Deductive program verification for a language with a Rust-like typing discipline
Xavier Denis

To cite this version:
Xavier Denis. Deductive program verification for a language with a Rust-like typing discipline. [Internship report] Université de Paris. 2020. hal-02962804

HAL Id: hal-02962804
https://hal.archives-ouvertes.fr/hal-02962804
Submitted on 9 Oct 2020

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

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Deductive program verification for a language with a Rust-like typing discipline

Xavier Denis 1

1 Université Paris-Saclay, CNRS, Inria, Laboratoire de recherche en informatique, 91405, Orsay, France.

October 8, 2020

Abstract

Deductive program verification seeks to eliminate bugs in software by translating programs annotated with specifications into logical formulas which are then solved using semi-automated tools. When verifying programs using a mutable heap, it is often required to show that pointers do not alias each other, ensuring there is only one way to modify structures in memory. This leads to cumbersome proof obligations and makes verification much more challenging. Newer languages like Rust feature pointers as well but prevent aliasing through the type system. This opens the door to simpler approaches to verification, free of tedious proof obligations.

We propose a technique for the verification of Rust programs by translation to a functional language. The challenge of this translation is the handling of mutable borrows, pointers with control of aliasing in a region of memory. To overcome this, we used a technique inspired by prophecy variables to predict the final values of borrows. The main contribution of this work is to prove this translation correct. We developed a proof-of-concept tool to show the viability of this approach.

1 Introduction

Over the past 50 years programming languages have made major strides, allowing programmers to reason about and abstract ever larger software projects. Yet, when performance and efficiency become concerns, they resort to low-level programming languages like C/C++ or even assembly. These languages offer control over memory and in particular allow unrestricted usage of pointers to build complex data structures and efficient algorithms. This power comes at a cost. Reasoning about the correctness of pointer programs is very tricky. The challenge is aliasing, when a value can be accessed through more than one name. When two variables are aliased, changing either also changes the other. This makes it difficult to reason about code because programmers must keep in mind all potential aliases to understand the state of their programs.

Languages like C which have pervasive aliasing make this incredibly challenging and it often is a source of bugs in software. For example, Figure 1 performs a swap using XOR to avoid allocating a temporary variable[3]. But there’s a bug! If the user provides the same pointer to both arguments, this function will write 0 to it instead. Aliasing and related issues like buffer overflows occur constantly, and cause many safety and correctness issues in C software.

In most programs, programmers make the implicit assumption that values are not aliased, but in C the compiler offers no help to verify this. When attempting to formally verify a C program, such aliasing assumptions must become explicit, and it can easily turn into a nightmare [5].
Many approaches exist in the literature to overcome aliasing issues in the formal verification of programs in C-like languages. This work takes another path: instead considering a language like Rust, which offers a strong type system to control aliasing.

1.1 The Rust Programming Language

The Rust programming language is a recent entry in the field of systems programming languages. Its 1.0 release, published in 2015\[2\] aims to “empower everyone to build reliable and efficient software”\[1\]. Rust provides memory-safety without requiring a garbage collector through its type system\[11\]. The type system uses a system of ownership to ensure that mutable references cannot alias. When the xorSwap program of Figure 1 is translated to Rust, as shown in Figure 2, the bug is no longer possible: a call to that function using the same argument twice will trigger a type checking error.

Ownership in Rust

In Rust every memory cell has a unique owner, which has exclusive read and write permissions. This is sufficient to program in Rust using a functional programming style. The program of Figure 3 illustrates this: it constructs a pair, and then increments the second component, not by mutation but by producing a new pair. But this style is limiting and more imperative programming style is desirable.

Borrows and Lifetimes

To perform memory mutation, Rust uses safe pointers called references that can borrow these permissions from their owner. But then aliasing arises and it is where the Rust-specific type system comes into play: such a borrow restricts the permission of the original owner for a limited period of time so that aliasing is controlled. When a reference is created it can come in one of two forms: either unique and mutable or shareable but immutable. The Rust compiler infers the lifetime of references after which the permissions are restored to the owner.

The program of Figure 4 illustrates this, exploiting the ownership and borrowing mechanisms of Rust. When x is mutably borrowed into y, it transfers its read and write permissions to y and so loses access to its own contents. The function inc, takes ownership of its argument, consuming
fn main() {
    let mut x = 0;
    let y = &mut x;
    inc(y);
    inc(y);
    assert_eq!(y, 2);
}

fn inc(x: &mut i32) {
    *x += 1;
}

Figure 4: Incrementing a reference twice

it, so Rust implicitly reborrows y before calling inc. Reborrowing consists in borrowing the permissions of a borrow for a shorter lifetime than the original borrow. This mechanism makes borrows flexible and intuitive to use, because after each call to inc, morally we should be allowed to use y again. During compilation Rust statically verifies that borrows are used correctly, inferring the lifetime of each borrow.

1.2 Verification

What does it mean for a program to be correct? A common answer is that the program should satisfy a logical specification. This specification encodes the properties expected of a program. For example, a specification of xor_swap could be that the values of x and y are exchanged. To verify that programs satisfy specifications many techniques can be used, from model checking[7], to dependent types[10] or deductive verification[9].

Deductive verification of programs works by translating a program and its specification into a collection of verification conditions such that their truth implies the program follows its specification. These verification conditions can be discharged using a variety of tools, though commonly, automated SMT solvers are used. This highly automated approach to program verification is appealing because it allows engineers to focus their attention on developing a specification rather than proving logical formulas.

Verification conditions can be generated by several techniques, including the weakest precondition calculus. This approach starts with the postcondition of a specification and asks what the weakest precondition that upholds the postcondition is. A rule is determined for each syntactic element of the language, and then recursively applied to translate a whole program to this logical form.

Deductive verification tools for languages with aliasing like C generate non-aliasing conditions[9] as part of the verification. By leveraging the ownership property of Rust programs, we can eliminate these conditions and simplify the verification conditions required to prove specifications true.

1.3 Contributions

We present a schema for the deductive verification of Rust programs by translation to a functional language. This translation handles both mutable and immutable borrows as well as owned pointers. This paper is structured in several sections, Section 2 presents μMIR, a fragment of Rust allowing only owned data. Using μMIR, we detail the type system which enforces ownership and its semantics. We then present a schema for the verification of μMIR and prove it correct.

The Section 3 section extends μMIR with mutable and immutable references into MiniMir. We explain how the introduction of references impacts the type system and semantics. Then we present a translation of MiniMir to a functional language with non-determinism and extend the proof of μMIR to handle references.
A basic language with ownership

Rust is a complex programming language, targeted at industrial use with a large syntax and underspecified operational semantics. During compilation, the Rust compiler translates programs into MIR, an intermediate language with a greatly simplified syntax and a graph structure. Since 2018, with the introduction of non-lexical lifetimes, the rules for borrow checking are formulated on the MIR graph rather than in Rust. This makes MIR an attractive starting point for verification of Rust, with its smaller syntax and simpler static analysis, translations and proofs stay smaller. We begin by formalizing a fragment of MIR containing only owned values called µMIR. This restriction makes it impossible to express many programs but gives room to focus on the other defining characteristic of µMIR, its graph structure.

2.1 The µMIR language

A program $P$ is a collection of function declarations, and must contain a function $\text{main}$ which acts as the entry point. Function declarations are in turn composed of a triple $(\Delta, \ell, \sigma)$ consisting of a set of labeled statements $\Delta$, an entry label $\ell$, and a function signature $\sigma$. Function signatures are made of the function name, a collection of input parameter names and types and the return type. The syntax of µMIR is described in Figure 5.

In Section 4, the translation, we developed a proof-of-concept implementation and showed it is capable of verifying real Rust programs.
\[
\ell_0: t_1 := 1; t_2 := 2; t_3 := (t_1, t_2); x := box t_3; goto \ell_4
\]

\[
\ell_4: t_4 := unbox x; (t_5, t_6) := t_4; t_7 := t_6 + 1; goto \ell_5
\]

\[
\ell_5: t_8 := (t_5, t_7); x := box t_8; goto \ell_9
\]

\[
\ell_9: t_9 := unbox x; (x_1, x_2) := t_9; goto \ell_12
\]

\[
\ell_{12}: t_{10} := 3; t_{11} := x_2 = t_{10}; assert t_{11}; goto \ell_{14}
\]

\[
\ell_{14}: drop x_2; drop t_{10}; drop t_{11}; goto \ell_{17}
\]

\[
\ell_{17}: ret := (); return ret
\]

Figure 6: Figure 3 translated to \(\mu\)MIR

Figure 6 displays how the program of Figure 3 is expressed in \(\mu\)MIR. To save space we put several statements on a single line. The code size blows up but decomposes the individual operations that happened in Figure 3 in a manner very similar to actual MIR.

2.2 A type system for ownership

The type system of \(\mu\)MIR is responsible for enforcing the unique ownership of every value in a program. Operations which manipulate boxes consume their inputs, removing them from the typing context and introducing new bindings for the results. Because of the imperative, graph structure of \(\mu\)MIR, the typing judgements take a different form from most languages. The presence of cycles within a graph make traditional natural deduction trees impossible to use. Instead, each program point is assigned a typing context, and typing relates the contexts before and after the evaluation of a statement.

Each label \(\ell\) of a function is associated with a partial variable context \(\Gamma\). The partial variable context is a collection of items of the form \(x : T\), where \(x\) is a variable name and \(T\) is a type. In a \(\mu\)MIR program \(P\), each function \(f\) is given a whole context \(\Xi\) which is the collection of the partial contexts for all labels in \(f\). Additionally, we use \(\Sigma\) to refer to the collection of signatures found in a program.

Typing judgements for instructions have the form \(\Gamma \vdash_f I \triangleright \Gamma'\), which relate the partial contexts before and after executing the instruction \(I\) in the function \(f\). In this representation, the mechanism of ownership becomes clearer, for example looking at \(\text{[BOX]}\) shows how when a box is created, the original variable \(y\) is destroyed to ensure the new pointer \(x\) remains the unique owner.

\[
\Sigma; y : T, \Gamma \vdash_f x^\text{box} : = \text{box } y^T \triangleright \Gamma, x : \text{box } T \quad \text{(BOX)}
\]

Typing judgements for statements have the form \(\Sigma; \Xi; P \vdash_{f,a} S\) and verify that the statement with label \(a\) in function \(f\), types with the expected partial context.

\[
\Sigma; \Xi \vdash_{f} I \vdash \Sigma; \Xi_{\ell} \quad \Sigma; \Xi; P \vdash_{f,a} I; \text{ goto } \ell \quad \text{(SEQUENCE)}
\]

The rule for \(\text{[BOX]}\) checks that the instruction \(I\) can be typed using \(\Xi_{a}\), producing \(\Xi_{\ell}\). In this approach, each statement checks an edge of the \(\mu\)MIR graph. The rules for (FUNCTION) and (PROGRAM) check that each function forms a graph. The full typing rules can be found in Appendix A.
2.3 Operational Semantics of \( \mu \text{MIR} \)

