Typechecking Protocols with Mungo and StMungo

Citation for published version:

Digital Object Identifier (DOI):
10.1145/2967973.2968595

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
18th International Symposium on Principles and Practice of Declarative Programming PPDP 2016

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Typechecking Protocols with Mungo and StMungo

Dimitrios Kouzapas  Ornela Dardha  Roly Perera  Simon J. Gay
School of Computing Science, University of Glasgow, UK

Abstract
We report on two tools which extend Java with support for static typechecking of communication protocols. Our Mungo tool extends Java with typestate definitions, which allow classes to be associated with state machines defining permitted sequences of method calls. A complementary tool, StMungo, takes a communication protocol specified in the Scribble protocol description language, and generates a typestate specification for each endpoint, capturing the permitted sequences of messages along that channel. Endpoint implementations can be validated by Mungo against their typestate definitions and then compiled as usual with javac. We formalise Mungo's typestate inference system and demonstrate the Scribble, Mungo and StMungo toolchain via a typechecked SMTP client that can communicate with a real-world SMTP server.

1. Introduction
In this paper we present two tools which extend the Java development process with support for static typechecking of communication protocols. Mungo extends Java with typestate definitions, which associate classes with state machines defining permitted sequences of method calls [42]. To associate a typestate definition with a class, the programmer adds a @Typestate annotation to the class telling Mungo where to find the typestate definition file. Mungo will then ensure that instances of the class are used in a manner consistent with the declared typestate.

StMungo (Scribble-to-Mungo) uses this typestate feature to connect Java to the broader setting of communication protocols specified in the Scribble protocol language [40]. Given a Scribble protocol projected to a particular endpoint (a so-called local protocol), StMungo will generate a typestate specification capturing the sequences of sends and receives permitted along that endpoint. Each endpoint implementation can be validated separately by Mungo against its typestate definition and then compiled as usual with javac.

The separate typechecking of each endpoint is integral to our approach, and is justified by the theory of multiparty session types [25], the formal foundation of Scribble. Multiparty session types provide an important safety guarantee: once each endpoint implementation is known to conform to its local protocol, the various implementations can be composed into a system free of communication errors.

Our work contributes to a line of research applying session types to real-world programming languages [9, 15–17, 22, 28, 32, 33, 35, 38]. In particular, our work builds on that of Gay et al. [23], which first connected session types to the object-oriented notion of typestate. They observed that the valid sequences of messages for a given endpoint could be captured by a typestate definition for a class, allowing the channel endpoint to be modelled as an object. While an important idea, this earlier work lacked a practical implementation and relied on typestate declaration on parameters and return types.

Mungo improves on this earlier work by employing an inference system, removing the need for typestate declarations on parameters and return types. The Mungo/StMungo toolchain offers other practical advances over previous efforts to combine session types with objects. For example, SJ [28] only supports binary session types, whereas StMungo generates Mungo specifications from multiparty session types. Furthermore, Mungo permits non-local use of objects with typestates. Using the @Typestate annotation means we avoid any need for language extensions.

Tracking object typestates requires a mechanism for managing object aliasing. For Mungo, we require objects which declare a typestate to be used linearly. While this is probably too restrictive for general-purpose programming, it is a standard technique for enabling typed communication among channels; most session type systems impose similar constraints on channel usage. Objects which lack typestate definitions can be used unrestrictedly alongside linear objects. In future work (§ 8) we will investigate more flexible alias control mechanisms, drawing on the substantial existing literature.

1.1 Contributions
The main contributions of the paper are as follows:

Mungo. We describe the Mungo typestate checker for Java. Mungo currently supports a subset of Java; support for the full language is discussed in § 8.

StMungo. We describe StMungo (§ 3), which translates Scribble local protocols into Mungo typestate specifications. StMungo also generates Java method stubs for each endpoint.

SMTP case study. A substantial example, a statically typechecked SMTP client (§ 4), illustrates the end-to-end toolchain provided by Scribble, StMungo and Mungo.

Typestate inference system. We formalise the essential features of Mungo as a core object-oriented calculus (§ 5). We define a typestate inference system for that language and prove its type-safety (§ 6).

2. Mungo
Mungo extends Java with an optional typestate system. The tool is implemented in Java using the JastAdd framework [24], a metac-
We can now define a stack implementation Stack that conforms to the StackProtocol specification, using an integer array to store the elements. The annotation @Typestate("StackProtocol") is used to associate the typestate definition with the class:

```java
@Typestate("StackProtocol")
class Stack {
  private int[] stack; private int head;
  Stack() { stack = new int[MAX]; head = 0; }
  void push(int d) { stack[head++] = d; }
  int pop() { return stack[head--]; }
  Check isEmpty() {
    if(head == 0) return Check.EMPTY;
    return Check.NONEMPTY;
  }
}
```

Finally, having implemented StackProtocol, we can define a stack client that makes use of the Stack implementation, with Mungo verifying that Stack instances are used correctly.

For illustrative purposes, the client defines two helper methods:

```java
public static void main(String[] args) {
  StackUser su = new StackUser();
  Stack s = new Stack(); Stack s2;
  s = su.pushN(s2,64); s = su.popAll(s);
}
```

### Recursion and internal choice.
Method pushN() illustrates the consumption of a recursive typestate offering a choice. The loop of the form do-while(exp) requires s to initially be either Empty or NonEmpty; at each iteration, the client decides (in the terminology of session types, it makes an internal choice) whether to push another element or exit, leaving the stack in the NonEmpty state. This is compatible with the recursive structure of the NonEmpty state, which permits an unbounded number of push() operations, looping back to NonEmpty each time.

### Recursion and external choice.
Method popAll(Stack s) also illustrates the consumption of a recursive typestate, but here the stack rather than the client makes the choice. (In session type terminology, the client offers an external choice.) This takes the form of a labelled do-while(true) in conjunction with a switch. The switch statement inspects the Check enumeration returned by isEmpty; in the NONEMPTY case, the loop continues, and in the EMPTY case the loop terminates. Due to their particular control flow, loops...
of the form `label: do { switch { block } } while(true)` are a suitable pattern for consuming a recursive typestate when the condition on the recursion is an external choice (i.e. based on an enumeration label).

**Linear objects.** Mungo ensures linear usage of objects that follow a typstate protocol; aliasing on objects allows for different method calls on an object that might lead to an inconsistent typstate. Notice that in line 15 of the `StackUser` example:

```java
s = su.pushN(s,16); s2 = su.popAll(s);
```

the return value of `popAll()` is assigned to `s2`. Now, suppose line 16 were replaced with the following:

```java
s = su.pushN(s,64); s = su.popAll(s);
```

In this case Mungo would report a linearity error on argument `s` in `su.pushN(s, 64)` informing the programmer that variable `s` is uninitialised, because the usage of variable `s` in line 15 as an argument consumed its linear value.

**Inferring typstate for fields.** Using fields to store objects can lead to a more idiomatic object-oriented style than explicitly passing values between methods. To show how this works, we define a second client, `StackUser2`, that stores a `Stack` as a field.

```
class StackUser2 {
    private Stack s;
    StackUser2() { s = new Stack(); }
    boolean pushN(int n)
    { do{ s.push(n--); }while(n>0); return true; }
    void popAll()
    { loop : do { System.out.println(s.pop());
            switch(s.isEmpty()) {
                case EMPTY: break loop;
                case NONEMPTY: continue loop;
            } while(true); }
    void finish() { s.deallocate(); }
    public static void main(String[] args)
    (StackUser2 su = new StackUser2();
    if(su.pushN(15) || su.pushN(32))
    su.pushN(32);
    su.popAll(); su.finish(); } }
```

To track the typstate of a field we need to know the possible sequences in which methods of its containing class may be called. That, in turn, requires having a typstate for the containing class. In this case, to track the typstate of the field `s`, Mungo requires us to provide a typstate for `StackUser2`. This state machine will then drive typstate checking for those fields of `StackUser2` which have their own typstate definitions. For example we could define the following `StackUserProtocol` for `StackUser2`:

```
typstate StackUserProtocol {
    Init = { boolean pushN(int): Cons,
             void finish(): end}
    Cons = { boolean pushN(int): Cons,
             void popAll(): Init }
```

Typchecking the field `s` of `StackUser2` follows the possible sequences of method calls specified by `StackUserProtocol`, and also takes into account the constructor body of `StackUser2`. Then Mungo can guarantee that if a `StackUser2` instance is used according to `StackUserProtocol` then the `Stack` field of the object is also used according to `StackProtocol`.

**Short-circuit boolean expressions.** Line 16 above illustrates a final technical detail of typstate inference. The inference algorithm takes into account the fact that logical disjunction short-circuits if the first disjunct evaluates to true. Mungo will ensure that the typstate of `su` is consistent with there either being one, two or three successive invocations of `pushN()`.

### 3. StMungo: Scribble-to-Mungo

The integration of session types and typstate, defined by Gay et al. [23], consists of a formal translation of session types for communication channels into typstate specifications for channel objects. The main idea is that a channel object has methods for sending and receiving messages and the typstate specification defines the order in which these methods can be called; therefore it is a specification of the permitted sequences of messages, i.e. a channel protocol.

We extend this translation from binary to multiparty session types [25] and implement it as the StMungo (Scribble to Mungo) tool\(^\text{3}\), which translates Scribble [40, 45] local protocols into typstate specifications and skeleton socket-based implementation code. The resulting code is typechecked using Mungo. A Scribble local protocol describes the communication between one role and all the other participants in a multiparty scenario, including the way in which messages sent to different participants are interleaved. This interleaving is not captured by binary session types and by tools based on them, like SJ [28]. StMungo is based on the principle that each role in the multiparty communication can be abstracted as a Java class following the typstate corresponding to the role’s local protocol. The typstate specification generated from StMungo together with the Mungo typechecker can guide the user in the design and implementation of distributed multiparty communication-based programs with guarantees on communication safety and soundness. StMungo is the first tool to provide a practical embedding of Scribble multiparty protocols into object-oriented languages with typstate.

