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

Verified compilation of open modules (i.e., modules whose functionality depends on other modules) provides 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 closed-world assumptions about the internal working of compilers, which not only incurs high complexity in verification but also makes it difficult for external users to apply the verification results. In this paper, we propose an approach to verified compositional compilation with no closed-world 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 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 physical semantics of open modules and that are ignorant of internal compilation processes. Such direct refinements support all the compositionality and adequacy properties essential for verified compilation of open modules. We demonstrate that our compiler correctness theorems are open to composition, intuitive and easy 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). Our development is fully formalized in Coq based CompCertO and supports the full compilation chain of CompCert with its Clight source language.

1 INTRODUCTION

Verified compilation ensures that behaviors of source programs can be faithfully transported to executable target code, a property indispensable for end-to-end formal verification of software. As contemporary software is usually composed of program modules independently developed, compiled and linked, researchers have developed a wide range of techniques for *verified compositional compilation* or VCC [Gu et al. 2015; Jiang et al. 2019; Koenig and Shao 2021; Song et al. 2020; Stewart et al. 2015; Wang et al. 2019] that support modules mutually invoking each other (i.e., open), being written in different languages (i.e., heterogeneous) and transformed by different compilers. However, as it stands now, the proposed approaches are inherently flawed at supporting open modules (e.g. libraries) as they either deviate from the physical semantics of open modules or expose internal working of compilers, resulting in correctness theorems with closed-world assumptions that are difficult to work with and incur high cost in verification. In this paper, we investigate an approach to eliminating these flaws while retaining the full benefit of VCC, i.e., obtaining correctness of compiling open modules that is *fully composable*, *adequate*, and *truly open*.

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 physical semantics*:

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

The first property states that refinement is transitive. It is essential for composing proofs for multi-pass compilers. The second property guarantees that refinement is 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 physical semantics and is essential to propagate verified properties to final target programs.

We use the example in Fig. 1 to illustrate the importance of the above properties in VCC where heterogeneous modules are compiled through vastly different compilation chains. Here, a source C module $\mathtt{a.c}$ is compiled to assembly $\mathtt{a.s}$ in three passes through two intermediate representations $\mathtt{a.i}_1$ and $\mathtt{a.i}_2$, and then linked with a library module $\mathtt{b.s}$ 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 $\mathtt{a.s} + \mathtt{b.s}$ refines the combined source semantics $\llbracket \mathtt{a.c} \rrbracket \oplus L_b$ where L_b is the semantic specification of $\mathtt{b.s}$, i.e., $\llbracket \mathtt{a.s} + \mathtt{b.s} \rrbracket \preccurlyeq \llbracket \mathtt{a.c} \rrbracket \oplus L_b$. The proof proceeds as follows:

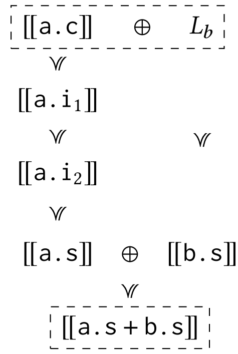

$\llbracket \mathtt{a.c} \rrbracket \quad \oplus \quad L_b$
$\llbracket \mathtt{a.i}_1 \rrbracket$
$\llbracket \mathtt{a.i}_2 \rrbracket$
$\llbracket \mathtt{a.s} \rrbracket \quad \oplus \quad \llbracket \mathtt{b.s} \rrbracket$
$\llbracket \mathtt{a.s} + \mathtt{b.s} \rrbracket$

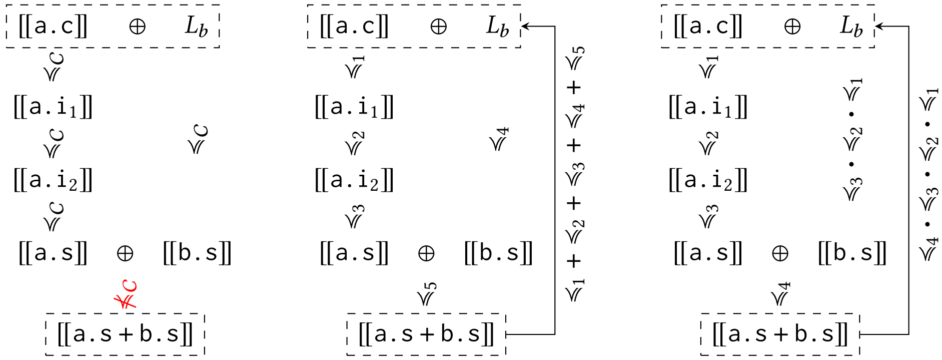
Fig. 1. Motivating Example

(1) Prove every pass respects refinement, from which we get $\llbracket \mathtt{a.i}_1 \rrbracket \preccurlyeq \llbracket \mathtt{a.c} \rrbracket$, $\llbracket \mathtt{a.i}_2 \rrbracket \preccurlyeq \llbracket \mathtt{a.i}_1 \rrbracket$ and $\llbracket \mathtt{a.s} \rrbracket \preccurlyeq \llbracket \mathtt{a.i}_2 \rrbracket$. Furthermore, show $\mathtt{b.s}$ meets its specification, i.e., $\llbracket \mathtt{b.s} \rrbracket \preccurlyeq L_b$;
(2) By vertical compositionality, compose the refinement relations for compiling $\mathtt{a.c}$ to get $\llbracket \mathtt{a.s} \rrbracket \preccurlyeq \llbracket \mathtt{a.c} \rrbracket$;
(3) By horizontal compositionality, compose the above refinement with that for $\mathtt{b.t}$ to get $\llbracket \mathtt{a.s} \rrbracket \oplus \llbracket \mathtt{b.s} \rrbracket \preccurlyeq \llbracket \mathtt{a.c} \rrbracket \oplus L_b$;
(4) By adequacy of linking at the target level and a final vertical composition, conclude $\llbracket \mathtt{a.s} + \mathtt{b.s} \rrbracket \preccurlyeq \llbracket \mathtt{a.c} \rrbracket \oplus L_b$.

1.2 Problems with 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 *languages 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, $\llbracket \mathtt{a.c} \rrbracket : C$ denotes semantics of $\mathtt{a.c}$ with interface C for interaction with environment through function calls and returns in C. Similarly, $\llbracket \mathtt{a.s} \rrbracket : \mathcal{A}$ denotes semantics of $\mathtt{a.s}$ where $\mathcal{A}$ allows for interaction at the assembly level. Note that semantics may not have their native interfaces. $\llbracket \mathtt{a.s} \rrbracket : C$ asserts that $\llbracket \mathtt{a.s} \rrbracket$ actually converts assembly level calls/returns to C function calls/returns for interacting with C modules. In this case, the "wrapped" semantics *deviate from their physical semantics*, hence is not adequate. When the interface of semantics $\llbracket M \rrbracket$ for module M is not explicitly given, it either can be inferred from the context or is simply the native interface for the language of M. Refinements may relate source and target semantics with different interfaces. We write $\preccurlyeq: \mathcal{I}_1 \Leftrightarrow \mathcal{I}_2$ to denote that $\preccurlyeq$ is a refinement between two semantics with interfaces $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively. For instance, $\llbracket \mathtt{b.s} \rrbracket \preccurlyeq_{\mathsf{ac}} L_b$ asserts that $\llbracket \mathtt{b.s} \rrbracket : \mathcal{A}$ is refined by $L_b : C$ with $\preccurlyeq_{\mathsf{ac}}: \mathcal{A} \Leftrightarrow C$ that relates open semantics at the C and assembly levels.

For VCC, it is essential that variance of open semantics and refinements does not impede compositionality and adequacy. The existing approaches achieve this by forcing all refinements to have certain coherent shapes, i.e., imposing *algebraic structures* on refinements. We categorize



(a) CompComp (b) CompCertM (c) CompCertO

Fig. 2. Refinements in Existing Approaches to VCC

these approaches by such 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 use a constant refinement relation $\preccurlyeq_{\mathcal{I}}$: $\mathcal{I} \Leftrightarrow \mathcal{I}$. 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 $\preccurlyeq_C$: $C \Leftrightarrow C$ 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, the verification results severely deviate from physical semantics since not all languages conform to the C interface. In particular, the 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 to choose refinement relations for different passes from a finite set $\{\preccurlyeq_1, \ldots, \preccurlyeq_n\}$ relating these interfaces, in which $\preccurlyeq_i$: $\mathcal{I}_1 + \ldots + \mathcal{I}_m \Leftrightarrow \mathcal{I}_1 + \ldots + \mathcal{I}_m$. 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 $1 \leq i \leq n$. 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 an example where semantics have both C and assembly interfaces, e.g., [[a.s]] : $\mathcal{A} + C$. This is the approach adopted by CompCertM to recover adequacy [Song et al. 2020]. However, this approach has several disadvantages. First, one must know beforehand that all the refinements in compilation are included in $\{\preccurlyeq_1, \ldots, \preccurlyeq_n\}$, which is essentially a *closed-world* assumption. Second, horizontal composition only works for modules *self-related* by all the refinements $\preccurlyeq_i$ $(1 \leq i \leq n)$, which is another closed-world restriction. Finally, since $\preccurlyeq_i$s are summarized from intermediate compiler passes, the top-level refinement inevitably depends on internals of compilers which hinders further compositional verification.

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 $(\_ \cdot \_)$. In particular, $L \preccurlyeq_1 \cdot \preccurlyeq_2 L''$ if there is some L' s.t. $L \preccurlyeq_1 L'$ and $L' \preccurlyeq_2 L''$. With the freedom to choose language interfaces, adequacy is still guaranteed.

With the bottom-up construction of refinements, no a priori knowledge about the whole compilation is needed for compositionality. Fig. 2c illustrates how it works. However, dependency on internals of compilation still exists. Note that vertical composition of refinements for compiling `a.c` results in a product refinement $[[\texttt{a.s}]] \preccurlyeq_3 \cdot \preccurlyeq_2 \cdot \preccurlyeq_1 [[\texttt{a.c}]]$. To horizontally compose with it, it is necessary to show L_b refines $[[\texttt{b.s}]]$ via the same product, i.e., to construct intermediate semantics bridging $\preccurlyeq_1$, $\preccurlyeq_2$ and $\preccurlyeq_3$. Therefore, even though this approach allows more flexible vertical composition, it is still dependent on the details of compilation for horizontal composition.

In summary, the existing approaches for VCC either lack adequacy because of deviation from physical semantics or lack compositionality that is truly extensional because of their dependency on internals of compilation. Such dependency makes the obtained correctness theorems for compiling open modules (e.g., libraries) difficult to further compose with. It also incurs high cost in verification.

1.3 Challenges for Direct Refinement of Open Modules

The ideal approach to VCC should produce refinements between source and target open modules that *1)* relate their semantics at their native language interfaces for adequacy, *2)* support vertical and horizontal composition without assuming internal details of compilation for truly open compositionality. For example, the refinement between `a.c` and `a.s` could be $\preccurlyeq_{\text{ac}}: \mathcal{A} \Leftrightarrow C$ s.t. $[[\texttt{a.s}]] \preccurlyeq_{\text{ac}} [[\texttt{a.c}]]$. It directly relates assembly and C open semantics, and could be further horizontally composed with $[[\texttt{b.s}]] \preccurlyeq_{\text{ac}} L_b$ and vertically composed by adequacy to get $[[\texttt{a.s} + \texttt{b.s}]] \preccurlyeq_{\text{ac}} [[\texttt{a.c}]] \oplus L_b$. Such refinements are easy to work with because of their extensionality, and can always be composed further with other refinements when necessary, thereby effectively support VCC for open programs and libraries (note that even the top-level refinement is still open to horizontal and vertical composition). We shall call them *direct refinements of open modules*.

The main challenge in getting direct refinements is tied to the well-known problem of proving "real" vertical composition for open refinements where the composed refinement must directly relates source and target semantics. That is, given any $\preccurlyeq_1 \cdot \preccurlyeq_2$, how to show it is equivalent to a single direct refinement $\preccurlyeq_3$. This is considered very technical and involved (see [Chung-Kil Hur and Vafeiadis 2012; 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 compositionality directly. Some introduces intrusive changes to deal with complex rely-guarantee conditions on interleaving module states, which either destroy adequacy or weaken compositionality [Song et al. 2020; Stewart et al. 2015]. Indeed, CompComp instruments the semantics of languages with *effect annotations* to expose internal effects and to make the construction of interpolating states feasible; CompCertM partially avoids the problem when restricting vertical composition to *closed* programs; CompCertO provides ad-hoc merging of refinements that still exposes the intermediate states of compilation.

Even if the problem of real vertical composition was solved, it is not clear if the solution can scale to realistic compilers with complex optimizations which have additional assumptions on programs (e.g. control or data flow analysis). Furthermore, to show that VCC with direct refinements are indeed useful in practice, it needs to support heterogeneous modules with free interaction between them and, even more, end-to-end and compositional program verification.

1.4 Our Contributions

In this paper, we are concerned with VCC of imperative programs with first-order states and support of pointers, e.g., C and assembly programs. In this setting, we address all of the above challenges.

First, we propose an approach to proving real vertical composition and to direct refinements of open modules with full support of compositionality and adequacy. Second, we demonstrate its effectiveness in verification of the *full* compilation chain of CompCert starting from its Clight source language. Third, we show the same approach easily supports end-to-end refinement verification.

A critical observation we make is that interpolating states for proving vertical compositionality of refinements can be constructed by exploiting properties on memory injections in CompCert. With it we discover that a *Kripke relation with memory protection* can serve as a uniform and composable interface for characterizing evolution of memory states across external calls. By adopting this relation in the refinement of CompCert's passes, we successfully combined their refinement proofs into a direct refinement from C modules to assembly modules, which does not have the weaknesses of existing approaches described in Sec. 1.2. We summarize our technical contributions below:

- We prove that `injp`—a Kripke Memory Relation with a notion of protection on evolving memory states across external calls—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 achieved 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 compositionality of `injp`. Combining with full compositionality and adequacy, we derive end-to-end refinements from high-level source specifications to physical semantics of linked assembly modules in a straightforward manner.

The above developments are fully formalized in Coq based on the latest release of CompCertO [Koenig and Shao 2021] which is in turn based on CompCert v.3.10 (See the supplementary materials). We choose CompCert because it is the most realistic and sophisticated verified compiler with non-trivial memory model supporting pointers and complex optimizations relying on memory invariants. Our development demonstrates that realistic verified compilers supporting the complete features of VCC and direct refinements of open modules are achievable without fundamental changes to verification frameworks and with reasonable effort. Therefore, our approach provides a promising direction for further evolving the techniques for compositional compiler verification.

