neq \perp \\ \emptyset & \text{else} \end{cases} \right) [u_1, A_0] \quad (14)$$

where $\tau u_1 \in \{W, R\}$ is the type of the access which can be determined by checking whether the single (by construction of the programs with atomicity mutexes) incoming edge of u_1 is a write or a read. The case distinction ensures that only the digests associated with potentially reachable accesses are recorded, while the digest A' in this case is guaranteed to be identical to the digest before executing the access sequence due to access stability (Eq. (11)). The constraint system is then solved (line 6). In the post-processing phase (line 9 to 16) for each global the set of accumulated accesses is considered. For any two program points u_0 and u_1 , a potential race for a global g is then flagged if

$$\exists \tau_0, A_0, \tau_1, A_1 : (u_0, \tau_0, A_0), (u_1, \tau_1, A_1) \in [\mathcal{R}_g] \wedge (\tau_0 = W \vee \tau_1 = W) \wedge (A_0 \parallel_g^? A_1) = \top,$$

i.e., at least one of the accesses is a write, and it cannot be excluded that they are unordered w.r.t. each other. We remark that the tuples (u_0, τ_0, A_0) and (u_1, τ_1, A_1) are allowed to coincide, as two accesses with the same digest may still race as they could be performed by different (concrete) threads.

Remark 4. Where an analyzer does not have concrete memory locations, but only abstract memory locations, as may be the case when analyzing programs with dynamic memory allocation with an allocation site abstraction, the check is performed for all accesses to abstract memory locations that potentially overlap.

7 Experiments and Benchmark Set

The GOBLINT static analyzer [50] is based on thread-modular abstract interpretation of the local trace semantics [42, 46]. While it has supported data race

	CoOPERACE	GOBLINT	INFER	DEAGLE	RACERF
Correct true	754	712	747	685	674
Correct false	6	0	0	0	68
Incorrect true	1	0	213	1	0
Incorrect false	0	0	0	0	4

Table 1. SV-COMP 2025 results for no-data-race [9] of tools with at least 650 correct true verdicts. *Correct true (correct false)* is the number of programs where a tool correctly deduced race-freedom (raciness). *Incorrect true (incorrect false)* is the number of programs where a tool incorrectly claimed race-freedom (raciness).

detection for a long time, digest-driven data race detection proposed here serves as the theoretical underpinning and justification for this feature. GOBLINT implements various digests, and the digest-driven algorithm we propose in Section 6 is what emerged after unifying various older ad-hoc mechanisms.

GOBLINT participates in the data race track of Sv-COMP since its inception in 2021, receiving the highest score in 2021, 2023, and 2024⁸ and the second-highest score in 2025 — beaten only by CoOPERACE which internally calls GOBLINT. [6–8, 11] Table 1 shows the 2025 results. Among these, GOBLINT is the only tool producing no incorrect verdicts. We pose the following research question about digest-driven data race detection as implemented in GOBLINT:

RQ What impact do different digests and combinations of digests have on the number of solved tasks in the Sv-COMP data race benchmark set?

We modify GOBLINT to allow us to selectively change the predicate $\parallel_g^?$ for some digests to always return \top . Then, we compare for how many tasks GOBLINT still succeeds in proving data-race freedom depending on which digests are used to exclude races. GOBLINT implements the following digests:⁹

- L** Locksets (c.f. Figure 6 and [43], plus support for Reader/Writer-Locks)
- TF** Threadflag for multi- vs. single-threaded mode (c.f. Figure 4)
- TID** History-based thread *ids* [46] (recording parts of the creation history)
- J** Must-joined threads [46] (based on the history-based thread *ids*)
- FR** Tracking allocated memory that has not escaped its thread, i.e., is *fresh*¹⁰
- SL** Symbolic per-element locksets [50, Sections 5&6]*
- R** Region analysis [47]*

⁸ DEAGLE initially scored higher but was disqualified for fingerprinting tasks [8].

⁹ Digests marked with a * go beyond the framework presented here in that they combine time and space aspects. We include them as they nevertheless give rise to a predicate $\parallel_g^?$ akin to ours and can thus be employed in the digest-based algorithm.

¹⁰ It may seem surprising that FR can be considered a time-separation property. However, any access where the accessed memory has not escaped its thread yet must be ordered w.r.t. all other accesses to the same memory: Either both accesses happen in the same thread, or the other access happens later after the memory has escaped.