We illustrate StMungo on a multiparty protocol that models the process of booking flights through a university travel agent. The full details of this example are given in App. B. There are three participants involved: Researcher (abbreviated `R`), who intends to travel; Agent (A), who is able to make travel reservations; and Finance (F), who approves expenditure from the budget. After the request, quote and check messages requesting authorisation for a trip, Finance can choose to approve or refuse the request. The **global protocol** is defined as follows.

```
global protocol BuyTicket(role R, role A, role F){
    request(Travel) from R to A;
    quote(Price) from A to R;
    check(Price) from R to F;
    choice at F { approve(Code) from F to R,A;
                 ticket(String) from A to R;
                 invoice(Code) from R to F;
                 payment(Price) from F to A; }
    or { refuse(String) from F to R,A; }
}
```

The Scribble tool is used to check the above protocol definition for well-formedness and to derive a local version of the protocol for each role, according to the multiparty session types theory [25]. This is known as **endpoint projection**. Here we show the local protocol for Researcher, which describes only the messages involving that role. The `self` keyword indicates that `R` is the local endpoint.

```
local protocol BuyTicket_R(self R, role A, role F){
    request(Travel) to A;
    quote(Price) from A to R;
    check(Price) to F;
    choice at F { approve(Code) from F to R;
                 ticket(String) from R;
                 or { refuse(String) from F; }
}
```

Notice that the exchange of invoice and payment between Agent and Finance is not included. Similarly, the local projection for Agent omits the check message and the local projection for Finance omits

\(^3\) The tool is developed and maintained by the second author and can be downloaded from our web page [1].
the request, quote and ticket messages. StMungo converts the BuyTicket_R local protocol into the RProtocol typestate protocol:

```java
1 typestate RProtocol {
2   State0={ void send_requestTravelToA(Travel): State1 }
3   State1={ Price receive_quotePriceFromA(): State2 }
4   State2={ void send_checkPriceToF(Price): State3 }
5   State3={ Choice1 receive_Choice1LabelFromF(): }
6       <APPROVE, RESUBMIT, REFUSE>: State4, State5; }
7   State4={ Code receive_approveCodeFromF(): State5 }
8   State5={ String receive_ticketStringFromA(): end }
9   State6={ String receive_requestTravelFromF(): end }
10
11   rec X1 { choice at S: _220(String) from S; }
12   or { _250(String) from S; continue X1; }
13
14   rec Z1 { ...
15       data(String) to S; ...
16   rec Z3 { choice at C { subject(String) to S;
17       continue Z3; }
18   or { dataline(String) to S;
19       continue Z3; }
20   or { atad(String) to S;
21       _250(String) from S;
22       continue Z1; }
23   } } ...
24}
```

StMungo generates an API for this role, class ARole given in App. B, which provides an implementation of RProtocol. When instantiated, it connects to the other role objects in the session (ARole and FRole). The method calls, describing the messages exchanged with the other roles, follow the interleaving specified by the RProtocol typestate. Alternatively, the developer may choose to ignore this API (and the Mungo socket library that it depends on), and use only the generated typestate protocols to develop his/her own implementation. He/she also has the ability to further refine the generated state machine, e.g., give appropriate names to states, or use anonymous states to have a coarser state refinement.

4. Case Study: Typechecking SMTP

In order to show the practicality and robustness of our StMungo and Mungo toolchain, we have developed a substantial case study in which we statically typecheck an SMTP client. We use this client to communicate with the \texttt{gmail} server. The full source code of the SMTP client can be found in [1].

SMTP (Simple Mail Transfer Protocol) is an internet standard electronic mail transfer protocol, which typically runs over a TCP (Transmission Control Protocol) connection. We consider the version defined in RFC 5321 [41]. An SMTP interaction consists of an exchange of text-based commands between the client and the server. For example, the client sends the EHLO command to identify itself and open the connection with the server. The commands \texttt{MAIL FROM: <address>} and \texttt{RCPT TO: <address>} specify the e-mail address of the sender and the receiver of the e-mail, respectively. The \texttt{DATA} command allows the client to specify the text of the e-mail. The \texttt{QUIT} command is used to terminate the session and close the connection. The responses from the server have the following format: three digits followed by an optional dash "-", such as 250-, and then some text, like OK. The server might reply to EHLO with 250 \texttt{<text>} or to \texttt{MAIL FROM} or \texttt{RCPT TO} with 250 OK.

To typecheck the SMTP protocol using StMungo and Mungo, we first represent the text-based commands as messages in a Scribble global protocol, based on Hu’s work [27].

```java
1 local protocol SMTP_C( role S, role C ) {
2   _220(String) from S; ...
3   rec X1 { choice at S: _250dash(String) from S; continue X1; }
4   or { _250(String) from S; ...
5   rec Z1 { ...
6       data(String) to S; ...
7   rec Z3 { choice at C { subject(String) to S;
8       continue Z3; }
9   or { dataline(String) to S;
10       continue Z3; }
11   or { atad(String) to S;
12       _250(String) from S;
13       continue Z1; }
14 } } ...
15}
```

StMungo translates the local protocol (SMTP.C) into a typestate specification (CProtocol). In addition, it generates a skeletal implementation based on sockets, although other implementations are possible. Every interaction in the local protocol becomes a method call in the typestate specification, as we will see shortly. State definitions group methods into choices and impose sequencing.

Running the StMungo tool on SMTP.C produces the files CProtocol.protocol, CRole.java and CMain.java:

1. CProtocol.protocol, captures the interactions local to the SMTP.C role as a typestate specification.
2. CRole.java, is a class that implements CProtocol by communication over Java sockets. This is an API that can be used to implement the SMTP client endpoint.
3. CMain.java, is a skeletal implementation of the SMTP client endpoint. This runs as a Java process and provides a main() method which uses CRole to communicate with the other parties in the session, in this case the SMTP server.

The CProtocol generated by StMungo is defined in the following.

```java
1 typestate CProtocol {
2   State0={ String receive_220StringFromS(): State1 }
3   ...
4   State3={ Choice1 receive_Choice1LabelFromS(): ...
5       <_250DASH, _250>: State4, State5 }]
6   State4={ String receive_250dashStringFromS(): State3 }
7   State5={ String receive_250StringFromS(): State6 }
8   ...
9   State27={ void send_dataStringToS(String): State28 }
10   ...
11   State29={ void send_SUBJECTToS(): State30,
12       void send_DATALINEtoS(): State31,
13       void send_ATADToS(): State32 }]
14}
```

The receive and send messages in the SMTP.C local protocol are interpreted as typestate methods in the CProtocol typestate specification. For example, the message \texttt{_220(String)} received from S given in line 2 in SMTP.C becomes a method with signature:

```
String receive_220StringFromS()
```
given in line 2 in CProtocol.

Similarly, the message \texttt{data(String)} sent to S and given in line 9 of SMTP.C becomes a method with the following signature:

```
void send_dataStringToS(String)
```
given in line 10 in CProtocol.

Let us now comment on choice. The \texttt{external} choice made at role S different from \texttt{self} is given in lines 4-18 of SMTP.C. For every external choice in the local protocol there is an enumerated type in the typestate, such as the following:

```
enum Choice1 { _250DASH, _250 }
```
The values of Choice1 are determined by the first interaction of every branch in the choice. The external choice itself is translated as a receive method returning the enumerated type Choice1 and given in lines 4-5 of CProtocol:

```java
Choice1 receive_CHOICE1LabelFromS() :
  _250DASH: State4, _250: State5
```

After choosing one of the branches, _250DASH or _250, the payload of type String is received via another method call, following the choice: receive_250DASHStringFromS() in line 7 and receive_250StringFromS() in line 8, respectively for the two available choices.

The internal choice made at self, namely role C (lines 11-17 of SMTP_C), is translated into a set of send methods, one for each branch of the choice (lines 12-14 of CProtocol). When running the program, only one of the methods will be called, thus performing a single message selection corresponding to it.

CRole implements all the methods in CProtocol. In this implementation, since communication occurs on Java sockets, we declare and create a new socket to connect to the g-mail server. This is given in lines 2 and 4 in CRole, respectively.

```java
private Socket socketS = null; ...
public CRole()
{ socketS = new Socket("smtp.gmail.com", 587); }
```

We now describe the correspondence between the text-based commands in SMTP and the method calls in Mungo. Consider “SUBJECT: Hello World”, which is an atomic command starting with the keyword SUBJECT and followed by the subject text. In our framework we use an intermediate layer to split the above command into two separate method calls, as shown in lines 7-9 in CMain. The first, send_SUBJECTToS(), selects the command SUBJECT. The second, send_subjectStringToS("Hello World"), completes and sends the message “SUBJECT: Hello World”. The intermediate layer is also used when receiving a command from the server, by splitting it into a choice and the corresponding text.

Finally, CMain.java contains the main method where the CRole object is created and used to implement the client logic.

```java
public static void main(String[] args) {
CRole currentC = new CRole();
  ...
  switch(/* label to be sent*/)
  {
    case /*ATAD*/:
      currentC.send_subjectStringToS(/*subject*/);
      String _250msg =
        currentC.receive_250StringFromS();
      continue _Z1;
    ...
```


\[
o ::= C[f \rightarrow o] | c \quad r ::= \text{root} | r.f \\
e ::= \ldots | e @ r \quad v ::= e | r \\
S ::= \ldots | (S)_E \quad s ::= T \text{m}(T) | E \text{m}(T) : l | l \\
E ::= [] | r.(\text{m}(E)) | r.f = v | E \text{; } r \text{ switch } (E) \{ e \}_E | E \text{; } r \text{ if } (E) \text{ else } e.
\]

\[
\ell ::= r.(\text{f}.\text{new } C) | r.l | r.(T \text{ m } T') | r.f = v | \tau | \text{if}
\]

**Figure 2.** Runtime syntax

\(r\), rather than an arbitrary expression. The other expression forms include sequential composition \(e; e'\), switch expressions, \(\text{if } \ldots \text{ else }\) expression, labelled expressions \(\lambda : e\), and continue expressions which jump to the enclosing expression labelled by \(\lambda\).

