José Miguel Gonçalves Duarte

Bachelor in ⟨Computer Science⟩

Bridging the Gap between Typestates and Rust in Production Software

Dissertation submitted in partial fulfillment
of the requirements for the degree of

Master of Science in
Computer Science

Adviser: António Ravara
Full Professor, NOVA University Lisbon

FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

⟨month⟩, **⟨year⟩**

Bridging the Gap between Typestates and Rust in Production Software

Dedicatory lorem ipsum.

Acknowledgements

Acknowledgments are personal text and should be a free expression of the author.

However, without any intention of conditioning the form or content of this text, I would like to add that it usually starts with academic thanks (instructors, etc.); then institutional thanks (Research Center, Department, Faculty, University, FCT / MEC scholarships, etc.) and, finally, the personal ones (friends, family, etc.).

But I insist that there are no fixed rules for this text, and it must, above all, express what the author feels.

"You cannot teach a man anything; you can only help him discover it in himself." — Galileo

Abstract

As software becomes more prevalent in our lives, bugs are able to cause significant disruption. Thus, preventing them becomes a priority when trying to develop dependable systems. While reducing their occurrence possibility to zero is infeasible, existing approaches are able to eliminate certain subsets of bugs.

Rust is a systems programming language that addresses memory-related bugs by design, eliminating bugs like *use-after-free*. To achieve this, Rust leverages the type system along with information about object lifetimes, allowing the compiler to keep track of objects throughout the program and checking for memory misusage. While preventing memory-related bugs goes a long way in software security, other categories of bugs remain in Rust. One of which would be Application Programming Interface (API) misusage, where the developer does not respect constraints put in place by an API, thus resulting in the program crashing.

Typestates elevate state to the type level, allowing for the enforcement of API constraints at compile-time. Relieving the developer from the burden that is keeping track of the possible computation states at runtime, preventing possible API misusage during development. While Rust does not support typestates by design, the type system is powerful enough to express and validate typestates.

This thesis' goal is to bridge the gap between typestates and production Rust, developing a practical tool enabling programmers to take advantage of typestates in their Rust code. The tool takes the form of an embedded DSL backed by Rust macros, keeping the approach grounded in Rust syntax and easy to use. The developer specifies typestates through the use of special annotations in the code. From the specification, a state machine is extracted and checked for common typestate pitfalls, thus providing correctness properties beyond simple typestates. The tool, leveraging on Rust's type system, statically ensures the compliance of the code regarding the typestate.

Keywords: Behavioral types, typestates, meta-programming, macros, Rust

Resumo

À medida que as nossas vidas estão cada vez mais dependentes de software, os erros do mesmo têm o potencial de causar problemas significativos. Prevenir estes erros torna-se uma tarefa prioritária durante o desenvolvimento de sistemas confiáveis. Erradicar erros por completo é impossível, mas é possível eliminar certos conjuntos.

Rust é uma linguagem de programação de sistemas que, por desenho, endereça erros de gestão de memória. Para o conseguir, a linguagem inclui no sistema de tipos informação sobre o tempo de vida dos objetos, permitindo assim que o compilador conheça a utilização dos mesmos e detecte erros de utilização de memória. Apesar da prevenção de erros de memória ter um papel importante na segurança de software, existem ainda outras categorias de erros em Rust, como o uso incorrecto de interfaces de programação, em que o programador não respeita as restrições impostas pela mesma, o que resulta numa falha do programa.

Typestates elevam o conceito de estado para o sistema de tipos, permitindo a aplicação das restrições da interface durante a fase de compilação. Este conceito permite assim aliviar o programador da responsabilidade que é conceptualizar e manter o estado do programa em mente durante o desenvolvimento, prevenindo o mau uso das interfaces. Apesar de Rust não suportar *typestates* de uma forma natural, o sistema de tipos permite expressar e validar *typestates*.

O objetivo desta tese é aproximar os *typestates* do Rust em produção, desenvolvendo uma ferramenta que permite aos programadores tirar partido dos *typestates*. A ferramenta toma a forma de uma DSL embebida em Rust, apoiada por macros, permitindo que a abordagem não se desvie da sintaxe de Rust e seja fácil de usar. O programador especifica *typestates* pelo uso de anotações no código. Apartir da especificação, extrai-se uma máquina de estados que é depois verificada por erros comuns de *typestates*, garantindo propriedades extra em comparação com *typestates* comuns. A ferramenta tira partido do sistema de tipos de Rust para garantir que o código está em acordo com os *typestates*.

Palavras-chave: Tipos comportamentais, *typestates*, meta-programação, macros, Rust

Contents

List of Figures

List of Tables

Glossary

Acronyms

API Application Programming Interface xi, xvii, 2, 3, 16, 25, 40, 41, 42, 45, 54, 56
AST Abstract Syntax Tree 43, 44

DFS Depth-First Search 52

p4 Pre-Processor-Pretty-Printer 21
PPX PreProcessor eXtensions 21

Symbols

1

Introduction

1.1 Context

Bugs permeate our lives as users — whether in an instant messaging application or a game they are present. Luckily, most are harmless as such applications are not critical, resulting in some unsent messages or texture glitches.

In systems programming, one of the most demanding domains in computer science, bugs and their respective consequences come at a high cost to both service providers and consumers. There are reports from several industries where bugs lead to huge monetary losses and in extreme cases, death. In 2014, the Heartbleed [24] bug, caused due to a missing bound check, compromised the security of any OpenSSL user, enabling the theft of critical information (e.g. cryptographic keys). In 2018, a bug in Coinbase (a popular cryptocurrency exchange) allowed for account balance manipulation [76]. In 2019 and 2020, after several crashes [5], the Boeing 737 Max was grounded to fix existing problems. While grounded, more software-related issues were found [50, 49], delaying re-certification. In 2020, as the number of COVID-19 cases grew, contact tracing apps were deployed as a mitigation strategy — due to a bug the UK's National Health Service app failed to ask users to self-isolate [43].

The previous examples are not isolated incidents. The language and nature of the bugs are different for each case, but to put it simply, there is no silver bullet and the next best alternative is to do our best to mitigate them — building tools and abstractions which allow developers to increase their code's safety.

1.2 Problem

Languages like C/C++ have dominated the systems programming landscape for years and one of the main problems with both is the lack of memory management. Leaving such responsibility to the developer has proven to be *a less than ideal* solution. Memory management is responsible for 70% of the bugs found in projects like Chromium [44] and Microsoft products [45].

```
Integer a = null;
a + 5; // NullPointerException: `a` is `null'
```

Listing 1.1: Java's null reference example.

To address such problem, several tools and languages have been and continue to be developed — so far, Rust has been the only one to achieve *mainstream* status. Rust aims to provide memory safety without affecting performance or productivity. To achieve such ambitious goal, Rust validates code with the borrow checker, which then enforces memory safety rules, targeting the problem at the root.

Addressing memory safety is not enough though. Languages which side-step the problem of having manual management through the use of a garbage collector (e.g. Java and Go) still suffer from other kinds of bugs. As discussed in the end of Section 1.1, we can only mitigate their occurrence, hence we are required to reach out to new mechanisms.

Typestates are an approach which aims to tame stateful computations; to do so typestates lift the concept of state to the type level, this enables the compiler to reason about state and provides the developer with information of the expected computation state at runtime.

1.2.1 The Billion Dollar Mistake

> *This led me to suggest that the null value is a member of every type, and a null check is required on every use of that reference variable, and it may be perhaps a billion dollar mistake. — [26]*

Consider Listing 1.1, the program compiles and will crash with a `NullPointerException`. While everyone can see the explicit `null` attribution the compiler does not issue an error or warning. The original author of the `null`, Tony Hoare, considers this to be his "*billion dollar mistake*". Since in complex codebases, this error is hard to track down among all possible states and has supposedly caused more than a billion dollars in damages.

While in Java it manifests as an exception, in C/C++ tracking them down is usually more complicated as the only feedback the user receives is the infamous `SEGFAULT`. Again, after so many years of programming, developers ought to have better tools, as debugging errors like these is neither an effective time use nor pleasant.

1.2.2 API Misuse

Consider Java's `Scanner`, the API allows the developer to write code like Listing 1.2. Such code will compile without issuing any errors or warnings (even with the `-Xlint:all` flag), however, it will also crash during runtime. Since it is not possible to read from a closed source, the thrown exception is an `IllegalStateException`, informing the user that the attempted operation is illegal for the current object state. Ideally we want such illegal states to be detected at compile time.

```java
Scanner s = new Scanner(System.in);          // open the stream
s.nextLine();                                // read
s.close();                                   // close the stream
s.nextLine();                                // IllegalStateException
```

Listing 1.2: Java's Scanner misuse example.

```java
Scanner[Open] s = new Scanner(System.in);    // open the stream
s.nextLine();                                // read
Scanner[Closed] s = s.close();               // close the stream
s.nextLine();                                // compile-time error
```

Listing 1.3: Typestated Scanner example. Notice how the compiler is able to detect the error.

As shown in Listing 1.3, using a *typestated* Java example, the code allows us to trace the state of the object, but even better, the compiler is now able to tell us there is an error during compilation. This approach also solves Listing 1.1, as the type is required to be explicitly *nullable*. The remaining question is:

> *How can we avoid API misusages without creating a new full-fledged programming language?*

1.3 State of the Art

Behavioral types are types which capture aspects of computation, they are further discussed in Section 2.3. The current landscape of behavioral types in mainstream languages is bare. While projects exist, most are academic and of little impact in the way programmers write their code. In this document I focus on two approached to behavioral types — session types and typestates.

Session types will often refer to endpoints and their messages, capturing aspects of communication between them. Languages like ATS provide session type features and further enable the generation of source code in other languages such as Erlang [82]. ATS also serves as research playground for other topic related with session types [81]. There are also tools that plug into existing languages. These may come under the form of libraries such as session types for Haskell [2, Section 3.3], [21, Chapter 10] and OCaml [21, Chapter 11] extending the language to provide session types through existing mechanisms. In OCaml's case, this is done without reaching for external tools or language extensions, relying purely on the existing type system. However, existing session types research is not only based on functional languages. Session C [2, Section 4.1] makes use of Scribble [83] to capture the communication pattern of the algorithm. The tool then generates the required endpoints that guide the design and implementation of the program. Java has been the target several other research efforts, for example SessionJ [2, Section 2.2.1], [30], a Java extension which is an implementation of Moose [2, Section 2.1.1]. Another session type enabling project is Mungo & StMungo [38, 77], also targeting Java. They define specification languages which check that the code complies with the required properties. StMungo converts Scribble protocols to Java classes with typestates which are then checked by Mungo, this enables developers to write effectively session-typed Java. By itself, Mungo is a typechecker with support for typestates.

Typestates capture the state of the program, allowing the developer to express the state of objects during runtime, at compile-time. I discuss typestates further in Section 2.3.2. Fugue [12] is a protocol checker that achieves similar functionality to typestates. The tool provides a series of annotations to be used in code which are then processed into protocols to be checked by Fugue. Using the tool, the authors found several errors which would inhibit application scaling in a Microsoft internal project. Languages like Plaid [1] and Obsidian [7, 8] put typestates to use, trying to bridge the gap between academia and industrial usage. Plaid is an object-oriented language with first class support for typestates. Obsidian is a relatively new language which targets the Hyperledger Fabric blockchain. The language aims to make writing smart contracts simpler and less error prone through the addition of linear types and typestate mechanisms to the language. In [7] the effectiveness of the approach is put to test, achieving positive results when compared with the Solidity programming language.

The `state_machine_future` crate [19], provides typestated futures in Rust as well as some state machine related guarantees, such as every state being reachable from the start, there are no states unable to reach the final state and that all state transitions are valid. Furthermore, these guarantees are provided at compile-time — for example, invalid state transitions will fail to compile. The crate, however, revolves around futures, requiring an asynchronous runtime and thus making it unsuitable for other kinds of applications. Other crates exist, they focus on finite state machines but are unable to provide static guarantees.

Like other mainstream programming languages, Rust does not have first class support for session types. Implementations are rare and rooted in the meta-programming system. The work done by [34, 48] introduces bi-directional session types to Rust, since then, this line of work has been expanded by [41], extending it to multiparty session types. While Rust dropped typestate support during early development (Rust 0.4), that does not mean Rust is not able to provide them. The type system is able to emulate typestates with efficiency, the approach however comes at the cost of verbosity. Regardless of the verbosity typestates are used by the embedded systems development sphere of the Rust community.

1.4 Objectives & Contributions

In this thesis I try to bridge the gap between typestates and Rust, aiming for an elegant and usable solution, allowing for effective usage of typestates in Rust. To achieve such solution I expect to develop an embedded Rust DSL, enabling the flexibility of a dedicated language inside the Rust ecosystem. To this effect I expect the contributions of this thesis to be a typestate specification DSL to be embedded in Rust, this topic is further developed in **??**.

Typestate DSL. One of the main goals of the DSL is to be non-intrusive and easy to pick up — both the syntax and tooling. Such requires the syntax to extend over Rust's current syntax, introducing minimal changes where necessary. However, it should also be powerful enough to specify useful protocols in it.

Static Guarantees. As any language, it is useless if no information is extracted from it, besides the obvious parsing step, the DSL should be able to extract a typestate model from the original specification and generate adequate output code. The extracted model should also be checked for a series of properties such as state reachability and termination.

Tooling & Usability. The DSL should not require more than the import of the library, building any project using the DSL should not require extra steps as it would degrade possible adoption. A survey should accompany the final product to confirm usability claims.

Artifacts. Finally, the DSL should be shipped as a crate (i.e. library) and available in `crates.io`, Rust's package registry, this implies that the documentation should be available in `docs.rs`. In addition to the DSL library, I am planning writing an article on the DSL, including the results from usability testing, and developing a library to facilitate DSL development for Rust.

1.5 Report Organization

This document is organized as follows:

Chapter 2 provides a review over existing systems programming languages (Section 2.1), the Rust programming language (Section 2.2) and behavioral types (Section 2.3).

Chapter 3 describes existing work regarding language preprocessing (Section 3.1), Rust macros (Section 3.2) and existing approaches to behavioral types (Section 3.3).

?? illustrates the development roadmap of this project, detailing the required work to achieve the goals proposed in Section 1.4.

2

Background

2.1 Systems Programming Languages

The definition of the term *systems programming language* is not agreed upon, being somewhat flexible and ever-changing due to constant shift in requirements for applications.

Before the cloud, in the age of C, a systems programming language would most likely be a language able to provide an adequate interface between the programmer and the machine. Nowadays, the definition is more vague, as machines and software grow in complexity, and the definition of system grows from single computer to a distributed system, interfacing with the hardware in a more direct fashion is mostly not required. Systems programming languages become about being able to produce a standalone binary able to run on a variety of machines without requiring extra software.

2.1.1 C

C is a general-purpose programming language, while it can be considered a high-level programming language when put besides assembly, it also fits the description of a low-level level programming language when besides languages like Python. It was originally designed by Dennis Ritchie for the PDP-11 and has been around since 1972 [4], C is by no means modern, being older than myself and most likely to outlive me.

Designed in a different time, C's mental model is also different, the language is simple and straight forward, the designers had goals to achieve and designed the language with them in mind. Such mentality is noticeable when using the language, it is simple as the hardware was and the level of control C provides is unparalleled, being both a major benefit and a hindrance. An expert programmer is able to take advantage of the language to produce highly-efficient software, but a novice programmer will often find himself battling memory and pointer management bugs.

The language influence echoes in the modern languages, whether in the form of syntax (i.e. the famous C-style syntax) or in the problems it tries to solve. Languages such as Java take from C their syntax as well as one problem to solve, memory management; other languages like Julia [3] aim to achieve similar performance.

While not as popular as other languages, C was able to stay relevant in the modern development landscape, some of the most used software in the world is either written or powered by C. The Linux kernel, which powers servers, the world's most powerful computers and serves as a base for Android and other mobile devices, git, Redis and nginx are also software examples which reached the top of their respective fields.

2.1.2 C++

Introduced in 1985 as an extension to C; the author, Bjarne Stroustrup writes:

> *C++ is based on the idea of providing both:*
>
> - *direct mappings of built-in operations and types to hardware to provide efficient memory use and efficient low-level operations, and*
> - *affordable and flexible abstraction mechanisms to provide user-defined types with the same notational support, range of uses, and performance as built-in types.*
>
> — *[65, Section 1.2]*

The language has since gone on to conquer the programming world, being used in a wide variety of software and hardware. Currently, companies such as Google, Amazon and Microsoft have widespread adoption of C++ in their codebases. Industries requiring the best performance as possible of the host, such as scientific computing, financial software, AAA games and visual effects will most likely be running C++.

