Fully Composable and Adequate Verified Compilation with Direct Refinements between Open Modules

LING ZHANG, Shanghai Jiao Tong University, China
YUTING WANG*, Shanghai Jiao Tong University, China
JINHUA WU, Shanghai Jiao Tong University, China
JÉRÉMIE KOENIG, Yale University, USA
ZHONG SHAO, Yale University, USA

Verified compilation of open modules (i.e., modules whose functionality depends on other modules) provides a foundation for end-to-end verification of modular programs ubiquitous in contemporary software. However, despite intensive investigation in this topic for decades, the proposed approaches are still difficult to use in practice as they rely on assumptions about the internal working of compilers which make it difficult for external users to apply the verification results. We propose an approach to verified compositional compilation without such assumptions in the setting of verifying compilation of heterogeneous modules written in first-order languages supporting global memory and pointers. Our approach is based on the memory model of CompCert and a new discovery that a Kripke relation with a notion of memory protection can serve as a uniform and composable semantic interface for the compiler passes. By absorbing the rely-guarantee conditions on memory evolution for all compiler passes into this Kripke Memory Relation and by piggybacking requirements on compiler optimizations onto it, we get compositional correctness theorems for realistic optimizing compilers as refinements that directly relate native semantics of open modules and that are ignorant of intermediate compilation processes. Such direct refinements support all the compositionality and adequacy properties essential for verified compilation of open modules. We have applied this approach to the full compilation chain of CompCert with its Clight source language and demonstrated that our compiler correctness theorem is open to composition and intuitive to use with reduced verification complexity through end-to-end verification of non-trivial heterogeneous modules that may freely invoke each other (e.g., mutually recursively).

CCS Concepts: • **Software and its engineering → Formal software verification**; **Compilers**; • **Theory of computation → Program verification**.

Additional Key Words and Phrases: Verified Compositional Compilation, Direct Refinement, Kripke Relation

1 INTRODUCTION

Verified compilation ensures that behaviors of source programs are faithfully transported to target code, a property desirable for end-to-end verification of software whose development involves compilation. As software is usually composed of modules independently developed and compiled, researchers have developed a wide range of techniques for *verified compositional compilation* or VCC that support modules invoking each other (i.e., open), being written in different languages (i.e., heterogeneous) and transformed by different compilers [Patterson and Ahmed 2019].

We are concerned with VCC for first-order languages with global memory states and support of pointers (e.g., see Gu et al. [2015]; Jiang et al. [2019]; Koenig and Shao [2021]; Song et al. [2020]; Stewart et al. [2015]; Wang et al. [2019]). As it stands now, the proposed approaches are inherently limited at supporting open modules (e.g. libraries) as they either deviate from the native semantics of modules or expose the semantics of intermediate representations for compilation, resulting in correctness theorems that are difficult to work with for external users. In this paper, we investigate an approach that eliminates these limitations while retaining the full benefits of VCC, i.e., obtaining correctness of compiling open modules that is *fully composable*, *adequate*, and *extensional*.

*Corresponding author

1.1 Full Compositionality and Adequacy in Verified Compilation

Correctness of compiling open modules is usually described as refinement between semantics of source and target modules. We shall write L (possibly with subscripts) to denote semantics of open modules and write $L_1 \preccurlyeq L_2$ to denote that L_1 is refined by L_2. Therefore, the compilation of any module M_2 into M_1 is correct iff $[[M_1]] \preccurlyeq [[M_2]]$ where $[[M_i]]$ denotes the semantics of M_i.

To support the most general form of VCC, it is critical that the established refinements are *fully composable*, i.e., both *horizontally and vertically composable*, and *adequate for native semantics*:

$$\begin{aligned} \textbf{Vertical Compositionality:} &\quad L_1 \preccurlyeq L_2 \Rightarrow L_2 \preccurlyeq L_3 \Rightarrow L_1 \preccurlyeq L_3 \\ \textbf{Horizontal Compositionality:} &\quad L_1 \preccurlyeq L_1' \Rightarrow L_2 \preccurlyeq L_2' \Rightarrow L_1 \oplus L_2 \preccurlyeq L_1' \oplus L_2' \\ \textbf{Adequacy for Native Semantics:} &\quad [[M_1 + M_2]] \preccurlyeq [[M_1]] \oplus [[M_2]] \end{aligned}$$

The first property states that refinements are transitive. It is essential for composing proofs for multi-pass compilers. The second property guarantees that refinements are preserved by semantic linking (denoted by $\oplus$). It is essential for composing correctness of compiling open modules (possibly through different compilers). The last one ensures that, given any modules, their semantic linking coincides with their syntactic linking (denoted by +). It ensures that linked semantics do not deviate from native semantics and is essential to propagate verified properties to final target programs.

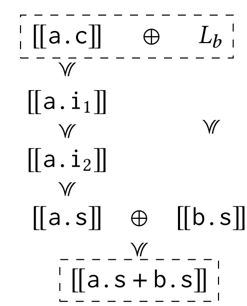


Fig. 1. Motivating Example

We use the example in Fig. 1 to illustrate the importance of the above properties in VCC where heterogeneous modules are compiled through different compilation chains and linked into a final target module. In this example, a source C module `a.c` is compiled into an assembly module `a.s` through a multi-pass optimizing compiler like CompCert: it is first compiled to $\texttt{a.i}_1$ in an intermediate representation (IR) for optimization (e.g., the RTL language of CompCert) and then to $\texttt{a.i}_2$ in another IR for code generation (e.g., the Mach language of CompCert). Finally, it is linked with a library module `b.s` which is not compiled at all (an extreme case where the compilation chain is empty). The goal is to prove that the semantics of linked target assembly `a.s + b.s` refines the combined source semantics $[[\texttt{a.c}]] \oplus L_b$ where L_b is the semantic specification of `b.s`, i.e., $[[\texttt{a.s} + \texttt{b.s}]] \preccurlyeq [[\texttt{a.c}]] \oplus L_b$. The proof proceeds as follows:

(1) Prove every pass respects refinement, from which $[[\texttt{a.i}_1]] \preccurlyeq [[\texttt{a.c}]]$, $[[\texttt{a.i}_2]] \preccurlyeq [[\texttt{a.i}_1]]$ and $[[\texttt{a.s}]] \preccurlyeq [[\texttt{a.i}_2]]$. Moreover, show `b.s` meets its specification, i.e., $[[\texttt{b.s}]] \preccurlyeq L_b$;
(2) By vertically composing the refinement relations for compiling `a.c`, we get $[[\texttt{a.s}]] \preccurlyeq [[\texttt{a.c}]]$;
(3) By further horizontally composing with $[[\texttt{b.s}]] \preccurlyeq L_b$, we get $[[\texttt{a.s}]] \oplus [[\texttt{b.s}]] \preccurlyeq [[\texttt{a.c}]] \oplus L_b$;
(4) By adequacy for assembly and vertical composition, conclude $[[\texttt{a.s} + \texttt{b.s}]] \preccurlyeq [[\texttt{a.c}]] \oplus L_b$.

1.2 Problems with the Existing Approaches to Refinements

Despite the simplicity of VCC at an intuitive level, full compositionality and adequacy are surprisingly difficult to prove for any non-trivial multi-pass compiler. First and foremost, the formal definitions must take into account the facts that each intermediate representation has different semantics and each pass may imply a different refinement relation. To facilitate the discussion below, we classify different open semantics by *language interfaces* (or simply interfaces) which formalize their interaction with environments. We write $L : \mathcal{I}$ to denote that L has a language interface $\mathcal{I}$. For instance, $[[\texttt{a.c}]] : C$ denotes that the semantics of `a.c` has the interface C which only allows for interaction with environments through function calls and returns in C. Similarly, $[[\texttt{a.s}]] : \mathcal{A}$ denotes the semantics of `a.s` where $\mathcal{A}$ only allows for interaction at the assembly level.

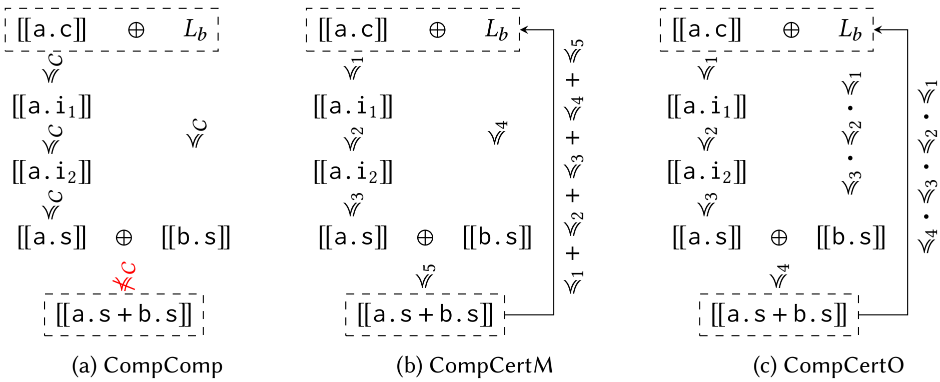


Fig. 2. Refinements in the Existing Approaches to VCC

Note that the interface for a module may not match its native semantics. For example, [[a.s]] : C asserts that [[a.s]] actually converts assembly level calls/returns to C function calls/returns for interacting with C environments (e.g., extracting arguments from registers and memory to form an argument list for C function calls). In this case, [[a.s]] *deviates* from the native semantics of a.s. When the interface of $[[M]]$ is not explicitly given, it is implicitly the native interface of M. We write $\preccurlyeq\colon \mathcal{I}_1 \Leftrightarrow \mathcal{I}_2$ to denote a refinement between two semantics with interfaces $\mathcal{I}_1$ and $\mathcal{I}_2$. For instance, given $\preccurlyeq_{\mathrm{ac}}\colon \mathcal{A} \Leftrightarrow C$ that relates open semantics at the C and assembly levels, [[b.s]] $\preccurlyeq_{\mathrm{ac}} L_b$ asserts that [[b.s]] is the native semantics of b.s and is refined by the C level specification L_b.

For VCC, it is essential that variance of open semantics and refinements does not impede compositionality and adequacy. The existing approaches achieve this by imposing *algebraic structures* on refinements. We categorize them by their algebraic structures below, and explain the problems facing them via three well-known extensions of CompCert [Leroy 2023] (the state-of-the-art verified compiler) to support VCC, i.e., Compositional CompCert (CompComp) [Stewart et al. 2015], CompCertM [Song et al. 2020] and CompCertO [Koenig and Shao 2021].

Constant Refinement. An obvious way to account for different semantics in VCC is to force every semantics to use the same language interface $\mathcal{I}$ and a constant refinement $\preccurlyeq_{\mathcal{I}}\colon \mathcal{I} \Leftrightarrow \mathcal{I}$. CompComp adopts this "one-type-fits-all" approach by having every language of CompCert to use C function calls/returns for module-level interactions and using a uniform refinement relation $\preccurlyeq_C\colon C \Leftrightarrow C$ known as *structured simulation* [Stewart et al. 2015]. In this case, vertical and horizontal compositionality is established by proving transitivity of $\preccurlyeq_C$ and symmetry of *rely-guarantee conditions* of $\preccurlyeq_C$. However, because the C interface is adopted for assembly semantics, adequacy at the target level is lost, making end-to-end compiler correctness not provable as shown in Fig. 2a.

Sum of Refinements. A more relaxed approach allows users to choose language interfaces for different IRs from a finite collection $\{\mathcal{I}_1, \ldots, \mathcal{I}_m\}$ and refinements for different passes from a finite set $\{\preccurlyeq_1, \ldots, \preccurlyeq_n\}$ relating these interfaces, i.e., $\preccurlyeq_i\colon \mathcal{I}_1 + \ldots + \mathcal{I}_m \Leftrightarrow \mathcal{I}_1 + \ldots + \mathcal{I}_m$. In essence, a constant refinement is split into a sum of refinements s.t. $L \preccurlyeq_1 + \ldots + \preccurlyeq_n L'$ holds if $L \preccurlyeq_i L'$ for some $1 \le i \le n$. Then, every compiler pass can use $\preccurlyeq_1 + \ldots + \preccurlyeq_n$ as the uniform refinement relation, which is proven both composable and adequate under certain well-formedness constraints. Fig. 2b depicts such an example where semantics have both C and assembly interfaces (e.g., [[a.s]] : $\mathcal{A}+C$) and the refinement relations $\preccurlyeq_i\colon \mathcal{A} + C \Leftrightarrow \mathcal{A} + C (1 \le i \le 5)$ are tailored for each pass. This is the approach adopted by CompCertM [Song et al. 2020]. However, the top-level refinement $\preccurlyeq_1 + \ldots + \preccurlyeq_n$ is difficult to use by a third party without introducing complicated dependency on intermediate results of compilation. For example, horizontal composition with $\leqslant_1 + \ldots + \leqslant_n$ only works for modules *self-related* by all the refinements $\leqslant_i$ $(1 \leq i \leq n)$. Since $\leqslant_i$s are tailored for individual passes, they inevitably depends on the intermediate semantics used in compilation. Such dependency is only exacerbated as new languages, compilers and optimizations are introduced.

Product of Refinements. The previous approach effectively "flattens" the refinements for individual compiler passes into an end-to-end refinement. A different approach adopted by CompCertO [Koenig and Shao 2021] is to "concatenate" the refinements for individual passes into a chain of refinements by a product operation ($\_ \cdot \_$) such that $L \leqslant_1 \cdot \leqslant_2 L''$ if $L \leqslant_1 L'$ and $L' \leqslant_2 L''$ for some L'. Fig. 2c illustrates how it works. Vertical composition is simply the concatenation of refinements. For example, composing refinements for compiling `a.c` results in $[[\texttt{a.s}]] \leqslant_3 \cdot \leqslant_2 \cdot \leqslant_1 [[\texttt{a.c}]]$. Adequacy is trivially guaranteed with native interfaces. However, horizontal composition still depends on the intermediate semantics of compilation because of the concatenation. For example, in Fig. 2c, to horizontally compose with $[[\texttt{a.s}]] \leqslant_3 \cdot \leqslant_2 \cdot \leqslant_1 [[\texttt{a.c}]]$, it is necessary to show L_b refines $[[\texttt{b.s}]]$ via the same product, i.e., to construct intermediate semantics bridging $\leqslant_1$, $\leqslant_2$ and $\leqslant_3$.

Summary. The existing approaches for VCC either lack adequacy because they force non-native language interfaces on semantics for open modules (e.g., CompComp) or lack compositionality that is truly extensional because they depend on intermediate semantics used in compilation (e.g., CompCertM and CompCertO). Such dependency makes their correctness theorems for compiling open modules (e.g., libraries) difficult to further compose with and incurs a high cost in verification.

1.3 Challenges for Direct Refinement of Open Modules

The ideal approach to VCC should produce refinements that directly relate the native semantics of source and target open modules without mentioning any intermediate semantics and support both vertical and horizontal composition. We shall call them *direct refinements of open modules*. For example, a direct refinement between `a.c` and `a.s` could be $\leqslant_{\mathsf{ac}}\colon \mathcal{A} \Leftrightarrow C$ s.t. $[[\texttt{a.s}]] \leqslant_{\mathsf{ac}} [[\texttt{a.c}]]$. It relates assembly and C without mentioning intermediate semantics, and could be further horizontally composed with $[[\texttt{b.s}]] \leqslant_{\mathsf{ac}} L_b$ and vertically composed by adequacy to get $[[\texttt{a.s} + \texttt{b.s}]] \leqslant_{\mathsf{ac}} [[\texttt{a.c}]] \oplus L_b$. Note that even the top-level refinement is still open to horizontal and vertical composition, making direct refinements effective for supporting VCC for open modules.

The main challenge in getting direct refinements is tied to their "real" vertical composition, i.e., given any direct refinements $\leqslant_1$ and $\leqslant_2$, how to show $\leqslant_1 \cdot \leqslant_2$ is equivalent to a direct refinement $\leqslant_3$. This is considered very technical and involved (see Hur et al. [2012b]; Neis et al. [2015]; Patterson and Ahmed [2019]; Song et al. [2020]) because of the difficulty in constructing *interpolating* program states for transitively relating evolving source and target states across *external calls* of open modules. This problem also manifests in proving transitivity for *logical relations* where construction of interpolating terms of higher-order types is not in general possible [Ahmed 2006]. In the setting of compiling first-order languages with memory states, all previous work avoids proving real vertical composition of direct refinements. Some produce refinement without adequacy by introducing intrusive changes to semantics to make construction of interpolating states possible. For example, CompComp instruments the semantics of languages with *effect annotations* to expose internal effects for this purpose. Some essentially restrict vertical composition to *closed* programs (e.g., CompCertM). Some leave the top-level refinement a combination of refinements that still exposes the intermediate steps of compilation (e.g., CompCertO). Finally, even if the problem of vertical composition was solved, it is not clear if the solution can support realistic optimizing compilers.

1.4 Our Contributions

In this paper, we propose an approach to direct refinements for VCC of imperative programs that addresses all of the above challenges. Our approach is based on the memory model of CompCert which supports first-order states and pointers. We show that in this memory model interpolating states for proving vertical compositionality of refinements can be constructed by exploiting the properties on memory invariants known as *memory injections*. It is based on a new discovery that a *Kripke relation with memory protection* can serve as a uniform and composable relation for characterizing the evolution of memory states across external calls. With this relation we successfully combined the correctness theorems of CompCert's passes into a direct refinement between C and assembly modules. We summarize our technical contributions below:

- We prove that `injp`—a Kripke Memory Relation with a notion of memory protection—is both uniform (i.e., memory transformation in every compiler pass respects this relation) and composable (i.e., transitive modulo an equivalence relation). The critical observation making this proof possible is that interpolating memory states can be constructed by exploiting memory protection *inherent* to memory injections and the *functional* nature of injections.
- Based on the above observation, we show that a direct refinement from C to assembly can be derived by composing open refinements for all of CompCert's passes starting from Clight. In particular, we show that compiler passes can use different Kripke relations sufficient for their proofs (which may be weaker than `injp`) and these relations will later be absorbed into `injp` via refinements of open semantics. Furthermore, we show that assumptions for compiler optimizations can be formalized as *semantic invariants* and, when piggybacked onto `injp`, can be transitively composed. Based on these techniques, we upgrade the proofs in CompCertO to get a direct refinement from C to assembly for the full CompCert, including all of its optimization passes. These experiments show that direct refinements can be obtained without fundamental changes to the verification framework of CompCert.
- We demonstrate the simplicity and usefulness of direct refinements by applying it to end-to-end verification of several non-trivial examples with heterogeneous modules that *mutually* invoke each other. In particular, we observe that C level refinements can be absorbed into the direct refinement of CompCert by transitivity of `injp`. Combining direct refinements with full compositionality and adequacy, we derive end-to-end refinements from high-level source specifications to syntactically linked assembly modules in a straightforward manner.

The above developments are fully formalized in Coq based on the latest CompCertO (over CompCert v.3.10). [1] While the formalisation of our approach is tied to CompCert's block-based memory model [Leroy et al. 2012], and applied to its particular chain of compilation, we present evidence in §7 that variants of `injp` could be adapted for alternate memory models for first-order languages, and that it may be extended to support new optimizations. Therefore, this work provides a promising direction for further evolving the techniques for VCC.

1.5 Structure of the Paper

Below we first introduce the key ideas supporting this work in §2. We then introduce necessary background and discuss the technical challenges for building and applying direct refinements in §3. We present our technical contributions in §4, §5 and §6. We discuss the generality and limitations of our approach in §7. We discuss evaluation and related work in §8 and finally conclude in §9.

2 KEY IDEAS

[1] The artifact is located at https://doi.org/10.5281/zenodo.8424965.

```c
/* client.c */
int result;

void encrypt(int i,
     void(*p)(int*));

void process(int *r)
{
  result = *r;
}

int request(int i)
{
  encrypt(i,process);
  return i;
}
```

(a) Client in C

```
/* server.s */
key:
  .long 42
encrypt:
  // allocate frame
  Pallocframe 24 16 0
  // RSP[8] = i XOR key
  Pmov key RAX
  Pxor RAX RDI
  Pmov RDI 8(RSP)
  // call p(RSP + 8)
  Plea 8(RSP) RDI
  Pcall RSI
  // free frame
  Pfreeframe 24 16 0
  Pret
```

(b) Server in Asm

```
/* server_opt.s
 * key is an constant
 * and inlined in code */
encrypt:
  // allocate frame
  Pallocframe 24 16 0
  // RSP[8] = i XOR 42
  Pxori 42 RDI

  Pmov RDI 8(RSP)
  // call p(RSP + 8)
  Plea 8(RSP) RDI
  Pcall RSI
  // free frame
  Pfreeframe 24 16 0
  Pret
```

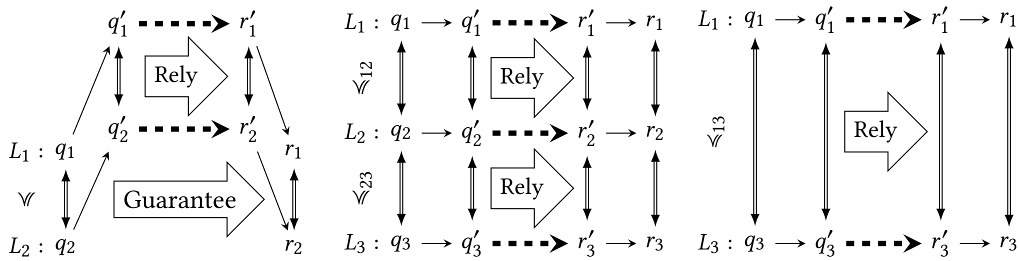
(c) Optimized Server

Fig. 3. An Example of Encryption Client and Server

We introduce a running example with heterogeneous modules and callback functions to illustrate the key ideas of our work. This example is representative of mutual dependency between modules that often appears in practice and it shows how free-form invocation between modules can be supported by our approach. As we shall see in §6, our approach also handles more complicated programs with mutually *recursive* heterogeneity without any problem.

The example is given in Fig. 3. It consists of a client written in C (Fig. 3a) and an encryption server hand-written in x86 assembly by using CompCert's assembly syntax where instruction names begin with `P` (Fig. 3b). For now, let us ignore Fig. 3c which illustrates how optimizations work in direct refinements. Users invoke `request` to initialize an encryption request. It is relayed to the function `encrypt` in the server with the prototype `void encrypt(int i, void (*p)(int*))` which respects a calling convention placing the first and second arguments in registers `RDI` and `RSI`, respectively. The main job of the server is to encrypt `i` (`RDI`) by XORing it with an encryption key (stored in the global variable `key`) and invoke the callback function `p` (`RSI`). Finally, the client takes over and stores the encrypted value in the global variable `result`. The pseudo instruction `Pallocframe m n o` allocates a stack frame of `m` bytes and stores its address in register `RSP`. In this frame, a pointer to the caller's stack frame is stored at the `o`-th byte and the return address is stored at the `n`-th byte. Note that `Pallocframe 24 16 0` in `encrypt` reserves 8 bytes on the stack from `RSP + 8` to `RSP + 16` for storing the encrypted value whose address is passed to the callback function `p`. `Pfreeframe m n o` frees the frame and restores `RSP` and the return address `RA`.

With the running example, our goal is to verify its end-to-end correctness by exploiting the direct refinement $\preccurlyeq_{\mathsf{ac}}: \mathcal{A} \Leftrightarrow C$ derived from CompCert's compilation chain as shown in Fig. 4. The verification proceeds as follows. First, we establish $[\![\texttt{client.s}]\!] \preccurlyeq_{\mathsf{ac}} [\![\texttt{client.c}]\!]$ by the correctness of compilation. Then, we prove $[\![\texttt{server.s}]\!] \preccurlyeq_{\mathsf{ac}} L_{\mathsf{S}}$ manually by providing a specification L_{S} for the server that respects the direct refinement. At the source level, the combined semantics is further refined to a single top-level specification L_{CS}. Finally, the source and target level refinements are absorbed into the direct refinement by vertical composition and adequacy, resulting in a *single*



(a) Rely-Guarantee Simulation (b) Naive Vertical Composition (c) A Direct Refinement

Fig. 5. Basic Concepts of Open Simulations

direct refinement between the top-level specification and the target program:

$$[[\texttt{client.s} + \texttt{server.s}]] \preccurlyeq_{\mathsf{ac}} L_{\mathsf{CS}}$$

The refinements of open modules discussed in our paper are based on forward simulations between small-step operational semantics (often in the form of *labeled transition systems* or LTS) which have been witnessed in a wide range of verification projects [Gu et al. 2015; Jiang et al. 2019; Koenig and Shao 2021; Song et al. 2020; Stewart et al. 2015; Wang et al. 2019]. Fig. 5a depicts a refinement $L_2 \preccurlyeq L_1$ between two open semantics (LTS) L_1 and L_2. The source (target) semantics L_1 (L_2) is initialized with a query (i.e., function call) q_1 (q_2) and may invoke an external call q_1' (q_2') as the execution goes. The execution continues when q_1' (q_2') returns with a reply r_1' (r_2') and finishes with a reply r_1 (r_2). For the refinement to hold, an invariant between the source and target program states must hold throughout the execution which is denoted by the vertical double arrows in Fig. 5a. Furthermore, this refinement relies on external calls satisfying certain well-behavedness conditions (known as *rely-conditions*; e.g., external calls do not modify the private memory of callers). In turn, it guarantees the entire source and target execution satisfy some well-behavedness conditions (known as *guarantee-conditions*, e.g., they do not modify the private memory of their calling environments). The rely-guarantee conditions are essential for horizontal composition: two refinements $L_1 \preccurlyeq L_2$ and $L_1' \preccurlyeq L_2'$ with complementary rely-guarantee conditions can be composed into a single refinement $L_1 \oplus L_2 \preccurlyeq L_1' \oplus L_2'$. However, vertical composition of such refinements is difficult. A naive vertical composition of two refinements (one between L_1 and L_2 and another between L_2 and L_3) simply concatenates them together like Fig. 5b, instead of generating a single refinement between L_1 and L_3 like Fig. 5c. This exposes the intermediate semantics (i.e., L_2) and imposes serious limitations on VCC as discussed in §1.[2] Therefore, to the best of our knowledge, none of the existing approaches fully support the verification outlined in Fig. 4.

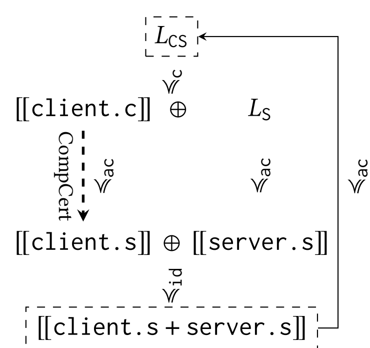


Fig. 4. Verifying the Running Example

To address the above problem, we develop direct refinements with the following distinguishing features: *1)* they always relate the semantics of modules at their native interfaces, thereby supporting

[2]To simplify the presentation, we often elide the guarantee conditions in figures for simulation.

adequacy, *2)* they do not mention the intermediate process of compilation, thereby supporting heterogeneous modules and compilers, *3)* they provide direct memory protection for source and target semantics via a Kripke relation, thereby enabling horizontal composition of refinements for heterogeneous modules, and most importantly *4)* they are vertically composable. The first three features are manifested in the very definition of direct refinements, which we shall discuss in §2.1 below. We then discuss the vertical composition of direct refinements in §2.2, which relies on the discovery of the uniformity and transitivity of a Kripke relation for memory protection.

2.1 Refinement Supporting Adequacy, Heterogeneity and Horizontal Composition

To illustrate the key ideas, we use the top-level direct refinement $\leqslant_{\mathsf{ac}}$ in Fig. 4 as an example. In the remaining discussions we adopt the block-based memory model of CompCert [Leroy et al. 2012] where a memory state consists of a disjoint set of *memory blocks*. $\leqslant_{\mathsf{ac}}$ is a forward simulation that directly relates C and assembly modules with their native language interfaces. By the definition of these interfaces (See §3.1), a C query $q_C = v_f[sg](\vec{v})@m$ is a function call to v_f with signature sg, a list of arguments $\vec{v}$ and a memory state m; a C reply $r_C = v'@m'$ carries a return value v' and an updated memory state m'. An assembly query $q_{\mathcal{A}} = rs@m$ invokes a function with the current register set rs and memory state m. An assembly reply $r_{\mathcal{A}} = rs'@m'$ returns from a function with the updated registers rs' and memory m'. By definition, $L_2 \leqslant_{\mathsf{ac}} L_1$ means that L_1 and L_2 *behave* like C and assembly programs at the boundary of modules, respectively. However, there is no restriction on how L_1 and L_2 are actually *implemented* internally, which enables specifications like L_S in Fig. 4.

The rely and guarantee conditions imposed by $\leqslant_{\mathsf{ac}}$ are symmetric and bundled with the simulation invariants at the boundary of modules. They make assumptions about how C and assembly queries should be related at the call sites and provide conclusions about how the replies should be related after the calls return. Given any matching source and target queries $q_C = v_f[sg](\vec{v})@m_1$ and $q_{\mathcal{A}} = rs@m_2$, it is assumed that

(1) The memory states are related by a memory invariant j known as a *memory injection function* [Leroy et al. 2012], i.e., memory blocks in m_1 are projected by j into those in m_2;
(2) The function pointer v_f in C query q_C is related to the program counter register;
(3) The arguments $\vec{v}$ in q_C are projected either to registers or to outgoing argument slots in the stack frame `RSP` according to the C calling convention;
(4) The outgoing arguments region in target stack frame is *freeable* and not in the image of j.

The first three requirements ensure that C arguments and memory are related to assembly registers and memory according to CompCert's C calling convention. The last one ensures outgoing arguments are protected, thereby preserving the invariant of open simulation across external calls.

After the function calls return, the source and target queries $r_C = res@m_1'$ and $r_{\mathcal{A}} = rs'@m_2'$ must satisfy the following requirements:

(1) The updated memory states m_1' and m_2' are related by an updated memory injection j';
(2) The C-level return value res is related to the value stored in the register for return value;
(3) For any callee-saved register r, $rs'(r) = rs(r)$;
(4) The stack pointer register and program counter are restored.
(5) The access to memory during the function call is protected by a *Kripke Memory Relation* `injp` such that the private stack data for other function calls are not touched.

The first two requirements ensure that return values and memories are related according to the calling convention. The following two ensure that registers are correctly restored before returning. The last requirement plays a critical role in rely-guarantee reasoning and enables horizontal composition of direct refinements as we shall see soon.