**Configurations and runtime syntax.** Fig. 2 extends the source syntax with additional runtime constructs used by the operational semantics. A configuration \(h, e\) is the pair of a heap \(h\) and runtime expression \(e\). The heap \(h\) is defined as an object \(C[f : o]\), where \(C\) is the class of the object and \(f : o\) are its fields; the contents \(o\) of each field is either a constant \(c\) or another object. The “heap” is a tree of objects, with neither cycles nor sharing, due to the linearity of object references enforced by the type system (see §6).

The expression \(e\) in a configuration \(h, e\) is a runtime expression in which every (compile-time) path of the form this, \(r.f\), or \(x\) has been replaced by a runtime path which refers to a heap value. A runtime path \(r\) in a heap \(h\) is either the static path root denoting \(h\) itself or the composite path \(r'.f\) denoting the field \(f\) of the object denoted by \(r'\), where \(r'\) is also a path in \(h\). Runtime expressions also include the form \(e @ r\), which is an expression \(e\) which has been tagged with \(\tau\) to track the active receiver. A value \(v\) is either a constant \(c\) or runtime path \(r\). Every runtime expression is either a value, or uniquely of the form \(E[e]\), where \(E\) is an evaluation context (an expression with a hole). As usual, the notation \(E[e]\) denotes the plugging of the hole in \(E\) with an expression \(e\).

The operational semantics is annotated with labels \(\ell\) that denote the creation of a new object \(r.(\text{f}.\text{new } C)\), an enum value choice \((v = l)\), method call \((r.f : T')\), assigning a field \((r.f = v)\), the conditional label \((\text{if } E)\), and the silent label \((r)\). The definition of states is extended to the set of enum values \((\ell : S)_E\) and we define action labels \(s\) for labels: internal choice \(T \text{m}(T)\), external choice \(E \text{m}(T) : l\), and for enum values \(l\).

**Labelled reduction semantics.** We define heap access and update functions that are used by the reduction relation in Fig. 3: \(h(\text{root}) = h\); \(h(\text{f}. f) = o\) and \(h(\text{f}. f' \rightarrow o') = h(\text{f}. f) \rightarrow C[f : o; f : o']\) if \(h(\text{f}) = C[f : o]\). The root object is accessed via \(h(\text{root})\). The access of a field \(hr(f)\) inductively defined on the access of \(h(\text{r})\). Similarly, we use the heap access function to update object fields as in \(h(\text{r} . f = v)\). Fig. 3 defines the labelled reduction semantics; hereafter by “expression” we shall mean runtime expression, and by “path” runtime path, unless otherwise indicated. Rule R-SEQ discards the value \(v\) in a \(\tau\) label and proceeds with the evaluation of \(e\). Rules R-TRUE and R-FALSE are the usual rules for the \(\text{if } \ldots \text{ else }\) expression and are annotated with label \(\text{if}\). Rule R-New is labelled with \(r.(\text{f}.\text{new } C)\) and overwrites the contents of the field \(f.f\) by a new object \(C[f \rightarrow \text{init}(T)]\) whose fields are all initialised to the value \(\text{init}(T)\), where \(T\) is the type of the field, defined as: \(\text{init}(C) = \text{null}\); \(\text{init}(E) = E_{\text{init}}\); \(\text{init}(\text{boole}) = \text{true}\); and \(\text{init}(\text{void}) = s\), where for every enumerated type \(E\) we require there to be a distinguished element \(E_{\text{init}} \in \text{enum}(E)\). The result of R-New is the void value \(\ast\). There is no allocation of a fresh location; instead the object is constructed at an existing location \(r.f\). There are two assignment rules, depending on whether the value being assigned is a constant or an object path. Both forms return the void value \(\ast\). A constant \(c\) has no associated typestate and may be used unrestrictedly; therefore the R-Asgn\(C\) rule is labelled with \(\tau\) and simply updates the heap to store \(c\) in \(r.f\). A path

\[
\text{Figure 3. Operational semantics}
\]

\(r',\) on the other hand, refers to an object and must be used linearly. Therefore the effect of the R-Asgn\(R\) rule is to relocate the object from \(r'\) to \(r.h\), leaving \(\text{null}\) at its old location. The annotation label for R-Asgn\(R\) is \(r.f = v\). The R-Call rule is labelled with \(r.T \text{ m } T'\) and resolves the method \(m\) by first looking up the receiver \(r\) in the heap, which must be an object \(C[f : o]\), and then selecting the method \(m\) from the definition of \(C\). Prior to executing the selected method, we convert its body \(e\), which is a source-level expression, into a runtime expression by substituting the runtime path \(r\) for this and also \(v\) for the formal parameter. In addition, the resulting runtime expression is tagged with \(\tau\) recording the fact that \(r\) is the active receiver. The active receiver tag \(\tau r\) on a value is removed using a \(\tau\) label when the value is fully evaluated and it is not an enum label, as defined by rule R-VALUE. If the value returned by the method is an enum label \(l'\), then it must occur as the scrutinee of a switch expression; rule R-Switch defines the reduction via action \(r.(l')\), of the switch expression to the branch indicated by \(l'\). The \(r\) is used in the reduction label to indicate which object made the choice. Rule R-Label is labelled with \(\tau\), and says that a labelled expression \(\lambda : e\) discards the \(\lambda\) and substitutes a copy of the labelled expression for every occurrence of continue \(\lambda\) that occurs in the loop body \(e\). Rule R-Ctx lifts these rules to an arbitrary expression using an evaluation context. It is easy to show that the operational semantics is deterministic.

Assume a heap consisting of an instance of class \(C\), where given fields\((C) = T f\), each field of \(C\) is initialised with the corresponding value \(\text{init}(T)\). Execution can then be initiated using a top-level expression that substitutes path \(\text{this}\) with path root.

6. Typestate Inference

In this section we formalise a typestate inference system and prove its safety properties. The system presented here infers a typestate
The type inference is syntax-driven, meaning that at any point of the derivation there is only one rule that can be applied. Rules S-Term and S-Rec1 define the subtyping relation for typestates and under recursion, respectively. The last rule defines a reduction on a runtime typestate, as defined in Fig. 2. It states that a typestate reduces to a subtype if it is a subtyping relation. Finally, rules S-Enum and S-Empty define the subtyping relation for enumerated types and the empty typestate, respectively.

The type inference system infers the typestates of a program. A sound inference system should be able to guarantee that a well-typed program is included in the trace of the inferred type for every value of the enumerated type. The subtyping relation generalises to inferred types and typing contexts. Finally, we define a transition relation on typestates as follows.

**Definition 6.2 (Transition on typestates).** Transition relation $S \xrightarrow{t} S'$ is defined as:

$$
T \leftarrow E \leftarrow m(T) : S \xrightarrow{m(T)} S' \xrightarrow{E m(T)} \leftarrow E m(T) \xrightarrow{\mu \times X / S} S' \xrightarrow{\mu \times X / S} S' \xrightarrow{\mu \times X / S} S' \xrightarrow{\mu \times X / S} S' \xrightarrow{\mu \times X / S} S'$$

The first two rules state that a method prefix typestate reduces to its continuation under a label denoting the prefix method signature itself. The next two rules state that reduction can occur in a set of typestates and under recursion, respectively. The last rule defines a reduction on a runtime typestate, as defined in Fig. 2. It states that a branching typestate reduces to one of its components by using the corresponding enumerated value.

### 6.1 Typestate inference rules

Before introducing the typestate inference rules, we define the typing judgments:

$$
\Delta \vdash e : U + \Delta' \Delta \vdash C[S] \vdash \text{class } C : S : \{\vec{F}, \vec{M} \} \vdash \vec{D}
$$

The first one is the typing judgement for expressions. The judgement is read from right to left. It takes as input the typing context $\Delta'$ and the expression $e$, and algorithmically computes the type $U$. The effects of the expression on $\Delta'$ are then captured in $\Delta$. However, it is interesting to notice that the judgement can also be read from left to right in a type system fashion, where the expression “consumes” $\Delta'$ in order to produce $\Delta$. The second judgement infers the typestates of the fields of a class when the class is used according to its declared typestate. The last two typing judgments state the well-formedness of classes and, respectively, programs.

The typestate inference rules for expressions are given in Fig. 6. We illustrate the most important rules using examples. The full typestate derivation of the example code can be found in App. C. The type inference is syntax-driven, meaning that at any point of the derivation there is only one rule that can be applied. Rules Void, Bool, Enum and Null type the constants with their corresponding types.
under any typing context without producing any effect on it, namely the left and right typing contexts are the same. Rules **STRENGTHEN** and **WEAKEN** allow arbitrary removal and addition, respectively, of inactive typestate assumptions.