Just like C, C++ is far from perfect. The language is enormous, with very complicated parts (e.g. templates) and compilation for big projects is very slow, the author acknowledges this in [70]. Furthermore, as the language provides a high level of control over the system, it has manual memory management, suffering from the same problems as C. Even with smart pointers (e.g. `unique_ptr`) the problem is not considered solved, as they introduce overhead in the most demanding applications.

2.1.3 Ada

Ada was developed in 1980, during a standardization effort in the USA's Department of Defense, with the goal of unifying projects spanning over 450 programming languages [66]. Ada's main focus was the development of embedded applications, currently the Ada language is mostly used in the critical domain due to the strong emphasis on safety, some Ada success stories are the London Metro Victoria Line and the Paris Metro Line [59]. The language is also used in several other domains, such as aviation, space vehicles, financial systems and more [18].

In comparison with the other languages in this section, Ada is eclipsed, barely showing in the GitHub rankings [51]. However, given that Ada's compiler is mostly a product, it makes sense that most Ada code is not open-source. Regardless, when one views the list of features Ada has, the first arising question is "*why is Ada not popular?*".

An old article in AdaPower [23] provides some possible insight over the question, referring to the compiler's price and the Hoare's harsh critics. From my point of view, the critics to the compiler and ecosystem pricing still make sense, as access to the full tooling is limited. The lack of programmers goes on to deepen the lack of adoption in the industry and this cycle ends up limiting Ada's reach in the market.

2.1.4 Go

The Go programming language (or `golang`) is a Google project, according the language folklore, it was designed by the authors while they waited for their C++ code to compile. Go tried to address several of the criticisms to C, namely memory management, which it solved by using a garbage collector. While it has made a name for itself in the network and distributed systems sector, being the main language behind projects like Docker [13] and Kubernetes [40], Go's categorization as a systems programming language can be discussed.

Sometimes, however, the performance might not be enough, as was the case for Discord, the popular internet voice server company, as demand increased, Go was not able to meet the expected performance requirements and the company replaced it with Rust [29]. In [70], one of Go's authors, Rob Pike, says that he regrets categorizing Go as a systems programming language, being rather a server programming language that evolved into a cloud infrastructure language. Regardless of discussion, Go has proven to be a viable alternative to existing counterparts, compromising extreme performance in name of safety and simplicity.

2.1.5 Summary

I reviewed four system programming languages, suited for different kinds of environments, C, C++ and Ada can be considered the traditional system languages kind, with a strong emphasis on efficiency and support for embedded devices. Go on the other hand, could be considered a new generation systems programming language, a language for cloud infrastructure. Among the four, only Ada places strong emphasis on safety, with several features allowing for more guarantees at compile time, such as contract based programming and non-nullable types by default, being the only one which does not suffer from the "*billion dollar mistake*" [26].

2.2 The Rust Language

Rust is a fairly recent systems programming language, it started as a side project of the author Graydon Hoare and the language public history dates back to 2010 [25]. In 2012

Mozilla picked up Rust to help develop the Servo browser engine, the successor to the previous Gecko engine; as a way to test Rust's capabilities [35].

2.2.1 What makes Rust different?

In comparison with other languages, one of the first things someone new to Rust ought to notice is the emphasis put on safety. Being a competitor to C++ and achieving memory safety while still providing C++-level performance is quite an accomplishment. Rust, however, also aims to allow users to be productive without sacrificing safety or performance.

The key to all the promises Rust makes is the ownership system and borrow checker. The borrow checker is a completely new mechanism when compared with other mainstream languages. However, it is a product of years of research both in academia and the industry. This mechanism merits most of Rust's accomplishments and also the biggest problem, the learning curve. While Rust has become more accessible over the years, ownership and the borrow checker still require some effort on the part of the developer to learn. I provide a small overview of ownership, the borrow checker and their part in Rust's promise of "*fearless concurrency*".

2.2.2 Ownership

Ownership is the mechanism used by Rust to ensure no memory block stays allocated longer than it is required to. Through ownership, the compiler is able to free memory when required, inserting the respective deallocation calls in the output program. Behind ownership, there are three rules:

> - *Each value in Rust has a variable that's called the owner.*
> - *There can only be one owner at a time.*
> - *When the owner goes out of scope, the value will be dropped.*
>
> — *[68, Section 4.1]*

To illustrate the rules, consider Listing 2.1, where we have two variables `x` and `y`. First, `"Hello"`[1] is assigned to `x`, thus `x` now owns `"Hello"`. After, `x` is assigned to `y`, consider the second rule of ownership, since we can only have one owner, `x`'s value ownership is transferred to `y`. Since we transferred `x`'s value to `y`, `x` is no longer valid, consequently, when compiling the code an error will be issued due to `x` being moved.

Notice how `String::from` is used instead of another type, since `String` type does not implement `Copy` it can only be moved. If the used type implemented `Copy`, the value would have been copied instead of moved.

So far this illustrates the first two rules. The last rule can be considered invisible, as it happens during compilation and the user would not notice it usually. What happens is that at the end of the scope, any variable whose owner is in scope, will be freed. While

```rust
let x = String::from("Hello");  // ok: `x` is assigned "Hello"
let y = x;                      // ok: `x` is moved into `y`
println!("{}", x);              // error: `x` was moved in the previous line
```

Listing 2.1: Example of the move-by-default mechanism to enforce ownership.

```rust
let x = String::from("Hello");  // ok: `x` is assigned "Hello"
let y = &x;                     // ok: `x` is borrowed to `y`
println!("{}", x);              // ok: `x` can be printed since it is still valid
```

Listing 2.2: Example using borrowing to allow for more than one reader on the same variable.

the developer is not required to explicitly free the memory, the compiler will insert the calls for the developer.

2.2.3 Borrowing

If the developer could only copy or move memory the usability of the language would be severely limited. For example, functions that read a variable and produce a new value, not requiring the variable to be consumed would be impossible. To cope with this, Rust allows values to be *borrowed*, in other words, the owner of the variable allows for it to be read by others.

To borrow a value, one writes `&value`, this creates a read-only reference to `value`. There can be an unlimited number of read-only references to a value, but only a single mutable reference. This is discussed in Section 2.2.4. Consider the example Listing 2.2. In the example, `x` is now possible to be printed since it was not moved into `y`. Rather, `y` borrowed `x` through a reference.

Going back to the rules (Section 2.2.2), Rust's references obey them just like all other values. The variable containing them has ownership *over the reference*; it still is a single owner (if `let z = y;` was to be added, the reference would be copied instead of moved); and finally, when the owner goes out of scope *the reference is dropped*, but not the original value.

Mutable Borrows

One last thing to consider are mutable borrows. As previously discussed, in Rust it is possible to create multiple immutable references but only one mutable reference. Regarding mutable references there are two cases to consider:

N **mutable references,** see Listing 2.3. Understanding why only one mutable reference can exist at a time is trivial, as multiple mutable references to the same object would allow it to be mutated concurrently, which could lead to inconsistent values.

```rust
let mut s = String::from("hello");
let r1 = &mut s; // ok: first mutable borrow
let r2 = &mut s; // error: `s` was mutably borrowed in the previous line
```

Listing 2.3: Example error while using multiple mutable borrows over the same variable.

```rust
let mut s = String::from("hello");
let r1 = &s;     // ok: first immutable borrow
let r2 = &s;     // ok: second immutable borrow
let r3 = &mut s; // error: `s` was immutably borrowed in the previous lines
```

Listing 2.4: Example error while using a mutable borrow in conjunction with immutable ones.

N **immutable references and** 1 **mutable reference,** see Listing 2.4. The reason behind not allowing a mutable reference to coexist is similar. Consider that each value can be executed by a different thread, the first two (`r1` and `r2`) are only read and the third (`r3`) can be read and written. While there will be no conflicts between writers, it is possible for the readers to read an inconsistent value, since it can happen during the write operation.

2.2.4 Concurrency

> *Initially, the Rust team thought that ensuring memory safety and preventing concurrency problems were two separate challenges to be solved with different methods. Over time, the team discovered that the ownership and type systems are a powerful set of tools to help manage memory safety and concurrency problems! By leveraging ownership and type checking, many concurrency errors are compile-time errors in Rust rather than runtime errors. — [68, Section 16]*

Rust provides several kinds of mechanisms to prevent concurrency related problems. Mechanisms as *message-passing*, *shared-state* and traits to enable developers to extend upon the existing abstractions.

Message-passing

Rust's message-passing library is inspired on Go's approach to concurrency, prioritizing message passing over other kinds of concurrent approaches, such as locking.

> *Do not communicate by sharing memory; instead, share memory by communicating. — [15, Concurrency]*

Rust defines channels which have two ends, the transmitter and the receiver. The former can also be seen as the sender, and when is declared with the message type, the latter is also declared with the message type, they can be the same or distinct.

The ownership system comes in when the transmitter sends a message, when received the ownership of the message is taken on by the receiver end. This enforces that values cannot be in both sides of the communication at the same time, preventing concurrent accesses.

Shared-state

Along with message-passing, Rust allows memory to be shared in a concurrent, safe way. Just as before, Rust's ownership system also helps with mutexes' biggest problem, locking and unlocking.

In a language like Java, whenever a thread is able to call `lock` on a mutex, it is required to call `unlock` on it, only then can other threads can use it. The problem is that this approach is subject to human error, forgetting to call unlock or calling unlock in the wrong place is possible. Making use of the ownership system, Rust is able to know when the lock reached the end of the scope and should be dropped.

2.2.5 Why Rust instead of Language X?

The main obstacle between typestates and programming languages is the requirement for aliasing control. In short, typestates are incompatible with aliasing (details are provided in Section 2.3.2).

So to implement a language from the ground up, it is required that aliasing is handled, however, instead of building a new one, the goal is to extend an existing one, Rust. As discussed in Section 2.2.3, Rust's ownership system allows for aliasing control. Using moves to enforce the consumption of values, immutable references for pure functions and mutable ones for limited mutability, it is possible to emulate typestates. This takes care of aliasing concerns.

When designing on top of another language, two more ingredients are required, a powerful extension mechanism (i.e. Rust's macros, discussed in Section 3.2) and a strong type system, able to provide the necessary abstractions. Rust provides both, the type systems goes as far as allowing zero-sized types, allowing type-level abstractions to incur no runtime overhead. This is a key ingredient in our DSL, aiming to provide the minimal possible runtime with an expressive language.

2.3 Behavioral Types

As previously discussed, with the growth in software complexity, developers are required to develop better tools to tame such complexity. Such tools require a theoretical body of work to support them, behavioral types are part of such body of work. The theory behind them encompasses several domains, and they can be applied over a wide range of entities, from an object to a web service.

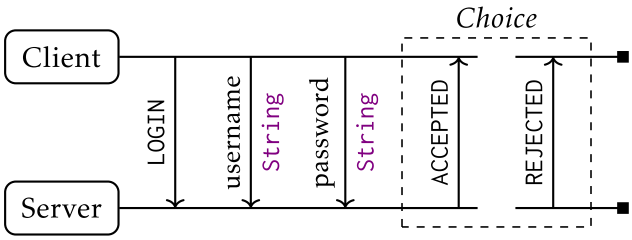

Figure 2.1: Communication protocol example. The communication establishment step is omitted for simplicity. In this protocol the client tries to login to a service by sending a message `LOGIN` followed by the username and password, both of type `String`. The server then replies with either an `ACCEPTED` or `REJECTED`, if the login was successful or not, respectively.

The work on behavioral types arose in the context of type systems able to capture properties of computations [31]. Session types and typestates are part of this field of study, both capturing distinct property kinds while aiming for a common goal, stronger type systems and better static assurances.

> *Roughly speaking, a behavioral type describes a software entity, such as an object, a communication channel, or a Web Service, in terms of the sequences of operations that allow for a correct interaction among the involved entities. — [2]*

Behavioral types allow developers to model a protocol, define the communication messages and possible interactions and check that certain requirements are met when implementing. Consider the protocol from Figure 2.1, where a user tries to authenticate. A developer can use it as a specification (for simplicity consider the uppercase messages to be simple strings), using behavioral types the developer could be able to specify the described interactions and all boilerplate could be generated for him. While using strings as a payload is not very "*interesting*", consider instead that the object in transit is an encrypted payload, the boilerplate will take care of decryption and deserialization. Furthermore, consider the constraint that *all interactions end with a message from the server*. If the specification has an interaction that is not compliant with such rule, the code should not compile, raising an error.

2.3.1 Session Types

Session types are a subset of behavioral types, focused on communication, from entities in a distributed system to threads in a computer. Session types are based on process calculi and can be thought as "*types for protocols*" [27, 28]. They elevate communication to the type level, allowing expressing them as types in a program, in turn this enables the compiler to reason about the protocol during compile-time [75, 22].

In Rust, a channel is created with `let (tx, rx) = channel::<SenderT, ReceiverT>()`, where `SenderT` and `ReceiverT` are the types sent and received by the channel. Channels

$$\begin{aligned}
\textbf{Login} &:= \{user : \texttt{String},\ password : \texttt{String}\} \\
\textbf{Message} &:= \{user : \texttt{String},\ message : \texttt{String}\} \\
\textbf{Status} &:= \{user : \texttt{String}\} \\
\textbf{SReply} &:= \{status : \texttt{String}\} \\
Server &= ?\textbf{Login}.\oplus\langle !Ok.?\textbf{Message}.\oplus\langle Ok.End, Err.End\rangle, !Err.End\rangle \\
Client &= !\textbf{Login}.\&\langle ?Ok.\&\langle ?\textbf{Status}.!\textbf{SReply}, !\textbf{Message}.\&\langle Ok.End, Err.End\rangle\rangle, ?Err.End\rangle
\end{aligned}$$

Figure 2.2: Session type example, equivalent to **??**.

are well-typed, meaning that if `SenderT = String`, sending another type over the channel will result in a type error.

Session types extend on this notion, not only allowing for a single type to be sent or received, but also model the protocol. Consider **??**, the example has unnecessary complexity, for each receive the developer is required to match all possible replies. Ideally, we declare the steps and possible outcomes beforehand.

For example, in plain English:

1. Send login credentials.
2. If successful, send a message to user `jmgd`.
3. Otherwise, exit.

And now using session types (Figure 2.2 with syntax adapted from [75], where the first four assignments (:=) are simple aliases, to simplify reading):

Consider ! to be *sends*, ? to be *receives*, . the *sequence* operator finally, & the *choice offering* and ⊕ the *choice selection*. Using session types effectively offloads complexity to the type system, resulting in more complex types, but simpler implementations, since protocol compliance can be checked during compilation and boilerplate can be added by the compiler. No message is matching required, the compiler does it for the developer. Using session types it is possible to write it in a simpler form, where a type is assigned to each endpoint. Notice how the server provides more than one operation, but the user does not call them all.

2.3.2 Typestates

> *... traditional strong type checking was enhanced with **typestate checking** a new mechanism in which the compiler guarantees that for all execution paths, the sequence of operations on each variable obeys a finite state grammar associated with that variable's type. — [64]*

The first language to make use of typestates was NIL [64], afterwards languages like Hermes [63] and Plaid [1] extended the concept with new techniques.

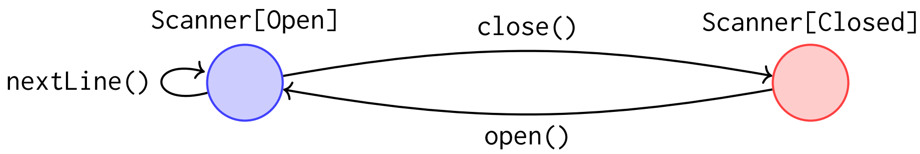

Figure 2.3: The `Scanner` typestate automata, based on Listing 1.3.

Automata

A possible question on the reader's mind is "*how are automata and typestates related?*". This section tries to address that question and exemplify how automata helps prove typestates properties. It is possible to express typestates as automata, as the reader can observe in Figure 2.3. Each state is a possible state the object can be in, transitions are done through methods. Methods can either mutate the object state, such as `open` and `close`, or leave it unchanged, such as `nextLine`.

Real-world scenario. In production applications, the API is not this simple. In fact, the `Scanner` API is not this simple, however it was simplified for the example. Complex APIs can be designed by a team and implemented by another, specifications can be changed and during project development some details may be lost. Such details can be costly, imagine for example that a method call reaches a state, which has no outgoing edges, but it is not a final state. This is a problem addressed by existing automata algorithms. Representing typestates as automata, extracting all necessary information and applying such algorithms provides the API with extra safety.

The case for typestates

As discussed in Section 1.1, bugs in systems programming are costly, thus, bugs must be minimized. Several tools, such as static analyzers, fuzzers, testing frameworks and others, aid in this purpose, if we have all these external tools, why should we not try and leverage the programming language itself?

Moving towards better languages. Programming languages allow the programmer to express a set of actions to be taken by the computer, they are tools which enable us to achieve a goal. Being essential to our work, better tools enable developers to be more productive and achieve higher quality work. The remaining question is "*why do we not create better languages?*". Even when considering languages to be cheap to develop, the amount of work between a *working* language to be *production ready* is not cheap. Furthermore, while adopting a new language for a hobby project is easy, the same does not apply for enterprise level projects, requiring several developers to know the ins and outs of the language.

Static typed languages. The current trend is to move from dynamically typed languages, to statically typed ones, or at the very least, add typing support to existing dynamic languages. Typescript [72], Reason [55] and PureScript [53] are all examples of languages

```java
1 public class Read {
2     public static void main(String[] args) {
3         Scanner s = new Scanner(System.in);
4         s.nextLine();
5         s.close();
6         s.nextLine();
7     }
8 }
```

Listing 2.5: The Read Java program, which reads two lines from stdin.

built to bridge the gap between static type systems and JavaScript. Python and Ruby, two popular dynamic languages, have also pushed for type adoption with the addition of type hint support in recent releases [73, 58].

Where do typestates fit? Typestates are a complex subject, able to be adopted at several levels, just like type hints, they can be partially used in some languages, through tools such as Mungo [77], by contract-style assertions as in Ada2012, Eiffel or pre-0.4 Rust, or finally by leveraging the existing type system to write typestate enabled code as it is possible in Rust [14]. Typestate-related concepts were also used in Singularity OS [2, Section 6], a reliable operating system prototype where programs were written using Sing# — a language derived from C# which supports behavioral typing, specifically contracts in a similar capacity to typestates.

Why use typestates? By leveraging the state to the type system, the compiler is able to aid the programmer during development, a given set of transitions will be impossible by default, since the types do not implement them. By reducing the need for developers to check for a certain set of conditions through the use of typestates, it becomes possible to reduce the number of runtime assertions and completely eliminate the need for illegal state exceptions since illegal transitions are checked at compile time.

Typestates in action

As a simple example, consider the Java application in Listing 2.5 which simply which reads two lines from `stdin`. The application will throw an exception on line 6, since the programmer closed the `Scanner` in line 5. In this example, the error is simple to catch, the program is short and the `Scanner` can either be open or closed, however, real-world applications are not that simple.

In the case of *typestated* programming, the type system will provide the programmer with better tools to express state, furthermore, the compiler will then catch errors regarding state, such as the previous *use-after-close*.

Listing 2.6 shows the `Read` program written in a *typestated* fashion, notice that the `Scanner` type is now augmented with state and the compiler is able to catch the misuse of the `Scanner[Closed]` interface.

```
public class Read {
    public static void main(String[] args) {
        Scanner[Open] s = new Scanner(System.in);
        s.nextLine();
        Scanner[Closed] s = s.close();
        s.nextLine(); // compiler error
    }
}
```

Listing 2.6: The Read program, written in a Java-like *typestated* fashion.

```
state File {
    val filename;
}
state OpenFile case of File = {
    val filePtr;
    method read() { ... }
    method close() { this <- ClosedFile; }
}
state ClosedFile case of File {
    method open() { this <- OpenFile; }
}
method readClosedFile(f) {
    f.open();
    val x = f.read();
    f.close();
    x;
}
```

Listing 2.7: The `File` declaration and usage in Plaid (taken from [47]).

Plaid is a typestate-oriented programming language [1], instead of `class`es users write `typestate`s. Each typestate represents a class and possible states, the class methods and behavior change during runtime as state changes, in contrast with other languages (e.g. Java) where public methods and fields are always available. In Listing 2.7, the `File` passes through states as it is open, read and closed in `readClosedFile`.

This property allows the type system to enforce certain properties at compile time, such as certain methods will never be called in a given state since it is not possible by design (i.e. they are not available in the interface).

Obsidian is a language targeting Hyperledger Fabric [20], among other features it makes use of typestates to reduce the amount of bugs when dealing with assets.

In [7] an empirical study tested and proved Obsidian claims, when compared with Solidity, the leading blockchain language, users inserted fewer bugs and were able to start developing safer code faster.

Consider Listing 2.8, in which a light switch is modeled, the same can either be `On` or `Off`, but not both. The `brightness` field can only be accessed if `LightSwitch` is in the `On` state, however the `switchLocation` field can be accessed from both states. Furthermore,

```
contract LightSwitch {
    state On {
      int brightness;
    }
    state Off;
    int switchLocation available in On, Off;
}
```

Listing 2.8: Obsidian state declaration example.

```
transaction OffToOn() {
   LightSwitch s = new LightSwitch(); // LightSwitch is in Off upon instantiation
   s.turnOn();
}
```

Listing 2.9: Correct state usage example in Obsidian.

```
transaction OffToOff() {
   LightSwitch s = new LightSwitch(); // LightSwitch is in Off upon instantiation
   s.turnOff(); // error: turnOff() requires that s is On, but here s is Off
}
```

Listing 2.10: Invalid state transition example in Obsidian. Since `LightSwitch` is instantiated as `Off`, calling `turnOff` is not valid.

consider that upon instantiation, the `LightSwitch` is set to the `Off` state. Notice that in Listing 2.9 the user is able to call `turnOn`, as the switch is in the `Off` state, as expected. However, the user is unable to call `turnOff` in Listing 2.10, since the switch is already set to the `Off` state. The Obsidian compiler is able to notice such invalid transitions and provide an error during compile time.

Rust. As discussed in Section 2.2, Rust takes the commitment with safety with seriousness, providing the necessary tools to users. While Rust does not support first-class typestates, it is possible to emulate them using the type system (as demonstrated in [14]), this is discussed in further sections of this document.

While the file example does not apply in Rust, since files and other objects are closed as they leave the scopes, enforcing protocols is important and an aspect not covered by the language. Consider Listing 2.11, the example is expected to call first `F1`, followed by `F2` and finally `F3`, however such does not happen and the error may only be caught during runtime.

As the next paragraph discusses, this behavior can be prevented using the language's type system. However, such utilization requires complex (and possibly hard to read) types. Since it is not "*part*" of the language, most users will neither use it nor be aware of it.

Embedded Rust. As any systems programming language, Rust penetrated the embedded development space. Providing features in line with the area's requirements, along with

```rust
fn main() {
    let protocol = Protocol::new();
    protocol.F1();
    protocol.F3(); // possible crash during runtime
    protocol.F2();
}
```

Listing 2.11: Rust example of an unchecked failure protocol compliance. The protocol expected operation order is `F1`, `F2`, `F3`, however, the developer placed the operations in the wrong order. This mistake is only caught during runtime.

community efforts to make Rust viable in embedded systems.

The Embedded Rust Book's [67] Chapter 4 is dedicated to static guarantees, introducing programmers to the concepts of typestate in Section 4.1, and their usage in embedded systems.

As for real-world usage, typestates are abundantly used in the area (not just discussed in the book), under [61] one finds several repositories (suffixed with `-hal`) which implement typestates (e.g. `gpio.rs` from `stm32h7xx-hal`).

3

Related Work

3.1 Language Preprocessors

Language preprocessors are a mechanism which runs during compilation, some languages will apply the preprocessor during different compilation stages while others will only apply the preprocessor in a single stage.

3.1.1 OCaml

The OCaml ecosystem currently uses OCaml PPX (PreProcessor eXtensions), previous to version 4.02, OCaml made use of p4 (Pre-Processor-Pretty-Printer), also known as Camlp4.

Camlp4 is a parsing library which provides extensible grammars, allowing users to extend OCaml syntax, Camlp4 is also able to redefine the core syntax, OCaml even introduced a revised syntax [54] to enable Camlp4.

In a nutshell, the Camlp4 library would allow developers to develop an extension syntax, when the compiler would pass the source code as text to the preprocessor, which, in turn would generate valid OCaml source code. The library has been deprecated due to being confusing to users and tools alike. Users were required to learn the revised OCaml syntax which complicates the development process. These criticisms are found throughout documents which discuss Camlp4 [78].

PPX

In OCaml version 4.02 syntax extensions were introduced, to enable preprocessor extensions. This meta programming mechanism came to replace Pre-Processor-Pretty-Printer (p4), which was not well liked by the community given it was too complex. The resources on PreProcessor eXtensions (PPX) are not as widespread as the resources for similar mechanisms in other languages (i.e. Rust macros). There are two main entry points to the PPX system, attribute and extension nodes [42, Sections 8.12 & 8.13].

```
let a = 12 [@attr pl]
let b = "some string" [@@attr pl]
[@@@attr pl]
```

Listing 3.1: Example of the three kinds of attributes, taken from [56]. The first line attaches to the 12 expression. The second attaches to the whole `let` binding (i.e `let b = "some string"`). Finally, the third line, does not attach to a particular member of the AST.

Attribute Nodes are attached to the existing AST nodes, they are not forcefully compiled, that is, if the compiler is not aware of a matching extension they will be ignored. There are three kinds of attribute nodes (example in Listing 3.1):

> - `[@attr payload]` - *attached with a postfix notation on "algebraic" categories.*
> - `[@@attr payload]` - *attached to "blocks" such as type declarations, class fields, etc.*
> - `[@@@attr payload]` - *not attached to any specific node in the syntax tree.*
>
> — *[42, Section 8.12]*

One of the main kinds of PPXs are *derivers* (see Listing 3.2.2 for the Rust equivalent). Deriveres are mostly used to generate error-prone code where the implementation pattern is common to a series of sittuations. Examples include but are not limited to: comparison functions, pretty printers and serializers [56].

Extension Nodes are similar in syntax to the attribute nodes (instead of `@` they use `%`). Extension nodes are meant to be placeholders in the syntax tree. That means they get replaced with the expanded code (like attribute macros in Rust Listing 3.2.2). They are also required to be expanded by a PPX during compile-time, if such does not happen an `Uninterpreted expression` error is issued.

> - `[%attr payload]` - *used for "algebraic" categories.*
> - `[%%attr payload]` - *used in structures and signatures, both in the module and object languages.*
>
> — *[42, Section 8.13]*

Ecosystem Presence. The current state of affairs regarding the PPX brings up mixed reactions. From my research, the environment is well maintained, with regular commits to the main PPX repositories. However, the entry-barrier is high due to the lack of introductory materials. Despite this, PPX has seen use in the ReasonML community, more specifically in the ReasonReact framework, where the Tailwind CSS dialect is supported by PPX to enhance developer ergonomics.

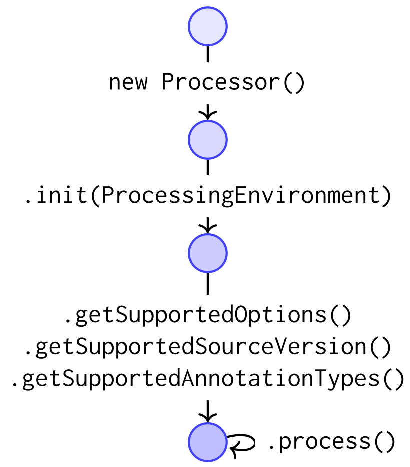

Figure 3.1: Java's annotation processor lifecycle.

```
@Retention(RetentionPolicy.RUNTIME)
@Target(ElementType.ANNOTATION_TYPE)
@interface Foo {}
```

Listing 3.2: Example code for Java's annotation declaration.

3.1.2 Java

In Java, meta programming takes the form of annotations, these are processed by user code during the compilation process. Besides annotations, there is another project able to "*extend*" Java. The ExtendJ research compiler (formerly JastAddJ) [16] aims to provide a "*hackable*" Java compiler for research purposes, such as static analysis tool development to Java features prototyping.

Java Annotations

Java annotations were first introduced in Java 5 [10], they are a form of metadata which can be added to Java source code. Annotations can be used in conjunction with several components of the Java language, such as classes, interfaces, documentation and others. These are processed by build-time tools or by run-time libraries to achieve new semantic effects, a popular example of such library would be the compile-time dependency injection framework Dagger 2 [9]. Another popular library using annotations is the Checker Framework [6], besides the classic `@NonNull` example, the tool provides several other kinds of annotations. The annotations are then checked by Checker Framework annotation processor. An example would be the `@Tainted`/`@Untainted` annotations, which serve the purpose of annotating data to indicate whether it can be trusted. This helps avoid potentially harmful code from being executed (e.g. malicious SQL queries).

Implementing an Annotation. To implement an annotation, start by declaring it as in Listing 3.2. The annotation may contain parameters that allow to add configuration when the declaration is used. Supported types are:

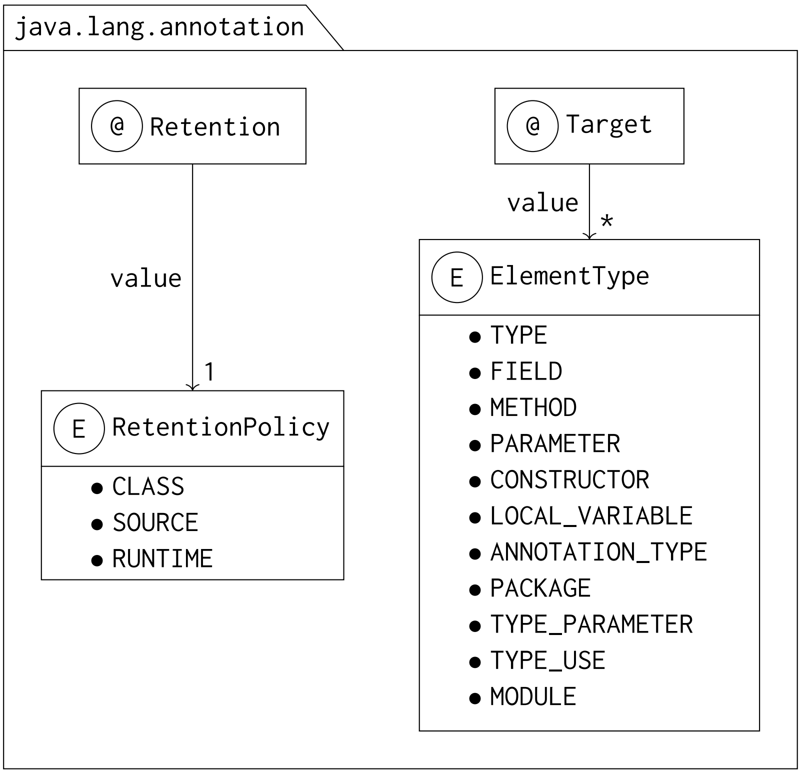

Figure 3.2: `java.lang.annotation` class diagram.

- Primitive types (e.g. `int`, `long`, etc).
- `String`
- `Class<T>`
- `enum` types.
- Other annotation types.
- An array of the above.

At this point the annotation is processed by the compiler but does not do anything useful. To address that, the code needs to either handle the annotation at runtime, through reflection. Or at compile-time, through an annotation processor. Since processing the annotation at runtime incurs a cost, I'll only discuss the annotation processor approach.

Annotation Processor. Putting it simply, is a specific class registered at compile-time as able to process annotations. The compiler can then make use of the class to process the new annotations. The class itself will usually extend the `AbstractProcessor` class, overriding some methods present in Figure 3.1. The processor will then be called for each annotation belonging to the package.

Annotation processors are also able to generate code. This is usually done by means of a library such as JavaPoet [60]. After generation, the output code is then compiled and subject to the same treatment as handwritten files. If the generated code, generates more code, this process repeats itself until no more code is generated.

```
@any Person people;
people += new Person("Bob");
people += new Person("Gene");
people += new Person("Tina");
for (Person person : people) {
    System.out.println(person.getName());
}
```

Listing 3.3: The `@any` annotation allows an object to carry several instances of itself. In the example, `@any Person` is rather a collection of `Person`. This extension is enabled by the ExtendJ compiler.

Ecosystem Presence. Java annotations are ubiquitous. Examples include but are not limited to the development of REST APIs, Android applications and database tools. As discussed in Section 3.1.2, annotations are picked up by several tools and serve a plethora of purposes, from cutting boilerplate to providing an extra layer of security and assurance. However, being ubiquitous does not imply that resources are widely available. Learning to develop annotations seems to be an almost exotic topic in Java, with few quality resources available.

ExtendJ & JastAdd

ExtendJ is an extensible compiler aiming at facilitating the development of Java compiler tools. The compiler supports Java from version 5 up to 8. The extensions are written in JastAdd [33], a meta-compilation system upon which ExtendJ is built. It is possible to extend the compiler during any of the following phases: *Scanning*, *Parsing*, *Analysis* and *Code Generation*. Extending the language with new syntax requires the modification of the *Scanner* and *Parser*. The *Analysis* phase occurs after parsing, when types are checked. Hence, to extend type analysis, one must modify it in the compiler. Finally, *Code Generation* has two possible extension methods in ExtendJ: *direct bytecode generation* and *desugaring*. The latter being the simpler approach and recommended being tried before the former. Desugaring can be used to prototype new languages constructs, by mapping them to the respective Java code.

Ecosystem Presence. While both ExtendJ and JastAdd are powerful tools, they lack of support for versions after Java 8. Their usage is generally confined to academia being unsuited for industrial usage. Documentation on getting up and running is also limited, being mostly based on papers and examples rather than entry-level explanations.

3.1.3 Kotlin

While Kotlin also allows and makes use of Java annotations, it is also possible to write plugins for the Kotlin compiler. Compiler plugins are much more complex pieces of software in comparison with annotations, due to the amount of detail required to take into account. An example of such detail is the amount of Kotlin backends available, not all targeting the Java Virtual Machine. This is also a motivation to write a compiler plugin, as annotations may not be compatible with all backends.

Kotlin Compiler Plugins

The Kotlin compiler plugin stack is illustrated in Figure 3.3. From top to bottom, the first two parts are related to Gradle, the main build system for Kotlin. These parts to not work on the plugin itself, but rather help the plugin coexist with the rest of the Kotlin ecosystem.

`Plugin`. The plugin interacts only in the Gradle segment, it provides an entrypoint from a `build.gradle` plugin and allows plugin configuration.

`Subplugin`. The subplugin acts as the glue between Gradle and Kotlin. It sets up a series on options for the layer below from the configuration provided in the first layer. It also defines a plugin ID to avoid name clashing with other plugins and Maven coordinates, which allow the plugin to be downloaded.

`CommandLineProcessor`. This layer reads the arguments for `kotlinc -Xplugin`. The options from the previous layer are passed through here. Finally, it writes `CompilerConfigurationKeys` which will be passed to the layer bellow.

`ComponentRegistar`. This component just reads the passed keys and registers extensions to be used by the compiler. It is possible to register several extensions at a time.

`Extension`. The extension is the main part of the plugin. There are multiple types of extensions able to deal with the input at different levels, from the class level to the code generation.

Ecosystem Presence. Just like the previous languages, the Kotlin compiler plugins suffer from the same discoverability problem. While depending on it are widely used (e.g. Kotlin serialization [37]), the resources to learn how to develop such tools are rare.

3.2 Rust Macros

Just like C and C++, Rust offers macros as part of the language. In essence, Rust macros are just like other languages macro's, running during compile-time to generate code. In Rust, macros refer to a family of features (see Figure 3.4), *declarative* macros and *procedural* macros.

3.2.1 Declarative Macros

Declarative macros (also known as *macros-by-example*) can be declared with `macro_rules!` and are called with function syntax (see Listing 3.4).

> *Each macro by example has a name, and one or more rules. Each rule has two parts: a matcher, describing the syntax that it matches, and a transcriber, describing*

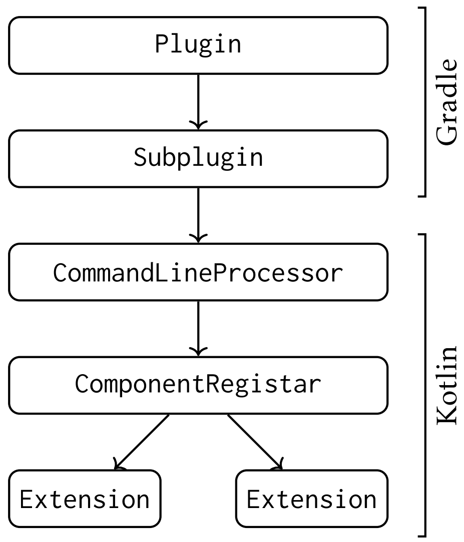

Figure 3.3: Kotlin compiler plugin architecture stack [46].

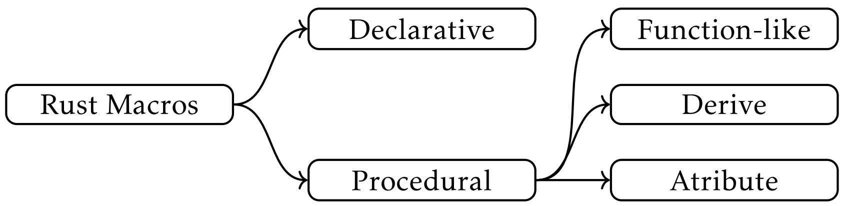

Figure 3.4: Rust macro's family tree

> *the syntax that will replace a successfully matched invocation. Both the matcher and the transcriber must be surrounded by delimiters. Macros can expand to expressions, statements, items (including traits, impls, and foreign items), types, or patterns. — [69, Section 3.1]*

Transcribing. When a macro is invoked, the macro expander loops through the declared rules, transcribing the first successful match. It transcribes the first successful match; if this results in an error, then future matches are not tried. An error is thrown if the compiler cannot determine unambiguously how to parse the macro [69, Section 3.1 - Transcribing].

Metavariables. To specify a macro a user first declares a pattern which will match a given form of syntax. *Metavariables* are used to achieve such goal, they are declared with "`$ name : fragment-specifier`" in the macro matcher and can match thirteen different kinds of syntax fragments [69, Section 3.1 - Metavariables]. In Listing 3.4, the metavariable `n` is of kind `literal` which will match literals such as `'E'`, `"Elite"` and `420` [69, Section 8.2.1].

Repetitions are indicated by placing the tokens to be repeated inside `$(...)`, followed by a repetition operator, optionally with a separator token between. This is valid both for the matcher and the transcriber. Repetition operators are the same as the regular expression ones:

- `*` — indicates zero or more repetitions.

```
macro_rules! say_hello {
    ($n:literal) => { for 0..$n { println!("Hello, world!"); } }
}
fn main() { say_hello!(5); }
```

Listing 3.4: Example `macro_rules!` usage. When executed, the code above will print "`Hello, world!`" five times.

```
1 macro_rules! using_a {
2     ($e:expr) => { { let a = 42; $e } }
3 }
4 let four = using_a!(a / 10);
```

Listing 3.5: Definition of the `using_a` macro and usage. The macro simply declares a variable `a`, set to 42 and then writes an expression which was passed in.

```
1 let four = {
2     let a = 42;
3     a / 10
4 };
```

Listing 3.6: Listing 3.5 line 9's macro expansion. Declarations with a blue background will be placed in a different *scope* than the others, thus the `a` for lines 2 and 3 will not be considered the same.

- `+` — indicates at least one repetition.
- `?` — indicates zero or one repetition.

Hygiene works by attaching an invisible *syntactic context* to all identifiers [79]. Identifiers are compared over two pieces of information, the *textual value* and their *syntactic context*. The textual value consists of the variables name (e.g. `four`), the syntactic context is a kind of scope added to variables declared inside the macro. This is done to keep the macro declared variables from interfering with existing ones.

When expanding a declarative macro[1] variables declared inside the macro belong in a different scope, consider the macro declared in Listing 3.5 and the respective expansion in Listing 3.6. As illustrated by Listing 3.6, line 2 is considered to be in a different context than the rest of the expanded code. This will rightfully raise an error (shown in Listing 3.7), since line's 3 `a` will not exist due to not being in the same syntactic context as line 2.

3.2.2 Procedural Macros

Rust also has another macro mechanism, *procedural macros*, these can take three forms: *function-like macros*, *derive macros* and *attribute macros*. In a nutshell, procedural macros

[1] The same mechanism does not apply to procedural macros, which are not hygienic. Their output will interfere with existing code if precautions are not taken [39].

```
error[E0425]: cannot find value `a` in this scope
  --> src/main.rs:13:21
    |
  9 | let four = using_a!(a / 10);
    |                     ^ not found in this scope
```

Listing 3.7: The expansion in Listing 3.6 will result in an error during compile time since the as in line 2 and 3 are considered to belong to different contexts.

```
html! {
    h1 { "Hello, world!" }
    p.intro {
        "This is an example of the "
        a href="https://github.com/lambda-fairy/maud" { "Maud" }
        " template language."
    }
}
```

Listing 3.8: HTML DSL embedded in Rust. Example taken from [80].

allow users to run code at compile time, consuming and producing Rust syntax.

Function-like Macros

Function-like macros and declarative macros are similar regarding invocation, being indistinguishable from each other, and output, completely replacing the original call. However, the similarities stop there as their implementation methods are completely different.

Definition. Function-like macros are defined by a public function with the `proc_macro` attribute and a signature of type `(TokenStream) -> TokenStream`. Everything contained inside the call delimeters of the macro invocation is input to the function, as previously referred, the output will completely replace the macro call.

Domain Specific Languages. While the macros discussed next also provide their contribution for domain specific languages in Rust, function-like macros provide the necessary tools to write an embedded DSL. The Rust ecosystem developers have developed HTML DSLs [80, 62] (see the example in Listing 3.8) and the possibility to run Python inside Rust[32].

Derive Macros

Derive macros likely are the most common kind of procedural macro in Rust, they are usually used to *derive* a `trait` implementation from a `struct` (see Listing 3.9). They define new inputs for the `derive` attribute, and can also create new items given the token stream of a `struct`, `enum` or `union`.

```rust
#[derive(Debug)]
struct Coordinate {
    x: f32,
    y: f32,
    x: f32,
}
```

Listing 3.9: Example usage of #[derive(...)], in this case deriving Debug enables the structure to be printed with "println!("{:?}", coord)".

```rust
#[derive(Error)]
enum CoordinateError {
    #[error("Invalid coordinates {0}")]
    InvalidCoordinates(Coordinates),
}
```

Listing 3.10: Example usage of a derive macro with helper attributes, in this case the error(...) defines an error message with a Coordinates parameter.

Definition. Just like function-like macros, derive macros are defined as a public function with the proc_macro_derive attribute and a signature of (TokenStream) -> TokenStream. The input is a token stream of the item with the derive attribute, the output is a set of items that are appended to the module or block where the input token stream is in. In Listing 3.9 the Debug implementation will be appended to the end of the structure.

Helper Attributes. Derive macros are also able to add additional attributes to the scope of the current item. Such attributes are called *derive macro helper attributes* and they are *inert*, that is, they are not processed by themselves but rather serve as annotations (see Listing 3.10).

Attribute Macros

Attribute macros define new outer attributes, in contrast to the attributes discussed in Listing 3.2.2, attribute macros are processed as independent units and not as an annotation. They can be attached to items (see [69, Section 6]), including items in extern blocks, inherent and trait implementations, and trait definitions.

Definition. Like the other macros, attribute macros are also declared by a public function with the proc_macro_attribute, however, their function signature takes two parameters instead of one, being (TokenStream, TokenStream) -> TokenStream.

The first parameter is the token tree following the attribute name, for example, in Listing 3.11 it would contain the token tree of ("/hello/<name>/<age>"), in the case the attribute is written as a bare attribute name (e.g. #[attribute]), the token tree is empty.

The second parameter is the token tree of the item the macro is attached to, the function output will *replace* such item with the return item or items.

```
#[get("/hello/<name>/<age>")]
fn hello(name: String, age: u8) -> String {
    format!("Hello, {} year old named {}!", age, name)
}
```

Listing 3.11: Attribute macros are commonly used in web frameworks to provide an easy way to declare an endpoint. In this example (taken from [57]) the user declares that `GET` requests to `hello/` have two path parameters (`name` and `age`) and should be handled by the `hello` function.

Macro Type	Input Processing	Output Processing	Invocation
Declarative	Pattern Matching	Replace	`macro!`
Function-like	User programmed	Replace	`macro!`
Derive	User programmed	Append	`#[derive(...)]`
Attribute	User programmed	Replace	`#[attribute]`

Table 3.1: Rust macros properties summary.

While attribute macros are able to replace the input stream, they can also leave the stream unchanged and check for code properties (e.g. if all variables start with a given prefix).

3.2.3 Summary

In summary, Rust enables metaprogramming through macros, the same can be divided into two categories, declarative macros, with work through pattern matching, and procedural macros. Their main characteristics are summarized in Table 3.1.

Declarative macros (Section 3.2.1) work mainly through pattern matching, they are the best tool to avoid code repetition without putting in the effort of writing a token parsing macro. However, for more complex tasks, declarative macro's readability quickly degrades leading to an unpleasant developing experience.

Procedural macros (Section 3.2.2) can be further subdivided into three categories, being *function-like*, *derive* and *attribute* macros. Function-like macros can be considered as an alternative to declarative ones, they allow for more functionality and flexibility being possible for the code behind them to be replaced from one to the other without changes on the user's part. In comparison with other procedural macros, function-like macros allow for the creation of an embedded DSL inside Rust while the others are mainly annotations. Derive macros are mainly used to extend existing structures with traits that can be derived automatically (e.g. `Debug`). Finally, attribute macros can be used to modify existing code or simply check for code properties (e.g. if an `enum` fields are sorted).

3.3 Approaches to Behavioral Types

As previously discussed, there are several kinds of approaches to behavioral types, some aim to bridge modern languages and behavioral types, others build a language from scratch. Building a new language is a more attractive approach since there is no requirement for retrofitting. This approach is more common in the typestate domain, with Vault and Plaid being prime examples. The library approach receives more attention from the session types domain, where projects aim to implement them in existing languages such as Java, Go and Rust.

3.3.1 Session Types

As established so far, session types are mostly used for communication protocols, defining message types and their order in a conversation. Session types also share common ground with typestates as works StMungo [11, 38, 77] and others [22, 74] demonstrate.

StMungo it is a transpiler from Scribble [83] to Java based on session types and typestate. The transpilation process takes Scribble local protocols as input, generating Mungo typestate specifications and Java skeleton implementation code. The output is then checked by Mungo [11, 38, 77]. This process is based on a formal translation of session types into typestate specifications for channel objects, and extends the translation from binary to multiparty session types.

Session Types for Rust. As far as I am aware, the work on Rust session types was started by Jespersen et al. [34], such work was limited since it only supported binary session types for channels. It builds on a Haskell-based approach [52], mirroring the implementation interface.

The type constructs in the original session types formulation have correspondents in the Rust implementation, this is part of a DSL embedded in the Rust type system. The library makes use of `unsafe` to allow for transmutation (i.e. unsafe type casting) and sending untyped values over the channels. Finally, the library is able to provide compile-time safety, that is, the code will not compile if the channels protocols do not match.

Multiparty Session Types for Rust. Work on multiparty session types started with Lagaillardie et al. [41]. This work makes use of the Scribble [83] toolchain, just like StMungo; and it is a thin wrapper over previous work done by Kokke [36]. Similarly to the previously presented work [34], this work also takes advantage Rust's type system to provide compile-time safety. While using Scribble allows the library to make use of a tried and tested toolchain, it also implies the usage of an external tool, which in previous works was not necessary [34, 36].

3.3.2 Typestate

In the work of Ancona et al. [2, Section 2.3] several approaches to typestates are enumerated. While most approaches create a new language, approaches like Fugue [12] simply build on top of existing languages. This kind of approach is extremely valuable as it bridges the gap between existing programming languages and the theoretical field.

```
[WithProtocol(”open”, ”closed”)]
class OuterSocket {
    [InState(”connected”, WhenEnclosingState=”open”),
        NotAliased(WhenEnclosingState=”open”)]
    [Unavailable(WhenEnclosingState=”closed”)]
    private Socket innerSocket;
}
```

Listing 3.12: Relating a class's states with the `innerSocket` states. In this example, the `OuterSocket`'s open state is related with the connected state of the socket. This ensures that the `OuterSocket` is a well-behaved client of `innerSocket`.

Vault is a programming language with the aim of researching lifetime tracking and the symbolic state of objects [17]. Vault introduces two new concepts — *adoption* and *focus*, which serve to relax constrains imposed by a linear type system. Since aliasing can be controlled through the linear type system, Vault is able to check for states, hence supporting typestate. Vault bridges the best of both worlds by splitting programs into two groups: the ones able to be checked for protocols (i.e. *typestated*) and the ones free of aliasing restrictions and thus unable to verify protocol rules.

The adoption mechanism works by means of an *adopter* (i.e. which adopts a linear reference) and an *adoptee* (i.e. the adopted reference). Through adoption, the adopted linear reference is consumed, and thus cannot be directly accessed. Furthermore, the lifetime of each reference alias is tied to the lifetime of the adopter. When the adopter is freed, all adopted references recover their linear type.

The focusing mechanism provides a temporarily linear view on a nonlinear object. The focused object is required to be live and of the same type in the end of the focus usage. Access to the parent of the focused object is temporarily revoked, disabling alias access.

Fugue is a software checker that enables interface protocols (i.e. typestates) to be specified as annotations [12]. It provides two main protocol checking functions, *resource protocols* and *state-machine protocols*. Resource protocols relate to the allocation and release of resources, since Rust takes care of such concerns through ownership I will not discuss this feature of Fugue.

State-machine protocols allow the programmer to constrain the sequence of method calls on an object. This is also known as typestate, as one can only transition between valid states. In Fugue, the developer adds annotations to the object's methods and from them, a state-machine is derived. Fugue also allows for states to relate to one another. Consider the example in Listing 3.12; by relating the states in the `OuterSocket` class with the `innerSocket` field states Fugue can ensure that `OuterSocket` is a well-behaved client of the field's class.

Plaid is a typestate-oriented language. The idea, proposed in [1], is based on support for first-class typestates in an object-oriented setting. In Plaid, objects are described by their

```
@Typestate("StateIteratorProtocol")
class StateIterator { /* ... */ }
```

Listing 3.13: Mungo's `Typestate` annotation. Normal Java code ends up ignoring the annotation. However, Mungo is able to process it and check the class calls against the specification to ensure typestate compliance. In this case the class specification is `StateIteratorProtocol`.

state rather than members. While the object is able to have fields common to all states, there is also the possibility for fields to be exclusive to a given state. For the example of the `File` which can be either in the `Open` state or the `closed`, the former state would have an OS file descriptor, while the closed state would not. The path to the file could be available for both states, since it would allow the file to be re-opened.

In Plaid, methods can make the object transition between states. Building on the file example, the method open would transition the file from the `Closed` state to the `Open` state. Plaid also introduces a series of aliasing control keywords, `unique` disallows aliasing on an object while allowing for state transitions, `immutable` disallows mutation (i.e. state transitions), `shared` makes an object behave like it normally would in Java, allowing aliasing (since it allows aliasing, it also requires runtime checks over state on sensitive operations).

Mungo is a static analysis tool [11, 38, 77] for Java programs. It checks typestate properties and can be divided into two components, a Java-like language to define typestate specifications and a typechecker, which checks that objects follow the typestate specification. Specifications are written as separate files and can then be used in Java classes through annotations, as demonstrated in Listing 3.13. The annotations enable Mungo to be unobtrusive in projects since annotations are not required to be processed (as seen in Section 3.1.2).

> *If a class has a typestate specification, the Mungo typechecker analyses each object of that class in the program and extracts the method call behaviour (sequences of method calls) through the object's life. Finally, it checks the extracted information against the sequences of method calls allowed by the typestate specification. — [11, Section 1.2]*

3.3.3 Summary

In summary, behavioral types is a topic which for now, is still mostly confined to the academia circles. Despite the efforts put into the development of tools for "*business*" languages, the tools were either abandoned (e.g. Fugue) or superseded by other developments in the field (e.g. the initial work in session types for Rust). Languages developed for research purposes (e.g. Vault and Plaid) seem to make little to no effect on the outside world. While adoption of the language itself is not expected, such could be expected for the mechanisms, though it does not seem to be the case. Finally, in the case of tools (e.g. Scribble and Mungo), they seem to pick the most traction from academia. The motivation seems to be based on the possibility of extension and continuous improvement. However, they seem to suffer the same destiny as others, causing little to no impact in the outside world.

4

The #[typestate] macro

I now present the core contribution of this thesis, the `#[typestate]` macro. In Section 4.1, I start by demonstrating how to implement Rust typestates by hand. In Section 4.2.1 I discuss the macro high-level architecture, the DSL is discussed in Section 4.2, followed by the validation process in Section 4.3 and extra features offered by the macro in **??**.

4.1 Typestates: The Hard Way

In this section I demonstrate the development process from a state machine specification to a functional prototype, developing all the required components by hand. The example will be a vending machine, its automaton is illustrated in Figure 4.1. To simplify the example, consider the following:

- The machine houses an infinite stock of each of the available snacks.
- Each snack is addressed by its index and the only information available about it is its price.
- The machine does not make change.

We start by designing our *typestated* structure, the `VendingMachine`; to do so, we will use a `State` generic type parameter to model the current state.

```
struct VendingMachine<State>;
```

However, since `State` is an unused type parameter the compiler issue an error; we can fix the error in one of two ways:

- Declaring a `PhantomData`[1] field using `State` as its type parameter. This approach is useful if the types used in `State` do not carry more information other than its type.

  ```
  struct VendingMachine<State> { state: PhantomData<State> }
  ```

- Declaring a field of type `State`. This approach allows us to use more information other than its type alone, such as structure fields.

  ```
  struct VendingMachine<State> { state: State }
  ```

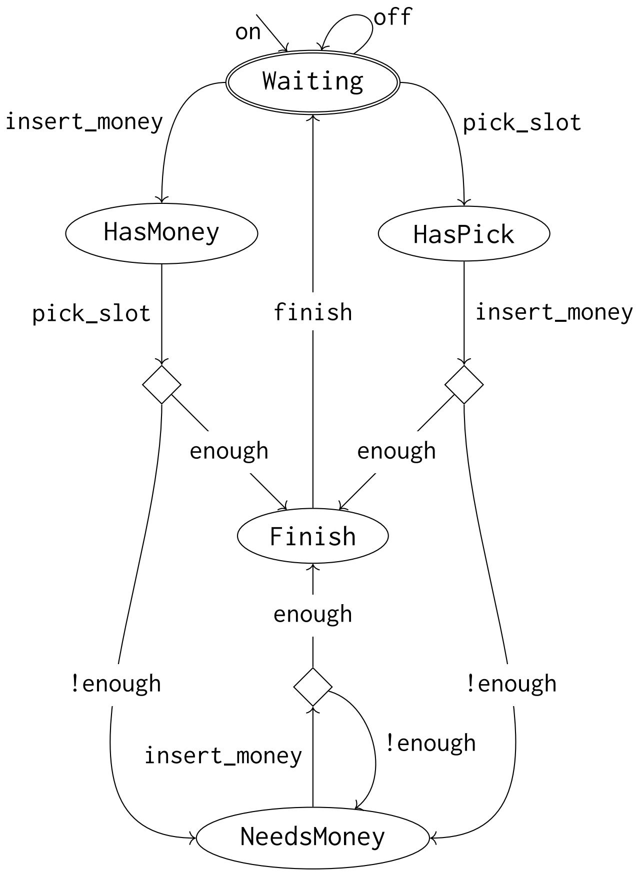

Figure 4.1: Vending machine automaton.

There are cases where all states are simply markers (i.e. do not carry additional information), however, consider that the vending machine is required to keep track of both the client's pick along with the inserted money so far. Given we are modelling our machine "by states", we should not be required to track neither of those in the initial or final states (i.e. `Waiting` and `Finish`, respectively). With that in mind, we are required to take the second approach, enabling states to have inner values.

While our vending machine is now able to deal with the concept of state, it is unable to sell anything, we need some place to store the items available for sale and all the money we made. We will use a vector for the items and an unsigned 64-bit integer for monetary values, see Listing 4.1. These values are available for any state, as they are "part of the machine" and not specific to a given state.

Currently, we have a machine supporting states, but no states. To address this we need to declare each state as a structure; each structure can then contain its own fields, only available for that state.

[1] `PhantomData` is a zero-sized type used to "pretend" that it owns a previously-unused type parameter (or lifetime). This is required since Rust's compiler will complain in the case that a type parameter is unused. To know more about `PhantomData`, please refer to its documentation page — `https://doc.rust-lang.org/std/marker/struct.PhantomData.html`; or to its page on *The Rustonomicon* — `https://doc.rust-lang.org/nomicon/phantom-data.html`.

```rust
struct VendingMachine<State> {
    /// The money made so far.
    balance: u64,
    /// The available item's prices.
    items: Vec<u64>,
    /// The current machine state.
    state: State,
}
```

Listing 4.1: The vending machine main struct.

```rust
/// The machine is waiting for interaction.
struct Waiting;
/// The machine has received some amount of money
struct HasMoney {
    /// The insert amount of money
    money: u64
}
/// The machine has received a slot pick.
struct HasPick {
    /// The selected slot.
    picked_slot: usize
}
/// The machine has received both money and a slot pick,
/// but not enough money to complete the purchase.
struct NeedMoney {
    money: u64,
    picked_slot: usize
}
/// The purchase is complete.
struct Finish;
```

Listing 4.2: The vending machine's states, as illustrated in Figure 4.1.

Looking back at Figure 4.1, we can infer the following:

- The `Waiting` and `Finish` states do not require any fields.
- The `HasMoney` and `HasPick` states require their own fields, the money inserted so far and the slot picked by the client, respectively.
- The `NeedMoney` state requires both the money and picked slot.

The states' structure declarations are listed and documented in Listing 4.2.

Moving on to transitions, we need to ensure that there are no aliases to the current state; Rust's borrow checker helps us achieve that goal, we can restrict the usage of the current state to only be possible in the case `self` is owned, the borrow checker will then make sure that is true when time comes to use the method.

To declare a transition, we first open an `impl`[2] block which will contain our transition, the block will implement a concrete state of the state machine by specifying the generic type parameter to be one of the declared states, line 1 of Listing 4.3; inside the block, we declare the transition function, it will take `self` as a first parameter, consuming the first

```
1  impl VendingMachine<Waiting> {
2      fn on() -> Self { /* ... */ }
3      fn off(self) { /* ... */ }
4      fn insert_money(self, money: u64) -> VendingMachine<HasMoney> { /* ... */ }
5      fn pick_slot(self, picked_slot: usize) -> VendingMachine<HasPick> { /* ... */ }
6  }
```

Listing 4.3: The vending machine's `Waiting` implementation[3].

```
1  impl VendingMachine<Waiting> {
2      /// The user has inserted some amount of money into the machine.
3      fn insert_money(self, money: u64) -> VendingMachine<HasMoney> {
4          VendingMachine::<HasMoney> {
5              contents: self.contents, // pass the machine's contents
6              state: HasMoney {        // new state
7                  money                // pass the received money
8              }
9          }
10     }
11     // ...
12 }
```

Listing 4.4: The implementation of `insert_money` for the machine's `Waiting` state.

state, and return the next state; exemplified in lines 4 & 5 of Listing 4.3.

To better understand what is going on, lets implement the `insert_money` transition; all we need to do is simply transition from the `Waiting` state (declared as the generic parameter in line 1 of Listing 4.4), to the `HasMoney` state, declared as the generic parameter of the `VendingMachine` return type, line 3 of Listing 4.4.

Before we go further, a quick recap over what has been done so far — we have declared the vending machine, its states and its *some* of its transitions.

I say "some" transitions, because we have not addressed how the diamonds in Figure 4.1 work. We use the diamonds to represent a decision between N possible paths, I will refer to them as *decision nodes*; this representation closely resembles *Deterministic Object Automata* [71]. To model our decision nodes, we can use Rust's enumerations, these allow us to declare possible outcomes and force the API client to match them.

We continue our path, following the `pick_slot` transition from the `HasMoney` state, we have *either* the `Finish` state or the `NeedsMoney` state, a decision node; its implementation is described in Listing 4.5.

Using the `CheckFinish` enumeration, we are now able to properly define `HasMoney`'s `pick_slot` function; if the user has inserted enough money, a purchase is made (Listing 4.6

[2]The `impl` keyword is used for implementation blocks, whether it is for inherent or trait implementations. For further details, refer to *The Rust Reference* — https://doc.rust-lang.org/reference/items/implementations.html.

[3]`Self` is a keyword which acts as a type alias to the "current" type, it is native to Rust and works in the context of traits and their implementations. In Listing 4.3 the `Self` will refer to `VendingMachine<Waiting>`. For more information on `Self`, refer to https://doc.rust-lang.org/std/keyword.SelfTy.html

```
// To simplify naming, we reuse the state's names
enum CheckFinish {
    NeedsMoney(VendingMachine<NeedsMoney>),
    Finish(VendingMachine<Finish>),
}
```

Listing 4.5: Vending machine's decision node as a Rust `enum`.

```
1  impl VendingMachine<HasMoney> {
2      fn pick_slot(self, picked_slot: usize) -> CheckFinish {
3          let money = self.state.money;
4          let price = self.contents[picked_slot]; // get the pick's price
5          // Check if there is enough money
6          if money >= price {
7              // If yes, return the `Finish` state
8              CheckFinish::Finish(VendingMachine::<Finish> {
9                  // update the machine's balance
10                 balance: self.balance + money,
11                 contents: self.contents,
12                 state: Finish,
13             })
14         } else {
15             // If not, return the `NeedMoney` state
16             CheckFinish::NeedMoney(VendingMachine::<NeedMoney> {
17                 balance: self.balance,
18                 contents: self.contents,
19                 state: NeedMoney { money, picked_slot },
20             })
21         }
22     }
23 }
```

Listing 4.6: The `pick_slot` implementation for the vending machine during the `HasMoney` state.

— lines 6-13), otherwise, the vending machine asks for more money (Listing 4.6 — lines 14-22), in either case, it returns a variant of the declared `enum`.

The API client will now be required to match the enumeration, which implies the user needs to (or at least try to) deal with all possible outcomes; exemplified in Listing 4.7.

This concludes the implementation of the state machine, the states I did not cover follow the same implementation pattern, as the automaton is "symmetric", although the functions perform different actions.

To test if our typestates work, we can try to call a function in a state where such function is unavailable (Listing 4.8); this will not compile the compiler will even be helpful enough as to tell us that `finish` was not found for the `Waiting` state (Listing 4.9).

```
1 let mut vm: CheckFinish = vm.pick_slot(0);
2 while let CheckFinish::NeedMoney(vm_) = vm {
3     vm = vm_.insert_money(1);
4 }
5 match vm {
6     CheckFinish::Finish(vm) => vm.finish().off(),
7     CheckFinish::NeedMoney(_) =>
8         unreachable!("if we left the loop this should be unreachable"),
9 }
```

Listing 4.7: Matching `CheckFinish` in two different ways; lines 2-4 — using a `while` loop, lines 5-9 — using common `match`.

```
let vm = VendingMachine::<Waiting>::on() // Start the vending machine
    .finish();                           // Finish a purchase
```

Listing 4.8: Calling the `finish` function in the `Waiting` state.

```
no method named `finish` found for struct `VendingMachine<Waiting>`
in the current scope items from traits can only be used if the trait is
implemented and in scope the following trait defines an item `finish`,
perhaps you need to implement it:
candidate #1: `Hasher`
```

Listing 4.9: The error resulting from Listing 4.8.

4.1.1 Future Proofing

Our API seems to be rock-solid, methods cannot be called in state they do not belong to and the compiler will even provide helpful messages.

However, there is a problem, nothing stops a developer from extending the API by implementing a "foreign" type (in this context, consider "foreign" to be a type which is not a state), such as the unit type — `()`. Disregarding the fact that implementing the unit type as a type parameter of our vending machine makes no sense; we need to avoid these situations and to do so *The Rust API Guidelines*[4] offer an answer!

We can implement the "sealed trait pattern", which is just a way of stopping downstream users from modifying our state hierarchy.

Following the guidelines, we need to first create a public `trait` which every state will implement (Listing 4.10 — lines 13-23); we need to further restrict the state set with a private `trait` (Listing 4.10 — lines 1-11), also implemented by every state, it is required to be private so downstream users are unable to access and implement it.

[4] https://rust-lang.github.io/api-guidelines/future-proofing.html#sealed-traits-protect-against-downstream-implementations-c-sealed

```
mod private {
    /// The `Sealed` trait, unable to implemented by downstream users.
    pub trait Sealed {}

    // The trait implementations for each state.
    impl Sealed for Waiting {}
    impl Sealed for HasMoney {}
    impl Sealed for HasPick {}
    impl Sealed for NeedMoney {}
    impl Sealed for Finish {}
}

/// The `State` trait. While any user can *technically* implement it,
/// its bound requires `private::Sealed` to also be implemented,
/// which is impossible because it is not accessible to downstream users.
pub trait State: private::Sealed {}

// The `State` trait implementations.
impl State for Waiting {}
impl State for HasMoney {}
impl State for HasPick {}
impl State for NeedMoney {}
impl State for Finish {}
```

Listing 4.10: The implementation of the sealed trait pattern for our vending machine automaton.

4.2 Typestates: The DSL

Now that we know how to build our own typestates, we want to automate part of the process. In this section I present the macro's DSL, I start by exploring its architecture followed by its syntax, going through the simpler constructs and how they relate to the typestate first, finishing on more advanced features.

4.2.1 Architecture

Before discussing how the automaton extraction works, it is necessary to discuss the macro architecture and provide some insight into its inner workings. This section starts by providing an overview over the macro architecture, afterwards I will dive into the parsing and code generation details.

The macro's architecture is illustrated in Figure 4.2, everything starts by attaching `#[typestate]` to a module, our macro will be expanded during compilation and thus our code will be run. We are given the Abstract Syntax Tree (AST) of the module, from which we run a series of visitors (described Section 4.2.1.2) which will extract the typestate's state machine, afterwards we perform some checks over the state machine (described in Section 4.3), if the checks fail, an error is issued, pointing the user to the relevant code, if all checks pass the user is ready to start implementing the typestate's functionalities.

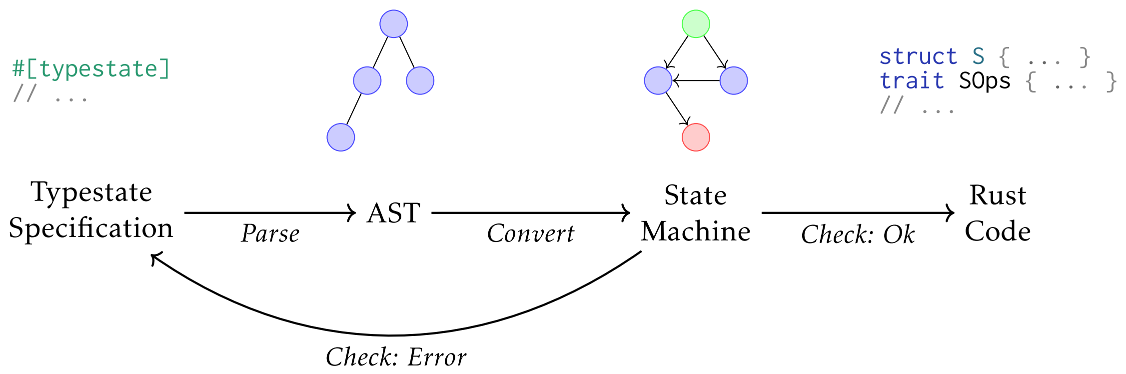

Figure 4.2: From DSL specification to Rust code. First the DSL is parsed, then converted to a state machine and the properties checked (in the case some property is not respected, an error is issued). Once the properties are validated, the Rust code is generated.

4.2.1.1 Parsing

The macro's parsing procedure leverages the syn crate[5] whenever possible, this allowed me to focus on getting the most information out of the user's code rather than worrying about how to parse Rust.

As out macro can only be attached to modules, we instruct syn to expect and parse a module item[6]; this simple step already saves us from manually ensuring the macro is attached to the right type. The resulting item is the module's AST, from which we will run a series of visitors, each analyzing a different part of the code.

4.2.1.2 Visitors

The macro is split into three separate visitors, each performs a pass over different item kinds and if necessary, mutates the tree by generating new code and either adding or replacing existing nodes. The following visitors are described in their running other.

The structure visitor will visit all structures, as the name states; currently, a user can declare one of three possible structures — a structure annotated with `#[automaton]` (of which there can only be one), one annotated with `#[state]` (of which there can be N) and one without annotations (of which there can be *none*). From the visited structures we can extract the automaton's structure and its states, these are added to the graph and the sealed trait pattern is implemented for each structure.

The enumeration visitor solely visits enumerations; it checks that all enumeration variants exist as states and establishes edges between them and the enumeration node. This visitor is also known as the non-deterministic state visitor since each enumeration represents a decision to be made during runtime.

[5] syn is a parsing library for Rust's `TokenStream`, for more information please see https://docs.rs/syn/1.0.72/syn/index.html.

[6] https://doc.rust-lang.org/reference/items/modules.html

```
#[typestate] mod vending_machine_api {}
```

Listing 4.11: The vending machine's API module, annotated with the #[typestate] macro.

```
error: Missing `#[automaton]` struct.
   |
   | #[typestate]
   | ^^^^^^^^^^^^
```

Listing 4.12: The error issued by the code in Listing 4.11.

The trait visitor, or the transitions visitor, is responsible for the extraction of all the transitions out of the declared traits. This visitor entered in conflict with the first one since the first one generated traits which would then be visited; to avoid this problem `typestate` declares an additional, undocumented and inert macro (i.e. a macro that returns its input); the `#[generated]` macro. When the visitor sees an item attached with `#[generated]` it ignores the item, which later gets processed by Rust's macro system and the annotation is naturally removed.

4.2.2 Syntax & Automaton Extraction

`#[typestate]`'s DSL syntax is interlinked with its automaton extraction process, as such, I will discuss them in conjunction. As we go, I will present parts of the syntax and explain how it relates with the automaton. We will reuse the vending machine example, illustrated in Figure 4.1 and model it using our DSL.

The `#[typestate]` macro is the DSL's entrypoint and it only supports being attached to modules. Given that we want to access several parts of Rust's syntax (e.g. `struct`, `enum`, etc) we can take one of two approaches — either analyze the whole file, or annotate and process the best next thing, the module.

The module provides most of the syntax elements available to "top-level" Rust, while being possible to analyze using the macro system; inside a module we can declare structures, enumerations, free functions and so on.

To start modeling the vending machine we first declare a module, to which we will call `vending_machine_api`, and annotate it with `#[typestate]`; as shown in Listing 4.11. This alone is not enough, as the macro will throw an error due to the lack of an automaton; shown in Listing 4.12.

The `#[automaton]` annotation is attachable to structures only, and allows the macro to know which of the declared structures is the automaton.

Listing 4.13 fixes the error of Listing 4.11, by adding the `VendingMachine` structure and annotating it with `#[automaton]` the macro is now able to know which structure is the main state machine (i.e. which structure will be "typestated").

```
#[typestate] mod vending_machine_api {
    #[automaton] pub struct VendingMachine;
}
```

Listing 4.13: Listing 4.11; with an automaton declaration.

```
mod vending_machine_api {
    mod private {
        pub trait Sealed {}
    }
    pub trait State: private::Sealed {}
    pub struct VendingMachine<S> where S: State {
        state: S
    }
}
```

Listing 4.14: Code resulting from Listing 4.13 expansion.

```
#[typestate] mod vending_machine_api {
    #[automaton] pub struct VendingMachine;
    #[state] pub struct Waiting;
    #[state] pub struct HasMoney { money: u64 }
    #[state] pub struct HasPick { picked_slot: usize }
    #[state] pub struct Finish;
    #[state] pub struct NeedMoney {
        pub money: u64,
        pub picked_slot: usize,
    }
}
```

Listing 4.15: Listing 4.13; with all states declared.

Notice how the code from Listing 4.14 does not contain any reference to the current state, this is added by macro through the `#[automaton]` annotation, along with the sealed pattern skeleton, described in Section 4.1.1.

Once again, this still does not make the macro happy, while we now have an automaton, we are lacking initial and final states; as shown in Listing 4.17.

The `#[state]` annotation, like the `#[automaton]` annotation, is only attachable to structures; it marks structures as states and also implements the necessary traits to include the state in the sealed trait state set (Section 4.1.1).

As we can observe in Listing 4.15, declaring states is as simple as attaching the annotation to an existing structure. In Listing 4.16 we can see the expansion of the `NeedMoney` state; implementing the sealed trait pattern.

While we have declared our states, we still have the same error (Listing 4.17); that is because, currently, we only have loose states, we have not connected them in any meaningful way.

```
mod vending_machine_api {
    // ...
    pub struct NeedMoney {
        pub money: u64,
        pub picked_slot: usize,
    }
    // using the qualified path (i.e. `private::Sealed`) we sidestep the
    // requirement of being *inside* the `private` module
    // to implement the `Sealed' trait
    impl private::Sealed for NeedMoney {}
    impl State for NeedMoney {}
}
```

Listing 4.16: Expansion of the NeedMoney state, declared in Listing 4.15.

```
error: Missing initial state. To declare an initial state you can use a
function with signature like `fn f() -> T` where `T` is a declared state.
--> vm-typestate/src/main.rs:15:1
    |
    | #[typestate]
    | ^^^^^^^^^^^^
    |

error: Missing final state. To declare a final state you can use a
function with signature like `fn f(self) -> T` where `T` is not a declared state.
--> vm-typestate/src/main.rs:15:1
    |
    | #[typestate]
    | ^^^^^^^^^^^^
    |
```

Listing 4.17: The error issued by the code in Listing 4.11.

Function declarations allow us to declare transitions without any kind of annotations; we can simply look at the function signature and infer the kind of transition, however to do so, we first need to establish rules, those are:

- If a function takes `self` and returns a valid state, the function is considered to be a transition between the current state and the returned state.

  ```
  fn (self, ...) -> State;
  ```

- If a function *does not* take `self` as an argument and returns the current state, it describes the current state as an initial state.

  ```
  fn (...) -> State;
  ```

- If a function takes `self` as an argument and *does not* return a valid state, it describes the consumed state as a final state.

  ```
  fn (self, ...) -> ...;
  ```

```rust
#[typestate] mod vending_machine_api {
    #[state] pub struct Waiting;
    // The trait is named after the `Waiting` state,
    // thus, the macro knows which state is the *current* one.
    pub trait Waiting {
        // Does not consume self, returns the current state: initial state
        fn on() -> Waiting;
        // Consumes self, does not return: final state
        fn off(self);
        // Consume self and return a valid state: transitions
        fn insert_money(self, money: u64) -> HasMoney;
        fn pick_slot(self, picked_slot: usize) -> HasPick;
    }
}
```

Listing 4.18: Declaration of the `Waiting` state functions.

To declare functions, we first need to declare a `trait` with the same name as the target state, by doing this, the macro is able to know which state we are currently referring to; inside the trait, we can declare all functions to be implemented by the current state.

If the reader is familiarized with Rust, they might have realized that traits cannot share names with structures, enumerations or others; in our DSL that works because during expansion the trait is renamed as: `TraitName + State => TraitNameState`.

In Listing 4.18, we use the `Waiting` state as it contains all the previously described types of transitions.

Implementing the states and transitions is similar to what we did in Section 4.1, while we have taken care of the sealed pattern, how the machine behaves is left to us.

When using the DSL, instead of declaring an implementation for the target state, as follows:

```rust
impl VendingMachine<Waiting> { /* ... */ }
```

You implement a trait for the target state:

```rust
impl WaitingState for VendingMachine<Waiting> { /* ... */ }
```

This way, the compiler is able to point out which methods are missing (and in the future, tools like `rust-analyzer`[7] might add all missing signatures for the developer). The rest of the implementation is made in the same way as the one in Section 4.1.

4.2.2.1 Summary

In Section 4.2.2 I have introduced the basic features of the DSL; in Table 4.1 I provide a quick overview of the available annotations, `#[typestate]`, `#[automaton]` and `#[state]`; in Table 4.2 I review the transition inference rules for function declarations.

[7] https://rust-analyzer.github.io/

Annotation	Attaches to	Declares
`#[typestate]`	Module	API
`#[automaton]`	Structure	Automaton/Typestate
`#[state]`	Structure	State

Table 4.1: Overview of the DSL's annotations.

Function signature	Consumes a state	Returns a state	Inferred
`fn (self, ...) -> State;`	✓	✓	Transition
`fn (...) -> State;`		✓	Initial State
`fn (self, ...) -> ...;`	✓		Final State

Table 4.2: Overview of the transition inference rules.

```
1 pub trait NeedMoney {
2     fn insert_money(self, money: u64) -> CheckFinish;
3     fn get_message(&self) -> String;
4     fn update_pick(&mut self, new_pick: usize);
5 }
```

Listing 4.19: The `NeedMoney`, extended with the `get_message` and `update_pick` functions.

4.2.3 Advanced Features

In Section 4.2.2 we have learned about the basic features of the DSL, armed with them, the reader should be able to write typestates. However, some typestates will require more complex mechanisms, both to develop and use, that is the purpose of this section. Once more, we will expand on the vending machine example; illustrated in Figure 4.1.

4.2.3.1 Self-transitions

Consider that we are asked to display a message containing the amount left to pay in the `NeedMoney` state; to do so we can simply add a new function to the `NeedMoney` trait, like in line 3 of Listing 4.19. Notice how the new method takes `&self` instead of `self`, thus, it takes the state as an *immutable* reference, instead of consuming the state; disabling mutation of the current state. Mutable references are also supported, consider that the user should be able to update its selected snack; line 4 of Listing 4.19 declares a method taking a mutable reference to the current state, which in turn updates the user's snack selection.

When working with automata we need to consider that every transition has both a source and a destination, in the case of functions that take references to `self`, immutable or not, they still represent transitions, in this case, the source and destination are the same state; hence the name of *self-transitions*.

```rust
impl NeedMoneyState for VendingMachine<NeedMoney> {
    // ...
    /// Return the message to be displayed.
    fn get_message(&self) -> String {
        let state = &self.state;
        let unpaid_amount = self.contents[state.picked_slot] - state.money;
        format!("{} left to go!", &unpaid_amount)
    }
    /// Update the current user pick.
    fn update_pick(&mut self, new_pick: usize) {
        self.state.picked_slot = new_pick;
    }
}
```

Listing 4.20: The implementation of NeedMoney's new functions, as declared in lines 3 & 4 of Listing 4.19.

```rust
#[typestate(enumerate)] mod vending_machine { /* ... */ }
```

Listing 4.21: Using the enumerate macro attribute.

4.2.3.2 State enumeration

There are some cases in which an enumeration might come in handy, one of them is when you are required to loop forever, and you may "stop during processing" (i.e. not complete a full Waiting to Waiting cycle); in this case you will need a variable that can contain one of the many possible states the machine might be in, given that you cannot replace a variable's type once it is assigned, you will need to use Rust's enumerations.

For large state machines, writing an enumeration by hand not only it is not practical, it is also error-prone; to address these issues #[typestate] offers the enumerate macro attribute.

By changing the attached #[typestate] annotation to #[typestate(enumerate)], as demonstrated in Listing 4.21, it will generate the enumeration described in Listing 4.22. Along with the enumeration, the macro will also implement the Into conversion trait between the enumeration and the respective states; this way, if the API client wishes to convert a VendingMachine<Waiting> into EVendingMachine, they will be able to perform the conversion using .into().

4.2.3.3 State constructors

A small quality-of-life improvement is the automatic declaration of state constructors, shortening the declaration of a new state instance; these are only generated for states containing named fields and the constructor's parameters will be named after them. Its usage is similar to that of the enumerate attribute, as shown in Listing 4.23, declaring #[typestate(state_constructors)] will generate the constructors with the default name new_state, demonstrated in Listing 4.24.

```
enum EVendingMachine {
    Waiting(VendingMachine<Waiting>),
    HasMoney(VendingMachine<HasMoney>),
    HasPick(VendingMachine<HasPick>),
    NeedMoney(VendingMachine<NeedMoney>),
    Finish(VendingMachine<Finish>),
}
```

Listing 4.22: The resulting enumeration of the `enumerate` attribute, demonstrated in Listing 4.21.

```
#[typestate(state_constructors)] mod vending_machine { /* ... */ }
```

Listing 4.23: Using the `state_constructors` macro attribute.

```
impl NeedMoney {
    pub fn new_state(money: u64, picked_slot: usize) -> Self {
        Self { money, picked_slot }
    }
}
```

Listing 4.24: The generated constructor for the `NeedMoney` state; using the attribute shown in Listing 4.23.

4.3 Validation

In this section I will be discussing the validation strategies used in my work, I start by discussing the guarantees provided by the macro, followed by the typestate validation strategy, finally, I present the automaton validation strategy.

Guarantees. My library aims to provide guarantees related with automata, not typestates; this is the case because Rust's compiler is able to reason over typestates already, as long as we put it to good use we can rely on the borrow checker and type system to catch typestate related errors (i.e. calling a method in the wrong state).

Regarding automata, my macro provides the following:

Non-empty language. The language of the automaton should not be empty; the macro ensures the presence of final states.

Usefulness. All states should be useful, that is, all states should be reachable from the initial state and be able to reach the final state.

Minimality is not present in the list of provided guarantees because it is unclear how the macro could provide feedback to the user; while the macro can simply state — *"The presented automaton is not minimal"*, such message does not help the user correcting the problem.

4.3.1 The Automaton and the Graph

The automaton is modelled as a directed graph, this approach is more efficient than that of projects like OFlat which uses sets. Originally I used the `petgraph` library[8], however the library turned out to be inadequate to the problem at hand, `petgraph`'s `GraphMap`[9] required node types to be `Copy`[10] and the types I am storing are neither `Copy` nor defined by me.

To fix the problem, I have implemented a directed graph using adjacency lists, that is, for each node, there is a list containing its neighboring nodes and the respective connecting edges. This approach takes from the FADo project which also uses adjacency lists; to simplify some algorithms, I have added extra structures such as the inverse δ, or δ^{-1} (in automata, the delta set δ represents an automaton's transitions, δ^{-1} is the delta set where each transition has had their direction inverted).

The empty language verification is easy to address, since the automaton is required to have end states, I simply store all end states in a set, then I am only required to check if the set is empty or not.

Usefulness can be checked by first performing a graph search (I have opted for Depth-First Search (DFS)). Useful states are those that reach the end state(s) (i.e. productive states) and reachable from the initial state(s). The end state set comes in useful here, since we can simply iterate over all states in the set and start the graph exploration, visited nodes will be the productive ones, in the case that not all states are productive the verification stops here and issues an error, highlighting the culprits in the code. Checking for useful states is then as simple as repeating the exploration procedure starting on the initial states, the set of visited states can then be intersected with the set of productive states to compute the useful states, once more, in the case that not all existing states are useful, an error is issued, highlighting the state at fault.

4.4 Visualizing Typestates

Along with all the previously described features, I have implemented an embedded typestate visualization; the visualization supports exporting Graphviz DOT[11], PlantUML state diagrams[12] and embedded documentation using Mermaid.js[13] and the Aquamarine crate[14] (detailed in Section 4.4.2). All formats have their own feature flags (only `aquamarine` is part of the default set of features), and all formats leverage the graph used by the macro for analysis to export their visualizations.

[8] https://docs.rs/petgraph/0.5.1/petgraph/index.html
[9] https://docs.rs/petgraph/0.5.1/petgraph/graphmap/struct.GraphMap.html
[10] https://doc.rust-lang.org/std/marker/trait.Copy.html
[11] https://graphviz.org/doc/info/lang.html
[12] https://plantuml.com/state-diagram
[13] https://mermaid-js.github.io/mermaid/#/stateDiagram
[14] https://docs.rs/aquamarine/0.1.9/aquamarine

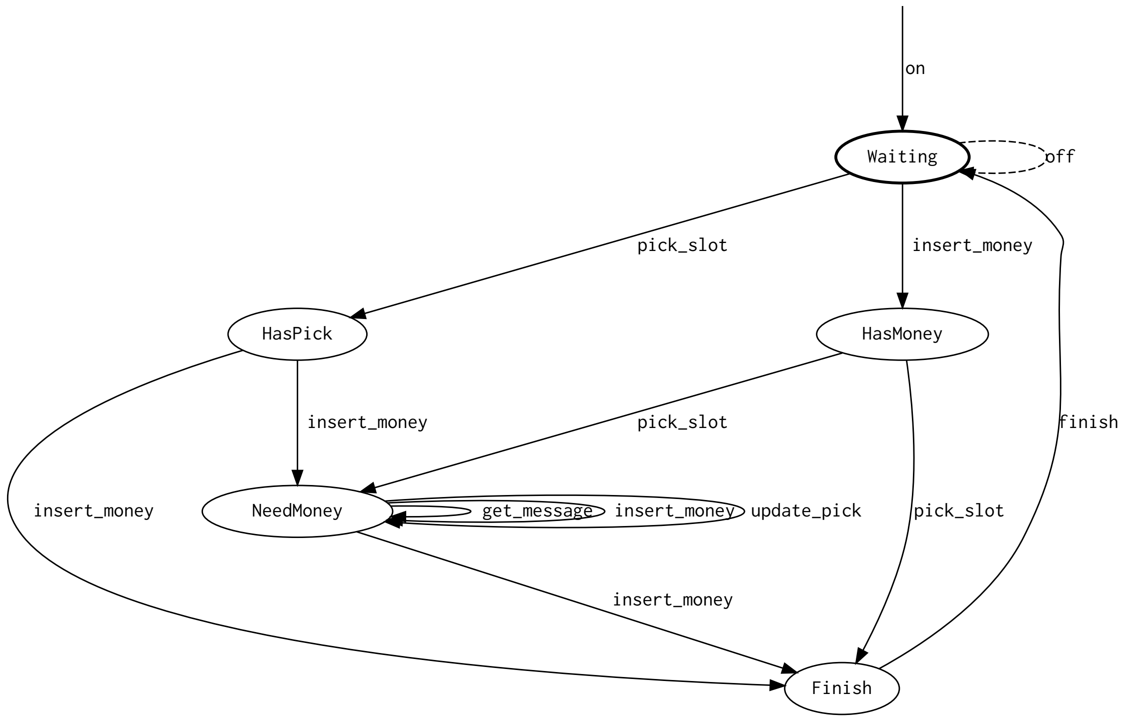

Figure 4.3: The vending machine's DOT typestate, rendered using the command — `dot -Tsvg VendingMachine.dot`.

4.4.1 Debugging with Visualizations

The visualization feature was born out of necessity, having a tool to visualize the typestate graph extracted by the macro was invaluable, reducing the time spent debugging the macro and the generated typestates. However, while it was born to debug the macro, it can also be used to visually debug the typestate; in large systems it is hard to mentally "render" the typestate and having an actual picture of the system helps immensely.

DOT was the first format to be exported as it was the first one that came to mind, it is very simple and there are a lot of tools which leverage the format. To use this feature the user can simply run cargo with any command that expands the code along with `–features typestate/export-dot`; this will export all typestates of the project into their own `$TYPESTATE_NAME.dot` file.

PlantUML offers the *state diagram* format, providing a more concise way of describing the typestate by allowing us to have dedicated initial and final states, as well as decision nodes. Just like the previous feature, exporting PlantUML is done using features; in this case the flag is `–features typestate/export-plantuml`, which will export all typestates into separate `$TYPESTATE_NAME.uml` files.

Customization of the exported formats is possible through environment variables, these are listed in Table 4.3.

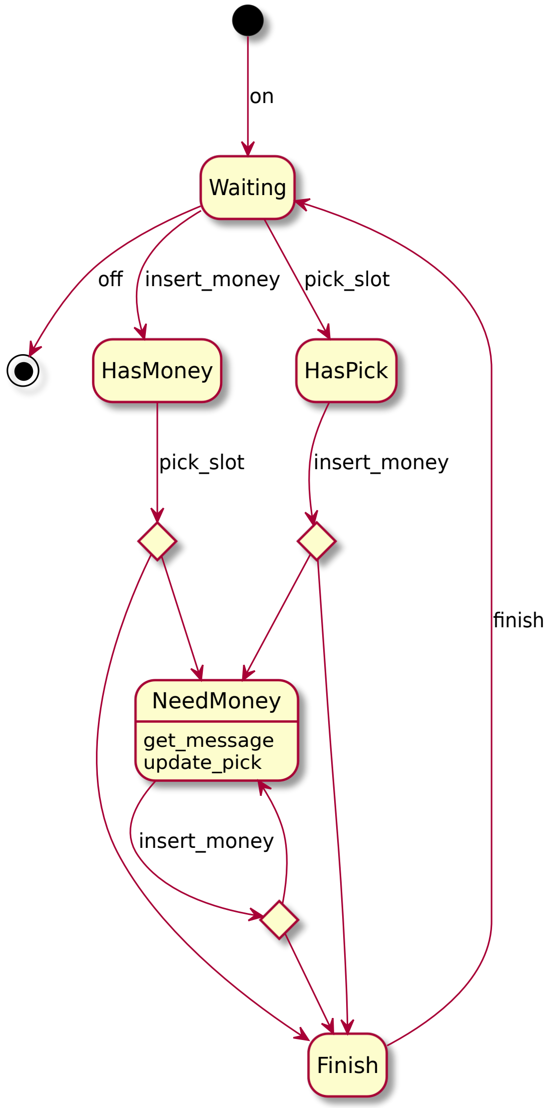

Figure 4.4: The vending machine's PlantUML typestate, rendered using the command — `plantuml -tsvg VendingMachine.uml`.

4.4.2 Embedding Visualizations in the Documentation

Exporting typestates in a way that enables the developer to visualize it is a valuable tool as it aids development, debugging and communication. However, when focusing on communication, the best way to ensure the API client gets to see the typestate would be to embed it in the documentation; as documentation is the *de facto* way to communicate between a library's author and its users.

Unfortunately, embedding images in Rust documentation requires a link to that image, which in turn, requires some other place to host the image; this constraint makes it more complicated to embed the DOT or PlantUML render inside the documentation. Ideally, we want everything in one place, generated in one step!

Tool	Environment Variable	Description
DOT	`DOT_PAD`	Specifies how much, in inches, to extend the drawing area around the minimal area needed to draw the graph.
	`DOT_NODESEP`	In `DOT`, nodesep specifies the minimum space between two adjacent nodes in the same rank, in inches.
	`DOT_RANKSEP`	In `DOT`, sets the desired rank separation, in inches.
PlantUML	`PLANTUML_NODESEP`	nodesep specifies the minimum space between two adjacent nodes in the same rank.
	`PLANTUML_RANKSEP`	Sets the desired rank separation.
Both	`EXPORT_FOLDER`	Declare the target folder for the exported files.

Table 4.3: All configuration parameters for the DOT and PlantUML visualization features.

Fortunately, Aquamarine addresses that problem; it allows the declaration of Mermaid.js diagrams as documentation and then renders them as HTML inside the Rust documentation. Its syntax is *very similar* to PlantUML's, thus this feature's implementation process was mostly copying the PlantUML generation code and fixing any bugs which appeared.

Rendering the state diagram starts by adding *doc comments*[15] to the module during the macro processing, the *doc comment* contains the diagram description in the Mermaid.js specification language; the expanded code for the vending machine example (Figure 4.1) can be seen in Listing 4.25. When the user runs the documentation command — `cargo doc`; the Aquamarine attribute is attached and the comment is processed by the `aquamarine` macro, the final diagram is then made available in the documentation; pictured in Figure 4.5.

Bundling the macro in way that users can depend on this feature is not a trivial task; we want users to simply import the `typestate` library and be able to embed their typestates in the documentation. Rust applies some restrictions to procedural macro libraries, namely, such libraries cannot export anything else other than the defined macros; this is a deal-breaker since the `typestate` crate *is* a procedural macro crate and forcing the user to explicitly import Aquamarine into their project is more overhead than necessary.

The solution for this is to create a *frontend* crate which imports both the `typestate` macro and Aquamarine, and then exports both, this sidesteps the previous issue since the crate exporting the items *is not* the macro crate; this process is pictured in Figure 4.6, Figure 4.7 and Figure 4.8.

[15] `https://doc.rust-lang.org/reference/comments.html#doc-comments`

[16] typestate-deps is the set of dependencies for the macro (e.g. syn, quote, etc); it is dashed as it is not exported.

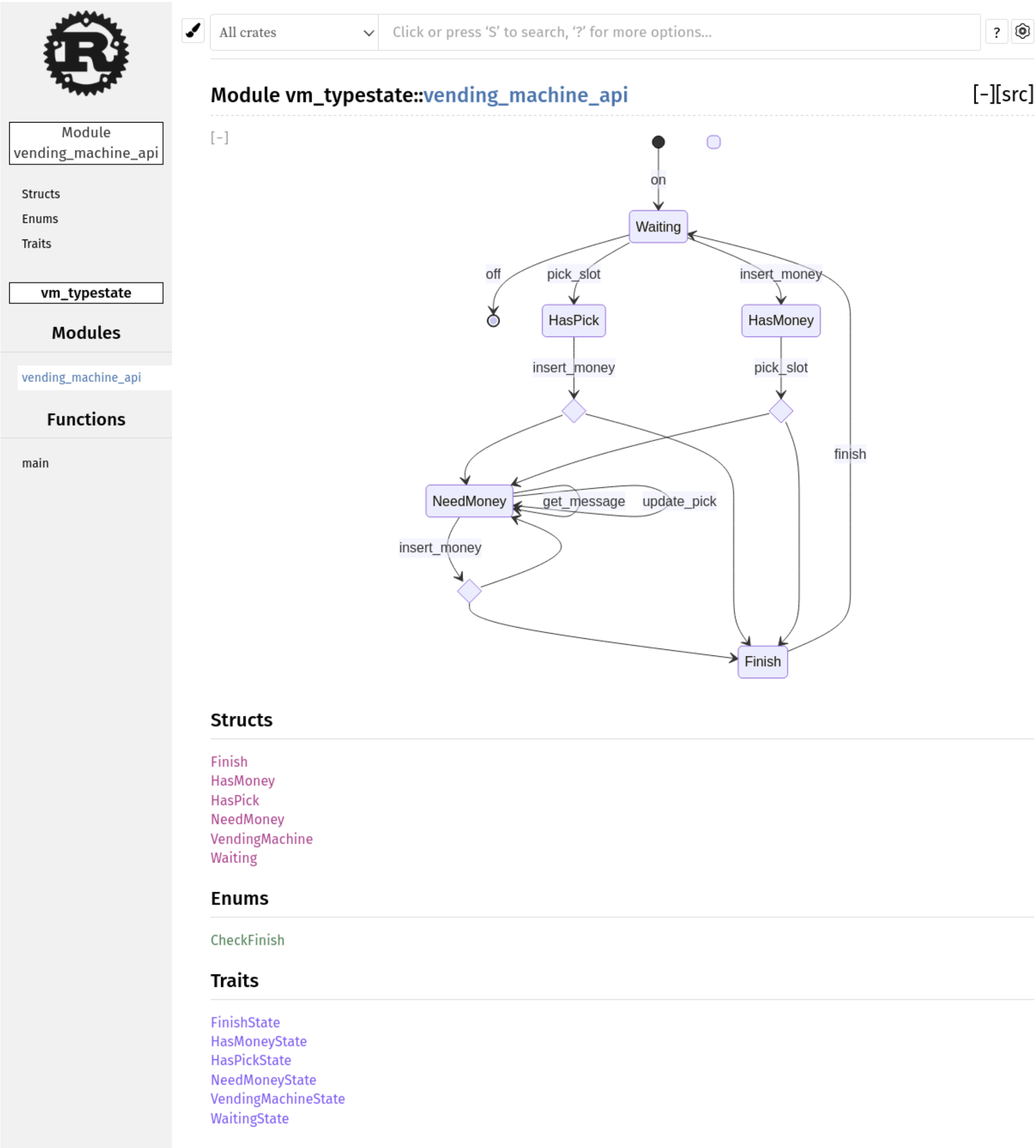

Figure 4.5: The vending machine API documentation page. Result of Listing 4.25 when rendered using `cargo doc`.

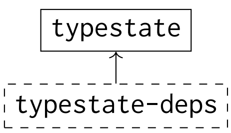

Figure 4.6: The original configuration, the macro depends only on `typestate-deps`[16] and does not export any dependency.

```
///```mermaid
///stateDiagram-v2
///  [*] --> Waiting : on
///  Waiting --> [*] : off
///  Waiting --> HasPick : pick_slot
///  Waiting --> HasMoney : insert_money
///  Finish --> Waiting : finish
///  NeedMoney --> NeedMoney : update_pick
///  NeedMoney --> NeedMoney : get_message
///  state C_NeedMoney <<choice>>
///  NeedMoney --> C_NeedMoney: insert_money
///  C_NeedMoney --> Finish
///  C_NeedMoney --> NeedMoney
///  state C_HasMoney <<choice>>
///  HasMoney --> C_HasMoney: pick_slot
///  C_HasMoney --> NeedMoney
///  C_HasMoney --> Finish
///  state C_HasPick <<choice>>
///  HasPick --> C_HasPick: insert_money
///  C_HasPick --> Finish
///  C_HasPick --> NeedMoney
///```
mod vending_machine_api { /* ... */ }
```

Listing 4.25: *Doc comments* resulting for the expansion of the vending machine example (Figure 4.1).

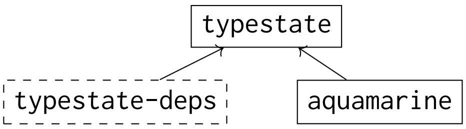

Figure 4.7: The naive attempt, the macro depends on `typestate-deps`[16] and `aquamarine`, but it only tries to export `aquamarine`, this fails because `typestate` is a procedural macro crate.

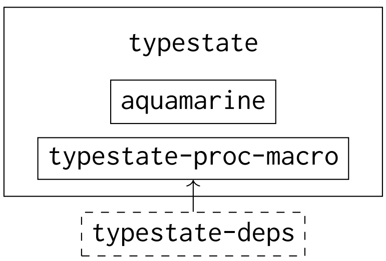

Figure 4.8: The macro was isolated in its own crate — `typestate-proc-macro`, which depends on `typestate-deps`[16]; the `typestate` crate now depends and exports both `aquamarine` and `typestate-proc-macro`.

Bibliography

[1] J. Aldrich et al. "Typestate-oriented programming". In: *Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications - OOPSLA '09*. New York, New York, USA: ACM Press, 2009, p. 1015. ISBN: 9781605587684. DOI: 10.1145/1639950.1640073. URL: http://www.cs.cmu.edu/%7B~%7Daldrich/papers/onward2009-state.pdf%20http://dl.acm.org/citation.cfm?doid=1639950.1640073 (cit. on pp. 4, 15, 18, 33).

[2] D. Ancona et al. "Behavioral types in programming languages". In: *Foundations and Trends in Programming Languages* 3.2-3 (2016), pp. 95–230. ISSN: 23251131. DOI: 10.1561/2500000031 (cit. on pp. 3, 4, 14, 17, 32).

[3] J. Bezanson et al. "Julia: A fresh approach to numerical computing". In: *SIAM Review* 59.1 (2017), pp. 65–98. ISSN: 00361445. DOI: 10.1137/141000671. arXiv: 1411.1607 (cit. on p. 7).

[4] D. M. R. Brian W. Kernighan. *The ANSI C Programming Language*. 2nd ed. Prentice Hall, 1988. ISBN: 9780131103627,0131103628 (cit. on p. 7).

[5] D. Campbell. *The many human errors that brought down the Boeing 737 Max*. 2019. URL: https://www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas-faa (cit. on p. 1).

[6] Checker Framework. "The Checker Framework Manual : Custom pluggable types for Java". In: 0.page 15 (2018), p. 253. URL: https://checkerframework.org/ (cit. on p. 23).

[7] M. Coblenz et al. "Can advanced type systems be usable? An empirical study of ownership, assets, and typestate in Obsidian". In: *Proceedings of the ACM on Programming Languages* 4.OOPSLA (2020), pp. 1–28. ISSN: 2475-1421. DOI: 10.1145/3428200 (cit. on pp. 4, 18).

[8] M. Coblenz et al. "Obsidian: Typestate and assets for safer blockchain programming". In: *ACM Transactions on Programming Languages and Systems* 42.3 (2020). ISSN: 15584593. DOI: 10.1145/3417516. arXiv: 1909.03523 (cit. on p. 4).

[9] *Dagger 2*. URL: https://dagger.dev/ (cit. on p. 23).

[10] J. Darcy. *JSR 269: Pluggable Annotation Processing API*. URL: https://jcp.org/en/jsr/detail?id=269 (cit. on p. 23).

[11] O. Dardha et al. "Mungo and StMungo: Tools for typechecking protocols in Java". In: *Behavioural Types: from Theory to Tools English* (2017), pp. 309–328 (cit. on pp. 32, 34).

[12] R. DeLine and M. Fähndrich. "The Fugue protocol checker: Is your software Baroque?" In: *Submitted manuscript* January (2004). URL: http://research.microsoft.com/apps/pubs/default.aspx?id=67458%7B%5C%%7D5Cnhttp://research.microsoft.com/en-us/projects/fugue/ (cit. on pp. 4, 32, 33).

[13] *Docker GitHub organization*. URL: https://github.com/docker (visited on 01/20/2021) (cit. on p. 9).

[14] J. Duarte. *Rusty Typestates*. 2020. URL: https://rustype.github.io/notes/notes/rust-typestate-series/rust-typestate-index.html (cit. on pp. 17, 19).

[15] *Effective Go*. URL: https://golang.org/doc/effective%7B%5C_%7Dgo.html (visited on 01/22/2021) (cit. on p. 12).

[16] T. Ekman and G. Hedin. "The JastAdd Extensible Java Compiler". In: 42.10 (2007), pp. 1–18. DOI: 10.1145/1297105.1297029 (cit. on p. 23).

[17] M. Fähndrich and R. DeLine. "Adoption and focus: Practical linear types for imperative programming". In: *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)* (2002), pp. 13–24. ISSN: 1558-1160. DOI: 10.1145/543552.512532 (cit. on p. 33).

[18] M. B. Feldman. *Who's Using Ada*. 2014. URL: https://www2.seas.gwu.edu/%7B~%7Dmfeldman/ada-project-summary.html (visited on 01/20/2021) (cit. on p. 8).

[19] N. Fitzgerald. *state_machine_future - Easily create type-safe 'Future's from state machines — without the boilerplate*. 2019. URL: https://github.com/fitzgen/state%7B%5C_%7Dmachine%7B%5C_%7Dfuture (cit. on p. 4).

[20] T. L. Foundation. *Hyperledger Fabric*. (Visited on 01/15/2021) (cit. on p. 18).

[21] S. Gay and A. Ravara. *Behavioural types: From theory to tools english*. 2017, pp. 1–375. ISBN: 9788793519817. DOI: 10.13052/rp-9788793519817 (cit. on p. 3).

[22] S. J. Gay et al. "Modular session types for objects". In: *Logical Methods in Computer Science* 11.4 (2015), pp. 1–76. ISSN: 18605974. DOI: 10.2168/LMCS-11(4:12)2015 (cit. on pp. 14, 32).

[23] M. Heaney. *Why Ada isn't Popular*. 1998. URL: http://www.adapower.com/index.php?Command=Class%7B%5C&%7DClassID=Advocacy%7B%5C&%7DCID=39 (visited on 01/25/2020) (cit. on p. 9).

[24] *Heartbleed Bug*. 2021. URL: https://heartbleed.com/ (visited on 01/14/2021) (cit. on p. 1).

[25] G. Hoare. *rust-lang/rust - first commit*. 2010. URL: https://github.com/rust-lang/rust/commit/c01efc669f09508b55eced32d3c88702578a7c3e (cit. on p. 9).

[26] T. Hoare. *Null References: The Billion Dollar Mistake*. 2009. URL: https://www.infoq.com/presentations/Null-References-The-Billion-Dollar-Mistake-Tony-Hoare/ (visited on 01/25/2020) (cit. on pp. 2, 9).

[27] K. Honda. "Types for Dyadic Interaction 2 Typed Terms". In: *October* April 1992 (1993), pp. 1–17 (cit. on p. 14).

[28] K. Honda, V. T. Vasconcelos, and M. Kubo. "Language primitives and type discipline for structured communication-based programming". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 1381 (1998), pp. 122–138. ISSN: 16113349. DOI: 10.1007/bfb0053567 (cit. on p. 14).

[29] J. Howarth. *Why Discord is switching from Go to Rust*. 2020. URL: https://blog.discord.com/why-discord-is-switching-from-go-to-rust-a190bbca2b1f (visited on 01/20/2021) (cit. on p. 9).

[30] R. Hu, N. Yoshida, and K. Honda. "Session-based distributed programming in Java". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 5142 LNCS (2008), pp. 516–541. ISSN: 03029743. DOI: 10.1007/978-3-540-70592-5_22 (cit. on p. 3).

[31] H. Hüttel et al. "Foundations of session types and behavioural contracts". In: *ACM Computing Surveys* 49.1 (2016), pp. 1–36. ISSN: 15577341. DOI: 10.1145/2873052 (cit. on p. 14).

[32] *inline-python - Inline Python code directly in your Rust code*. URL: https://github.com/fusion-engineering/inline-python (visited on 01/19/2021) (cit. on p. 29).

[33] *JastAdd*. URL: https://jastadd.cs.lth.se/web/ (cit. on p. 25).

[34] T. B. L. Jespersen, P. Munksgaard, and K. F. Larsen. "Session types for rust". In: *WGP 2015 - Proceedings of the 11th ACM SIGPLAN Workshop on Generic Programming, co-located with ICFP 2015* (2015), pp. 13–22. DOI: 10.1145/2808098.2808100 (cit. on pp. 4, 32).

[35] S. Klabnik. "The History of Rust". In: *Applicative 2016 on - Applicative 2016*. New York, New York, USA: ACM Press, 2016, p. 80. ISBN: 9781450344647. DOI: 10.1145/2959689.2960081. URL: http://dl.acm.org/citation.cfm?doid=2959689.2960081 (cit. on p. 10).

[36] W. Kokke. "Rusty Variation Deadlock-free Sessions with Failure in Rust". In: *Electronic Proceedings in Theoretical Computer Science, EPTCS* 304.Ice 2019 (2019), pp. 48–60. ISSN: 20752180. DOI: 10.4204/EPTCS.304.4 (cit. on p. 32).

[37] *Kotlin/kotlinx.serialization*. URL: https://github.com/Kotlin/kotlinx.serialization (cit. on p. 26).

[38] D. Kouzapas et al. "Typechecking protocols with Mungo and StMungo: A session type toolchain for Java". In: *Science of Computer Programming* 155 (2018), pp. 52–75. ISSN: 01676423. DOI: 10.1016/j.scico.2017.10.006. URL: https://doi.org/10.1016/j.scico.2017.10.006 (cit. on pp. 4, 32, 34).

[39] Koxiaet. *How to Write Hygienic Rust Macros*. 2020. URL: https://gist.github.com/Koxiaet/8c05ebd4e0e9347eb05f265dfb7252e1 (visited on 01/18/2021) (cit. on p. 28).

[40] *Kubernetes GitHub organization*. URL: https://github.com/kubernetes (visited on 01/20/2020) (cit. on p. 9).

[41] N. Lagaillardie, R. Neykova, and N. Yoshida. *Implementing multiparty session types in rust*. Vol. 12134 LNCS. Springer International Publishing, 2020, pp. 127–136. ISBN: 9783030500283. DOI: 10.1007/978-3-030-50029-0_8. URL: http://dx.doi.org/10.1007/978-3-030-50029-0%7B%5C_%7D8 (cit. on pp. 4, 32).

[42] X. Leroy et al. *The OCaml system release 4.11 - Documentation and user's manual*. 2020. URL: https://caml.inria.fr/pub/docs/manual-ocaml/ (visited on 02/02/2021) (cit. on pp. 21, 22).

[43] S. Mageit. *NHS COVID-19 contact tracing app fails to ask users to self-isolate*. 2020. URL: https://www.healthcareitnews.com/news/emea/nhs-covid-19-contact-tracing-app-fails-ask-users-self-isolate (cit. on p. 1).

[44] *Memory safety - The Chromium Projects*. URL: https://www.chromium.org/Home/chromium-security/memory-safety (cit. on p. 1).

[45] (. Miller, Matt. *Trends, challenges and strategic shifts in the software vulnerability mitigation landscape*. 2019. URL: https://git.io/JLdDc (cit. on p. 1).

[46] K. Most. *Writing Your First Kotlin Compiler Plugin*. 2018. URL: https://resources.jetbrains.com/storage/products/kotlinconf2018/slides/5%7B%5C_%7DWriting%20Your%20First%20Kotlin%20Compiler%20Plugin.pdf (visited on 02/04/2021) (cit. on p. 27).

[47] J. Mota. "Coping with the reality : adding crucial features to a typestate-oriented language". PhD thesis. FCT-NOVA, 2020 (cit. on p. 18).

[48] P. Munksgard. *session-types*. URL: https://github.com/Munksgaard/session-types (visited on 01/20/2021) (cit. on p. 4).

[49] S. O'Kane. *Boeing finds another software problem on the 737 Max*. 2020. URL: https://www.theverge.com/2020/2/6/21126364/boeing-737-max-software-glitch-flaw-problem (cit. on p. 1).

[50] S. O'Kane. *Southwest and United Airlines extend 737 Max cancellations after new flaw found*. 2019. URL: https://www.theverge.com/2019/6/27/18761434/737-max-new-flaw-cancellation-extended-southwest-united-airlines-faa (cit. on p. 1).

[51] T. Palmer. *tjpalmer/languish*. URL: https://tjpalmer.github.io/languish/ (visited on 01/25/2021) (cit. on p. 8).

[52] R. Pucella and J. A. Tov. "Haskell session types with (almost) no class". In: *Haskell'08 - Proceedings of the ACM SIGPLAN 2008 Haskell Symposium* (2008), pp. 25–36. DOI: 10.1145/1411286.1411290 (cit. on p. 32).

[53] *PureScript*. 2021. URL: https://www.purescript.org/ (visited on 01/14/2021) (cit. on p. 16).

[54] D. de Rauglaudre. *Camlp4 - Reference Manual*. 2003. URL: https://caml.inria.fr/pub/docs/manual-camlp4/manual007.html (cit. on p. 21).

[55] *Reason · Reason lets you write simple, fast and quality type safe code while leveraging both the JavaScript & OCaml ecosystems*. URL: https://reasonml.github.io/ (cit. on p. 16).

[56] N. Rebours. *An introduction to OCaml PPX ecosystem*. 2019. URL: https://tarides.com/blog/2019-05-09-an-introduction-to-ocaml-ppx-ecosystem (cit. on p. 22).

[57] *Rocket Web Framework*. 2021. URL: https://rocket.rs/ (visited on 01/19/2021) (cit. on p. 31).

[58] *ruby/rbs*. 2021. URL: https://github.com/ruby/rbs (visited on 01/14/2021) (cit. on p. 17).

[59] *SIGAda*. URL: https://www.sigada.org/ (visited on 01/20/2021) (cit. on p. 8).

[60] Square. *square/javapoet*. URL: https://github.com/square/javapoet (cit. on p. 24).

[61] *stm32-rs*. 2021. URL: https://github.com/stm32-rs/ (cit. on p. 20).

[62] B. Stokke. *typed-html - Type checked JSX for Rust*. URL: https://github.com/bodil/typed-html (visited on 01/19/2021) (cit. on p. 29).

[63] R. E. Strom et al. *Hermes : A Tutorial and Reference Manual*. 1990. URL: https://researcher.watson.ibm.com/researcher/files/us-bacon/Strom90HermesTutorial.pdf (cit. on p. 15).

[64] R. E. Strom. "Mechanisms for compile-time enforcement of security". In: *Proceedings of the 10th ACM SIGACT-SIGPLAN symposium on Principles of programming languages - POPL '83*. New York, New York, USA: ACM Press, 1983, pp. 276–284. ISBN: 0897910907. DOI: 10.1145/567067.567093. URL: http://portal.acm.org/citation.cfm?doid=567067.567093 (cit. on p. 15).

[65] B. Stroustrup. *The C ++ Programming*. 1986, p. 1346. ISBN: 978-0321563842 (cit. on p. 8).

[66] *The Ada Programming Language*. URL: https://web.archive.org/web/20160522063844/http://groups.engin.umd.umich.edu/CIS/course.des/cis400/ada/ada.html (visited on 01/20/2021) (cit. on p. 8).

[67] *The Embedded Rust Book*. 2021. URL: https://rust-embedded.github.io/book/ (cit. on p. 20).

[68] *The Rust Programming Language*. 2021. URL: https://doc.rust-lang.org/book/ (visited on 01/18/2021) (cit. on pp. 10, 12).

[69] *The Rust Reference*. 2021. URL: https://doc.rust-lang.org/reference (visited on 01/18/2021) (cit. on pp. 27, 30).

[70] C. Torre et al. *Panel: Systems Programming in 2014 and Beyond*. 2014. URL: https://channel9.msdn.com/Events/Lang-NEXT/Lang-NEXT-2014/Panel-Systems-Programming-Languages-in-2014-and-Beyond (cit. on pp. 8, 9).

[71] A. Trindade, J. Mota, and A. Ravara. "Typestates to automata and back: A tool". In: *Electronic Proceedings in Theoretical Computer Science, EPTCS* 324.Ice (2020), pp. 25–42. ISSN: 20752180. DOI: 10.4204/EPTCS.324.4 (cit. on p. 40).

[72] *Typed JavaScript at Any Scale*. URL: https://www.typescriptlang.org/ (cit. on p. 16).

[73] *typing — Support for type hints — Python 3.9.1 documentation*. URL: https://docs.python.org/3/library/typing.html (visited on 01/14/2021) (cit. on p. 17).

[74] C. Vasconcelos and A. Ravara. "From object-oriented code with assertions to behavioural types". In: *Proceedings of the ACM Symposium on Applied Computing* Part F1280 (2017), pp. 1492–1497. DOI: 10.1145/3019612.3019733 (cit. on p. 32).

[75] V. T. Vasconcelos, S. J. Gay, and A. Ravara. "Type checking a multithreaded functional language with session types". In: *Theoretical Computer Science* 368.1-2 (2006), pp. 64–87. ISSN: 03043975. DOI: 10.1016/j.tcs.2006.06.028 (cit. on pp. 14, 15).

[76] Vicompany. *Coinbase disclosed on HackerOne: Ethereum account balance manipulation*. 2018. URL: https://hackerone.com/reports/300748 (cit. on p. 1).

[77] A. L. Voinea, O. Dardha, and S. J. Gay. "Typechecking java protocols with [st]mungo". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 12136 LNCS (2020), pp. 208–224. ISSN: 16113349. DOI: 10.1007/978-3-030-50086-3_12 (cit. on pp. 4, 17, 32, 34).

[78] Whitequark. *A Guide to Extension Points in OCaml*. 2014. URL: https://whitequark.org/blog/2014/04/16/a-guide-to-extension-points-in-ocaml/ (visited on 01/14/2021) (cit. on p. 21).

[79] L. Wirth. *The Little Book of Rust Macros*. 2021. URL: https://veykril.github.io/tlborm (cit. on p. 28).

[80] C. Wong. *maud - Compile-time HTML templates for Rust*. URL: https://github.com/lambda-fairy/maud (visited on 01/19/2021) (cit. on p. 29).

[81] H. Xi and H. Wu. "Linearly Typed Dyadic Group Sessions for Building Multiparty Sessions". In: (2016). arXiv: 1604.03020 (cit. on p. 3).

[82] H. Xi et al. "Session Types in a Linearly Typed Multi-Threaded Lambda-Calculus". In: (2016). arXiv: 1603.03727 (cit. on p. 3).

[83] N. Yoshida et al. "The scribble protocol language". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 8358 LNCS.October 2007 (2014), pp. 22–41. ISSN: 16113349. DOI: 10.1007/978-3-319-05119-2_3 (cit. on pp. 3, 32).