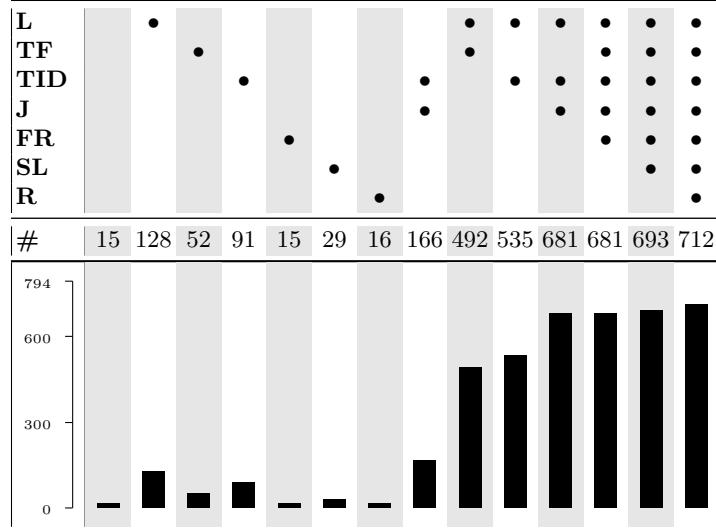


Fig. 8. The number of tasks where each digest succeeded in proving race freedom, out of a total of 794 race-free tasks in the benchmark set. None of the approaches produced any false negatives for the other 235 tasks in the benchmark set, which are racy.

The benchmarks were conducted on a machine with two Intel Xeon Platinum 8260 @ 2.40GHz processors with 24 cores each and 256GB of RAM running Ubuntu 24.04.1 LTS. BENCHEXEC [10] was used to limit each run to 5 minutes and 5GB of memory. With these settings, the system ran out of memory for 4 tasks, 3 tasks timed out, and the analyzer crashed for 7 tasks. Where execution terminated, it did so within at most 20s, where for all but 6 tasks the runtime was below 10s. As the analysis was always performed with the same settings, and only the definition of the predicate $\parallel_g^?$ was changed, we do not further detail runtimes.¹¹ Figure 8 summarizes the evaluation results: Each column corresponds to one configuration, and a • in a row indicates that this configuration uses the given digest to exclude races. The number indicates for how many out of a total of 794 race-free tasks the configuration succeeded in establishing race freedom.

Interestingly, for 15 of the 794 tasks, none of the digests is necessary to prove race freedom. These programs only contain accesses to shared memory locations marked as atomic using the `_Atomic` specifier from C11 or its GCC equivalent. When it comes to single digests, **L** succeeds in proving race freedom for a sizable chunk of tasks, as do **TF** and **TID**. Here, **TID** subsumes **TF**. The other digests are less successful on their own, succeeding for less than 30 tasks each. While enabling **J** on top of **TID** almost doubles the number of proven tasks, it is only the combination of thread-based and lock-based techniques that enables

¹¹ For **TID**, prior experiments [42, Chapter 5.3.2] on large, real-world programs, have established a median slowdown of around 1.2× (with a maximum slowdown of 5.2×) in the context of value analyses.

race-freedom to be proven for the majority of tasks (**L+TF**: 492, **L+TID**: 535, **L+TID+J**: 681). Enabling **FR** and **TF** on top of **L+TID+J** does not yield an improvement, but enabling **SL** and **R** modestly increases the number of successful tasks to 712. Overall, the experiments show that digest-based data race detection and the *combination* of digests reasoning about mutexes, created threads, and joins underlie the success of GOBLINT. The impact of the more specialized techniques used by GOBLINT on the other hand is rather limited.

Threats to Validity. All digests remained enabled, with only $\parallel_g^?$ modified to always return T. This may lead to underestimating their impact, as a digest may help show program points unreachable. However, we do not expect programs to contain many unreachable accesses. Additionally, digests can constrain other digests with which program points are reached. As our digests do not exploit guards, we expect such improvements (through the value analysis) to be rare.

8 Related Work

Detecting data races is a well-studied program analysis problem and there is a wealth of dynamic [19, 32, 37, 39, 41, 48] and static race detectors [18, 20, 22, 23, 26, 30, 38, 49–51]. A recent comparison of sound static race detectors [27] concludes that, to this day, open challenges remain—both w.r.t. showing time- and space-separation of accesses. Heeding this call for further research, our work provides a solid foundation for reasoning about time separation of accesses.

For the unsound static race detector RACERD, Gorogiannis et al. [24] state under which (idealized) conditions the tool becomes sound. Their definition of race is for an interleaving semantics, and they require that there is an interleaving that can be extended by performing either of the racy accesses next. This differs from our setting building on the local trace semantics, where, in general, no local view of the execution can be extended directly by either racy access, rendering their definition inapplicable for local traces. Chopra et al. [13], for an analysis of interrupt-driven kernels, define data races based on overlapping sections of executions which also does not apply to the local trace semantics.