1.5 Structure of the Paper

In the rest of the paper, we first talk about the background and key ideas of our approach in Sec. 2. We then present our technical contributions in Sec. 3, Sec. 4 and Sec. 5. We discuss evaluation and related work in Sec. 6 and finally conclude in Sec. 7.

```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

2 KEY IDEAS

We introduce a running example with heterogeneous modules and callback functions to illustrate the usefulness of direct refinements. 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 later, our approach also handles more complicated programs with mutually *recursive* heterogeneity without any problem (discussed in Sec. 5).

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 stored 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`-the 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 as an argument to the callback function `p`. `Pfreeframe m n o` frees the frame and restores `RSP` and `RA`.

With the running example, our goal is to verify its end-to-end correctness by exploiting the direct refinement $\preccurlyeq_{\mathrm{ac}}: \mathcal{A} \Leftrightarrow C$ derived from CompCert's compilation chain as shown in Fig. 4. The verification proceeds as follows. First, we establish $[\![\texttt{client.s}]\!] \preccurlyeq_{\mathrm{ac}} [\![\texttt{client.c}]\!]$ by the correctness of compilation. Then, we prove $[\![\texttt{server.s}]\!] \preccurlyeq_{\mathrm{ac}} L_{\mathsf{S}}$ 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 direct refinement* between the top-level specification and the target program:

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

The above verification is feasible thanks to the following benefits of direct refinements. First and foremost, direct refinements are truly extensional as they are ignorant of how modules are complied (if they are compiled at all), thereby can be easily adopted to handle free-form heterogeneous modules such as hand-written assembly with callback. Second, they respects adequacy, thereby can relate physical semantics of linked modules. Third, they always relate open modules and support full compositionality, thereby can be further composed with other refinement relations when necessary (e.g. the C level refinement to L_{CS}). This is fundamentally different from the closed nature of existing approaches described in Sec. 1.2.

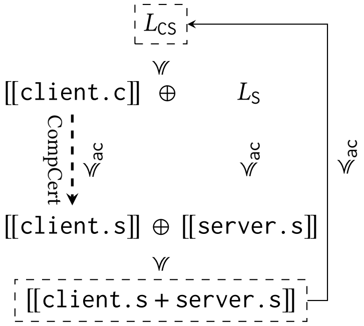


Fig. 4. Verifying the Running Example

In the subsections below, we give an in-depth exposure of the advantages of direct refinements by elaborating on how they directly relate source and target semantics while ignoring internals of compilation, and our approach to obtaining direct refinements.

2.1 Background

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

2.1.1 Block-based Memory Model. In CompCert's memory model [Leroy et al. 2012], a memory state m (of type `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 `block` and o has type `Z` (integers). The value of memory cell (one byte) at (b, o) is denoted by $m[b, o]$. Values are either undefined, 32- or 64-bit integers or floats, or pointers and defined by $\texttt{val} := \texttt{Vundef} \mid i_{32} \mid i_{64} \mid f_{32} \mid f_{64} \mid \texttt{Vptr}(b, o)$. 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. A memory cell have the following permissions ordered from high to low: `Freeable` $\geqslant$ `Writable` $\geqslant$ `Readable` $\geqslant$ `Nonempty` where `Freeable` enables all operations, `Writable` enables all but free, `Readable` enables only read, and `Nonempty` 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 $j : \texttt{block} \rightarrow \lfloor \texttt{block} \times \texttt{Z} \rfloor$ 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 $\texttt{meminj} = \texttt{block} \rightarrow \lfloor \texttt{block} \times \texttt{Z} \rfloor$. v_1 and v_2 are related under j (denoted by $v_1 \hookrightarrow_v^j v_2$) if either v_1 is `Vundef`, or they are both equal scalar values, or pointer 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, a *memory injection* between the source memory state m_1 and the target state m_2 under j (denoted by $m_1 \hookrightarrow_m^j m_2$) if the following properties are satisfied which ensure preservation of permissions and values under injection:

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

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

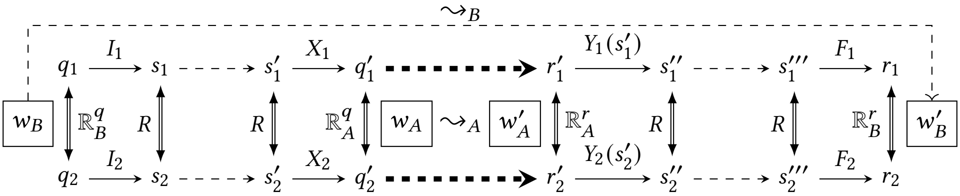


Fig. 5. Open Simulation between LTS

an identity injection function. As we shall see, reasoning about permissions and states under refinements is a major source of complexity in our work.

2.1.2 A Framework for Open Simulations. We adopt a language-independent framework for open semantics and simulations with customizable language interfaces for adequately describing language semantics at different levels, as introduced 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 language interfaces may be used at different stages of compilation. The relevant ones for our discussion are shown as follows (we omit language interfaces for intermediate languages in CompCert):

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	$\mathcal{A} = \langle \mathtt{regset} \times \mathtt{mem}, \mathtt{regset} \times \mathtt{mem} \rangle$	$rs@m$	$rs'@m'$

Here, the C interface is used for front-end languages where $v_f[sg](\vec{v})@m$ is a function call to v_f with signature sg and with a list of arguments $\vec{v}$ and a memory state m and $v'@m'$ carries a return value v' and an updated memory state m'. The assembly interface supports queries and replies carrying pairs of register sets (denoted by rs) and memory as program states.

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 $\rightarrow \subseteq S \times E^* \times S$ internal transitions emitting events of type 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 LTS. 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 $\mathbb{R} = \langle W, \mathbb{R}^q : \mathcal{K}_W(A_1^q, A_2^q), \mathbb{R}^r : \mathcal{K}_W(A_1^r, A_2^r) \rangle$ with type $\mathbb{R} : A_1 \Leftrightarrow A_2$. Simulation conventions serve as interfaces of open simulations by relating source and target language interfaces. For example, the basic C-level convention $\mathtt{c} : C \Leftrightarrow C = \langle \mathtt{meminj}, \mathbb{R}^q_\mathtt{c}, \mathbb{R}^r_\mathtt{c} \rangle$ 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.

$$
\begin{aligned}
(v_f[sg](\vec{v})@m, v'_f[sg](\vec{v'})@m') \in \mathbb{R}^q_\mathtt{c}(j) \quad &\Leftrightarrow \quad v_f \hookrightarrow^j_v v'_f \land \vec{v} \hookrightarrow^j_v \vec{v'} \land m \hookrightarrow^j_m m' \\
(v@m, v'@m') \in \mathbb{R}^r_\mathtt{c}(j) \quad &\Leftrightarrow \quad v \hookrightarrow^j_v v' \land m \hookrightarrow^j_m m'
\end{aligned}
$$

Open 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

Kripke invariant R, as shown in Fig. 5. We shall write such a simulation as $L_1 \leqslant_{\mathbb{R}_A \twoheadrightarrow \mathbb{R}_B} L_2$ and, for simplicity, write $L_1 \leqslant_{\mathbb{R}} L_2$ to denote $L_1 \leqslant_{\mathbb{R} \twoheadrightarrow \mathbb{R}} L_2$.

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 in presence of mutual calls between open modules. For illustration, the Kripke worlds at the boundary of modules is displayed in Fig. 5. The evolution of worlds across external calls is governed by an *accessibility relation* $\leadsto_A$ used to describe the *rely-condition* $w_A \leadsto_A w'_A$. By assuming external calls meet the rely-condition, one needs to prove the *guarantee condition* $w_B \leadsto_B w'_B$, i.e., the whole execution results in evolution of worlds respecting $\leadsto_B$. As a result, 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. $r \in \diamond\mathbb{R}^r(w) \Leftrightarrow \exists\, w', w \leadsto w' \wedge r \in \mathbb{R}^r(w')$. 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. We often write $\mathbb{R}_K$ to emphasize a convention $\mathbb{R}$ is parameterized by the KMR K.

Definition 2.1. A Kripke Memory Relation is a tuple $\langle W, f, \leadsto, R\rangle$ where W is a set of worlds, $f : W \rightarrow \texttt{meminj}$ a function for extracting injections from worlds, $\leadsto \subseteq W \times W$ an accessibility relation between worlds and $R : \mathcal{K}_W(\texttt{mem}, \texttt{mem})$ a Kripke relation over memory states that is compatible with the memory operations. We write $w \leadsto w'$ for $(w, w') \in\leadsto$.

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

Definition 2.2 (Kripke Relation with Memory Protection). $\texttt{injp} = \langle W_{\texttt{injp}}, f_{\texttt{injp}}, \leadsto_{\texttt{injp}}, R_{\texttt{injp}}\rangle$ where $W_{\texttt{injp}} = (\texttt{meminj} \times \texttt{mem} \times \texttt{mem})$, $f_{\texttt{injp}}(j, \_, \_) = j$, $(m_1, m_2) \in R_{\texttt{injp}}(j, m_1, m_2) \Leftrightarrow m_1 \hookrightarrow^{j}_{m} m_2$ and

$$\begin{aligned}(j, m_1, m_2) \leadsto_{\texttt{injp}} (j', m'_1, m'_2) \ \Leftrightarrow\ & j \subseteq j' \wedge \texttt{unmapped}(j) \subseteq \texttt{unchanged-on}(m_1, m'_1)\\ & \wedge \texttt{out-of-reach}(j, m_1) \subseteq \texttt{unchanged-on}(m_2, m'_2).\\ & \wedge \texttt{mem-acc}(m_1, m'_1) \wedge\ \texttt{mem-acc}(m_2, m'_2)\end{aligned}$$

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

$$\begin{aligned}(b_1, o_1) \in \texttt{unmapped}(j) \quad & \Leftrightarrow\ j(b_1) = \emptyset\\ (b_2, o_2) \in \texttt{out-of-reach}(j, m_1) & \Leftrightarrow\ \forall\, b_1\ o'_2,\ j(b_1) = \lfloor(b_2, o'_2)\rfloor \Rightarrow (b_1, o_2 - o'_2) \notin \texttt{perm}(m_1, \texttt{Nonempty}).\end{aligned}$$

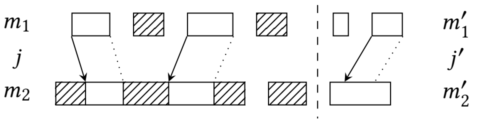


Fig. 6. Kripke Worlds Related by injp

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. 6 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; those blocks are never 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 across external calls. When `injp` is used at incoming side, it denotes that the simulation guarantees the unmapped and out-of-reach regions at initial queries are not modified by the simulation itself.

$$\begin{tikzcd}
L_{\mathsf{S}}: & \texttt{encrypt}(i,p)@m_1 \arrow[r, "I_1"] \arrow[dd, Leftrightarrow, "\mathbb{C}^q"] & ([i,p],m_1) \arrow[r, "K_1"] \arrow[dd, Leftrightarrow, "R"'] & ([i,p],m_1') \arrow[r, "X_1"] \arrow[dd, Leftrightarrow, "R"'] & p(b_0)@m_1' \arrow[rrr, dashed, very thick] \arrow[dd, Leftrightarrow, "\mathbb{C}^q"'] & & & ()@m_1'' \arrow[dd, Leftrightarrow, "\mathbb{C}^r"] & \cdots \\
\rotatebox{90}{$\preccurlyeq_{\mathbb{C}}$} & & & & & \boxed{w} \arrow[r, squiggly, "\texttt{injp}"] & \boxed{w'} & & \\
{[\![\texttt{server.s}]\!]}: & rs@m_2 \arrow[r, "I_2"] & rs@m_2 \arrow[r, dashed, "K_2"] & rs'@m_2' \arrow[r, "X_2"] & rs'@m_2' \arrow[rrr, dashed, very thick] & & & rs''@m_2'' & \cdots
\end{tikzcd}$$

Fig. 7. Direct Refinement of the Hand-written Server

2.2 Direct Refinement of Open Modules for CompCert

We now define $L_1 \preccurlyeq_{\mathsf{ac}} L_2$ as $L_2 \preccurlyeq_{\mathbb{C}} L_1$ where the simulation convention $\mathbb{C} : C \Leftrightarrow \mathcal{A}$ is parameterized by `injp` and relates open semantics of C and assembly.[1] Given $q_C = v_f[sg](\vec{v})@m_1$, $q_{\mathcal{A}} = rs@m_2$, $r_C = res@m_1'$, and $r_{\mathcal{A}} = rs'@m_2'$. $\mathbb{C}^q(q_C, q_{\mathcal{A}})$ requires that

(1) The memory states are related by an injection function j, i.e., $m_1 \hookrightarrow_m^j m_2$;
(2) The function pointer in C query is related to the PC register, i.e., $v_f \hookrightarrow_v^j rs(\mathsf{PC})$;
(3) The arguments in C query $\vec{v}$ 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 ensures 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.

For replies, $\mathbb{C}^r(r_C, r_{\mathcal{A}})$ requires that

(1) The updated memory states are related by $m_1' \hookrightarrow_m^{j'} m_2'$ where $j \subseteq j'$ and protected by `injp`, i.e., $(j, m_1, m_2) \leadsto_{\texttt{injp}} (j', m_1', m_2')$;
(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) $rs'(\mathsf{RSP}) = rs(\mathsf{RSP})$, $rs'(\mathsf{PC}) = rs(\mathsf{RA})$.

The first two requirements ensure that return values and memories are related according to the calling convention and the private regions are protected. The last two ensure that registers are correctly restored before returning. Finally, the direct refinement contains additional *semantic invariants* at the C level to ensure that read-only global variables are never modified and well-typedness of function calls and returns. They will be further discussed in Sec. 4.

2.3 Effectiveness of the Direct Refinement

We now illustrate how the above simple definition works for VCC of heterogeneous modules, including how it directly relates source and target semantics, how it ensures simulation by exploiting memory protection provided by `injp`, and how it handles compiler optimizations. The discussion is informal here; a formal development will be presented in Sec. 5.

The first thing to notice is that the definition of direct refinements does not mention anything about compilation: it is basically a formalized C calling convention with direct relations between source and target program states described via injections, together with invariants for protecting register values and memory states across external calls. Therefore, the definition is extensional and works for arbitrary code that meets its requirements. Take the refinement of hand-written assembly in Fig. 4 as an example, we need to prove $L_{\mathsf{S}} \preccurlyeq_{\mathbb{C}} [\![\texttt{server.s}]\!]$ by hand. The first few steps of the proof are depicted in Fig. 7, where L_{S} is an LTS hand-written by users and $[\![\texttt{server.s}]\!]$ is derived from CompCert assembly semantics. Because we are free to design L_{S} as long as it respects

[1] Note that the direction of refinement is reverted because of forward simulation, which is common in work based on CompCert as forward simulations are easier to prove and can be flipped into backward simulations [Sevcík et al. 2013].

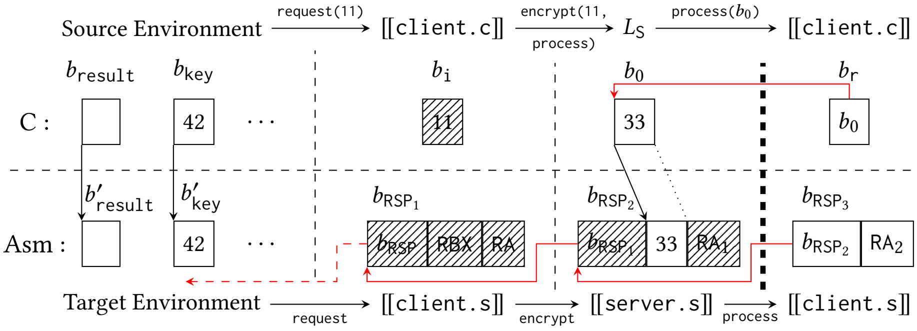


Fig. 8. Snapshot of the Memory State after Call Back

the direct refinement, we choose a form easy to comprehend where the internal executions are all in big steps. Now, suppose the environment calls encrypt, the source and target queries are initially related by $\mathbb{C}^q$ s.t. $rs(\texttt{RDI}) = i$ and $rs(\texttt{RSI}) = p$ by the calling convention. Then, according to I_1 and I_2, execution enters internal states related by an invariant R. Now, target execution takes internal steps until it hits an external call. It 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 invokes the callback function p with RSP+8. This corresponds to one big-step execution K_1 at the source level which allocates a memory block b_0, stored i XOR key at b_0, and preparing to call p with b_0. Therefore, the injection in the invariant R maps b_0 to RSP+8. The execution continues with external call to p, returns from p and goes on until encrypt returns.

Another point to note is that the requirement $(j, m_1, m_2) \leadsto_{\texttt{injp}} (j', m_1', m_2')$ between calls and returns is essential for protecting private values in stack memory so that simulation is preserved across external calls. This is true for any semantics related by the direct refinement, even for hand-written assembly. We illustrate how it works with an example. The environment calls request in the client with 11 which in turn calls encrypt in the server to generate an encrypted value 11 XOR 42 = 33 , whose address is passed back to the client by calling process. Fig. 8 depicts the snapshot of the memory states and their injection relation right after the call back function is invoked (i.e., at line 8 in Fig. 3a), where black arrows between blocks denote injections; red arrows denote pointers. The source semantics allocates one block for each local variable (b_i for i, b_0 for the encrypted value and b_r for r) while the target semantics stores their values in registers or stacks (11 is stored in RDI while the encrypted value 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 also stores private values including pointers to previous frames ($b_{\texttt{RSP}}$), return addresses (RA), and callee-saved registers (e.g., RBX). We use j, m_1 and m_2 to denote the injection, source and target memory states right at the call to process (they are to the left of the thick dashed line in Fig. 8), and j', m_1', m_2' to denote the injection and memory states after process returns. Then, $(j, m_1, m_2) \leadsto_{\texttt{injp}} (j', m_1', m_2')$ ensures that all the shaded memory areas are never modified between the call and return of process because they are out-of-reach from j. Only the stack-allocated encrypted value can be modified because the source block is also modifiable. Therefore, the return address or stack pointer of encrypt is never modified by process, thereby guaranteeing the simulation invariant to continue to hold after process returns. A similar situation can be observed at the call site to encrypt in the client, where even the source block b_i is protected because it is unmapped by injection. Note that this intuitive and direct protection of memory through injp is not present in previous work. CompCertO does not have a direct relation between source and target memory [Koenig and Shao 2021]. Therefore, the memory protection must be broken down into a sequence of relations between intermediate states, with which memory protection is hard to enforce. In CompCertM, memory injections are enriched with explicit private and public memory to identify which memory regions need protection [Song et al. 2020], which introduces extra mechanisms and proofs. By contrast, our memory protection is naturally derived from the rely conditions in `injp` that already appeared in the vanilla CompCert.

Lastly, the semantic invariants implied by the direct refinement not only enable compiler optimizations based on static value analysis but also similar optimizations for hand-written assembly. For example, since the key value is never modified in the running example, we can inline 42 in the code, resulting in an optimized server as shown in Fig. 3c. Then, we reuse L_{S} and designate the global variable `key` as a constant. By exploiting the semantic invariants, we can prove $L_{\mathsf{S}} \leqslant_{\mathbb{C}} [[\texttt{server\_opt.s}]]$ and derive a similar end-to-end correctness theorem as shown in Fig. 4.