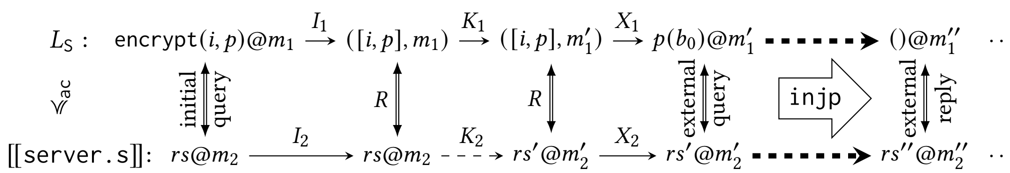


Fig. 6. Direct Refinement of the Hand-written Server

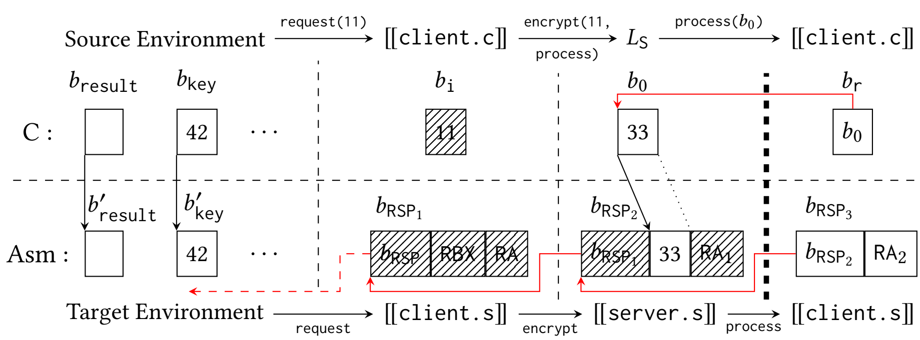


Fig. 7. Snapshot of the Memory State after Call Back

2.1.1 Adequacy and Heterogeneity via Direct Refinement. By definition, $\preccurlyeq_{\text{ac}}$ is basically a formalized C calling convention for CompCert with direct relations between C and assembly operational semantics and with invariants for protecting register values and memory states. Adequacy is automatically guaranteed as syntactic linking coincides with semantics linking at the assembly level. That is, given any assembly modules `a.s` and `b.s`, $[\![\texttt{a.s} + \texttt{b.s}]\!] \preccurlyeq_{\text{id}} [\![\texttt{a.s}]\!] \oplus [\![\texttt{b.s}]\!]$.

Moreover, $\preccurlyeq_{\text{ac}}$ does not mention anything about compilation. It works for any heterogeneous module and compilation chain that meet its requirements, even for hand-written assembly. Take the refinement of $[\![\texttt{server.s}]\!] \preccurlyeq_{\text{ac}} L_S$ in Fig. 4 as an example. The first few steps of the simulation are depicted in Fig. 6, where L_S is an LTS hand-written by users and $[\![\texttt{server.s}]\!]$ is derived from the CompCert assembly semantics. Because L_S is only required to respect the C interface, we choose a form easy to comprehend where its internal executions are in big steps. Now, suppose the environment calls `encrypt` with source and target queries initially related by CompCert's calling convention s.t. $rs(\texttt{RDI}) = i$ and $rs(\texttt{RSI}) = p$. After the initialization I_1 and I_2, the execution enters internal states related by an invariant R. Then, the target execution takes internal steps K_2 until reaching an external call. This corresponds to executing lines 5-13 in Fig. 3b, which allocates the stack frame RSP, performs encryption by storing `i XOR key` at the address RSP+8, and calls back p with RSP+8. At the source level, these steps correspond to one big-step execution K_1 which allocates a memory block b_0, stores `i XOR key` at b_0, and prepares to call p with b_0. Therefore, the memory injection in R maps b_0 to RSP+8. The source and target execution continue with transitions X_1 and X_2 to the external calls to p, return from p and go on until they return from `encrypt`.

2.1.2 Horizontal Composition via Kripke Memory Relations. The Kripke Memory Relation (KMR) `injp` provides essential protection for private values on the stack, which ensures that simulations between heterogeneous modules can be established and their horizontal composition is feasible.

We illustrate these points via our running example. Assume that the environment calls `request` in the client with 11 which in turn calls `encrypt` in the server to get the value 11 `XOR` 42 = 33 whose address is passed back to the client by calling `process`. Fig. 7 depicts a snapshot of the memory states and the injection right after `process` is entered (i.e., at line 8 in Fig. 3a), where boxes denote allocated memory blocks, black arrows between blocks denote injections, and red arrows denote pointers. The source semantics allocates one block for each local variable (b_i for `i`, b_0 for the encrypted value 33 and b_r for `r`) while the target semantics stores their values in registers or stacks (11 is stored in `RDI` while 33 on the stack because its address is taken and may be modified by the callee). One stack frame is allocated for each function call which stores private data including pointers to previous frames (b_{RSP}), return addresses (RA), and callee-saved registers (e.g., `RBX`).

`injp` is essential for proving simulation for open modules as it guarantees simulation can be re-established after external calls return. Informally, at every external call site, `injp` marks all memory regions outside the footprint (domain and image) of the current injection as *private* and does not allow the external call to modify those memory regions. From the perspective of `server.s`, when the snapshot in Fig. 7 is taken, the execution is inside the thick dashed line in Fig. 6 and protected by `injp`. Therefore, all the shaded memory in Fig. 7 are marked as private and protected against the callback to `process`. Indeed, they correspond to either memory values turned into temporary variables (e.g., b_i) or private stack data (e.g., b_{RSP}, `RBX` and RA) that should not be touched by `process`. Such protection ensures that when `process` returns, all the private stack values (e.g., the return addresses) are still valid, thereby re-establishing the simulation invariants.

The role of `injp` is reversed for the incoming calls from the environment: it guarantees that the entire execution from the initial query to the final reply will not touch any private memory of the environment. Therefore, `injp` is used to impose a reliance on memory protection for external calls and to provide a *symmetric* guarantee of memory protection for the environment callers. Any simulations with compatible language interfaces that satisfy this rely-guarantee condition can be horizontally composed. For example, we can horizontally compose $[\![\texttt{client.s}]\!] \preccurlyeq_{\mathsf{ac}} [\![\texttt{client.c}]\!]$ and $[\![\texttt{server.s}]\!] \preccurlyeq_{\mathsf{ac}} L_{\mathsf{S}}$ into $[\![\texttt{client.s}]\!] \oplus [\![\texttt{server.s}]\!] \preccurlyeq_{\mathsf{ac}} [\![\texttt{client.c}]\!] \oplus L_{\mathsf{S}}$ in Fig. 4.

2.2 Uniform and Transitive KMR for Vertical Composition of Direct Refinements

Direct refinements are only useful if they can be vertically composed, which is critical for composing refinements obtained from individual compiler passes into a single top-level refinement such as $\preccurlyeq_{\mathsf{ac}}$ and for further composition with source-level refinements as shown in Fig. 4.

We discuss our approach for addressing this problem by using CompCert and CompCertO as the concrete platforms. It is based on the following two observations. First, `injp` in fact captures the rely-guarantee conditions for memory protection needed by every compiler pass in CompCert. At a high-level, it means that the rely-guarantee conditions as depicted in Fig. 5 can all be replaced by `injp` (modulo the details on language interfaces). Second, `injp` is transitively composable, i.e., any vertical pairing of `injp` can be proved equivalent to a single `injp`. It means that given two refinements $L_2 \preccurlyeq_{12} L_1$ and $L_3 \preccurlyeq_{23} L_2$ as depicted in Fig. 5b, when their rely-guarantee conditions are uniformly represented by `injp`, they can be merged into the direct refinement $L_3 \preccurlyeq_{13} L_1$ in Fig. 5c with a single `injp` as the rely-guarantee condition. We shall present the technical challenges leading to these observations in §3 and elaborate on the observations themselves in §4.

By the above observations, an obvious approach for applying direct refinements to realistic optimizing compilers is to prove open simulation for every compiler pass using `injp`, and vertically compose those simulations into a single simulation. However, for a non-trivial compiler like CompCert, it means we need to rewrite a significant part of its proofs. More importantly, optimization passes in CompCert need stronger rely-guarantee conditions than `injp` as they are based on value analysis. To address the first problem, we start from the refinement proofs with least restrictive

KMRs for individual passes in CompCertO [Koenig and Shao 2021], and exploit the properties that these KMRs can eventually be "absorbed" into `injp` in vertical composition to generate a direct refinement parameterized by `injp`. To address the second problem, we propose a notion of *semantic invariant* that captures the rely-guarantee conditions for value analysis. When piggybacked onto `injp`, this semantic invariant can be transitively composed along with `injp` and eventually pushed to the C level. It then becomes a condition for enabling optimizations at the source level, e.g., for supporting the refinement of the optimized server in Fig. 3c. We discuss those solutions in §5.

Finally, we observe that source-level refinements can also be parameterized by `injp`, which enables end-to-end program verification as depicted in Fig. 4 as we shall discuss in §6.

3 BACKGROUND AND CHALLENGES

3.1 Background

We introduce necessary background, including the memory model, the framework for simulation-based refinement, and `injp` which is critical for direct refinements.

3.1.1 Block-based Memory Model. By Leroy et al. [2012], a memory state m (of type $\texttt{mem}$) consists of a disjoint set of *memory blocks* with unique identifiers and linear address space. A memory address or pointer (b, o) points to the o-th byte in the block b where b has type $\texttt{block}$ and o has type $\texttt{Z}$ (integers). The value at (b, o) is denoted by $m[b, o]$. Values (of type $\texttt{val}$) are either undefined ($\texttt{Vundef}$), 32- or 64-bit integers or floats, or pointers of the form $\texttt{Vptr}(b, o)$. For simplicity, we often write b for $\texttt{Vptr}(b, 0)$. The memory operations including allocation, free, read and write are provided and governed by permissions of cells. The permission of a memory cell is ordered from high to low as $\texttt{Freeable} \geqslant \texttt{Writable} \geqslant \texttt{Readable} \geqslant \texttt{NA}$ where $\texttt{Freeable}$ enables all operations, $\texttt{Writable}$ enables all but free, $\texttt{Readable}$ enables only read, and $\texttt{NA}$ enables none. If $p_1 \geqslant p_2$ then any cell with permission p_1 also implicitly has permission p_2. $\texttt{perm}(m, P)$ denotes the set of memory cells with at least permission P. For example, $(b, o) \in \texttt{perm}(m, \texttt{Readable})$ iff the cell at (b, o) in m is readable. An address with no permission at all is not in the footprint of memory.

Transformations of memory states are captured via partial functions $j : \texttt{block} \to \lfloor \texttt{block} \times \texttt{Z} \rfloor$ called *injection functions*, s.t. $j(b) = \emptyset$ if b is removed from memory and $j(b) = \lfloor (b', o) \rfloor$ if b is shifted (injected) to (b', o) in the target memory. We define $\texttt{meminj} = \texttt{block} \to \lfloor \texttt{block} \times \texttt{Z} \rfloor$. v_1 and v_2 are related under j (denoted by $v_1 \hookrightarrow^j_v v_2$) if either v_1 is $\texttt{Vundef}$, or they are both equal scalar values, or pointers shifted according to j, i.e., $v_1 = \texttt{Vptr}(b, o)$, $j(b) = \lfloor (b', o') \rfloor$ and $v_2 = \texttt{Vptr}(b', o + o')$.

Given this relation, there is a *memory injection* between the source memory state m_1 and the target state m_2 under j (denoted by $m_1 \hookrightarrow^j_m m_2$) if the following properties are satisfied which ensure preservation of permissions and values under injection:

$$\forall\, b_1\ b_2\ o\ o'\ p,\ \ j(b_1) = \lfloor (b_2, o') \rfloor \Rightarrow (b_1, o) \in \texttt{perm}(m_1, p) \Rightarrow (b_2, o + o') \in \texttt{perm}(m_2, p)$$
$$\forall\, b_1\ b_2\ o\ o',\ \ j(b_1) = \lfloor (b_2, o') \rfloor \Rightarrow (b_1, o) \in \texttt{perm}(m_1, \texttt{Readable}) \Rightarrow m_1[b_1, o] \hookrightarrow^j_v m_2[b_2, o + o']$$

Memory injections are necessary for verifying compiler transformations of memory structures (e.g., merging local variables into stack-allocated data and generating a concrete stack frame). For the remaining passes, a simpler relation called *memory extension* is used instead, which employs an identity injection. Reasoning about permissions under refinements is a major source of complexity.

3.1.2 A Framework for Open Simulations. In CompCertO [Koenig and Shao 2021], a *language interface* $A = \langle A^q, A^r \rangle$ is a pair of sets A^q and A^r denoting acceptable queries and replies for open modules, respectively. Different interfaces may be used for different languages. The relevant ones for our discussion have been introduced in §2.1 and listed as follows:

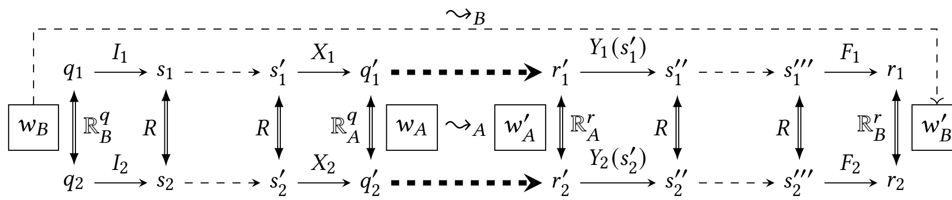


Fig. 8. Open Simulation between LTS

Languages	**Interfaces**	**Queries**	**Replies**
C/Clight	$C = \langle \mathtt{val} \times \mathtt{sig} \times \mathtt{val}^* \times \mathtt{mem}, \mathtt{val} \times \mathtt{mem} \rangle$	$v_f[sg](\vec{v})@m$	$v'@m'$
Asm	$\mathcal{A} = \langle \mathtt{regset} \times \mathtt{mem}, \mathtt{regset} \times \mathtt{mem} \rangle$	$rs@m$	$rs'@m'$

Open labeled transition systems (LTS) represent semantics of modules that may accept queries and provide replies at the *incoming side* and provide queries and accept replies at the *outgoing side* (i.e., calling external functions). An open LTS $L : A \twoheadrightarrow B$ is a tuple $\langle D, S, I, \rightarrow, F, X, Y \rangle$ where A (B) is the language interface for outgoing (incoming) queries and replies, $D \subseteq B^q$ a set of initial queries, S a set of internal states, $I \subseteq D \times S$ ($F \subseteq S \times B^r$) transition relations for incoming queries (replies), $X \subseteq S \times A^q$ ($Y \subseteq S \times A^r \times S$) transitions for outgoing queries (replies), and $\rightarrow \subseteq S \times \mathcal{E}^* \times S$ internal transitions emitting events of type $\mathcal{E}$. Note that $(s, q^O) \in X$ iff an outgoing query q^O happens at s; $(s, r^O, s') \in Y$ iff after q^O returns with r^O the execution continues with an updated state s'.

Kripke relations are used to describe evolution of program states in open simulations between LTSs. A Kripke relation $R : W \rightarrow \{S \mid S \subseteq A \times B\}$ is a family of relations indexed by a *Kripke world* W; for simplicity, we define $\mathcal{K}_W(A, B) = W \rightarrow \{S \mid S \subseteq A \times B\}$. A *simulation convention* relating two language interfaces A_1 and A_2 is a tuple $\mathbb{R} = \langle W, \mathbb{R}^q : \mathcal{K}_W(A_1^q, A_2^q), \mathbb{R}^r : \mathcal{K}_W(A_1^r, A_2^r) \rangle$ which we write as $\mathbb{R} : A_1 \Leftrightarrow A_2$. Simulation conventions serve as interfaces of open simulations by relating source and target language interfaces. For example, a C-level convention $\mathtt{c} : C \Leftrightarrow C = \langle \mathtt{meminj}, \mathbb{R}_{\mathtt{c}}^q, \mathbb{R}_{\mathtt{c}}^r \rangle$ relates C queries and replies as follows, where the Kripke world consists of injections and, in a given world j, the values and memory in queries and replies are related by j.

$$
\begin{aligned}
(v_f[sg](\vec{v})@m, v_f'[sg](\vec{v}')@m') \in \mathbb{R}_{\mathtt{c}}^q(j) \quad &\Leftrightarrow \quad v_f \hookrightarrow_v^j v_f' \land \vec{v} \hookrightarrow_v^j \vec{v}' \land m \hookrightarrow_m^j m' \\
(v@m, v'@m') \in \mathbb{R}_{\mathtt{c}}^r(j) \quad &\Leftrightarrow \quad v \hookrightarrow_v^j v' \land m \hookrightarrow_m^j m'
\end{aligned}
$$

Open forward simulations describe refinement between LTS. To establish an open (forward) simulation between $L_1 : A_1 \twoheadrightarrow B_1$ and $L_2 : A_2 \twoheadrightarrow B_2$, one needs to find two simulation conventions $\mathbb{R}_A : A_1 \Leftrightarrow A_2$ and $\mathbb{R}_B : B_1 \Leftrightarrow B_2$ that connect queries and replies at the outgoing and incoming sides, and show the internal execution steps and external interactions of open modules are related by an invariant R. This simulation is denoted by $L_1 \leqslant_{\mathbb{R}_A \twoheadrightarrow \mathbb{R}_B} L_2$ and formally defined as follows (for simplicity, we shall write $L_1 \leqslant_{\mathbb{R}} L_2$ to denote $L_1 \leqslant_{\mathbb{R} \twoheadrightarrow \mathbb{R}} L_2$):

Definition 3.1. Given $L_1 : A_1 \twoheadrightarrow B_1$, $L_2 : A_2 \twoheadrightarrow B_2$, $\mathbb{R}_A : A_1 \Leftrightarrow A_2$ and $\mathbb{R}_B : B_1 \Leftrightarrow B_2$, $L_1 \leqslant_{\mathbb{R}_A \twoheadrightarrow \mathbb{R}_B} L_2$ holds if there is some Kripke relation $R \in \mathcal{K}_{W_B}(S_1, S_2)$ that satisfies:

(1) $\forall\, q_1\; q_2,\; (q_1, q_2) \in \mathbb{R}_B^q(w_B) \Rightarrow (q_1 \in D_1 \Leftrightarrow q_2 \in D_2)$

(2) $\forall\, w_B\; q_1\; q_2\; s_1,\; (q_1, q_2) \in \mathbb{R}_B^q(w_B) \Rightarrow (q_1, s_1) \in I_1 \Rightarrow \exists\, s_2, (s_1, s_2) \in R(w_B) \land (q_2, s_2) \in I_2.$

(3) $\forall\, w_B\; s_1\; s_2\; t,\; (s_1, s_2) \in R(w_B) \Rightarrow s_1 \xrightarrow{t} s_1' \Rightarrow \exists\, s_2', (s_1', s_2') \in R(w_B) \land s_2 \xrightarrow{t}{}^{*} s_2'.$

(4) $\forall\, w_B\; s_1\; s_2\; q_1,\; (s_1, s_2) \in R(w_B) \Rightarrow (s_1, q_1) \in X_1 \Rightarrow$
$\quad \exists w_A\; q_2,\; (q_1, q_2) \in \mathbb{R}_A^q(w_A) \land (s_2, q_2) \in X_2 \land$
$\quad\quad \forall\, r_1\; r_2\; s_1', (r_1, r_2) \in \mathbb{R}_A^r(w_A) \Rightarrow (s_1, r_1, s_1') \in Y_1 \Rightarrow \exists\, s_2', (s_1', s_2') \in R(w_B) \land (s_2, r_2, s_2') \in Y_2.$

(5) $\forall\, w_B\; s_1\; s_2\; r_1,\; (s_1, s_2) \in R(w_B) \Rightarrow (s_1, r_1) \in F_1 \Rightarrow \exists\, r_2, (r_1, r_2) \in \mathbb{R}_B^r(w_B) \land (s_2, r_2) \in F_2.$

Here, property (1) requires initial queries to match; (2) requires initial states to hold under the invariant R; (3) requires internal execution to preserve R; (4) requires R to be preserved across external calls, and (5) requires final replies to match. According to these properties, a complete forward simulation looks like Fig. 8. From the above definition, it is easy to prove the horizontal and vertical compositionality of open simulations and adequacy for assembly modules, i.e., $\forall\ (L_1, L_2, L_1', L_2'),\ L_1 \leqslant_{\mathbb{R}} L_2 \Rightarrow L_1' \leqslant_{\mathbb{R}} L_2' \Rightarrow L_1 \oplus L_1' \leqslant_{\mathbb{R}} L_2 \oplus L_2'$ and $\forall\ (M_1, M_2 : \mathtt{Asm}),\ [[M_1]] \oplus [[M_2]] \leqslant_{\mathtt{id}} [[M_1 + M_2]]$.

The Kripke worlds (e.g., memory injections) may evolve as the execution goes on. *Rely-guarantee* reasoning about such evolution is essential for horizontal composition of simulations. For illustration, the Kripke worlds at the boundary of modules are displayed in Fig. 8. The evolution of worlds across external calls is governed by an *accessibility relation* $w_A \leadsto_A w_A'$ for describing the *rely-condition*. By assuming $w_A \leadsto_A w_A'$, one needs to prove the *guarantee condition* $w_B \leadsto_B w_B'$, i.e., the evolution of worlds in the whole execution respects $\leadsto_B$. Simulations with symmetric rely-guarantee conditions can be horizontally composed, even with mutual calls between modules.

Note that the accessibility relation and evolution of worlds between queries and replies is not encoded explicitly in the definition of simulation conventions. Instead, they are implicit by assuming a modality operator $\diamond$ is always applied to $\mathbb{R}^r$ s.t. $r \in \diamond\mathbb{R}^r(w) \Leftrightarrow \exists\ w', w \leadsto w' \land r \in \mathbb{R}^r(w')$. For simplicity, we often ignore accessibility and modality when talking *purely* about properties of simulations conventions in the remaining discussion.

Accessibility relations are mainly for describing evolution of memory states across external calls. For this, simulation conventions are parameterized by *Kripke Memory Relations* or KMR.

Definition 3.2. A Kripke Memory Relation is a tuple $\langle W, f, \leadsto, R\rangle$ where W is a set of worlds, $f : W \to \mathtt{meminj}$ a function for extracting injections from worlds, $\leadsto \subseteq W \times W$ an accessibility relation between worlds and $R : \mathcal{K}_W(\mathtt{mem}, \mathtt{mem})$ a Kripke relation over memory states that is compatible with the memory operations. We write $w \leadsto w'$ for $(w, w') \in \leadsto$.

We write $\mathbb{R}_K$ to emphasize that a convention $\mathbb{R}$ is parameterized by the KMR K, meaning $\mathbb{R}_K$ shares the same type of worlds with K and inherits its accessibility relation.

The most interesting KMR is `injp` as it provides protection on memory w.r.t. injections.

Definition 3.3 (Kripke Relation with Memory Protection). $\mathtt{injp} = \langle W_{\mathtt{injp}}, f_{\mathtt{injp}}, \leadsto_{\mathtt{injp}}, R_{\mathtt{injp}}\rangle$ where $W_{\mathtt{injp}} = (\mathtt{meminj} \times \mathtt{mem} \times \mathtt{mem})$, $f_{\mathtt{injp}}(j, \_, \_) = j$, $(m_1, m_2) \in R_{\mathtt{injp}}(j, m_1, m_2) \Leftrightarrow m_1 \hookrightarrow_m^j m_2$ and

$$\begin{array}{rcl}(j, m_1, m_2) \leadsto_{\mathtt{injp}} (j', m_1', m_2') & \Leftrightarrow & j \subseteq j' \land \mathtt{unmapped}(j) \subseteq \mathtt{unchanged\text{-}on}(m_1, m_1') \\ & & \land\ \mathtt{out\text{-}of\text{-}reach}(j, m_1) \subseteq \mathtt{unchanged\text{-}on}(m_2, m_2'). \\ & & \land\ \mathtt{mem\text{-}acc}(m_1, m_1') \land\ \mathtt{mem\text{-}acc}(m_2, m_2')\end{array}$$

Here, $\mathtt{mem\text{-}acc}(m, m')$ denotes monotonicity of memory states such as valid blocks can only increase and read-only data does not change in value. $\mathtt{unchanged\text{-}on}(m, m')$ denotes memory cells whose permissions and values are not changed from m to m' and

$$\begin{array}{lcl}(b_1, o_1) \in \mathtt{unmapped}(j) & \Leftrightarrow & j(b_1) = \emptyset \\ (b_2, o_2) \in \mathtt{out\text{-}of\text{-}reach}(j, m_1) & \Leftrightarrow & \forall\ b_1\ o_2',\ j(b_1) = \lfloor (b_2, o_2') \rfloor \Rightarrow (b_1, o_2 - o_2') \notin \mathtt{perm}(m_1, \mathsf{NA}).\end{array}$$

Intuitively, a world (j, m_1, m_2) evolves to (j', m_1', m_2') under `injp` only if j' is strictly larger than j and any memory cells in m_1 and m_2 not in the domain (i.e., unmapped by j), or image of j (i.e., out of reach by j from m_1) will be protected, meaning their values and permissions are unchanged from m_1 (m_2) to m_1' (m_2'). An example is shown in Fig. 9 where the shaded regions in m_1 are unmapped by j and unchanged while those in m_2 are out-of-reach from j and unchanged. m_1' and m_2' may contain newly allocated blocks which are not protected by `injp`. When `injp` is used at the outgoing side, it denotes that the simulation relies on knowing that the unmapped and out-of-reach regions at the call side are not modified by external calls. When `injp` is used at incoming side, it denotes that the simulation guarantees such regions at initial queries are not modified by the simulation itself.

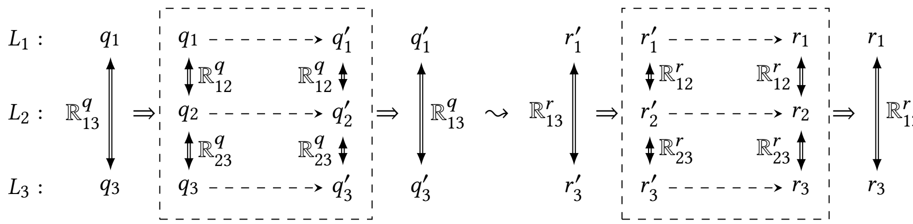


Fig. 10. Vertical Composition of Open Simulations by Refinement of Simulation Conventions

3.2 Challenges for Vertically Composing Open Simulations

As discussed in §2.2, the challenge for constructing direct refinements for multi-pass optimizing compilers lies in their vertical composition. The most basic vertical composition for open simulations is stated below which is easily proved by pairing of individual simulations [Koenig and Shao 2021].

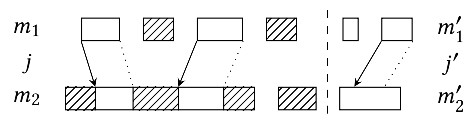


Fig. 9. Kripke Worlds Related by `injp`

Theorem 3.4 (V. Comp). *Given $L_1 : A_1 \twoheadrightarrow B_1$, $L_2 : A_2 \twoheadrightarrow B_2$ and $L_3 : A_3 \twoheadrightarrow B_3$, and given $\mathbb{R}_{12} : A_1 \Leftrightarrow A_2$, $\mathbb{S}_{12} : B_1 \Leftrightarrow B_2$, $\mathbb{R}_{23} : A_2 \Leftrightarrow A_3$ and $\mathbb{S}_{23} : B_2 \Leftrightarrow B_3$,*

$$L_1 \leqslant_{\mathbb{R}_{12} \twoheadrightarrow \mathbb{S}_{12}} L_2 \Rightarrow L_2 \leqslant_{\mathbb{R}_{23} \twoheadrightarrow \mathbb{S}_{23}} L_3 \Rightarrow L_1 \leqslant_{\mathbb{R}_{12} \cdot \mathbb{R}_{23} \twoheadrightarrow \mathbb{S}_{12} \cdot \mathbb{S}_{23}} L_3.$$

Here, $(\_ \cdot \_)$ is a composed simulation convention s.t. $\mathbb{R} \cdot \mathbb{S} = \langle W_{\mathbb{R}} \times W_{\mathbb{S}}, \mathbb{R}^q \cdot \mathbb{S}^q, \mathbb{R}^r \cdot \mathbb{S}^r \rangle$ where for any q_1 and q_3, $(q_1, q_3) \in \mathbb{R}^q \cdot \mathbb{S}^q(w_{\mathbb{R}}, w_{\mathbb{S}}) \Leftrightarrow \exists q_2, (q_1, q_2) \in \mathbb{R}^q(w_{\mathbb{R}}) \wedge (q_2, q_3) \in \mathbb{S}^q(w_{\mathbb{S}})$ (similarly for $\mathbb{R}^r \cdot \mathbb{S}^r$). Then, given any compiler with N passes and their refinement relations $L_1 \leqslant_{\mathbb{R}_{12} \twoheadrightarrow \mathbb{S}_{12}} L_2, \ldots, L_N \leqslant_{\mathbb{R}_{N,N+1} \twoheadrightarrow \mathbb{S}_{N,N+1}} L_{N+1}$, we get their concatenation $L_1 \leqslant_{\mathbb{R}_{12} \cdot \ldots \cdot \mathbb{R}_{N,N+1} \twoheadrightarrow \mathbb{S}_{12} \cdot \ldots \cdot \mathbb{S}_{N,N+1}} L_{N+1}$, which exposes internal compilation and weakens compositionality as we have discussed in §1.2.