A line of work closely tied to the time-separation aspect of data race detection is *May-Happen-in-Parallel* (MHP) analysis [1–5, 17, 31, 36, 52], which attempts to determine sets of statements that may execute in parallel. Approaches there are, once more, often based on flavors of interleaving semantics, rather than a local view. Typically, control flow within threads, i.e., whether given statements are reachable at all, is abstracted away. Approaches may, e.g., extract a graph-based overapproximation of the *inter*-thread control flow in a first step, with an analysis of this graph as a second step. [5, 17, 31] Our framework, on the other hand, is integrated into a thread-modular abstract interpreter and thus seamlessly combines MHP reasoning for races with value analyses. Furthermore, as opposed to the more monolithic approaches in the MHP literature, our framework can be instantiated with different digests and their admissibility and the soundness of their predicate $\parallel_g^?$ can be established modularly for each digest.

Digests were proposed as a way to refine the static analysis of the *values* of global variables of multi-threaded programs [42, 46] with later work [43] proposing further instances of digests and generalizing the setup along various axes, —within the scope of value analysis. We do not study value analyses, but instead show how digests can be repurposed to obtain principled static data race checkers in an extensible framework allowing for modular soundness proofs.

9 Conclusion and Future Work

We have provided a framework for reasoning about which accesses cannot happen simultaneously for digest-driven abstract interpretation. Giving two definitions of data races for the local trace semantics and establishing their equivalence allowed us to derive a sound digest-based data race detection algorithm. It relies on a novel predicate $\parallel^?$ to check whether two accesses with given digests may happen in parallel. We have shown how a generic definition of this predicate can be derived in terms of building blocks provided by any digest, and how, for some digests, bespoke definitions can yield more precise results. Digest-Driven Abstract Interpretation underlies our implementation in the static analyzer GOBLINT. To evaluate the impact of digests on the results of GOBLINT, we have turned specific digests on or off, finding that it is the combination of digests that underlies its success in Sv-COMP. Combining the lockset digest with digests reasoning on thread *ids* and joins increases the number of successful tasks by more than fourfold when compared to the thread-related digests and by more than fivefold when compared to the lockset digest alone.

There are many directions for future work: Preliminary experiments show that digests can capture further synchronization primitives such as barriers, and that our techniques also apply to the analysis of other concurrency issues such as deadlocks. Going beyond time separation, it is also worth exploring how to generalize digests to also tackle space separation, by, e.g., enhancing pointers with allocation time stamps. Lastly, it would be interesting to investigate how digests can serve as succinct explanations of analysis results to end users that do not require them to understand the inner workings of the analyzer and are thus easily digestible.

Data Availability Statement. An artifact [44] allowing for the reproduction of our experimental results is available on Zenodo.

Acknowledgments. This research is supported in part by the National Research Foundation, Singapore, and Cyber Security Agency of Singapore under its National Cybersecurity R&D Programme (Fuzz Testing NRF-NCR25-Fuzz-0001). Any opinions, findings and conclusions, or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore, and Cyber Security Agency of Singapore. This work is also supported in part by Deutsche Forschungsgemeinschaft (DFG) — 378803395/2428 CONVEY.

Bibliography

- [1] Agarwal, S., Barik, R., Sarkar, V., Shyamasundar, R.K.: May-happen-in-parallel analysis of x10 programs. In: PPoPP '07, p. 183–193, ACM (2007), DOI: [10.1145/1229428.1229471](https://doi.org/10.1145/1229428.1229471)
- [2] Albert, E., Flores-Montoya, A., Genaim, S.: Analysis of may-happen-in-parallel in concurrent objects. In: Giese, H., Rosu, G. (eds.) Formal Techniques for Distributed Systems - Joint 14th IFIP WG 6.1 International Conference, FMOODS 2012 and 32nd IFIP WG 6.1 International Conference, FORTE 2012, Stockholm, Sweden, June 13–16, 2012. Proceedings, Lecture Notes in Computer Science, vol. 7273, pp. 35–51, Springer (2012), DOI: [10.1007/978-3-642-30793-5_3](https://doi.org/10.1007/978-3-642-30793-5_3)
- [3] Albert, E., Genaim, S., Gordillo, P.: May-happen-in-parallel analysis for asynchronous programs with inter-procedural synchronization. In: Blazy, S., Jensen, T.P. (eds.) Static Analysis - 22nd International Symposium, SAS 2015, Saint-Malo, France, September 9–11, 2015, Proceedings, Lecture Notes in Computer Science, vol. 9291, pp. 72–89, Springer (2015), DOI: [10.1007/978-3-662-48288-9_5](https://doi.org/10.1007/978-3-662-48288-9_5)
- [4] Albert, E., Genaim, S., Gordillo, P.: May-happen-in-parallel analysis with returned futures. In: D’Souza, D., Kumar, K.N. (eds.) Automated Technology for Verification and Analysis - 15th International Symposium, ATVA 2017, Pune, India, October 3–6, 2017, Proceedings, Lecture Notes in Computer Science, vol. 10482, pp. 42–58, Springer (2017), DOI: [10.1007/978-3-319-68167-2_3](https://doi.org/10.1007/978-3-319-68167-2_3)
- [5] Barik, R.: Efficient computation of may-happen-in-parallel information for concurrent Java programs. In: LCPC ’06, vol. 4339 LNCS, pp. 152–169, Springer (2006), DOI: [10.1007/978-3-540-69330-7_11](https://doi.org/10.1007/978-3-540-69330-7_11)
- [6] Beyer, D.: Software verification: 10th comparative evaluation (SV-COMP 2021). In: Groote, J.F., Larsen, K.G. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 27th International Conference, TACAS 2021, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2021, Luxembourg City, Luxembourg, March 27 - April 1, 2021, Proceedings, Part II, Lecture Notes in Computer Science, vol. 12652, pp. 401–422, Springer (2021), DOI: [10.1007/978-3-030-72013-1_24](https://doi.org/10.1007/978-3-030-72013-1_24)
- [7] Beyer, D.: Competition on software verification and witness validation: SV-COMP 2023. In: Sankaranarayanan, S., Sharygina, N. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 29th International Conference, TACAS 2023, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2022, Paris, France, April 22–27, 2023, Proceedings, Part II, Lecture Notes in Computer Science, vol. 13994, pp. 495–522, Springer (2023), DOI: [10.1007/978-3-031-30820-8_29](https://doi.org/10.1007/978-3-031-30820-8_29)