2.4 Challenges for Establishing Direct Refinements

Having demonstrated the usefulness of using open simulation as direct refinements, we now face the problem of how to construct such a direct refinement for multi-pass optimizing compilers like CompCert. The obvious approach is to vertically compose the refinements proved for individual passes together. The most basic vertical composition for open simulations is stated as follows and can be easily proved by parallel pairing of individual simulations [Koenig and Shao 2021].

Theorem 2.3 (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, $(q_1, q_3) \in \mathbb{R}^q \cdot \mathbb{S}^q(w_{\mathbb{R}}, w_{\mathbb{S}}) \Leftrightarrow \exists q_2, (q_1, q_2) \in \mathbb{R}^q(w_{\mathbb{R}}) \land (q_2, q_3) \in \mathbb{S}^q(w_{\mathbb{S}})$ (similarly for $\mathbb{R}^r \cdot \mathbb{S}^r$). That is, the composed simulation assumes queries and replies are "concatenation" of individual queries and replies, and fed into and obtained from paralleling simulations, respectively. 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 Sec. 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

$$\begin{aligned} &\forall\, w_{\mathbb{S}}\ q_1\ q_2,\ (q_1, q_2) \in \mathbb{S}^q(w_{\mathbb{S}}) \Rightarrow \exists\, w_{\mathbb{R}},\ (q_1, q_2) \in \mathbb{R}^q(w_{\mathbb{R}}) \land \\ &\qquad\qquad\qquad\qquad \forall\, r_1\ r_2,\ (r_1, r_2) \in \mathbb{R}^r(w_{\mathbb{R}}) \Rightarrow (r_1, r_2) \in \mathbb{S}^r(w_{\mathbb{S}}) \end{aligned}$$

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 (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 eventually converted back to a rely for $\mathbb{S}$. Therefore, $\mathbb{S}$ is a refinement more *general* than $\mathbb{R}$ and $\mathbb{R}$ is more *specialized* than $\mathbb{S}$. 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, described as follows [Koenig and Shao 2021]:

Theorem 2.4. *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. 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 2.3 and Theorem 2.4, which is the desired direct refinement. This composition is illustrated in Fig. 9 where the parts enclosed by dashed boxes represent the concatenation of

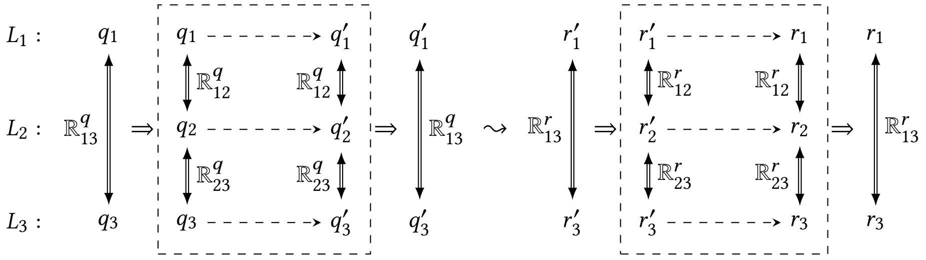
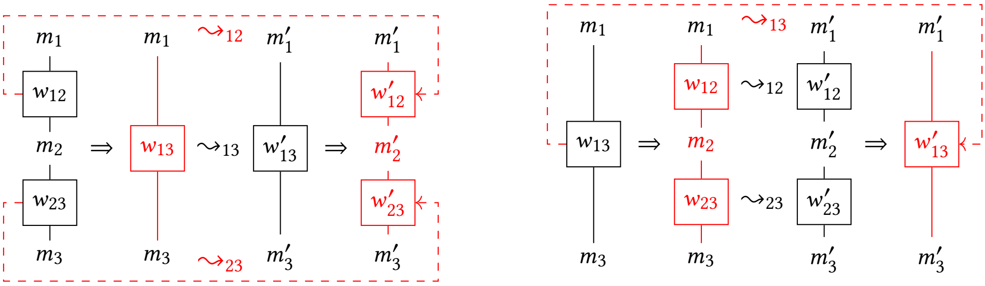


Fig. 9. Vertical Composition of Open Simulations by Refinement of Simulation Conventions



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

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

Fig. 10. Composition of KMRs

$L_1 \leqslant_{\mathbb{R}_{12} \twoheadrightarrow \mathbb{R}_{12}} L_2$ 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 parallely running simulations underlying the direct refinement.

However, there exist significant conceptual and technical challenges for obtaining such direct refinements and for successfully applying them to realistic optimizing compilers, which are also the root causes for existing approaches to opt for weaker refinements as discussed in Sec. 1.2.

Challenge 1: Composition of KMRs. A major obstacle is to show that 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:

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

K and L are equivalent, written as $K \equiv L$ iff $K \sqsubseteq L$ 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. $K_{13} \sqsubseteq K_{12} \cdot K_{23}$. A more intuitive interpretation is depicted in Fig. 10a where black symbols are $\forall$-quantified (assumptions we know) and red ones are $\exists$-quantified (conclusions we need to construct); note that Fig. 10a exactly mirrors the refinement on the outgoing side in Fig. 9. 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. 10b.

In both cases in Fig. 10, we need to construct interpolating states for relating source and target memory (i.e., m'_2 in Fig. 10a and m_2 in Fig. 10b). This is in general considered very difficult. 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 (unlike functions), and *2)* KMR (e.g., injp) may introduce memory protections across 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 destroy 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.

Challenge 2: End-to-end Direct Refinement for Optimizing Compilers. Even if a solution to composing KMRs is found, there are still problems to be solved for applying it to realistic optimizing compilers. First, we need to control the complexity of proofs when facing realistic compilers. Ideally, we would like to reuse the existing proofs as much as possible. However, it is not clear if the solution to Challenge 1 can indeed enable such reuse. Second, optimization passes generate additional rely-guarantee conditions on open semantics that cannot be composed into KMRs and that are embedded in the intermediate languages and interfere with direct refinements.

2.5 Our Approach

We discuss our approach to addressing the above challenges by using CompCert and CompCertO as the concrete platforms. To overcome the first challenge, we exploit the observation that `injp` in fact captures the rely-guarantee conditions for memory protection needed by any compiler pass in CompCert. Therefore, `injp` can be viewed as the most general KMR and adopted uniformly by all the compiler passes. Then, compositionality of KMRs depicted in Fig. 10 is reduced to transitivity of `injp`, i.e., `injp` ≡ `injp` · `injp`. The proof is based on the discovery that constructing interpolating states for `injp` is possible because *1)* it encodes a *partial functional transformation* on memory states and *2)* any memory states not in the domain or range of the partial function is protected 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 above solutions are discussed in Sec. 3.

To solve the second challenge, we notice that, although conceptually every compiler pass can use `injp`, it requires extensive rewriting of proofs. Instead, we start from the refinement proofs with least restrictive KMRs for individual passes in CompCertO, and exploit the properties that these KMRs can eventually be "absorbed" into `injp` in vertical composition to generate the direct refinement parameterized only by `injp`. CompCert also supports optimizations based on static value analysis, which rely on a *semantic invariant* that cannot be absorbed into `injp`. We discover that when piggybacked onto `injp` this semantic invariant can be transitively composed along with `injp`. By permutation of refinements, it is pushed to C level and becomes a condition for enabling optimization at the source level. Moreover, the pass for eliminating unused global variables (`Unusedglob`) can also be handled by absorbing its refinement into `injp`. In the end, we get an version of CompCert with end-to-end direct refinement $\leqslant_{\mathbb{C}}$. These solutions are discussed in Sec. 4.

Finally, we observe that source level refinements can be viewed as compilation using `injp`. Therefore, direct refinements can be easily extended to be end-to-end as we shall see in Sec. 5.

3 A UNIFORM AND COMPOSABLE KRIPKE MEMORY RELATION

The critical observation we make—also the cornerstone of this work—is that `injp` can serve as a uniform and composable KMR. We discuss its uniformity, i.e., `injp` directly captures the rely-guarantee conditions for memory protection for all compiler passes, and prove its transitivity.

3.1 Uniformity of `injp`

We show that `injp` is both a reasonable guarantee condition and a reasonable rely condition for memory protection for all the compiler passes in CompCert. The critical observation is that a notion of private and public memory can naturally be derived from `injp` where the private memory corresponds to regions unmapped by and out-of-reach from injections and the public memory corresponds to memory in the domain and image of injections. Then, any access to the public memory related by injection will never go out of the public memory. Therefore, the memory access is protected by `injp`. Details can be found in Appendix B.

3.2 Transitivity of injp

The goal is to show the two refinements in Fig. 10 holds when $K_{ij} = \texttt{injp}$, i.e., $\texttt{injp} \equiv \texttt{injp} \cdot \texttt{injp}$. As discussed in Sec. 2.4 the critical step is to construct interpolating memory states and Kripke worlds that transitively relate interpolating states to source and target states. Conceptually, this is possible because given an injection j and the source memory m_1, to build an interpolating memory m_2, we can project the values in m_1 through j to m_2. Furthermore, any state of m_2 not in the image of j would be determined by memory protection provided by `injp`. Below we elaborate on these key ideas and proof steps. A complete proof of transitivity of `injp` is given in Appendix C.

$$\begin{tikzcd}
m_1 \arrow[rr] \arrow[d, "j_{12}"'] & & m_1' \arrow[dd, "j'_{13}"'] & & m_1 \arrow[r] \arrow[d, "j_{12}"'] \arrow[dr, phantom, "\rightsquigarrow_{\texttt{injp}}"] & m_1' \arrow[d, "j'_{12}"] \arrow[dd, bend left, "j'_{13}"] \\
m_2 \arrow[d, "j_{23}"'] & \rightsquigarrow_{\texttt{injp}} & & \Rightarrow & m_2 \arrow[r] \arrow[d, "j_{23}"'] \arrow[dr, phantom, "\rightsquigarrow_{\texttt{injp}}"] & m_2' \arrow[d, "j'_{23}"] \\
m_3 \arrow[rr] & & m_3' & & m_3 \arrow[r] & m_3'
\end{tikzcd}$$

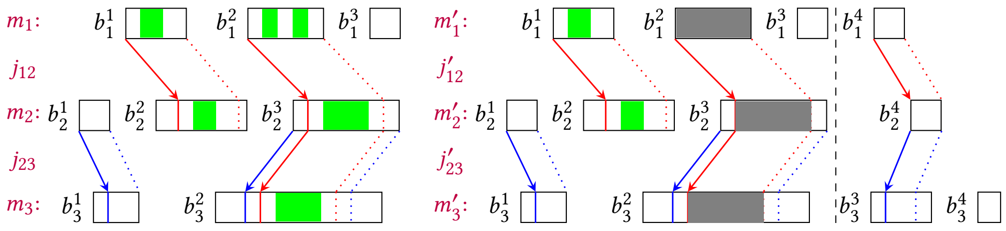
Fig. 11. Construction of Interpolating States

3.2.1 $\texttt{injp} \sqsubseteq \texttt{injp} \cdot \texttt{injp}$. By definition, we need to prove the following lemma:

Lemma 3.1. $\texttt{injp} \sqsubseteq \texttt{injp} \cdot \texttt{injp}$ *holds. That is,*

$$\begin{aligned}
&\forall j_{12}\ j_{23}\ m_1\ m_2\ m_3,\ m_1 \hookrightarrow_m^{j_{12}} m_2 \Rightarrow m_2 \hookrightarrow_m^{j_{23}} m_3 \Rightarrow \exists j_{13},\ m_1 \hookrightarrow_m^{j_{13}} m_3 \land \\
&\quad \forall m_1'\ m_3'\ j_{13}',\ (j_{13}, m_1, m_3) \rightsquigarrow_{\texttt{injp}} (j_{13}', m_1', m_3') \Rightarrow m_1' \hookrightarrow_m^{j_{13}'} m_3' \Rightarrow \\
&\qquad \exists m_2'\ j_{12}'\ j_{23}', (j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j_{12}', m_1', m_2') \land m_1' \hookrightarrow_m^{j_{12}'} m_2' \\
&\qquad\qquad \land (j_{23}, m_2, m_3) \rightsquigarrow_{\texttt{injp}} (j_{23}', m_2', m_3') \land m_2' \hookrightarrow_m^{j_{23}'} m_3'.
\end{aligned}$$

This lemma conforms to the graphic representation in Fig. 10a. To prove it, an obvious choice is to pick $j_{13} = j_{23} \cdot j_{12}$ (i.e., function composition of j_{12} and j_{23}). Then we are left to prove the existence of interpolating state m_2' and the memory and accessibility relations as shown in Fig. 11.



(a) Before

(b) After

Fig. 12. Constructing of an Interpolating Memory State

We use the concrete example in Fig. 12 to motivate the construction of m_2'. Here, the white and green areas correspond to locations in `perm(_, Nonempty)` (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 $(j_{23} \cdot j_{12}, m_1, m_3) \rightsquigarrow_{\texttt{injp}} (j_{13}', m_1', m_3')$, we need to define j_{12}' and j_{23}' and then build m_2' satisfying $m_1' \hookrightarrow_m^{j_{12}'} m_2'$, $m_2' \hookrightarrow_m^{j_{23}'} m_3'$, $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j_{12}', m_1', m_2')$, $(j_{23}, m_2, m_3) \rightsquigarrow_{\texttt{injp}} (j_{23}', m_2', m_3')$. m_1'

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 with 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}. In our example, these regions are the gray areas in Fig. 12b. The *permissions* in those regions are then 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. The remaining old memory regions should have the same values and permissions as in m_2.

In summary, the values in m_2' can be derived from m_1' because of the following two reasons. First, as memory injections get composed, unmapped and out-of-reach regions get *bigger*, meaning more memory regions gets protected. For example, in Fig. 12, 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 $j_{23} \cdot j_{12}$. Protected regions must have unchanged values and permissions. The only unprotected regions are those in the domain and image of the composed injections (i.e., gray areas in Fig. 12), whose values can be easily fixed because injections are partial functions: we can deterministically project the values and permission from a source state into the interpolating state.

3.2.2 `injp` $\cdot$ `injp` $\sqsubseteq$ `injp`. By definition, we need to prove:

Lemma 3.2. `injp` $\cdot$ `injp` $\sqsubseteq$ `injp` *holds. That is,*

$$\forall j_{13}\ m_1\ m_3,\ m_1 \hookrightarrow_m^{j_{13}} m_3 \Rightarrow \exists j_{12}\ j_{23}\ m_2,\ m_1 \hookrightarrow_m^{j_{12}} m_2 \wedge m_2 \hookrightarrow_m^{j_{23}} m_3 \wedge$$
$$\forall m_1'\ m_2'\ m_3'\ j_{12}'\ j_{23}',\ (j_{12}, m_1, m_2) \leadsto_{\texttt{injp}} (j_{12}', m_1', m_2') \Rightarrow (j_{23}, m_2, m_3) \leadsto_{\texttt{injp}} (j_{23}', m_2', m_3') \Rightarrow$$
$$m_1' \hookrightarrow_m^{j_{12}'} m_2' \Rightarrow m_2' \hookrightarrow_m^{j_{23}'} m_3' \Rightarrow \exists j_{13}',\ (j_{13}, m_1, m_3) \leadsto_{\texttt{injp}} (j_{13}', m_1', m_3') \wedge m_1' \hookrightarrow_m^{j_{13}'} m_3'.$$

This lemma conforms to the graphic representation in Fig. 10b. 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 are satisfied by exploiting the guarantees provided by `injp`.

4 DERIVATION OF THE DIRECT REFINEMENT FOR COMPCERT

CompCert compiles `Clight` programs into `Asm` programs through 19 passes [Leroy 2023], including several optimization passes working on the `RTL` intermediate language. In this section, we discuss the vertical composition of open simulations for all these passes into the direct refinement $\leqslant_{\mathbb{C}}$ following the approach discussed in Sec. 2.5. It consists of the following three steps. First, we prove the open simulation for all these passes with appropriate simulation conventions. In particular, we directly reuse the proofs of non-optimizing passes in CompCertO. For the optimization passes, we adapt the original proofs in CompCert to match the semantic invariants for handling optimizations. Second, we prove a collection of properties for refining simulation conventions in preparation for

Table 1. Significant Passes of CompCert

Languages/Passes	Outgoing $\twoheadrightarrow$ Incoming	Language/Pass	Outgoing $\twoheadrightarrow$ Incoming
`Clight`	$\mathcal{C} \twoheadrightarrow \mathcal{C}$	`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`	$\mathcal{C} \twoheadrightarrow \mathcal{C}$	`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`	$\mathcal{C} \twoheadrightarrow \mathcal{C}$	**`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`	$\mathcal{C} \twoheadrightarrow \mathcal{C}$	**`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`	$\mathcal{C} \twoheadrightarrow \mathcal{C}$	**`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`	$\mathtt{asm}_{\mathtt{injp}} \twoheadrightarrow \mathtt{asm}_{\mathtt{injp}}$

vertical composition. Those properties enables absorption of KMRs into `injp` and composition of semantic invariants. They rely critically on the transitivity of `injp` in Sec. 3. Finally, we vertically compose the simulation proofs and refine the incoming and outgoing simulation conventions into the single convention $\mathbb{C}$. We elaborate on the above steps in the subsequent subsections.

4.1 Open Simulation of Individual Passes

We list the compiler passes and their simulation types in Table 1 (passes on the right follows the last pass 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 which will be used in Sec. 4.3. Note that we have omitted passes with the identity simulation convention (i.e., with simulations $L_1 \leqslant_{\mathrm{id}} L_2$) in Table 1 as they do not affect the proofs. [2] Since the non-optimizing passes can be directly reused, the only non-trivial work is to prove open simulations for optimizations.

4.1.1 Simulation Conventions and Semantic Invariants. We first introduce relevant simulation conventions and semantic invariants for simulation proofs. The simulation conventions $\mathtt{c}_K : \mathcal{C} \Leftrightarrow \mathcal{C}$, $\mathtt{ltl}_K : \mathcal{L} \Leftrightarrow \mathcal{L}$, $\mathtt{mach}_K : \mathcal{M} \Leftrightarrow \mathcal{M}$, and $\mathtt{asm}_K : \mathcal{A} \Leftrightarrow \mathcal{A}$ relate the same language interfaces with queries and replies native to the associated intermediate languages, and are most commonly used throughout the verification. They are parameterized by 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 Sec. 3.1). Nevertheless, it is useful because the compiler proofs become simpler and more nature when using least restrictive KMRs which may be weaker than `injp`. CompCertO defines several KMRs weaker than `injp`. `id` is used when memory is unchanged. `ext` is used when the source and target memory shares the same structure. `inj` is a simplified version of `injp` without its memory protection. The simulation conventions $\mathtt{CL} : \mathcal{C} \Leftrightarrow \mathcal{L}$, $\mathtt{LM} : \mathcal{L} \Leftrightarrow \mathcal{M}$ and $\mathtt{MA} : \mathcal{M} \Leftrightarrow \mathcal{A}$ 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 this case). As discussed before, some refinements rely on invariants on the source semantics. The semantic invariant `wt` enforces that arguments and

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

return values of function calls respect function signatures. ro is critical for ensuring the correctness of optimizations, which will be discussed next.

4.1.2 Open Simulation of Optimization Passes. The optimizing passes Constprop, CSE and Deadcode perform constant propagation, common subexpression elimination and dead code elimination, respectively. They make use of a static analysis algorithm for collecting information of variables during the execution (e.g. a constant global variable always has its initial value). More specifically, for each function, the algorithm starts with the known initial values of read-only (constant) global variables. It simulates the program 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.

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. Therefore, 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 pass is similar. As an example, we only discuss constant propagation whose correctness theorem is stated as follows:

```
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. 13. An Example of Constant Propagation

Lemma 4.1. $\forall (M\ M' : RTL), \texttt{Constprop}(M) = M' \Rightarrow [[M]] \leqslant_{\texttt{ro}\cdot\texttt{c}_{\texttt{injp}}} [[M']]$.

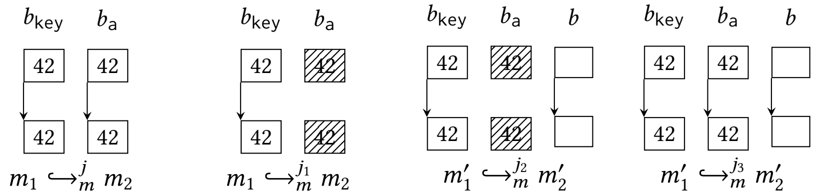
We discuss the proof of this lemma by illustrating how ro and injp help establish the open simulation for Constprop through a concrete example as depicted in Fig. 13. This example covers optimization for both global constants (key) and local variables (a) which are the focus of static analysis. By static analysis of Fig. 13a, *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 value 42 because foo (if well-behaved) will not modify a constant global variable. Furthermore, a has 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. 13b.

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 4.2. $\texttt{ro} : C \Leftrightarrow C = \langle W_{\texttt{ro}}, \mathbb{R}^q_{\texttt{ro}}, \mathbb{R}^r_{\texttt{ro}} \rangle$ 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, its relations only relate the same queries and replies, i.e., enforcing invariants only on one side. This kind of simulation conventions


b_{key}
b_{a}
b
42
$m_1 \hookrightarrow^{j}_{m} m_2$
$m_1 \hookrightarrow^{j_1}_{m} m_2$
$m_1' \hookrightarrow^{j_2}_{m} m_2'$
$m_1' \hookrightarrow^{j_3}_{m} m_2'$

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

Fig. 14. Memory Injections from Call to Return of `foo`

are what we called *semantic invariants*. The symbol tables (of type `symtbl` and a mapping from global symbols to memory addresses) are provided together with memory, so that the semantics can locate memory blocks of global definitions. $\texttt{ro-valid}(se, m)$ 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. 13a 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., $\texttt{ro-valid}(se, m) \Rightarrow \texttt{mem-acc}(m, m') \Rightarrow \texttt{ro-valid}(se, m')$). Therefore, 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. 14 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 *1)* the arguments to `foo` do not point to b_{a} and *2)* other pointers in m do not point to b_{a}. Therefore, we can simply remove b_{a} from the domain of j to get a shrunk yet valid memory injection j_1. Then, b_{a} is *unmapped* from the injection and protected during the call to `foo`. The injection of b_{a} is added back after the call returns and the simulation continues.

Finally, we talk a bit about the `Unusedglob` pass which removes unused static global variables from source modules. This pass was excluded from CompCertO because the original framework does not support the source and target semantics having different set of global symbols. We solve this problem by maintaining a skeleton of global definitions which stays the same throughout the compilation and maintaining local symbol tables that are subset of such skeletons. An interesting observation is that unlike other passes, `injp` is not needed for memory protection at the outgoing side (only `inj` is used) as this pass only changes global symbols, not external execution.

4.2 Properties for Refining Simulation Conventions

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

4.2.1 *Commutativity of KMRs and Structural Conventions.*

Lemma 4.3. *For* $\mathsf{XY} \in \{\mathsf{CL}, \mathsf{LM}, \mathsf{MA}\}$ *and* $K \in \{\texttt{ext}, \texttt{inj}, \texttt{injp}\}$ *we have* $\mathsf{X}_K \cdot \mathsf{XY} \sqsubseteq \mathsf{XY} \cdot \mathsf{Y}_K$.

This lemma is provided by CompCertO [Koenig and Shao 2021]. X and Y denote the simulation conventions for the source and target languages, respectively. For instance, $\mathsf{X} = \mathtt{c}$ and $\mathsf{Y} = \mathtt{ltl}$ when $\mathsf{XY} = \mathsf{CL}$. 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).

4.2.2 *Absorption of KMRs into* `injp`. After we move the simulation conventions parameterized over different KMRs to the same level, we try to absorb all KMRs into `injp`. The following properties are needed for this purpose.

Lemma 4.4. *For any* $\mathbb{R}$, $(1)\mathbb{R}_{\mathtt{injp}} \cdot \mathbb{R}_{\mathtt{injp}} \equiv \mathbb{R}_{\mathtt{injp}}$ $(2)\mathbb{R}_{\mathtt{injp}} \sqsubseteq \mathbb{R}_{\mathtt{inj}}$ $(3)\mathbb{R}_{\mathtt{injp}} \cdot \mathbb{R}_{\mathtt{inj}} \cdot \mathbb{R}_{\mathtt{injp}} \sqsubseteq \mathbb{R}_{\mathtt{injp}}$ $(4)\mathbb{R}_{\mathtt{inj}} \cdot \mathbb{R}_{\mathtt{inj}} \sqsubseteq \mathbb{R}_{\mathtt{inj}}$ $(5)\mathbb{R}_{\mathtt{ext}} \cdot \mathbb{R}_{\mathtt{inj}} \equiv \mathbb{R}_{\mathtt{inj}}$ $(6)\mathbb{R}_{\mathtt{inj}} \cdot \mathbb{R}_{\mathtt{ext}} \equiv \mathbb{R}_{\mathtt{inj}}$ $(7)\mathbb{R}_{\mathtt{ext}} \cdot \mathbb{R}_{\mathtt{ext}} \equiv \mathbb{R}_{\mathtt{ext}}$.

This lemma is a collection of refinement properties for simulation conventions lifted from their parameterizing KMRs. Property (1) is a direct consequence of $\mathtt{injp} \cdot \mathtt{injp} \equiv \mathtt{injp}$ (Sec. 3), which is critical for merging to simulations using `injp`. Property (2) indicates we can replace $\mathbb{R}_{\mathtt{inj}}$ with $\mathbb{R}_{\mathtt{injp}}$ at the outgoing side of a simulation. Property (3) is for absorbing $\mathbb{R}_{\mathtt{inj}}$ into surrounding $\mathbb{R}_{\mathtt{injp}}$ at the incoming side. These three properties in essence depend on the transitivity and uniformity of `injp` discussed in Sec. 3. The remaining properties are provided by CompCertO and their proofs are easy. Property (4) states $\mathbb{R}_{\mathtt{inj}} \cdot \mathbb{R}_{\mathtt{inj}}$ is refined by $\mathbb{R}_{\mathtt{inj}}$. Note that the refinement from another direction is not provable because of lack of memory protection for constructing interpolating states (therefore `injp` is needed in this case). Properties (5-6) indicate $\mathbb{R}_{\mathtt{ext}}$ may be absorbed into $\mathbb{R}_{\mathtt{inj}}$ and property (7) indicates $\mathbb{R}_{\mathtt{ext}}$ is transitive.

4.2.3 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.

Lemma 4.5. *For any* $\mathbb{R}_K : C \Leftrightarrow C$, *we have* $(1)\mathbb{R}_K \cdot \mathtt{wt} \equiv \mathtt{wt} \cdot \mathbb{R}_K \cdot \mathtt{wt}$ *and* $(2)\mathbb{R}_K \cdot \mathtt{wt} \equiv \mathtt{wt} \cdot \mathbb{R}_K$.

`wt` is easy to handle with the above properties. They enable elimination and permutation of `wt`. `ro` is more difficult to handle as it does not commute with simulation conventions. To eliminate redundant `ro`, we piggyback `ro` onto `injp` and prove the following transitivity property:

Lemma 4.6. $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \equiv \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$

The proof is similar to $\mathtt{c}_{\mathtt{injp}} \equiv \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}}$. The key is to make sure properties of `ro` are propagated to intermediate states when injections are splitting and merging (see Appendix D).

Finally, we need that `ro` and `wt` are commutative at the top level, which is straightforward to prove because they are independent from each other.

Lemma 4.7. $\mathtt{ro} \cdot \mathtt{wt} \equiv \mathtt{wt} \cdot \mathtt{ro}$

4.3 Proving Direct Open Simulation for CompCert

We first insert self-simulations into the compiler passes, as shown in Table 1. This is to supply extra $\mathbb{R}_{\mathtt{inj}}$, $\mathbb{R}_{\mathtt{injp}}$, and `ro` for absorbing $\mathbb{R}_{\mathtt{ext}}$ ($\mathbb{R}_{\mathtt{inj}}$) into $\mathbb{R}_{\mathtt{inj}}$ ($\mathbb{R}_{\mathtt{injp}}$) by properties in Lemma 4.4, and transitive composition of `ro`. Self-simulations are obtained by the following lemma.

Theorem 4.8. *If p is a program written in* `Clight` *or* `RTL` *and* $\mathbb{R} \in \{\mathtt{c}_{\mathtt{ext}}, \mathtt{c}_{\mathtt{inj}}, \mathtt{c}_{\mathtt{injp}}\}$, *or p is written in* `Asm` *and* $\mathbb{R} \in \{\mathtt{asm}_{\mathtt{ext}}, \mathtt{asm}_{\mathtt{inj}}, \mathtt{asm}_{\mathtt{injp}}\}$, *then* $[[p]] \leqslant_{\mathbb{R} \twoheadrightarrow \mathbb{R}} [[p]]$ *holds.*

We then 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

$$\begin{aligned}\mathbb{R} = {} & \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \\ & \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \cdot \mathtt{ltl}_{\mathtt{ext}} \cdot \mathtt{ltl}_{\mathtt{injp}} \cdot \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}} \\ \mathbb{S} = {} & \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \\ & \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \cdot \mathtt{ltl}_{\mathtt{ext}} \cdot \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{inj}} \cdot \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}.\end{aligned}$$

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 2.4 to get the simulation $L_1 \leqslant_{\mathbb{C} \twoheadrightarrow \mathbb{C}} L_2$. The direct simulation convention is $\mathbb{C} = \mathtt{ro}{\cdot}\mathtt{wt}{\cdot}\mathtt{CAinjp}{\cdot}\mathtt{asm}_{\mathtt{injp}}$. `ro` enables optimizations at C level while `wt` ensures well-typedness. `CAinjp` is the key component discussed informally in Sec. 2.2; its formal definition is given in Appendix E. The tailing $\mathtt{asm}_{\mathtt{injp}}$ is irrelevant as assembly code is self-simulating by Theorem 4.8.

The final correctness theorem is shown below:

Theorem 4.9. *Compilation in CompCert is correct in terms of open simulations,*

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

Below we explain how the refinements are carried out at the outgoing side. Refinements at the incoming side is similar and discussed in Appendix F. The following is the sequence of refined simulation conventions $\mathbb{C} \sqsubseteq \mathbb{R}_n \sqsubseteq \ldots \sqsubseteq \mathbb{R}_1 \sqsubseteq \mathbb{R}$. It begins with the composition of all initial outgoing conventions (including those for self-simulations) and ends with the unified convention.

(1) $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
$\cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \cdot \mathtt{ltl}_{\mathtt{ext}} \cdot \mathtt{ltl}_{\mathtt{injp}} \cdot \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}$

(2) $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
$\cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \cdot \mathtt{ltl}_{\mathtt{ext}} \cdot \mathtt{ltl}_{\mathtt{injp}} \cdot \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}$

(3) $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
$\cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \cdot \mathtt{ltl}_{\mathtt{ext}} \cdot \mathtt{ltl}_{\mathtt{injp}} \cdot \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}$

(4) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
$\cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \cdot \mathtt{ltl}_{\mathtt{ext}} \cdot \mathtt{ltl}_{\mathtt{injp}} \cdot \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}$

(5) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{CL} \cdot \mathtt{LM} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{injp}}$

(6) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{CL} \cdot \mathtt{LM} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{injp}}$

(7) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{CL} \cdot \mathtt{LM} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{injp}}$

(8) $\mathtt{wt} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{CL} \cdot \mathtt{LM} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{injp}}$

(9) $\mathtt{ro} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{CL} \cdot \mathtt{LM} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{injp}}$

(10) $\mathtt{ro} \cdot \mathtt{wt} \cdot \mathtt{CAinjp} \cdot \mathtt{asm}_{\mathtt{injp}}$

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 4.4 for $\mathtt{c}_{\mathtt{injp}}$ and properties (5-7) to compose $\mathtt{c}_{\mathtt{ext}}$ and absorb it into $\mathtt{c}_{\mathtt{inj}}$. We also apply Lemma 4.6 to merge consecutive $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$. In step (2), we move $\mathtt{wt}$ to higher positions by property (2) in Lemma 4.5. In step (3), we eliminate the first $\mathtt{wt}$ by property (1) in Lemma 4.5 and move the remaining $\mathtt{wt}$ higher by property (2) in Lemma 4.5 and Lemma 4.7. In step (4), we lift conventions over $\mathtt{CL}$, $\mathtt{LM}$ and $\mathtt{MA}$ to higher positions by Lemma 4.3. In step (5), we absorb $\mathtt{c}_{\mathtt{ext}}$ into $\mathtt{c}_{\mathtt{inj}}$ again and further turns $\mathtt{c}_{\mathtt{inj}}$ into $\mathtt{c}_{\mathtt{injp}}$ by applying $\mathtt{c}_{\mathtt{injp}} \sqsubseteq \mathtt{c}_{\mathtt{inj}}$ (property (2) in Lemma 4.4). In step (6), we compose $\mathtt{c}_{\mathtt{injp}}$ by applying $\mathtt{c}_{\mathtt{injp}} \equiv \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{injp}}$. In step (7), we apply Lemma 4.6 again to eliminate the second $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$. In step (8), we commute the two semantic invariants of the source semantics by Lemma 4.7. Finally, we merge $\mathtt{c}_{\mathtt{injp}}$ with $\mathtt{CL} \cdot \mathtt{LM} \cdot \mathtt{MA}$ into $\mathtt{CAinjp}$.

5 END-TO-END VERIFICATION OF HETEROGENEOUS MODULES

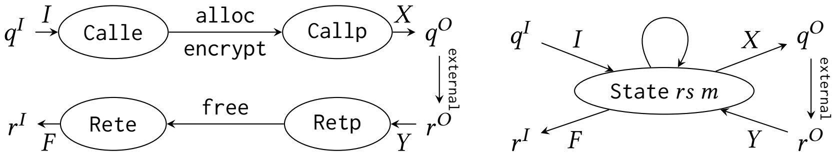
In this section, we give a formal account of end-to-end verification of heterogeneous modules based on direct refinements. Because of limit in space, we only discuss end-to-end verification of the running example in Fig. 4. More complicated examples with *mutually recursive* calls can be found in Appendix H. 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.

5.1 Refinement for the Hand-written Server

We give a formal definition of LTS for L_S along with a transition diagram in Fig. 15a.

Definition 5.1. LTS of L_S:

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



(a) L_S

(b) [[server_opt.s]]

Fig. 15. The Specification and Open Semantics of server_opt.s

$$\begin{tikzcd}
q^I_C \arrow[r, "I"] \arrow[d, leftrightarrow, "\mathbb{C}^q(w)"] & \texttt{Calle}\ i\ v_f\ m \arrow[r, "\texttt{alloc}\ sp", "\texttt{store}\ sp"'] \arrow[d, leftrightarrow, "R^a(w)"] & \texttt{Callp}\ sp\ v_f\ m_1 \arrow[r, "X"] \arrow[d, leftrightarrow, "R^b(w)"'] & q^O_C \arrow[r, phantom, "\rightsquigarrow"] \arrow[d, leftrightarrow, "\mathbb{C}^q(w')"'] & r^O_C \arrow[r, "Y"] \arrow[d, leftrightarrow, "\mathbb{C}^r(w')"] & \texttt{Retp}\ sp\ m_2 \arrow[r, "\texttt{free}\ sp"] \arrow[d, leftrightarrow, "R^c(w)"] & \texttt{Rete}\ m_3 \arrow[r, "F"] \arrow[d, leftrightarrow, "R^d(w)"'] & r^I_C \arrow[d, leftrightarrow, "\mathbb{C}^r(w)"'] \\
q^I_{\mathcal{A}} \arrow[r, "I"] & (rs, tm) \arrow[r, "\texttt{Pallocframe}", "\texttt{...}\ \texttt{Pcall}"'] & (rs_1, tm_1) \arrow[r, "X"] & q^O_{\mathcal{A}} \arrow[r, phantom, "\rightsquigarrow"] & r^O_{\mathcal{A}} \arrow[r, "Y"] & (rs_2, tm_2) \arrow[r, "\texttt{Pfreeframe}", "\texttt{Pret}"'] & (rs_3, tm_3) \arrow[r, "F"] & r^I_{\mathcal{A}}
\end{tikzcd}$$

Fig. 16. Open Simulation between the Server and its Specification

$$\begin{aligned} Y_S &:= \{(\texttt{Callp}\ sp\ v_f\ m, res@m', \texttt{Retp}\ sp\ m')\}; \\ F_S &:= \{(\texttt{Rete}\ m, \texttt{Vundef}@m)\}. \end{aligned}$$

The LTS has four internal states as depicted in Fig. 15a. Initialization is encoded in I. If the incoming query q^I contains a function pointer $\texttt{Vptr}(b_e, 0)$ which points to encrypt, L_S enters Calle $i\ v_f\ m$ 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 [[server_opt.s]] is given by CompCertO whose transition diagram is shown in Fig. 15b. All the states, including queries and replies, are composed of register sets and memory.

Theorem 5.2. $L_S \leqslant_{\mathbb{C}}$ [[server_opt.s]]

Given the open semantics, we need to prove the above forward simulation. We discuss the key ideas behind its proof and leave the complete proof in Appendix G. 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 ro · wt · CAinjp · asm$_{\texttt{injp}}$ and switch the order of ro and wt by Lemma 4.7. By the vertical compositionality (Theorem 2.3), we first prove $L_S \leqslant_{\texttt{wt}} L_S$ which is a straightforward self-simulation and [[server_opt.s]] $\leqslant_{\texttt{asm}_{\texttt{injp}}}$ [[server_opt.s]] is proved by Theorem 4.8. Then, we are left with $L_S \leqslant_{\texttt{ro}\cdot\texttt{CAinjp}}$ [[server_opt.s]]. By definition, we can easily show $L_S \leqslant_{\texttt{ro}} L_S$. Note that this self-simulation does not convey much information on its own, its real purpose is to propagate the protection in ro-valid to the simulation invariant defined below.

We are left with proving $L_S \leqslant_{\texttt{CAinjp}}$ [[server_opt.s]], i.e., to show the simulation diagram in Fig. 16 holds which is a complete picture of the example in Fig. 7. Here, the assumptions in forward simulation and conclusions we need to prove are represented as black and red arrows, respectively. For this, 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

Table 2. Comparison between VCC based on CompCert

	Direct Refinement	V. Comp	H. Comp	Adequacy	End-to-end Verification	Free-Form Heterogeneity
CompComp	No	Yes	Yes	No	No	Yes
CompCertM	No	RUSC	RUSC	Yes	Yes	Yes
CompCertO	No	Trivial	Yes	Yes	Unknown	Yes
CompCertX	No	CAL	CAL	Yes	CAL	No
This Work	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

`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. $o \leq 8$ 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.

5.2 End-to-end Correctness Theorem

Lemma 5.3 (Source-level Refinement). $L_{\mathsf{CS}} \leqslant_{\mathtt{ro}\cdot\mathtt{wt}\cdot\mathtt{c}_{\mathtt{injp}}} [\![\mathtt{client.c}]\!] \oplus L_{\mathsf{S}}$

We prove the above source-level refinement where L_{CS} is the top-level specification (defined in Appendix G). Its proof follows the same pattern as Theorem 5.2. The proof is considerably simpler because the source and target semantics share the same C interface. The simulation invariant R is mainly about the accessibility of `injp`. We omit the details due to limits in space.

As depicted in Fig. 4, to prove the forward simulation between the top-level specification and the target linked program. We exploit the horizontal compositionality and adequacy of assembly linking already provided by CompCertO's framework.

Theorem 5.4 (H. Compositionality and Adequacy).

$$\forall\ (L_1, L_2, L_1', L_2'),\ L_1 \leqslant_{\mathbb{R}\twoheadrightarrow\mathbb{R}} L_2 \Rightarrow L_1' \leqslant_{\mathbb{R}\twoheadrightarrow\mathbb{R}} L_2' \Rightarrow L_1 \oplus L_1' \leqslant_{\mathbb{R}\twoheadrightarrow\mathbb{R}} L_2 \oplus L_2'$$
$$\forall\ (M_1, M_2 : \mathsf{Asm}),\ [\![M_1]\!] \oplus [\![M_2]\!] \leqslant_{\mathtt{id}} [\![M_1 + M_2]\!]$$

Lemma 5.5. $[\![\mathtt{client.c}]\!] \oplus L_{\mathsf{S}} \leqslant_{\mathbb{C}} [\![\mathtt{client.s}]\!] \oplus [\![\mathtt{server\_opt.s}]\!]$

Proof. Immediate from Theorem 4.9, Theorem 5.2, and Theorem 5.4. □

For end-to-end open semantics with direct convention $\mathbb{C}$, we need to absorb Theorem 5.3 into it. The following theorem is easily derived by inserting `injp` and applying Lemma 4.5, 4.6 and 4.7.

Lemma 5.6. $\mathbb{C} \equiv \mathtt{ro} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathbb{C}$

The final end-to-end simulation is immediate by vertically composing Lemma 5.3, Lemma 5.5 and refining the simulation convention using Lemma 5.6.

Theorem 5.7. $L_{\mathsf{CS}} \leqslant_{\mathbb{C}} [\![\mathtt{client.s} + \mathtt{server\_opt.s}]\!]$

6 RELATED WORK

Our entire Coq development took about 7 person months. We added 15k lines of code on top of CompCertO. A detailed evaluation is in Appendix I. Below we compare our work with other frameworks for compositional compiler verification and program verification.

6.1 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 Table 2, including whether they support refinements that directly relate physical semantics of open modules and are ignorant of internal compilation processes, whether they support vertical and horizontal composition, whether they are adequate for physical semantics, whether they support end-to-end verification based on refinement, and whether they support heterogeneous modules that may be defined in different languages, complied through different passes and freely invoke each other, including mutually recursive calls. An answer that is not a simple "Yes" or "No" denotes that special constraints are enforced to support the specific feature. Note that our work is the only one that simultaneously supports all the features.

Compositional CompCert. CompComp supports VCC based on *interaction semantics* which is a specialized version of open semantics that only works with C interfaces [Stewart et al. 2015]. We have already talked about its merits and flaws in Sec. 1.2. It is interesting to note that CompComp can also be obtained based on our approach. If we adopt C-level simulation convention with `injp` (i.e., $\mathtt{c}_{\mathtt{injp}}$) for every compiler pass and compose them together by transitivity of $\mathtt{c}_{\mathtt{injp}}$, we basically get an alternative implementation of CompComp without its extra mechanisms or complexity.

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 the property of contexts that are self-relating under all of these simulation relations, horizontal and vertical compositionality are achieved. However, such compositionality is not extensional and difficult to use for even small examples. For example, the complete refinement relation $\leqslant_{R_1+\ldots+R_9}$ in CompCertM should carry all 9 RUSC relations $R_1, \ldots, R_9$ (6 for individual compiler passes and 3 for source-level verification). To prove that a refinement between hand-written assembly program `a.s` and its specification L_S can be horizontally composed with another refinement $\leqslant_{R_1+\ldots+R_9}$ (e.g., obtained from compilation), one needs to prove L_S and $[\![\mathtt{a.s}]\!]$ are self-simulating over *all* 9 simulation relations (the self-simulation for assembly language can be proved once and for all; that for L_S can only be proved manually). 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 resulting refinement is open to further horizontal or vertical composition. On the other hand, CompCertM supports behavior refinement of *closed* programs which we do not support yet. For this, we need to close the open simulation with program loading. We plan to finish this and get a behavior refinement theorem like in the original CompCert.

CompCertO. Vertical composition is a trivial parallel 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 convention for the overall compilation 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 where $\mathtt{c}_{\mathtt{vaext}}$ is an ad-hoc combination of KMR and internal invariants for optimizations. $\mathcal{R}^*$ means that $\mathcal{R}$ can be used for an arbitrary number of times. Note that the top-level summation of KMRs is similar to RUSC in CompCertM. Therefore, to horizontally compose these refinements, we need to go through the same process as in CompCertM, only more complicated because the necessity to reason about how simulations conform to internal invariants of optimizations and how such simulation can be repeated over all possible combination of KMRs indefinitely. Therefore, it is unknown if the correctness theorem of CompCertO suffices for end-to-end program verification. In this work, we have completely fixed these problems.

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. Compositional verification of compilation for concurrent programs is a topic different from traditional VCC as it assumes working with multiple threads and execution environments. CASCompCert is an extension of CompComp that supports compositional compilation of concurrent programs 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 adopted to achieve VCC for concurrency with cleaner interface and less restrictions.

6.2 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. 2012]. 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 language is used to formalize the semantics and compiler correctness is stated using contextual equivalence or logical relations. It seems that our techniques are not directly applicable to those work because relational reasoning on higher-order states cannot deterministically fix the interpolating states. An interesting direction to explore is to combine our techniques with those work to deal with linear memory space with pointers in higher-order states.

The high-level idea of constructing interpolating memory state for proving transitivity of `injp` can also be found in some of the work on proving program equivalence using bisimulation [Chung-Kil Hur and Vafeiadis 2012] and logical relations [Ahmed 2006]. However, these work has considerably simpler memory model and does not deal with pointers. Furthermore, previous work considers it extremely difficult to construct interpolating states without extra mechanisms such as annotation of private and public memory. We discover that the notion of public and private memory inferred from `injp` which already exists in the vanilla CompCert suffices for this purpose. There is no need to make any changes to program semantics and verification framework for this.

6.3 Frameworks for Compositional Program Verification

Researchers have proposed frameworks for compositional program verification based on novel semantics [Chappe et al. 2023; He et al. 2021; Sammler et al. 2023; Xia et al. 2019] and *separation logics* [Song et al. 2023]. These frameworks aim at broader goals compared to VCC and may be combined with our approach to generate stronger end-to-end verification techniques. A detailed comparison is in Appendix J.

7 CONCLUSION

Existing approaches to verified compositional compilation have difficulties in supporting open modules as their correctness theorems either do not connect with physical semantics or inevitably depend on internal working of compilation. We have proposed an approach to compositional compiler correctness via construction of refinements relating the source and target semantics at their native interfaces and that do not depend on any assumption on compilation, which overcomes the weaknesses of existing approaches. We have realized our approach in CompCert and demonstrated its effectiveness through end-to-end verification of non-trivial heterogeneous programs.

REFERENCES

Amal Ahmed. 2006. Step-Indexed Syntactic Logical Relations for Recursive and Quantified Types. In *ESOP*. 69–83.

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 (jan 2023), 31 pages. https://doi.org/10.1145/3571254

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

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).* ACM, New York, 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).* ACM, New York, 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 (oct 2021), 29 pages. https://doi.org/10.1145/3485512

Chung-Kil Hur, Derek Dreyer, Georg Neis, and Viktor Vafeiadis. 2012. The marriage of bisimulations and Kripke logical relations. In *POPL'12*. 59–72.

Hanru Jiang, Hongjin Liang, Siyang Xiao, Junpeng Zha, and Xinyu Feng. 2019. Towards Certified Separate Compilation for Concurrent Programs. In *Proc. 40th ACM Conference on Programming Language Design and Implementation (PLDI'19).* ACM, New York, 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. *SIGPLAN Not.* 52, 1 (jan 2017), 175–189. https://doi.org/10.1145/3093333.3009850

Jérémie Koenig and Zhong Shao. 2021. CompCertO: Compiling Certified Open C Components. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation* (Virtual, Canada) *(PLDI 2021).* Association for Computing Machinery, New York, NY, USA, 1095–1109. https://doi.org/10.1145/3453483.3454097

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 *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation* (London, UK) *(PLDI 2020).* Association for Computing Machinery, 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 *Proceedings of the 20th ACM SIGPLAN International Conference on Functional Programming* (Vancouver, BC, Canada). ACM Press, 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 (jul 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 (jun 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 *ESOP'14*. 128–148.

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. *Proceedings of the ACM on Programming Languages* 7, POPL (2023), 775–805.

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 International Publishing, Cham, 146–162.

Jaroslav Sevcík, Viktor Vafeiadis, Francesco Zappa Nardelli, Suresh Jagannathan, and Peter Sewell. 2013. CompCertTSO: A Verified Compiler for Relaxed-Memory Concurrency. *J. ACM* 60, 3 (2013), 22:1–22:50. https://doi.org/10.1145/2487241.

2487248

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 (Jan. 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. *Proceedings of the ACM on Programming Languages* 7, POPL (2023), 1121–1151.

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, 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 (Jan. 2019), 30 pages. https://doi.org/10.1145/3290375

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. *Proceedings of the ACM on Programming Languages* 4, POPL (2019), 1–32.

Junpeng Zha, Hongjin Liang, and Xinyu Feng. 2022. Verifying Optimizations of Concurrent Programs in the Promising Semantics. In *Proceedings of the 43rd ACM SIGPLAN International Conference on Programming Language Design and Implementation* (San Diego, CA, USA) *(PLDI 2022).* Association for Computing Machinery, New York, NY, USA, 903–917. https://doi.org/10.1145/3519939.3523734

A FRAMEWORK FOR OPEN SIMULATION

We present the remaining part of the framework. They are the horizontal composition of open semantics and the definition of open simulation.

Definition A.1 (Composition of Open LTS). Given $L_1, L_2 : A \twoheadrightarrow A$, their composition is defined as

$$L_1 \oplus L_2 := \langle D_1 \cup D_2, (S_1 + S_2)^*, I, \rightarrow, F, X, Y \rangle.$$

where I, F, X, Y are defined using the rules below:

$$\frac{q \in D_i \quad (q, s) \in I_i}{(q, (i, s)) \in I}\ \texttt{init} \qquad \frac{s \xrightarrow{t}_i s'}{(i, s) :: \vec{k} \xrightarrow{t} (i, s') :: \vec{k}}\ \texttt{step} \qquad \frac{(s, r) \in F_i}{([i, s], r) \in F}\ \texttt{fin}$$

$$\frac{(s, q) \in X_i \quad q \in D_j \quad (q, s') \in I_j}{(i, s) :: \vec{k} \xrightarrow{\texttt{nil}} (j, s') :: (i, s) :: \vec{k}}\ \texttt{mut-q} \qquad \frac{(s, r) \in F_i \quad (s', r, s'') \in Y_j}{(i, s) :: (j, s') :: \vec{k} \xrightarrow{\texttt{nil}} (j, s'') :: \vec{k}}\ \texttt{mut-r}$$

$$\frac{(s, q) \in X_i \quad \forall j, q \notin D_j}{((i, s) :: \vec{k}, q) \in X}\ \texttt{ext-q} \qquad \frac{(s, r, s') \in Y_i}{((i, s) :: \vec{k}, r, (i, s') :: \vec{k}) \in Y}\ \texttt{ext-r}$$

Open simulations are used to represent compiler correctness. They are forward simulations parameterized by simulation conventions for relating incoming and outgoing queries and replies.

Definition A.2. Given two open LTS $L_1 : A_1 \twoheadrightarrow B_1$ and $L_2 : A_2 \twoheadrightarrow B_2$, and given two simulation conventions $\mathbb{R}_A : A_1 \Leftrightarrow A_2$ and $\mathbb{R}_B : B_1 \Leftrightarrow B_2$, an open forward simulation between L_1 and L_2 is a Kripke relation $R \in \mathcal{K}_{W_B}(S_1, S_2)$ that satisfies the following properties:

(* Initial queries match *)
$\forall\ q_1\ q_2,\ (q_1, q_2) \in \mathbb{R}_B^q \Rightarrow (q_1 \in D_1 \Leftrightarrow q_2 \in D_2)$
(* Initial states satisfy simulation *)
$\forall\ w_B\ q_1\ q_2\ s_1,\ (q_1, q_2) \in \mathbb{R}_B^q(w_B) \Rightarrow (q_1, s_1) \in I_1 \Rightarrow \exists\ s_2, (s_1, s_2) \in R(w_B) \land (q_2, s_2) \in I_2.$
(* Final states satisfy simulation *)
$\forall\ w_B\ s_1\ s_2\ r_1,\ (s_1, s_2) \in R(w_B) \Rightarrow (s_1, r_1) \in F_1 \Rightarrow \exists\ r_2, (r_1, r_2) \in \mathbb{R}_B^r(w_B) \land (s_2, r_2) \in F_2.$
(* Stepping relations satisfy simulation *)
$\forall\ w_B\ s_1\ s_2\ t,\ (s_1, s_2) \in R(w_B) \Rightarrow s_1 \xrightarrow{t} s_1' \Rightarrow \exists\ s_2', (s_1', s_2') \in R(w_B) \land s_2 \xrightarrow{t}^* s_2'.$
(* External calls satisfies simulations *)

$$\begin{tikzcd}
(b_1, o_1) \arrow[r, "\mathtt{read}"] \arrow[d, "j"'] & (b_2, o_2) \arrow[r, "\mathtt{read}"] \arrow[d, "j"'] & (b_3, o_3) \arrow[r, "\mathtt{read}"] \arrow[d, "j"'] & \cdots \\
(b'_1, o'_1) \arrow[r, "\mathtt{read}"] & (b'_2, o'_2) \arrow[r, "\mathtt{read}"] & (b'_3, o'_3) \arrow[r, "\mathtt{read}"] & \cdots
\end{tikzcd}$$

Fig. 17. A Sequence of Reads from the Closed Public Memory

$$\begin{aligned}
&\forall\, w_B\ s_1\ s_2\ q_1,\ (s_1, s_2) \in R(w_B) \Rightarrow (s_1, q_1) \in X_1 \Rightarrow \\
&\quad \exists w_A\ q_2,\ (q_1, q_2) \in \mathbb{R}^q_A(w_A) \land (s_2, q_2) \in X_2 \land \\
&\qquad \forall\, r_1\ r_2\ s'_1, (r_1, r_2) \in \mathbb{R}^r_A(w_A) \Rightarrow (s_1, r_1, s'_1) \in Y_1 \Rightarrow \exists\, s'_2, (s'_1, s'_2) \in R(w_B) \land (s_2, r_2, s'_2) \in Y_2.
\end{aligned}$$

We write $L_1 \leqslant_{\mathbb{R}_A \twoheadrightarrow \mathbb{R}_B} L_2$ when such a relation exists.

From the above definition, it is easy to prove the horizontal and vertical compositionality of open simulations and their conformance to syntactic linking:

Theorem A.3 (H. Compositionality). *Given $L_1, L'_1 : A_1 \twoheadrightarrow A_1$, $L_2, L'_2 : A_2 \twoheadrightarrow A_2$ and $\mathbb{R} : A_1 \Leftrightarrow A_2$,*

$$L_1 \leqslant_{\mathbb{R} \twoheadrightarrow \mathbb{R}} L_2 \Rightarrow L'_1 \leqslant_{\mathbb{R} \twoheadrightarrow \mathbb{R}} L'_2 \Rightarrow L_1 \oplus L'_1 \leqslant_{\mathbb{R} \twoheadrightarrow \mathbb{R}} L_2 \oplus L'_2.$$

The vertical compositionality defined below is the same as the one defined in Theorem 2.3.

Theorem A.4 (V. Compositionality). *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 $\mathbb{R}_A : A_1 \Leftrightarrow A_2$, $\mathbb{R}_B : B_1 \Leftrightarrow B_2$, $\mathbb{S}_A : A_2 \Leftrightarrow A_3$ and $\mathbb{S}_B : B_2 \Leftrightarrow B_3$,*

$$L_1 \leqslant_{\mathbb{R}_A \twoheadrightarrow \mathbb{R}_B} L_2 \Rightarrow L_2 \leqslant_{\mathbb{S}_A \twoheadrightarrow \mathbb{S}_B} L_3 \Rightarrow L_1 \leqslant_{\mathbb{R}_A \cdot \mathbb{S}_A \twoheadrightarrow \mathbb{R}_B \cdot \mathbb{S}_B} L_3.$$

Theorem A.5 (Conformance to Syntactic Linking). *Given assembly modules M_1, M_2 : $\mathtt{Asm}$, $[\![\_]\!] : \mathtt{Asm} \to (\mathcal{A} \twoheadrightarrow \mathcal{A})$ and the identity simulation convention $\mathtt{id} : \mathcal{A} \Leftrightarrow \mathcal{A}$,*

$$[\![M_1]\!] \oplus [\![M_2]\!] \leqslant_{\mathtt{id} \twoheadrightarrow \mathtt{id}} [\![M_1 + M_2]\!]$$

B UNIFORMITY OF injp

B.1 Public and Private Memory with respect to Memory Injections

We present a notion of public and private memory derived from injections which provides a notion of protection that is in turn precisely captured by injp.

Definition B.1. Given $m_1 \hookrightarrow^j_m m_2$, the public memory regions in m_1 and m_2 are defined as follows:

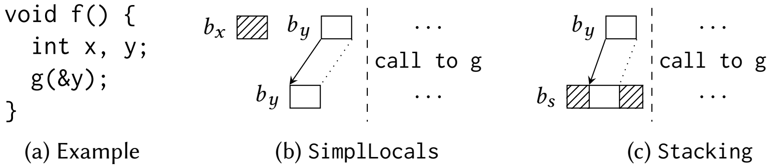
$$\begin{aligned}
&\mathtt{pub\text{-}src\text{-}mem}(j) &&= \{(b, o) \mid j(b) \neq \emptyset\}; \\
&\mathtt{pub\text{-}tgt\text{-}mem}(j, m_1) &&= \{(b, o) \mid \exists b'\ o', j(b') = \lfloor (b, o') \rfloor \land (b', o - o') \in \mathtt{perm}(m_1, \mathtt{Nonempty})\}.
\end{aligned}$$

By definition, a cell (b, o) is public in the source memory if it is in the domain of injection, and (b, o) is public in the target memory if it is mapped from some valid public source memory. With this definition and preservation of pointer values enforced by memory injection, we can easily prove the following property:

Lemma B.2. *Given $m_1 \hookrightarrow^j_m m_2$,*

$$\begin{aligned}
&\forall\, b_1\ o_1,\ (b_1, o_1) \in \mathtt{pub\text{-}src\text{-}mem}(j) \Rightarrow (b_1, o_1) \in \mathtt{perm}(m_1, \mathtt{Readable}) \Rightarrow \\
&\qquad m_1[b_1, o_1] = \mathtt{Vptr}(b'_1, o'_1) \Rightarrow (b'_1, o'_1) \in \mathtt{pub\text{-}src\text{-}mem}(j).
\end{aligned}$$

That is, access of pointers in a readable and public source location gets back another public location. This property implies that readable public memory regions form a “closure” such that the sequences of reads are bounded inside these regions, as shown in Fig. 17. Here, the horizontal arrows indicates a pointer (b_{i+1}, o_{i+1}) is obtained from reading the in-memory value at (b_i, o_i) with possible adjustment using pointer arithmetic. Note that all memory cells at (b_i, o_i)s and (b'_i, o'_i)s



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

(a) Example (b) SimplLocals (c) Stacking

Fig. 18. Protection of Private Memory by injp

have at least Readable permission. By Lemma B.2, (b_i, o_i)s are all in public regions. The mirroring reads (b'_i, o'_i)s at the target level are also in public regions by definition.

B.2 Uniform Rely-Guarantee Conditions via injp

We need to show that injp is both a reasonable guarantee condition and a reasonable rely condition for the compiler passes in CompCert.

B.2.1 injp *as a Guarantee Condition.* Given any source and target programs of a compiler pass in CompCert, we show that their execution between initial queries and the final replies respects injp. The critical point is that the initially unmapped and out-of-reach regions are not modified by internal execution. We argue by using an open simulation $[[M_1]] \leqslant_{\mathtt{c}_{\mathtt{injp}} \twoheadrightarrow \mathtt{c}_{\mathtt{injp}}} [[M_2]]$ between C modules M_1 and M_2; note that the same argument applies to other stages of compilation.

During the forward simulation, assume M_1 and M_2 takes incoming queries $v_{f_1}[sg](\vec{v}_1)@m_1$ and $v_{f_2}[sg](\vec{v}_2)@m_2$, respectively. By definition, all incoming values and memories are related by some initial injection j (i.e., $v_{f_1} \hookrightarrow^j_v v_{f_2}$, $\vec{v}_1 \hookrightarrow^j_v \vec{v}_2$ and $m_1 \hookrightarrow^j_m m_2$). In particular, the pointers in them are related by j (e.g., $v_{f_1} = \mathtt{Vptr}(b_1, o_1)$, $j(b_1) = \lfloor (b_2, o'_1) \rfloor$ and $v_{f_2} = \mathtt{Vptr}(b_2, o_1 + o'_1)$). Therefore, any sequence of reads starting from pointers stored in the arguments of queries only inspect public memories in the source and target, as already shown in Fig. 17. Note that by definition:

$$
\begin{aligned}
(b, o) \in \mathtt{pub\text{-}src\text{-}mem}(j) \quad & \Leftrightarrow (b, o) \notin \mathtt{unmapped}(j) \\
(b, o) \in \mathtt{pub\text{-}tgt\text{-}mem}(j, m) & \Leftrightarrow (b, o) \notin \mathtt{out\text{-}of\text{-}reach}(j, m)
\end{aligned}
$$

That is, if only public memories are inspected or modified, then any value in the unmapped or out-of-reach regions of the initial memory is *not modified* by memory protection of injp.

Finally, M_1 and M_2 themselves may perform external calls that may modify memory. However, because the outgoing calls have injp as a rely-condition and injections only get bigger but never change in values injection Fig. 8, 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 internal execution.

B.2.2 injp *as a Rely Condition.* In fact, the conditions in injp are exactly part of CompCert's assumptions on external calls [Leroy 2023]. That is, unmapped source memory and out-of-reach target memory contain exactly the private data we would like to protect across external calls. We show that injp provides adequate memory protection for preventing external calls from interfering with internal execution by inspecting two compiler passes. Protection for the remaining compiler passes follows a similar pattern. We shall use the code in Fig. 18a as an example where g is an external function.

The first pass is called SimplLocals which turns local variables whose memory addresses are not taken from in-memory variables to temporary ones. As shown in Fig. 18b, before SimplLocals, both x and y are allocated in memory. After SimplLocals, x is turned into a temporary variable. The injection j between source and target then projects x out (i.e., $j(b_x) = \emptyset$). It is critical to prevent g from modifying value in x at the source level, which may break the simulation as x is not visible at the target level. We note that b_x is unmapped by j, thereby protected by injp by default.

The second pass is called `Stacking` which lays out the structure of concrete stack frames. Before `Stacking` a stack frame only contains stack-allocated data. After it the frame is expanded with the return address, spilled registers, arguments, etc. Those new locations are private to the function and should not be modified by external calls. Continuing with our example as shown in Fig. 18c, the only stack-allocated data is y. Therefore, the injection j for `Stacking` is defined as $j(b_y) = \lfloor (b_s, o) \rfloor$ where b_s is the concrete stack frame and o is the offset at which y reside in b_s. Since the image of stack-allocated data is disjoint from private data, all private data is out-of-reach in the target memory, thereby protected by `injp` (cannot be modified by calls to `g`).

Finally, our running example in Fig. 8 demonstrates how `injp` protects memory of heterogeneous modules which may not even be compiled. When `client.c` calls `encrypt` in `server.s`, it assumes `encrypt` will not modify $b_{\mathtt{i}}$ and b_{RSP_1} as they are unmapped or out-of-reach, so that the simulation still holds after the call returns. Similarly, when `server.s` performs the callback to `client.c`, it assumes anything in its stack frame except for the stack-allocated data 33 is not modified. Here, the injection is derived from the direct refinement, not from compilation. Nevertheless, the protection provided by `injp` still suffices for proving the open simulation.

C TRANSITIVITY OF injp

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

We have used a simplified version of definitions of `perm`, $\hookrightarrow_m$ and $\rightsquigarrow_{\mathtt{injp}}$ in Sec. 3. To present a more detailed proof of the KMR with memory protection (`injp`), we present full definitions of `perm` and $\rightsquigarrow_{\mathtt{injp}}$. 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 $\mathtt{perm}_{\mathtt{cur}}(m, p) \subseteq \mathtt{perm}_{\mathtt{max}}(m, p)$. 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:

$\mathtt{max\text{-}perm\text{-}dec}(m_1, m_2) \Leftrightarrow$
$\quad \forall\ b\ o\ p,\ b \in m_1 \Rightarrow (b, o) \in \mathtt{perm}_{\mathtt{max}}(m_2, p) \Rightarrow (b, o) \in \mathtt{perm}_{\mathtt{max}}(m_1, p)$

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

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

have the same permission or does not have any permission *)
(6) $\forall\ b_1\ o_1\ b_2\ o_2\ k\ p,\ \ j(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \Rightarrow (b_2, o_2) \in \mathtt{perm}_k(m_2, p)$
$\Rightarrow (b_1, o_1) \in \mathtt{perm}_k(m_1, p) \lor (b_1, o_1) \notin \mathtt{perm}_{\mathtt{max}}(m_1, \mathtt{Nonempty})$

Definition C.2. Fefinition of memory accessibility `mem-acc`.

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

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 $m_1 \hookrightarrow^{j}_{m} m_2$, 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 C.3. Accessibility relation of `injp`

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

C.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 C.4. *Given $m_1 \hookrightarrow^{j_{12}}_{m} m_2$ and $m_2 \hookrightarrow^{j_{23}}_{m} m_3$, we have*

$$m_1 \hookrightarrow^{j_{23} \cdot j_{12}}_{m} m_3$$

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

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

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

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 C.1, we know that $m_1[b_1, o_1] \hookrightarrow^{j_{23} \cdot j_{12}}_{v} m_3[b_3, o_3]$. 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 $\mathtt{Vundef} \hookrightarrow^{j_{12}}_{v} \mathtt{Vundef} \land \mathtt{Vundef} \hookrightarrow^{j_{23}}_{v} m_3[b_3, o_3]$ 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 C.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 $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$, 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 $(b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$. If $b_2 = b_2'$, from $(b_2, o_2) \in \texttt{out-of-reach}(j_{12}, m_1)$ we can directly prove $(b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$.

If $b_2 \neq b_2'$, we assume that $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$, by property (1) of $m_1 \hookrightarrow_m^{j_{12}} m_2$ we get $(b_2', o_2') \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$. 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 $(b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$. □

C.3 Proof of Lemma 3.1

Based on definitions and lemmas before, we prove Lemma 3.1 in this section:

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

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 C.4 we can prove $m_1 \hookrightarrow_m^{j_{13}} m_3$. After the external call, given $(j_{13}, m_1, m_3) \rightsquigarrow_{\texttt{injp}} (j_{13}', m_1', m_3')$ 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. C.3.1. Then the proof reduce to prove $m_1' \hookrightarrow_m^{j_{12}'} m_2'$, $m_2' \hookrightarrow_m^{j_{23}'} m_3'$, $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j_{12}', m_1', m_2')$ and $(j_{23}, m_2, m_3) \rightsquigarrow_{\texttt{injp}} (j_{23}', m_2', m_3')$, they are proved in Sec. C.3.2

C.3.1 Construction and properties of j_{12}', j_{23}' and m_2'.

Definition C.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 $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1', \texttt{Nonempty})$ 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 C.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. 12b. 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

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

where $\texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$ 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$(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$ 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 $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$.

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 $\texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$ to find whether there exists a corresponding position $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$ 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 C.7 as follows.

Lemma C.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 C.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 $\exists b_1, j_{12}(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \wedge (b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$ 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 C.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 C.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 C.12.

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

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

C.3.2 Proof of remaining formulas. Recall that we are still proving Lemma 3.1, 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 C.13. $m_1' \hookrightarrow_m^{j_{12}'} m_2'$

Proof. We check the properties in Definition C.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 $\texttt{perm}_k(m_1', p) \subseteq \texttt{perm}_{\texttt{max}}(m_1', \texttt{Nonempty})$, we know $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1', \texttt{Nonempty})$ 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 C.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 $(j_{13}, m_1, m_3) \leadsto_{\texttt{injp}} (j_{13}', m_1', m_3')$, 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 $j_{12}'(b_1) = \lfloor(b_2, o_2 - o_1)\rfloor \wedge (b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1', \texttt{Nonempty})$ and $j_{12}'(b_1') = \lfloor(b_2', o_2' - o_1')\rfloor \wedge (b_1', o_1') \in \texttt{perm}_{\texttt{max}}(m_1', \texttt{Nonempty})$ 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 $(b_1, o_1) \in \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$

and $(b'_1, o'_1) \in \mathtt{perm}_{\mathtt{max}}(m_1, \mathsf{Nonempty})$. This follows from the $\mathtt{max\text{-}perm\text{-}dec}(m_1, m'_1)$ invariant in $(j_{13}, m_1, m_3) \leadsto_{\mathtt{injp}} (j'_{13}, m'_1, m'_3)$.

(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 $(b_1, o_1) \notin \mathtt{perm}_{\mathtt{max}}(m'_1, \mathsf{Nonempty})$ 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 $(b_1, o_1) \in \mathtt{perm}_k(m_1, p) \vee (b_1, o_1) \notin \mathtt{perm}_{\mathtt{max}}(m_1, \mathsf{Nonempty})$ by property (6) of $m_1 \hookrightarrow_m^{j_{12}} m_2$. Finally $(b_1, o_1) \in \mathtt{perm}_k(m'_1, p) \vee (b_1, o_1) \notin \mathtt{perm}_{\mathtt{max}}(m'_1, \mathsf{Nonempty})$ 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 $(b_1, o_1) \in \mathtt{perm}_{\mathtt{max}}(m'_1, \mathsf{Nonempty})$(otherwise the conclusion holds trivially), by $\mathtt{max\text{-}perm\text{-}dec}(m_1, m'_1)$ we can derive that $(b_1, o_1) \in \mathtt{perm}_{\mathtt{max}}(m_1, \mathsf{Nonempty})$. 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 C.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 C.9 we get $(b_2, o_2) \in \mathtt{unchanged\text{-}on}(m_2, m'_2)$ 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 C.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 C.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 $j'_{23}(b_2) = \lfloor (b_3, o_3 - o_2) \rfloor \wedge (b_2, o_2) \in \mathtt{perm}_{\mathtt{max}}(m'_2, \mathsf{Nonempty})$ and $j'_{23}(b'_2) = \lfloor (b'_3, o'_3 - o'_2) \rfloor \wedge (b'_2, o'_2) \in \mathtt{perm}_{\mathtt{max}}(m'_2, \mathsf{Nonempty})$ 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 $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$ and $(b'_2, o'_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$. This follows from $\texttt{max-perm-dec}(m_2, m'_2)$ (Lemma C.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 $(b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m'_2, \texttt{Nonempty})$ 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 $(b_1, o_1) \in \texttt{perm}_k(m'_1, p) \vee (b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m'_1, \texttt{Nonempty})$, therefore $(b_2, o_2) \in \texttt{perm}_k(m'_2, p) \vee (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m'_2, \texttt{Nonempty})$.
- 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 C.9). If $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m'_2, \texttt{Nonempty})$(otherwise the conclusion holds trivially), then $(b_2, o_2) \in \texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$ holds ($\texttt{max-perm-dec}(m_2, m'_2)$). According to Lemma C.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 $(b_2, o_2) \in \texttt{perm}_k(m_2, p) \vee (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$ by property (6) of $m_2 \hookrightarrow_m^{j_{23}} m_3$. Finally we can prove that
  $$(b_2, o_2) \in \texttt{perm}_k(m'_2, p) \vee (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m'_2, \texttt{Nonempty}).$$
  - 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
  $$(b_2, o_2) \in \texttt{perm}_k(m'_2, p) \vee (b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m'_2, \texttt{Nonempty})$$

□

Lemma C.15. $(j_{12}, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j'_{12}, m'_1, m'_2)$

Proof. According to Definition C.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 C.8, Lemma C.9 and Lemma C.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 C.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.

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

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 $(b_2, o_2) \notin \texttt{perm}_{\texttt{max}}(m_2, \texttt{Nonempty})$. By property (1) of $m_1 \hookrightarrow_m^{j_{12}} m_2$, we can get $(b_1, o_1) \notin \texttt{perm}_{\texttt{max}}(m_1, \texttt{Nonempty})$. Therefore $(b_3, o_3) \in \texttt{out-of-reach}(j_{23} \cdot j_{12}, m_1)$. □

C.4 Proof of Lemma 3.2

We prove Lemma 3.2 in this section:

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

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.

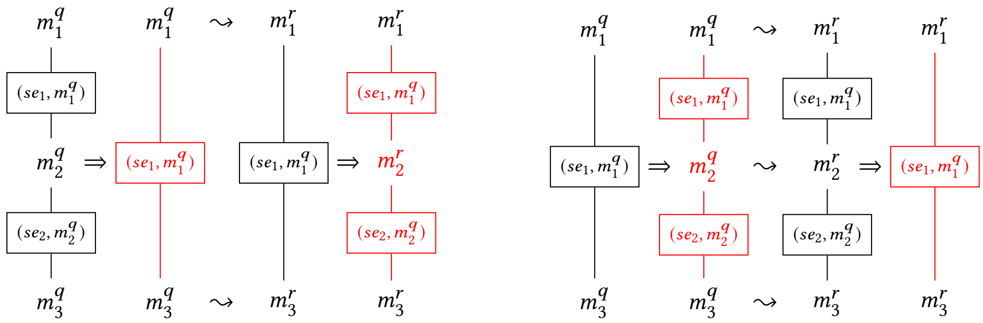
(4) Given $j_{12}(b_1) = \lfloor (b_2, \delta) \rfloor$, we know that $j_{13}(b_1) \neq \emptyset$. Therefore $b_1 \in m_1$ by $m_1 \hookrightarrow_m^{j_{13}} m_3$. Since $b_1 = b_2$, $b_2 \in m_1$.

(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 C.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. $j_{13} \subseteq j'_{13}$.



(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. 19. Transitivity of $\texttt{ro} \cdot \texttt{c}_{\texttt{injp}}$

(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
$$j_{12}(b_1) = \emptyset \text{ and } \exists b_2, j_{12}'(b_1) = \lfloor (b_2, o_2 - o_1) \rfloor \wedge j_{23}'(b_2) = \lfloor (b_3, o_3 - o_2) \rfloor$$
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 $m_2 \xhookrightarrow{j_{23}}_m m_3$ we can derive that $j_{23}(b_2) = \emptyset$. Finally we get $b_3 \notin m_3$ by $\texttt{inject-sep}(j_{23}, j_{23}', m_2, m_3)$.

□

D TRANSITIVITY OF ro · injp

The following is the proof for Lemma 4.6.

Proof. Since $\texttt{ro}$ is an invariant of source queries and replies, the proof follows the same pattern and construction of memory states as $\texttt{c}_{\texttt{injp}} \equiv \texttt{c}_{\texttt{injp}} \cdot \texttt{c}_{\texttt{injp}}$ which follows directly from the transitivity of $\texttt{injp}$. The desired properties about $\texttt{ro}$ in the proof here are presented in Fig. 19 where black and red symbols are assumptions and conclusions, respectively. Note that the world of $\texttt{ro}$ does not evolve as $\texttt{injp}$. $\rightsquigarrow$ stands for the $\texttt{mem-acc}$ relation between memories.

For the $\sqsubseteq$ side (Fig. 19a), we are given that $\texttt{ro-valid}(se_1, m_1^q)$ and $\texttt{ro-valid}(se_2, m_2^q)$ according to $\mathbb{R}_{\texttt{ro}}^q$ defined in Definition 4.2. Thus $\mathbb{R}_{\texttt{ro}}^q(w_{12})(m_1^q, m_3^q)$ where $w_{12} = (se_1, m_1^q)$ is trivially satisfied. For the $\mathbb{R}_{\texttt{ro}}^r$ for memories of replies, Note that the required properties $\texttt{mem-acc}(m_1^q, m_1^r)$ and $\texttt{mem-acc}(m_2^q, m_2^r)$ are included in the $\texttt{injp}$ accessibility from $\mathbb{R}_{\texttt{c}_{\texttt{injp}}}^r$ of the upper level. Consequently, we have proofed $\mathbb{R}_{\texttt{ro}}^r(w_{12})(m_1^r, m_2^r)$ and $\mathbb{R}_{\texttt{ro}}^r(w_{23})(m_2^r, m_3^r)$ where $w_{23} = (se_2, m_2^q)$.

For another side (Fig. 19b), it seems that the validity of m_2^q required by $\mathbb{R}^q_{\mathtt{ro}}$ is hard to prove. One can not derive it from the validity of m_1^q because of different symbol tables and the existence of value injections like $\mathtt{Vundef} \hookrightarrow_v^j v$. However, we take m_2^q as exactly m_1^q in the construction algorithm described in Lemma 3.2. The symbol table se_2 is also the same as se_1. As a result, this validity of m_2^q comes for free! The $\mathtt{mem\text{-}acc}(m_1^q, m_1^r)$ for $\mathbb{R}^r_{\mathtt{ro}}(w_{13})$ is given by $\mathbb{R}^r_{\mathtt{ro}}(w_{12})$.

From a higher perspective, the way we prove the transitivity of `injp` implies that the incoming memory is directly passed downside to each compilation pass as its initial source memory. Therefore, as long as the source program respects `ro`, each pass can assume that read-only variables are consistent with the symbol table throughout whole execution. This together with `injp` enable the optimizations using static analyzer in the middle of the compiler.

□

E DEFINITION OF THE KEY COMPONENT OF DIRECT REFINEMENT

The significant part of $\mathbb{C}$ is $\mathtt{CAinjp} : C \Leftrightarrow \mathcal{A}$ which directly relates source and target semantics. 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 accompanying Coq artifact for a complete definition.

Definition E.1. $\mathtt{CAinjp} : C \Leftrightarrow \mathcal{A} = \langle W_{\mathtt{CAinjp}}, \mathbb{R}^q_{\mathtt{CAinjp}}, \mathbb{R}^r_{\mathtt{CAinjp}} \rangle$ where $W_{\mathtt{CAinjp}} = (W_{\mathtt{injp}} \times \mathtt{sig} \times \mathtt{regset})$ and $\mathbb{R}^q_{\mathtt{CAinjp}} : \mathcal{K}_{W_{\mathtt{CAinjp}}}(C^q, \mathcal{A}^q)$ and $\mathbb{R}^r_{\mathtt{CAinjp}} : \mathcal{K}_{W_{\mathtt{CAinjp}}}(C^r, \mathcal{A}^r)$ are defined as:

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

  (1) $m_1 \hookrightarrow_m^j m_2, \quad v_f \hookrightarrow_v^j rs(\mathtt{PC}) \quad \vec{v} \hookrightarrow_v^j \mathtt{get\text{-}args}(sg, rs(\mathtt{RSP}), rs, m_2)$
  (2) $\mathtt{outgoing\text{-}arguments}(sg, rs(\mathtt{RSP})) \subseteq \mathtt{out\text{-}of\text{-}reach}(j, m_1)$
  (3) $\mathtt{outgoing\text{-}arguments}(sg, rs(\mathtt{RSP})) \subseteq \mathtt{perm}(m_2, \mathtt{Freeable})$

  $\mathtt{get\text{-}args}(sg, rs(\mathtt{RSP}), rs, m_2)$ 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. $\mathtt{outgoing\text{-}arguments}(sg, rs(\mathtt{RSP}))$ 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.
- $(r@m_1', rs'@m_2') \in \mathbb{R}^r_{\mathtt{CAinjp}}((j, m_1, m_2), sg, rs)$ if there is a j' s.t.

  (1) $(j, m_1, m_2) \leadsto_{\mathtt{injp}} (j', m_1', m_2')$
  (2) $m_1' \hookrightarrow_m^{j'} m_2', \quad r \hookrightarrow_v^{j'} \mathtt{get\text{-}result}(sg, rs')$
  (3) $\mathtt{outgoing\text{-}arguments}(sg, rs(\mathtt{RSP})) \subseteq \mathtt{out\text{-}of\text{-}reach}(j, m_1)$
  (4) $rs'(\mathtt{RSP}) = rs(\mathtt{RSP}), \quad rs'(\mathtt{PC}) = rs(\mathtt{RA}), \quad \forall r \in \mathtt{callee\text{-}save\text{-}regs}, rs'(r) = rs(r)$

  $\mathtt{get\text{-}result}(sg, rs')$ 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.

F REFINEMENT AT THE INCOMING SIDE

The original simulation conventions at the incoming side are parameterized by `inj` which does not have memory protection as in `injp`. One can modify the proofs of CompCert to make `injp` an incoming convention. However, we show that this is unnecessary: with the inserted self-simulations over `injp`, conventions over `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) $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
$\cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \cdot \mathtt{ltl}_{\mathtt{ext}} \cdot \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{inj}} \cdot \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}$

(2) $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{c}_{\mathtt{injp}} \cdot \mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$
$\cdot \mathtt{c}_{\mathtt{inj}} \cdot \mathtt{wt} \cdot \mathtt{c}_{\mathtt{ext}} \cdot \mathtt{CL} \cdot \mathtt{ltl}_{\mathtt{ext}} \cdot \mathtt{LM} \cdot \mathtt{mach}_{\mathtt{inj}} \cdot \mathtt{mach}_{\mathtt{ext}} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{inj}} \cdot \mathtt{asm}_{\mathtt{injp}}$

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

Steps (1-3) are the same as for the outgoing side except for using property (4) in Lemma 4.4. 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 4.3. In step (6), we absorb $\mathtt{asm}_{\mathtt{ext}}$ into $\mathtt{asm}_{\mathtt{inj}}$ by properties (5-7) in Lemma 4.4. 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 4.4). In step (8), we absorb $\mathtt{inj}$ into $\mathtt{injp}$ at both levels by property (3) in Lemma 4.4. In step (9), we eliminate a redundant $\mathtt{ro} \cdot \mathtt{c}_{\mathtt{injp}}$ by Lemma 4.6. The last two steps are the same as above.

G VERIFICATION OF THE ENCRYPTION SERVER AND CLIENT EXAMPLE

G.1 Refinement of the Hand-written Server

The following is the proof for Theorem 5.2.

Proof. At the top level, $\mathbb{C}$ is expanded to $\mathtt{ro} \cdot \mathtt{wt} \cdot \mathtt{CAinjp} \cdot \mathtt{asm}_{\mathtt{injp}}$. As the invariant $\mathtt{ro}$ and $\mathtt{wt}$ in C level are commutative, i.e., $\mathtt{ro} \cdot \mathtt{wt} \equiv \mathtt{wt} \cdot \mathtt{ro}$ as stated in Lemma 4.7, we can change their order in $\mathbb{C}$. By the vertical compositionality, we first prove $L_{\mathsf{S}} \leqslant_{\mathtt{wt}} L_{\mathsf{S}}$ and $[\![\mathtt{server\_opt.s}]\!] \leqslant_{\mathtt{asm}_{\mathtt{injp}}} [\![\mathtt{server\_opt.s}]\!]$, 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 $\mathtt{key}$, we need to use $\mathtt{ro}$ together with $\mathtt{CAinjp}$ to establish the simulation $L_{\mathsf{S}} \leqslant_{\mathtt{ro} \cdot \mathtt{CAinjp}} [\![\mathtt{server\_opt.s}]\!]$. Note that for the unoptimized version we can prove $L_{\mathsf{S}} \leqslant_{\mathtt{CAinjp}} [\![\mathtt{server.s}]\!]$ and prove $\mathtt{ro}$ using self simulation like $\mathtt{wt}$.

The key of this proof is to establish a relation $R \in \mathcal{K}_{W_{\mathtt{ro} \cdot \mathtt{CAinjp}}}(S_{\mathsf{S}}, \mathtt{regset} \times \mathtt{mem})$ satisfying the simulation diagram Fig. 16. Given $w \in W_{\mathtt{ro}} \times W_{\mathtt{CAinjp}} = ((se, m_0), ((j, m, tm), sg, rs))$, if $sg \neq \mathtt{int} \to \mathtt{ptr} \to \mathtt{void} \lor m_0 \neq m$ then $R(w) = \emptyset$. Assume $sg = \mathtt{int} \to \mathtt{ptr} \to \mathtt{void} \land m_0 = m$ (these conditions are provided by I of L_{S} and related incoming queries), then $R(w)$ is defined as follows:

(a) $(\mathtt{Calle}\ i\ \mathtt{Vptr}(b, o)\ m, (rs, tm)) \in R(w) \Leftrightarrow$ (* initial state *)
(a.1) $rs(\mathtt{RDI}) = i \land \mathtt{Vptr}(b, 0) \hookrightarrow_{v}^{j} rs(\mathtt{RSI}) \land rs(\mathtt{PC}) = \mathtt{Vptr}(b_e, 0) \land m \hookrightarrow_{m}^{j} tm \land \mathtt{ro\text{-}valid}(se, m)$
(b) $(\mathtt{Callp}\ sp\ \mathtt{Vptr}(b, o)\ m_1, (rs_1, tm_1)) \in R(w) \Leftrightarrow$ (* before external call *)
(b.1) $rs_1(\mathtt{RSP}) = \mathtt{Vptr}(b_s, 0) \land rs_1(\mathtt{RDI}) = \mathtt{Vptr}(b_s, 8) \land j'\ sp = \lfloor b_s, 8 \rfloor$
(b.2) $\land rs_1(\mathtt{RA}) = \mathtt{Vptr}(b_g, 5) \land m_1 \hookrightarrow_{m}^{j'} tm_1 \land \mathtt{Vptr}(b, o) \hookrightarrow_{v}^{j} rs_1(\mathtt{PC})$
(b.3) $\land \forall r, r \in \mathtt{callee\text{-}save\text{-}regs} \to rs_1(r) = rs(r)$
(b.4) $\land (j, m, tm) \leadsto_{\mathtt{injp}} (j', m_1, tm_1) \land \mathtt{ro\text{-}valid}(se, m_1)$
(b.5) $\land tm_1[b_s, 0] = rs(\mathtt{RSP}) \land tm_1[b_s, 16] = rs(\mathtt{RA})$

(b.6) $\quad \wedge\{(b_s, o) \mid 0 \le o < 8 \vee 16 \le o < 24\} \subseteq \texttt{out-of-reach}(j', m_1)$

(b.7) $\quad \wedge\{(b_s, o) \mid 0 \le o < 8 \vee 16 \le o < 24\} \subseteq \texttt{perm}_{\texttt{cur}}(tm_1, \texttt{Freeable})$

(c) $\quad (\texttt{Retp}\ sp\ m_2, (rs_2, tm_2)) \in R(w) \Leftrightarrow$ `(* after external call *)`

(c.1) $\quad rs_2(\texttt{RSP}) = \texttt{Vptr}(b_s, 0) \wedge j''\ sp = \lfloor b_s, 8 \rfloor$

(c.2) $\quad rs_2(\texttt{PC}) = (b_g, 5) \wedge m_2 \hookrightarrow_m^{j''} tm_2$

(c.3) $\quad \wedge \forall r, r \in \texttt{callee-save-regs} \to rs_2(r) = rs(r)$

(c.4) $\quad \wedge (j, m, tm) \leadsto_{\texttt{injp}} (j'', m_2, tm_2)$

(c.5) $\quad \wedge tm_2[b_s, 0] = rs(\texttt{RSP}) \wedge tm_2[b_s, 16] = rs(\texttt{RA})$

(c.6) $\quad \wedge\{(b_s, o) \mid 0 \le o < 8 \vee 16 \le o < 24\} \subseteq \texttt{out-of-reach}(j'', m_2)$

(c.7) $\quad \wedge\{(b_s, o) \mid 0 \le o < 8 \vee 16 \le o < 24\} \subseteq \texttt{perm}_{\texttt{cur}}(tm_2, \texttt{Freeable})$

(d) $\quad (\texttt{Rete}\ m_3, (rs_3, tm_3)) \in R(w) \Leftrightarrow$ `(* final state *)`

(d.1) $\quad rs_3(\texttt{RSP}) = rs(\texttt{RSP}) \wedge rs_3(\texttt{PC}) = rs(\texttt{RA}) \wedge m_3 \hookrightarrow_m^{j''} tm_3$

(d.2) $\quad \wedge \forall r, r \in \texttt{callee-save-regs} \to rs_3(r) = rs(r)$

(d.3) $\quad \wedge (j, m, tm) \leadsto_{\texttt{injp}} (j'', m_3, tm_3)$

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. 8. (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. 16. 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

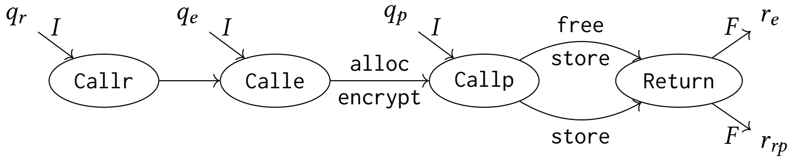


Fig. 20. The Top-level Specification $L_{\mathtt{CS}}$

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 $\mathbb{R}^r_{\mathtt{CAinjp}}$. $rs_2(\mathtt{PC}) = (b_g, 5)$ in (c.2) is derived from $rs_1(\mathtt{RA}) = (b_g, 5)$ in (b.2) via the relation between PC and RA stated in $\mathbb{R}^r_{\mathtt{CAinjp}}$. After the external call, condition (d) can be derived from (c) by following internal execution. Since $L_{\mathtt{S}}$ frees sp, $[\![\mathtt{server\_opt.s}]\!]$ 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 and other properties needed by $\mathbb{R}^r_{\mathtt{CAinjp}}$. The `injp` accessibility also implies $\mathtt{mem\text{-}acc}(m, m_3)$ for $\mathbb{R}^r_{\mathtt{ro}}$. Therefore, we are able to establish the guarantee condition and prove that $L_{\mathtt{S}} \leqslant_{\mathbb{C}} [\![\mathtt{server\_opt.s}]\!]$. □

G.2 End-to-end Correctness Theorem

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

Definition G.1. LTS of $L_{\mathtt{CS}}$:

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

There are four internal states in $L_{\mathtt{CS}}$ as depicted in its transition diagram Fig. 20, 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 $L_{\mathtt{CS}}$ 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 $L_{\mathtt{CS}}$ can only be called but cannot perform external calls.

The remaining proof follows Sec. 5. 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 $L_{\mathtt{S}}$ does not mark `key` as read-only, and the simulation

```
/* 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. 21. Heterogeneous Sum with Mutual Recursion

invariant for Theorem 5.2 does not contain ro-valid conditions as they play no role without optimizations.

H 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. 21. 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 → 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.

$$\begin{tikzcd}
 & \boxed{L_{CA}} \arrow[d, phantom, sloped, "\leqslant_{\mathbb{K}}"] & \\
L_C \arrow[d, phantom, sloped, "\leqslant_{\mathbb{K}}"] & \oplus & L_A \arrow[dd, phantom, sloped, "\leqslant_{\mathbb{C}}"] \\
\llbracket M_C \rrbracket \arrow[d, phantom, sloped, "\leqslant_{\mathbb{C}}"] & & \\
\llbracket \texttt{CompCert}(M_C) \rrbracket \arrow[uu, bend left=60, "\leqslant_{\mathbb{C}}"] & \oplus \arrow[d, phantom, sloped, "\leqslant_{\texttt{id}}"] & \llbracket M_A \rrbracket \\
 & \boxed{\llbracket \texttt{CompCert}(M_C) + M_A \rrbracket} \arrow[uuuu, bend right=60, "\leqslant_{\mathbb{C}}"'] &
\end{tikzcd}$$

Fig. 22. Verification of the Mutual Sum ($\mathbb{K} := \texttt{ro} \cdot \texttt{wt} \cdot \texttt{c}_{\texttt{injp}}$)

The outline of the verification is presented in Fig. 22. 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 H.1 and prove the simulation between L_A and $\llbracket M_A \rrbracket$ which is declared in Theorem H.2. Secondly, we 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 H.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 H.3) and prove $L_C \leqslant_{\texttt{ro}\cdot\texttt{wt}\cdot\texttt{c}_{\texttt{injp}}} \llbracket M_C \rrbracket$ (in Theorem H.4). We can compose this proof with the compiler correctness by utilizing Theorem 5.6 to prove $L_C \leqslant_{\mathbb{C}} \llbracket \texttt{CompCert}(M_C) \rrbracket$. With L_C, it is simpler to prove the source refinement declared in Theorem H.6. Finally, we combine these proofs to obtain the single refinement between top-level specification and the target linked program as declared in Theorem H.7.

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

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

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. 21, 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 H.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 A.2. Given $w \in W_{\texttt{CAinjp}} = ((j, m_1, m_2), sg, rs)$, if $sg \neq \texttt{int} \rightarrow \texttt{int}$ then $R(w) = \emptyset$. Assume $sg = \texttt{int} \rightarrow \texttt{int}$, then $R(w)$ is defined as follows:

(a) $(\texttt{Callg}\ i\ m_1, (rs, m_2)) \in R(w) \Leftrightarrow$ `(* initial state *)`

(a.1) $rs(\texttt{RDI}) = i \wedge rs(\texttt{PC}) = \texttt{Vptr}(b_g, 0) \wedge m_1 \hookrightarrow_m^{j} m_2$

(b) $(\texttt{Callf}\ v_f\ i\ m_1', (rs', m_2')) \in R(w) \Leftrightarrow$ `(* before external call *)`

(b.1) $rs'(rbx) = i \wedge rs'(\texttt{RA}) = \texttt{Vptr}(b_g, 13) \wedge m_1' \hookrightarrow_m^{j'} m_2' \wedge v_f \hookrightarrow_v^{j'} rs'(\texttt{PC})$

(b.2) $\wedge \forall r, (r \in \texttt{callee-saved-regs} \wedge r \neq \texttt{RBX}) \longrightarrow rs'(r) = rs(r)$

(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) $\wedge (j, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j', m_1', m_2')$

(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) $rs'(\texttt{RBX}) = i \wedge rs'(\texttt{PC}) = (b_g, 13) \wedge rs'(rax) = res \wedge m_1' \hookrightarrow_m^{j'} m_2'$

(c.2) $\wedge \forall r, (r \in \texttt{callee-saved-regs} \wedge r \neq \texttt{RBX}) \longrightarrow rs'(r) = rs(r)$

(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) $\wedge (j, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j', m_1', m_2')$

(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) $rs'(\texttt{RAX}) = res \wedge rs'(\texttt{RSP}) = rs(\texttt{RSP}) \wedge rs'(\texttt{PC}) = rs(\texttt{RA}) \wedge m_1' \hookrightarrow_m^{j'} m_2'$

(d.2) $\wedge \forall r, r \in \texttt{callee-saved-regs} \longrightarrow rs'(r) = rs(r)$

(d.3) $\wedge (j, m_1, m_2) \rightsquigarrow_{\texttt{injp}} (j', m_1', m_2')$

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. 21);

(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. 21 (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 E.1, 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 H.3. The C-level specification L_C is defined as follows:

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

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

$$\begin{aligned}
S_T \;&:= \{\texttt{Callf}\ i\ m\} \cup \{\texttt{Callg}\ i\ m\} \cup \{\texttt{Return}\ i\ m\};\\
I_T \;&:= \{(\texttt{Vptr}(b_f, 0)[\texttt{int} \rightarrow \texttt{int}]([i])@m), (\texttt{Callf}\ i\ m)\} \cup\\
&\quad\; \{(\texttt{Vptr}(b_g, 0)[\texttt{int} \rightarrow \texttt{int}]([i])@m), (\texttt{Callg}\ i\ m)\};\\
\rightarrow_T &:= \{(\texttt{Callf}\ i\ m, \texttt{Return}\ r\ m') \mid r = sum(i, m), m' = cache(i, m)\} \cup\\
&\quad\; \{(\texttt{Callg}\ i\ m, \texttt{Return}\ r\ m') \mid r = sum(i, m), m' = cache(i, m)\};\\
F_T \;&:= \{(\texttt{Return}\ r\ m, r@m))\};
\end{aligned}$$

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 H.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.

Table 3. Statistics of Our Development in Coq

Files	CompCertO	This work	Additions(+)
Maps.v	1647	1850	203
Memory.v	4382	5850	1468
InjectFootprint.v	325	2417	2092
SimplLocalsproof.v	2006	2585	579
ValueAnalysis.v	1926	2304	378
Deadcodeproof.v	1036	1722	686
Constpropproof.v	515	1045	530
CSEproof.v	1121	1594	473
Unusedglobproof.v	1271	1582	311
CA.v	(New)	516	516
Callconv.v	1057	1638	581
Compiler.v	639	735	96
Client-Server	(New)	7329	7329
Mutual Sum	(New)	3128	3128
Total	15925	34295	18370

Theorem H.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 5.6. The former one is proved in Theorem H.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 H.2. The verification of $L_C \leqslant_{\mathbb{C}} \texttt{CompCert}(M_C)$ is proved by applying Lemma 5.6, Theorem H.4 and the compiler correctness theorem. □

I EVALUATION

Our framework is built on top of the a recent version of CompCertO which is in turn based on CompCert v3.10. The statistics for our development relative to CompCertO is shown in Table 3 in which we only list files that were modified or newly introduced. Column 2 and 3 show the lines of code (LOC) for every file (counted by using `coqwc`) in the original CompCertO and in our updated version, respectively. Column 4 shows the LOC that were added in the updated version. Note that most files were extended without much modification to the existing code, except for `Memory.v`, `Compiler.v` and `SimplLocalsproof.v`.

The most significant proof effort is for proving the transitivity of `injp` discussed in Sec. 3.2, which is summarized in rows 2-4. A technical detail is that the memory permission in CompCert was originally represented as a function from blocks and offsets to permissions. However, the domain of this function (footprint of permissions in memory) is not known, which is critical for construction of interpolating states. Therefore, we have changed the functional representation of permission into a tree-like map from which we can extract the footprint of permissions. These changes are made in `Maps.v` and `Memory.v`. The main proof of transitivity is in `InjectFootprint.v` with relevant low-level memory properties implemented in `Memory.v`. Total LOC for this part is about 2.5k.

To test if `injp` can indeed serve as a guarantee-condition for compiler passes as discussed in Sec. 3.1. We have experimented with `SimplLocals` by modifying its simulation to be $[\![p]\!] \leqslant_{\texttt{c}_{\texttt{injp}}} [\![p']\!]$ where p and p' are source and target programs. We have proved this new simulation with a moderate amount of work as shown in row 5 which reaffirms the uniformity of `injp`. We have defined `ro` in `ValueAnalysis.v` and repaired the proof of three optimizing pass using $\texttt{ro}\cdot\texttt{c}_{\texttt{injp}}$. We also have fixed the Unusedglob pass. The amount of these works are shown in rows 6-10. Note that the LoC of Unusedglobproof.v is from vanilla CompCert 3.10 as CompCertO does not support it.

The effort for unifying interfaces as described in Sec. 4 is shown in rows 11-13. We have added about 500 LOC for defining CAinjp and proving $\texttt{CAinjp} \equiv \texttt{c}_{\texttt{injp}} \cdot \texttt{CL} \cdot \texttt{LM} \cdot \texttt{MA}$ in CA.v. We have also added 633 LOC in Callconv.v and Compiler.v to unify the simulation conventions of CompCertO.

The effort for developing our Client-Server examples is 4631 LoC as shown in row 14. About $3k$ LoC are used to verify the running example (with and without optimization). Remaining parts are for the more complicate client with mutual recursion discussed in Sec. 5 (the server is reused). To get a rough idea of the difference in proof effort between our approach and CompCertM. We develop the mutual recursive summation example which needs a total of 3124 LoC (880 spec + 2244 proof) to verify the end-to-end refinement between top-level specification and the target assembly as shown in row 15. By comparison, CompCertM uses 5764 LoC (1550 spec + 4214 proof) to develop the example (we count all the Coq files in directory demo/mutrec in the CompCertM artifact[3]). Note that CompCertM's example only make use of source-level RUSC relations and have not proved self-simulation for RUSC relations derived from compiler passes. So their proof is in fact incomplete as an end-to-end open refinement. It indicates that our approach may require less effort to achieve preservation of open semantics. Furthermore, our examples employ little automation where the properties of assembly instructions (about 160 of them) are proved instruction-by-instruction. With better automation the proof effort can be significantly reduced.

From the above discussion, we can see that our framework piggybacks on the existing proofs of CompCertO and is therefore fairly lightweight. The novel technical contribution of this work is to discover injp as a uniform and composable interface, fully formalize it in Coq and utilize it in VCC. The examples show potential for our approach to be applicable to verify realistic open libraries which would be valuable for a wide range of verification projects.

J FRAMEWORKS FOR COMPOSITIONAL PROGRAM VERIFICATION

Researchers have proposed frameworks for compositional program verification based on novel semantics [Sammler et al. 2023; Xia et al. 2019] and *separation logics* [Song et al. 2023]. 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. However, the languages used in DimSum are very simple with primitive memory models. Compilation of these languages are also trivial, without any complex optimizations. Therefore, it is unclear if their framework can scale to realistic languages or compilers. 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.

[3] https://github.com/snu-sf/CompCertM/tree/v3.6_stable/demo/mutrec

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. Since the horizontal composition of two refinements requires specific knowledge of specifications of each other to control interaction, CCR can be thought as having closed assumptions on programs. It is interesting to investigate if the program specific conditions imposed by CCR can be handled or piggybacked upon our open framework.

K 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 compose the degree of openness of the result of final theorem 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.

K.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 with Sec. H.

Their open simulations are parameterized by different *memory relations* which mirrors 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 $\mathtt{Beh}(c \oplus p) \supseteq \mathtt{Beh}(c \oplus p')$. Note that the behavior $\mathtt{Beh()}$ 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, i.e. the closed-world restriction is exactly the fixed $\mathcal{R}$ and programs 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 ours depicted in Fig. 22. 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

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

Note that the verification here is slightly different with ours. They memory relations in $\mathcal{R}_e$ here include specific semantics invariant which ensures that the variables `memorized1` and `memorized2` have desired values in the incoming memories. But `static` variables can be changed by previous executions of the module. In other words, they describe and verify the behavior of the program in an ideal memory environment, i.e. the program always returns the correct summation for input i. This can be viewed as another kind of closed world assumption. 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 H.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 $\mathtt{CompCert}(M_C)$, then the correctness of CompCertM states that $\llbracket M_C \rrbracket \succcurlyeq_{\mathcal{R}_c} \llbracket \mathtt{CompCert}(M_C) \rrbracket$ The adequacy property for linking assembly modules is stated as $\mathtt{Beh}(\llbracket \mathtt{CompCert}(M_C) \rrbracket \oplus \llbracket M_A \rrbracket) \supseteq \mathtt{Beh}(\llbracket \mathtt{CompCert}(M_C) \rrbracket + \llbracket M_A \rrbracket)$ There are two approaches to the end-to-end semantics preservation. Note that these two approaches are speculative because CompCertM did not attempt to compose them.

Firstly, we can compose the three parts vertically in the form of *behavior refinement*. However, this approach only makes sense when the composed module is a closed program.

$$\mathtt{Beh}(L_{CA}) \supseteq \mathtt{Beh}(\llbracket \mathtt{CompCert}(M_C) \rrbracket + \llbracket M_A \rrbracket)$$

Since the behavior refinement is transitively composable, we need to show $\mathtt{Beh}(\llbracket M_C \oplus M_A \rrbracket) \supseteq \mathtt{Beh}(\llbracket \mathtt{CompCert}(M_C) \rrbracket \oplus \llbracket M_A \rrbracket)$. According to the definition of $\succcurlyeq_{\mathcal{R}_c}$, it suffices to prove that $\llbracket M_A \rrbracket$ 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, it is unreasonable 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

$$L_{CA} \succcurlyeq_{\mathcal{R}_e \cup \mathcal{R}_c} \llbracket \mathtt{CompCert}(M_C) \rrbracket \oplus \llbracket M_A \rrbracket$$

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)* $\llbracket \mathtt{CompCert}(M_C) \rrbracket$ and $\llbracket M_A \rrbracket$ 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. This highlights the limitations imposed by the closed-world assumption introduced in RUSC, which can increase the difficulty of the proofs and reduce the extensibility of the proof results. Our direct refinement approach overcomes these obstacles.

K.2 CompCertO

In CompCertO, the simulation convention of the overall simulation for the compiler is stated as $\mathbb{C}_{\mathtt{CCO}} = \mathcal{R}^* \cdot \mathtt{wt} \cdot \mathtt{CL} \cdot \mathtt{LM} \cdot \mathtt{MA} \cdot \mathtt{asm}_{\mathtt{vainj}}$ 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 set of simulation conventions parameterized over used KMRs similar as 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 $\mathbb{C}_{\mathtt{CCO}}$ similar as what we do in Sec. 5.

As discussed in Sec. 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_S using $\mathbb{C}_\mathsf{CCO}$.

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

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

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 Sec. 4.1. 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 $L_\mathcal{M} \leqslant_\mathsf{MA} [[\mathtt{server.s}]]$. 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. 8, we use `injp` together with the structural simulation convention $\mathsf{CA} \equiv \mathsf{CL} \cdot \mathsf{LM} \cdot \mathsf{MA}$. Specifically, the saved values of registers are protected as `out-of-reach` in the memory (`injp`) such that these registers can be correctly restored before return to satisfy the requirements of calling convention. In $\mathbb{C}_\mathsf{CCO}$, the rely-condition for callee-save registers is defined in LM, the rely-condition for RSP and RA is defined in MA. While they do not provide any memory protection for the saved values on the stack. This makes it extremely challenging to establish a simulation between L_S and $[[\mathtt{server.s}]]$ through intermediate specifications. In fact, we came up with the idea of direct refinement during our attempts to prove this.