**Typestate Linearity.** In the typestate inference system we adopt linearity in order to forbid aliasing. We use the following example to explain rules **SEQ**, **PARN**, **PANC**, **ASGC**, **ASGR**, **NEW**, that require treatment of linearity. Consider the following code that uses the implementation of class Stack in section §1:

```java
s = new Stack; k = s
```

The code expression matches rule **SEQ**. We assume $\Delta_0 = s : Stack[end], k : Stack[S]$ as an input typing context and $S \trianglerighteq \trianglerighteq StackProtocol$. Rule **SEQ** requires an inference for the second expression before the first, because the output typing context of the second expression is the input typing context of the first expression. In order to type the second expression by **ASGC** we need to infer a typestate for $s$. To respect linearity we take $\Delta_1 = s : Stack[end], k : Stack[end]$ as input. The derivation is as:

**PARN**

```java
\Delta_2 = s : Stack[S], k : Stack[end] \vdash s : Stack[S] + \Delta_3
\Delta_2 \vdash k : s : void + \Delta_0
\Delta_2 = k : s : void + \Delta_0
```

The outer typing context for **PARN** is $\Delta_2 = s : Stack[S], k : Stack[end]$, meaning that $k$ has an inactive typestate before assignment. Rule **PARN** on its own “guesses” a type for a path expression. However, the combination of **PARN** and **ASGR** is the key to this inference since it enforces a match on the type of $s$ in the output typing context $\Delta_2$ and the type of $k$ in the input typing context $\Delta_0$. For the first expression in (1) we use rule **NEW**. By assumption we satisfy its premise; we have $S \trianglerighteq StackProtocol$, meaning path $s$ is used according to the StackProtocol typestate (this is shown in $\Delta_2$). Rule **NEW** infers a type void for the first expression. Since it is not a class type it satisfies the premise of rule **SEQ** which requires the type of the first expression not to be a class type, so it can be discarded without violating linearity. It also requires that the type of the first expression is not of type bool to disallow dead code after a continue expression (see rule **CONTINUE**). The type of the sequential expression is the type of the latter expression, void, We summarize the derivations described so far in the following:

![Figure 6. Typestate inference rules for expressions](image-url)
every branch is the same as the one for switch, namely \( \Delta_l \). The inferred output contexts of the branches are then joined and used in input to infer a typestate for the method call expression in the condition of the switch. The condition should have an enumeration type that matches the type of the switch definition. Finally, the type of switch is the join of the types of its branches. For the true branch we use rule \( \text{PanR} \):

\[
P\Delta_l \cdot x : \text{Stack}[S], \text{this : StackUser[end], loop} : X
\]

\[
\Delta_1 \vdash x : \text{Stack}[S] + \Delta_1
\]

For the false branch we first use rule \( \text{Seq0} \) and then continue \( \text{Continue} \) to infer the typestate of the continue loop expression. \( \text{Continue} \) requires loop to be mapped to a recursive variable \( X \) in the input typing context. It then outputs a typing context where all paths mapped to a typestate are updated to the typestate \( X \), as in:

\[
\text{Continue} \quad \Delta_1 \vdash x : \text{Stack}[X], \text{this : StackUser}[X]
\]

The type of the continue expression is bot, since we want \( \text{join}(\_, \_) \) to be defined (cf. Fig. 5). To complete the typing of the false branch, we apply rule \( \text{Call} \) for \( x \cdot \text{pop()} \) and conclude with rule \( \text{Seq0} \). The output typing context is:

\[
\Delta_1 \vdash x : \text{Stack}[X], \text{this : StackUser}[X]
\]

We join the output typing contexts \( \Delta_1 \) and \( \Delta_2 \) of the true and false branch, respectively and use the result as an input typing context for the method call \( x \cdot \text{isEmpty()} \), as stated by the premises of Switch. The output typing context of Switch is:

\[
\Delta_1 \vdash x : \text{Stack}[\text{Choice isEmpty}()]\text{join}(S, \text{int pop}() : X)], \text{this : StackUser}[\text{join}(end, X)]
\]

To complete the inference of \( \text{LEXpr} \) we close the recursive variable \( X \) in \( \Delta_1 \) and obtain the output typing context for the labelled expression in lines 4-5, which is:

\[
\Delta_6 \vdash x : \text{Stack}[\mu X.\text{Choice isEmpty}()]\text{join}(S, \text{int pop}() : X)], \text{this : StackUser}[\mu X.\text{join}(end, X)]
\]

Notice the equivalence of the type \( \mu X.\text{join}(end, X) \), that appears in the mapping of path this, and the type end, meaning that rule \( \text{equiv} \) can be applied.

Rule \( \text{If} \) types the conditional expression in a similar way as rule \( \text{Switch} \). Both conditional branches are individually inferred and then joined to obtain the output typing context of the if ... else expression. We further require that the condition has type bool.

Method Call. Rule \( \text{Call} \) records the method call trace of paths in a program, to respect the principle that the trace of the execution of an object follows its inferred typestate. It uses the function \( \text{initT} \), defined by \( T \neq C \implies \text{initT}(T) = T \) and \( \text{initT}(C) = C[\text{end}] \).

Rule \( \text{Call} \) requires type checking the method body every time a method is called. This is a simplification for presentation purposes. It means that if an algorithm is directly extracted from the rules, it is unable to construct a type in the case of a recursive method call. However, the rules can be used to derive typings if suitable pre- and post-conditions are put into the derivation by hand. The implementation of Mungo's type inference system uses a more complex notion of partial typestate so that method bodies do not need to be checked at every call site; recursive methods are also supported.

As an example of the rule \( \text{Call} \), consider the following code that uses class \( \text{StackUser} \):

\[
s = c \cdot \text{push}(s)
\]

and \( \Delta_0 = s : \text{Stack}[S], c : \text{StackUser}[\text{Stack popAll}(\text{Stack}) : \text{end}]) \), the input typing context. By applying rule \( \text{LgenR} \) on the above assignment with input \( \Delta_0 \), the output typing context in the premise of the rule is \( \Delta_1 = s : \text{Stack}[\text{end}], c : \text{StackUser}[\text{Stack popAll}(\text{Stack}) : \text{end}] \). At this point we can apply rule \( \text{Call} \) on \( c \cdot \text{push}(s) \) and have the following derivation:

\[
\text{Stack push}(\text{Stack } x) \{ x \text{ push}(2); x \} \in \text{methods}(\text{Stack push}) \quad (1)
\]

\[
\Delta_2 \vdash x \cdot \text{push}(2); x[\text{this : Stack}[S] + \Delta_1 \quad (2)
\]

\[
\Delta \vdash \text{c push}(s) : \text{Stack}[S] + \Delta_1 \quad (3)
\]

The premise of \( \text{Call} \), given in (1), performs a lookup in the methods of the class of the receiver, \( \text{ListCons} \), to obtain the definition of method \( \text{Stack push}(\text{Stack}) \). Next, in (2), the premise infers a typestate for the body of the method in which \( c \) has been substituted for the keyword this. Both the method call and its body use the same input typing context. The output typing context of the body of the method should contain a typestate assumption for the method parameter and the receiver, as follows: \( \Delta_2 = \Delta_1, x : \text{Stack}[\text{[void push(int) : S]}] \). Then, in (3) \( \text{Call} \) requires a typestate inference in order to match the typestate of the method parameter with the type of the method call argument. For this rule \( \text{PanR} \) is used where \( \Delta_3 \) also updates the type of the receiver:

\[
\Delta_3 = s : \text{Stack}[\text{end}],
\]

\[
c : \text{StackUser}[\text{Stack push}(\text{Stack}) : \{ \text{Stack popAll(\text{Stack}) : \text{end}])}
\]

Rule \( \text{Call} \) requires that the types of the receiver \( c \) in the input and output typing contexts for the body of the method are equivalent, according to the relation \( \text{seq} \). This is to respect the abstraction principle: the client would know how a method uses its receiver. For example, assume method \( \text{Stack push}(\text{Stack}) \) is defined as:

\[
\text{Stack push}(\text{Stack } x) \{ x \cdot \text{push}(2); x = \text{this . popAll}(x); x \}
\]

If we infer a typestate for the body of \( \text{Stack push}(\text{Stack}) \) with input context \( \Delta_1 \) we get: an output typing context \( \Delta' \), such that:

\[
\Delta'(c) = \text{StackUser}[\text{Stack popAll}(\text{Stack}) : \{ \text{Stack popAll(\text{Stack}) : \text{end}])}
\]

Given that \( \Delta_1(c) = \text{StackUser}[\text{Stack popAll}(\text{Stack}) : \text{end}], \) it is revealed that the body of \( \text{Stack push}(\text{Stack}) \) calls method \( \text{Stack popAll(\text{Stack}) \text{ on its receiver object, thus violating the abstraction principle.}

Classes and Programs. The rules for classes and programs are given in Fig. 7. They make use of inference rules for the fields of a class, which we explain first. The typestates of the fields of a class are inferred when method calls of that class take place. This procedure is described by the inference rules for typestates. Rule \( \text{Set-S} \)-\( \text{R} \) requires the inference and join of the typestates of all branches in an internal choice. Rule \( \text{Method} \)-\( \text{SY} \) relies on the \( \text{infer(T)} \) definition that maps a type \( T \) to the corresponding inferred type \( U \) as: \( \text{infer}(T) = C \implies T = \text{infer}(T) = C[\text{end}] \), for some \( S \). Rule \( \text{Method} \)-\( \text{SY} \) infers a method- prefixed typestate, where first it infers an inference of the continuation typestate, and then uses the output typing context to infer the method prefix; it infers a typestate for a method definition by first inferring a typestate for its body. The auxiliary function \( \text{infer}(T) \) is used to check that the return and parameter type of the method match the types of the inferred ones.

As in \( \text{Call} \), a self-call should preserve the typestate of the receiver up to type equivalence. Rule \( \text{Enum-S} \)-\( \text{R} \) is similar to rule \( \text{Method} \)-\( \text{SY} \). It requires the inference and join of the typestates of all the external choices and then infers the method prefix. Rule \( \text{End-S} \)-\( \text{R} \) requires all fields of the class to finish in the inactive typestate. Rules \( \text{Rec-S} \)-\( \text{R} \) and \( \text{Var-S} \)-\( \text{R} \) are similar to rules \( \text{LEXpr} \) and \( \text{Continue} \), where they bind and use a recursive variable, respectively. Rule \( \text{Class} \) initiates the inference of the typestate of the class. It states that a class declaration is well-typed if every field of the class has an inactive typestate and this is assumed in the typing context in the premise of \( \text{Class} \). A program is well-typed if all of its classes are well-typed, as stated by rule \( \text{Program} \). To illustrate the rules, we show a typestate inference for \( \text{StackUser} \) in App. C.