- [8] Beyer, D.: State of the art in software verification and witness validation: SV-COMP 2024. In: Finkbeiner, B., Kovács, L. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 30th International Conference, TACAS 2024, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2024, Luxembourg City, Luxembourg, April 6-11, 2024, Proceedings, Part III, Lecture Notes in Computer Science, vol. 14572, pp. 299–329, Springer (2024), DOI: [10.1007/978-3-031-57256-2_15](https://doi.org/10.1007/978-3-031-57256-2_15)
- [9] Beyer, D.: NoDataRace-Main – BenchExec results (2025), URL <https://sv-comp.sosy-lab.org/2025/results/results-verified/no-data-race.NoDataRace-Main.table.html#/>
- [10] Beyer, D., Löwe, S., Wendler, P.: Reliable benchmarking: requirements and solutions. Int. J. Softw. Tools Technol. Transf. **21**(1), 1–29 (2019), DOI: [10.1007/S10009-017-0469-Y](https://doi.org/10.1007/S10009-017-0469-Y)
- [11] Beyer, D., Strejcek, J.: Improvements in software verification and witness validation: SV-COMP 2025. In: Gurinkel, A., Heule, M. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 31st International Conference, TACAS 2025, Held as Part of the International Joint Conferences on Theory and Practice of Software, ETAPS 2025, Hamilton, ON, Canada, May 3-8, 2025, Proceedings, Part III, Lecture Notes in Computer Science, vol. 15698, pp. 151–186, Springer (2025), DOI: [10.1007/978-3-031-90660-2_9](https://doi.org/10.1007/978-3-031-90660-2_9)
- [12] Blackshear, S., Gorogiannis, N., O’Hearn, P.W., Sergey, I.: Racerd: compositional static race detection. Proc. ACM Program. Lang. **2**(OOPSLA) (2018), DOI: [10.1145/3276514](https://doi.org/10.1145/3276514)
- [13] Chopra, N., Pai, R.R., D’Souza, D.: Data races and static analysis for interrupt-driven kernels. In: Caires, L. (ed.) Programming Languages and Systems - 28th European Symposium on Programming, ESOP 2019, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2019, Prague, Czech Republic, April 6-11, 2019, Proceedings, Lecture Notes in Computer Science, vol. 11423, pp. 697–723, Springer (2019), DOI: [10.1007/978-3-030-17184-1_25](https://doi.org/10.1007/978-3-030-17184-1_25)
- [14] Cousot, P., Cousot, R.: Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: Graham, R.M., Harrison, M.A., Sethi, R. (eds.) Conference Record of the Fourth ACM Symposium on Principles of Programming Languages, Los Angeles, California, USA, January 1977, pp. 238–252, ACM (1977), DOI: [10.1145/512950.512973](https://doi.org/10.1145/512950.512973)
- [15] Cousot, P., Cousot, R.: Systematic design of program analysis frameworks. In: Aho, A.V., Zilles, S.N., Rosen, B.K. (eds.) Conference Record of the Sixth Annual ACM Symposium on Principles of Programming Languages, San Antonio, Texas, USA, January 1979, pp. 269–282, ACM Press (1979), DOI: [10.1145/567752.567778](https://doi.org/10.1145/567752.567778)
- [16] Dacík, T., Vojnar, T.: Racerf: Lightweight static data race detection for c code (2025), URL <https://arxiv.org/abs/2502.04905>, to appear at ECOOP 2025