The operational semantics of \( \mu \text{MIR} \) is given by a reduction relation over an abstract heap machine. The configurations of the \( \mu \text{MIR} \) machine are of the form \( \langle f; \ell | S | F | H \rangle \), where \( f \) is the name of the function being executed and \( \ell \) is a label in \( f \), \( S \) is the call stack, \( F \) is the frame, and \( H \) is the heap. The stack is composed of triples \( [f; \ell, x, F] \) of a return label, a variable name for the result and a frame. A frame \( F \) is a partial function from variable names to addresses. We support pointer arithmetic: adding an address and an integer to obtain an address. The heap maps those addresses to a value which is either: an address, an integer, a boolean value, or unit. Complex values such as pairs or sums are stored in contiguous regions of the heap. Operations which must move or copy these values calculate the size of the values from their types:

\[
|T_1 \times T_2| = |T_1| + |T_2|
|T_1 + T_2| = 1 + \max(|T_1|, |T_2|)
|\text{box } T| = |\text{bool}| = |\text{int}| = |\text{unit}| = 1
\]

**Definition 2.1 (Notations).** If \( F \) is a partial function, and \( A \) is a subset of its domain, then \( A \leftarrow F \) denotes the domain restriction removing \( A \) from the domain of \( F \), and is defined as

\[ A \leftarrow F = \{(x, v) \mid (x, v) \in F, x \notin A\} \]

Below, we include the rule for \texttt{drop}, which deallocates a variable. When a variable is dropped, we lookup it’s address in the current frame and remove it from the heap. The remaining reductions are given in Appendix B.

\[
\frac{P_{f; \ell} = \texttt{drop } x^T; \texttt{goto } \ell, \quad \langle f; \ell | S | F \oplus \{(x, a)\} | H \rangle \rightarrow_P \langle f; \ell' | S | F | \{a\} \leftarrow H \rangle}{(\text{DROP})}
\]

2.4 Type preservation by reduction

We would like to ensure that the only way for a well-typed \( \mu \text{MIR} \) program to get stuck is by failing an assertion. This property allows us to reduce the safety of a program to the validity of its assertions. But if we look at the semantics from Section 2.3, it is clear that the machine can easily get stuck when the frame and heap contain invalid addresses or missing data. To correct this, we define a notion of \textit{well-typed configurations} which restrict us to only the configurations that could appear when evaluating a well-typed program. We can then prove the standard preservation of typing for these configurations, showing that for well-typed programs only assertions can block evaluation.

**Definition 2.2 (Heap Fragment Type).** When we write \( H \vdash a : T \), we mean to say that the heap fragment \( H \) starting at location \( a \), corresponds to a value of type \( T \).

\[
\begin{align*}
H_1 \vdash a : T_1 \\
H_2 \vdash a + |T_1| : T_2 \\
H = H_1 \oplus H_2
\end{align*}
\]

\[
H \vdash a : T_1 \times T_2
\]

\[
H \oplus \{(a, i)\} \vdash a : T_0 + T_1
\]

\[
\begin{align*}
H \vdash p : T \\
H \oplus \{(a, p)\} \vdash a : \text{box } T
\end{align*}
\]

\[
\begin{align*}
&c \text{ is a literal of } T \quad T \in \{\text{int, bool, unit}\} \\
&\{(a, c)\} \vdash a : T
\end{align*}
\]

A well-typed configuration is just a configuration where the heap \( H \) contains exactly the variables accessible in the frame \( F \).
Definition 2.3. A frame $F$ is well-typed at $f;\ell$ for a portion of a heap $H$ if $f$ is typed with $\Xi$ in $P$, and:

$$H = \bigoplus_{x \in F} H_x \quad \text{dom}(F) = \text{dom}(\Xi)$$

$$\forall x \in F, H_x \vdash x : \Xi(\ell)(x)$$

A configuration $\langle f;\ell \mid S \mid F \mid H \rangle$ is well-typed for a well-typed program $P$ when it satisfies the following conditions:

$$\forall i \in [1,|S|], S[i] = [f_i;\ell_i,x_i,F_i] \Rightarrow \text{well-typed } F_i f_i;\ell_i H_i$$

$$H = H_0 \oplus \bigoplus_{i\in[1,|S|]} H_i$$

We can now define what it means for reduction to preserve types, it simply ensures that the heap is composed exactly of the values expected at a given program point.

Theorem 2.4 (Type Preservation). Given a well-typed configuration $C$, if $C \rightarrow_P C'$, then $C'$ is well-typed.

We don’t prove this lemma and instead we will prove an extended version in Section 3.4.

2.5 Verification of safety for $\mu$MIR programs

To verify $\mu$MIR code, we translate it to a functional language. Then we prove that when the translation does not get stuck, neither does the $\mu$MIR program. This might seem redundant since Section 2.4 already proved preservation of typing, but by translating to a functional language it becomes possible to leverage existing deductive verification tools. To verify $\mu$MIR code, we will translate it to a functional language and use existing tools to verify the translated program. This approach is also easily extensible to arbitrary specifications which can be represented as pure logical functions.

Simplification In the following sections, we only consider programs without function calls, and therefore we ignore the stacks of the $\mu$MIR machine. The problems raised by function calls are orthogonal to the primary challenge of this proof and the one in Section 3.5.3. As a result, programs only consists in the body of the main function.

2.5.1 The $\mu$ML language

For $\mu$MIR, we will target a simple ML family language which we call $\mu$ML. It is an untyped ML dialect equipped with assertions, and call-by-value semantics described by an abstract machine with environment. The rules of the $\mu$ML abstract machine can be found in Appendix E.

$$\langle Expression, e \rangle ::= \langle let \rangle \ x \ \langle '=' \rangle \ \langle e \rangle \ \langle in \rangle \ \langle e \rangle \ | \ \langle e \rangle \ \langle e' \rangle \ | \ \langle x \rangle \ | \ \langle v \rangle \ | \ \langle e \rangle \ \langle op \rangle \ \langle e' \rangle \ | \ \langle match \rangle \ \langle e \rangle \ \langle with \rangle \ \langle [\ i \ inj_0 \ x_0 \rightarrow e \ i \ inj_1 \ x_1 \rightarrow e \ i \ end \ ] \ \langle let \rangle \ \langle x, y \rangle \ = \ \langle e \rangle \ \langle assert \rangle \ \langle t \rangle \ \langle e \rangle \ \langle \rangle \ | \ \langle [e \ i \ \langle e' \rangle \ | \ \langle x \rangle \ | \ \langle v \rangle \ | \ \langle rec \rangle \ \langle FunDef \rangle \ \langle and \rangle \ ... \ \langle and \rangle \ \langle FunDef \rangle \rangle \rangle$$

$$\langle FunDef \rangle ::= \langle fun \rangle \ f \ x \ ... \ x = \langle Expr \rangle$$

$$\langle Values, v \rangle ::= \langle \langle \ v \rangle \ \langle , \ v \rangle \ \rangle \ | \ \langle inj_i \ \langle v \rangle \ | \ n \ | \ \langle rec \rangle \ \langle FunDef \rangle \ \langle and \rangle \ ... \ \langle and \rangle \ \langle FunDef \rangle \rangle$$
2.5.2 Translating from $\mu$MIR to $\mu$ML

The translation takes a well-typed $\mu$MIR CFG and produces a set of mutually recursive $\mu$ML functions with the same entrypoint as $\mu$MIR. A labeled statement becomes a function where the arguments are the entire domain of the partial variable context associated with the label. Each $\text{goto } \ell$ is compiled to a function call, and the arguments are the variables in the domain of $\Xi_\ell$.

Most instructions from $\mu$MIR are translated to their direct counterparts in $\mu$ML. For example, here is the traduction of the construction of a pair:

$$[\ell: x := (y, z); \text{goto } \ell'] \triangleq \text{fun } \ell \bar{a} = \text{let } x = (y, z) \text{ in } \ell' \bar{a}$$

where $\bar{a} = \text{dom}(\Xi_\ell)$ and $\bar{a}' = \text{dom}(\Xi_{\ell'})$.

Interestingly, the operations related to the $\text{box}$ type are entirely erased since we are not interested in the memory layout in $\mu$ML:

$$[\ell: x^{\text{box} T} := \text{box } y^T; \text{goto } \ell'] \triangleq \text{fun } \ell \bar{a} = \text{let } x = y \text{ in } \ell' \bar{a}$$

$$[\ell: x^T := \text{unbox } y^{\text{box} T}; \text{goto } \ell'] \triangleq \text{fun } \ell \bar{a} = \text{let } x = y \text{ in } \ell' \bar{a}$$

where $\bar{a} = \text{dom}(\Xi_{\ell'})$.

The full translation rules are presented in Appendix C.

Translating Figure 6 When we run the translation we produce the following set of functions.

```ml
let rec l0 () = let t1 = 1 in let t2 = 2 in
  let t3 = (t1, t2) in let x = box t3 in l4 x
and l4 x = let t4 = x in let (t5, t6) = t4 in
  let t7 = t6 + 1 in l7 t5 t7
and l7 t5 t7 = let t8 = (t5, t7) in let x = t8 in l9 x
and l9 x = let t9 = x in let (x1, x2) = t9 in l11 x1 x2
and l11 x1 x2 = assert { t11 ]; 114 x1 t10 t11
and l14 x1 t10 t11 = let ret = () in ret
```

2.5.3 Correctness of the translation

We have a translation, but what does it actually produce? To ensure the translation is correct, we will show that whenever the $\mu$ML translation of a program is safe, that is, it does not get stuck, then so is the original program.

Theorem 2.5 (Safety). Given a well-typed program $\Gamma \vdash P$, if $C \sim P$ is safe, then $P$ is safe.

In order to prove Theorem 2.5 we establish a simulation $\sim_p$ between the input program $P$ and its translation $\sim_p$. We will give the exact definition of $\sim_p$ later, but what’s important is that it restricts the $\mu$MIR heap and $\mu$ML environment to ensure that the values in the environment correspond to regions of heap memory. Using this simulation we prove auxiliary lemmas, from which the proof to Theorem 2.5 will be formed.

The proof of safety is achieved using the following three lemmas.

Lemma 2.6 (Preservation of Simulation). Given a $\mu$MIR configuration $C$ and a $\mu$ML configuration $K$ such that $C \sim_p K$, if $C \rightarrow_p C'$ then $K \rightarrow K'$ and $C' \sim_p K'$.

Lemma 2.7 (Progress). Given a $\mu$MIR configuration $C$ and a $\mu$ML configuration $K$ such that $C \sim_p K$, if $K$ is not stuck then $C$ is not stuck.
Lemma 2.8 (Terminal Configurations). Given a terminal $\mu$ML configuration $K$, for any $\mu$MIR configurations $C$ such that $C \sim_P K$, then $C$ is terminal.

Proof of Theorem 2.5 Suppose that $C$ is not safe, therefore there exists a trace $C \rightarrow^* P C'$ which gets stuck. By iterating Lemma 2.6 there exists $K'$, such that $C' \sim_P K'$. Because $K'$ is safe, it cannot be stuck and must either be terminal or continue reducing. If $K'$ is a terminal configuration then by Lemma 2.8 there is a contradiction since $C'$ is not terminal. If $K'$ is not terminal then there exists $K''$ such that $K' \rightarrow_K K''$ and by Lemma 2.7 there exists $C''$ such that $C' \rightarrow_P C''$, therefore $C'$ is not stuck.

2.5.4 Simulation Invariant

In order to describe the simulation relation $\sim_P$ which relates $\mu$MIR and $\mu$ML programs, we show how to translate a region of a heap into a $\mu$ML value. This relation is called the readback of the heap. The region of memory associated with each $\mu$MIR variable will be translated to a $\mu$ML value. Because $\mu$MIR features only owned values and no borrowing, heap regions are intrinsically separated, which makes the readback a fairly direct and natural operation.