In Fig. 8 we give the inference rules for runtime expressions. We show only the ones that are different with respect to the rules in Fig. 6. Rule \( \text{Switch-Ar} \)-\( \text{R} \) is similar to \( \text{Switch} \), the difference being the condition of the switch, which is evaluated to an active receiver.
\[ \Delta' \vdash C[S] \quad T : m(T2 \ x) \{ e \} \in \text{methods}(C) \quad \forall t, S' \xrightarrow{T} S \implies S \xrightarrow{T} S \quad \forall H \in \vec{T}, \Delta_H \vdash C[\{H\}] \]

\[ \Delta, : C[S'], x : \text{infer}(T(T)) \implies \Delta' : C[S], x : \text{init}(T(T)) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]

\[ \forall \ell \in E, \Delta \vdash C[S] \quad E \vdash m(T x) \{ e \} \in \text{methods}(C) \]

\[ \Delta \vdash C[\{E(m(T x))\} \{ e \} : E + \Delta'' \quad \Delta' = \text{join}(\Delta \upharpoonright C[S]) \]
situations including scientific computation [37] and event-driven programming [26]. SJ implements a library for binary sessions that have a pre-defined interface. The Java syntax is extended with communication statements that enable typechecking. The scope of a session is restricted to the body of a single method. Mungo lifts these restrictions by allowing the abstraction of multiparty session types as user-defined objects that can be passed and used throughout different program scopes. Gay et al. [23] outlined an implementation of their type system as a language called Bica, which is not currently maintained and is unusable. Mungo improves on Bica by using type inference to remove the need for typestate declarations on methods.

The work in [26] extends Session Java with runtime type inspection and asynchronous communication semantics to enable an event-driven framework based on binary session types. As a use case, they implemented a binary session-type SMTP server that uses a reactive structure to handle multiple clients concurrently. In our work, we implement an SMTP client by using StMungo, which automatically generates code from a global protocol. Extending Mungo with runtime typestate inspection would enable us to investigate event-driven programming with multiparty session types.

Capcchi et al. [9] proposed that a class defines sessions instead of methods. A session generalizes a method to an extended session typed dialogue over a communication channel. As far as we know, this new paradigm has not yet been implemented.

The work in [36] typechecks the operations of a library that implements multiparty session types using a restricted set of MPI [30] primitives. In contrast, our framework typechecks Java statements and expressions, instead of higher-level operations. The work in [35] uses Scribble to automatically generate MPI code based on user-defined kernels that produce and consume data. The generated code does not require typechecking. On the other hand, the StMungo translation can be used together with the Mungo typechecker to develop more flexible multiparty session type implementations.

Monitoring based on Scribble definitions. Neykova et al. [34] have used Scribble protocol definitions to achieve dynamic monitoring in Python, by translating local protocols into finite state machines that intercept communication and check the validity of runtime messages. Subsequently, [33] implements a session-based Actor framework that uses runtime monitoring to integrate multiparty session types. A hybrid approach has been used by Hu [27] to analyse an SMTP client in Java. Hu’s SMTP API implements multiparty session types using a pattern in which each communication method returns the receiver object with a new type that determines which communication methods are available at the next step. If the pattern is used properly, then standard Java typechecking can verify correctness of communication, but runtime monitoring is needed to check linearity constraints. In contrast, our analysis of SMTP is able to statically check all aspects of the protocol implementation.

The receiver-returning pattern is at the basis of functional programming with session types [22] and has been used to achieve protocol checking in Idris [29] and as a replacement for explicit typestate in Rust [39].

Typestate. There have been many efforts to add typestate to practical languages, since their introduction in [42]. Vault [12, 19] is an extension of C, and Fugue [13] applies similar ideas to C#. Plural [6] is based on Java and has been used to study access control systems [5] and transactional memory [4], and to evaluate the effectiveness of typestate in Java APIs [6]. In contrast, Mungo follows Gay et al. which is inspired by session types; the possible sequences of method calls are explicitly defined, rather than being consequences of pre- and post-conditions. Like Plural, a typestate in Mungo can depend on the return value of a method call.

Sing# [18] is an extension of C# which was used to implement Singularity, an operating system based on message-passing. It incorporates typestate-like contracts, which are a form of session type, to specify protocols. Bono et al. [8] have formalised a core calculus based on Sing# and proved type safety.

Aldrich et al. [2, 43] proposed a new paradigm of typed, state-oriented programming, implemented in the Plaid language. Instead of class definitions, a program consists of state definitions containing methods that cause transitions to other states. Transitions are specified in a similar way to Plural’s pre- and post-conditions. Like classes, states are organised into an inheritance hierarchy. The most recent work [20, 44] uses gradual typing to integrate static and dynamic typestate checking. We focus on the object-oriented paradigm in order to be able to apply our results to Java.

Bodden and Hendren [7] developed the Clara framework, which combines static typestate analysis with runtime monitoring. The monitoring is based on the tracematches approach [3], using regular expressions to define allowed sequences of method calls. The static analysis attempts to remove the need for runtime monitoring, but if this is not possible, the runtime monitor is optimised. Mungo uses a purely static analysis, and can allow the state after a method call to depend on the method’s (enumerated type) result.

Typestate systems must control aliasing; otherwise method calls via aliases can cause inconsistent state changes. Literature includes the “adoption and focus” approach of Vault and Fugue, the permission-based approaches of Plural and Plaid, and an expressive fine-grained system by Militão et al. [31]. Also relevant is recent work by Crafa and Padovani [11] which applies the chemical approach to concurrent typestate oriented programming, allowing objects to be accessed and modified concurrently by several processes, each potentially changing only part of their state. We expect that many of these systems can be applied to Mungo. However, linear typing has not been a limiting factor for the applications described in the present paper.

8. Concluding Remarks and Future Work

Concluding Remarks. We have presented two tools, Mungo and StMungo, which extend the Java development process with support for typestate checking of communication protocols. Mungo extends Java with typestate definitions, which associate classes with state machines defining permitted sequences of method calls. StMungo uses the typestate feature to connect Java to Scribble, the latter being a language used to specify communication protocols. In order to illustrate the practicality and robustness of Mungo and StMungo, we have implemented a substantial use case, an SMTP client, which we were able to statically typecheck. We use this client to communicate with the Gmail server. Finally, we have formalised the essential features of Mungo by defining a typestate inference system for a core object-oriented language. We proved safety and progress properties (Theorem 6.3). These properties guarantee the coherence of the typestate inference system with respect to the declared typestate in a program (Corollary 6.4).

Future Work. The combination of Mungo and StMungo is effective for statically checking the correct implementation of communication protocols. We intend to extend Mungo to increase its power for general-purpose programming with typestate. Our first aim is to generalise the use of linear typing as a mechanism for the alias control required by typestate systems. Candidates include the “adoption and focus” technique of Vault and Fugue, the permission-based approaches of Plural and Plaid, and the system by Militão et al. [31]. Another aim is to support generics and inheritance. Inheritance between typestate classes requires a subtyping relation between their typestate specifications, based on standard definitions of subtyping for session types [21]. Method calls on an object whose type is a generic parameter must be typechecked against the typestate specification of the parameter’s upper bound. To extend typechecking to exception handlers, we need to allow typestate specifications to define the state transitions corresponding
to exceptions, and check that these transitions are consistent with the states of fields at the point where an exception is thrown. Existing work on exceptions in session types [10] provides inspiration, but doesn’t address the complexities of Java’s exception mechanism. Using these Mungo extensions with SiMungo for more sophisticated protocol verification will also require extensions to Scribble to support generic protocols, inheritance between protocols, and more general handling of exceptions.

Acknowledgements This research was supported by UK EPSRC grant EP/K034413/1 From Data Types to Session Types: A Basis for Concurrency and Distribution. We thank Laura Voina for her contribution to Mungo and SiMungo. We thank Garrett Morris, Raymond Hu and Nobuko Yoshida for useful comments and discussion.

References
A. Progress and Subject Reduction

A.1 Auxiliary Results

In the following we use $\Delta(v : U)$ to denote $\Delta$ where the value $v$ is updated to the type $U$.

**Lemma A.1 (Typability of Heap Update).** Let $h$ be a heap and $r$ a runtime path such that $\Delta \vdash h$ and $r : U \in \Delta$.

1. If $U \models C[S]$ and $\Delta \vdash o : U + \Delta$, then $\Delta \vdash h[r \mapsto o]$.
2. If $U = C[S]$ and $\Delta \vdash o : C[S'] + \Delta'$, then $\Delta' \vdash h[r \mapsto o]$, where $\Delta' = \Delta[r : C[S']]$.

**Proof.** Both cases follow by using rule $\text{Heap}$ and for 1. typing rules for constants are used, and for 2. rule $\text{Object}$ is used.

**Lemma A.2** (Replacement). If

- $d$ is a derivation for $\Delta \vdash E[e] : U + \Delta'$,
- $d'$ is a subderivation of $d$ concluding $\Delta \vdash e : U_e + \Delta_e$,
- the position of $d'$ in $d$ corresponds to the position of the hole in $E$,
- $\Delta' \vdash e' : U_e + \Delta_e$, such that $U_e \leq_{\text{st}} U_e$,

then $\Delta' \vdash E[e'] : U + \Delta'$ such that $U' \leq_{\text{st}} U$.

**Proof.** Follows [23], by replacing the derivation $d'$ in $d$ with the derivation for $\Delta' \vdash e' : U_e + \Delta_e$.

**Lemma A.3** (Substitution). If $U, U'$ be inferred types such that $\text{join}(U, U')$ is defined. Then, $U \leq_{\text{st}} \text{join}(U, U')$ and $U' \leq_{\text{st}} \text{join}(U, U')$.

**Lemma A.4** (Subtyping and join). The following relate subtyping and join on inferred types $U$ and typing contexts $\Delta$.

- Let $U, U'$ be inferred types such that $\text{join}(U, U')$ is defined. Then, $U \leq_{\text{st}} \text{join}(U, U')$ and $U' \leq_{\text{st}} \text{join}(U, U')$.
- Let $\Delta, \Delta'$ such that $\text{join}(\Delta, \Delta')$ is defined. Then, $\Delta \leq_{\text{st}} \text{join}(\Delta, \Delta')$ and $\Delta' \leq_{\text{st}} \text{join}(\Delta, \Delta')$.

**Proof.** The proof follows immediately by combining the definition of subtyping in Fig. 4 and the definition of join Fig. 5.