- [17] Di, P., Sui, Y., Ye, D., Xue, J.: Region-based may-happen-in-parallel analysis for C programs. In: ICPP, pp. 889–898, IEEE (2015), ISBN 978-1-4673-7587-0, doi: [10.1109/ICPP.2015.98](https://doi.org/10.1109/ICPP.2015.98)
- [18] Dietsch, D., Heizmann, M., Klumpp, D., Schüssle, F., Podelski, A.: Ultimate taipan and race detection in ultimate - (competition contribution). In: Sankaranarayanan, S., Sharygina, N. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 29th International Conference, TACAS 2023, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2022, Paris, France, April 22-27, 2023, Proceedings, Part II, Lecture Notes in Computer Science, vol. 13994, pp. 582–587, Springer (2023), doi: [10.1007/978-3-031-30820-8_40](https://doi.org/10.1007/978-3-031-30820-8_40)
- [19] Effinger-Dean, L., Lucia, B., Ceze, L., Grossman, D., Boehm, H.: Ifrit: interference-free regions for dynamic data-race detection. In: Leavens, G.T., Dwyer, M.B. (eds.) Proceedings of the 27th Annual ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications, OOPSLA 2012, part of SPLASH 2012, Tucson, AZ, USA, October 21-25, 2012, pp. 467–484, ACM (2012), doi: [10.1145/2384616.2384650](https://doi.org/10.1145/2384616.2384650)
- [20] Engler, D.R., Ashcraft, K.: RacerX: effective, static detection of race conditions and deadlocks. In: Scott, M.L., Peterson, L.L. (eds.) Proceedings of the 19th ACM Symposium on Operating Systems Principles 2003, SOSP 2003, Bolton Landing, NY, USA, October 19-22, 2003, pp. 237–252, ACM (2003), doi: [10.1145/945445.945468](https://doi.org/10.1145/945445.945468)
- [21] Erhard, J., Bentele, M., Heizmann, M., Klumpp, D., Saan, S., Schüssle, F., Schwarz, M., Seidl, H., Tilscher, S., Vojdani, V.: Correctness witnesses for concurrent programs: Bridging the semantic divide with ghosts. In: Shankaranarayanan, K., Sankaranarayanan, S., Trivedi, A. (eds.) Verification, Model Checking, and Abstract Interpretation, pp. 74–100, Springer Nature Switzerland, Cham (2025), ISBN 978-3-031-82700-6
- [22] Farzan, A., Klumpp, D., Podelski, A.: Sound sequentialization for concurrent program verification. In: Jhala, R., Dillig, I. (eds.) PLDI ’22: 43rd ACM SIGPLAN International Conference on Programming Language Design and Implementation, San Diego, CA, USA, June 13 - 17, 2022, pp. 506–521, ACM (2022), doi: [10.1145/3519939.3523727](https://doi.org/10.1145/3519939.3523727)
- [23] Gavrilenco, N., de León, H.P., Furbach, F., Heljanko, K., Meyer, R.: BMC for weak memory models: Relation analysis for compact SMT encodings. In: Dillig, I., Tasiran, S. (eds.) Computer Aided Verification - 31st International Conference, CAV 2019, New York City, NY, USA, July 15-18, 2019, Proceedings, Part I, Lecture Notes in Computer Science, vol. 11561, pp. 355–365, Springer (2019), doi: [10.1007/978-3-030-25540-4_19](https://doi.org/10.1007/978-3-030-25540-4_19)
- [24] Gorogiannis, N., O’Hearn, P.W., Sergey, I.: A true positives theorem for a static race detector. Proc. ACM Program. Lang. **3**(POPL), 57:1–57:29 (2019), doi: [10.1145/3290370](https://doi.org/10.1145/3290370)
- [25] Handjieva, M., Tzolovski, S.: Refining static analyses by trace-based partitioning using control flow. In: Levi, G. (ed.) Static Analysis, pp. 200–214, Springer Berlin Heidelberg, Berlin, Heidelberg (1998), ISBN 978-3-540-49727-1

- [26] He, F., Sun, Z., Fan, H.: Deagle: An SMT-based verifier for multi-threaded programs (competition contribution). In: Fisman, D., Rosu, G. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 28th International Conference, TACAS 2022, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2022, Munich, Germany, April 2-7, 2022, Proceedings, Part II, Lecture Notes in Computer Science, vol. 13244, pp. 424–428, Springer (2022), DOI: [10.1007/978-3-030-99527-0_25](https://doi.org/10.1007/978-3-030-99527-0_25)
- [27] Holter, K., Saan, S., Lam, P., Vojdani, V.: Sound static data race verification for c: Is the race lost? ACM Trans. Program. Lang. Syst. (2025), ISSN 0164-0925, DOI: [10.1145/3732933](https://doi.org/10.1145/3732933), just Accepted
- [28] Kästner, D., Miné, A., Schmidt, A., Hille, H., Mauborgne, L., Wilhelm, S., Rival, X., Feret, J., Cousot, P., Ferdinand, C.: Finding all potential run-time errors and data races in automotive software. In: WCX™ 2017-SAE World Congress Experience, pp. 1–9, SAE International (2017)
- [29] Lamport: How to Make a Multiprocessor Computer That Correctly Executes Multiprocess Programs . IEEE Transactions on Computers **28**(09), 690–691 (1979), ISSN 1557-9956, DOI: [10.1109/TC.1979.1675439](https://doi.org/10.1109/TC.1979.1675439)
- [30] Liu, B., Liu, P., Li, Y., Tsai, C., Silva, D.D., Huang, J.: When threads meet events: efficient and precise static race detection with origins. In: Freund, S.N., Yahav, E. (eds.) PLDI '21: 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation, Virtual Event, Canada, June 20-25, 2021, pp. 725–739, ACM (2021), DOI: [10.1145/3453483.3454073](https://doi.org/10.1145/3453483.3454073)
- [31] Lu, F., Wang, X., Zeng, Q., Yuan, G., Bao, Y.: Segment-based may-happen-in-parallel analysis for c programs. Concurrency and Computation: Practice and Experience **37**(21-22), e70203 (2025), DOI: [10.1002/cpe.70203](https://doi.org/10.1002/cpe.70203)
- [32] Marino, D., Musuvathi, M., Narayanasamy, S.: Literace: effective sampling for lightweight data-race detection. In: Hind, M., Diwan, A. (eds.) Proceedings of the 2009 ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2009, Dublin, Ireland, June 15-21, 2009, pp. 134–143, ACM (2009), DOI: [10.1145/1542476.1542491](https://doi.org/10.1145/1542476.1542491)
- [33] Mauborgne, L., Rival, X.: Trace partitioning in abstract interpretation based static analyzers. In: Sagiv, M. (ed.) Programming Languages and Systems, pp. 5–20, Springer Berlin Heidelberg, Berlin, Heidelberg (2005), ISBN 978-3-540-31987-0
- [34] Miné, A., Mauborgne, L., Rival, X., Feret, J., Cousot, P., Kästner, D., Wilhelm, S., Ferdinand, C.: Taking static analysis to the next level: proving the absence of run-time errors and data races with astrée. In: 8th European Congress on Embedded Real Time Software and Systems (ERTS 2016) (2016)
- [35] Montagu, B., Jensen, T.: Trace-based control-flow analysis. In: PLDI '21, p. 482–496, ACM (2021), DOI: [10.1145/3453483.3454057](https://doi.org/10.1145/3453483.3454057)
- [36] Naumovich, G., Avrunin, G.S., Clarke, L.A.: An efficient algorithm for computing mhp information for concurrent Java programs. In: ES-