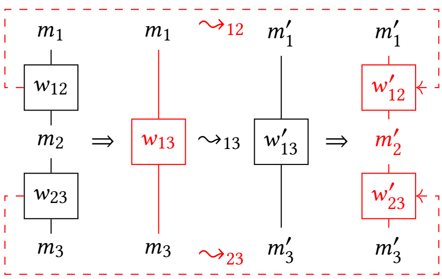
The above problem may be solved if the composed simulation convention can be *refined* into a single convention directly relating source and target queries and replies. Given two simulation conventions $\mathbb{R}, \mathbb{S} : A_1 \Leftrightarrow A_2$, $\mathbb{R}$ is *refined* by $\mathbb{S}$ if

$$\forall\, w_{\mathbb{S}}\; q_1\; q_2,\; (q_1, q_2) \in \mathbb{S}^q(w_{\mathbb{S}}) \Rightarrow \exists\, w_{\mathbb{R}},\; (q_1, q_2) \in \mathbb{R}^q(w_{\mathbb{R}}) \wedge$$
$$\forall\, r_1\; r_2,\; (r_1, r_2) \in \mathbb{R}^r(w_{\mathbb{R}}) \Rightarrow (r_1, r_2) \in \mathbb{S}^r(w_{\mathbb{S}})$$

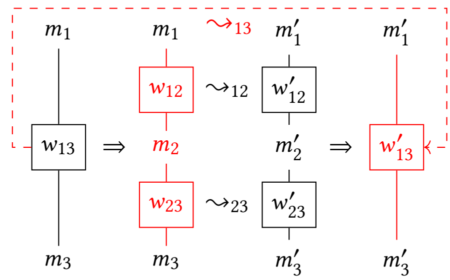
which we write as $\mathbb{R} \sqsubseteq \mathbb{S}$. If both $\mathbb{R} \sqsubseteq \mathbb{S}$ and $\mathbb{S} \sqsubseteq \mathbb{R}$, then $\mathbb{R}$ and $\mathbb{S}$ are equivalent and written as $\mathbb{R} \equiv \mathbb{S}$. By definition, $\mathbb{R} \sqsubseteq \mathbb{S}$ indicates any query for $\mathbb{S}$ can be converted into a query for $\mathbb{R}$ and any reply resulting from the converted query can be converted back to a reply for $\mathbb{S}$. By wrapping the incoming side of an open simulation with a more general convention and its outgoing side with a more specialized convention, one gets another valid open simulation [Koenig and Shao 2021]:

Theorem 3.5. *Given $L_1 : A_1 \twoheadrightarrow B_1$ and $L_2 : A_2 \twoheadrightarrow B_2$, if $\mathbb{R}'_A \sqsubseteq \mathbb{R}_A : A_1 \Leftrightarrow A_2$, $\mathbb{R}_B \sqsubseteq \mathbb{R}'_B : B_1 \Leftrightarrow B_2$ and $L_1 \leqslant_{\mathbb{R}_A \twoheadrightarrow \mathbb{R}_B} L_2$, then $L_1 \leqslant_{\mathbb{R}'_A \twoheadrightarrow \mathbb{R}'_B} L_2$.*

Now, we would like to prove the "real" vertical composition generating direct refinements (simulations). Given any $L_1 \leqslant_{\mathbb{R}_{12} \twoheadrightarrow \mathbb{R}_{12}} L_2$ and $L_2 \leqslant_{\mathbb{R}_{23} \twoheadrightarrow \mathbb{R}_{23}} L_3$, if we can show the existence of simulation conventions $\mathbb{R}_{13}$ directly relating source and target semantics s.t. $\mathbb{R}_{13} \equiv \mathbb{R}_{12} \cdot \mathbb{R}_{23}$, then $L_1 \leqslant_{\mathbb{R}_{13} \twoheadrightarrow \mathbb{R}_{13}} L_3$ holds by Theorem 3.4 and Theorem 3.5, which is the desired direct refinement. This composition is illustrated in Fig. 10 where the parts enclosed by dashed boxes represent the concatenation of $L_1 \leqslant_{\mathbb{R}_{12} \twoheadrightarrow \mathbb{R}_{12}} L_2$ and $L_2 \leqslant_{\mathbb{R}_{23} \twoheadrightarrow \mathbb{R}_{23}} L_3$. The direct queries and replies are split and merged for interaction with parallelly running simulations underlying the direct refinement.



(a) $K_{13} \sqsubseteq K_{12} \cdot K_{23}$



(b) $K_{12} \cdot K_{23} \sqsubseteq K_{13}$

Fig. 11. Composition of KMRs

Since open simulations are parameterized by KMRs, a major obstacle to their "real" vertical composition is to prove KMRs for individual simulations can be composed into a single KMR. For this, one needs to define refinements between KMRs. Given any KMRs K and L, $K \sqsubseteq L$ (i.e., K is refined by L) holds if the following is true:

$$
\begin{aligned}
\forall\, w_L,\ (m_1, m_2) \in R_L(w_L) \Rightarrow \exists\, w_K,\ & (m_1, m_2) \in R_K(w_K) \wedge f_L(w_L) \subseteq f_K(w_K) \wedge \\
& \forall\, w'_K\ m'_1\ m'_2,\ w_K \rightsquigarrow_K w'_K \Rightarrow (m'_1, m'_2) \in R_K(w'_K) \Rightarrow \\
& \quad \exists\, w'_L,\ w_L \rightsquigarrow_L w'_L \wedge (m'_1, m'_2) \in R_L(w'_L) \wedge f_K(w'_K) \subseteq f_L(w'_L).
\end{aligned}
$$

We write $K \equiv L$ to denote that K and L are equivalent, i.e., $K \sqsubseteq L$ and $L \sqsubseteq K$.

Continue with the proof of real vertical composition. Assume $\mathbb{R}_i$ is parameterized by KMR K_i, showing the existence of $\mathbb{R}_{13}$ s.t. $\mathbb{R}_{13} \sqsubseteq \mathbb{R}_{12} \cdot \mathbb{R}_{23}$ amounts to proving a parallel refinement over the parameterizing KMRs, i.e., there exists K_{13} s.t. $K_{13} \sqsubseteq K_{12} \cdot K_{23}$ where $K_{12} \cdot K_{23} = \langle W_{12} \times W_{23}, f_{12} \times f_{23}, \rightsquigarrow_{12} \times \rightsquigarrow_{23}, R_{12} \times R_{23} \rangle$. A more intuitive interpretation is depicted in Fig. 11a where black symbols are $\forall$-quantified (assumptions we know) and red ones are $\exists$-quantified (conclusions we need to construct). Note that Fig. 11a exactly mirrors the refinement on the outgoing side in Fig. 10. For simplicity, we not only use w_i to represent worlds, but also to denote $R_i(w_i)$ (where R_i is the Kripke relation given by KMR K_i) when it connects memory states through vertical lines. A dual property we need to prove for the incoming side is shown in Fig. 11b.

In both cases in Fig. 11, we need to construct interpolating states for relating source and target memory (i.e., m'_2 in Fig. 11a and m_2 in Fig. 11b). The construction of m'_2 is especially challenging, for which we need to decompose the evolved world w'_{13} into w'_{12} and w'_{23} s.t. they are accessible from the original worlds w_{12} and w_{23}. It is not clear at all how this construction is possible because *1)* m'_2 may have many forms since Kripke *relations* are in general non-deterministic and *2)* KMR (e.g., injp) may introduce memory protection for external calls which may not hold after the composition.

Because of the above difficulties, existing approaches either make substantial changes to semantics for constructing interpolating states, thereby destroying adequacy [Stewart et al. 2015], or do not even try to merge Kripke memory relations, but instead leave them as separate entities [Koenig and Shao 2021; Song et al. 2020]. As a result, direct refinements cannot be achieved.

4 A UNIFORM AND TRANSITIVE KRIPKE MEMORY RELATION

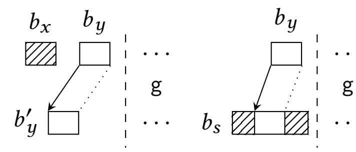
To overcome the challenge for vertically composing open simulations, we exploit the observation that `injp` in fact can be viewed as a most general KMR. Then, the compositionality of KMRs discussed in §3.2 is reduced to transitivity of `injp`, i.e., `injp` ≡ `injp` · `injp`.

$$\begin{tikzcd}
(b_1, o_1) \arrow[r, "\mathsf{read}"] \arrow[d, "j"'] & (b_2, o_2) \arrow[r, "\mathsf{read}"] \arrow[d, "j"'] & \cdots \\
(b_1', o_1') \arrow[r, "\mathsf{read}"] & (b_2', o_2') \arrow[r, "\mathsf{read}"] & \cdots
\end{tikzcd}$$

Fig. 12. Closure of Public Memory

```
void f() {
  int x, y;
  g(&y);
}
```

(a) Example



(b) SimplLocals (c) Stacking

Fig. 13. Protection of Private Memory by `injp`

4.1 Uniformity of `injp`

We show that `injp` is both a reasonable guarantee condition and a reasonable rely condition for all the compiler passes in CompCert. It is based on the observation that a notion of private and public memory can be derived from injections and coincides with the protection provided by `injp`.

4.1.1 Public and Private Memory via Memory Injections.

Definition 4.1. Given $m_1 \hookrightarrow_m^j m_2$, the public memory regions in m_1 and m_2 are defined as follows:

$\mathtt{pub\text{-}src\text{-}mem}(j) \quad = \{(b, o) \mid j(b) \neq \emptyset\};$
$\mathtt{pub\text{-}tgt\text{-}mem}(j, m_1) = \{(b, o) \mid \exists b'\ o', j(b') = \lfloor(b, o')\rfloor \wedge (b', o - o') \in \mathtt{perm}(m_1, \mathsf{NA})\}.$

By definition, a cell (b, o) is public in the source memory if it is in the domain of j, and (b, o) is public in the target memory if it is mapped by j from some valid public source memory. Any memory not public with respect to j is private. We can see that private memory corresponds exactly to unmapped and out-of-reach memory defined by `injp`, i.e., for any b and o, $(b, o) \in \mathtt{pub\text{-}src\text{-}mem}(j) \Leftrightarrow (b, o) \notin \mathtt{unmapped}(j)$ and $(b, o) \in \mathtt{pub\text{-}tgt\text{-}mem}(j, m) \Leftrightarrow (b, o) \notin \mathtt{out\text{-}of\text{-}reach}(j, m)$.

With Definition 4.1 and the properties of memory injection (see §3.1.1), we can easily prove access of pointers in a readable and public source location gets back another public location.

Lemma 4.2. *Given* $m_1 \hookrightarrow_m^j m_2$,

$\forall\, b_1\ o_1,\ (b_1, o_1) \in \mathtt{pub\text{-}src\text{-}mem}(j) \Rightarrow (b_1, o_1) \in \mathtt{perm}(m_1, \mathtt{Readable}) \Rightarrow$
$\qquad m_1[b_1, o_1] = \mathtt{Vptr}(b_1', o_1') \Rightarrow (b_1', o_1') \in \mathtt{pub\text{-}src\text{-}mem}(j).$

It implies that readable public memory regions form a "closure" such that the sequences of reads are bounded inside these regions, as shown in Fig. 12. The horizontal arrows indicates a pointer value (b_{i+1}, o_{i+1}) is read from (b_i, o_i) with possible adjustment with pointer arithmetic. Note that all memory cells at (b_i, o_i)s and (b_i', o_i')s have `Readable` permission. By Lemma 4.2, (b_i, o_i)s are all in public regions. By Definition 4.1, the mirroring reads (b_i', o_i')s are also in public regions.

4.1.2 `injp` *as a Uniform Rely Condition.* `injp` is adequate for preventing external calls from interfering with internal execution for all compiler passes of CompCert. [3] To illustrate this point, we discuss the effect of `injp` on two of CompCert's passes using the code in Fig. 13a as an example where g is an external function. The first pass is `SimplLocals` which converts local variables whose memory addresses are not taken into temporary ones. As shown in Fig. 13b, x is turned into a temporary variable at the target level which is not visible to g. Therefore, x at the source level becomes *private data* as its block b_x is unmapped by j, thereby protected by `injp` and cannot be modified by g. The second pass is `Stacking` which expands the stack frames with private regions for return addresses, spilled registers, arguments, etc. Continuing with our example, the only public stack data in Fig. 13c is y. All the private data is out-of-reach, thereby protected by `injp`.

[3] In fact, the properties in Definition 3.3 are exactly from CompCert's assumptions on external calls.

4.1.3 `injp` *as a Uniform Guarantee Condition.* For `injp` to serve as a uniform guarantee condition, it suffices to show the private memory of the environment is protected between initial calls and final replies. During an open forward simulation, all incoming values and memories are related by some initial injection j (e.g., $\vec{v_1} \hookrightarrow_v^j \vec{v_2}$ and $m_1 \hookrightarrow_m^j m_2$). In particular, the pointers in them are related by j. Therefore, any sequence of reads starting from pointers stored in the initial queries only inspect public memories in the source and target, as already shown in Fig. 12. Therefore, the private (i.e., unmapped or out-of-reach) regions of the initial memories are *not modified* by internal execution. Moreover, because injection functions only grow bigger during execution but never change in value and the outgoing calls have `injp` as a rely-condition, the initially unmapped (out-of-reach) regions will stay unmapped (out-of-reach) and be protected during external calls by `injp`. Therefore, we conclude that `injp` is a reasonable guarantee condition for any open simulation.

4.2 Transitivity of `injp`

The goal is to show the two refinements in Fig. 11 hold when K_{ij} = `injp`, i.e., `injp` ≡ `injp`·`injp`. As discussed in §3.2 the critical step is to construct interpolating memory states that transitively relate source and target states. The construction is based on two observations: *1)* the memory injections deterministically decide the value and permissions of public memory because they encode *partial functional transformations* on memory states, and *2)* any memory not in the domain or range of the partial function is protected (private) and unchanged throughout external calls. Although the proof is quite involved, the result can be reused for all compiler passes thanks to `injp`'s uniformity. The formal proof of transitivity of `injp` can be found in Appendix A.

4.2.1 `injp` ⊑ `injp` · `injp`. By definition, we need to prove the following lemma:

Lemma 4.3. `injp` ⊑ `injp` · `injp` *holds. That is,*

$$\begin{array}{l}\forall j_{12}\ j_{23}\ m_1\ m_2\ m_3,\ m_1 \hookrightarrow_m^{j_{12}} m_2 \Rightarrow m_2 \hookrightarrow_m^{j_{23}} m_3 \Rightarrow \exists j_{13},\ m_1 \hookrightarrow_m^{j_{13}} m_3 \land \\ \quad \forall m_1'\ m_3'\ j_{13}',\ (j_{13}, m_1, m_3) \leadsto_{\texttt{injp}} (j_{13}', m_1', m_3') \Rightarrow m_1' \hookrightarrow_m^{j_{13}'} m_3' \Rightarrow \\ \quad\quad \exists m_2'\ j_{12}'\ j_{23}', (j_{12}, m_1, m_2) \leadsto_{\texttt{injp}} (j_{12}', m_1', m_2') \land m_1' \hookrightarrow_m^{j_{12}'} m_2' \\ \quad\quad\quad\quad\quad \land (j_{23}, m_2, m_3) \leadsto_{\texttt{injp}} (j_{23}', m_2', m_3') \land m_2' \hookrightarrow_m^{j_{23}'} m_3'.\end{array}$$

This lemma conforms to the graphic representation in Fig. 11a. To prove it, an obvious choice is to pick $j_{13} = j_{23} \cdot j_{12}$. Then we are left to prove the existence of interpolating state m_2' and the memory and accessibility relations as shown in Fig. 14. By definition, m_2' consists of memory blocks newly allocated with respect to m_2 and blocks that already exist in m_2. The latter can be further divided into public and private memory regions with respect to injections j_{12} and j_{23}. Then, m_2' is constructed following the ideas that *1)* the public and newly allocated memory should be projected from the updated source memory m_1' by j_{12}', and *2)* the private memory is protected by `injp` and should be copied over from m_2 to m_2'.

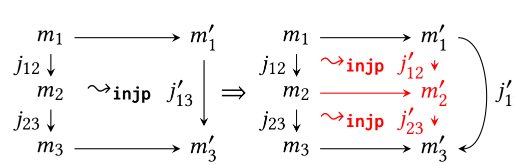
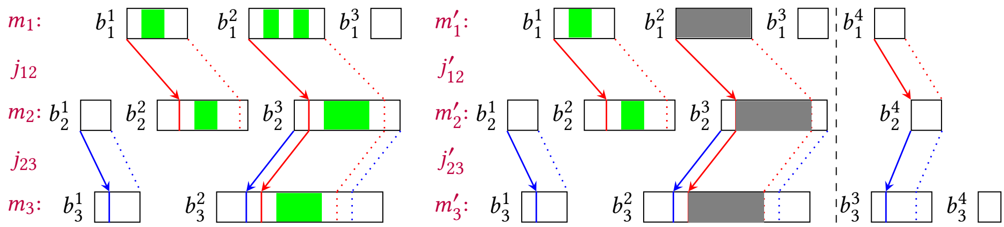


Fig. 14. Construction of Interpolating States

We use the concrete example in Fig. 15 to motivate the construction of m_2'. Here, the white and green areas correspond to locations in `perm(_, NA)` (i.e., having at least some permission) and in `perm(_, Readable)` (i.e., having at least readable permission). Given $m_1 \hookrightarrow_m^{j_{12}} m_2$, $m_2 \hookrightarrow_m^{j_{23}} m_3$ and $(j_{23} \cdot j_{12}, m_1, m_3) \leadsto_{\texttt{injp}} (j_{13}', m_1', m_3')$, we need to define j_{12}' and j_{23}' and then build m_2' satisfying $m_1' \hookrightarrow_m^{j_{12}'} m_2'$, $m_2' \hookrightarrow_m^{j_{23}'} m_3'$, $(j_{12}, m_1, m_2) \leadsto_{\texttt{injp}} (j_{12}', m_1', m_2')$, $(j_{23}, m_2, m_3) \leadsto_{\texttt{injp}} (j_{23}', m_2', m_3')$. m_1'



(a) At the External Call

(b) After the External Call

Fig. 15. Constructing of an Interpolating Memory State

and m'_3 are expansions of m_1 and m_3 with new blocks and possible modification to the public regions of m_1 and m_3. Here, m'_1 has a new block b_1^4 and m'_3 has two new block b_3^3 and b_3^4.

We first fix j'_{12}, j'_{23} and the shape of blocks in m'_2. We begin with m_2 and introduce a newly allocated block b_2^4 whose shape matches b_1^4 in m'_1. Then, j'_{12} is obtained by expanding j_{12} with identity mapping from b_1^4 to b_2^4. Furthermore, j'_{23} is also expanded with a mapping from b_2^4 to a block in m'_3; this mapping is determined by j'_{13}.

We then set the values and permissions for memory cells in m'_2 so that it satisfies injection and the `unchanged-on` properties for readable memory regions implied by $(j_{12}, m_1, m_2) \leadsto_{\texttt{injp}} (j'_{12}, m'_1, m'_2)$ and $(j_{23}, m_2, m_3) \leadsto_{\texttt{injp}} (j'_{23}, m'_2, m'_3)$. The values and permissions for newly allocated blocks are obviously mapped from m'_1 by j'_{12}. Those for old blocks are fixed as follows. By memory protection provided in $(j_{23} \cdot j_{12}, m_1, m_3) \leadsto_{\texttt{injp}} (j'_{13}, m'_1, m'_3)$, the only memory cells in m_1 that may have been modified in m'_1 are those mapped all the way to m_3 by $j_{23} \cdot j_{12}$, while the cells in m_3 that may be modified in m'_3 must be in the image of $j_{23} \cdot j_{12}$. To match this fact, the only old memory regions in m'_2 whose values and permissions may be modified are those both in the image of j_{12} and the domain of j_{23}. Those are the public memory with respect to j_{12} and j_{23} and displayed as the gray areas in Fig. 15b. Following idea *1)* above, the *permissions* in those regions are projected from m'_1 by applying the injection function j_{12}. Note that *values* in those regions are projected only if they are *not read-only* in m_2. Following idea *2)* above, the remaining old memory regions are private with respect to j_{12} and j_{23} and should have the same values and permissions as in m_2.

Note that the accessibility relations $(j_{12}, m_1, m_2) \leadsto_{\texttt{injp}} (j'_{12}, m'_1, m'_2)$ and $(j_{23}, m_2, m_3) \leadsto_{\texttt{injp}} (j'_{23}, m'_2, m'_3)$ can be derived from $(j_{23} \cdot j_{12}, m_1, m_3) \leadsto_{\texttt{injp}} (j'_{13}, m'_1, m'_3)$ because the latter enforces *stronger* protection than the former. This is due to unmapped and out-of-reach regions getting *bigger* as memory injections get composed. For example, in Fig. 15, b_1^1 is mapped by j_{12} but becomes unmapped by $j_{23} \cdot j_{12}$; the image of b_2^1 in b_3^1 is in-reach by j_{23} but becomes out-of-reach by $j_{23} \cdot j_{12}$.

4.2.2 $\texttt{injp} \cdot \texttt{injp} \sqsubseteq \texttt{injp}$. By definition, we need to prove:

Lemma 4.4. $\texttt{injp} \cdot \texttt{injp} \sqsubseteq \texttt{injp}$ *holds. That is,*

$$\begin{array}{l}\forall j_{13}\ m_1\ m_3,\ m_1 \hookrightarrow_m^{j_{13}} m_3 \Rightarrow \exists j_{12}\ j_{23}\ m_2,\ m_1 \hookrightarrow_m^{j_{12}} m_2 \wedge m_2 \hookrightarrow_m^{j_{23}} m_3 \wedge \\ \quad \forall m'_1\ m'_2\ m'_3\ j'_{12}\ j'_{23},\ (j_{12}, m_1, m_2) \leadsto_{\texttt{injp}} (j'_{12}, m'_1, m'_2) \Rightarrow (j_{23}, m_2, m_3) \leadsto_{\texttt{injp}} (j'_{23}, m'_2, m'_3) \Rightarrow \\ \qquad m'_1 \hookrightarrow_m^{j'_{12}} m'_2 \Rightarrow m'_2 \hookrightarrow_m^{j'_{23}} m'_3 \Rightarrow \exists j'_{13},\ (j_{13}, m_1, m_3) \leadsto_{\texttt{injp}} (j'_{13}, m'_1, m'_3) \wedge m'_1 \hookrightarrow_m^{j'_{13}} m'_3.\end{array}$$

This lemma conforms to Fig. 11b. To prove it, we pick j_{12} to be an partial identity injection $(j_{12}(b) = \lfloor b, 0 \rfloor$ when $j_{13}(b) \neq \emptyset)$, $j_{23} = j_{13}$ and $m_2 = m_1$. Then the lemma is reduced to proving the existence of j'_{13} that satisfies $(j_{13}, m_1, m_3) \leadsto_{\texttt{injp}} (j'_{13}, m'_1, m'_3)$ and $m'_1 \hookrightarrow_m^{j'_{13}} m'_3$. By picking $j'_{13} = j'_{12} \cdot j'_{23}$, we can easily prove these properties by exploiting $\texttt{injp}$.

Table 1. Significant Passes of CompCert

Languages/Passes	Outgoing $\twoheadrightarrow$ Incoming	Language/Pass	Outgoing $\twoheadrightarrow$ Incoming
Clight	$C \twoheadrightarrow C$	Constprop	$\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
Self-Sim	$\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$	CSE	$\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
SimplLocals	$\mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{c}_{\mathtt{inj}}$	Deadcode	$\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
Csharpminor	$C \twoheadrightarrow C$	Unusedglob	$\mathtt{c}_{\mathtt{inj}} \twoheadrightarrow \mathtt{c}_{\mathtt{inj}}$
Cminorgen	$\mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{c}_{\mathtt{inj}}$	Allocation	$\mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \twoheadrightarrow \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL}$
Cminor	$C \twoheadrightarrow C$	**LTL**	$\mathcal{L} \twoheadrightarrow \mathcal{L}$
Selection	$\mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \twoheadrightarrow \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}}$	Tunneling	$\mathtt{ltl}_{\mathtt{ext}} \twoheadrightarrow \mathtt{ltl}_{\mathtt{ext}}$
CminorSel	$C \twoheadrightarrow C$	**Linear**	$\mathcal{L} \twoheadrightarrow \mathcal{L}$
RTLgen	$\mathtt{c}_{\mathtt{ext}} \twoheadrightarrow \mathtt{c}_{\mathtt{ext}}$	Stacking	$\mathtt{ltl}_{\mathtt{injp}} \cdot \mathtt{LM} \twoheadrightarrow \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{inj}}$
RTL	$C \twoheadrightarrow C$	**Mach**	$\mathcal{M} \twoheadrightarrow \mathcal{M}$
Self-Sim	$\mathtt{c}_{\mathtt{inj}} \twoheadrightarrow \mathtt{c}_{\mathtt{inj}}$	Asmgen	$\mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \twoheadrightarrow \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA}$
Tailcall	$\mathtt{c}_{\mathtt{ext}} \twoheadrightarrow \mathtt{c}_{\mathtt{ext}}$	**Asm**	$\mathcal{A} \twoheadrightarrow \mathcal{A}$
Inlining	$\mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{c}_{\mathtt{inj}}$	Self-Sim	$\mathtt{asm}_{\mathtt{inj}} \twoheadrightarrow \mathtt{asm}_{\mathtt{inj}}$
Self-Sim	$\mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{c}_{\mathtt{injp}}$	Self-Sim	$\mathtt{asm}_{\mathtt{injp}} \twoheadrightarrow \mathtt{asm}_{\mathtt{injp}}$

5 DERIVATION OF THE DIRECT REFINEMENT FOR COMPCERT

In this section, we discuss the proofs and composition of open simulations for the compiler passes of CompCert into the direct refinement $\leqslant_{\mathrm{ac}}$ following the ideas discussed in §2.2. CompCert compiles `Clight` programs into `Asm` programs through 19 passes [Leroy 2023], including several optimization passes working on the `RTL` intermediate language. First, we prove the open simulations for all these passes with appropriate simulation conventions. In particular, we directly reuse the proofs of non-optimizing passes in CompCertO and update the proofs of optimizing passes with semantic invariants. Second, we prove a collection of properties for refining simulation conventions in preparation for vertical composition. Those properties enable absorption of KMRs into `injp` and composition of semantic invariants. They rely critically on transitivity of `injp`. Finally, we vertically compose the simulations and refine the incoming and outgoing simulation conventions into a single simulation convention $\mathbb{C}$, thereby establishing $\leqslant_{\mathbb{C}}$ as the top-level refinement $\leqslant_{\mathrm{ac}}$.

5.1 Open Simulation of Individual Passes

We list the compiler passes and their simulation types in Table 1 (passes on the right follow the passes on the left) together with their source and target languages and interfaces (in bold fonts). The passes in black are reused from CompCertO, while those in red are reproved optimizing passes. The passes in blue are *self-simulating* passes we inserted; they will be used in §5.3 for composing simulation conventions. Note that we have omitted passes with the identity simulation convention (i.e., with simulations $L_1 \leqslant_{\mathtt{id}} L_2$) in Table 1 as they do not affect the proofs. [4]

5.1.1 Simulation Conventions and Semantic Invariants. We first introduce relevant simulation conventions and semantic invariants shown in Table 1. The simulation conventions $\mathtt{c}_K : C \Leftrightarrow C$, $\mathtt{ltl}_K : \mathcal{L} \Leftrightarrow \mathcal{L}$, $\mathtt{mach}_K : \mathcal{M} \Leftrightarrow \mathcal{M}$, and $\mathtt{asm}_K : \mathcal{A} \Leftrightarrow \mathcal{A}$ relate the same language interfaces with queries and replies native to the associated intermediate languages. They are parameterized by a KMR K to allow different compiler passes to have different assumptions on memory evolution. Conceptually, this parameterization is unnecessary as we can simply use `injp` for every pass due to its uniformity (as discussed in §4.1). Nevertheless, it is useful because the compiler proofs become simpler and more natural with the least restrictive KMRs which may be weaker than `injp`.

[4]The omitted passes are `Cshmgen`, `Renumber`, `Linearize`, `CleanupLabels` and `Debugvar`

CompCertO defines several KMRs weaker than `injp`: `id` is used when memory is unchanged; `ext` is used when the source and target memory share the same structure; `inj` is a simplified version of `injp` without its memory protection. The simulation conventions $\texttt{CL} : \mathcal{C} \Leftrightarrow \mathcal{L}$, $\texttt{LM} : \mathcal{L} \Leftrightarrow \mathcal{M}$ and $\texttt{MA} : \mathcal{M} \Leftrightarrow \mathcal{A}$ capture the calling convention of CompCert: `CL` relates C-level queries and replies with those in the `LTL` language where the arguments are distributed to abstract stack slots; `LM` further relates abstract stack slots with states on an architecture independent machine; `MA` relates this state to registers and memory in the assembly language (X86 assembly in our case). As discussed before, some refinements rely on invariants on the source semantics. The semantic invariant `wt` enforces that arguments and return values of function calls respect function signatures. `ro` is critical for ensuring the correctness of optimizations, which will be discussed next.

5.1.2 Open Simulation of Optimizations. The optimizing passes `Constprop`, `CSE` and `Deadcode` perform constant propagation, common subexpression elimination and dead code elimination, respectively. They make use of a static value analysis algorithm for collecting information of variables during the execution. For each function, this algorithm starts with the known initial values of read-only (constant) global variables. It simulates the function execution to analyze the values of global or local variables after executing each instruction. In particular, for global *constant* variables, their references at any point should have the initial values of constants. For local variables stored on the stack, their references may have initial values or may not if interfered by other function calls. When the analysis encounters a call to another function, it checks whether the address of current stack frame is leaked to the callee directly through arguments or indirectly through pointers in memory. If not, then the stack frame is considered *unreachable* from its callee. Consequently, the references to unreachable local variables after function calls remain to be their initial values. Based on this analysis, the three passes then identify and perform optimizations.

```
1 const int key = 42;
2 void foo(int*);
3 int double_key() {
4   int a = key;
5   foo(&key);
6   return a + key;
7 }
```

(a) Source Program

```
1 const int key = 42;
2 void foo(int*);
3 int double_key() {
4   int a = 42;
5   foo(&key);
6   return 84;
7 }
```

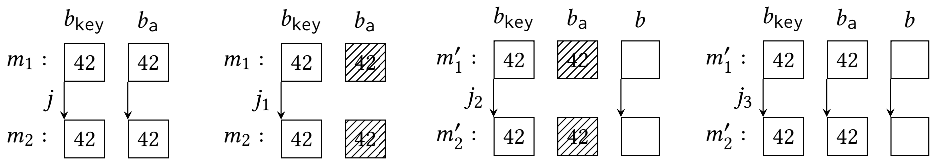
(b) Target Program

Fig. 16. An Example of Constant Propagation

Most of the proofs of closed simulations for those passes can be adapted to open simulation straightforwardly. The only and main difficulty is to prove that information derived from static analysis is consistent with the dynamic memory states in incoming queries and after external calls return. We introduce the semantic invariant `ro` and combine it with `injp` to ensure this consistency. The above optimization passes all use $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$ as their simulation conventions (because `RTL` conforms to the C interface). The adaptation of optimization proofs for those passes is similar. As an example, we only discuss constant propagation whose correctness theorem is stated as follows:

Lemma 5.1. $\forall (M\ M' : \mathit{RTL}), \texttt{Constprop}(M) = M' \Rightarrow [\![M]\!] \leqslant_{\texttt{ro}\cdot\texttt{c}_{\texttt{injp}}} [\![M']\!]$.