The readback of a heap region is guided by the type of the variable, it extends the heap typing relation covered in Section 2.4, associating a $\mu$MIR value to the concerned region of memory.

Definition 2.9 (Readback). $R(H, a, T, v)$ is a 4-place relation between a heap, address, type and a $\mu$ML value.

\[
R(H_1, a, T_1, v_1) \quad R(H_2, a + |T_1|, T_2, v_2) \quad \text{H} = H_1 \oplus H_2 \\
R(H, a, T_1 + T_2, (v_1, v_2))
\]

\[
R(H, a + 1, T_i, v) \\
R(\{((a, i), a, T_0 + T_1, \text{inj}_i, v) \}
\]

\[
R(H \oplus \{(a, c), a, T, c\})
\]

The correspondence between a heap, frame and environment is given by HeapEnv which selects the correct elements from the readback to populate the environment.

Definition 2.10 (HeapEnv). $\text{HeapEnv}(F, H, \Gamma, E)$ is a 4-place relation between a $\mu$MIR frame and heap, a partial variable environment and a $\mu$MIR environment where:

\[
\text{dom}(F) = \text{dom}(E) \\
H = \bigoplus_{x \in \text{dom}(F)} H_x \\
\forall x \in \text{dom}(F), R(H_x, F(x), \Gamma(x), E(x))
\]

The final simulation relation $\sim_P$ uses HeapEnv to relate a $\mu$MIR heap to a $\mu$ML environment and restricts $\mu$ML programs to the translation of the corresponding $\mu$MIR label. The full relation is given in Appendix D along with the proof of Theorem 2.4. The proof proceeds by case analysis on the reductions of $\mu$MIR, shuffling memory around to show that the resulting readback is exactly what was expected. We exclude it for space considerations.

2.6 Recap

In Section 2 we presented a small unstructured language with an ownership discipline enforced by typing. This language simulates the behavior of owned values in MIR. We then showed how to translate $\mu$MIR programs to $\mu$ML, a standard ML dialect and proved Theorem 2.5 showing that this translation is correct and permits the verification of $\mu$MIR programs.
3 Support for borrows and lifetimes

During function calls in \( \mu \text{MIR} \) every argument is consumed, making it impossible to call a function with the same argument twice. To solve this, Rust uses borrows which allow a variable to lend its read and write permissions temporarily. While a value is borrowed, the original owner is frozen until the end of the borrow’s lifetime. We can pass a function a borrowed reference as an argument, giving it temporary ownership of the contents, while recovering control when the borrow expires. We extend \( \mu \text{MIR} \) with the operations required to create and manipulate borrows as well as ghost operations used to ensure their safety. We call this resulting language MiniMir, because it’s a mini language that does the maximum! \(^1\)

3.1 The MiniMir language

Just like in \( \mu \text{MIR} \), programs are collections of function declarations. The syntax of signatures is more complex, functions can be parameterized over lifetime variables \( \alpha \) and lifetime constraints \( \alpha \leq \beta \). Let us consider an example:

\[
\text{fn \ fst\_proj \ <\alpha\,|\,> \ (p: \&mut\alpha\,x\int\,x\int) \to \&mut\alpha\,x\int}
\]

The signature for \( \text{fst\_proj} \) takes as input a mutable borrow alive for \( \alpha \) of a pair of ints (represented at runtime as a pointer to a pair of ints), and returns a borrow lasting for the same lifetime \( \alpha \) of a single int. Here, function is parameterized over \( \alpha \), allowing us to instantiate it with different lifetimes at different points in a program.

The instructions and statements are extended with operations to create a mutable borrow \( (\&\text{mut}_{\alpha}, T := \&\text{mut}_{\alpha} y^{P T}) \), to turn a mutable borrow into an immutable borrow \( (\text{immut} \ y^{\text{mut}_{\alpha}, T}) \) and to unnest borrows \( (x^{\text{mut}_{\alpha}, T := \text{unnest} y^{\text{mut}_{\alpha}, P T}) \). Unnesting is an essential operation when working with borrows. It collapses a layer of indirection between borrows, transforming a \( \&\text{mut}_{\alpha} \&\text{mut}_{\beta} T \) into a \( \&\text{mut}_{\alpha} T \). To interact with product types, a borrow of a pair can be destructed into a pair of borrows \( \text{let} (\text{ref} \ x^{P T_0}, \text{ref} \ y^{P T_1}) := \ast P (T_0 \times T_1) \).

The statements of MiniMir includes a new kind of match \( \text{match} \ *x \{ \ldots \} \) which allows programs to turn a borrow on a sum into a borrow on the value contained in the sum. When this occurs, programs are free to modify the value held in the sum but cannot change the constructor of the sum.

To verify the safety of borrows, we also add several ghost instructions, to thaw (end) a lifetime and to impose an ordering over lifetimes.

We can see this translation applied to Figure 4 in Figure 8. In this translation we inlined the \( \text{inc} \) function to make presentation simpler.

\(^1\)Reference to the famous slogan for a French cleaning product “Mini Mir, Mini Prix, mais il fait le maximum” reference needed
3.2 Extending types with borrowing

By creating pointers to values, borrows introduce aliasing. To prevent that, when a value is borrowed for a lifetime $\alpha$, the original name will be made inaccessible or frozen until the end of $\alpha$. To verify this safety property, the type system tracks a partial order on lifetimes, ensuring that borrows cannot outlive their prescribed lifetime. When the type system encounters a `thaw $\alpha$` instruction, it checks that all relevant borrows have been released and restores access to frozen variables.

We extend the type system of $\mu$MIR with partial lifetime contexts, which consist of a collection of elements $\alpha \leq \beta$. The partial variable context for MiniMir consists of elements of the form $x : \tau^\alpha T$ or $x : \tau T$, the first denoting a variable is frozen for lifetime $\alpha$ while the second denotes it is not frozen.

The whole context of a function $(\Xi, \Lambda)$ also collects the partial lifetime contexts for every label in the function. The forms of judgements extend naturally, using the lifetime contexts where appropriate. The judgements for instructions and statements are extended with partial lifetime contexts, while the judgement for functions is extended with a whole lifetime context.

The typing judgement for $x : \text{\&mut}^\alpha T := \text{\&mut}^\alpha y T$ expresses how the original value $y$ is frozen until $\alpha$ expires while granting $x$ access for that lifetime. No modifications are made to the partial lifetime context $L$ as creating a borrow does not immediately place it in an ordered relation.

\[
\Sigma; y : \tau^* T, \Gamma; L \vdash_f x : \text{\&mut}^\alpha y^\tau T \rightarrow \Gamma, x : \tau^* T, y : \tau^\alpha T; L
\]  

(BORROW-MUT)

When a lifetime is ended using a `thaw $\alpha$`, the type system ensures that everything borrowed for $\alpha$ has been dropped and that all lifetimes $\beta \leq \alpha$ have already been thawed. After a lifetime is thawed, all variables in the context which were frozen for $\alpha$ are unfrozen, restoring access. The complete type system for MiniMir is included in Appendix F.

3.3 Operational Semantics of MiniMir

The operational semantics of MiniMir changed little compared to $\mu$MIR. Because instructions like `thaw` are ghost, they become no-ops in the semantics. The primary addition of MiniMir, the mutable borrow, creates a new pointer to a value. The extended semantics for MiniMir is included in Appendix G.

3.4 Type preservation by reduction

Simplification In the following sections, as in the end of Section 2, we only consider programs without function calls. Again, the problems raised by function calls are orthogonal to the primary
challenge of this proof and the one in Section 3.5.3.

The banality of the semantics for mutable references is exactly what we desired. They create pointers that the type system ensures can only be used safely. To prove this we extend Theorem 2.3 to the full language of MiniMir.

We extend the heap fragment typing of Section 2.4 to include reference types. Since mutable references are non-aliasing, the heap fragment types must ensure that there are never two active pointers to the same region of memory. To ensure mutable borrows are only used once in a heap, we use a borrow store. The borrow store holds tokens for the lender and the borrower. By consuming the borrow store, the heap typing can ensure each borrow is used only once.

Definition 3.1 (Borrow Store). A borrow store is a finite set of elements of the form \( \text{take}_m(a, T) \) or \( \text{give}_m(a, T) \), where \( a \) is an address, \( T \) is a type and \( r \) is either \( i \) for immutable or \( m \) for mutable.

A borrow store \( B \) is safe if for every address \( a \) appearing in \( B \) it contains exactly the tokens \( \text{take}_m(a, T) \) and \( \text{give}_m(a, T) \) or contains \( \text{give}_i(a, T) \) and zero or more \( \text{take}_i(a, T) \).

We extend heap fragment typing and well-typing of Section 2.4. The judgments have the form, \( B; H \models a : T \). The definition of a well-typed configuration is then extended to ensure borrow stores are safe.

Definition 3.2 (Heap Fragment Type for MiniMir). Below are the heap typing rules for mutable and immutable references. The borrow store checks that both the lender and borrower agree on the addresses and types borrowed. The full rules are found in Appendix I.

\[
\begin{align*}
\text{give}_m(a, T); \emptyset \models a : T &\quad \text{give}_i(a, T), B; H \models a : T \\
B; H \models a : T &\quad \text{take}_m(a, T), B; \{ (p, a) \} \oplus H \models p : \text{mut}_m T \\
\text{take}_i(a, T); \{ (p, a) \} \models p : \text{mut}_i T
\end{align*}
\]

Definition 3.3. A well-typed configuration \( \langle f; \ell | - | F | H \rangle \) of a well-typed program \( P \) if it satisfies the following conditions:

\[
\begin{align*}
dom(\Xi_\ell) &= \dom(F) \\
H &= \bigoplus_{x \in F} H_x \\
B &= \bigoplus_{x \in F} B_x \\
safe(B) &\quad B_x; H_x \models x : T \Xi_\ell(x, n)
\end{align*}
\]

Using these expanded definitions, the proof of preservation extends easily to handle mutable and immutable references. Whenever a borrow is created or dropped, the corresponding tokens are inserted or removed from the borrow store.

Theorem 3.4 (Type Preservation). Given a well-typed MiniMir configuration \( C \), if \( C \rightarrow P \) \( C' \), then \( C' \) is well-typed.

The interesting cases of this proof are discussed in Appendix I.

3.5 Verification by translation

We extend our translation from \( \mu \text{MIR} \) with support for mutable and immutable references. Our encoding of mutable borrows into a functional language relies on their non-aliasing. When a borrow is created through \( x : \text{mu}_m y \), the type safety of MiniMir tells us that \( y \) cannot
fun l1 () = let t1 = 0 in let t2 = (t1, any) in let t1 = t2 in l3 t1 t2

and fun l3 t1 t2 = let t3 = t2 in let t4 = t3 + 1 in
  let t5 = (t4, any) in let t4 = t5 in let temp = t2 in
  let t2 = (t4, t5) in l5 t2 t3

and fun l5 t1 t2 = assume { *t5 = t5}; 19 t1 t2

and fun l19 t1 t2 = let t6 = t2 in let t7 = t6 + 1 in
  let t8 = (t7, any) in let t7 = t8 in let temp = t2 in
  let t2 = (t8, t7) in l13 t1 t2 t8

and fun l13 t1 t2 t8 = assume { *t8 = t8 }; 115 t1 t2

and fun l115 t1 t2 t8 = assume { *t2 = t2 }; 117 t1 t2

and fun l117 t1 = let t4 = t1 in assert { t4 = 2}; return ()

Figure 9: Translation of Figure 8 to MiniML

be used until the end of $\alpha$. At the end of $\alpha$, $y$ will have been updated with all the changes performed on $x$. In some sense, when we translate $x^{\&\text{mut},\alpha} : \&\text{mut},y^T$, we would like to replace $y$ with the final value pointed to by $x$. Since we can’t see into the future, we non-deterministically guess a value for $y$. Our translation represents mutable borrows as a pair of the current and final value being borrowed, like in RustHorn\[12\]. When the borrow is created we assign to $y$ the final value of the borrow. As the translated program executes, the current value of $x$ is updated. When the borrow is frozen, we rule out any executions that guessed the wrong final value by checking that the current and final values are equal.