**Lemma A.5** (Typability of Subterms). If $d$ is a derivation for $\Delta \vdash E[e] : U + \Delta'$ then there exist $\Delta'$ and $U'$ such that $d$ has a subderivation $d'$ concluding $\Delta \vdash e : U' + \Delta'$ and the position of $d'$ in $d$ corresponds to the position of the hole in $E$.

**Proof.** The proof proceeds by induction on the structure of context $\Delta$.

- $E = []$: follows trivially by assumption.
- $E = r.m'E'$: by assumption $\Delta \vdash r.m'[E'[e]] : U + \Delta''$. By inversion on rule $\text{Call} \vdash E'[e] : U + \Delta''$, $r : C([T m'(T') : S])$, where the typing context $\Delta''$ and the type of $r$ are inferred by the premise of $\text{Call}$. We conclude by induction hypothesis on $E'$.
- $E = r.f = E'$: by assumption $\Delta \vdash r.f = E'[e] : U + \Delta'$. There are two rules that can be applied for assignment, rule $\text{AssignC}$ and rule $\text{AssignR}$. By inversion on the former we obtain $\Delta \vdash E'[e] : U + \Delta''$, $r : U'$; by inversion on the latter we obtain $\Delta \vdash E'[e] : C[S] + \Delta''$, $r : C[end]$, where the typing context $\Delta''$ and the type for $r$ are inferred by the premise of the rule. We conclude by induction hypothesis on $E'$.
- $E = E';e'$: by assumption $\Delta \vdash E'[e'] : U + \Delta''$. By inversion on rule $\text{Seq} \vdash E'[e'] : U'' + \Delta''$, where the typing context $\Delta''$ and the type $U''$ are inferred by the premise of the rule. We conclude by induction hypothesis on $E'$.

The rest of the cases follow the same idea as the above.

A.2 Progress and Subject Reduction

**Proof of Theorem 6.3.** Let $\widetilde{D}$ be a set of declarations such that $\vdash \widetilde{D}$. In a context parametrized by $\widetilde{D}$, let $e$ be a run time expression and suppose $\Delta \vdash h, e : U + \Delta'$.

Then, either $e$ is a value, or there exists $f, h'$ and $e'$ such that $h, e \xrightarrow{f} h', e'$, and there exist $\Delta'$ and $U'$ such that $\Delta \xrightarrow{f} \Delta'$ and $\Delta' \vdash h', e' : U' + \Delta''$ and $U' \leq_{\text{st}} U$. **Proof.** The proof proceeds by induction on the structure of the expression $e$ with respect to contexts. We present first the inductive case. Let $e = E[e_1]$ where $e_1$ is not a value and $E \neq []$. By assumption and inversion on rule $\text{Config}$ we have $\Delta \vdash E[e_1] : U + \Delta'$. By Lemma A.5 there exist $\Delta_1$ and $U_1$ such that $\Delta \xrightarrow{f} \Delta'$ and $\Delta' \vdash h, e_1 : U_1 + \Delta_1$. By induction hypothesis there exist $h', \ell$ such that $h, e_1 \xrightarrow{\ell} h', e_2$. By induction hypothesis we also have $\Delta \xrightarrow{\ell} \Delta'$ and $\Delta' \vdash h, e_2 : U_2 + \Delta_1$, which by inversion on $\text{Config}$ means that $\Delta' \vdash h$ and $\Delta' \vdash e_2 : U_2 + \Delta_1$, where $U_2 \leq_{\text{st}} U$. By rule R-Ctx we have $h, E[e_1] \xrightarrow{\ell} h', E[e_2]$ by Lemma A.2 we obtain $\Delta' \vdash E[e_2] : U' + \Delta''$ with $U' \leq_{\text{st}} U$. We conclude by rule $\text{Config}$.

The base cases when $e$ is of the form $E[v]$ with $E$ elementary, not being of the form $E[E'[e]]$ with $E' \neq []$, and not of the form $E[e_1]$ are in the following. If $e$ is a value, then there is nothing to prove. For $e$ is not a value, by the operational semantics rules, we have the following cases for $e$ with respect to contexts.
• \( e = v; e' \). By hypothesis and reduction rule R-Seq

\[ h,(v;e') \xrightarrow{\ell} h,e' \]

By hypothesis and typing rule CONFIG \( \Delta \vdash h \) and \( \Delta \vdash v; e': U \vdash \Delta'' \). By inversion and typing rule Seq

\[
\begin{align*}
\Delta &\vdash v: U' \vdash \Delta_1 \quad U' \neq \mathcal{C}[S] \\
\Delta_1 &\vdash e': U \vdash \Delta''
\end{align*}
\]

By reduction rule Ty-To \( \Delta \xrightarrow{\tau} \Delta \). Since \( U' \neq \mathcal{C}[S] \) and value \( v \) is of type \( U' \) it means \( v \) is some constant \( c \). Hence, the judgement \( \Delta \vdash v: U' \vdash \Delta_1 \) is obtained by applying one of the following typing rules: VOID, ENUM, or BOOL. By inversion this implies \( \Delta_1 = \Delta \). Then, by rewriting the premise of the typing rule for \( e' \) we have \( \Delta \vdash e': U \vdash \Delta'' \). We conclude by rule CONFIG.

• \( e = (r.f = \text{new} \ C) \). By hypothesis and typing rule R-New

\[ h,r.f = \text{new} \ C \xrightarrow{\ell} h[r.f \mapsto \mathcal{C}[f : \mathcal{I}mp(T)]] \]

such that fields \( \mathcal{C}[S] = T \). By hypothesis and typing rule CONFIG \( \Delta \vdash h \) and \( \Delta \vdash r.f = \text{new} \ C : U \vdash \Delta'' \). By inversion and typing rule New we have:

\[
\begin{align*}
\text{New} \\
S \xleftarrow{\text{stmt}} \text{typestate}(C) & \quad \forall r.f', f'. C'[S'] \in \Delta_1 \implies S' = \text{end} \\
\Delta_1, r.f : \mathcal{C}[\text{end}] \vdash r.f = \text{new} \ C : \text{void} + \Delta_1, r.f : C[S]
\end{align*}
\]

where \( \Delta = \Delta_1, r.f : C[\text{end}], U = \text{void} \) and \( \Delta'' = \Delta_1, r.f : C[S] \). By rule Ty-New we have

\[
\Delta_1, r.f : C[\text{end}] \xrightarrow{\text{new}} \Delta_1, r.f : C[S] = \Delta''
\]

such that \( S \xleftarrow{\text{stmt}} \text{typestate}(C) \) and for all fields \( r.f', f'. C'[S'] \in \Delta_1 \) and state \( S' = \text{end} \). By applying typing rule VOID we have:

\[
\Delta'' \vdash \text{void} + \Delta''
\]

It remains to prove \( \Delta'' \vdash h' \) namely,

\[
\Delta_1, r.f : C[S] \vdash h[r.f \mapsto \mathcal{C}[f : \mathcal{I}mp(T)]]
\]

Recall that, by hypothesis \( \Delta_1, r.f : C[\text{end}] \vdash h \). Now we want to type the updated reference \( r.f \) to \( C[f : \mathcal{I}mp(T)] \). By rule OBJECT and an empty set of labels \( \bar{s} \)

\[
\text{typestate}(C) = S \\
\Delta_1, r.f : C[S] \vdash C[f : \mathcal{I}mp(T)] : C[S] + \Delta_1, r.f : C[S]
\]

We conclude by Lemma A.1.

• \( e = (r.f = c) \). By hypothesis and by rule R-AsgnC

\[ h,r.f = c \xrightarrow{\ell} h[r.f \mapsto c] \]

By hypothesis and by rule CONFIG \( \Delta \vdash h \) and \( \Delta \vdash r.f = c : U \vdash \Delta'' \). By inversion and typing rule AsgnC we have

\[
\begin{align*}
\text{AsgnC} \\
U' \neq \mathcal{C}[S] & \quad \Delta \vdash c : U' + \Delta', r.f : U' \\
\Delta \vdash r.f = c : \text{void} + \Delta', r.f : U'
\end{align*}
\]

where \( U = \text{void} \) and \( \Delta'' = \Delta', r.f : U' \). Since the value assigned to \( r.f \) is a constant \( c \) the judgement of the premise \( \Delta \vdash c : U' + \Delta', r.f : U' \)

must have been obtained by one of the following typing rules: VOID, ENUM, or BOOL. This implies that \( \Delta = \Delta', r.f : U' \). By Ty-To, \( \Delta \xrightarrow{\tau} \Delta \).

We have to prove that \( \Delta \vdash h[r.f \mapsto c], \text{void} + \Delta', r.f : U' \). By rule VOID, \( \Delta \vdash \text{void} + \Delta', r.f : U' \). Recall that, by hypothesis and rule Heap and inversion we have

\[
\begin{align*}
\text{Heap} \\
h(r.f) = c' & \quad \Delta', r.f : U' + c' : U' + \Delta', r.f : U' \\
\Delta', r.f : U' + h
\end{align*}
\]

By updating the heap to \( h[r.f \mapsto c] \), using the typing judgement for \( c \) in the premise of AsgnC and Lemma A.1 we derive \( \Delta', r.f : U' + h[r.f \mapsto c] \). We conclude by rule CONFIG.