Instead of presenting its proof, we illustrate how `ro` and `injp` help establish the open simulation for `Constprop` through a concrete example as depicted in Fig. 16. This example covers optimization for both global constants (e.g., `key`) and local variables (e.g., `a`). By static analysis of Fig. 16a, *1)* `key` contains 42 at line 4 because `key` is a constant global variable and, *2)* both `key` and `a` contain 42 after the external call to `foo` returns to line 6. Here, the analysis confirms `key` has the value 42 because `foo` (if well-behaved) will not modify a constant global variable. Furthermore, `a` has the value 42 because it resides on the stack frame of `double_key` which is unreachable from `foo`. As a result, the source program is optimized to that in Fig. 16b.



(a) Before foo (b) Start of foo (c) End of foo (d) After foo

Fig. 17. Memory Injections from Call to Return of foo

We first show that ro guarantees the dynamic values of global constants are consistent with static analysis. That is, global variables are correct in incoming memory and are protected during external calls. ro is defined as follows:

Definition 5.2. $\texttt{ro} : C \Leftrightarrow C = \langle W_{\texttt{ro}}, \mathbb{R}^q_{\texttt{ro}}, \mathbb{R}^r_{\texttt{ro}} \rangle$ where $W_{\texttt{ro}} = (\texttt{symtbl} \times \texttt{mem})$ and
$\mathbb{R}^q_{\texttt{ro}}(se, m) = \{(v_f[sg](\vec{v})@m, v_f[sg](\vec{v})@m) \mid \texttt{ro-valid}(se, m)\}$
$\mathbb{R}^r_{\texttt{ro}}(se, m) = \{(res@m', res@m') \mid \texttt{mem-acc}(m, m')\}$

Note that although ro takes the form of a simulation convention, it only relates the same queries and replies, i.e., enforcing invariants only on the source side. This kind of simulation conventions are what we called *semantic invariants*. A symbol table *se* (of type symtbl) is provided together with memory, so that the semantics can locate memory blocks of global definitions and find the initial values of global variables. $\texttt{ro-valid}(se, m)$ states that the values of global constant variables in the incoming memory m are the same as their initial values. Therefore, the optimization of key into 42 at line 4 of Fig. 16a is correct. For the external call to foo, monotonicity $\texttt{mem-acc}(m, m')$ ensures that read-only values in memory are unchanged, therefore the above property is preserved from external queries to replies (i.e., $\texttt{ro-valid}(se, m) \Rightarrow \texttt{mem-acc}(m, m') \Rightarrow \texttt{ro-valid}(se, m')$). As a result, replacing key with 42 at line 6 makes sense.

We then show that injp guarantees the dynamic values of unreachable local variables are consistent with static analysis. That is, unreachable stack values are unchanged by external calls. This protection is realized by injp with *shrinking* memory injections. Fig. 17 shows the protection of a when calling foo. Before the external call to foo, the source block b_{a} and b_{key} are *mapped* to target blocks by the current injection j. If the analysis determines that the value of a is unchanged during foo, it indicates that the arguments and m do not contain any pointer to b_{a}. Therefore, we can simply remove b_{a} from j to get a shrunk yet valid memory injection j_1. Then, b_{a} is protected during the call to foo. b_{a} is added back to the injection after foo returns and the simulation continues.

Finally, Unusedglob which removes unused static global variables is verified by assuming that global symbols remain the same throughout the compilation and with a weaker KMR inj.

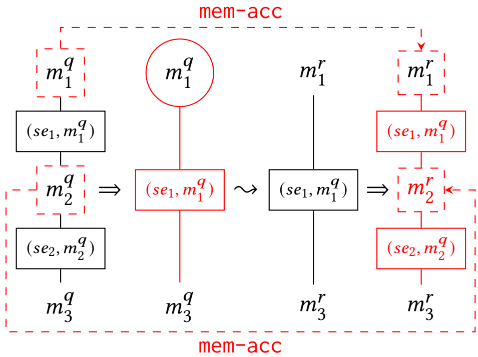
5.2 Properties for Refining Simulation Conventions

We present properties necessary for composing the simulation conventions in Table 1.

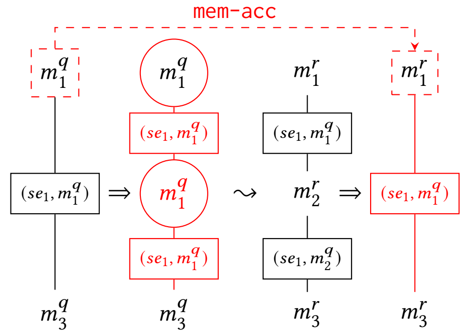
5.2.1 *Commutativity of KMRs and Structural Conventions.*

Lemma 5.3. *For* $\mathsf{Z} \in \{\mathsf{CL}, \mathsf{LM}, \mathsf{MA}\}$ *and* $K \in \{\texttt{ext}, \texttt{inj}, \texttt{injp}\}$ *we have* $\mathsf{X}_K \cdot \mathsf{Z} \sqsubseteq \mathsf{Z} \cdot \mathsf{Y}_K$.

This lemma is provided by CompCertO [Koenig and Shao 2021]. X and Y denote the simulation conventions for the source and target languages of Z, respectively (e.g., X = c and Y = ltl when Z = CL). If $K = \texttt{injp}$ we get $\texttt{c}_{\texttt{injp}} \cdot \mathsf{CL} \sqsubseteq \mathsf{CL} \cdot \texttt{ltl}_{\texttt{injp}}$. This lemma indicates at the outgoing (incoming) side a convention lower (higher) than CL, LM, MA may be lifted over them to a higher position (pushed down to a lower position).



(a) $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \sqsubseteq \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$



(b) $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \sqsubseteq \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$

Fig. 18. Transitivity of $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$

5.2.2 Absorption of KMRs into `injp`. The lemma below is needed for absorbing KMRs into `injp`:

Lemma 5.4. *For any* $\mathbb{R}$, $(1)\mathbb{R}_{\texttt{injp}} \cdot \mathbb{R}_{\texttt{injp}} \equiv \mathbb{R}_{\texttt{injp}}$ $(2)\mathbb{R}_{\texttt{injp}} \sqsubseteq \mathbb{R}_{\texttt{inj}}$ $(3)\mathbb{R}_{\texttt{injp}} \cdot \mathbb{R}_{\texttt{inj}} \cdot \mathbb{R}_{\texttt{injp}} \sqsubseteq \mathbb{R}_{\texttt{injp}}$ $(4)\mathbb{R}_{\texttt{inj}} \cdot \mathbb{R}_{\texttt{inj}} \sqsubseteq \mathbb{R}_{\texttt{inj}}$ $(5)\mathbb{R}_{\texttt{ext}} \cdot \mathbb{R}_{\texttt{inj}} \equiv \mathbb{R}_{\texttt{inj}}$ $(6)\mathbb{R}_{\texttt{inj}} \cdot \mathbb{R}_{\texttt{ext}} \equiv \mathbb{R}_{\texttt{inj}}$ $(7)\mathbb{R}_{\texttt{ext}} \cdot \mathbb{R}_{\texttt{ext}} \equiv \mathbb{R}_{\texttt{ext}}$.

The simulation convention $\mathbb{R}$ is parameterized over a KMR. Property (1) is a direct consequence of $\texttt{injp} \cdot \texttt{injp} \equiv \texttt{injp}$, which is critical for merging simulations using `injp`. The remaining ones either depend on transitivity of `injp`, or trivially hold as shown by Koenig and Shao [2021].

5.2.3 Composition of Semantic Invariants. Lastly, we also need to handle the two semantic invariants `ro` and `wt`. They cannot be absorbed into `injp` because their assumptions are fundamentally different. Therefore, our goal is to permute them to the top-level and merge any duplicated copies. The following lemmas enable elimination and permutation of `wt`:

Lemma 5.5. *For any* $\mathbb{R}_K : C \Leftrightarrow C$, *we have* $(1)\mathbb{R}_K \cdot \texttt{wt} \equiv \texttt{wt} \cdot \mathbb{R}_K \cdot \texttt{wt}$ *and* $(2)\mathbb{R}_K \cdot \texttt{wt} \equiv \texttt{wt} \cdot \mathbb{R}_K$.

`ro` is more difficult to handle as it does not commute with arbitrary simulation conventions. To eliminate redundant `ro`, we piggyback `ro` onto `injp` and prove the following transitivity property:

Lemma 5.6. $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \equiv \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$

Its proof follows the same steps for proving $\texttt{c}_{\texttt{injp}} \equiv \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}}$ with additional reasoning for establishing properties of `ro`. A graphic presentation of the proof is given in Fig. 18 which mirrors Fig. 11. We focus on explaining the additional reasoning and have omitted the $\rightsquigarrow_{\texttt{injp}}$ relations and the worlds for `injp` in Fig. 18. Note that by definition the worlds (se, m) for `ro` do not evolve like those for `injp`. A red circle around a memory state m indicates it is required to prove `ro-valid` in $\mathbb{R}^q_{\texttt{ro}}$ holds for m. The `mem-acc` relations over dashed arrows are the properties over replies in $\mathbb{R}^r_{\texttt{ro}}$ and must also be verified.

The above additional properties are proved based on two observations. First, the properties for queries (i.e., `ro-valid`) are propagated in refinement along with copying of memory states. For example, to prove the refinement in Fig. 18a, we are given that $\texttt{ro-valid}(se_1, m_1^q)$ and $\texttt{ro-valid}(se_2, m_2^q)$ according to initial $\mathbb{R}^q_{\texttt{ro}}$ relations. By choosing (se_1, m_1^q) to be the world for the composed $\mathbb{R}^q_{\texttt{ro}}$, $\texttt{ro-valid}(se_1, m_1^q)$ holds trivially for m_1^q in the circle. To prove the refinement in Fig. 18b, we need to prove that the interpolating memory state after the initial decomposition satisfies $\mathbb{R}^q_{\texttt{ro}}$. By choosing m_1^q to be this state (in the middle circle in Fig. 18b and according to the proof of Lemma 4.4),

$\texttt{ro-valid}(se_1, m_1^q)$ follows directly from the initial assumption. Second, the properties for replies (i.e., mem-acc) have already been encoded into $\leadsto_{\texttt{injp}}$ by Definition 3.3. For example, m_2^r in Fig. 18a is constructed by following exactly Lemma 4.3. Therefore, $\texttt{mem-acc}(m_2^q, m_2^r)$ trivially holds.

Finally, at the top level, we need ro and wt to commute which is straightforward to prove:

Lemma 5.7. $\texttt{ro} \cdot \texttt{wt} \equiv \texttt{wt} \cdot \texttt{ro}$

5.3 Proving the Direct Open Simulation for CompCert

We first insert self-simulations into the compiler passes, as shown in Table 1. This is to supply extra $\mathbb{R}_{\texttt{inj}}$, $\mathbb{R}_{\texttt{injp}}$, and ro for absorbing $\mathbb{R}_{\texttt{ext}}$ ($\mathbb{R}_{\texttt{inj}}$) into $\mathbb{R}_{\texttt{inj}}$ ($\mathbb{R}_{\texttt{injp}}$) by properties in Lemma 5.4 and for transitive composition of ro. Self-simulations are obtained by the following lemma:

Theorem 5.8. *If p is a program written in* Clight *or* RTL *and* $\mathbb{R} \in \{\texttt{c}_{\texttt{ext}}, \texttt{c}_{\texttt{inj}}, \texttt{c}_{\texttt{injp}}\}$, *or p is written in* Asm *and* $\mathbb{R} \in \{\texttt{asm}_{\texttt{ext}}, \texttt{asm}_{\texttt{inj}}, \texttt{asm}_{\texttt{injp}}\}$, *then* $[[p]] \leqslant_{\mathbb{R} \twoheadrightarrow \mathbb{R}} [[p]]$ *holds.*

We unify the conventions at the incoming and outgoing sides. We start with the simulation $L_1 \leqslant_{\mathbb{R} \twoheadrightarrow \mathbb{S}} L_2$ which is the transitive composition of compiler passes in Table 1 where

$$\mathbb{R} = \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{ltl}_{\texttt{injp}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$$

$$\mathbb{S} = \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{inj}} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}.$$

We then find two sequences of refinements $\mathbb{C} \sqsubseteq \mathbb{R}_n \sqsubseteq \ldots \sqsubseteq \mathbb{R}_1 \sqsubseteq \mathbb{R}$ and $\mathbb{S} \sqsubseteq \mathbb{S}_1 \sqsubseteq \ldots \sqsubseteq \mathbb{S}_m \sqsubseteq \mathbb{C}$, by which and Theorem 3.5 we get the simulation $L_1 \leqslant_{\mathbb{C} \twoheadrightarrow \mathbb{C}} L_2$. The direct simulation convention is $\mathbb{C} = \texttt{ro} \cdot \texttt{wt} \cdot \texttt{CAinjp} \cdot \texttt{asm}_{\texttt{injp}}$. ro enables optimizations at C level while wt ensures well-typedness. The definition of CAinjp has already been discussed informally in §2.1; its formal definition is given as follows. Note that, to simplify the presentation, we have omitted minor constraints such as function values should not be undefined, stack pointers must have a pointer type, etc. Interested readers should consult the our artifact for a complete definition.

Definition 5.9. $\texttt{CAinjp} : C \Leftrightarrow \mathcal{A} = \langle W_{\texttt{CAinjp}}, \mathbb{R}^q_{\texttt{CAinjp}}, \mathbb{R}^r_{\texttt{CAinjp}} \rangle$ where $W_{\texttt{CAinjp}} = (W_{\texttt{injp}} \times \texttt{sig} \times \texttt{regset})$ and $\mathbb{R}^q_{\texttt{CAinjp}} : \mathcal{K}_{W_{\texttt{CAinjp}}}(C^q, \mathcal{A}^q)$ and $\mathbb{R}^r_{\texttt{CAinjp}} : \mathcal{K}_{W_{\texttt{CAinjp}}}(C^r, \mathcal{A}^r)$ are defined as:

- $(v_f[sg](\vec{v})@m_1, rs@m_2) \in \mathbb{R}^q_{\texttt{CAinjp}}((j, m_1, m_2), sg, rs)$ if

  (1) $m_1 \hookrightarrow^j_m m_2, \quad v_f \hookrightarrow^j_v rs(\mathsf{PC}) \quad \vec{v} \hookrightarrow^j_v \texttt{get-args}(sg, rs(\mathsf{RSP}), rs, m_2)$

  (2) $\texttt{outgoing-arguments}(sg, rs(\mathsf{RSP})) \subseteq \texttt{out-of-reach}(j, m_1)$

  (3) $\texttt{outgoing-arguments}(sg, rs(\mathsf{RSP})) \subseteq \texttt{perm}(m_2, \texttt{Freeable})$

  $\texttt{get-args}(sg, rs(\mathsf{RSP}), rs, m_2)$ is a list of values for arguments at the assembly level obtained by inspecting locations for arguments in rs and m_2 corresponding to the signature sg which are determined by CompCert's calling convention. $\texttt{outgoing-arguments}(sg, rs(\mathsf{RSP}))$ is a set of addresses on the stack frame for outgoing function arguments computed from the given signature sg and the value of stack pointer.
- $(r@m_1', rs'@m_2') \in \mathbb{R}^r_{\texttt{CAinjp}}((j, m_1, m_2), sg, rs)$ if there is a j' s.t.

  (1) $(j, m_1, m_2) \leadsto_{\texttt{injp}} (j', m_1', m_2')$

  (2) $m_1' \hookrightarrow^{j'}_m m_2', \quad r \hookrightarrow^{j'}_v \texttt{get-result}(sg, rs')$

  (3) $\texttt{outgoing-arguments}(sg, rs(\mathsf{RSP})) \subseteq \texttt{out-of-reach}(j, m_1)$

  (4) $rs'(\mathsf{RSP}) = rs(\mathsf{RSP}), \quad rs'(\mathsf{PC}) = rs(\mathsf{RA}), \quad \forall r \in \texttt{callee-save-regs}, rs'(r) = rs(r)$

  $\texttt{get-result}(sg, rs')$ is the return value stored in a register designated by CompCert's calling convention for the given signature sg. callee-save-regs is the set of callee-save registers.

The tailing $\texttt{asm}_{\texttt{injp}}$ is irrelevant as assembly code is self-simulating by Theorem 5.8. The final correctness theorem is shown below:

THEOREM 5.10. *Compilation in CompCert is correct in terms of open simulations,*

$$\forall\ (M : \texttt{Clight})\ (M' : \texttt{Asm}),\ \texttt{CompCert}(M) = M' \Rightarrow [\![M]\!] \leqslant_{\mathbb{C}} [\![M']\!].$$

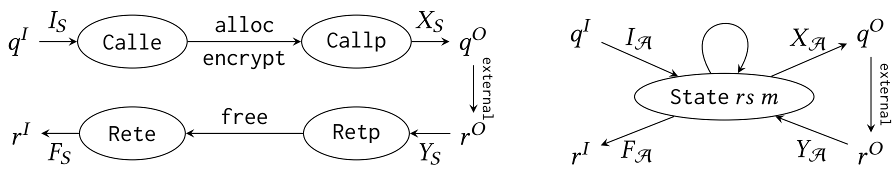
We explain how the refinements are carried out at both sides. The following is the sequence of refined simulation conventions $\mathbb{C} \sqsubseteq \mathbb{R}_n \sqsubseteq \ldots \sqsubseteq \mathbb{R}_1 \sqsubseteq \mathbb{R}$ at the outgoing side. It begins with $\mathbb{R}$ and ends with $\mathbb{C}$.

(1) $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{ltl}_{\texttt{injp}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(2) $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{ltl}_{\texttt{injp}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(3) $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{ltl}_{\texttt{injp}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(4) $\texttt{wt} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{ltl}_{\texttt{injp}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(5) $\texttt{wt} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{injp}}$
(6) $\texttt{wt} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{injp}}$
(7) $\texttt{wt} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{injp}}$
(8) $\texttt{wt} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{injp}}$
(9) $\texttt{ro} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{injp}}$
(10) $\texttt{ro} \cdot \texttt{wt} \cdot \texttt{CAinjp} \cdot \texttt{asm}_{\texttt{injp}}$

In each line, the letters in red are simulation conventions transformed by the refinement operation at that step. In step (1), we merge consecutive simulation conventions by applying property (1) in Lemma 5.4 for $\texttt{c}_{\texttt{injp}}$ and properties (5-7) to compose $\texttt{c}_{\texttt{ext}}$ and absorb it into $\texttt{c}_{\texttt{inj}}$. We also apply Lemma 5.6 to merge consecutive $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$. In step (2), we move $\texttt{wt}$ to higher positions by property (2) in Lemma 5.5. In step (3), we eliminate the first $\texttt{wt}$ by property (1) in Lemma 5.5 and move the remaining $\texttt{wt}$ higher by property (2) in Lemma 5.5 and Lemma 5.7. In step (4), we lift conventions over $\texttt{CL}$, $\texttt{LM}$ and $\texttt{MA}$ to higher positions by Lemma 5.3. In step (5), we absorb $\texttt{c}_{\texttt{ext}}$ into $\texttt{c}_{\texttt{inj}}$ again and further turns $\texttt{c}_{\texttt{inj}}$ into $\texttt{c}_{\texttt{injp}}$ by applying $\texttt{c}_{\texttt{injp}} \sqsubseteq \texttt{c}_{\texttt{inj}}$ (property (2) in Lemma 5.4). In step (6), we compose $\texttt{c}_{\texttt{injp}}$ by applying $\texttt{c}_{\texttt{injp}} \equiv \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}}$. In step (7), we apply Lemma 5.6 again to eliminate the second $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$. In step (8), we commute the two semantic invariants of the source semantics by Lemma 5.7. Finally, we merge $\texttt{c}_{\texttt{injp}}$ with $\texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA}$ into $\texttt{CAinjp}$.

The original simulation conventions at the incoming side are parameterized by $\texttt{inj}$ which does not have memory protection as in $\texttt{injp}$. One can modify the proofs of CompCert to make $\texttt{injp}$ an incoming convention. However, we show that this is unnecessary: with the inserted self-simulations over $\texttt{injp}$, conventions over $\texttt{inj}$ may be absorbed into them. The following is the refinement sequence $\mathbb{S} \sqsubseteq \mathbb{S}_1 \sqsubseteq \ldots \sqsubseteq \mathbb{S}_m \sqsubseteq \mathbb{C}$ that realizes this idea.

(1) $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{inj}} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(2) $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{inj}} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(3) $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{inj}} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(4) $\texttt{wt} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{inj}} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(5) $\texttt{wt} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{ext}} \cdot \texttt{CL} \cdot \texttt{ltl}_{\texttt{ext}} \cdot \texttt{LM} \cdot \texttt{mach}_{\texttt{inj}} \cdot \texttt{mach}_{\texttt{ext}} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$
(6) $\texttt{wt} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{inj}} \cdot \texttt{c}_{\texttt{injp}} \cdot \texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$
$\cdot \texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{injp}} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{ext}} \cdot \texttt{asm}_{\texttt{ext}} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{ext}} \cdot \texttt{asm}_{\texttt{inj}} \cdot \texttt{asm}_{\texttt{injp}}$



(a) L_S (b) [[server_opt.s]]

Fig. 19. Specification and Open Semantics of server_opt.s

(7) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
$\cdot \mathsf{CL} \cdot \mathsf{LM} \cdot \mathsf{MA} \cdot \mathtt{asm}_{\mathtt{injp}} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}$
(8) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathsf{CL} \cdot \mathsf{LM} \cdot \mathsf{MA} \cdot \mathtt{asm}_{\mathtt{injp}} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}$
(9) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathsf{CL} \cdot \mathsf{LM} \cdot \mathsf{MA} \cdot \mathtt{asm}_{\mathtt{injp}}$
(10) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathsf{CL} \cdot \mathsf{LM} \cdot \mathsf{MA} \cdot \mathtt{asm}_{\mathtt{injp}}$
(11) $\mathtt{ro} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathsf{CL} \cdot \mathsf{LM} \cdot \mathsf{MA} \cdot \mathtt{asm}_{\mathtt{injp}}$
(12) $\mathtt{ro} \cdot \mathtt{wt} \cdot \mathsf{CAinjp} \cdot \mathtt{asm}_{\mathtt{injp}}$

Steps (1-3) are the same as for the outgoing side except for using property (4) in Lemma 5.4. In step (4), we split $\mathtt{c}_{\mathtt{injp}}$ into two, one will be used to absorb the $\mathtt{asm}_{\mathtt{inj}}$ at the target level. In step (5), we push all simulation conventions parameterized over KMRs starting with the second split $\mathtt{c}_{\mathtt{injp}}$ to target level by Lemma 5.3. In step (6), we absorb $\mathtt{asm}_{\mathtt{ext}}$ into $\mathtt{asm}_{\mathtt{inj}}$ by properties (5-7) in Lemma 5.4. In step (7), we compose the consecutive $\mathtt{c}_{\mathtt{inj}}$ and $\mathtt{asm}_{\mathtt{inj}}$ by $\mathbb{R}_{\mathtt{inj}} \cdot \mathbb{R}_{\mathtt{inj}} \sqsubseteq \mathbb{R}_{\mathtt{inj}}$ (property (4) in Lemma 5.4). In step (8), we absorb inj into injp at both levels by property (3) in Lemma 5.4. In step (9), we eliminate a redundant $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$ by Lemma 5.6. The last two steps are the same as above.

6 END-TO-END VERIFICATION OF HETEROGENEOUS MODULES

In this section, we give a formal account of end-to-end verification of heterogeneous modules based on direct refinements. The discussion focuses on the running example in Fig. 4 and its variants. More detailed development of those examples can be found in Appendix B. We also develop an additional example adapted from CompCertM in Appendix C.

6.1 Refinement for the Hand-written Server

We use server_opt.s instead of server.s to illustrate how optimizations are enabled by ro. The proof for the unoptimized server is similar with only minor adjustments. A formal definition of LTS for L_S is given below and its transition diagram is given in Fig. 19a.

Definition 6.1. LTS of L_S:

$$
\begin{aligned}
S_S &:= \{\mathtt{Calle}\ i\ v_f\ m, \mathtt{Callp}\ sp\ v_f\ m, \mathtt{Retp}\ sp\ m, \mathtt{Rete}\ m\};\\
I_S &:= \{(\mathtt{Vptr}(b_e, 0)[\mathtt{int} \to \mathtt{ptr} \to \mathtt{void}]([i, v_f])@m, \mathtt{Calle}\ i\ v_f\ m)\};\\
\to_S &:= \{(\mathtt{Calle}\ i\ v_f\ m, \mathtt{Callp}\ sp\ v_f\ m') \mid m' = m[sp \leftarrow (i\ \mathtt{XOR}\ m[b_k])]\} \cup\\
&\quad\ \{(\mathtt{Retp}\ sp\ m, \mathtt{Rete}\ m') \mid \mathtt{free}\ m\ sp = m'\};\\
X_S &:= \{(\mathtt{Callp}\ sp\ \mathtt{Vptr}(b_p, 0)\ m, \mathtt{Vptr}(b_p, 0)[\mathtt{ptr} \to \mathtt{void}]([\mathtt{Vptr}(sp, 0)])@m)\};\\
Y_S &:= \{(\mathtt{Callp}\ sp\ v_f\ m, res@m', \mathtt{Retp}\ sp\ m')\};\\
F_S &:= \{(\mathtt{Rete}\ m, \mathtt{Vundef}@m)\}.
\end{aligned}
$$

The LTS has four internal states as depicted in Fig. 19a. Initialization is encoded in I_S. If the incoming query q^I contains a function pointer $\mathtt{Vptr}(b_e, 0)$ which points to encrypt, L_S enters $\mathtt{Calle}\ i\ v_f\ m$

$$\begin{tikzcd}
q^I_C \arrow[r, "I_S"] \arrow[d, leftrightarrow, "\mathbb{C}^q"] & \texttt{Calle}\ i\ v_f\ m \arrow[r, "\texttt{alloc}\ sp", "\texttt{store}\ sp"'] \arrow[d, leftrightarrow, "R"] & \texttt{Callp}\ sp\ v_f\ m_1 \arrow[r, "X_S"] \arrow[d, leftrightarrow, "R"'] & q^O_C \arrow[r, dashed] \arrow[d, leftrightarrow, "\mathbb{C}^q"'] & r^O_C \arrow[r, "Y_S"] & \texttt{Retp}\ sp\ m_2 \arrow[r, "\texttt{free}\ sp"] \arrow[d, leftrightarrow, "R"] & \texttt{Rete}\ m_3 \arrow[r, "F_S"] \arrow[d, leftrightarrow, "R"'] & r^I_C \arrow[d, leftrightarrow, "\mathbb{C}^r"'] \\
q^I_{\mathcal{A}} \arrow[r, "I_{\mathcal{A}}"] & (rs, tm) \arrow[r, "\texttt{Pallocframe}", "\texttt{...\ Pcall}"'] & (rs_1, tm_1) \arrow[r, "X_{\mathcal{A}}"] & q^O_{\mathcal{A}} \arrow[r, dashed] & r^O_{\mathcal{A}} \arrow[u, leftrightarrow, "\mathbb{C}^r"] \arrow[r, "Y_{\mathcal{A}}"] & rs_2, tm_2 \arrow[r, "\texttt{Pfreeframe}", "\texttt{Pret}"'] & rs_3, tm_2 \arrow[r, "F_{\mathcal{A}}"] & r^I_{\mathcal{A}}
\end{tikzcd}$$

Fig. 20. Open Simulation between the Server and its Specification

where i and v_f are its arguments. The first internal transition allocates the stack frame sp and stores the result of encryption i `XOR` $m[b_k]$ in sp where b_k contains `key`. Then, it enters `Callp` which is the state before calling `process`. If the pointer $v_f = \texttt{Vptr}(b_p, 0)$ of the current state points to an external function, L_S issues an outgoing C query q^O with a pointer to its stack frame as its argument. After the external call, Y_S updates the memory with the reply and enters `Retp`. The second internal transition frees sp and enters `Rete` and finally returns. Note that complete semantics of L_S is accompanied by a local symbol table which determines the initial value of global variables (`key`) and whether it is a constant (read-only). The only difference between specifications for `server_opt.s` and `server.s` is whether `key` is read-only in the symbol table. The semantics of assembly module $[[\texttt{server\_opt.s}]]$ is given by CompCertO whose transition diagram is shown in Fig. 19b. All the states, including queries and replies, are composed of register sets and memories.

Theorem 6.2. $L_S \leqslant_{\mathbb{C}} [[\texttt{server\_opt.s}]]$.

Given the open semantics, we need to prove the above forward simulation. The most important points are how `ro` enables optimizations and how `injp` preserves memory across external calls.

At the top level, we expand $\mathbb{C}$ to $\texttt{ro} \cdot \texttt{wt} \cdot \texttt{CAinjp} \cdot \texttt{asm}_{\texttt{injp}}$ and switch the order of `ro` and `wt` by Lemma 5.7. By the vertical compositionality (Theorem 3.4), we first establish $L_S \leqslant_{\texttt{wt}} L_S$ with the well-typed outgoing arguments and return value. $[[\texttt{server\_opt.s}]] \leqslant_{\texttt{asm}_{\texttt{injp}}} [[\texttt{server\_opt.s}]]$ is proved by Theorem 5.8. Then, we are left with $L_S \leqslant_{\texttt{ro}\cdot\texttt{CAinjp}} [[\texttt{server\_opt.s}]]$. By definition, we can easily show $L_S \leqslant_{\texttt{ro}} L_S$ because L_S never changes read-only variables. Therefore, we are able to propagate the protection in `ro-valid` downwards.

We are left with proving $L_S \leqslant_{\texttt{CAinjp}} [[\texttt{server\_opt.s}]]$, i.e., to show the simulation diagram in Fig. 20 holds which is a complete picture of Fig. 6. Here, the assumptions in forward simulation and conclusions we need to prove are represented as black and red arrows, respectively. For the proof, we need an invariant $R \in \mathcal{K}_{W_{\texttt{ro}\cdot\texttt{CAinjp}}}(S_S, \texttt{regset} \times \texttt{mem})$. The most important point is that `ro` and `injp` play essential roles in establishing the invariant. First, `ro-valid` is propagated throughout R to prove that value of `key` read from the memory is 42 from `Calle` to `Callp`, hence matches the constant in `server_opt.s`. Second, `injp` is essential for deriving that memory locations in sp with offset o s.t. $o < 8$ and $16 \leq o$ are unchanged since they are designated out-of-reach by R. Therefore, the private stack values of the server are protected. For the unoptimized server, the only difference is that $L_S \leqslant_{\texttt{CAinjp}} [[\texttt{server.s}]]$ can be proved without the help of `ro`.

6.2 End-to-end Correctness Theorem

Lemma 6.3. $L_{CS} \leqslant_{\texttt{ro}\cdot\texttt{wt}\cdot\texttt{c}_{\texttt{injp}}} [[\texttt{client.c}]] \oplus L_S$.

We first prove the above source-level refinement where L_{CS} is the top-level specification. Its proof follows the same pattern as Theorem 6.2 but considerably simpler because the source and target semantics share the same C interface. We then prove the forward simulation between the top-level specification and the linked assembly as depicted in Fig. 4, which is immediate from the horizontal compositionality and adequacy for assembly described in §3.1.2, Theorem 5.10 and Theorem 6.2:

```
/* client.c */
#define N 10
int input[N] = {...};
int result[N];
int i;
void encrypt(int i,
        void(*p)(int*));
```

```
void request(int *r) {
  if (i == 0) encrypt(input[i++], request);
  else if (0 < i && i < N) {
    result[i-1] = *r;
    encrypt(input[i++], request);
  } else result[i-1] = *r;
}
```

Fig. 21. Client with Multiple Encryption Requests

Lemma 6.4. $[[\texttt{client.c}]] \oplus L_S \leqslant_{\mathbb{C}} [[\texttt{client.s} + \texttt{server\_opt.s}]]$.

For end-to-end open semantics, we need to absorb Lemma 6.3 into Lemma 6.4. The following theorem is easily derived by inserting `injp` and applying Lemma 5.5, 5.6 and 5.7.

Lemma 6.5. $\mathbb{C} \equiv \texttt{ro} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{injp}} \cdot \mathbb{C}$.

The final end-to-end simulation is immediate by vertically composing Lemma 6.3, Lemma 6.4 and refining the simulation convention using Lemma 6.5.

Theorem 6.6. $L_{CS} \leqslant_{\mathbb{C}} [[\texttt{client.s} + \texttt{server\_opt.s}]]$.

6.3 Verification of Mutually Recursive Client and Server

We introduce a variant of the running example with mutual recursion in Fig. 23. The server remains the same while the client is changed. `request` itself is passed as a callback function to `encrypt`, resulting in recursive calls to `encrypt` for encrypting and storing an array of values. To perform the same end-to-end verification for this example, we only need to define a new top-level specification $L_{CS}{}'$ and prove $L_{CS}{}' \leqslant_{\texttt{ro}\cdot\texttt{wt}\cdot\texttt{c}_{\texttt{injp}}} [[\texttt{client.c}]] \oplus L_S$. Other proofs are either unchanged (e.g., the refinement of the server) or can be derived from Theorem 5.10, full compositionality and adequacy. More detailed proofs can be found in Appendix B.

7 GENERALITY AND LIMITATIONS OF OUR APPROACH

In this section, we explain how our approach to VCC may be generalized to other memory models, compilers and optimizations for first-order languages based on the high-level structures of our solutions. We also discuss the existing and possible limitations of our approach.

7.1 Supporting Different Memory Models and Compilers

At a high level, `injp` is simply a general and transitive relation on evolving *functional memory invariants* (represented as injections) enhanced with *memory protection* to guard against modification to private memory by external calls. Many other first-order memory models can be viewed as employing either a richer or a simplified version of injection as memory invariants and equipped with a similar notion of memory protection. For example, the memory model of CompCertS [Besson et al. 2015] extends injections to map *symbolic values*. The *memory refinements* in the *CH_2O* memory model [Krebbers 2016] function like injections except that pointer offsets are represented as abstract *paths* pointing into aggregated data structures. The memory model defined by Kang et al. [2015] explicitly divides a memory state into public and private memory. Its memory invariant is an equivalence relation between public source and target memory which is essentially an identity injection. Therefore, uniform KMRs may be defined for those memory models as variants of `injp`.

To prove the transitivity of these KMRs, the key is the construction of interpolating memory states after external calls as described in §4.2. This construction is based on the following general ideas: *1)* as KMRs are transitively composed, more memory gets protected, *2)* the private memory should be identical to the initial memory, and *3)* the public memory should be projected from the updated source memory via memory invariants. As we can see, these ideas are applicable to any memory model with functional memory invariants and a notion of private memory. Therefore, our approach should work for the aforementioned memory models and compilers based on them.

7.2 Supporting Additional Optimization Passes

Given any new optimization pass whose additional rely-guarantee condition can be represented as a semantics invariant I, we may piggyback I onto an enriched `injp` to achieve direct refinement. To see that, note that any I consists of two parts: a condition for initial queries (e.g., `ro-valid` in `ro`) and a condition for replies (e.g., `mem-acc` in `ro`). By extending `injp` to include the latter (just like that Definition 3.3 includes `mem-acc`), if the enriched `injp` is still transitive, then we can easily prove the following proposition which is generalized from Lemma 5.6.

Proposition 7.1. *For any* $I : C \Leftrightarrow C$ *and enriched* `injp`, $I \cdot \mathtt{c}_{\mathtt{injp}} \equiv I \cdot \mathtt{c}_{\mathtt{injp}} \cdot I \cdot \mathtt{c}_{\mathtt{injp}}$.

The proof follows exactly the steps for proving Lemma 5.6. It is based on the two observations we made near the end of §5.2.3, i.e., *1)* the properties for initial queries of I hold along with copying of memory states and *2)* the properties for replies trivially hold as they are part of the enriched `injp`.

7.3 Limitations

We discuss several limitations of our approach and possible solutions. First, it does not yet support behavior refinements for whole programs (i.e., preservation of event traces in CompCert [Leroy 2023]). This is a technical limitation and can be solved by adding a lemma to reduce open simulations in CompCertO to closed simulations in CompCert. Second, open simulations assume given *any* input injection j, the execution outputs *some* injection j' related to j by `injp`. This may not work for memory models with fixed definition of injection functions (e.g., see [Wang et al. 2022]). A possible solution is to enrich `injp` to account for this fixed definition. Finally, given a new optimization, if its rely-guarantee condition cannot be described as a semantic invariant or if `injp` enriched with its semantic invariant I becomes intransitive, then direct refinements may not be derivable. In this case, we may need to place stronger restrictions on this optimization for our approach to work.

8 EVALUATION AND RELATED WORK

Our Coq development took about 7 person months and 18.3k lines of code (LOC) on top of CompCertO. We have added 3.7k LOC to prove the transitivity of `injp`, 3k LOC to verify the compiler passes as discussed in §5.1, 1.2k LOC for composing simulation conventions as described in the rest of §5 and 7.3k LOC for the Client-Server examples. We have also ported CompCertM's example on mutually recursive summation [Song et al. 2020] into our framework, which adds 3.1k LOC. For now, the cost for examples is relatively high. However, we observe that a lot of proofs on low-level computation such as pointer arithmetic can be automated by proof scripts, many proofs with predictable patterns can be automatically generated by inspecting the structures of programs, and a lot of duplicated lemmas existing in those examples can be eliminated. We plan to carry out those exercises in the future which will simplify the proofs significantly. Below we compare our work with other frameworks for compositional compiler verification and program verification. A detailed comparison of our framework with CompCertM and CompCertO based on the running example can be found in Appendix D.

Table 2. Comparison between Work on VCC Based on CompCert

	CompComp	CompCertM	CompCertO	CompCertX	**This Work**
Direct Refinement	No	No	No	No	**Yes**
Vertical Composition	Yes	RUSC	Trivial	CAL	**Yes**
Horizontal Composition	Yes	RUSC	Yes	CAL	**Yes**
Adequacy	No	Yes	Yes	Yes	**Yes**
End-to-end Verification	No	Yes	Unknown	CAL	**Yes**
Free-form Heterogeneity	Yes	Yes	Yes	No	**Yes**
Behavior Refinement	No	Yes	No	Yes	**No**

8.1 Verified Compositional Compilation for First-Order Languages

In this work, we are concerned with VCC of first-order imperative programs with global memory states and support of pointers. A majority of work in this setting is based on CompCert. We compare them from the perspectives listed in the first column of Table 2. An answer that is not a simple "Yes" or "No" denotes that special constraints are enforced to support the given feature.

Compositional CompCert. CompComp supports VCC based on *interaction semantics* which is a specialized version of open semantics with C interfaces [Stewart et al. 2015]. We have already talked about its merits and limitations in §1.2. It is interesting to note that CompComp can also be obtained based on our approach by adopting $\mathtt{c}_{\mathtt{injp}}$ for every compiler pass and exploiting the transitivity of $\mathtt{c}_{\mathtt{injp}}$, which does not require the instrumentation of semantics in CompComp.

CompCertM. CompCertM supports adequacy and end-to-end verification of mixed C and assembly programs. A distinguishing feature of CompCertM is Refinement Under Self-related Contexts or RUSC [Song et al. 2020]. A RUSC relation is a *fixed* collection of simulation relations. By exploiting contexts that are self-relating under all of these simulation relations, horizontal and vertical compositionality are achieved. However, refinements based on RUSC relations can be difficult to use as they are not extensional. For example, the complete open refinement relation $\leqslant_{R_1+\ldots+R_9}$ in CompCertM carries 9 RUSC relations $R_1, \ldots, R_9$ (6 for compiler passes and 3 for source-level verification). To establish the refinement between `a.s` and its specification L_S, one needs to prove L_S are self-simulating over *all* 9 simulation relations. This can quickly get out of hand as more modules and more compiler passes are introduced. By contrast, we only need to prove direct refinement *for once* and the refinement is open to further horizontal or vertical composition. On the other hand, CompCertM supports behavior refinement of closed programs which we do not yet (See §7.3).

CompCertO. Vertical composition is a trivial pairing of simulations in CompCertO, which exposes internal compilation steps. CompCertO tries to alleviate this problem via ad-hoc refinement of simulation conventions. The resulting top-level convention is $\mathbb{C}_{\mathtt{CCO}} = \mathcal{R}^* \cdot \mathtt{wt} \cdot \mathtt{CL} \cdot \mathtt{LM} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{vainj}}$ where $\mathcal{R} = \mathtt{c}_{\mathtt{injp}} + \mathtt{c}_{\mathtt{inj}} + \mathtt{c}_{\mathtt{ext}} + \mathtt{c}_{\mathtt{vainj}} + \mathtt{c}_{\mathtt{vaext}}$ is a sum of conventions parameterized over KMRs. In particular, $\mathtt{c}_{\mathtt{vaext}}$ is an ad-hoc combination of KMR and internal invariants for optimizations. $\mathcal{R}^*$ means that $\mathcal{R}$ may be repeated for an arbitrary number of times. Since the top-level summation of KMRs is similar to that in CompCertM, we need to go through a reasoning process similar to CompCertM, only more complicated because of the need to reason about internal invariants of optimizations in $\mathtt{c}_{\mathtt{vaext}}$ and indefinitely repeated combination of all the KMRs by $\mathcal{R}^*$. Therefore, it is unknown if the correctness theorem of CompCertO suffices for end-to-end program verification.

CompCertX. CompCertX [Gu et al. 2015; Wang et al. 2019] realizes a weaker form of VCC that only allows assembly contexts to invoke C programs, but not the other way around. Therefore, it does not support horizontal composition of modules with mutual recursions. The compositionality and program verification are delegated to Certified Abstraction Layers (CAL) [Gu et al. 2015, 2018]. Furthermore, CompCertX does not support stack-allocated data (e.g., our server example). However, its top-level semantic interface is similar to our interface, albeit not carrying a symmetric rely-guarantee condition. This indicates that our work is a natural evolution of CompCertX.

VCC for Concurrent Programs. VCC for concurrent programs needs to deal with multiple threads and their linking. CASCompCert is an extension of CompComp that supports compositional compilation of concurrency with no (or benign) data races [Jiang et al. 2019]. To make CompComp's approach to VCC work in a concurrent setting, CASCompCert imposes some restrictions including not supporting stack-allocated data and allowing only nondeterminism in scheduling threads. A recent advancement based on CASCompCert is about verifying concurrent programs [Zha et al. 2022] running on weak memory models using the promising semantics [Kang et al. 2017; Lee et al. 2020]. We believe the ideas in CASCompCert are complementary to this work and can be combined with our approach to achieve VCC for concurrency with cleaner interface and less restrictions.

8.2 Verified Compositional Compilation for Higher-Order Languages

Another class of work on VCC focuses on compilation of higher-order languages. In this setting, the main difficulty comes from complex language features together with higher-order states. A prominent example is the Pilsner compiler [Neis et al. 2015] that compiles a higher-order language into some form of assembly programs. The technique Pilsner adopts is called *parametric simulations* that evolves from earlier work on reasoning about program equivalence via bisimulation [Hur et al. 2012a]. Another line of work is multi-language semantics [Patterson and Ahmed 2019; Patterson et al. 2017; Perconti and Ahmed 2014; Scherer et al. 2018] where a language combining all source, intermediate and target languages is used to formalize semantics. Compiler correctness is stated as contextual equivalence or logical relations. It seems that our techniques are not directly applicable to those work because relations on higher-order states cannot deterministically fix the interpolating states. A possible solution is to divide the higher-order memory into a first-order and a higher-order part such that the former does not contain pointers to the latter (forming a closure). By encapsulating higher-order programs inside first-order states, we may be able to apply our approach.

The high-level ideas for constructing interpolating states for proving transitivity of `injp` can also be found in some of the work on program equivalence [Ahmed 2006; Hur et al. 2012b]. To the best of our knowledge, our approach is the first concrete implementation of these ideas that works for a realistic optimizing compiler for imperative languages with non-trivial memory models.

8.3 Frameworks for Compositional Program Verification

Researchers have proposed frameworks for compositional program verification based on novel semantics, refinements and separation logics [Chappe et al. 2023; Gu et al. 2015, 2018; He et al. 2021; Sammler et al. 2023; Song et al. 2023; Xia et al. 2019]. These frameworks aim at broader program verification and may be combined with our approach to generate more flexible end-to-end verification techniques. For example, to support more flexible certified abstraction layers, we may combine our approach with data abstraction in CAL and extend horizontal linking to work with abstraction layers. It is not entirely clear whether their solutions can be successfully applied to or combined with VCC of realistic optimizing compilers like CompCert. However, comparing with these frameworks is still meaningful as it provides different perspectives and potential directions for improving our work. We discuss representative frameworks in these categories below.

DimSum. DimSum [Sammler et al. 2023] is a framework for multi-language program verification. Program semantics are defined as LTSs which emit *events* to communicate with the environment. The concept of events in DimSum is similar to the language interfaces in CompCertO and in our work. For verification of heterogeneous programs, it uses *wrappers* to relate the events between two languages (a C-like language called Rec and assembly in its paper), which is similar to simulation conventions. The rely-guarantee protocol is expressed in the wrappers by angelic non-determinism and memory protection is expressed in separation logic. On one hand, it is unclear if their framework can scale to realistic languages or compilers like CompCert. For example, it is interesting to investigate if their wrappers can support more complicated languages and compiler optimizations which can be handled by our framework and refinement relations. On the other hand, DimSim allows assembly modules that exploit a flat memory model. Therefore, their framework supports refinements between semantics using different memory models, which we do not support yet.

Conditional Contextual Refinement. Conditional Contextual Refinement (CCR) is a framework which combines contextual refinement and separation logics to achieve both conditional and composable verification of program semantics [Song et al. 2023]. CCR employs separation logics to constrain the behavior of open modules to achieve horizontal and vertical composition of refinements, such *separation logic wrapper* plays a similar role as simulation conventions in this paper. On one hand, separation logics provide more fine-grained control of shared resources. On the other hand, they have specific requirements of contexts unlike the open protocols encoded in our direct refinements. The horizontal composition of two refinements requires specific knowledge of specifications of each other to control interaction. It is interesting to investigate if the program specific conditions imposed by CCR can be handled or piggybacked upon our framework.

9 CONCLUSION AND FUTURE WORK

We have proposed an approach to compositional compiler correctness for first-order languages via direct refinements between source and target semantics at their native interfaces, which overcomes the limitations of the existing approaches on compositionality, adequacy and other important criteria for VCC. In the future, we plan to support behavior (trace) refinement for closed programs by reducing our open simulation into the whole-program correctness theorem for the original CompCert. We also plan to combine our work with refinement-based program verification like certified abstraction layers to support more substantial applications. Another research direction is to apply our approach to different memory models and compilers for first-order and higher-order languages, which will better test the limit of our approach and the usefulness of our discoveries.

ACKNOWLEDGMENTS

We would like to thank our shepherd Yannick Zakowski and the anonymous referees for their helpful feedback which improved this paper significantly. This work is supported in part by the National Natural Science Foundation of China (NSFC) under Grant No. 62002217 and 62372290, and by the Natural Science Foundation of the United States (NSF) under Grant No. 1763399, 2019285, and 2313433. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies.

REFERENCES

Amal J. Ahmed. 2006. Step-Indexed Syntactic Logical Relations for Recursive and Quantified Types. In *Proc. 15th European Symposium on Programming (ESOP'06) (LNCS, Vol. 3924)*, Peter Sestoft (Ed.). Springer, Cham, 69–83. https://doi.org/10.1007/11693024_6

Frédéric Besson, Sandrine Blazy, and Pierre Wilke. 2015. A Concrete Memory Model for CompCert. In *Proc. 6th Interactive Theorem Proving (ITP'15) (LNCS, Vol. 9236)*, Christian Urban and Xingyuan Zhang (Eds.). Springer, Cham, 67–83. https://doi.org/10.1007/978-3-319-22102-1_5

Nicolas Chappe, Paul He, Ludovic Henrio, Yannick Zakowski, and Steve Zdancewic. 2023. Choice Trees: Representing Nondeterministic, Recursive, and Impure Programs in Coq. *Proc. ACM Program. Lang.* 7, POPL, Article 61 (January 2023), 31 pages. https://doi.org/10.1145/3571254

Ronghui Gu, Jérémie Koenig, Tahina Ramananandro, Zhong Shao, Xiongnan(Newman) Wu, Shu-Chun Weng, Haozhong Zhang, and Yu Guo. 2015. Deep Specifications and Certified Abstraction Layers. In *Proc. 42nd ACM Symposium on Principles of Programming Languages (POPL'15)*, Sriram K. Rajamani and David Walker (Eds.). ACM, New York, NY, USA, 595–608. https://doi.org/10.1145/2775051.2676975

Ronghui Gu, Zhong Shao, Jieung Kim, Xiongnan (Newman) Wu, Jérémie Koenig, Vilhelm Sjober, Hao Chen, David Costanzo, and Tahnia Ramananandro. 2018. Certified Concurrent Abstraction Layers. In *Proc. 2018 ACM Conference on Programming Language Design and Implementation (PLDI'18)*, Jeffrey S. Foster and Dan Grossman (Eds.). ACM, New York, NY, USA, 646–661. https://doi.org/10.1145/3192366.3192381

Paul He, Eddy Westbrook, Brent Carmer, Chris Phifer, Valentin Robert, Karl Smeltzer, Andrei Ştefănescu, Aaron Tomb, Adam Wick, Matthew Yacavone, and Steve Zdancewic. 2021. A Type System for Extracting Functional Specifications from Memory-Safe Imperative Programs. *Proc. ACM Program. Lang.* 5, OOPSLA, Article 135 (October 2021), 29 pages. https://doi.org/10.1145/3485512

Chung-Kil Hur, Derek Dreyer, Georg Neis, and Viktor Vafeiadis. 2012a. The marriage of bisimulations and Kripke logical relations. In *Proc. 39th ACM Symposium on Principles of Programming Languages (POPL'12)*, John Field and Michael Hicks (Eds.). ACM, New York, NY, USA, 59–72. https://doi.org/10.1145/2103656.2103666

Chung-Kil Hur, Georg Neis, Derek Dreyer, and Viktor Vafeiadis. 2012b. *The Transitive Composability of Relation Transition Systems.* Technical Report, MPI-SWS-2012-002. MPI-SWS.

Hanru Jiang, Hongjin Liang, Siyang Xiao, Junpeng Zha, and Xinyu Feng. 2019. Towards certified separate compilation for concurrent programs. In *Proc. 2019 ACM Conference on Programming Language Design and Implementation (PLDI'19)*, Kathryn S. McKinley and Kathleen Fisher (Eds.). ACM, New York, NY, USA, 111–125. https://doi.org/10.1145/3314221.3314595

Jeehoon Kang, Chung-Kil Hur, Ori Lahav, Viktor Vafeiadis, and Derek Dreyer. 2017. A promising semantics for relaxed-memory concurrency. In *Proc. 44th ACM Symposium on Principles of Programming Languages (POPL'17)*, Giuseppe Castagna and Andrew D. Gordon (Eds.). ACM, New York, NY, USA, 175–189. https://doi.org/10.1145/3009837.3009850

Jeehoon Kang, Chung-Kil Hur, William Mansky, Dmitri Garbuzov, Steve Zdancewic, and Viktor Vafeiadis. 2015. A formal C memory model supporting integer-pointer casts. In *Proc. 2015 ACM Conference on Programming Language Design and Implementation (PLDI'15)*, David Grove and Stephen M. Blackburn (Eds.). ACM, New York, NY, USA, 326–335. https://doi.org/10.1145/2737924.2738005

Jérémie Koenig and Zhong Shao. 2021. CompCertO: Compiling Certified Open C Components. In *Proc. 2021 ACM Conference on Programming Language Design and Implementation (PLDI'21)*. ACM, New York, NY, USA, 1095–1109. https://doi.org/10.1145/3453483.3454097

Robbert Krebbers. 2016. A formal C memory model for separation logic. *J. Autom. Reason.* 57 (2016), 319–387. https://doi.org/10.1007/s10817-016-9369-1

Sung-Hwan Lee, Minki Cho, Anton Podkopaev, Soham Chakraborty, Chung-Kil Hur, Ori Lahav, and Viktor Vafeiadis. 2020. Promising 2.0: Global Optimizations in Relaxed Memory Concurrency. In *Proc. 2020 ACM Conference on Programming Language Design and Implementation (PLDI'20)*. ACM, New York, NY, USA, 362–376. https://doi.org/10.1145/3385412.3386010

Xavier Leroy. 2005–2023. The CompCert Verified Compiler. https://compcert.org/.

Xavier Leroy, Andrew W. Appel, Sandrine Blazy, and Gordon Stewart. 2012. *The CompCert Memory Model, Version 2.* Research Report RR-7987. INRIA. 26 pages. https://hal.inria.fr/hal-00703441

Georg Neis, Chung-Kil Hur, Jan-Oliver Kaiser, Craig McLaughlin, Derek Dreyer, and Viktor Vafeiadis. 2015. Pilsner: a compositionally verified compiler for a higher-order imperative language. In *Proc. 2015 ACM SIGPLAN International Conference on Functional Programming (ICFP'15)*, Kathleen Fisher and John H. Reppy (Eds.). ACM, New York, NY, USA, 166–178. https://doi.org/10.1145/2784731.2784764

Daniel Patterson and Amal Ahmed. 2019. The next 700 Compiler Correctness Theorems (Functional Pearl). *Proc. ACM Program. Lang.* 3, ICFP, Article 85 (August 2019), 29 pages. https://doi.org/10.1145/3341689

Daniel Patterson, Jamie Perconti, Christos Dimoulas, and Amal Ahmed. 2017. FunTAL: Reasonably Mixing a Functional Language with Assembly. *SIGPLAN Not.* 52, 6 (2017), 495–509. https://doi.org/10.1145/3140587.3062347

James T. Perconti and Amal Ahmed. 2014. Verifying an Open Compiler Using Multi-language Semantics. In *Proc. 23rd European Symposium on Programming (ESOP'14) (LNCS, Vol. 8410)*, Zhong Shao (Ed.). Springer, Cham, 128–148. https://doi.org/10.1007/978-3-642-54833-8_8

Michael Sammler, Simon Spies, Youngju Song, Emanuele D'Osualdo, Robbert Krebbers, Deepak Garg, and Derek Dreyer. 2023. DimSum: A Decentralized Approach to Multi-Language Semantics and Verification. *Proc. ACM Program. Lang.* 7, POPL, Article 27 (January 2023), 31 pages. https://doi.org/10.1145/3571220

Gabriel Scherer, Max New, Nick Rioux, and Amal Ahmed. 2018. Fabous Interoperability for ML and a Linear Language. In *Foundations of Software Science and Computation Structures*, Christel Baier and Ugo Dal Lago (Eds.). Springer, Cham, 146–162.

Youngju Song, Minki Cho, Dongjoo Kim, Yonghyun Kim, Jeehoon Kang, and Chung-Kil Hur. 2020. CompCertM: CompCert with C-Assembly Linking and Lightweight Modular Verification. *Proc. ACM Program. Lang.* 4, POPL, Article 23 (January 2020), 31 pages. https://doi.org/10.1145/3371091

Youngju Song, Minki Cho, Dongjae Lee, Chung-Kil Hur, Michael Sammler, and Derek Dreyer. 2023. Conditional Contextual Refinement. *Proc. ACM Program. Lang.* 7, POPL, Article 39 (January 2023), 31 pages. https://doi.org/10.1145/3571232

Gordon Stewart, Lennart Beringer, Santiago Cuellar, and Andrew W. Appel. 2015. Compositional CompCert. In *Proc. 42nd ACM Symposium on Principles of Programming Languages (POPL'15).* ACM, New York, NY, USA, 275–287. https://doi.org/10.1145/2676726.2676985

Yuting Wang, Pierre Wilke, and Zhong Shao. 2019. An Abstract Stack Based Approach to Verified Compositional Compilation to Machine Code. *Proc. ACM Program. Lang.* 3, POPL, Article 62 (January 2019), 30 pages. https://doi.org/10.1145/3290375

Yuting Wang, Ling Zhang, Zhong Shao, and Jérémie Koenig. 2022. Verified Compilation of C Programs with a Nominal Memory Model. *Proc. ACM Program. Lang.* 6, POPL, Article 25 (January 2022), 31 pages. https://doi.org/10.1145/3498686

Li-yao Xia, Yannick Zakowski, Paul He, Chung-Kil Hur, Gregory Malecha, Benjamin C. Pierce, and Steve Zdancewic. 2019. Interaction Trees: Representing Recursive and Impure Programs in Coq. *Proc. ACM Program. Lang.* 4, POPL, Article 51 (January 2019), 32 pages. https://doi.org/10.1145/3371119

Junpeng Zha, Hongjin Liang, and Xinyu Feng. 2022. Verifying Optimizations of Concurrent Programs in the Promising Semantics. In *Proc. 2021 ACM Conference on Programming Language Design and Implementation (PLDI'22).* ACM, New York, NY, USA, 903–917. https://doi.org/10.1145/3519939.3523734

A TRANSITIVITY OF injp

A.1 More complete definitions of memory injection and injp accessibility

We have used a simplified version of definitions of perm, $\hookrightarrow_m$ and $\leadsto_{\texttt{injp}}$ in Sec. 4. To present a more detailed proof of the KMR with memory protection (injp), we present full definitions of perm and $\leadsto_{\texttt{injp}}$. We also present a more complete definition of $\hookrightarrow_m$ which is still not 100% complete because we ignore two properties for simplicity. They are about alignment and range of size δ in mapping $j(b) = \lfloor (b', \delta) \rfloor$. They are not essential for this proof as preconditions and can be proved similarly as other properties of $\hookrightarrow_m$. Readers interested in these details can find them in our artifact.

By the definition of CompCert memory model, a memory cell has both maximum and current permissions such that $\texttt{perm}_{\texttt{cur}}(m, p) \subseteq \texttt{perm}_{\texttt{max}}(m, p)$. During the execution of a program, the current permission of a memory cell may be lowered or raised by an external call. However, the maximum permission can only decrease in both internal and external calls. This invariant was defined in CompCert as:

$$\begin{array}{l}\texttt{max-perm-dec}(m_1, m_2) \Leftrightarrow \\ \quad \forall\, b\ o\ p,\ b \in m_1 \Rightarrow (b, o) \in \texttt{perm}_{\texttt{max}}(m_2, p) \Rightarrow (b, o) \in \texttt{perm}_{\texttt{max}}(m_1, p)\end{array}$$

Definition A.1. Definition of memory injection $\hookrightarrow_m$.

$$\begin{array}{l}
m_1 \hookrightarrow_m^j m_2 := \{| \\
\quad \text{(* Preservation of permission under injection *)} \\
\quad (1)\ \forall\, b_1\ b_2\ o_1\ o_2\ k\ p,\ j(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor \Rightarrow (b_1, o_1) \in \texttt{perm}_k(m_1, p) \Rightarrow (b_2, o_2) \in \texttt{perm}_k(m_2, p) \\
\quad \text{(* Preservation of memory values for currently readable cells under injection *)} \\
\quad (2)\ \forall\, b_1\ b_2\ o_1\ o_2,\ j(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor \Rightarrow (b_1, o_1) \in \texttt{perm}_{\texttt{cur}}(m_1, \texttt{Readable}) \\
\quad\quad \Rightarrow m_1[b_1, o_1] \hookrightarrow_v^j m_2[b_2, o_2] \\
\quad \text{(* Invalid source blocks must be unmapped *)} \\
\quad (3)\ \forall\, b_1,\ b_1 \notin m_1 \Rightarrow j(b_1) = \emptyset \\
\quad \text{(* The range of } j \text{ must only contain valid blocks *)} \\
\quad (4)\ \forall\, b_1\ b_2\ \delta,\ j(b_1) = \lfloor (b_2, \delta) \rfloor \Rightarrow b_2 \in m_2 \\
\quad \text{(* Two disjoint source cells with non-empty permission} \\
\quad\quad \text{do not overlap with each other after injection *)} \\
\quad (5)\ \forall\, b_1\ b_2\ o_1\ o_2\ b_1'\ b_2'\ o_1'\ o_2',\ b_1 \neq b_1' \Rightarrow j(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor \Rightarrow j(b_1') = \lfloor (b_2', o_2' - o_1') \rfloor \Rightarrow \\
\quad\quad (b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA}) \Rightarrow (b_1', o_1') \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA}) \Rightarrow b_2 \neq b_2' \vee o_2 \neq o_2'
\end{array}$$

(* Given a target cell, its corresponding source cell either
have the same permission or does not have any permission *)
(6) $\forall\, b_1\ o_1\ b_2\ o_2\ k\ p,\ j(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \Rightarrow (b_2, o_2) \in \mathtt{perm}_k(m_2, p)$
$\Rightarrow (b_1, o_1) \in \mathtt{perm}_k(m_1, p) \lor (b_1, o_1) \notin \mathtt{perm}_{\mathtt{max}}(m_1, \mathsf{NA})$

Definition A.2. Definition of memory accessibility mem-acc.

$$\begin{array}{lcl}
\mathtt{ro\text{-}unchanged}(m, m') & \Leftrightarrow & \forall (b, o) \in m, (b, o) \notin \mathtt{perm}_{\mathtt{max}}(m, \mathtt{Writable}) \Rightarrow m'[b, o] = v \\
& & \Rightarrow (b, o) \in \mathtt{perm}_{\mathtt{cur}}(m', \mathtt{Readable}) \Rightarrow (m[b, o] = v \land \\
& & (b, o) \in \mathtt{perm}_{\mathtt{cur}}(m, \mathtt{Readable})) \\
\mathtt{mem\text{-}acc}(m, m') & \Leftrightarrow & \mathtt{validblock}(m) \subseteq \mathtt{validblock}(m') \land \\
& & \mathtt{max\text{-}perm\text{-}dec}(m, m') \land\ \mathtt{ro\text{-}unchanged}(m, m')
\end{array}$$

For the complete definition of $\leadsto_{\mathtt{injp}}$, we further define the separation property for injection as:

$\mathtt{inject\text{-}sep}(j, j', m_1, m_2) \Leftrightarrow$
$\forall\, b_1\ b_2\ \delta,\ \ j(b_1) = \emptyset \Rightarrow j'(b_1) = \lfloor(b_2, \delta)\rfloor \Rightarrow b_1 \notin m_1 \land b_2 \notin m_2$

This invariant states that when we start from $m_1 \hookrightarrow_m^j m_2$, after executing on source and target semantics, the future injection j' only increases from j by relating newly allocated blocks. Note that we write $b \in m$ for $b \in \mathtt{validblock}(m)$.

Definition A.3. Accessibility relation of injp

$$\begin{array}{lcl}
(j, m_1, m_2) \leadsto_{\mathtt{injp}} (j', m_1', m_2') & \Leftrightarrow & j \subseteq j' \land \mathtt{unmapped}(j) \subseteq \mathtt{unchanged\text{-}on}(m_1, m_1') \\
& & \land\ \mathtt{out\text{-}of\text{-}reach}(j, m_1) \subseteq \mathtt{unchanged\text{-}on}(m_2, m_2') \\
& & \land\ \mathtt{mem\text{-}acc}(m_1, m_1') \land \mathtt{mem\text{-}acc}(m_2, m_2') \\
& & \land\ \mathtt{inject\text{-}sep}(j, j', m_1, m_2).
\end{array}$$

A.2 Auxiliary Properties

In this section we present several lemmas about properties of memory injection and injp accessibility. These lemmas are used in the proof of injp refinement.

Firstly, the memory injections are composable.

Lemma A.4. *Given $m_1 \hookrightarrow_m^{j_{12}} m_2$ and $m_2 \hookrightarrow_m^{j_{23}} m_3$, we have*

$$m_1 \hookrightarrow_m^{j_{23} \cdot j_{12}} m_3$$

This property is proved and used in CompCert, we do not repeat the proof here.

Lemma A.5. *Given $m_1 \hookrightarrow_m^{j_{23} \cdot j_{12}} m_3$, $(b_1, o_1) \in \mathtt{perm}_{\mathtt{cur}}(m_1, \mathtt{Readable})$ and $j_{23} \cdot j_{12}(b_1) = \lfloor(b_3, o_3 - o_1)\rfloor$, then*

$$\exists v_2, m_1[b_1, o_1] \hookrightarrow_v^{j_{12}} v_2 \land v_2 \hookrightarrow_v^{j_{23}} m_3[b_3, o_3].$$

Note that $j_{23} \cdot j_{12}(b_1) = \lfloor(b_3, o_3 - o_1)\rfloor$ iff $\exists\, b_2\ o_2, j_{12}(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \land j_{23}(b_2) = \lfloor(b_3, o_3 - o_2)\rfloor$.

Proof. According to property (2) in Definition A.1, we know that $m_1[b_1, o_1] \hookrightarrow_v^{j_{23} \cdot j_{12}} m_3[b_3, o_3]$. We divide the value $m_1[b_1, o_1]$ into:

- If $m_1[b_1, o_1] = \mathtt{Vundef}$, we take $v_2 = \mathtt{Vundef}$. Then $\mathtt{Vundef} \hookrightarrow_v^{j_{12}} \mathtt{Vundef} \land \mathtt{Vundef} \hookrightarrow_v^{j_{23}} m_3[b_3, o_3]$ trivially holds.
- If $m_1[b_1, o_1]$ is a concrete value, we take $v_2 = m_1[b_1, o_1]$. In such case we have $m_1[b_1, o_1] = v_2 = m_3[b_3, o_3]$.

- If $m_1[b_1, o_1] = \texttt{Vptr}(b'_1, o'_1)$, we can derive that $\texttt{Vptr}(b'_1, o'_1) \hookrightarrow_v^{j_{23} \cdot j_{12}} m_3[b_3, o_3]$ implies $\exists b'_3\ o'_3, s.t. m_3[b_3, o_3] = \texttt{Vptr}(b'_3, o'_3)$ and $j_{23} \cdot j_{12}(b'_1) = \lfloor (b'_3, o'_3 - o'_1) \rfloor$. Therefore
$$\exists b'_2\ o'_2, j_{12}(b'_1) = \lfloor (b'_2, o'_2 - o'_1) \rfloor \wedge j_{23}(b'_2) = \lfloor (b'_3, o'_3 - o'_2) \rfloor$$
We take $v_2 = \texttt{Vptr}(b'_2, o'_2)$ and $m_1[b_1, o_1] \hookrightarrow_v^{j_{12}} v_2 \wedge v_2 \hookrightarrow_v^{j_{23}} m_3[b_3, o_3]$ can be derived from the formula above.

□

Lemma A.6. *Given $m_1 \hookrightarrow_m^{j_{12}} m_2$, $m_2 \hookrightarrow_m^{j_{23}} m_3$ and $j_{23}(b_2) = \lfloor (b_3, o_3 - o_2) \rfloor$. If $(b_2, o_2) \in \texttt{out-of-reach}(j_{12}, m_1)$ and $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$, then*
$$(b_3, o_3) \in \texttt{out-of-reach}(j_{23} \cdot j_{12}, m_1)$$

Proof. According to the definition of out-of-reach, If $j_{12}(b_1) = \lfloor (b'_2, o'_2 - o_1) \rfloor$ and $j_{23}(b'_2) = \lfloor (b_3, o_3 - o_1) \rfloor$, we need to prove that $(b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$. If $b_2 = b'_2$, from $(b_2, o_2) \in \texttt{out-of-reach}(j_{12}, m_1)$ we can directly prove $(b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$.

If $b_2 \neq b'_2$, we assume that $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$, by property (1) of $m_1 \hookrightarrow_m^{j_{12}} m_2$ we get $(b'_2, o'_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$. Now (b_2, o_2) and (b'_2, o'_2) are two different positions in m_2 which are mapped to the same position (m_3, o_3) in m_3. This scenario is prohibited by the non-overlapping property (5) of $m_2 \hookrightarrow_m^{j_{23}} m_3$. So $(b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$. □

A.3 Proof of Lemma 4.3

Based on definitions and lemmas before, we prove Lemma 4.3 in this section:
$$\begin{aligned}
&\forall j_{12}\ j_{23}\ m_1\ m_2\ m_3,\ m_1 \hookrightarrow_m^{j_{12}} m_2 \Rightarrow m_2 \hookrightarrow_m^{j_{23}} m_3 \Rightarrow \exists j_{13},\ m_1 \hookrightarrow_m^{j_{13}} m_3 \wedge \\
&\quad \forall m'_1\ m'_3\ j'_{13},\ (j_{13}, m_1, m_3) \leadsto_{\texttt{injp}} (j'_{13}, m'_1, m'_3) \Rightarrow m'_1 \hookrightarrow_m^{j'_{13}} m'_3 \Rightarrow \\
&\quad\quad \exists m'_2\ j'_{12}\ j'_{23}, (j_{12}, m_1, m_2) \leadsto_{\texttt{injp}} (j'_{12}, m'_1, m'_2) \wedge m'_1 \hookrightarrow_m^{j'_{12}} m'_2 \\
&\quad\quad\quad\quad \wedge (j_{23}, m_2, m_3) \leadsto_{\texttt{injp}} (j'_{23}, m'_2, m'_3) \wedge m'_2 \hookrightarrow_m^{j'_{23}} m'_3.
\end{aligned}$$
Given $m_1 \hookrightarrow_m^{j_{12}} m_2$ and $m_2 \hookrightarrow_m^{j_{23}} m_3$. We take $j_{13} = j_{23} \cdot j_{12}$, from Lemma A.4 we can prove $m_1 \hookrightarrow_m^{j_{13}} m_3$. After the external call, given $(j_{13}, m_1, m_3) \leadsto_{\texttt{injp}} (j'_{13}, m'_1, m'_3)$ and $m'_1 \hookrightarrow_m^{j'_{13}} m'_3$.

We present the construction and properties of j'_{12}, j'_{23} and m'_2 in Sec. A.3.1. Then the proof reduce to prove $m'_1 \hookrightarrow_m^{j'_{12}} m'_2$, $m'_2 \hookrightarrow_m^{j'_{23}} m'_3$, $(j_{12}, m_1, m_2) \leadsto_{\texttt{injp}} (j'_{12}, m'_1, m'_2)$ and $(j_{23}, m_2, m_3) \leadsto_{\texttt{injp}} (j'_{23}, m'_2, m'_3)$, they are proved in Sec. A.3.2

A.3.1 *Construction and properties of j'_{12}, j'_{23} and m'_2.*

Definition A.7. We construct the memory state m'_2 by the following three steps, j'_{12} and j'_{23} are constructed in step (1).

(1) We first extend m_2 by allocating new blocks, at the same time we extend j_{12}, j_{23} to get j'_{12} and j'_{23} such that $j'_{13} = j'_{23} \cdot j'_{12}$. Specifically, for each new block b_1 in m'_1 relative to m_1 which is mapped by j'_{13} as $j'_{13}(b_1) = \lfloor (b_3, \delta) \rfloor$, we allocate a new memory block b_2 from m_2 and add new mappings $(b_1, (b_2, 0))$ and $(b_2, (b_3, \delta))$ to j_{12} and j_{23}, respectively.
(2) We then copy the contents of new blocks in m'_1 into corresponding new blocks in m'_2 as follows. For each *mapped* new block b_1 in m'_1 where $j'_{12}(b_1) = \lfloor (b_2, 0) \rfloor$, we enumerate all positions $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m'_1, \texttt{NA})$ and copy the permission of (b_1, o_1) in m'_1 to (b_2, o_1) in m'_2. If $(b_1, o_1) \in \texttt{perm}_{\texttt{cur}}(m'_1, \texttt{Readable})$, we further set $m'_2[b_2, o_1]$ to v_2 where $m'_1[b_1, o_1] \hookrightarrow_m^{j_{12}'} v_2$. The existence of v_2 here is provided by Lemma A.5 with preconditions $m'_1 \hookrightarrow_m^{j'_{13}} m'_3$, $(b_1, o_1) \in \texttt{perm}_{\texttt{cur}}(m'_1, \texttt{Readable})$ and $j'_{13}(b_1) = \lfloor (b_3, \delta) \rfloor$ (because b_1 is a new block chosen in step (1)).

(3) Finally, we update the old blocks of m_2. If a position $(b_2, o_2) \in \texttt{pub-tgt-mem}(j_{12}, m_1) \cap \texttt{pub-src-mem}(j_{23})$, the permission and value of this position in m_2' should comes from the corresponding position (b_1, o_1) in m_1' as depicted in Fig. 15b. Note that the values are changed only if the position is not read-only in m_2. Other positions just remain unchanged from m_2 to m_2'. To complete the construction, we have to enumerate the set $\texttt{pub-tgt-mem}(j_{12}, m_1) \cap \texttt{pub-src-mem}(j_{23})$. We state that

$$\texttt{pub-tgt-mem}(j_{12}, m_1) \subseteq \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$$

where $\texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$ is enumerable. Note that $(b_2, o_2) \in \texttt{pub-tgt-mem}(j_{12}, m_1) \Leftrightarrow (b_2, o_2) \notin \texttt{out-of-reach}(j_{12}, m_1)$ by definition. If $(b_2, o_2) \in \texttt{pub-tgt-mem}(j_{12}, m_1)$, then there exists $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$ such that $j_{12}(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor$. The property (1) of $m_1 \hookrightarrow_m^{j_{12}} m_2$ ensures that $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$.
The concrete algorithm can be described as follows. For $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{None-empty})$, we can enumerate $\texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$ to find whether there exists a corresponding position $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$ such that $j_{12}(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor$. Note that the property (3) of $m_1 \hookrightarrow_m^{j_{12}} m_2$ ensures that we cannot find more than one of such position. If there exists such (b_1, o_1) and $j_{23}(b_2) \neq \lfloor (b_3, o_3) \rfloor$, We copy the permission of position (b_1, o_1) in m_1' to (b_2, o_2). If $(b_1, o_1) \in \texttt{perm}_{\texttt{cur}}(m_1', \texttt{Readable})$ and $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{Writable})$, we further set $m_2'[b_2, o_2]$ to v_2 where $m_1'[b_1, o_1] \hookrightarrow_v^{j_{12}'} v_2$.

We present several lemmas about j_{12}', j_{23}' and m_2' according to Definition A.7 as follows.

Lemma A.8.

$$(1) j_{12} \subseteq j_{12}' \ (2) j_{23} \subseteq j_{23}' \ (3)\texttt{inject-sep}(j_{12}, j_{12}', m_1, m_2) \ (4)\texttt{inject-sep}(j_{23}, j_{23}', m_2, m_3)$$

Proof. Directly from the construction step (1) □

Lemma A.9.

$$(1)\texttt{out-of-reach}(j_{12}, m_1) \subseteq \texttt{unchanged-on}(m_2, m_2') \ (2)\texttt{unmapped}(j_{23}) \subseteq \texttt{unchanged-on}(m_2, m_2')$$

Proof. For each changed position (b_2, o_2) from m_2 to m_2' in step (3), we enforce that $\exists b_1, j_{12}(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor \wedge (b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$ and $(b_2, o_2) \notin \texttt{unmapped}(j_{23})$. Thus, if $(b_2, o_2) \in \texttt{out-of-reach}(j_{12}, m_1)$ or $(b_2, o_2) \in \texttt{unmapped}(j_{23})$, then $(b_2, o_2) \in \texttt{unchanged-on}(m_2, m_2')$.
□

Lemma A.10.

$$\texttt{max-perm-dec}(m_2, m_2')$$

Proof. For unchanged position (b_2, o_2) in m_2, we trivially have $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2', p) \Leftrightarrow (b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, p)$. If (b_2, o_2) is changed in step (3), then the permission of (b_2, o_2) in m_2' is copied from some corresponding position (b_1, o_1) in $m_1'(j_{12}(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor)$. Given $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2', p)$, we get $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1', p)$. Form $\texttt{max-perm-dec}(m_1, m_1')$ we can further derive that $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, p)$. Finally, by property (1) of $m_1 \hookrightarrow_m^{j_{12}} m_2$ we can conclude that $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, p)$. □

Lemma A.11.

$$\texttt{ro-unchanged}(m_2, m_2')$$

Proof. For each position (b_2, o_2) which has changed value from m_2 to m_2' in step (3). We enforce that it is not read-only in m_2. □

Lemma A.12.

$$\texttt{mem-acc}(m_2, m_2')$$

Proof. From step(1) we have $m_2 \subseteq m_2'$. Together with Lemma A.10 and Lemma A.11 we can derive this lemma. □

A.3.2 Proof of remaining formulas. Recall that we are still proving Lemma 4.3, we have constructed j_{12}', j_{23}' and m_2'. Based on the construction and properties of them presented above, we present complete proofs of last four formulas separately in this section.

Lemma A.13. $m_1' \hookrightarrow_m^{j_{12}'} m_2'$

Proof. We check the properties in Definition A.1 as follows:

(1) Given $j_{12}'(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \wedge (b_1, o_1) \in \texttt{perm}_k(m_1', p)$. We prove $(b_2, o_2) \in \texttt{perm}_k(m_2', p)$ by cases of $j_{12}(b_1)$. Note that $j_{12}(b_1)$ is either $\emptyset$ or the same as $j_{12}'(b_1)$ because of $j_{12} \subseteq j_{12}'$.
- If $j_{12}(b_1) = \emptyset$, the mapping $j_{12}'(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor$ is added in step (1). As a result, we know $\exists b_3\ \delta, j_{13}'(b_1) = \lfloor b_3, \delta\rfloor$. Since $\texttt{perm}_k(m_1', p) \subseteq \texttt{perm}_{\texttt{max}}(m_1', \texttt{NA})$, we know $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1', \texttt{NA})$ and the permission of (b_1, o_1) in m_1' is copied to (m_2, o_2) in m_2' in step (2). Therefore $(b_2, o_2) \in \texttt{perm}_k(m_2', p)$.
- If $j_{12}(b_1) = \lfloor(b_2, o_2)\rfloor$, we further divide whether (b_2, o_2) is a public position by $j_{23}(b_2)$
  - If $j_{23}(b_2) = \emptyset$, i.e. $(b_2, o_2) \in \texttt{unmapped}(j_{23})$, According to Lemma A.9, we know $(b_2, o_2) \in \texttt{unchanged-on}(m_2, m_2')$. At the same time, we also get $(b_1, o_1) \in \texttt{unmapped}(j_{13})$ because of $j_{13} = j_{23} \cdot j_{12}$. Together with $(j_{13}, m_1, m_3) \rightsquigarrow_{\texttt{injp}} (j_{13}', m_1', m_3')$, we can conclude that $(b_1, o_1) \in \texttt{unchanged-on}(m_1, m_1')$.

    Therefore, we get $(b_1, o_1) \in \texttt{perm}_k(m_1, p)$. Using property (1) of $m_1 \hookrightarrow_m^{j_{12}} m_2$ we get $(b_2, o_2) \in \texttt{perm}_k(m_2, p)$. Since (b_2, o_2) is also unchanged between m_2 and m_2', $(b_2, o_2) \in \texttt{perm}_k(m_2', p)$.
  - If $j_{23}(b_2) = \lfloor(b_3, o_3 - o_2)\rfloor$, the permission of (b_2, o_2) in m_2' is set as the same as (b_1, o_1) in m_1' in step (3). So $(b_2, o_2) \in \texttt{perm}_k(m_2', p)$ holds trivially.

(2) Given $j_{12}'(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \wedge (b_1, o_1) \in \texttt{perm}_{\texttt{cur}}(m_1', \texttt{Readable})$, following the method in (1) we can prove $m_1'[b_1, o_1] \hookrightarrow_v^{j_{12}'} m_2'[b_2, o_2]$. Note that if (b_2, o_2) is read-only in m_2, from property (6) of $m_1 \hookrightarrow_m^{j_{12}} m_2$ we can derive that (b_1, o_1) is also read-only in m_1. Thus the values related by j are both unchanged in m_1' and m_2' thus can be related by j' where $j \subseteq j'$.

(3) Given $b_1 \notin m_1'$, we know $b_1 \notin m_1$, therefore $j_{12}(b_1) = \emptyset$. Since b_1 cannot be added to j_{12}' in step (1), we can conclude that $j_{12}'(b_1) = \emptyset$.

(4) Given $j_{12}'(b_1) = \lfloor(b_2, \delta)\rfloor$, It is easy to show b_2 is either old block in $m_2(j_{12}(b_1) = \lfloor(b_2, \delta)\rfloor)$ or newly allocated block$(j_{12}(b_1) = \emptyset)$, therefore $b_2 \in m_2'$.

(5) Given $j_{12}'(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \wedge (b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1', \texttt{NA})$ and $j_{12}'(b_1') = \lfloor(b_2', o_2' - o_1')\rfloor \wedge (b_1', o_1') \in \texttt{perm}_{\texttt{max}}(m_1', \texttt{NA})$ where $b_1 \neq b_1'$. We need to prove these two positions do not overlap $((b_2, o_2) \neq (b_2', o_2'))$ by cases of whether b_1 and b_1' are mapped by old injection j_{12}. Note that $j_{12} \subseteq j_{12}'$, so $j_{12}(b)$ is either $\emptyset$ or the same as $j_{12}'(b)$.
- $j_{12}(b_1) = j_{12}(b_1') = \emptyset$. The j_{12}' mappings of them are added in step (1). It is obvious that newly added mappings in step (1) never map different blocks in m_1' into the same block in m_2'. Therefore $b_2 \neq b_2'$.
- $j_{12}(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor, j_{23}(b_1') = \emptyset$. we can derive that $b_2 \in m_2$ by property (4) of $m_1 \hookrightarrow_m^{j_{12}} m_2$. While b_2' is newly allocated from m_2 in step (1). Therefore $b_2 \neq b_2'$.
- $j_{12}(b_1) = \emptyset, j_{12}(b_1') = \lfloor(b_2', o_2' - o_1')\rfloor$. Similarly we have $b_2 \neq b_2'$.

- $j_{12}(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor$, $j_{12}(b_1') = \lfloor(b_2', o_2' - o_1')\rfloor$. We can prove $(b_2, o_2) \neq (b_2, o_2')$ using the property (5) in $m_1 \hookrightarrow_m^{j_{12}} m_2$ by showing $(b_1, o_1) \in \mathtt{perm}_{\mathsf{max}}(m_1, \mathsf{NA})$ and $(b_1', o_1') \in \mathtt{perm}_{\mathsf{max}}(m_1, \mathsf{NA})$. This follows from $\mathtt{max\text{-}perm\text{-}dec}(m_1, m_1')$ in $(j_{13}, m_1, m_3) \rightsquigarrow_{\mathtt{injp}} (j_{13}', m_1', m_3')$.

(6) Given $j_{12}'(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \wedge (b_2, o_2) \in \mathtt{perm}_k(m_2', p)$. Similarly we prove $(b_1, o_1) \in \mathtt{perm}_k(m_1', p)$ or $(b_1, o_1) \notin \mathtt{perm}_{\mathsf{max}}(m_1', \mathsf{NA})$ by cases of $j_{12}(b_1)$:
- If $j_{12}(b_1) = \emptyset$, then b_1 and b_2 are new blocks by $\mathtt{inject\text{-}sep}(j_{12}, j_{12}', m_1, m_2)$. According to the construction steps , every nonempty permission of (b_2, o_2) in m_2' is copied from (b_1, o_1) in m_1'. Therefore $(b_1, o_1) \in \mathtt{perm}_k(m_1', p)$.
- If $j_{12}(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor$, then b_1 and b_2 are old blocks. We further divide $j_{23}(b_2)$ into two cases:
  - $j_{23}(b_2) = \emptyset$. In this case we have $(b_1, o_1) \in \mathtt{unchanged\text{-}on}(m_1, m_1')$ and $(b_2, o_2) \in \mathtt{unchanged\text{-}on}(m_2, m_2')$ (same as (1)). We can derive $(b_2, o_2) \in \mathtt{perm}_k(m_2, p)$, then $(b_1, o_1) \in \mathtt{perm}_k(m_1, p) \vee (b_1, o_1) \notin \mathtt{perm}_{\mathsf{max}}(m_1, \mathsf{NA})$ by property (6) of $m_1 \hookrightarrow_m^{j_{12}} m_2$. Finally $(b_1, o_1) \in \mathtt{perm}_k(m_1', p) \vee (b_1, o_1) \notin \mathtt{perm}_{\mathsf{max}}(m_1', \mathsf{NA})$ by $(b_1, o_1) \in \mathtt{unchanged\text{-}on}(m_1, m_1')$.
  - $j_{23}(b_2) = \lfloor(b_3, o_3)\rfloor$. We assume that $(b_1, o_1) \in \mathtt{perm}_{\mathsf{max}}(m_1', \mathsf{NA})$(other-wise the conclusion holds trivially), by $\mathtt{max\text{-}perm\text{-}dec}(m_1, m_1')$ we can derive that $(b_1, o_1) \in \mathtt{perm}_{\mathsf{max}}(m_1, \mathsf{NA})$. Therefore $(b_2, o_2) \in \mathtt{pub\text{-}tgt\text{-}mem}(j_{12}, m_1) \cap \mathtt{pub\text{-}src\text{-}mem}(j_{23})$ is copied from m_1' in step (3). As a result, we get $(b_1, o_1) \in \mathtt{perm}_k(m_1', p)$ from $(b_2, o_2) \in \mathtt{perm}_k(m_2', p)$.

□

Lemma A.14. $m_2' \hookrightarrow_m^{j_{23}'} m_3'$

Proof.

(1) Given $j_{23}'(b_2) = \lfloor(b_3, o_3 - o_2)\rfloor \wedge (b_2, o_2) \in \mathtt{perm}_k(m_2', p)$. We prove $(b_3, o_3) \in \mathtt{perm}_k(m_3', p)$ by cases of whether $b_2 \in m_2$.
- If $b_2 \notin m_2$ is a new block relative to m_2, then $(b_2, o_2) \in \mathtt{perm}_k(m_2', p)$ is copied from m_1' in step (2). Therefore we get $(b_1, o_1) \in \mathtt{perm}_k(m_1', p)$ and $j_{23}' \cdot j_{12}'(b_1) = \lfloor(b_3, o_3 - o_1)\rfloor$ according to step (1). From property (1) of $m_1' \hookrightarrow_m^{j_{13}'} m_3'$ we get $(b_3, o_3) \in \mathtt{perm}_k(m_3', p)$;
- If $b_2 \in m_2$, then $j_{23}(b_2) = \lfloor(b_3, o_3)\rfloor$ from $\mathtt{inject\text{-}sep}(j_{23}, j_{23}', m_2, m_3)$. We further divide whether $(b_2, o_2) \in \mathtt{out\text{-}of\text{-}reach}(j_{12}, m_1)$ using the same algorithm in step (2).
  - If $(b_2, o_2) \in \mathtt{out\text{-}of\text{-}reach}(j_{12}, m_1)$. According to Lemma A.9, we can derive $(b_2, o_2) \in \mathtt{unchanged\text{-}on}(m_2, m_2')$ and $(b_2, o_2) \in \mathtt{perm}_k(m_2, p)$. From $m_2 \hookrightarrow_m^{j_{23}} m_3$ we can derive $(b_3, o_3) \in \mathtt{perm}_k(m_3, p)$. By Lemma A.6, $(b_3, o_3) \in \mathtt{out\text{-}of\text{-}reach}(j_{13}, m_1)$. Therefore $(b_3, o_3) \in \mathtt{unchanged\text{-}on}(m_3, m_3')$ and $(b_3, o_3) \in \mathtt{perm}_k(m_3', p)$.
  - If $(b_2, o_2) \notin \mathtt{out\text{-}of\text{-}reach}(j_{12}, m_1)$, the permission of public position (b_2, o_2) in m_2' is copied from m_1' in step (3). Thus $(b_1, o_1) \in \mathtt{perm}_k(m_1', p)$ and $j_{13}'(b_1) = \lfloor(b_3, o_3 - o_1)\rfloor$. From property (1) of $m_1' \hookrightarrow_m^{j_{13}'} m_3'$ we get $(b_3, o_3) \in \mathtt{perm}_k(m_3', p)$.

(2) The proof is similar to (1). Lemma A.5 ensures that the constructed value v_2 in m_2' can be related to the value in m_3' as $v_2 \hookrightarrow_v^{j_{23}'} m_3'[b_3, o_3]$. Note that if (b_2, o_2) is read-only in m_2, the property (1) of $m_2 \hookrightarrow_m^{j_{23}} m_3$ provides that mapped position (b_3, o_3) is also read-only in m_3.

(3) Given $b_2 \notin m_2'$, we have $b_2 \notin m_2$ and $j_{23}(b_2) = \emptyset$. Also b_2 is not added into the domain of j_{23}' in step (1), so $j_{23}'(b_2) = \emptyset$.

(4) Given $j_{23}'(b_2) = \lfloor(b_3, o_3)\rfloor$. Similarly b_3 is either an old block in $m_3(j_{23}(b_2) = \lfloor(b_3, o_3)\rfloor)$ or a new block in $m_3'(j_{23}(b_2) = \emptyset)$. Therefore $b_3 \in m_3'$.

(5) Given $j_{23}'(b_2) = \lfloor(b_3, o_3 - o_2)\rfloor \wedge (b_2, o_2) \in \mathtt{perm}_{\mathsf{max}}(m_2', \mathsf{NA})$ and $j_{23}'(b_2') = \lfloor(b_3', o_3' - o_2')\rfloor \wedge (b_2', o_2') \in \mathtt{perm}_{\mathsf{max}}(m_2', \mathsf{NA})$ where $b_2 \neq b_2'$. We need to prove that $(b_3, o_3) \neq (b_3', o_3')$ by cases

of whether b_2 and b_2' are mapped by old injection j_{23}. Note that $j_{23} \subseteq j_{23}'$, so $j_{23}(b)$ is either $\emptyset$ or the same as $j_{23}'(b)$.

- $j_{23}(b_2) = j_{23}(b_2') = \emptyset$. The j_{23}' mappings of them are added in step (1). It is obvious that newly added mappings in j_{23}' never map different blocks in m_2' into the same block in m_3'. Therefore $b_3 \neq b_3'$.
- $j_{23}(b_2) = \lfloor(b_3, o_3 - o_2)\rfloor, j_{23}(b_2') = \emptyset$. we can derive that $b_3 \in m_3$ By property (4) of $m_2 \hookrightarrow_m^{j_{23}} m_3$. While $b_3' \notin m_3$ can be derived from $\texttt{inject-sep}(j_{23}, j_{23}', m_2, m_3)$. Therefore $b_3 \neq b_3'$.
- $j_{23}(b_2) = \emptyset, j_{23}(b_2') = \lfloor(b_3', o_3' - o_3')\rfloor$. Similarly we have $b_3 \neq b_3'$.
- $j_{23}(b_2) = \lfloor(b_3, o_3 - o_2)\rfloor, j_{23}(b_2') = \lfloor(b_3', o_3' - o_2')\rfloor$. We can prove $(b_3, o_3) \neq (b_3, o_3')$ using the property (5) in $m_2 \hookrightarrow_m^{j_{23}} m_3$ by showing $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$ and $(b_2', o_2') \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$. This follows from $\texttt{max-perm-dec}(m_2, m_2')$ (Lemma A.10).

(6) Given $j_{23}'(b_2) = \lfloor(b_3, o_3 - o_2)\rfloor \wedge (b_3, o_3) \in \texttt{perm}_k(m_3', p)$. Similarly we prove $(b_2, o_2) \in \texttt{perm}_k(m_2', p)$ or $(b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2', \texttt{NA})$ by cases of $j_{23}(b_2)$:

- If $j_{23}(b_2) = \emptyset$, then b_2 and b_3 are new blocks by $\texttt{inject-sep}(j_{23}, j_{23}', m_2, m_3)$. According to step (1), we know that $\exists b_1\ o_1, j_{13}'(b_1) = \lfloor(b_3, o_3 - o_1)\rfloor$. At the same time, we also know that the permission of (b_2, o_2) in new block of m_2' is copied from (b_1, o_1) in m_1'. Now from property (6) of $m_1' \hookrightarrow_m^{j_{13}'} m_3'$ we can derive that $(b_1, o_1) \in \texttt{perm}_k(m_1', p) \vee (b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1', \texttt{NA})$, therefore $(b_2, o_2) \in \texttt{perm}_k(m_2', p) \vee (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2', \texttt{NA})$.
- If $j_{23}(b_2) = \lfloor(b_3, o_3 - o_2)\rfloor$, then b_2 and b_3 are old blocks. We further divide b_2 into two cases:
  - If $(b_2, o_2) \in \texttt{out-of-reach}(j_{12}, m_1)$, we have $(b_2, o_2) \in \texttt{unchanged-on}(m_2, m_2')$ (Lemma A.9). If $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2', \texttt{NA})$(otherwise the conclusion holds trivially), then $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$ holds ($\texttt{max-perm-dec}(m_2, m_2')$). According to Lemma A.6, we get $(b_3, o_3) \in \texttt{unchanged-on}(m_3, m_3')$ and $(b_3, o_3) \in \texttt{perm}_k(m_3, p)$. Then we can derive that $(b_2, o_2) \in \texttt{perm}_k(m_2, p) \vee (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$ by property (6) of $m_2 \hookrightarrow_m^{j_{23}} m_3$. Finally we can prove that
  $$(b_2, o_2) \in \texttt{perm}_k(m_2', p) \vee (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2', \texttt{NA}).$$
  - If $(b_2, o_2) \notin \texttt{out-of-reach}(j_{12}, m_1)$, we know that $\exists b_1, j_{13}'(b_1) = \lfloor b_3, o_3 - o_1\rfloor$. From $m_1' \hookrightarrow_m^{j_{13}'} m_3'$ we can derive that $(b_1, o_1) \in \texttt{perm}_k(m_1', p) \vee (b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1', p)$. Meanwhile, the permission of $(b_2, o_2) \in \texttt{pub-tgt-mem}(j_{12}, m_1) \cap \texttt{pub-src-mem}(j_{23})$ is copied from m_1' in step (3). Therefore
  $$(b_2, o_2) \in \texttt{perm}_k(m_2', p) \vee (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2', \texttt{NA})$$

□

Lemma A.15. $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j_{12}', m_1', m_2')$

Proof. According to Definition A.3, most of the properties of $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j_{12}', m_1', m_2')$ have been proved in Lemma A.8, Lemma A.9 and Lemma A.12. From $(j_{13}, m_1, m_3) \rightsquigarrow_{\texttt{injp}} (j_{13}', m_1', m_3')$ we can get $\texttt{mem-acc}(m_1, m_1')$ and $\texttt{unmapped}(j_{13}) \subseteq \texttt{unchanged-on}(m_1, m_1')$. To get the last leaving property $\texttt{unmapped}(j_{12}) \subseteq \texttt{unchanged-on}(m_1, m_1')$ we only need to show

$$\texttt{unmapped}(j_{12}) \subseteq \texttt{unmapped}(j_{13})$$

where $j_{13} = j_{23} \cdot j_{12}$. This relations holds simply because of $\forall b, j_{12}(b) = \emptyset \Rightarrow j_{23} \cdot j_{12}(b) = \emptyset$. In other word, more regions in m_1 is protected in $(j_{13}, m_1, m_3) \rightsquigarrow_{\texttt{injp}} (j_{13}', m_1', m_3')$ than in $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j_{12}', m_1', m_2')$. □

Lemma A.16. $(j_{23}, m_2, m_3) \rightsquigarrow_{\texttt{injp}} (j'_{23}, m'_2, m'_3)$

Proof. Similarly, we only need to show

$$\texttt{out-of-reach}(j_{23}, m_2) \subseteq \texttt{out-of-reach}(j_{23} \cdot j_{12}, m_1)$$

Given $(b_3, o_3) \in \texttt{out-of-reach}(j_{23}, m_2)$, i.e.

$$\forall b_2\ o_2, j_{23}(b_2) = \lfloor (b_3, o_3) \rfloor \Rightarrow (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$$

We need to prove $(b_3, o_3) \in \texttt{out-of-reach}(j_{23} \cdot j_{12}, m_1)$. as follows. If $j_{23} \cdot j_{12}(b_1) = \lfloor (b_3, o_3) \rfloor$,i.e. $\exists b_2, j_{12}(b_1) = \lfloor (b_2, o_2) \rfloor \wedge j_{23}(b_2) = \lfloor (b_3, o_3) \rfloor$, we can derive that $(b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2, \texttt{NA})$. By property (1) of $m_1 \hookrightarrow_m^{j_{12}} m_2$, we can get $(b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1, \texttt{NA})$. Therefore $(b_3, o_3) \in \texttt{out-of-reach}(j_{23} \cdot j_{12}, m_1)$. □

Since we have proved all 4 required properties (Lemma A.13 to Lemma A.16) of the constructed memory state m'_2, Lemma 4.3 is proved.

A.4 Proof of Lemma 4.4

We prove Lemma 4.4 in this section:

$$\begin{aligned}
&\forall j_{13}\ m_1\ m_3,\ m_1 \hookrightarrow_m^{j_{13}} m_3 \Rightarrow \exists j_{12}\ j_{23}\ m_2,\ m_1 \hookrightarrow_m^{j_{12}} m_2 \wedge m_2 \hookrightarrow_m^{j_{23}} m_3 \wedge \\
&\quad \forall m'_1\ m'_2\ m'_3\ j'_{12}\ j'_{23},\ (j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j'_{12}, m'_1, m'_2) \Rightarrow (j_{23}, m_2, m_3) \rightsquigarrow_{\texttt{injp}} (j'_{23}, m'_2, m'_3) \Rightarrow \\
&\qquad m'_1 \hookrightarrow_m^{j'_{12}} m'_2 \Rightarrow m'_2 \hookrightarrow_m^{j'_{23}} m'_3 \Rightarrow \exists j_{13'},\ (j_{13}, m_1, m_3) \rightsquigarrow_{\texttt{injp}} (j'_{13}, m'_1, m'_3) \wedge m'_1 \hookrightarrow_m^{j'_{13}} m'_3.
\end{aligned}$$

Proof. Given $m_1 \hookrightarrow_m^{j_{13}} m_3$, take $j_{12} = \{(b, (b, 0)) | j_{13}(b) \neq \emptyset\}$, $j_{23} = j_{13}$ and $m_2 = m_1$. As a result, $m_2 \hookrightarrow_m^{j_{23}} m_3$ holds trivially. We show $m_1 \hookrightarrow_m^{j_{12}} m_1$ as follows:

(1) Given $j_{12}(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor \wedge (b_1, o_1) \in \texttt{perm}_k(m_1, p)$, according to the definition of j_{12} we know that $b_2 = b_1$ and $o_2 = o_1$. Therefore $(b_2, o_2) \in \texttt{perm}_k(m_1, p)$.

(2) Given $j_{12}(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor \wedge (b_1, o_1) \in \texttt{perm}_{\texttt{cur}}(m_1, p)$, similar to (1) we know $b_2 = b_1$ and $o_2 = o_1$. Therefore $m_1[b_1, o_1] = m_1[b_2, o_2]$. If $m_1[b_1, o_1]$ is not in the form of $\texttt{Vptr}(b'_1, o'_1)$, $m_1[b_1, o_1] \hookrightarrow_v^{j_{12}} m_1[b_2, o_2]$ holds trivially.
If $m_1[b_1, o_1] = \texttt{Vptr}(b'_1, o'_1)$, from $j_{12}(b_1) = \lfloor (b_1, 0) \rfloor$ we get $j_{13}(b_1) \neq \emptyset$. According to property (2) of $m_1 \hookrightarrow_m^{j_{13}} m_3$, $\exists v_3, \texttt{Vptr}(b'_1, o'_1) \hookrightarrow_m^{j_{13}} v_3$. Which means that $j_{12}(b'_1) = \lfloor (b'_1, 0) \rfloor$, therefore $\texttt{Vptr}(b'_1, o'_1) \hookrightarrow_v^{j_{12}} \texttt{Vptr}(b'_1, o'_1)$.

(3) Given $b_1 \notin m_1$, we can derive that $j_{13}(b_1) = \emptyset$ by $m_1 \hookrightarrow_m^{j_{13}} m_3$. Therefore $j_{12}(b_1) = \emptyset$ holds by definition.

(4) Given $j_{12}(b_1) = \lfloor (b_2, \delta) \rfloor$, we know that $j_{13}(b_1) \neq \emptyset$. Therefore $b_1 \in m_1$ by $m_1 \hookrightarrow_m^{j_{13}} m_3$. Since $b_1 = b_2$, $b_2 \in m_1$.

(5) Given $b_1 \neq b'_1$, $j_{12}(b_1) = \lfloor b_2, o_2 - o_1 \rfloor$ and $j_{12}(b'_1) = \lfloor b'_2, o'_2 - o'_1 \rfloor$. It is straightforward that $b_2 = b_1$, $b'_2 = b'_1$ therefore $b_2 \neq b'_2$.

(6) Given $j_{12}(b_1) = \lfloor b_2, o_2 - o_1 \rfloor$ and $(b_2, o_2) \in \texttt{perm}_k(m_1, p)$. Similarly we have $b_2 = b_1$, $o_2 = o_1$ and $(b_1, o_1) \in \texttt{perm}_k(m_1, p)$.

After external calls, given preconditions $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j'_{12}, m'_1, m'_2)$, $(j_{23}, m_2, m_3) \rightsquigarrow_{\texttt{injp}} (j'_{23}, m'_2, m'_3)$, $m'_1 \hookrightarrow_m^{j'_{12}} m'_2$ and $m'_2 \hookrightarrow_m^{j'_{23}} m'_3$. We can get $m'_1 \hookrightarrow_m^{j'_{13}} m'_3$ directly by Lemma A.4. For $(j_{13}, m_1, m_3) \rightsquigarrow_{\texttt{injp}} (j'_{13}, m'_1, m'_3)$,

(1) We can easily show $j_{13} = j_{23} \cdot j_{12}$ by the definition of j_{12}. Since $j_{12} \subseteq j_{12'}$, $j_{23} \subseteq j'_{23}$, we can conclude that $j_{23} \cdot j_{12} \subseteq j'_{23} \cdot j'_{12}$, i.e. $j_{13} \subseteq j'_{13}$.

(2)

$$\texttt{unmapped}(j_{13}) \subseteq \texttt{unchanged-on}(m_1, m'_1)$$

By definition of j_{12}, we have $\texttt{unmapped}(j_{12}) = \texttt{unmapped}(j_{13})$. Therefore the result comes directly from $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j'_{12}, m'_1, m'_2)$.

(3)
$$\texttt{out-of-reach}(j_{13}, m_1) \subseteq \texttt{unchanged-on}(m_3, m'_3)$$
Since $j_{23} = j_{13}$ and $m_2 = m_1$, the result comes directly from $(j_{23}, m_2, m_3) \rightsquigarrow_{\texttt{injp}} (j'_{23}, m'_2, m'_3)$.

(4) $\texttt{mem-acc}(m_1, m'_1)$ comes from $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j'_{12}, m'_1, m'_2)$.

(5) $\texttt{mem-acc}(m_3, m'_3)$ comes from $(j_{23}, m_2, m_3) \rightsquigarrow_{\texttt{injp}} (j'_{23}, m'_2, m'_3)$.

(6)
$$\texttt{inject-sep}(j_{13}, j'_{13}, m_1, m_3)$$
If $j_{13}(b_1) = \emptyset$ and $j'_{13}(b_1) = \lfloor (b_3, o_3 - o_1) \rfloor$, we get
$$j_{12}(b_1) = \emptyset \text{ and } \exists b_2, j'_{12}(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor \land j'_{23}(b_2) = \lfloor (b_3, o_3 - o_2) \rfloor$$
by $\texttt{inject-sep}(j_{12}, j'_{12}, m_1, m_2)$ we get $b_1 \notin m_1$ and $b_2 \notin m_2$. By property (3) of $m_2 \hookrightarrow_m^{j_{23}} m_3$ we can derive that $j_{23}(b_2) = \emptyset$. Finally we get $b_3 \notin m_3$ by $\texttt{inject-sep}(j_{23}, j'_{23}, m_2, m_3)$.

□

B VERIFICATION OF THE ENCRYPTION SERVER AND CLIENT EXAMPLE

B.1 Refinement of the Hand-written Server

The following is the proof for Theorem 6.2.

Proof. At the top level, $\mathbb{C}$ is expanded to $\texttt{ro} \cdot \texttt{wt} \cdot \texttt{CAinjp} \cdot \texttt{asm}_{\texttt{injp}}$. As the invariant ro and wt in C level are commutative, i.e., $\texttt{ro} \cdot \texttt{wt} \equiv \texttt{wt} \cdot \texttt{ro}$ as stated in Lemma 5.7, we can change their order in $\mathbb{C}$. By the vertical compositionality, we first prove $L_S \leqslant_{\texttt{wt}} L_S$ and $[\![\texttt{server\_opt.s}]\!] \leqslant_{\texttt{asm}_{\texttt{injp}}} [\![\texttt{server\_opt.s}]\!]$, which are both self simulation and straightforward (the latter one is provided by the adequacy theorem). Since the relation between source and target programs involves an optimization of constant propagation of the variable key, we need to use ro together with CAinjp to establish the simulation $L_S \leqslant_{\texttt{ro}\cdot\texttt{CAinjp}} [\![\texttt{server\_opt.s}]\!]$. Note that for the unoptimized version we can prove $L_S \leqslant_{\texttt{CAinjp}} [\![\texttt{server.s}]\!]$ and prove ro using self simulation like wt.

The key of this proof is to establish a relation $R \in \mathcal{K}_{W_{\texttt{ro}\cdot\texttt{CAinjp}}}(S_S, \texttt{regset} \times \texttt{mem})$ satisfying the simulation diagram Fig. 20. Given $w \in W_{\texttt{ro}} \times W_{\texttt{CAinjp}} = ((se, m_0), ((j, m, tm), sg, rs))$, if $sg \neq \texttt{int} \to \texttt{ptr} \to \texttt{void} \lor m_0 \neq m$ then $R(w) = \emptyset$. Assume $sg = \texttt{int} \to \texttt{ptr} \to \texttt{void} \land m_0 = m$ (these conditions are provided by I of L_S and related incoming queries), then $R(w)$ is defined as follows:

(a)	$(\texttt{Calle}\ i\ \texttt{Vptr}(b, o)\ m, (rs, tm)) \in R(w) \Leftrightarrow$ (* initial state *)
(a.1)	$\quad rs(\texttt{RDI}) = i \land \texttt{Vptr}(b, 0) \hookrightarrow_v^j rs(\texttt{RSI}) \land rs(\texttt{PC}) = \texttt{Vptr}(b_e, 0) \land m \hookrightarrow_m^j tm \land \texttt{ro-valid}(se, m)$
(b)	$(\texttt{Callp}\ sp\ \texttt{Vptr}(b, o)\ m_1, (rs_1, tm_1)) \in R(w) \Leftrightarrow$ (* before external call *)
(b.1)	$\quad rs_1(\texttt{RSP}) = \texttt{Vptr}(b_s, 0) \land rs_1(\texttt{RDI}) = \texttt{Vptr}(b_s, 8) \land j'\ sp = \lfloor b_s, 8 \rfloor$
(b.2)	$\quad \land rs_1(\texttt{RA}) = \texttt{Vptr}(b_g, 5) \land m_1 \hookrightarrow_m^{j'} tm_1 \land \texttt{Vptr}(b, o) \hookrightarrow_v^j rs_1(\texttt{PC})$
(b.3)	$\quad \land \forall r, r \in \texttt{callee-save-regs} \to rs_1(r) = rs(r)$
(b.4)	$\quad \land (j, m, tm) \rightsquigarrow_{\texttt{injp}} (j', m_1, tm_1) \land \texttt{ro-valid}(se, m_1)$
(b.5)	$\quad \land tm_1[b_s, 0] = rs(\texttt{RSP}) \land tm_1[b_s, 16] = rs(\texttt{RA})$
(b.6)	$\quad \land \{(b_s, o) \mid 0 \le o < 8 \lor 16 \le o < 24\} \subseteq \texttt{out-of-reach}(j', m_1)$
(b.7)	$\quad \land \{(b_s, o) \mid 0 \le o < 8 \lor 16 \le o < 24\} \subseteq \texttt{perm}_{\texttt{cur}}(tm_1, \texttt{Freeable})$
(c)	$(\texttt{Retp}\ sp\ m_2, (rs_2, tm_2)) \in R(w) \Leftrightarrow$ (* after external call *)
(c.1)	$\quad rs_2(\texttt{RSP}) = \texttt{Vptr}(b_s, 0) \land j''\ sp = \lfloor b_s, 8 \rfloor$
(c.2)	$\quad rs_2(\texttt{PC}) = (b_g, 5) \land m_2 \hookrightarrow_m^{j''} tm_2$
(c.3)	$\quad \land \forall r, r \in \texttt{callee-save-regs} \to rs_2(r) = rs(r)$
(c.4)	$\quad \land (j, m, tm) \rightsquigarrow_{\texttt{injp}} (j'', m_2, tm_2)$
(c.5)	$\quad \land tm_2[b_s, 0] = rs(\texttt{RSP}) \land tm_2[b_s, 16] = rs(\texttt{RA})$

(c.6) $\wedge\{(b_s, o) \mid 0 \le o < 8 \vee 16 \le o < 24\} \subseteq \texttt{out-of-reach}(j'', m_2)$
(c.7) $\wedge\{(b_s, o) \mid 0 \le o < 8 \vee 16 \le o < 24\} \subseteq \texttt{perm}_{\texttt{cur}}(tm_2, \texttt{Freeable})$
(d) $(\texttt{Rete}\ m_3, (rs_3, tm_3)) \in R(w) \Leftrightarrow$ `(* final state *)`
(d.1) $rs_3(\texttt{RSP}) = rs(\texttt{RSP}) \wedge rs_3(\texttt{PC}) = rs(\texttt{RA}) \wedge m_3 \hookrightarrow_m^{j''} tm_3$
(d.2) $\wedge \forall r, r \in \texttt{callee-save-regs} \to rs_3(r) = rs(r)$
(d.3) $\wedge (j, m, tm) \rightsquigarrow_{\texttt{injp}} (j'', m_3, tm_3)$

By definition the relation between internal states of L_S and assembly states evolve in four stages:

(a) Right after the initial call to `encrypt`, (a.1) indicates that the argument i and function pointer are stored in RDI and RSI, the program counter is at $(b_e, 0)$ (pointing to the first assembly instruction of `server_opt.s` in Fig. 3c). The $\texttt{ro-valid}(se, m)$ comes from $\mathbb{R}^q_{\texttt{ro}}$ and ensures that value of `key` in m_1 is 42.
(b) Right before the external call, (b.1) indicates that the argument is stored in RDI, which is a pointer $\texttt{Vptr}(b_s, 8)$. Here b_s is the stack block of the target assembly and sp is injected to $\texttt{Vptr}(b_s, 8)$ as depicted in Fig. 7. (b.2) indicates that the return address is set to the 5th assembly instruction in Fig. 3c (right after `Pcall RSI`) and the function pointer of p $\texttt{Vptr}(b_p, 0)$ is related to PC by j. (b.3) indicates that callee-save registers are not modified since the initial call. (b.4) maintains the `injp` accessibility and `ro-valid` for external call. (b.5), (b.6) and (b.7) indicate that the stored values (return address and previous stack block) on the stack are frame unchanged, protected and freeable.
(c) Right after the external call, we keep the necessary conditions from (b), except that the program counter PC now points to the value in RA before the external call. Note that the injection function is updated to j'' by the external call.
(d) Right before returning from `encrypt`, (d.1) indicates that the stack pointer is restored and the return address is set. (d.2) indicates all callee-save registers are restored and (d.3) indicates that guarantee condition `injp` is met.

To prove R is indeed an invariant to establish the simulation, we follow the diagram in Fig. 20. The most important points of the above proof is that `ro` and `injp` play essential roles in establishing the invariant (relevant conditions are displayed in red and blue in the invariant, respectively). Initially, the target semantics enters the function from $rs(\texttt{PC})$ which is related to the function pointer in q^I_C as mentioned in $\mathbb{R}^q_{\texttt{injp}}$. The condition (a) follows from $\mathbb{R}^q_{\texttt{injp}}$ and $\mathbb{R}^q_{\texttt{ro}}$ and hence holds at the initial states. Right before the execution calls, (b) holds by execution of the instructions from `Pallocframe` to `Pcall`. Note that $\texttt{ro-valid}(se, m)$ obtained from `ro` in (b.5) is essential for proving that the value of *key* read from m is 42, thus matches the constant in `server_opt.s`. Then, we need to show (c) holds after the source and target execution perform the external call and returns. This is the most interesting part where the memory protection provided by `injp` is essential. It is achieved by combining properties (b.1–7) with the rely-condition provided by `CAinjp` of the external call. For example, because we know the protected regions of the stack frame b_s is out-of-reach before the call, by the protection enforced by `injp` in $\mathbb{R}^r_{\texttt{CAinjp}}$, all values in $tm_1[b_s, o]$ $s.t.$ $0 \le o < 8 \vee 16 \le o < 24$ are unchanged, therefore if $tm_1[b_s, 0] = rs(\texttt{RSP})$ and $tm_1[b_s, 16] = rs(\texttt{RA})$ (condition (b.5)) holds before the call, they also hold after it (condition (c.5) holds). Besides using `injp`, we can derive (c.3) from (b.3) by the protection over callee-save registers enforced in $\mathbb{R}^r_{\texttt{CAinjp}}$. $rs_2(\texttt{PC}) = (b_g, 5)$ in (c.2) is derived from $rs_1(\texttt{RA}) = (b_g, 5)$ in (b.2) via the relation between PC and RA stated in $\mathbb{R}^r_{\texttt{CAinjp}}$. After the external call, condition (d) can be derived from (c) by following internal execution. Since L_S frees sp, $[\![\texttt{server\_opt.s}]\!]$ can free the corresponding region $(b_s, 8)$ to $(b_s, 16)$. The remaining part are also freeable by condition (c.7). Finally, the target semantics returns after executing `Pret` and condition (d) provides the updated `injp` world (j'', m_3, tm_3) with the accessibility from the initial world w

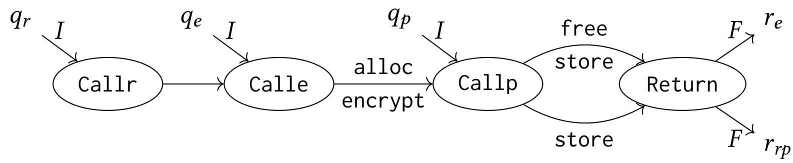


Fig. 22. The Top-level Specification $L_{\texttt{CS}}$

and other properties needed by $\mathbb{R}^r_{\texttt{CAinjp}}$. The `injp` accessibility also implies $\texttt{mem-acc}(m, m_3)$ for $\mathbb{R}^r_{\texttt{ro}}$. Therefore, we are able to establish the guarantee condition and prove that $L_{\texttt{S}} \leqslant_{\mathbb{C}} [[\texttt{server\_opt.s}]]$. □

B.2 End-to-end Correctness Theorem

The top-level specification $L_{\texttt{CS}}$ is defined as follows:

Definition B.1. LTS of $L_{\texttt{CS}}$:

$$
\begin{aligned}
S_T\ &:= \{\texttt{Callr}\ i\ m\} \cup \{\texttt{Calle}\ \mathit{flag}\ i\ v\ m\} \cup \{\texttt{Callp}\ \mathit{flag}\ \mathit{retv}\ \mathit{sp}\ m\} \cup \{\texttt{Return}\ \mathit{retv}\ m\};\\
I_T\ &:= \{(\texttt{Vptr}(b_r, 0)[\texttt{int} \to \texttt{int}]([i])@m, \texttt{Callr}\ i\ m)\} \cup\\
&\quad\ \{(\texttt{Vptr}(b_e, 0)[\texttt{int} \to \texttt{ptr} \to \texttt{void}]([i, v_c])@m, \texttt{Calle}\ \mathit{false}\ i\ v_c\ m)\} \cup\\
&\quad\ \{(\texttt{Vptr}(b_p, 0)[\texttt{ptr} \to \texttt{void}]([\texttt{Vptr}(\mathit{sp}, 0)])@m, \texttt{Callp}\ \mathit{false}\ \mathit{None}\ \mathit{sp}\ m)\};\\
\to_T &:= \{(\texttt{Callr}\ i\ m, \texttt{Calle}\ \mathit{true}\ i\ \texttt{Vptr}(b_p, 0)\ m)\} \cup\\
&\quad\ \{(\texttt{Calle}\ \mathit{flag}\ i\ \texttt{Vptr}(b_p, 0)\ m, \texttt{Callp}\ \mathit{true}\ \mathit{retv}\ \mathit{sp}\ m') \mid\\
&\quad\ m' = m[\mathit{sp} \leftarrow (i\ \texttt{xor}\ m[b_k])], \mathit{retv} = \mathit{flag}?\mathit{Some}(i) : \mathit{None}\} \cup\\
&\quad\ \{(\texttt{Callp}\ \mathit{true}\ \mathit{retv}\ \mathit{sp}\ m, \texttt{Return}\ \mathit{retv}\ m') \mid m' = m[\mathit{result} \leftarrow m[\mathit{sp}]], m'' = \mathit{free}\ m\ \mathit{sp}\} \cup\\
&\quad\ \{(\texttt{Callp}\ \mathit{false}\ \mathit{retv}\ \mathit{sp}\ m, \texttt{Return}\ \mathit{retv}\ m') \mid m' = m[\mathit{result} \leftarrow m[\mathit{sp}]]\};\\
F_T\ &:= \{(\texttt{Return}\ \mathit{Some}(i)\ m, i@m)\} \cup\\
&\quad\ \{(\texttt{Return}\ \mathit{None}\ m, \texttt{Vundef}@m)\};
\end{aligned}
$$

There are four internal states in $L_{\texttt{CS}}$ as depicted in its transition diagram Fig. 22, among which three states correspond to the three functions (`request`, `process` and `encrypt`). We use *flag* in `Calle` (`Callp`) to indicate whether it is called internally by `request` (`encrypt`) or called by the environment. The *retv* is the return value which is either an integer when $L_{\texttt{CS}}$ is invoked by `request` or empty by other functions. I_T contains three possible initial states corresponding to calling the three entry functions. $\to_T$ describes the big steps starting from each call states to another call state (e.g., `Callr` to `Calle`) or the return state. If the stack block *sp* is allocated by `encrypt`, it should be freed in the `Return` state. There are two final states in F_T: r_e returning from `request` with an integer as the return value and r_{rp} returning from `request` or `process` with no return value. Note that $L_{\texttt{CS}}$ can only be called but cannot perform external calls.

The remaining proof follows §6. We have shown how end-to-end refinement is derived using the optimized server. For unoptimized server, the proof is almost the same. The only difference is that the symbol table accompanying $L_{\texttt{S}}$ does not mark `key` as read-only, and the simulation invariant for Theorem 6.2 does not contain `ro-valid` conditions as they play no role without optimizations.

B.3 Verification of Mutually Recursive Client and Server

We introduce an variant of the running example with mutual recursions in Fig. 23. The server remains the same while `client.c` is modified so that its function `request` is also the callback function and a sequence of encrypted values are stored in a global array.

To perform the same end-to-end verification for this example, we only need to define a new top-level specification $L_{\texttt{CS}}'$ to capture the semantics of the multi-step encryption and prove

```
/* client.c */
#define N 10
int input[N]={...};
int result[N];
int i;

void encrypt(int i,
      void(*p)(int*));
```

```
void request(int*r){
  if(i == 0)
    encrypt(input[i++],request);
  else if(0 < i && i < N){
    result[i-1]=*r;
    encrypt(input[i++],request); }
  else result[i-1]=*r;
  return; }
```

Fig. 23. Client with Multiple Encryption Request

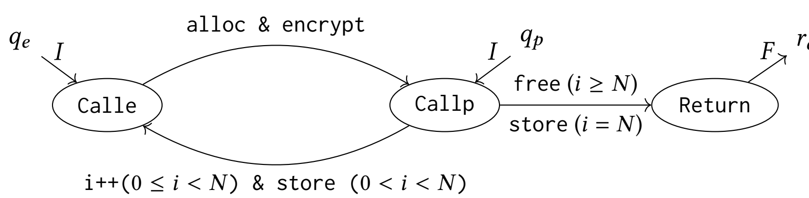


Fig. 24. The Top-level Specification $L_{\mathsf{CS}}{}'$ of Mutually Recursive Client and Server

$L_{\mathsf{CS}}{}' \leqslant_{\mathtt{ro}\cdot\mathtt{wt}\cdot\mathtt{c}_{\mathtt{injp}}} [[\mathtt{client}]] \oplus L_{\mathsf{S}}$. Other proofs are either unchanged (e.g., the refinement of server) or can be derived from the verified compiler and the horizontal compositionality. In the following paragraphs, we briefly talk about this new top-level specification and the updated proofs.

Definition B.2. The LTS of $L_{\mathsf{CS}}{}'$:

$$
\begin{aligned}
S_T \;&:= \{\mathtt{Callr}\ sp\ sps\ m\} \cup \{\mathtt{Calle}\ i\ sps\ v\ m\} \cup \{\mathtt{Return}\ m\};\\
I_T \;&:= \{(\mathtt{Vptr}(b_r,0)[\mathtt{ptr} \to \mathtt{void}]([\mathtt{Vptr}(sp,0)])@m, \mathtt{Callr}\ sp\ nil\ m)\} \cup\\
&\quad\ \{(\mathtt{Vptr}(b_e,0)[\mathtt{int} \to \mathtt{ptr} \to \mathtt{void}]([i, v_c])@m, \mathtt{Calle}\ i\ nil\ v_c\ m)\} \cup\\
\to_T \;&:= \{(\mathtt{Callr}\ sp\ sps\ m, \mathtt{Calle}\ i\ sps\ \mathtt{Vptr}(b_p,0)\ m') \mid m[b_i] == 0, \ldots\} \cup\\
&\quad\ \{(\mathtt{Callr}\ sp\ sps\ m, \mathtt{Calle}\ i\ sps\ \mathtt{Vptr}(b_p,0)\ m') \mid 0 < m[b_i] < N, \ldots\} \cup\\
&\quad\ \{(\mathtt{Callr}\ sp\ sps\ m, \mathtt{Return}\ m') \mid m[b_i] \geq N, \ldots\} \cup\\
&\quad\ \{(\mathtt{Calle}\ i\ sps\ \mathtt{Vptr}(b_p,0)\ m, \mathtt{Callr}\ sp\ (sp :: sps)\ m') \mid m'[sp \leftarrow i\ xor\ m[b_k]]\};\\
F_T \;&:= \{(\mathtt{Return}\ m, \mathtt{Vundef}@m)\};
\end{aligned}
$$

As we remove the function `process`, the new L_{CS} has only two call states and one return state as depicted in Fig. 24. `sps` in `Callr` and `Calle` is a list of blocks, each of which stores an encrypted result. We record these blocks in the program states because we need to de-allocate them before returning. As described in $\to_T$, there are three internal transitions for `Callr`, corresponding to three conditional branches in the source code. The transitions from `Callr` to `Calle` perform different memory operations depending on the value of `i` according to the code presented in Fig. 23. The transition from `Callr` to `Return` will de-allocate all the stack blocks in `sps`. The transition from `Calle` to `Callr` allocate a new block `sp` to store the encrypted result and add it to `sps`.

Given this new top-level specification, we need to prove Theorem 6.2 where the L_{CS} is replaced by $L_{\mathsf{CS}}{}'$. The key of this proof is that the simulation invariant must relate the call stack in the target LTS (i.e., the semantics linking of `client.c` and L_{S}) and `sps`, because each element in `sps` is allocated by a call to`encrypt` and stores the result of encryption. The complete proofs can be found in our Coq development.

```
/* C implementation of M_C */
static int memoized[1000] = {0};
int f(int i) {
  int sum;
  if (i == 0) return 0;
  sum = memoized[i];
  if (sum == 0)
  { sum = g(i-1) + i;
    memoized[i] = sum; }
  return sum;
}
/* C code corresponding to M_A */
static int s[2] = {0,0};
int g(int i){
  int sum;
  if (i == 0) return 0;
  if (i == s[0])
    { sum = s[1]; }
  else
    { sum = f(i-1) + i;
      s[0] = i;
      s[1] = sum; }
  return sum;
}
```

```
/* Assembly implementation of M_A */
g:  Pallocframe 24 16 0
    Pmov RBX 8(RSP) // save RBX
    /* begin */
    Pmov RDI RBX
    Ptestl RBX RBX  // i==0
    Pjne l0
    Pxorl_r RAX     // rv=0
    Pjmp l1
l0: Pmov s[0] RAX
    Pcmpl RAX RBX  // i==s[0]
    Pje l2
    Pleal -1(RBX) RDI
    Pcall f        // f(i-1)
    Pleal (RAX,RBX) RAX//sum=f(i-1)+i
    Pmov RBX s[0]  // s[0] = i
    Pmov RAX s[1]  // s[1] = sum
    Pjmp l1
l2: Pmov s[1] RAX  // rv=s[1]
    /* return */
l1: Pmov 8(RSP) RBX
    Pfreeframe 24 16 0
    Pret
```

Fig. 25. Heterogeneous Sum with Mutual Recursion

C A MUTUAL RECURSIVE EXAMPLE FOR SUMMATION

In this section, we present the application of our method to an example borrowed from CompCertM — two programs that mutually invoke each other to finish a summation task.

It consists of a `Clight` module M_C and a hand-written assembly module M_A. The code of M_A and M_C is shown in Fig. 25. Note that we have also shown a version of M_A at the C level for reference and given its function the name g; this program do not actually exist in our example. We note that `f` and `g` collaborate to implement the summation from 0 to i given an integer i. We shall use `int` $\rightarrow$ `int` to denote their signature. `f` perform caching of results for any i in a global array while `g` only caches for the most recent i. When they need to compute a fresh result, they mutually recursively call each other with a smaller argument. The assembly program uses pseudo X86 assembly instructions defined in CompCert where every instruction begins with a letter P. The only real pseudo instructions are `Pallocframe` and `Pfreeframe`. `Pallocframe 24 16 0` allocates a stack block b_s of 24 bytes (3 integers on 64-bit x86), saves RSP and RA to $(b_s, 0)$ and $(b_s, 16)$ and set RSP to `Vptr`$(b_s, 0)$. `Pfreeframe 24 16 0` recovers RSP and RA from $(b_s, 0)$ and $(b_s, 16)$ and frees the stack block b_s. By the calling convention and the signature of g, RDI is used to pass the only argument i. RBX is a callee-saved register that stores i during internal execution. It is saved to $(b_s, 8)$ at the beginning of g and restored at the end. Therefore, the sole purpose of b_s is to save and restore RSP, RA and RBX.

The outline of the verification is presented in Fig. 26. It is similar to Fig. 4 except for the additional L_C which will be discussed soon. Firstly, as what we do in the client-server example, we write down the specification for the assembly module M_A which is called L_A defined in Definition C.1 and prove the simulation between L_A and $[[M_A]]$ which is declared in Theorem C.2. Secondly, we

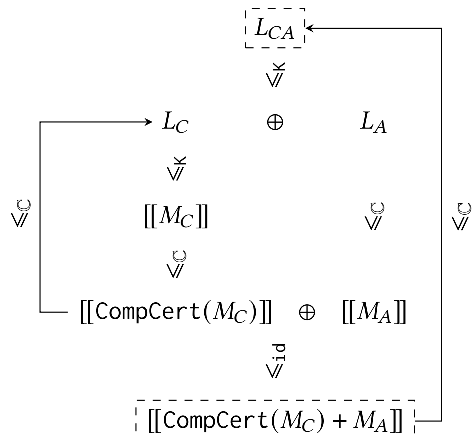


Fig. 26. Verification of the Mutual Sum ($\mathsf{K} := \texttt{ro} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{injp}}$)

define a top-level specification L_{CA} to abstract the semantics of the composition of M_C and M_A, which is shown and Definition C.5. Intuitively, L_{CA} says that the output is the summation from zero to the input. In this example, we additionally define a C-level specification for M_C called L_C (defined in Definition C.3) and prove $L_C \leqslant_{\texttt{ro}\cdot\texttt{wt}\cdot\texttt{c}_{\texttt{injp}}} [[M_C]]$ (in Theorem C.4). We can compose this proof with the compiler correctness by utilizing Theorem 6.5 to prove $L_C \leqslant_{\mathbb{C}} [[\texttt{CompCert}(M_C)]]$. With L_C, it is simpler to prove the source refinement declared in Theorem C.6. Finally, we combine these proofs to obtain the single refinement between top-level specification and the target linked program as declared in Theorem C.7.

Definition C.1. The open LTS of L_A is defined as follows:

$$
\begin{aligned}
S_A &:= \{\texttt{Callg}\ i\ m\} \cup \{\texttt{Callf}\ v_f\ i\ m\} \cup \{\texttt{Returnf}\ i\ r\ m\} \cup \{\texttt{Returng}\ r\ m\};\\
I_A &:= \{(\texttt{Vptr}(b_g, 0)[\texttt{int} \to \texttt{int}]([i])@m), (\texttt{Callg}\ i\ m)\};\\
\to_A &:= \{(\texttt{Callg}\ i\ m, \texttt{Returng}\ 0\ m) \mid i = 0\} \cup\\
&\quad\ \{(\texttt{Callg}\ i\ m, \texttt{Returng}\ r\ m) \mid i \neq 0 \land i = s[0] \land r = s[1]\} \cup\\
&\quad\ \{(\texttt{Callg}\ i\ m, \texttt{Callf}\ v_f\ i\ m) \mid i \neq 0 \land i \neq s[0] \land v_f = \texttt{find-func-pointer(f)}\} \cup\\
&\quad\ \{(\texttt{Returnf}\ i\ res\ m, \texttt{Returng}\ (i + res)\ m') \mid m' = m[s[0] \leftarrow i, s[1] \leftarrow (i + res)]\};\\
X_A &:= \{(\texttt{Callf}\ v_f\ i\ m, v_f[\texttt{int} \to \texttt{int}]([i-1])@m)\};\\
Y_A &:= \{(\texttt{Callf}\ v_f\ i\ m, r@m'), \texttt{Returnf}\ i\ r\ m')\};\\
F_A &:= \{(\texttt{Returng}\ i\ m, i@m)\}.
\end{aligned}
$$

By this definition, there are four kinds of internal states: `Callg` is at right after the initial call to g; `Callf` is right before the external call to `f`; `Returnf` is right after returning from `f`; and `Returng` is right before returning from g. The definitions of transition relations directly match the C-level version of g in Fig. 25, albeit in a big-step style. Note that when transiting internally from `Callg` $i\ m$ to `Callf` $v_f\ \ i\ m$, `find-func-pointer` is used to query the global symbol table for the function pointer to `f`. Also note that in L_A the memory state m is not changed from `Callg` to `Callf`, while in the assembly code M_A a new stack frame is allocated by `Pallocframe`. This indicates the stack frame is out-of-reach at the external call to `f` and should be protected during its execution. This point is also manifested in the proof below.

Theorem C.2. $L_A \leqslant_{\mathbb{C}} [[M_A]]$

Proof. The key is to identify a relation $R \in \mathcal{K}_{W_{\texttt{CAinjp}}}(S_A, \texttt{regset}\times\texttt{mem})$ satisfying all the properties in Definition 3.1. Given $w \in W_{\texttt{CAinjp}} = ((j, m_1, m_2), sg, rs)$, if $sg \neq \texttt{int} \to \texttt{int}$ then $R(w) = \emptyset$. Assume $sg = \texttt{int} \to \texttt{int}$, then $R(w)$ is defined as follows:

(a)	$(\texttt{Callg}\ i\ m_1, (rs, m_2)) \in R(w) \Leftrightarrow$ `(* initial state *)`
(a.1)	$rs(\texttt{RDI}) = i \wedge rs(\texttt{PC}) = \texttt{Vptr}(b_g, 0) \wedge m_1 \hookrightarrow^j_m m_2$
(b)	$(\texttt{Callf}\ v_f\ i\ m_1', (rs', m_2')) \in R(w) \Leftrightarrow$ `(* before external call *)`
(b.1)	$rs'(rbx) = i \wedge rs'(\texttt{RA}) = \texttt{Vptr}(b_g, 13) \wedge m_1' \hookrightarrow^{j'}_m m_2' \wedge v_f \hookrightarrow^{j'}_v rs'(\texttt{PC})$
(b.2)	$\wedge \forall r, (r \in \texttt{callee-saved-regs} \wedge r \neq \texttt{RBX}) \to rs'(r) = rs(r)$
(b.3)	$\wedge rs'(\texttt{RSP}) = \texttt{Vptr}(b_s, 0) \wedge \neg(\exists b\ o, j\ b = \lfloor b_s, o \rfloor)$
(b.4)	$\wedge (j, m_1, m_2) \leadsto_{\texttt{injp}} (j', m_1', m_2')$
(b.5)	$\wedge m_2'[b_s, 0] = rs(\texttt{RSP}) \wedge m_2'[b_s, 8] = rs(\texttt{RBX}) \wedge m_2'[b_s, 16] = rs(\texttt{RA})$
(c)	$(\texttt{Returnf}\ i\ res\ m_1', (rs', m_2')) \in R(w) \Leftrightarrow$ `(* after external call *)`
(c.1)	$rs'(\texttt{RBX}) = i \wedge rs'(\texttt{PC}) = (b_g, 13) \wedge rs'(rax) = res \wedge m_1' \hookrightarrow^{j'}_m m_2'$
(c.2)	$\wedge \forall r, (r \in \texttt{callee-saved-regs} \wedge r \neq \texttt{RBX}) \to rs'(r) = rs(r)$
(c.3)	$\wedge rs'(\texttt{RSP}) = \texttt{Vptr}(b_s, 0) \wedge \neg(\exists b\ o, j'\ b = \lfloor b_s, o \rfloor)$
(c.4)	$\wedge (j, m_1, m_2) \leadsto_{\texttt{injp}} (j', m_1', m_2')$
(c.5)	$\wedge m_2'[b_s, 0] = rs(\texttt{RSP}) \wedge m_2'[b_s, 8] = rs(\texttt{RBX}) \wedge m_2'[b_s, 16] = rs(\texttt{RA})$
(d)	$(\texttt{Returng}\ res\ m_1', (rs', m_2')) \in R(w) \Leftrightarrow$ `(* final state *)`
(d.1)	$rs'(\texttt{RAX}) = res \wedge rs'(\texttt{RSP}) = rs(\texttt{RSP}) \wedge rs'(\texttt{PC}) = rs(\texttt{RA}) \wedge m_1' \hookrightarrow^{j'}_m m_2'$
(d.2)	$\wedge \forall r, r \in \texttt{callee-saved-regs} \to rs'(r) = rs(r)$
(d.3)	$\wedge (j, m_1, m_2) \leadsto_{\texttt{injp}} (j', m_1', m_2')$

By definition the relation between internal states of L_A and assembly states evolve in four stages:

(a) Right after the initial call to g, (a.1) indicates that the argument i is stored in RDI and the program counter is at $(b_g, 0)$ (pointing to the first assembly instruction in Fig. 25);

(b) Right before the external call to f, (b.1) indicates i is stored in RBX, the return address is set to the 13th assembly instruction in Fig. 25 (right after `Pcall f`) and v_f matches with the program counter. (b.2) indicates callee saved registers—except for RBX–are not modified since the initial call. (b.3) indicates the entire stack frame b_s is out-of-reach. (b.4) maintains properties in injp. (b.5) indicates values on the stack frame is not modified since the initial call.

(c) Right after the external call to f, we have almost the same conditions as above, except that the program counter points to the return address set at the call to f.

(d) Right before returning from g, (d.1) indicates the return value is in RAX, the stack pointer is restored and the return address is set. (d.2) indicates all callee-saved registers are restored and (d.3) indicates the guarantee condition injp is met.

To prove R is indeed an invariant, we first show that condition (a) holds at the initial state. We then show by internal execution we can prove (b) holds right before the call to f. Now, the source and target execution proceed by calling and returning from f, after which we need to shown (c) holds. This is the most interesting part: it is achieved by combining properties (b.1–5) with the rely-condition provided by CAinjp for calling f. For example, because we know the stack frame b_s is out-of-reach at the call to f, by the accessibility enforced by injp in $\mathbb{R}^r_{\texttt{CAinjp}}$ in Definition 5.9, all values in $m_2'[b_s, o]$ are unchanged, therefore if $m_2'[b_s, 0] = rs(\texttt{RSP}) \wedge m_2'[b_s, 8] = rs(\texttt{RBX}) \wedge m_2'[b_s, 16] = rs(\texttt{RA})$ (condition (b.5)) holds before calling f, they also hold after (hence condition (c.5) holds). Similarly, we can derive (c.2) from (b.2) by the protection over callee-saved registers enforced in $\mathbb{R}^r_{\texttt{CAinjp}}$. Moreover, (PC) $= (b_g, 13)$ in (c.1) is derived from (RA) $= (b_g, 13)$ in (b.1) via the relation between PC and RA stated in $\mathbb{R}^r_{\texttt{CAinjp}}$. After the external call, we show condition (d) can be derived from (c) by following internal execution. We note that condition (d) provides exactly the guarantee-condition needed by $\mathbb{R}^r_{\texttt{CAinjp}}$ for the incoming call to g. Therefore, we successfully show $L_A \leqslant_{\mathbb{C}} [[M_A]]$ indeed holds.

□

Definition C.3. The C-level specification L_C is defined as follows:

S_C := $\{\texttt{Callf}\ i\ m\} \cup \{\texttt{Callg}\ v\ i\ m\} \cup \{\texttt{Returng}\ i\ sum\ m\} \cup \{\texttt{Returnf}\ sum\ m\}$;
I_C := $\{(\texttt{Vptr}(b_f, 0)[\texttt{int} \to \texttt{int}]([i])@m), (\texttt{Callf}\ i\ m)\}$;
$\to_C$:= $\{(\texttt{Callf}\ i\ m, \texttt{Returnf}\ 0\ m) \mid i == 0\} \cup$
$\{(\texttt{Callf}\ i\ m, \texttt{Returnf}\ sum\ m) \mid i \neq 0, m[b_m, 4 * i] \neq 0, sum = m[b_m, 4 * i]\} \cup$
$\{(\texttt{Callf}\ i\ m, \texttt{Callg}\ \texttt{Vptr}(b_g, 0)\ i\ m) \mid i \neq 0, m[b_m, 4 * i] = 0\}$
$\{(\texttt{Returng}\ i\ sum\ m, \texttt{Returnf}\ sum'\ m') \mid sum' = sum + i, m' = m[m[b_m, 4 * i] \leftarrow sum']\}$;
X_C := $\{(\texttt{Callg}\ v_g\ i\ m, v_g[\texttt{int} \to \texttt{int}]([i - 1])@m)\}$;
Y_C := $\{(\texttt{Callg}\ v_g\ i\ m, sum@m', \texttt{Returng}\ i\ sum'\ m')\}$;
F_C := $\{(\texttt{Returnf}\ sum\ m, sum@m)\}$;

The four internal states capture the execution of function f in M_C. From the initial state Callf, depending on the value of i and the cached value in $sum[b_m, 4 * i]$ where b_m is the memory block of memoized, Callf may return 0 if i is equal to 0, may return the cached value if it is not zero, and may enter Callg state to invoke function g. At Callg state, it emits the query to the environment and when it receives the reply which contains the summation of i, it would enter Returng state. Finally, Returng state would calculate the sum of i, cache it and enter the final state Returnf.

Theorem C.4. $L_C \leqslant_{\texttt{ro}\cdot\texttt{wt}\cdot\texttt{c}_{\texttt{injp}}} [[M_C]]$

By decomposing $\texttt{ro} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{injp}}$, the key is to prove that $L_C \leqslant_{\texttt{c}_{\texttt{injp}}} [[M_C]]$. Because we do not have to concern about the interleaving execution of L_C and its environment, the proof is straightforward.

Definition C.5. The top-level specification L_{CA} is defined below:

S_T := $\{\texttt{Callf}\ i\ m\} \cup \{\texttt{Callg}\ i\ m\} \cup \{\texttt{Return}\ i\ m\}$;
I_T := $\{(\texttt{Vptr}(b_f, 0)[\texttt{int} \to \texttt{int}]([i])@m), (\texttt{Callf}\ i\ m)\} \cup$
$\{(\texttt{Vptr}(b_g, 0)[\texttt{int} \to \texttt{int}]([i])@m), (\texttt{Callg}\ i\ m)\}$;
$\to_T$:= $\{(\texttt{Callf}\ i\ m, \texttt{Return}\ r\ m') \mid r = sum(i, m), m' = cache(i, m)\} \cup$
$\{(\texttt{Callg}\ i\ m, \texttt{Return}\ r\ m') \mid r = sum(i, m), m' = cache(i, m)\}$;
F_T := $\{(\texttt{Return}\ r\ m, r@m))\}$;

The specification contains two call states representing invocation of function f and g, and one return state. The internal transitions are big step of the execution, which omit the details of mutual recursion. The return value contained in the return state is determined by $sum(i, m)$, meaning that the return value depends on the contents of the memory, i.e., the contents of the initial contents of memorized in M_C and s in M_A. The memory of the return state is updated by *cache*, which cached the values generated during the execution to memorized and s.

Theorem C.6. $L_{CA} \leqslant_{\texttt{ro}\cdot\texttt{wt}\cdot\texttt{c}_{\texttt{injp}}} L_C \oplus L_A$

The key of this proof is to relate the memory operations of *cache* and the operations of $L_C \oplus L_A$. We achieve this by the induction of the input value i. Detailed proofs can be found in our supplementary code.

Theorem C.7. $L_{CA} \leqslant_{\mathbb{C}} [[\texttt{CompCert}(M_C) + M_A]]$

Proof. Firstly, applying vertical compositionality, we decompose the proof to $L_{CA} \leqslant_{\texttt{ro}\cdot\texttt{wt}\cdot\texttt{c}_{\texttt{injp}}} L_C \oplus L_A$ and $L_C \oplus L_A \leqslant_{\mathbb{C}} [[\texttt{CompCert}(M_C) + M_A]]$ by expanding $\mathbb{C}$ to $\texttt{ro} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{injp}} \cdot \mathbb{C}$ with

Lemma 6.5. The former one is proved in Theorem C.6. For the latter one, we first apply the horizontal compositionality to verify it modularly. The verification of $L_A \leqslant_{\mathbb{C}} [[M_A]]$ is proved in Theorem C.2. The verification of $L_C \leqslant_{\mathbb{C}}$ `CompCert`(M_C) is proved by applying Lemma 6.5, Theorem C.4 and the compiler correctness theorem. □

D COMPARISON USING THE RUNNING EXAMPLE

In this section, we carefully compare the difference between our direct refinement with other refinements in existing approaches to VCC using the running example. The comparison is mainly based on the (estimated) effort required to prove the running example. We also compare their results in the form of final theorems of semantics preservation.

Since CompComp does not support open semantics using $\mathcal{A}$ interface and the adequacy theorem for assembly code, we only introduce details about approaches using sum of refinements (CompCertM) and product of refinements (CompCertO) for further comparison here.

D.1 CompCertM

CompCertM uses Refinement Under Self-related Contexts (RUSC) to achieve vertical and horizontal composition of refinements. We roughly describe the framework of RUSC for presenting their verification and comparing it with ours (Appendix C).

Their open simulations are parameterized by different *memory relations* which mirror our use of KMRs. They do not need to lift memory relations to different simulation conventions because the semantics of all languages from C to $\mathcal{A}$ can perform C-style calls and returns. The RUSC refinement is parameterized over a fixed set of memory relations $\mathcal{R} = \{R_1, R_2, ..., R_n\}$. $p \geqslant_{\mathcal{R}} p'$ is defined as for any context program c, it c is self-related by all memory relations $R \in \mathcal{R}$, then $\mathrm{Beh}(c \oplus p) \supseteq \mathrm{Beh}(c \oplus p')$. Note that the behavior `Beh()` is only defined for closed program. Thanks to this definition, RUSC refinements under a fixed $\mathcal{R}$ can be easily composed vertically and horizontally if the *end modules* are self-related by all memory relations in $\mathcal{R}$. However, the disadvantage of RUSC-based approach is exactly the fixed $\mathcal{R}$ and the requirement that end programs are self-related by $\mathcal{R}$. Next, we demonstrate the impact of this restriction on VCC through the mutual summation example.

In CompCertM, they use the example of mutual summation to illustrate the source-level verification using RUSC. The structure of the proof is the same as depicted in Fig. 26. However, they actually use a different set of memory relations ($\mathcal{R}_e$) for source level verification with the set for compiler correctness ($\mathcal{R}_c$). At top level, they prove that

$$L_{CA} \geqslant_{\mathcal{R}_e} \texttt{a.spec} \oplus \texttt{b.spec} \geqslant_{\mathcal{R}_e} [[M_C]] \oplus [[M_A]]$$

Note that the verification here is slightly different with ours. The memory relations in $\mathcal{R}_e$ here include specific invariant which ensures that the variables `memorized1` and `memorized2` have desired values in the incoming memories. However, the values of these `static` variables cannot be determined at the invocation of a function. In other words, they describe and verify the behavior of this program in an ideal (instead of arbitrary) memory environment, i.e. the program always reads the correct summation from input i. On the other hand, we prove the preservation of open semantics for all possible memories. The return value of the program is determined by both the input i and the incoming memory as denoted by $sum(i, m)$ in Definition C.5. Given these differences, CompCertM use 5764 LoC to define the top-level memory relations, specification and complete the proof. We use 3124 LoC to complete our proof and link it with the result of VCC to achieve end-to-end direct refinement.

For further comparison, we now discuss how to compose the source verification with compiler correctness and adequacy of assembly linking within the framework of CompCertM. If M_C is compiled to $\texttt{CompCert}(M_C)$, then the correctness of CompCertM states that $[[M_C]] \geqslant_{\mathcal{R}_c} [[\texttt{CompCert}(M_C)]]$ The adequacy property for linking assembly modules is stated as $\texttt{Beh}([[\texttt{CompCert}(M_C)]] \oplus [[M_A]]) \supseteq \texttt{Beh}([[\texttt{CompCert}(M_C)]] + [[M_A]])$ There are two approaches to the end-to-end semantics preservation. Note that these two approaches are speculative because CompCertM did not present such composition.

Firstly, we can compose the three parts vertically in the form of *behavior refinement*. However, this approach only makes sense when the composed modules have closed semantics.

$$\texttt{Beh}(L_{CA}) \supseteq \texttt{Beh}([[\texttt{CompCert}(M_C)]] + [[M_A]])$$

Since the behavior refinement is transitively composable, we need to show $\texttt{Beh}([[M_C \oplus M_A]]) \supseteq \texttt{Beh}([[\texttt{CompCert}(M_C)]] \oplus [[M_A]])$. According to the definition of $\geqslant_{\mathcal{R}_c}$, it suffices to prove that $[[M_A]]$ is self-related by $\mathcal{R}_c$ which consists of six different memory relations, In CompCertM, all `Clight` and assembly modules can be self-related by all the relations in $\mathcal{R}_c$. Thus the result above can be easily obtained. However, we find that it is confusing to claim that any hand-written assembly program, even those do not obey the calling convention of CompCert, can satisfy $\mathcal{R}_c$ and safely be linked with programs compiled by CompCertM. The ability of CompCertM to prove such a property may come from its open semantics of assembly programs which can perform C-style calls and returns. The interaction between open modules through external calls in assembly-style is also limited by their "repaired semantics". In this regard, our direct refinement can better describe the desired properties of the assembly modules to be safely linked with compiled modules.

Secondly, for open semantics preservation in the form of RUSC refinement, one need to union the memory relations as $\mathcal{R}_e \cup \mathcal{R}_c$. Since the adequacy theorem is provided only in the form of behavior refinement, the conclusion is

$$L_{CA} \geqslant_{\mathcal{R}_e \cup \mathcal{R}_c} [[\texttt{CompCert}(M_C)]] \oplus [[M_A]]$$

To achieve this refinement, one need to show that the *end modules* are self-related by each $R \in \mathcal{R}_e \cup \mathcal{R}_c$. Excluding for the parts that have already been proved, we still need to show that *1)* L_{CA} is self-related by $\mathcal{R}_c$ and *2)* $[[\texttt{CompCert}(M_C)]]$ and $[[M_A]]$ are self-related by $\mathcal{R}_e$. These conditions are not demonstrated in CompCertM and we do not know whether they hold or not.

In other words, one need to show that *1)* the specification of source program satisfies all memory relations used in the compilation and *2)* the assembly modules satisfy the memory relations used for the source level verification. These limitations can increase the difficulty and reduce the extensionality of the proofs. Our direct refinement approach overcomes these obstacles.

D.2 CompCertO

In CompCertO, the simulation convention of the overall simulation for the compiler is stated as $\mathbb{C}_{\texttt{CCO}} = \mathcal{R}^* \cdot \texttt{wt} \cdot \texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA} \cdot \texttt{asm}_{\texttt{vainj}}$ where $\mathcal{R} = \texttt{c}_{\texttt{injp}} + \texttt{c}_{\texttt{inj}} + \texttt{c}_{\texttt{ext}} + \texttt{c}_{\texttt{vainj}} + \texttt{c}_{\texttt{vaext}}$ is a set of simulation conventions parameterized over used KMRs which is similar to CompCertM. $\mathcal{R}^*$ basically means that $\mathcal{R}$ can be used for zero or arbitrary times. Which means that the source verification can also be absorbed into $\mathbb{C}_{\texttt{CCO}}$ as what we do in §6.

As discussed in §1.2, the main difficulty in proving the running example using CompCertO is that the simulation convention is dependent on the details of compilation. We take `server.s` as an example for hand-written assembly and try to link it with $L_{\texttt{S}}$ using $\mathbb{C}_{\texttt{CCO}}$.

Firstly, for $\mathcal{R}^*$ we need to prove that $L_{\texttt{S}}$ is self-related using $\mathcal{R}$, thus the self-simulation can be duplicated for arbitrary times.

$$L_{\texttt{S}} \leqslant_{\texttt{c}_{\texttt{injp}} + \texttt{c}_{\texttt{inj}} + \texttt{c}_{\texttt{ext}} + \texttt{c}_{\texttt{vainj}} + \texttt{c}_{\texttt{vaext}}} L_{\texttt{S}}$$

This simulation means that L_s can take queries related by each of the KMRs, and choose one of them for its external calls. `vainj` and `vaext` are used to capture the consistency between static analyzer and the dynamic memories are we mentioned in §5.1. This simulation is conceptually correct but quite complex to prove.

Moreover, we need to define two extra specifications $L_{\mathcal{L}}$ and $L_{\mathcal{M}}$ for intermediate language interfaces and prove $L_{\mathsf{S}} \leqslant_{\mathsf{CL}} L_{\mathcal{L}}$, $L_{\mathcal{L}} \leqslant_{\mathsf{LM}} L_{\mathcal{M}}$ and $L_{\mathcal{M}} \leqslant_{\mathsf{MA}} [[\texttt{server.s}]]$. This approach not only requires a significant amount of effort but also presents a technical challenge which is how to achieve the protection of memory and registers for the target program. In Fig. 7, we use `injp` together with the structural simulation convention $\mathsf{CA} \equiv \mathsf{CL} \cdot \mathsf{LM} \cdot \mathsf{MA}$. For example, the saved values of registers are protected as `out-of-reach` in the memory (`injp`) such that these registers can be correctly restored to satisfy the calling convention. In $\mathbb{C}_{\mathsf{CCO}}$, LM requires that callee-save registers are protected, MA requires that RSP and RA are protected. While they do not provide any memory protection for saved values of these registers on the stack. This makes it extremely challenging to establish a simulation between L_{S} and $[[\texttt{server.s}]]$ through intermediate specifications. In fact, we came up with the idea of direct refinement during our attempts to prove this.