3.5.1 The MiniML language

MiniML is an extension of $\mu$ML with non-determinism. The any expression picks an arbitrary value, and a assume \{ e \} evaluates an assumption $e$, if it doesn’t reduce to true, then it diverges. The operational semantics of $\mu$ML are extended to include these constructs in Appendix\[J\].

(\text{Expression, e}) ::= \text{’any’} | \text{’assume’ ‘\{ e ‘\}’} | ...

3.5.2 Translating from MiniMir to MiniML

The translation of $\mu$MIR to $\mu$ML is adapted to MiniMir. When a borrow is created, the borrow is assigned the current value being borrowed and its final value. In the translation we use two operators to access borrows defined as: $\&x \triangleq \text{fst } x$ and $\&x \triangleq \text{snd } x$.

\[
[x^{\&\text{mut},\alpha} : \&\text{mut},y^T; \text{goto } \ell'] \triangleq \text{fun } \ell \ a = \text{let } x = (y, \text{any}) \text{ in let } y = \&x \text{ in } \ell' \ a'
\]

When a mutable borrow is made immutable, we use the assume expression to equate its current value and final value.

\[
[x^{\text{immut} y^{\&\text{mut}},\alpha} : \text{goto } \ell'] \triangleq \text{fun } \ell \ a = \text{assume } \{ *y = \&y \}; \ell' \ a'
\]

The full translation is presented in Appendix\[H\]. In Figure 9 the program of Figure 8 is translated to MiniML. Instructions with produce no output in the translation are elided entirely.
3.5.3 Correctness of translation

We now examine the correctness of the translation presented in the previous section. Our safety theorem has the same structure as in μMIR but because of the non-determinism of MiniML the notion of safety changes to be programs in which all traces are non blocking.

**Theorem 3.5 (Safety).** Given a well-typed MiniMir program $\vdash P$, if $[P]$ is safe, then $P$ is safe.

The proof of this theorem is structured in the same manner as for $\mu \text{MIR}$. We now examine the correctness of the translation presented in the previous section. Our safety theorem has the same structure as in μMIR but because of the non-determinism of MiniML the notion of safety changes to be programs in which all traces are non blocking.

**Theorem 3.5 (Safety).** Given a well-typed MiniMir program $\vdash P$, if $[P]$ is safe, then $P$ is safe.

The proof of this theorem is structured in the same manner as for $\mu \text{MIR}$. To establish a simulation between MiniMir and MiniML we must extend the translation of memory to handle borrower.

When we define the simulation between MiniMir and MiniML, we find that mutable borrows cause us a problem. Each time a borrow is created, the translated program must guess the final value of the borrow, a value which appears nowhere in the memory of the MiniMir program. The readback must make the correct guess to constrain the traces in the simulation. We simplify this problem by supposing the existence of a prophecy map, which contains the correct final value for every pair of borrowed address and type. Using this prophecy map, we can define the readback of MiniMir as an extension of the heap typing just like with μMIR.

**Definition 3.6 (Readback).** The readback of Definition 2.9 is extended with support for mutable and immutable borrows. For each value being readback, it will produce a mapping containing every sub-value within.

\[
\begin{align*}
R^\alpha(A(a), T) = v & \quad \text{for all } A(a), T, v \\
R^\alpha((\text{give}^m_i(a, T), A, \emptyset, a, T, (a, T, v))) & \quad \text{for all } A(a, T) = v \\
R^n((\text{take}_i(a, T), A, \{(p, a)\}, p, \&\text{mut}_a, T, (p, T, v)) & \quad \text{for all } A(H(a), T) = v \\
R^n(B, A, \{a\} \equiv H, H(a), T, E) & \quad \text{for all } B, A, \{a\} \equiv H, H(a), T, E
\end{align*}
\]

**Definition 3.7 (HeapEnv).** The relation HeapEnv shows how to construct an ML environment from a MiniMir configuration. It uses the heap types of a configuration to readback memory cells as ML values.

Formally, HeapEnv $(B, A, F, H, \Gamma, E)$ is a 6-place relation between an activeness, a borrow store, a prophecy map, a MiniMir frame and heap, a partial typing environment and a MiniML environment where:

\[
\begin{align*}
dom(F) = dom(E) & \quad H = \bigoplus_{x \in \dom(F)} H_x \\
E = \{ (x, V_x(F(x), T)) \mid x : \tau T \in \Gamma \}
\end{align*}
\]

\[
\forall x \in \dom(F), R^n(B_x, A, H_x, F(x), \Gamma(x, n), V_x)
\]

It turns out, rather essentially, that the prophecy map we need can be calculated from a MiniMir trace. To do this, we take a trace and walk it backwards, each time a thaw $\alpha$ is encountered, the end of a lifetime has been reached. At that moment the values of all variables that were frozen are readback.

\[
\text{HeapEnv} \quad (A, B, F', H', \Xi_{f,\ell}, E)
\]

\[
\begin{align*}
\mathcal{P}_{f,\ell} = \text{thaw } \alpha & \quad A' = A \oplus \bigoplus_{\text{give}^i_{\alpha}(a, T) \in B} \{ E \mid R^\alpha(B^*, A, H^*, a, \Xi_{f,\ell}(a, \bullet), E) \}
\end{align*}
\]

\[
\text{McFly}^*(A', \langle f; \ell \rangle \mid - \mid F' \mid H) \rightarrow^p \langle f'; \ell' \mid - \mid F'' \mid H' \mid B'' \mid A \rangle
\]

14
In order to use McFly∗ we use a simulation between MiniMir traces and MiniML configurations. The simulation relation, ∼∗ calculates the required prophecy map using McFly∗, and uses it to ensure that the heap translates to the MiniML environment. At the same time the code is constrained to be the translation of the initial configuration of the trace.

We structure the proof of Theorem 3.5 using the same three lemmas as before: progress, terminal configurations and preservation. Using these lemmas, the proof proceeds in the same manner as Theorem 2.5. The statements of the first two lemmas change to account for the non-determinism of MiniML but, the structure of their proofs remains the same, thus we leave them in Appendix I, and focus on the proof of Lemma 3.8.

Lemma 3.8 (Preservation of Simulation). Given a MiniMir trace Θ = C →∗ C′ and a MiniML configuration K such that Θ ∼∗ K, if C →∗ C′′, there exists a K′ such that K → K′ and C′′ →∗ C′ ∼∗ K′.

The general structure of the proof remains unchanged from µMIR, it proceeds by case analysis on the reductions of MiniMir. The reductions relating to owned values proceed exactly as before, shuffling information around. Instead, the essential difficulty of this proof comes down to showing that McFly∗ finds the correct final value for every borrow. The intuition is that once a value is frozen, it cannot change, and therefore at the moment that we find the prophecy it must have the same value as when it was frozen.

Consider the case of \texttt{immut}\ y^{\text{ Restricted}}. Here we freeze a mutable reference x, the translation of this gives assume { *y = ^y}; \ell \vec{a}. To preserve the simulation, the MiniMir configuration must reduce to \ell' \vec{a}, with memory compatible with the heap. In sum, this means showing that the final value of x is the same as it’s current value.

By the preservation of heap typing, we observe that when the borrow is frozen, the memory \( H_x \) of x must be transferred back to the variable which was borrowed. To show that McFly∗ found the correct final value, we note that by inversion on McFly∗, the prophecy for x must come from some future configuration \( C'' \) of C. We then use Lemma I.6 to show that the memory of \( C'' \) can be readout. Finally, since by typing frozen cells of memory cannot change by reduction, the readout of \( H_x \) must be the same at \( C'' \) as it was at C. Since this value forms the prophecy for x, it must be the case the the current and final values of the borrow are equal and that the MiniML program can progress.

The proof is detailed more formally in Appendix I.

4 Experimentation

As further validation of the translation presented in Section 3, we implemented a proof-of-concept tool as an extension to the Rust compiler. This tool takes Rust programs in their MIR representation and translates them to WhyML, the specification and programming language of the Why3 verification suite. The translated programs can then be checked using the Why3 prover interface. Using this tool we were able to verify simple programs working on structures such as linked lists.

One of the primary implementation challenges is determining where the thaw should be in MIR code. The borrow checker of Rust infers a position where it should be inserted but that information is hidden from other passes. Extracting that information is essential as the safety of this tool relies on correct placement of thaws to mark the end of lifetimes.

We also took advantage of this tool to test several simple extensions, such as support for preconditions, post-conditions and invariants in code being verified. Each of these is lowered, nearly directly to the equivalent Why3 constructs. This enabled us to verify the functional correctness of several programs. A few of these programs are included in Appendix K.
5 Conclusion

During this internship, we developed a schema to verify Rust-like programs by translation to a functional language. Our source language MiniMir, is translated to MiniML, an ML-like language with non-determinism. In our translation we represent mutable borrows as pairs of their current and future values. To prove that our translation is correct, we developed an original simulation technique between an execution trace and a functional configuration. The proof requires us to show that we can predict the future values of each borrow, and we show that we can statically identify points in the program which can be used to predict those values. Finally, we validated this technique experimentally by implementing this translation as a proof-of-concept tool. Our tool was able to verify safety properties for simple programs using list operations.

Related Work. The Frama-C tool for C allows the verification of C in the presence of aliasing through non-aliasing hypotheses which assert pair-wise non-aliasing of variables. Asserting that all variables are non-aliasing requires quadratic amounts of hypotheses, which overwhelms automation like SMT solvers. Other languages like Spark/Ada rule out all aliasing through their type system. Recent work has been done on how to add aliasing references like in Rust.

To verify Rust programs, the team behind Prusti translates programs to a separation logic with fractional permissions. Currently, their approach is limited in the properties it is able to prove and their implementation supports a more limited subset of Rust programs than the approach offered by MiniMir. Another approach is that of RustHorn, which translates programs to Constrained Horn Clauses using the same encoding of mutable references we use. RustHorn however cannot represent user specifications and can only show that programs don’t fail assertions. Additionally, their approach of translating to CHCs means that they rely entirely on automated solvers with no method to allow human guidance.

Future Work. The approach presented in section allows us to verify Rust-style programs using both mutable and immutable references. However, the proof of correctness is complex using an original form of simulation. Formalizing this development in Coq would give a much firmer base for further extensions to the language. The work on RustBelt, could serve a starting point for a Coq formalization, since key lemmas like type safety are already proven on the core language \( \lambda \)Rust.