• \( e = (r.f = r') \). By hypothesis and by rule R-AsgnR

\[ h,r.f = r \xrightarrow{r.f \mapsto r'} h'[r.f \mapsto h(r')] \]

where \( h' = h[r' \mapsto \text{null}] \). By hypothesis and by rule CONFIG \( \Delta \vdash h \) and \( \Delta \vdash r.f = r' : U \vdash \Delta'' \). By inversion and typing rule AsgnR

\[
\begin{align*}
\text{AsgnR} \\
\Delta \vdash r' : C[S] + \Delta_1, r.f : C[\text{end}] & \quad \Delta \vdash r.f = r' : \text{void} + \Delta_1, r.f : C[S]
\end{align*}
\]

where \( U = \text{void} \) and \( \Delta'' = \Delta_1, r.f : C[\text{end}] \) and for readability let \( \Delta_2 = \Delta_1, r.f : C[\text{end}] \). Let \( r' \neq r.f \). Since \( r' \) is a path typed by \( C[\text{end}] \), the premise of the above derivation is obtained by applying Paren. This implies that contexts \( \Delta \) and \( \Delta_2 \) differ only in the typing of \( r' \). By
inversion, \( \Delta(r, f) = \Delta_2(r, f) = C[\text{end}] \) and \( \Delta(r') = C[S] \) and \( \Delta_2(r') = \Delta_3(r') = C[\text{end}] \). By rule \( \text{Ty-AsgnR} \)

\[
\Delta_3, r', \Delta': C[S], r, f : C[\text{end}] \quad \leadsto \quad \Delta_3, r, f : C[S], r', : C[\text{end}]
\]

where \( \Delta = \Delta_1, r' : C[S], r, f : C[\text{end}] \) and \( \Delta' = \Delta_3, r, f : C[S], r' : C[\text{end}] \). Since \( \Delta' = \Delta' \), by applying rule \( \text{Void} \) we conclude \( \Delta' + : \text{void} + \Delta'' \). It remains to prove that

\[
\Delta_3, r, f : C[S], r', : C[\text{end}] \vdash h'(r, f \mapsto h(r'))
\]

where \( h' = h[r' \mapsto \text{null}] \). Recall that

\[
\Delta_3, r', : C[S], r, f : C[\text{end}] \vdash h
\]

The result follows immediately by applying twice Lemma A.1 for \( r, f \) and \( r' \). We conclude by \( \text{Constr} \). Let \( r' = r, f \). By rewriting \( \text{AsgnR} \) with \( r, f \) instead of \( r' \) we notice that the derivation holds if \( S = \text{end} \). Then the proof proceeds trivially.

- \( e = r.m(v) \). By hypothesis and by rule \( \text{R-Call} \)

\[
h, r, m(v) \quad \leadsto^t \quad h, e[v/x][r/\text{this}] @ r
\]

such that \( h(r) = C[f : o] \) and \( T \ m(T') \ x \ \{ e \} \in \text{methods}(C) \). By hypothesis and by rule \( \text{Config} \ Δ \vdash h \) and \( Δ \vdash r.m(v) : U + \Delta'' \). By inversion and typing rule \( \text{Call} \)

\[
T \ m(T') \ x \ \{ e \} \in \text{methods}(C) \quad S' =_{\text{def}} S
\]

\[
\Delta_2, r, C[S'], x : U' + e[r/\text{this}] : U + \Delta_1, r : C[S]
\]

\[
\Delta + v : U' + \Delta_2, r : C[(T \ m(T') : S)]
\]

where \( \Delta'' = \Delta_1, r : C[S] \) and for readability let \( \Delta'' = \Delta_2, r : C[(T \ m(T') : S)] \). Notice that \( v \neq r \), otherwise the method call \( r.m(v) \) would not be well-typed. Then, \( \Delta(r) = \Delta''(r) = C[(T \ m(T') : S)] \). Let \( \Delta = \Delta_3, r : C[(T \ m(T') : S)] \). By \( \text{Ty-Call} \)

\[
\Delta_3, r : C[(T \ m(T') : S)] \quad \leadsto^t \quad \Delta_3, r : C[S]
\]

We need to prove that \( Δ_3, r : C[S] \vdash h \) and also \( Δ_3, r : C[S] \vdash e[v/x][r/\text{this}] @ r : U + Δ'' \). By \( \text{ArR} \) it suffices to show \( Δ_1, r : C[S] \vdash e[v/x][r/\text{this}] : U + Δ'' \). By the premise of \( \text{Call} \),

\[
\Delta_3, r : C[S], x : U' + e[r/\text{this}] : U + \Delta_1, r : C[S]
\]

\[
Δ_2, r : C[S'], x : U' + \Delta_2, r : C[(T \ m(T') : S)]
\]

we can notice that \( Δ_2 \) and \( Δ_3 \) are such that either \( Δ_2 = Δ_3 \) with \( Δ_2(v) = Δ_3(v) = U' \) or \( Δ_2(v) = U'' \) and \( Δ_1 = Δ_3[v : U'/v : U''] \) By Lemma A.3 we have

\[
Δ_3, r : C[S'] + e[v/x][r/\text{this}] : U + Δ_1, r : C[S]
\]

Since \( S =_{\text{def}} S' \), we conclude by rule \( \text{Equiv} \). Recall that \( Δ_3, r : C[(T \ m(T') : S)] \vdash h \). By \( \text{Heap} \) we have

\[
h(r) = C[f : o] \quad Δ + C[f : o] : C[(T \ m(T') : S)] \vdash Δ_3, r : C[(T \ m(T') : S)] + h
\]

which by \( \text{Object} \) it means that

\[
\text{typestate}(C) = S_C \quad 3\exists, S_C \quad \leadsto \quad (T \ m(T') : S)
\]

\[
Δ + C[f : o] : C[(T \ m(T') : S)] \vdash Δ_3, r : C[(T \ m(T') : S)] + h
\]

We perform another reduction with label \( T \ m(T) \) and we have

\[
\text{typestate}(C) = S_C \quad 3\exists, S_C \quad \leadsto \quad (T \ m(T') : S) \quad \leadsto \quad T \ m(T)
\]

\[
Δ_3, r : C[S] + C[f : o] : C[S] \vdash Δ_3, r : C[S]
\]

We now can type \( Δ_3, r : C[S] + h \) by rule \( \text{Heap} \). We conclude by rule \( \text{Constr} \).

- \( e = v \cdot r \). By hypothesis and by rule \( \text{R-Value} \)

\[
h, v \cdot r \quad \leadsto \quad h, v
\]

for \( v \neq l \). By hypothesis and by rule \( \text{Constr} \ Δ \vdash h \) and \( Δ \vdash v \cdot r : U + Δ'' \). By inversion and typing rule \( \text{ArR} \)

\[
Δ + v : U + Δ''
\]

\[
Δ + v \cdot r : U + Δ''
\]

By reduction rule \( \text{Ty-In} \ Δ \quad \leadsto \quad Δ \). The thesis follows trivially.

- \( e = \text{switch} (l' \cdot r) \ \{ e \} \}_{E} \). By hypothesis and by rule \( \text{R-Switch} \)

\[
h, \text{switch} (l' \cdot r) \ \{ e \} \}_{E} \quad \leadsto \quad h, e_{l'}
\]

for some \( l' \in E \). By hypothesis and by rule \( \text{Constr} \ Δ \vdash h \) and \( Δ \vdash \text{switch} (l' \cdot r) \ \{ e \} \}_{E} : U + Δ'' \). By inversion and typing rule \( \text{Switch-ArR} \)

\[
\forall l \in E \quad Δ_3, r : C[S] + e_l : U_l + Δ'' \quad Δ + l' : E + Δ_3, r : C[(l : S_l)_{E}] \quad Δ_3 = \biguplus_{l \in E} Δ_l
\]

\[
Δ + \text{switch} (l' \cdot r) \ \{ e \} \}_{E} : \text{join}[(U_l)_{E}] + Δ''
\]
where $U = \text{join}([U]_{l: E})$. By inversion and typing rule $\text{Enum}$ we have that $\Delta = \Delta_1; r : C([I : S]_{l: E})$. By $\text{Tv-Label}$

$$\Delta_1; r : C([S]_{l: E}) \xrightarrow{(p)} \Delta_F, r : C[S]_F$$

where $l' \in E$ and $\Delta' \prec \Delta$. By Lemma A.4 we have that $U_r \prec \Delta \text{join}([U]_{l: E})$. The judgement $\Delta_F, r : C[S]_F \vdash e_r : U_r \vdash \Delta''$ holds by the premise of $\text{Switch}$ for $l' \in E$. We need to prove that $\Delta_F, r : C[S]_F \vdash h$. Recall that, by hypothesis $\Delta \vdash h$. By $\text{Heap}$ and $\text{Object}$ it means that there exist $\exists$, such that $\text{typestate}(C) = S_C$ and $S_C \xrightarrow{\exists} (l : [S]_{l: E})$ and

$$\Delta + C[f-o] : C([I : S]_{l: E}) + \Delta$$

By Definition 6.2, we have $(l : [S]_{l: E}) \xrightarrow{\exists} S_F$. By applying rule $\text{Object}$ on this reduction, we have

$$\Delta_F, r : C[S]_F \vdash C[f-o] : C[S]_F + \Delta_F, r : C[S]_F$$

We conclude by rules $\text{Heap}$ and $\text{Config}$.

- $e = \text{if}(tt) e_1 \text{else} e_2$. The case for $\text{if}(\text{if}) e_1 \text{else} e_2$ is completely analogous. By hypothesis and by rule $\text{R-True}$

$$h, \text{if}(tt) e_1 \text{else} e_2 \xrightarrow{\text{if}} h, e_1$$

By hypothesis and by rule $\text{Config} \vdash h$ and $\Delta \vdash \text{if}(tt) e_1 \text{else} e_2 : U \vdash \Delta''$. By inversion and typing rule $\text{If}$

$$\Delta_1 + e_1 : U_1 \vdash \Delta'' \quad \Delta_2 + e_2 : U_2 \vdash \Delta'' \quad \Delta_3 = \text{join}(\Delta_1, \Delta_2) \quad \Delta \vdash \text{tt} : \text{bool} \vdash \Delta_1$$

$$\Delta \vdash \text{if}(tt) e_1 \text{else} e_2 : \text{join}(U_1, U_2) + \Delta''$$

Where $U = \text{join}(U_1, U_2)$. Rule $\text{Box}$, implies that $\Delta = \Delta_1$. By $\text{Tv-If} \Delta \xrightarrow{\text{if}} \Delta'$ and $\Delta \prec \Delta$. By Lemma A.4 we have that $U_1 \prec \Delta \text{join}(U_1, U_2)$. Then, $\Delta_1 + e_1 : U_1 \vdash \Delta''$ follows directly by the premise of $\text{If}$ and by letting $\Delta' = \Delta_1$, since $\Delta_1 \prec \Delta \text{join}(\Delta_1, \Delta_2) = \Delta$. It remains to prove that $\Delta_1 \vdash h$. Since $\Delta_1 \prec \Delta$, the thesis follows trivially by applying $\text{Heap}$.