- EC/FSE '99, vol. 1687 LNCS, pp. 338–354, Springer (1999), doi: 10.1007/3-540-48166-4_21
- [37] O'Callahan, R., Choi, J.: Hybrid dynamic data race detection. In: Eigenmann, R., Rinard, M.C. (eds.) Proceedings of the ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming, PPOPP 2003, June 11-13, 2003, San Diego, CA, USA, pp. 167–178, ACM (2003), doi: 10.1145/781498.781528
 - [38] Pratikakis, P., Foster, J.S., Hicks, M.W.: LOCKSMITH: context-sensitive correlation analysis for race detection. In: Schwartzbach, M.I., Ball, T. (eds.) Proceedings of the ACM SIGPLAN 2006 Conference on Programming Language Design and Implementation, Ottawa, Ontario, Canada, June 11-14, 2006, pp. 320–331, ACM (2006), doi: 10.1145/1133981.1134019
 - [39] Raman, R., Zhao, J., Sarkar, V., Vechev, M.T., Yahav, E.: Scalable and precise dynamic datarace detection for structured parallelism. In: Vitek, J., Lin, H., Tip, F. (eds.) ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI '12, Beijing, China - June 11 - 16, 2012, pp. 531–542, ACM (2012), doi: 10.1145/2254064.2254127
 - [40] Rival, X., Mauborgne, L.: The trace partitioning abstract domain. ACM Trans. Program. Lang. Syst. **29**(5), 26-es (2007), ISSN 0164-0925, doi: 10.1145/1275497.1275501
 - [41] Savage, S., Burrows, M., Nelson, G., Sobalvarro, P., Anderson, T.E.: Eraser: A dynamic data race detector for multithreaded programs. ACM Trans. Comput. Syst. **15**(4), 391–411 (1997), doi: 10.1145/265924.265927
 - [42] Schwarz, M.: Thread-Modular Abstract Interpretation: The Local Perspective. Ph.D. thesis, Technical University of Munich (2025), URL <https://d-nb.info/137113345X/34>
 - [43] Schwarz, M., Erhard, J.: The digest framework: concurrency-sensitivity for abstract interpretation. International Journal on Software Tools for Technology Transfer (2024), ISSN 1433-2787, doi: 10.1007/s10009-024-00773-y
 - [44] Schwarz, M., Erhard, J.: Artifact for 'data race detection by digest-driven abstract interpretation' (2025), doi: 10.5281/zenodo.17128591
 - [45] Schwarz, M., Saan, S., Seidl, H., Apinis, K., Erhard, J., Vojdani, V.: Improving thread-modular abstract interpretation. In: Dragoi, C., Mukherjee, S., Namjoshi, K.S. (eds.) Static Analysis - 28th International Symposium, SAS 2021, Chicago, IL, USA, October 17-19, 2021, Proceedings, Lecture Notes in Computer Science, vol. 12913, pp. 359–383, Springer (2021), doi: 10.1007/978-3-030-88806-0_18
 - [46] Schwarz, M., Saan, S., Seidl, H., Erhard, J., Vojdani, V.: Clustered relational thread-modular abstract interpretation with local traces. In: European Symposium on Programming, pp. 28–58, Springer (2023), doi: 10.1007/978-3-031-30044-8_2
 - [47] Seidl, H., Vojdani, V.: Region analysis for race detection. In: International Static Analysis Symposium, pp. 171–187, Springer (2009)
 - [48] Serebryany, K., Iskhodzhanov, T.: Threadsanitizer: data race detection in practice. In: Proceedings of the Workshop on Binary Instrumentation and

- Applications, p. 62–71, WBIA ’09, Association for Computing Machinery, New York, NY, USA (2009), ISBN 9781605587936, doi: [10.1145/1791194.1791203](https://doi.org/10.1145/1791194.1791203)
- [49] Terauchi, T.: Checking race freedom via linear programming. In: Gupta, R., Amarasinghe, S.P. (eds.) Proceedings of the ACM SIGPLAN 2008 Conference on Programming Language Design and Implementation, Tucson, AZ, USA, June 7–13, 2008, pp. 1–10, ACM (2008), doi: [10.1145/1375581.1375583](https://doi.org/10.1145/1375581.1375583)
- [50] Vojdani, V., Apinis, K., Rõtov, V., Seidl, H., Vene, V., Vogler, R.: Static race detection for device drivers: the goblint approach. In: Lo, D., Apel, S., Khurshid, S. (eds.) Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering, ASE 2016, Singapore, September 3–7, 2016, pp. 391–402, ACM (2016), doi: [10.1145/2970276.2970337](https://doi.org/10.1145/2970276.2970337)
- [51] Young, J.W., Jhala, R., Lerner, S.: RELAY: static race detection on millions of lines of code. In: Crnkovic, I., Bertolino, A. (eds.) Proceedings of the 6th joint meeting of the European Software Engineering Conference and the ACM SIGSOFT International Symposium on Foundations of Software Engineering, 2007, Dubrovnik, Croatia, September 3–7, 2007, pp. 205–214, ACM (2007), doi: [10.1145/1287624.1287654](https://doi.org/10.1145/1287624.1287654)
- [52] Zhou, Q., Li, L., Wang, L., Xue, J., Feng, X.: May-happen-in-parallel analysis with static vector clocks. In: CGO ’18, pp. 228–240, ACM (2018), doi: [10.1145/3168813](https://doi.org/10.1145/3168813)

A Soundness of Predicate $\parallel^?$ for Lockset Digest

We first recall the proposition from Section 5.2:

Proposition 4. *The definition of $\parallel^?$ for the lockset digest given above is sound.*

Proof. The proof is by contraposition: Consider two sequences $\bar{\chi}_a$ and $\bar{\chi}_b$ of accesses to a global, say g , and local traces t_a, t_b and t_l where at the end of t_a and t_b , both threads hold some mutex, say m . Then, we have $m \in (\alpha_{\mathcal{A}} t_a) \cap (\alpha_{\mathcal{A}} t_b)$ and thus $(\alpha_{\mathcal{A}} t_a) \parallel^? (\alpha_{\mathcal{A}} t_b) = \text{false}$. We show that then the left-hand side of the implication in (12) does not hold either, i.e., the accesses are not in fact bidirectionally compatible.

For the left-hand side of the implication to not hold, either $\llbracket \bar{\chi}_b \rrbracket(t_b, \llbracket \bar{\chi}_a \rrbracket(t_a, t_l))$ or $\llbracket \bar{a} \chi_a \rrbracket(t_a, \llbracket \bar{\chi}_b \rrbracket(t_b, t_l))$ needs to return \emptyset . If both return \emptyset , nothing is to be shown. Now consider the case where one does not return \emptyset . We show that in this case, the other one must be \emptyset .

W.l.o.g., assume that $\emptyset \neq \llbracket \bar{\chi}_b \rrbracket(t_b, \llbracket \bar{\chi}_a \rrbracket(t_a, t_l))$ holds, i.e., the access \bar{a}_a can happen before the access \bar{a}_b . Let $\{t'\} = \llbracket \bar{\chi}_a \rrbracket(t_a, t_l)$. t' then, by construction, contains an action $\text{unlock}(m_g)$ that happens later than the $\text{unlock}(m_g)$ in t_l . As m is held at the end of t_a and executing the sequence \bar{a}_a consisting of locking m_g , accessing g , and unlocking m_g does not unlock m , at the end of t' the ego thread still holds m . We distinguish two cases:

- Both $\bar{\chi}_a$ and $\bar{\chi}_b$ are executed by the same thread, with m continuously held.
- The thread executing $\bar{\chi}_a$ has unlocked m after this access, and this unlock precedes the last lock of m by the ego thread in t_b .

In either case, t' is a subtrace of t_b . Now consider executing the accesses in the reverse order. Then, $\llbracket \bar{\chi}_b \rrbracket(t_b, t_l) = \emptyset$, as t_b contains t' and the $\text{unlock}(m_g)$ in which t_l ends is not the last unlock of m_g . Therefore, also $\llbracket \bar{\chi}_a \rrbracket(t_a, \llbracket \bar{\chi}_b \rrbracket(t_b, t_l)) = \emptyset$, and the left-hand side of the implication is false. \square

B Predicate $\parallel^?$ for Thread-ID Digests

A central instance of the digest framework are thread *ids* [43]. A digest \mathcal{A} that assigns to each thread an *id* is called a *thread id* digest. As the digest may contain information other than the thread *id* of the current thread, we require that there is a function $\text{tid} : \mathcal{A} \rightarrow \text{TID}$ that, given a digest, yields its thread *id*. We demand that the thread *id* of a given thread must remain constant during its execution. Again, as in previous work [43], we assume the existence of two helper functions *may_run* and *unique*:

- *unique* : $\text{TID} \rightarrow \text{Bool}$, yields, given a thread *id*, a boolean indicating whether the thread represented by the *id* is unique.
- *may_run* : $\mathcal{A} \rightarrow \mathcal{A} \rightarrow \text{Bool}$, where *may_run* a b must be true, in case the thread with digest b may have already started when the ego thread has the digest a .

Example 11. Consider the lightweight thread id digest in Figure 4. We define the set of thread ids TID as $\{\text{main}, \text{other}\}$ to allow differentiating between the **main** thread and other threads. The function tid is given by:

$$\text{tid } d = \begin{cases} \text{main} & \text{if } d = \text{ST}_{\text{main}} \vee d = \text{MT}_{\text{main}} \\ \text{other} & \text{otherwise} \end{cases}.$$

It extracts the thread id main out of the digests ST_{main} and MT_{main} . The function unique indicates that **main** is unique:

$$\text{unique } i = \begin{cases} \text{true} & \text{if } i = \text{main} \\ \text{false} & \text{otherwise} \end{cases}.$$

The function may-run is defined as follows:

$$\text{may_run } a \ b = \begin{cases} \text{false} & \text{if } a = \text{ST}_{\text{main}} \wedge b = \text{MT} \\ \text{true} & \text{otherwise} \end{cases}.$$

In case the ego thread has the digest ST_{main} , it can be excluded that a thread with digest MT has already been created. \square

We now define the predicate $\parallel^?$ for \mathcal{A} generically in terms of these helper functions:

$$a \parallel^? b = \begin{cases} \text{false} & \text{if } (\text{tid } a = \text{tid } b \wedge \text{unique}(\text{tid } a)) \\ & \quad \vee \neg \text{may_run } a \ b \vee \neg \text{may_run } b \ a \\ \top & \text{otherwise} \end{cases} \quad (15)$$

This definition excludes races in case the digests a and b refer to the same thread id and that the thread id of a is unique. This is sound as a single thread cannot race with itself. Additionally, it excludes races when either the thread with digest b may not be started when the ego thread has the digest a , or vice versa.

Example 12. Consider again the lightweight thread id digest with the definitions in Example 11. For this example, the definition in Eq. (15) coincides with the definition already given in Example 9. \square

The definition in Eq. (15) is also applicable to more intricate thread id digests, such as the ones proposed in earlier work [46, Section 6], where unique identities are also maintained for threads other than **main**.