Currently, we have not considered the questions of specification languages for Rust, the encoding for datatype invariants and ghost code more generally remains an open question. To put this translation into application and incorporate extensions, the tool developed for this internship needs to be extended to more gracefully handle real-world Rust programs.

References


A Complete Type System of $\mu$MIR

$$
\begin{array}{ccc}
\text{Copy(int)} & \text{Copy(bool)} & \text{Copy(unit)} \\
\text{Copy}(T_0) & \text{Copy}(T_1) & \text{Copy}(T_0) \\
\text{Copy}(T_0 \times T_1) & \text{Copy}(T_0 + T_1)
\end{array}
$$

\begin{align*}
\Sigma; \Gamma \vdash T \in \Gamma & \quad \text{(COPY-VAL)} \\
\Sigma; \Gamma \vdash x^T := \text{copy } y^T \rightarrow \Gamma, x : T \\
y : \text{box } T \in \Gamma & \quad \text{(COPY-REF)} \\
\Sigma; \Gamma \vdash x^T := \text{copy } *y^P \rightarrow \Gamma, x : T \\
\Sigma; y : \text{box } T, \Gamma \vdash x^T := \text{unbox } y^\text{box} \rightarrow \Gamma, x : T & \quad \text{(UNBOX)} \\
\Sigma; y : T, \Gamma \vdash x^T := \text{box } y^T \rightarrow \Gamma, x : \text{box } T & \quad \text{(BOX)}
\end{align*}

\begin{align*}
x : \text{box } T, y : \text{box } T \in \Gamma & \quad \text{(SWAP)} \\
\Sigma; \Gamma \vdash \text{swap}(x^P, y^P) \rightarrow \Gamma & \quad \text{T }\in \{\text{int, unit}\} \\
\Sigma; x : T, \Gamma \vdash \text{drop } x^T \rightarrow \Gamma & \quad \text{(DROP)} \\
\Sigma; y : T_1, \Gamma \vdash x^{T_0 + T_1} := \text{inj}_T, y^T \rightarrow \Gamma, x : T_0 + T_1 & \quad \text{(INTRO-SUM)} \\
\Sigma; y : T_0, z : T_1, \Gamma \vdash x^{T_0 \times T_1} := (y^{T_0}, z^{T_1}) \rightarrow \Gamma, x : T_0 \times T_1 & \quad \text{(INTRO-PAIR)} \\
\Sigma; \Gamma \vdash \text{let } x = c \rightarrow \Gamma, x : T_{C} & \quad \text{(CONST-INTRO)} \\
\Sigma; \Gamma \vdash \text{assert } x \rightarrow \Gamma & \quad \text{(ASSERT)} \\
x : \text{bool } \in \Gamma & \quad \text{(OP)} \\
\Sigma; \Gamma \vdash \text{let } x = \text{int, } z : \text{int, } \Gamma \vdash x^T := y^{\text{int op}} z^{\text{int op}} \rightarrow \Gamma, x : T_{\text{op}} & \quad \text{(ELIM-PAIR)} \\
\Sigma; \Gamma \vdash \text{let } x = \text{fn } g (x_0 : T_0, \ldots, x_{n-1} : T_{n-1}) \rightarrow T_n \in \Sigma \\
x_0 : T_0, \ldots, x_{n-1} : T_{n-1}, \Gamma \vdash \text{let } x = g(x_0, \ldots, x_{n-1}) \rightarrow \Gamma, x : T_n & \quad \text{(CALL)}
\end{align*}

\begin{align*}
\Sigma; e_0 \vdash I \rightarrow \Sigma; e_\ell & \quad \text{(SEQUENCE)} \\
\Sigma; e_{f,a} \vdash \text{goto } \ell & \quad \text{(RETURN)} \\
\text{where } \Sigma_{\text{ret } f} = \{T_n \mid \text{fn } g (x_0 : T_0, \ldots, x_{n-1} : T_{n-1}) \rightarrow T_n \in \Sigma\}
\end{align*}

\begin{align*}
\Sigma; \Xi_{a} \vdash x : T_0 + T_1, \Gamma_a & \quad \Xi_{a} = \{x : \Sigma_{\text{ret } f}\} \\
\Sigma; \Xi_{\ell} \vdash e_{\ell} \rightarrow \text{goto } \ell & \quad \text{RETURN} \\
\Sigma; e_{a} \vdash \text{match } x^{T_0 + T_1} \{ \text{inj}_0 y_0^{T_0} \rightarrow \text{goto } \ell_0 , \text{inj}_1 y_1^{T_1} \rightarrow \text{goto } \ell_1 \} & \quad \text{(MATCH-VAL)}
\end{align*}
**B Complete Operational Semantics of μMIR**

**Definition B.1 (Notations).** If \( F \) is a partial function, and \( A \) is a subset of its domain, then \( A \triangle F \) denotes the domain restriction removing \( A \) from the domain of \( F \), and is defined as

\[
A \triangle F = \{(x, v) \mid (x, v) \in F, x \not\in A\}
\]

The operation \( A \oplus B \) denotes the disjoint union of partial functions, it is only defined when \( \text{dom}(A) \cap \text{dom}(B) = \emptyset \). The notation \( a \perp b \) (disjoint sets) signifies that \( a \cap b = \emptyset \). The notation \( a_0 \perp a_1 \perp \ldots \perp a_n \) is used to denote the pairwise disjointness of the sets \( a_0, \ldots, a_n \). The notation \( M_H(t, s, n) \) (memory copy) is a shorthand for copying \( n \) cells of \( H \) starting at \( s \) to addresses starting at \( t \). It is defined as

\[
M_H(t, s, n) = \{(t + i, H(s + i)) \mid i \in [n]\}
\]

The notation \([n]\) is used for the index set \( \{i \mid 0 \leq i < n\} \). The notation \([a, b]\) is used for \([b] - [a]\), the set representing the right-open interval from \( a \) to \( b \).

In a program \( P \), the initial configuration is given by \( \langle \text{main}; \ell_0; \epsilon; \emptyset; \emptyset \rangle \), where \( \ell_0 \) is the entrrypoint of \( \text{main} \) in \( P \). The terminal configurations of \( P \) are of the form \( \langle \text{main}; \ell; \epsilon; \emptyset; \emptyset \rangle \), where \( P_{\text{main}, \ell} = \text{return } x \).

The stack has the following form:

\[ S ::= \epsilon | [f; \ell, x, F]; S \]

As the name implies, it represents the function calls currently being evaluated. Each element of the stack is a triple composed of a return label, a variable name for the result and a frame obtained from the caller at the moment the call is performed.

\[
\begin{align*}
P_{f, \ell} &= x^T := \text{copy } y^T; \text{ goto } \ell' \quad F(y) = a \quad [b, b + |T|] \perp \text{dom}(H) \\
&\langle f; \ell \mid S \mid F \mid H \rangle \rightarrow_P \langle \ell' \mid S \mid F + \{(x, b)\} \mid H + M_H(b, a, |T|) \rangle
\end{align*}
\]

\[
\begin{align*}
P_{f, \ell} &= x^T := \text{unbox } y^{\text{box}T}; \text{ goto } \ell' \quad A = \{a\} \cup [H(a), H(a) + |T|] \\
&\langle f; \ell \mid S \mid F + \{(y, a)\} \mid H \rangle \rightarrow_P \langle \ell' \mid S \mid F + \{(x, b)\} \mid A + H + M_H(b, H(a), |T|) \rangle
\end{align*}
\]

\[
\begin{align*}
P_{f, \ell} &= x^T := \text{box } y^T; \text{ goto } \ell' \quad [b] \perp [c, c + |T|] \perp \text{dom}(H) \quad A = [a, a + |T|] \\
&\langle f; \ell \mid S \mid F + \{(y, a)\} \mid H \rangle \rightarrow_P \langle \ell' \mid S \mid F + \{(x, b)\} \mid A + H + \{(b, c)\} + M_H(c, a, |T|) \rangle
\end{align*}
\]

\[
\begin{align*}
P_{f, \ell} &= x^T := \text{drop } x^T; \text{ goto } \ell' \quad \langle f; \ell \mid S \mid F + \{(x, a)\} \mid H \rangle \rightarrow_P \langle \ell' \mid S \mid F + \{a\} \rangle
\end{align*}
\]
\[ \mathcal{P}_{f, \ell} = \text{assert } x; \text{ goto } \ell' \quad \mathbf{H}(f(x)) = \text{true} \]

\[ \langle f; \ell \mid S \mid F \mid H \rangle \rightarrow_{p} \langle \ell' \mid S \mid F \mid H \rangle \]

\[ \mathcal{P}_{f, \ell} = \text{swap}(x^{pT}, y^{pT}); \text{ goto } \ell' \quad F(x) = a \quad F(y) = b \]

\[ \langle f; \ell \mid S \mid F \mid H \rangle \rightarrow_{p} \langle f; \ell \mid S \mid F \mid (H(a), H(a) + |T|) \cup H(b), H(b) + |T|) \rangle \ll H \]

\[ + \mathcal{M}(H(a), H(b), |T|) + \mathcal{M}(H(b), H(a), |T|) \]

\[ \mathcal{P}_{f, \ell} = x := c; \text{ goto } \ell' \quad \{ a \} \perp \text{dom}(H) \]

\[ i = H(a) \quad \{ b, b + |T_i| \} \perp \text{dom}(H) \]

\[ \mathcal{P}_{f, \ell} = \text{match } x^{T_0 + T_1} \{ \text{ inj}_0 y^{T_0} \rightarrow \text{ goto } \ell_0 , \text{ inj}_i y^{T_1} \rightarrow \text{ goto } \ell_1 \} \]

\[ \langle f; \ell \mid S \mid F + \{(x, a)\} \mid H \rangle \rightarrow_{p} \langle \ell_i \mid S \mid F + \{(y, b)\} \mid \{ a, a + |T_0 + T_1| \} \ll H \]

\[ + \mathcal{M}(H(a, a) + |T_0|, a, a + |T_0 + T_1|) \]

\[ \mathcal{P}_{f, \ell} = x^{T_0 + T_1} := (y^{T_0}, z^{T_1}); \text{ goto } \ell' \quad A = [a_0, a_0 + |T_0|] + [a_1, a_1 + |T_1|] \]

\[ \langle f; \ell \mid S \mid F + \{(y, a), (z, a)\} \mid H \rangle \rightarrow_{p} \langle \ell' \mid S \mid F + \{(x, c)\} \mid \{ a, b, a + |T_0 + T_1| \} \ll H \]

\[ + \mathcal{M}(H(a, c), a_0, |T_0|) + \mathcal{M}(H(c, a), a_1, |T_1|) \]

\[ \mathcal{P}_{f, \ell} = \text{let } (x_0, y^{T_1}) := x^{T_0 + T_1}; \text{ goto } \ell' \quad \{ a_0, a_0 + |T_0| \} \perp \{ a_1, a_1 + |T_1| \} \perp \text{dom}(H) \]

\[ A = [c, c + |T_0| + |T_1|] \]

\[ \mathcal{P}_{f, \ell} = \text{let } (x, y) := x^{T_0 + T_1}; \text{ goto } \ell' \quad \{ a_0, a_0 + |T_0| \} \perp \{ a_1, a_1 + |T_1| \} \perp \text{dom}(H) \]

\[ s = \max(|T_0|, |T_1|) \]

\[ \langle f; \ell \mid S \mid F + \{(y, a)\} \mid H \rangle \rightarrow_{p} \langle \ell' \mid S \mid F + \{(x, b)\} \mid \{ a_0, b, a + |T_0 + T_1| \} \rr H \]

\[ + \mathcal{M}(H(b, a) + |T_0 + T_1|, b, a + |T_0|) \]

\[ \mathcal{P}_{f, \ell} = \text{let } x = g(x_0, \ldots, x_{n-1}) \]

\[ \langle f; \ell \mid S \mid F + \{(y, a_i)\} \mid i \in [n] \mid H \rangle \rightarrow_{p} \langle g \mid \ell, x, F; S \mid \{ (x_i, a_i) \mid i \in [n] \} \mid H \rangle \]

\[ \mathcal{P}_{f, \ell} = \text{return } x \]

\[ \langle f; \ell \mid \ell', F'; S \mid F \mid H \rangle \rightarrow_{p} \langle \ell' \mid S \mid F' + \{(y, F(x))\} \mid H \rangle \]

C Translation from $\mu$MIR to $\mu$ML

\[[\ell; x^{box_T} := \text{ box } y^{T}; \text{ goto } \ell'] \triangleq \text{ let } x = y \text{ in } \ell \ a\]

\[[\ell; x^{T} := \text{ unbox } y^{box_T}; \text{ goto } \ell'] \triangleq \text{ let } x = y \text{ in } \ell \ a\]

20
\[ \ell: x^T := \text{copy } y^T; \text{goto } \ell' \] \triangleq \text{let } x = y \text{ in } \ell \bar{a} \\
\[ \ell: x^T := \text{copy } y^T; \text{goto } \ell' \] \triangleq \text{let } x = y \text{ in } \ell \bar{a} \\
\[ \ell: x^T := y \text{int op } z; \text{goto } \ell' \] \triangleq \text{let } x = y \text{ op } z \text{ in } \ell \bar{a} \\
\[ \ell: \text{swap}(x^P, y^P); \text{goto } \ell' \] \triangleq \text{let } (y, x) = (x, y) \text{ in } \ell \bar{a} \\
\[ \ell: \text{drop } x^T; \text{goto } \ell' \] \triangleq \text{let } x = y \text{ op } z \text{ in } \ell \bar{a} \\
\[ \ell: x := \text{C; goto } \ell' \] \triangleq \text{let } x = \text{C in } \ell \bar{a} \\
\[ \ell: x := \text{f}((\ldots)(x_0, \ldots, x_n), \ldots); \text{goto } \ell' \] \triangleq \text{let } x = \text{f}(x_0, \ldots, x_n) \text{ in } \ell \bar{a} \\
\[ \ell: x^T_0 \times T_1 := (y^T_0, z^T_1); \text{goto } \ell' \] \triangleq \text{let } x = (y, z) \text{ in } \ell \bar{a} \\
\[ \ell: \text{let } (x^T_0, y^T_1) := (y^T_0, z^T_1); \text{goto } \ell' \] \triangleq \text{let } (x, y) = (y, z) \text{ in } \ell \bar{a} \\
\[ \ell: x^T_{+T} := \text{inj}_j y^T; \text{goto } \ell' \] \triangleq \text{let } x = \text{inj}_j y \text{ in } \ell \bar{a} \\
\[ \text{return } x \] \triangleq x \\
\[ \begin{align*}
\text{match } x^T \{ \\
\text{inj}_0 y_0^T \rightarrow \ell_0 \\
\text{inj}_1 y_1^T \rightarrow \ell_1 \\
\} \end{align*} \] \begin{align*}
\triangleq \begin{cases}
\begin{align*}
\text{begin match } x \text{ with } \\
| \text{inj}_0 y_0 & \rightarrow \ell_0 \bar{a} \\
| \text{inj}_1 y_1 & \rightarrow \ell_1 \bar{a} \\
\end{cases} \\
\text{end}
\end{align*}
\end{align*} \\
\[ \mathcal{P} \] \triangleq [\mathcal{P}_0], \ldots, [\mathcal{P}_n] \\
\[ (\Delta, \ell, \text{fn } f \bar{a} \rightarrow T) \] \triangleq \text{rec fun } f \bar{a} = \ell \bar{a} \text{ and } [\Delta_0] \ldots \text{ and } [\Delta_n] \\

D \quad \text{Proof of simulation preservation for } \mu\text{MIR}

**Definition D.1** (Simulation Invariant). The relation \(\sim_p\) between a well-typed \(\mu\text{MIR}\) configuration and a \(\mu\text{ML}\) configuration is defined by the following conditions:

\[
\langle f; \ell | - | F | H \rangle \sim_p \langle \{\mathcal{P}_{f, \ell}, \Gamma\} | E | K \rangle \\
K = \text{ret } E' \cdot \ldots \cdot \text{ret } E'' \\
\text{HeapEnv}(F, H, \Gamma, E)
\]

**Proof of Lemma 2.6** The proof proceeds by case-analysis on the transition relation \(\rightarrow_p\). Each case must shuffle memory around to show that the resulting configuration will readback in a manner which preserves the simulation.
Case (intro-pair) Recall that the reduction for introducing a pair is the following: 
\[ \langle f;\ell \mid S \mid F \oplus \{(y,a_0),(z,a_1)\} \mid H \rangle \rightarrow \langle \ell' \mid S \mid F \oplus \{(x,c)\} \mid H' \rangle \]

where
\[ A = [a_0,a_0 + n_0] \oplus [a_1,a_1 + n_1] \]
\[ H' = A \oplus H \oplus M_H(c,a_0,n_0) \oplus M_H(c+n_0,a_1,n_1) \]

By inversion on \( \sim_p \), 
\[ K = \langle \text{let } x = (y,z) \text{ in } \ell \mid \bar{a} \mid E \mid K \rangle \]
which reduces to 
\[ K' = \langle \ell \mid \bar{a} \mid E \oplus \{x,y\} \mid K \rangle. \]

We know that \( y \) and \( z \) both have a readback judgement. When we translate their memories to the cells of \( x \), that readback will remain the same. Then it’s simple produce a readback for 
\[ R(A \oplus (H_1 \oplus H_2) \oplus M_H(c,a_0,n_0) \oplus M_H(c+n_0,a_1,n_1),c,T_1 \times T_2,(v_1,v_2)). \]
With this we can translate the memory of \( C' \) to the environment of \( K' \), preserving the simulation.

Case (assert) When when we evaluate an assertion, \( \text{assert } x^\text{bool} \), we know that \( H(F(x)) = \text{true} \). By hypothesis, we know that \( x \) can be translated to a \( \mu \text{MIR} \) value, which tells us that \( E(x) = \text{true} \). From this we can easily see that the assertion must then also evaluate to \( \text{true} \) in \( \mu \text{MIR} \). From this we preserve the simulation.

Case (swap) When we evaluate a swap, we produce from 
\[ C = \langle [f;\ell] \mid - \mid F \mid H \rangle \]
a configuration who’s heap is:
\[ A = [H(a),H(a) + |T|] \cup [H(b),H(b) + |T|] \]
\[ H' = A \oplus H + M_H(H(a),H(b),|T|) + M_H(H(b),H(a),|T|) \]

All this amounts to is that the memories of \( x \) and \( y \) are each translated to the other’s position. The readbacks will therefore swap as well. This corresponds to the translation of the swap which also swaps the two variables in \( \mu \text{ML} \), preserving the simulation.

The other cases work in the same manner, memory is translated between cells following the motion of data in and out of sum and product types.

\[ \square \]

E Complete Operational Semantics of \( \mu \text{ML} \)

\[
\begin{align*}
\langle f \mid e \mid E \mid K \rangle & \rightarrow \langle f \mid E \mid \text{arg } e \cdot K \rangle \\
\langle v \mid E \mid \text{arg } e \cdot K \rangle & \rightarrow \langle e \mid E \mid \text{fun } v \cdot K \rangle \\
\langle v \mid E \mid \text{fun } \text{rec } f \ x = e \ \text{and } \ldots \ \text{and } g \ y = e' \cdot K \rangle & \rightarrow \\
\langle e \mid [f \mapsto \text{rec } f \ x = e \ \text{and } \ldots \ \text{and } g \ y = e',\ldots,g \mapsto \ldots] \cdot E' \mid \text{ret } E \cdot K \rangle \\
\langle v \mid E \mid \text{ret } E' \cdot K \rangle & \rightarrow \langle v,E \mid E' \mid K \rangle \\
E(x) = (\text{rec } f \ x = e \ \text{and } \ldots \ \text{and } g \ y = e',E') & \\
\langle v \mid E \mid K \rangle & \rightarrow \langle \text{fst } E(x) \mid [x \mapsto \text{fst } E(x)] \cdot \text{snd } E(x) \mid K \rangle
\end{align*}
\]
\[
\langle x \mid E \mid K \rangle \rightarrow \langle E(x) \mid E \mid K \rangle
\]

\[
\langle \text{let } x = e \text{ in } e' \mid E \mid K \rangle \rightarrow \langle e \mid E \mid \text{let } x e' \mid K \rangle
\]

\[
\langle v \mid E \mid \text{let } x e' \mid K \rangle \rightarrow \langle e' \mid [x \mapsto (v,E)] \cdot E \mid K \rangle
\]

\[
\langle \text{let } (x, y) = e \text{ in } e' \mid E \mid K \rangle \rightarrow \langle e' \mid \text{pair } x y e' \mid K \rangle
\]

\[
\langle (v_0, v_1) \mid E \mid \text{pair } x y e' \mid K \rangle \rightarrow \langle e' \mid [x \mapsto (v_0,E)] \cdot [y \mapsto (v_1,E)] \cdot E' \mid K \rangle
\]

\[
\langle \text{match } e \text{ with } \mid \text{inj}_0 x_0 \rightarrow e_0 \mid \text{inj}_1 x_1 \rightarrow e_1 \text{ end } \mid E \mid K \rangle \rightarrow \langle e \mid \text{match } x_0 e_0 x_1 e_1 \mid K \rangle
\]

\[
\langle \text{inj}_i v \mid E \mid \text{match } x_0 e_0 x_1 e_1 \mid K \rangle \rightarrow \langle e_i \mid [x_i \mapsto (v,E)] \cdot E' \mid K \rangle
\]

\[
\langle e_0, e_1 \mid E \mid K \rangle \rightarrow \langle e_0 \mid E \mid \text{fst } e_1 \cdot K \rangle
\]

\[
\langle v_0 \mid E \mid \text{fst } e_1 \cdot K \rangle \rightarrow \langle e_1 \mid E \mid \text{snd } v_0 \cdot K \rangle
\]

\[
x, y \notin \text{dom}(E)
\]

\[
\langle v_1 \mid E \mid \text{snd } v_0 \cdot K \rangle \rightarrow \langle (x, y) \mid [x \mapsto (v_1,E)] \cdot [y \mapsto (v_0,E)] \cdot E \mid K \rangle
\]

\[
\langle \text{inj}_i e \mid E \mid K \rangle \rightarrow \langle e \mid E \mid \text{inj}_i \cdot K \rangle
\]

\[
\langle v \mid E \mid \text{inj}_i \cdot K \rangle \rightarrow \langle \text{inj}_i v \mid E \mid K \rangle
\]

\[
\langle e_0 \mid E \mid \text{left } e_1 \cdot K \rangle \rightarrow \langle e_0 \mid E \mid \text{left } e_1 \cdot K \rangle
\]

\[
\langle v_0 \mid E \mid \text{left } e_1 \cdot K \rangle \rightarrow \langle e_1 \mid E \mid \text{right } v_0 \cdot K \rangle
\]

\[
\langle v_1 \mid E \mid \text{right } v_0 \cdot K \rangle \rightarrow \langle r \mid E \mid K \rangle
\]

\[
\langle \text{assert } \{ e \} \mid E \mid K \rangle \rightarrow \langle e \mid E \mid \text{assert } \cdot K \rangle
\]

\[
\langle \text{true } \mid E \mid \text{assert } \cdot K \rangle \rightarrow \langle () \mid E \mid K \rangle
\]

\[
\langle e ; e' \mid E \mid K \rangle \rightarrow \langle e \mid E \mid \text{seq } e' \cdot K \rangle
\]

\[
\langle v \mid E \mid \text{seq } e' \cdot K \rangle \rightarrow \langle e' \mid E \mid K \rangle
\]
F  Complete Type System of MiniMir

\[ y : T \in \Gamma \quad \text{Copy}(T) \]
\[ \Sigma ; \Gamma ; L \vdash_f x^T := \text{copy } y^T \to \Gamma , x : T ; L \quad \text{(COPY-VAL)} \]

\[ y : P \ T \in \Gamma \quad P \in \{ \&\text{mut}_\alpha , \&\alpha , \text{box} \} \quad \text{Copy}(T) \]
\[ \Sigma ; \Gamma ; L \vdash_f x^T := \text{copy } \ast y^P \to \Gamma , x : T ; L \quad \text{(COPY-REF)} \]

\[ \Sigma ; y : T , \Gamma ; L \vdash_f x^T := \text{unbox } y^{\text{box}T} \to \Gamma , x : T ; L \quad \text{(UNBOX)} \]

\[ \Sigma ; y : T , \Gamma ; L \vdash_f x^{\text{box}T} := \text{box } y^T \to \Gamma , x : \text{box } T ; L \quad \text{(BOX)} \]

\[ \Sigma ; y : T , \Gamma ; L \vdash_f \text{&mut}_\alpha , T , y : \&\alpha T \quad \text{(BORROW-MUT)} \]

\[ P \in \{ \text{box}, \&\text{mut}_\beta \} \quad \alpha \leq \beta \in \mathcal{L} \]
\[ \Sigma ; y : \&\text{mut}_\alpha , P \ T , \Gamma ; L \vdash_f x^{\text{box}T} := \text{unnest } y^{\text{mut}_\alpha , P T} \to \Gamma , x : \&\text{mut}_\alpha T ; L \quad \text{(UNNEST)} \]

\[ P \in \{ \&\text{mut}_\alpha , \text{box} \} \quad x : PT , y : PT \in \Gamma \]
\[ \Sigma ; \Gamma ; L \vdash_f \text{swap}(x^{PT} , y^{PT}) \to \Gamma ; L \quad \text{(SWAP)} \]

\[ T \in \{ \text{int}, \text{unit}, \&\alpha \} \]
\[ \Sigma ; x : T , \Gamma ; L \vdash_f \text{drop } x^T \to \Gamma ; L \quad \text{(DROP)} \]

\[ \Sigma ; x : \&\text{mut}_\alpha T , \Gamma ; L \vdash_f \text{immut } x \to \Gamma , x : \&\alpha T ; L \quad \text{(IMMUT)} \]

\[ \Sigma ; y : T_1 , \Gamma ; L \vdash_f x^{T_0 + T_1} := \text{inj}_1 y^T \to \Gamma , x : T_1 + T_2 ; L \quad \text{(INTRO-SUM)} \]

\[ \Sigma ; y : T_1 , z : T_2 , \Gamma ; L \vdash_f x^{T_0 \times T_1} := (y^{T_0} , z^{T_1}) \to \Gamma , x : T_1 \times T_2 ; L \quad \text{(INTRO-PAIR)} \]

\[ \Sigma ; \Gamma ; L \vdash_f \text{let } x = C \to \Gamma , x : T_C ; L \quad \text{(CONST-INTRO)} \]
\[ \Sigma ; x : \text{bool} \in \Gamma \]
\[ \Sigma ; \Gamma ; L \vdash_f \text{assert } x \to \Gamma ; L \quad \text{(ASSERT)} \]

\[ y : \text{int}, z : \text{int} \in \Gamma \]
\[ \Sigma ; \Gamma ; L \vdash_f x^T := y^{\text{int} \text{op } z^{\text{int}}} \to \Gamma , x : T_{\text{op}} ; L \quad \text{(OP)} \]

\[ \Sigma ; z : T_1 \times T_2 , \Gamma ; L \vdash_f \text{let } (x^{T_0} , y^{T_1}) := z^{T_0 \times T_1} \to \Gamma , x : T_1 , y : T_2 ; L \quad \text{(ELIM-PAIR)} \]

\[ P \in \{ \&\text{mut}_\alpha , \&\alpha \} \]
\[ \Sigma ; z : P (T_1 \times T_2) , \Gamma ; L \vdash_f \text{let } (\text{ref } x , \text{ref } y) = z \to \Gamma , x : P T_1 , y : P T_2 ; L \quad \text{(ELIM-PAIR-REF)} \]

\[ \]
∀j, 0 ≤ j < l, βαj ≤ βbj ∈ L
∀i, 0 ≤ i < n + 1, Ti = T'[α0/βα0, ..., αm−1/βm−1]  
fn g(α0, ..., αm−1 | αa0 ≤ αb0, ..., αa1-1 ≤ αb1-1)(x0 : T0' ...xn-1 : Tn'-1) → Tn ∈ Σ  
Σ; x0 : T0, ..., xn-1 : Tn-1, Γ; L ⊢ f let x = g(β0, ..., βm-1)(x0, ..., xn) → Γ, x : Tn; L  
(CALL)  
Σ; Γ; L ⊢ f α ≤ β ⊃ Γ; L, α ≤ β  
(SUB-LIFETIME)  
L' = L \ {α ≤ β | ∃β, α ≤ β ∈ L}  
Γ' = {thawα(v) | v ∈ Γ}  
∀x : T, T ∈ Γ', α /∈ lifetimes(T)  
(THAW)  
where Σexp f is the set of lifetimes that survive the function f.

thawα(v) = \{x : T  
v = x : !α T  
otherwise\}  
(RETURN)

Σ; A; Σ ⊢ f I + Σ; Σ f; A  
(SEQUENCE)  
Σ; Σ, A ⊢ f a; goto l  
(MATCH-VAL)

Σ; x : T0 + T1; Σ f; A ⊢ inj0 y0 → ℓ0  
Σ; x : T0 + T1; Σ f; A ⊢ inj1 y1 → ℓ1  
(MATCH-REF)  
Σ; x : T0 + T1; Σ f; A ⊢ ref y0 → ℓ0  
Σ; x : T0 + T1; Σ f; A ⊢ ref y1 → ℓ1  

Σ = \{x : Σ ret f\}  
Σ; Σ, A ⊢ return x  
(MATCH-VAL)  
Σ; A; Σ ⊢ return x  
(MATCH-REF)  
Σ; A; Σ ⊢ return x  
(MATCH-VAL)  
Σ; Σ ret f ⊢ return x  
(MATCH-REF)  
Σ; Σ ret f ⊢ return x  
(MATCH-VAL)

Σ = \{Σ, Σ f, P\}  
Σ ⊢ P  
(PROGRAM)

G  Complete Operational Semantics of MiniMir

The semantics of μMIR are extended with the following rules:
\[ P_{f,\ell} = \text{immut } y^{\text{mut}_a T}; \text{ goto } \ell', \]
\[ \langle \ell | S | F | H \rangle \rightarrow_P \langle \ell' | S | F | H \rangle \] (IMMUT)

\[ P_{f,\ell} = x^{\text{mut}_a T} := \text{&mut}_a y^T; \text{ goto } \ell', \quad F(y) = a \quad b \not\in \text{dom}(H) \]
\[ \langle \ell | S | F | H \rangle \rightarrow_P \langle \ell' | S | F + \{(x, b)\} | H + \{(b, a)\} \rangle \] (BORROW-MUT)

\[ P_{f,\ell} = x^{\text{mut}_a T} := \text{unnest } y^{\text{mut}_a P^T}; \text{ goto } \ell', \quad b \not\in \text{dom}(H) \]
\[ \langle \ell | S | F + \{(y, a)\} | H + \{(a, p)\} \rangle \rightarrow_P \langle \ell' | S | F + \{(x, b)\} | H + \{(b, H(p))\} \rangle \] (UNNEST)

\[ P_{f,\ell} = \text{match } *x \{ \ldots \} i = H(a) \]
\[ \langle \ell | S | F + \{(x, a)\} | H \rangle \rightarrow_P \langle \ell_i | S | F + \{(y_i, H(a) + 1)\} | H \rangle \] (MATCH-REF)

H Translation from MiniMir to \( \mu \text{ML} \)
\[ \ell: \text{let } x = *y \text{ in } \ell' \]

\[ \ell: \text{let } y = \sim x \text{ in } \ell' \]

\[ \ell: \text{let } x = (**y, *^y) \text{ in } \ell' \]

\[ \ell: \text{let } t = *x \text{ in } \ell' \]

\[ \ell: \text{let } (x, y) = z \text{ in } \ell' \]

\[ \ell: \text{let } (x_n, y_n) = *z \text{ in } \ell' \]

\[ \ell: \text{let } (x, y) = z \]
begin match *x with
| inj0 y0 →
let y0 = (y0, any) in
assume { \(^x = inj0 \^y0 \)};
let x = (inj0 \^y0, \^x) in L_0
| inj1 y1 →
let y1 = (y1, any);
assume { \(^x = inj1 \^y1 \)};
let x = (inj1 \^y1, \^x) in L_1
end
I. Proof of simulation preservation for MiniMir

Definition I.1 (Heap Fragment Type for MiniMir). The heap types of MiniMir extend the judgements of \( \mu \text{MIR} \) with a borrow store, checking that every borrow has a source and that they agree on typing.

\[
\begin{align*}
B_1; H_1 &\vdash a :^n T_1 \\
B_2; H_2 &\vdash a + |T_1| :^n T_2 \\
B; H &\vdash a :^n (T_1 \times T_2)
\end{align*}
\]

\( T \in \{\text{int, bool, unit}\} \) is a constant of type \( T \)

\[\emptyset; \{(a, c)\} \vdash a :^n T\]

\( \text{take}_a^n(a, T), B; \{(p, a)\} \lor H \vdash p :^n \& \text{mut}_a T\)

\( \text{give}_a^n(a, T); \emptyset \vdash a :^n T\)

\( B; H \vdash a :^n T\)

\( B; H \vdash a : 1^n T\)

\( B; H \vdash a : ^{1\alpha} T\)

\( \text{take}_a^1(a, T); \{(p, a)\} \vdash p : ^n \& \text{mut}_a T\)

\text{Proof.} The proof proceeds by case-analysis on the reductions of MiniMir. We will show several cases which illustrate preservation for owned data, mutable borrows and immutable borrows.

Case (intro-pair) Given a configuration \( C \) with code \( x^{T_0 \times T_1} := (y^{T_0}, z^{T_1}) \), we know that that we must have \( B_y; H_y \vdash a_0 : T_1 \) and \( B_z; H_z \vdash a_1 : T_2 \). We from this we construct \( B_y + B_z; H_z \vdash c : T_1 \times T_2 \), here \( \text{dom}(H_z) = [c, c + |T_0 \times T_1|] \). It's immediately apparent that when we move the memories of \( y \) and \( z \) into the cells of \( H_y \), we obtain the desired heap typing.

Case (borrow-mut) The reduction of \( C \) with code \( x^{\& \text{mut}_a} := x^{\& \text{mut}_a} y^T \), adds a new pointer \( x \) holding the address of \( y \) to \( H \). By hypothesis we have \( B_y; H_y \vdash a : T \). We need to produce two new judgements after evaluating this instruction, one for \( x : \& \text{mut}_a T \) and one for \( y : ^{1\alpha} T \). To preserve typing we add a pair of tokens \( \text{give}_a^1(a, T), \text{take}_a^1(a, T) \) to \( B \). Using these tokens we can construct \( \{(\text{give}_a^1(a, T))\}; \emptyset \vdash a : ^{1\alpha} T \) for \( y \) and \( \{(\text{take}_a^1(a, T))\} \cup B_y; \{(p, a)\} \lor H_y \vdash a : \& \text{mut}_a T \).

Case (immutable) By hypothesis we have \( \{(\text{take}_a^1(a, T))\} \cup B_z; \{(p, a)\} \lor H_z \vdash p : \& \text{mut}_a T \). By the safety of \( B \) we know there must be \( \{(\text{give}_a^1(a, T))\} \cup B_y; H_y \vdash a' : ^{1\alpha} T' \). By inversion, this judgement must contain the a subtree for \( \{(\text{give}_a^1(a, T))\}; \emptyset \vdash a : ^{1\alpha} T' \). We must transform the judgement for \( x \) into one for an immutable reference. We do this by removing \( \text{give}_a^1(a, T), \text{take}_a^1(a, T) \) and inserting \( \text{give}_a^1(a, T), \text{take}_a^1(a, T) \) into the borrow store. As a result the ownership of \( H_x \)

\[\square\]

Here we give the complete definition of the readback for MiniMir.

Definition I.3 (Readback). The readback of a MiniMir heap constructs a map of address and type to MiniML value.
\[
\begin{align*}
\mathcal{R}^n(B_1, A, H_1, a, T_1, E_1) & \quad H = H_1 + H_2 \\
\mathcal{R}^n(B_2, A, H_2, a + |T_1|, T_2, E_2) & \quad B = B_1 + B_2 \\
\mathcal{R}^n(B, A, H, a, T_1 \times T_2, E_1 + E_2 + |a, (E_1(a), E_2(a + |T_1|))|) & \quad \Theta = \emptyset \\
\end{align*}
\]

Lemma I.4 (Progress). Given a MiniMir trace \( C \rightarrow^*_p C' \) and a MiniML configuration \( K \) such that \( C \rightarrow^*_p C' \sim_p K \), if \( K \) is not stuck then \( C \) is not stuck.

Lemma I.5 (Terminal Configurations). Given a terminal MiniML configuration \( K \), for any MiniMir trace \( \Theta \) such that \( \Theta \sim_p K \), then \( \Theta = C \not\sim_p \) and \( C \) terminal.

Proof. The only terminal configurations for MiniML possible with the simulation are those in relation with return instructions inside the main function of the MiniMir program.

Lemma I.6. If \( \mathcal{R}^{\alpha}(B_x, A, H_x, F(x), T, V_x) \), then for all \( \mathcal{R}^* (B_x', A', H_x', F(x), T, V_x') \), \( \text{dom}(V_x) \subseteq \text{dom}(V_x') \).

Proof. By induction over the type \( T \) we observe that when we perform a readback with a frozen activeness \( \alpha \) we will leave out subtrees of the active readback.

Definition I.7 (McFly). The McFly relation calculates the required prophecies from a MiniMir trace.

\[
\begin{align*}
\text{HeapEnv} & (A, B, F', H', \Xi_{f, \ell}, E) \\
\mathcal{P}_{f, \ell} & = \text{thaw } \alpha \quad A' = A \oplus \bigoplus_{\text{give}(x, T) \in B} E \mid \mathcal{R}^{\alpha}(B_x', A, H_x', a, \Xi_{f, \ell}(a, \bullet), E) \\
\text{McFly}^*(A', (\langle f; \ell \rangle | - | F | H) \rightarrow_p (f'; \ell' | - | F' | H' | B', A) & \\
\end{align*}
\]

At the end of a trace we may still have active borrows (if the trace is stuck), to handle this situation, we perform a readback of each borrowed variable. During this readback we do not require the heap to be separated, which avoids the need for any prophecies by allowing cells to be reused in several readbacks.
Proof. We find ourselves required to prove that for all variables in the frame of the initial configu-
ration, we encounter a borrow, we must show that there is a prophecy in
active until the end of the trace and we must also have a prophecy. Using this we can construct
on McFly, either there is a thaw for the lifetime of the borrow and we have a prophecy, or it is

Lemma I.8. Given a trace of well-typed MiniMir configurations Θ and a prophecy map A such
that McFly(A, Θ), then HeapEnv (A, B, F, H, Ξθ0, E).

Definition I.9 (Simulation Relation). The relation ∼R between a well-typed MiniMir trace Θ
and a Krivine configuration is defined by the following conditions:

\[ \text{McFly}^* (A, C \rightarrow_R C', E) \quad E = \bigoplus E_a \]
\[ \forall \text{get} \in (a, T) \in B, \exists H_a \subseteq H, B_a \subseteq B, R (B_a, \varnothing, H_a, a, T, E_a) \]
\[ \text{McFly}(A, C \rightarrow_R (f; \ell' | - | F | H)) \]

Lemma I.8. The proof proceeds by case-analysis on the reduction C →R C'. The cases related
to owned data ((intro-pair), (constant)) proceed like in μMIR. The most interesting cases of
this proof are those for creating and freezing a borrow.

Case (borrow-mut) To preserve our simulation, we must ensure that the translated code re-
duces properly to the next label and that the resulting memories stay linked by HeapEnv.
Because we create a new borrow, to have a readback, we need a prophecy map which in-
cludes this new borrow. We get this by Lemma I.8, we know that there must be a prophecy
for the borrowed variable.

Case (immut) As a reminder, the operational semantics tell us that the operation is a no-op.

The translation of \texttt{immut} gives us

\[ K = \langle \text{assume} \{ * x = x \}; \ell' \; a \; | \; E \; | \; K \rangle \]

To preserve the simulation, the machine must reduce the \texttt{assume}, which means proving that
\[ * x = x. \]

Let \texttt{F}(x) = a, by inversion on the HeapEnv, we know that there is \texttt{H}_x, V_x, B_x such that
\( R^*(\text{take}^a \alpha (a, T) \cup B_x, A, H_x, a, \text{mutation} T_x, V_x) \) so, \( E(x) = \langle V_x (H(a), T_x), A(H(a), T_x) \rangle \). By the safety of \( B \), there must be a variable \texttt{y} which consumes \texttt{get}^a \alpha (a, T), by assigning \texttt{y} the memory \texttt{H}_x in \texttt{C}', we can preserve the existence of the readback.

Let \( R^{\ast \alpha} (B_y, H_x, F(y), T, V_y) \) be the readback of \texttt{y} in \texttt{C}''. We know that \( (H(a), T_x) \in \text{dom}(V_y) \).

Let \( C'' \) be either the first configuration in \( \Theta \) such that \( P_{\ell; \ell''} = \text{thaw} \alpha \) or the last configuration of \( \Theta \). By applying Lemma I.8, we know that \( C'' \) must have a readback. Since \( (H(a), T_x) \in \text{dom}(V_y) \), by Lemma I.6, \( (H(a), T_x) \) must be included in the readback of \texttt{y} at \texttt{C}''. This means that by inversion on the readback of \texttt{C}'', there must be a
\( R^{\ast \alpha} (B_x, A', H_x, a, T_x, V_x) \).
Because we froze all the memory associated with \(H(a)\) at \(C\), we know that \(B'_x \subseteq B_x\) and \(H'_x \subseteq H_x\). By typing we know that \(B_x\) can only have immutable give and take tokens. Since that means we control all the memory, \(H_x = H'_x\). Finally since \(A' \subseteq A\), it must be that \(V'_x = V_x\).

All of this allows us to conclude that \(= x = A(H(a), T_x) = V'_x(H(a), T_x) = V_x(H(a), T_x) = * x\), so \(K\) reduces to \(K' = (\ell' \vec{a} \mid E' \mid K)\), preserving the simulation.

\(\square\)

### J Operational Semantics of MiniML

MiniML extends \(\mu\)ML with the following continuations

\[
K ::= \text{assume} \mid ...
\]

and the following reductions.

\[
\begin{align*}
\langle \text{assume} \{ e \} \mid E \mid K \rangle & \rightarrow \langle e \mid E \mid \text{assume} \cdot K \rangle \\
\langle \text{true} \mid E \mid \text{assume} \cdot K \rangle & \rightarrow \langle () \mid E \mid K \rangle \\
\langle \text{false} \mid E \mid \text{assume} \cdot K \rangle & \rightarrow \langle \text{false} \mid E \mid \text{assume} \cdot K \rangle \\
\langle \text{any} \mid E \mid K \rangle & \rightarrow \langle v \mid E \mid K \rangle
\end{align*}
\]

### K Example programs run on Proof-of-Concept tool

```rust
pub struct List {
    val: u32,
    next: Option<Box<List>>,
}

pub fn index_mut(mut l: &mut List, mut ix: usize) -> &mut u32 {
    while ix > 0 {
        match l.next {
            Some(ref mut n) => {
                l = n;
            }
            None => std::process::abort(),
        }
        ix -= 1;
    }
    &mut l.val
}

pub fn write(l: &mut List, ix: usize, val: u32) {
    *index_mut(l, ix) = val;
}
```
```rust
fn main() {
    let mut l = List {
        val: 1,
        next: Some(Box::new(List {
            val: 10,
            next: None,
        })),
    };
    write(&mut l, 0, 2);
    let l2 = List {
        val: 2,
        next: Some(Box::new(List {
            val: 10,
            next: None,
        })),
    };
    assert!(l, l2);
}

#[derive(PartialEq, Eq, Debug)]
pub struct List {
    head: Option<Box<Node>>,
}

#[derive(PartialEq, Eq, Debug)]
pub struct Node {
    val: u32,
    next: Option<Box<Node>>,
}

pub fn rev(l: &mut List) {
    let mut prev = None;
    let mut head = l.head.take();
    while let Some(mut curr) = head {
        let next = curr.next;
        curr.next = prev;
        prev = Some(curr);
        head = next;
    }
    l.head = prev;
}

fn main() {
    let mut l1 = List {
        head: Some(Box::new(Node {
            val: 1,
            next: Some(Box::new(Node {
                val: 10,
                next: None,
            })),
        })),
    }
```
let l2 = List {
    head: Some(Box::new(Node {
        val: 10,
        next: Some(Box::new(Node { val: 1, next: None }))
    }))
},
};
rev(&mut l1);
let l2 = List {
    head: Some(Box::new(Node {
        val: 10,
        next: Some(Box::new(Node { val: 1, next: None }))
    }))
},
};
assert_eq!(l1, l2);
}