- $e = (\lambda : e')$. By hypothesis and by rule $\text{R-Label}$

$$h, \lambda : e' \xrightarrow{\text{r}} h, e'(\lambda : e'/\text{continue} \lambda)$$

By hypothesis and by rule $\text{Config} \vdash h$ and $\Delta \vdash \lambda : e' : U \vdash \Delta'$. By inversion and rule $\text{Expr}$ we get

$$\Delta'' + e' : U \vdash \Delta', \lambda : X$$

$$\Delta = \{ r : C[S] \mid r : C[S] \in \Delta'' \} \cup \{ r : U' \mid r : U' \in \Delta'' \text{ and } U' \not\in C[S'] \}$$

$$\Delta \vdash \lambda : e' : U \vdash \Delta'$$

By rule $\text{Tv-Label} \Delta \xrightarrow{\text{r}} \Delta$. Since $\Delta \vdash h$, it remains to prove that $\Delta \vdash e'(\lambda : e'/\text{continue} \lambda) : U \vdash \Delta'$. From the second case of the Substitution Lemma A.3 we get:

$$\Delta'' + e'(\lambda : e'/\text{continue} \lambda) : U \vdash \Delta'$$

with

$$\Delta'' = \{ r : C[S] \mid r : C[S] \in \Delta'' \text{ and } r : C[S] \in \Delta \} \cup \{ r : U' \mid r : U' \in \Delta'' \text{ and } U' \not\in C[S'] \}$$

From the definition of $\Delta''$ we can obtain that $\Delta'' = \Delta$ as required. We conclude by rule $\text{Config}$.

### B. StMungo for Multiparty Session Types

In this section we illustrate StMungo on a multiparty protocol that models the process of booking flights through a university travel agent.

There are three participants involved: Researcher (abbreviated $R$), who intends to travel; Agent ($A$), who is able to make travel reservations; and Finance ($F$), who approves expenditure from the budget. In the Scribbler language, we first define the global protocol among three roles, which are abstract representations of the participants. The protocol consists of sequences of interactions. Every message (e.g. request) can be associated with a payload type (e.g. Travel1), a sender, and one or more receivers. Typically payload types are structured data types defined separately from the protocol specification.

In the following global protocol, after the quote and the check message requesting authorisation for a trip, Finance can choose to approve or refuse the request:

```scirb
1 global protocol BuyTicket(role R, role A, role F){
2 request(Travel) from R to A;
3 quote(Price) from A to R;
4 check(Price) from R to F;
5 choice at F {
6 approve(Code) from F to R,A;
7 ticket(String) from A to R;
8 invoice(Code) from A to F;
9 payment(Price) from F to A;
10 } or {
11 refuse(String) from F to R,A; }
```
The Scribble toolchain can be used to check the protocol definition for well-formedness and to derive a local version of the protocol for each role, according to the theory of multiparty session types [25]. This is known as endpoint projection. Here we show the projection for Researcher, which describes only the messages involving that role. The self keyword indicates that R is the local endpoint.

```plaintext
local protocol BuyTicket_R(self R, role A, role F){
  request(Travel) to A;
  quote(Price) from A;
  check(Price) to F;
  choice at F {
    approve(Code) from F;
    ticket(String) from R;
  } or {
    refuse(String) from F; }}
```

Notice that the exchange of invoice and payment between Agent and Finance is not included. Similarly, the local projection for Agent omits the check message and the local projection for Finance omits the request, quote and ticket messages.

For the R role, StMungo converts the `BuyTicket_R` local projection into the following `.mungo` files:

1. `RProtocol`, capturing the interactions local to the R role as a typestate specification.
2. `RRole`, a class that implements `RProtocol` by communication over Java sockets. This is an API that can be used to implement the Researcher endpoint.
3. `RMain`, a skeletal implementation of the Researcher endpoint. This runs as a Java process, and provides a `main()` method which uses `RRole` to communicate with the other parties in the session.

The `RProtocol` definition generated by StMungo is as follows:

```plaintext
typestate RProtocol {
  State0 = {
    void send_requestTravelToA(Travel): State1 }
  State1 = {
    Price receive_quotePriceFromA(): State2 }
  State2 = {
    void send_checkPriceToF(Price): State3 }
  State3 = {
    Choice1 receive_Choice1LabelFromF():
      <APPROVE: State4, REFUSE: State6> }
  State4 = {
    Code receive_approveCodeFromF(): State5 }
  State5 = {
    String receive_ticketStringFromA(): end }
  State6 = {
    String receive_refuseTravelFromF(): end }}

class RRole typestate RProtocol {
  /* Constructor and method definitions. */}
```

The `RRole` class provides an implementation of `RProtocol` based on Java sockets. When instantiated, it connects to the other role objects in the session (`ARole` and `FRole`); we omit the details here.

Finally, `RMain` provides skeletal implementation of the Researcher endpoint, using the `RRole` class to communicate with the other roles in the system:

```plaintext
public static void main(String[] args) {
  RRole r = new RRole();
  Travel t = // input travel;
  r.send_requestTravelToA(t);
  Price p = r.receive_quotePriceFromA();
  r.send_checkPriceToF(p);
  switch(r.receive_Choice1LabelFromF().getEnum()) {
    case APPROVE:
      Code c = r.receive_approveCodeFromF();
      println(r.receive_ticketStringFromA());
      break;
    case REFUSE:
      println(r.receive_refuseStringFromF());
      break; }}
```

As we already stated for SMTP, typically the programmer would flesh out the skeletal implementation with extra business logic. Mungo is able to statically check `RMain`, or any client of the `RRole` class, to ensure that methods of the protocol are called in a valid sequence and that all possible responses are handled.
C. Type Inference Examples

C.1 Typestate Linearity

Consider the following code that uses the implementation of class Stack in section § 1:

```java
class StackUser {
    void pushN(Stack x) {
        x.push(2); x
    }

    Stack popAll(Stack) {
        return new Stack; k = s
    }

    Stack pushAll(Stack x) {
        x.push(x.isEmpty())
    }
}
```

Also assume input typing context $\Delta_0 = [s : Stack[end], k : Stack[S]]$. The inference tree for the above code is:

\[
\begin{array}{c}
\Delta_3 \vdash s = \text{new Stack}; k = s \quad \text{new}
\end{array}
\]

\[
\begin{array}{c}
\Delta_2 \vdash s : Stack[S], k : Stack[end] \\
\Delta_2 \vdash s : Stack[S] + \Delta_1 \\
\Delta_1 \vdash s : Stack[end], k : Stack[end] \\
\Delta_2 \vdash k = s : \text{void} + \Delta_0 \\
\Delta_3 \vdash s = \text{new Stack} : \text{void} + \Delta_2 \\
\end{array}
\]

C.2 Recursion and Choice

Consider a class StackUser that defines methods that use a Stack object:

```java
class StackUser {
    {(Stack pushN(Stack) : {Stack popAll(Stack):end})} {
        Stack pushN(Stack x) {
            x.push(2); x
        }

        Stack popAll(Stack x) {
            loop :
            switch(x.isEmpty()) {
                case TRUE: x
                case FALSE: x.pop(); continue loop
            }
        }
    }
}
```

Method Stack popAll(Stack): Consider the input typing context $\Delta_0 = x : Stack[end], this : StackUser[end]$ and e is the switch expression in the body of method Stack popAll(Stack). The inference tree for the body of method Stack popAll(Stack) is:

\[
\begin{array}{c}
\Delta_1 \vdash x : Stack[[int pop() : X]], this : StackUser[X] \\
\Delta_1 \vdash x.pop() : \text{int} + \Delta_1' \\
\Delta_1' \vdash x : Stack[X], this : StackUser[X] \\
\Delta_1' \vdash \text{continue} \ loop : \text{bot} + \Delta_0, \text{loop} : X \\
\Delta_1 \vdash x : Stack[S], this : StackUser[end], \text{loop} : X \\
\Delta_2 \vdash x : Stack[S] + \Delta_0, \text{loop} : X \\
\Delta_3 = x : Stack[[Choice isEmpty() : join(S, int pop() : X)], this : StackUser[join(end, X)]] \\
\Delta_1 \vdash x.isEmpty() : Choice + join(\Delta_1, \Delta_2) \quad \text{switch}
\end{array}
\]

\[
\begin{array}{c}
\Delta_3 \vdash e : Stack[S] + \Delta_0, \text{loop} : X \\
\Delta_4 = x : Stack[\mu X. Choice isNotEmpty() : join(S, int pop() : X)], this : StackUser[\mu X. join(end, X)] \\
\Delta_4 \vdash \text{loop} : e : Stack[S] + \Delta_0 \\
\Delta = x : Stack[\mu X. Choice isNotEmpty() : join(S, int pop() : X)], this : StackUser[end] \\
\Delta \vdash \text{loop} : e : Stack[S] + \Delta_0 \quad \text{equiv}
\end{array}
\]
The inference tree for class StackUser is:

```
Method Stack pushN(Stack): Assume a typing context $\Delta_0 = x: \text{Stack}[\text{end}]$, this : StackUser[[Stack popAll(Stack) : end]] The inference tree for method Stack pushN(Stack) is:

```

C.3 Method Call

Consider the code

```
with input context $\Delta_0 = s : \text{Stack}[\text{end}]$, c : StackUser[[Stack popAll(Stack) : end]]. The derivation tree for the above code is:

```

C.4 Class inference

The inference tree for class StackUser is:

```

Method Call

Consider the code

```

with input context $\Delta_0 = s : \text{Stack}[\text{end}]$, c : StackUser[[Stack popAll(Stack) : end]]. The derivation tree for the above code is: