Model-View-Update-Communicate: Session Types meet the Elm Architecture

Simon Fowler
University of Edinburgh, Scotland
simon.fowler@ed.ac.uk

Abstract
Session types are a type discipline for communication channel endpoints which allow conformance to protocols to be checked statically. Safely implementing session types requires linearity, usually in the form of a linear type system. Unfortunately, linear typing is difficult to integrate with graphical user interfaces (GUIs), and to date most programs using session types are command line applications.

In this paper, we propose the first principled integration of session typing and GUI development by building upon the Model-View-Update (MVU) architecture, pioneered by the Elm programming language. We introduce \( \lambda_{\text{MVU}} \), the first formal model of the MVU architecture, and prove it sound. By extending \( \lambda_{\text{MVU}} \) with commands as found in Elm, along with linearity and model transitions, we show the first formal integration of session typing and GUI programming. We implement our approach in the Links web programming language, and show examples including a two-factor authentication workflow and multi-room chat server.

2012 ACM Subject Classification Software and its engineering—Concurrent programming languages

Keywords and phrases Session types, concurrent programming, Model-View-Update

Digital Object Identifier 10.4230/LIPIcs...

Related Version An extended version of the paper is available on arXiv [23].

Funding This work was supported by ERC Consolidator Grant Skye (grant no. 682315) and an ISCF Metrology Fellowship grant provided by the UK government’s Department for Business, Energy and Industrial Strategy (BEIS).

Acknowledgements I thank Jake Browning for sparking my interest in Elm and for his help with an early prototype of the Links MVU library; Sára Decova for a previous version of the multi-room chat server example; Sam Lindley for many useful discussions and suggestions; and James Cheney, April Gonçalves, and the anonymous reviewers for detailed comments. Finally, I think James McKinna for the pack of Jelly Babies when I received disappointing reviews for a previous draft.

1 Introduction

Modern applications are necessarily concurrent and distributed. Along with concurrency and distribution naturally comes communication, but communication protocols are typically informally described, resulting in costly runtime failures and code maintainability issues.

Session types [28, 29] are a type discipline for communication channel endpoints which allow conformance to a protocol to checked statically rather than after an application is deployed. Many distributed GUI applications, such as chat applications or multiplayer games, would benefit from session-typed communication with a server. Unfortunately, safely implementing session types requires a require a linear type system, but safely integrating linear resources and GUIs is nontrivial. As a consequence, to date most programs using session types are batch-style applications run on the command line.

The lack of a principled integration of GUI applications and session types is a significant barrier to their adoption. In this paper, we bridge this gap by extending the Model-View-Update (MVU) architecture, pioneered by the Elm programming language, to support linear...
resources. We present \(\lambda_{MVU}\), a core formalism of the MVU architecture, and an extended version of \(\lambda_{MVU}\) which supports session-typed communication. Informed by the formal development, we provide a practical implementation in the Links programming language [11].

**Session types by example.** Let us consider a two-factor authentication workflow, introduced by Fowler et al. [25]. A user first enters their credentials. If correct, the server can then either grant access, or send a challenge key. If challenged, the user enters the challenge code into a hardware token, which generates a response to be entered into the web page. The server then either authenticates the user or denies access.

We can describe the two-factor authentication example as a session type as follows:

\[
\text{TwoFactorServer} \triangleq
twoFactorServer
\]

\[
\text{TwoFactorClient} \triangleq
twoFactorClient
\]

The `TwoFactorServer` type shows the session type for the server, which firstly receives (\(\ell_0?\)) the credentials from the client, and then chooses \((\oplus)\) whether to authenticate, deny access, or issue a challenge. If the server issues a challenge, it sends (\(\ell_1!\)) the challenge string, awaits the response, and then chooses whether to accept or reject the request. The `ServerBody` type abstracts over the actions performed in the remainder of the application, for example taking out a loan. The `TwoFactorClient` type is the dual of the `TwoFactorServer` type: where the server sends, the client receives, and where the client sends, the server receives. The `&` construct denotes offering a choice of branches. Suppose we have constructs for sending along, receiving from, and closing an endpoint:

\[
\begin{align*}
\text{send} &: (A \times !A.S) \rightarrow S \\
\text{receive} &: ?A.S \rightarrow (A \times S) \\
\text{close} &: \text{End} \rightarrow 1
\end{align*}
\]

Let us also suppose we have constructs for selecting and offering a choice:

\[
\begin{align*}
\text{select} &: \ell_i.M : S_j \\
\text{offer} &: \{\ell_i(x_i) \rightarrow N_i\}_{i \in I} : A
\end{align*}
\]

where \(M\) has session type \(\oplus\{\ell_i : S_i\}_{i \in I}\), and \(j \in I\) where \(M\) has session type \&\{\ell_i : S_i\}_{i \in I}\), each \(x_i\) binds an endpoint with session type \(S_i\), and each \(N_i\) has type \(A\)

We can write a server implementation as follows:

```plaintext
twoFactorServer : TwoFactorServer \rightarrow 1
twoFactorServer(s) \triangleq
  let ((username, password), s) = receive s in
  if checkDetails(username, password) then
    let s = select Authenticated s in serverBody(s)
  else let s = select AccessDenied s in close s
```

To implement session-typed communication safely, we require a linear type system [50] to ensure each communication endpoint is used exactly once: as an example, without linearity it would be possible to attempt to receive the credentials twice.

**Linearity and GUIs.** We can also write a client application:

```plaintext
twoFactorClient : (Username \times Password \times TwoFactorClient) \rightarrow 1
twoFactorClient(username, password, s) \triangleq
  let s = send ((username, password), s) in
  offer s (Authenticated(s) \rightarrow clientBody(s))
    Challenge(s) \rightarrow let (key, s) = receive s in
    let s = send (generateResponse(key), s) in
    offer s (Authenticated(s) \rightarrow clientBody(s))
    AccessDenied(s) \rightarrow close s; loginFailed

AccessDenied(s) \rightarrow close s; loginFailed
```
However, such a client is of little use, as it sends only a pre-defined set of credentials, and the step where a user enters the response to the challenge is replaced by a function \texttt{generateResponse}. Ideally, we would like the credentials to be entered into a GUI, and for a button press to trigger the session communication with the server.

Let us attempt to write a GUI for the first stage of the two-factor authentication example; as HTML is well-understood, we concentrate on web pages in the remainder of the paper.

```html
render(c) \triangleq
<html>
  <body>
    <input id="username"></input>
    <input id="password"></input>
    <button onClick=login(c)>Submit</button>
  </body>
</html>
```

Given a channel \( c \) of type \texttt{TwoFactorClient}, the \texttt{render} function generates a web page with input boxes for the username and password, and a button to submit the credentials. The \texttt{login} function, triggered when the button is clicked, retrieves the username and password from the two input boxes, and sends the credentials along \( c \). The \texttt{handleResponse} function, which we omit, receives the response from the server and updates the web page.

On first inspection, this implementation seems sound since the endpoint \( c \) is used linearly. However, the above attempt is unsound due to the asynchronous nature of GUI programming: there is nothing stopping the user pressing the button twice and sending the credentials twice along \( c \), in contravention of the session type. As a further complication, suppose we augmented the protocol with a “forgotten password” branch, triggered by another button. This would require two instances of \( c \) in the GUI, again violating linearity:

```html
<button onClick=login(c)>Submit</button>
<button onClick=reset(c)>Reset password</button>
```

It is clear that directly embedding linear resources into a GUI is a non-starter. A more successful approach involves spawning a separate process which contains the linear resource, and which receives \textit{non-linear} messages from the GUI. Upon receiving a GUI message, the process can then perform the session communication, while ignoring duplicate GUI messages:

```latex
\begin{align*}
  \texttt{render}(c) & \triangleq \\
  \texttt{let pid = spawn handler(c) in} \\
  \begin{html}
    \begin{body}
      \begin{input id="username"></input>
      \begin{input id="password"></input>
      \begin{button onClick=login(pid)}>Submit</button>
    \end{body}
  \end{html}
  \\
  \texttt{login(pid) \triangleq \lambda().} \\
  \texttt{let user = getContents("username") in} \\
  \texttt{let pass = getContents("password") in} \\
  \texttt{pid! SubmitLogin(user, pass)} \\
  \texttt{handler(c) \triangleq} \\
  \texttt{case (get ()) \{} \\
  \texttt{SubmitLogin(user, pass) \rightarrow} \\
  \texttt{let c = send ((user, pass), c) in} \\
  \texttt{handleResponse(c)} \\
  \texttt{\}} \\
\end{align*}
```

The \texttt{render} function begins by spawning \texttt{handler(c)} as a separate process with an incoming message queue (or \textit{mailbox}), returning the process ID \texttt{pid}. As before, the \texttt{login} function is triggered by pressing the button, and retrieves the credentials from the web page. Instead of communicating on the channel directly, it sends a \texttt{SubmitLogin} message containing the credentials to the process ID of handler process, written \texttt{pid! SubmitLogin(user, pass)}. The handler process retrieves the message from its mailbox \texttt{(get ())}, and can then communicate with the server over the linear endpoint. Such an approach also scales to the “forgotten password” extension, by adding another GUI message.

The above approach is used by Fowler et al. [25], who provide the first integration of session types and web application development, including the ability to gracefully handle failures such as the user closing their browser mid-session. Unfortunately, the approach is
brittle and ad-hoc. All interaction with the web page occurs using imperative operations such as `getContents` and `setContents`; contrary to best practices such as the Model-View-Controller (MVC) [35] pattern, the state of the web page is not derived directly from the data contained by the application. Furthermore, there is no connection between the state of the handler process and what is displayed on the web page: this can easily lead to mismatches between the possible GUI messages which can be sent and which can be handled.

**Model-View-Update.** This paper is about doing better. Our approach is to formalise Model-View-Update, an architectural pattern for GUI development popularised by the Elm programming language [1], and extend it to support linear resources. MVU is an appealing starting point as it is particularly suited to functional programming. Furthermore, MVU has directly inspired popular technologies such as Redux [5] and the Flux architecture [4], which are used with the popular React [2] frontend web framework for JavaScript.

> The Elm programming language [1] is a functional programming language designed for writing web applications. Elm was originally designed to use functional reactive programming (FRP) [17], where time-varying *signals* can be used to construct reactive web applications. A paper describing Elm, and its core formal semantics, was published at PLDI 2013 [14].

For many languages, that would be the end of the story. But unusually for a research language, Elm gained a user community, and a standard architectural pattern known as The Elm Architecture grew organically to such a point that Elm abandoned FRP altogether [13]. At its core, The Elm Architecture is a descendant of MVC where a *model* contains the state of the application; a *view function* renders the model; and the rendered model produces *messages* which are handled by an *update* function to produce a new model. More generally, this pattern has been referred to as Model-View-Update, or MVU for short [3, 46].

Consider the following web application, where a user enters text into a text box, and the application displays the text, reversed:

```
model ≜ (contents = "")
update ≜ λ(UpdateBox(str), m).(contents = str)
view ≜ λmodel.html
  <input type = "text" value = {model.contents}
  onInput = {λstr. UpdateBox(str)}> <input>
  <div>
    {htmlText(reverseString model.contents))}
  </div>
```

We define two type aliases: the *Model* captures the state of the application and is defined as a record with a single *String* field, *contents*. *Messages* are produced as a result of user interaction. The *Message* type is defined as a singleton variant type with constructor `UpdateBox`, containing the updated value of the text box.

The *view* function renders a model. It has the type `Model → Html(Message)`, which is a function taking a *Model* as its argument, and returning HTML which may produce messages of type *Message*. The value = `{model.contents}` attribute of the input box states that the contents of the text box should reflect the *contents* field of the model. The onInput attribute is an *event handler*: its body is a function taking the current value of the input box (str) and producing an `UpdateBox` message containing the updated contents of the box. The contents of the div tag are derived from the reversed contents.

The *update* function takes a message and previous model as its arguments, and produces a new model. In this case, the *update* function constructs a new model where the *contents* field
Figure 1 Syntax and typing rules for $\lambda_{MVU}$ terms

is set to the payload of the UpdateBox message. Finally, the program is a 3-tuple containing the initial model, and the view and update functions.

To achieve our goal of a formal integration of session typing and GUI programming, we must first formalise MVU, and then generalise the architecture to support linear models and messages. Supporting linearity poses some challenges, as we will see in §3.

1.1 Contributions.

The overarching contribution of this paper is the first principled integration of session-typed communication with a GUI framework. Concretely, we make three contributions:
1. We introduce the first formal model of the MVU architecture, $\lambda_{MVU}$ (§2). We prove (§2.3) that $\lambda_{MVU}$ satisfies preservation and event progress properties.
2. We extend $\lambda_{MVU}$ with commands, linearity, and model transitions (§3), which allow $\lambda_{MVU}$ to support GUIs incorporating session-typed communication, and we prove the soundness of the extended calculus.
3. We implement the architecture in the Links web programming language. We show an extended example of a chat application where client code uses the linear MVU framework, and where client-server communication happens over session-typed channels (§4).

The implementation is available as an artifact [22].

2 Model-View-Update, Formally

In this section, we formalise MVU as a core calculus, $\lambda_{MVU}$, an extension of the simply-typed $\lambda$-calculus with products, sums, HTML, and event handling. Even without extensions, $\lambda_{MVU}$ is expressive enough to support many common applications such as form handling.
### 2.1 Syntax

**Types.** Figure 1 shows the syntax and typing rules for $\lambda_{MVU}$. Types are ranged over by $A, B, C$, and consist of the unit type $\mathbf{1}$, functions $A \to B$, products $A \times B$, sums $A + B$, and string and integer types. Types $\text{Html}(A)$ and $\text{Attr}(A)$ are the type of HTML elements and attributes which can produce messages of type $A$.

**Terms.** Terms, ranged over by $L, M, N$, include variables, $\lambda$ abstractions, anonymous recursive functions, function application, the unit value, string literals, integers, and sum and pair introduction and elimination. The remaining terms encode HTML elements and attributes. The $\text{htmlTag} t M N$ construct denotes an HTML element with tag name $t$ (for example, $\text{div}$), attributes $M$, and children $N$; the $\text{htmlText} M$ construct describes a text node with text $M$; and $\text{htmlEmpty}$ defines an empty HTML node.

The $\text{attr} a k M$ construct describes an attribute with key $ak$ and body $M$, where the key $ak$ is either an attribute name $at$ or an event handler name $h$. The $\text{attrEmpty}$ construct defines an empty attribute.

The $M \star N$ operator appends two HTML elements or attributes. Since both HTML elements and attributes support a unit element ($\text{htmlEmpty}$ and $\text{attrEmpty}$ respectively), elements and attributes together with $\star$ form two monoids.

**Events.** We model interaction with the Document Object Model (DOM) through events, which model those dispatched by a browser. An event signature is a 3-tuple $(ev, h, A)$ consisting of an event name $ev$, handler name $h$, and payload type $A$. We require a bijective mapping between event and handler names. Figure 2 describes example event signatures used in the remainder of the paper. We consider four primitive events: click, which is fired when an element is clicked; input, which is fired when the contents of a text field are changed; and keyUp and keyDown, which are fired when a key is pressed while focused on an element.

Event handlers are attached to elements as attributes, and generate a message in response to an event. We write $\text{handler}(ev)$ to refer to the handler for $ev$: for example, $\text{handler}(\text{click}) = \text{onClick}$. We write $\text{ty}(ev)$ to refer to the payload type of $ev$ and write $\text{ty}(h)$ for the payload type of an event handled by $h$. As an example, both $\text{ty}(\text{click}) = \mathbf{1}$ and $\text{ty}(\text{onClick}) = \mathbf{1}$.

**Term typing.** Term typing rules for $\lambda$-calculus constructs are standard, so are omitted. Rule $T\text{-htmlTag}$ states that $\text{htmlTag} t M N$ can be given type $\text{Html}(A)$ if its attributes $M$ have type $\text{Attr}(A)$ and children have type $\text{Html}(A)$. Text nodes $\text{htmlText} M$ do not produce any messages, and so have type $\text{Html}(A)$ if $M$ has type $\text{String}$ ($T\text{-htmlText}$); similarly, $\text{htmlEmpty}$ has type $\text{Html}(A)$ ($T\text{-htmlEmpty}$).

Rule $T\text{-attr}$ assigns attributes $\text{attr} a M$ type $\text{Attr}(A)$ for any $A$ if $M$ has type $\text{String}$. Rule $T\text{-evtattr}$ types event handler attributes $\text{attr} a h M$: if the event handler $h$ has type $\text{ty}(h) \to A$ (i.e., it produces messages of type $A$), then the attribute can be given type $\text{Attr}(A)$. Finally, $T\text{-attrempty}$ states that the empty attribute $\text{attrEmpty}$ has type $\text{Attr}(A)$ for any type $A$. We overload the $\star$ operator to append both HTML elements and attributes ($T\text{-htmlappend}$ and $T\text{-attrappend}$).

<table>
<thead>
<tr>
<th>Event name</th>
<th>Event Handler</th>
<th>Payload type</th>
<th>Payload Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>click</td>
<td>onClick</td>
<td>$\mathbf{1}$</td>
<td>Unit value</td>
</tr>
<tr>
<td>input</td>
<td>onInput</td>
<td>String</td>
<td>Updated contents of a text field</td>
</tr>
<tr>
<td>keyDown</td>
<td>onKeyUp</td>
<td>Int</td>
<td>Key code</td>
</tr>
<tr>
<td>keyUp</td>
<td>onKeyUp</td>
<td>Int</td>
<td>Key code</td>
</tr>
</tbody>
</table>

**Figure 2** Example event signatures
Values
\[ U, V, W ::= \lambda x. M \mid \text{rec } f(x). M \mid () \mid (V, W) \mid \text{inl } V \mid \text{inr } V \mid \epsilon \mid n \]

Events
\[ e ::= \text{ev}(V) \]

DOM Pages
\[ D ::= \text{domTag}(\vec{e}) t V D \mid \text{domText } V \mid \text{domEmpty} \mid D \ast D' \]

Active thread
\[ T ::= \text{idle } V_m \mid M \]

Function state
\[ F ::= (V_v, V_u) \]

Processes
\[ P, Q ::= \text{run } M \mid (T \mid F) \mid ((M)) \mid P \parallel Q \]

Configurations
\[ C ::= P \parallel D \]

Process contexts
\[ P ::= [ ] \mid P \parallel P \]

DOM contexts
\[ D ::= [ ] \mid \text{domTag}(\vec{e}) t V D \mid D \ast D \mid D \ast D \]

Thread contexts
\[ T ::= \text{run } E \mid (E \mid F) \mid ((E)) \]

Figure 3 Runtime syntax for $\lambda_{MVU}$

**Syntactic sugar.** We assume the usual encodings of records as pairs and variant types as binary sums, and use pattern matching notation. It is useful to be able to write HTML using XML-like notation, where an antiquoted expression \{M\} allows a term $M$ to be embedded within an HTML tree. The view function from the introduction desugars to:

\[
\lambda \text{model.} \\
\quad (\text{htmlTag input} \\
\quad \quad ((\text{attr type "text"}) \ast (\text{attr value model.contents})\ast \\
\quad \quad (\text{attr onInput (Astr.UpdateBox (str)))\ast \text{htmlEmpty}) \ast \\
\quad \quad \text{htmlTag div attrEmpty (htmlText reverseString (model.contents)))})
\]

The formal definitions and desugaring translations are unsurprising; the details can be found in the extended version [23].

2.2 Operational Semantics

We can now provide $\lambda_{MVU}$ with a small-step operational semantics.

2.2.1 Runtime Syntax

Figure 3 describes the runtime syntax of $\lambda_{MVU}$. Values, ranged over by $U, V, W$, are standard. An event $\text{ev}(V)$ consists of event name $\text{ev}$ and payload $V$. We write $\epsilon$ for an empty meta-level sequence, and use $\cdot$ for sequence concatenation. DOM pages, ranged over by $D$, are the runtime representation of HTML, where tags $\text{domTag}(\vec{e}) t V D$ contain an event queue $\vec{e}$ of events dispatched to the element.

**Concurrency.** Concurrency is vital when modelling GUI applications as event handling is asynchronous: computation triggered by a user interaction should not block the UI. Concurrency is also essential when considering session-typed communication. We therefore formulate the calculus as a concurrent $\lambda$-calculus in the style of Niehren et al. [42], by augmenting the simply-typed $\lambda$-calculus with processes and concurrent reduction.

**Processes.** An initialisation process $\text{run } M$ evaluates the initial system state written by a user, where $M$ is a 3-tuple containing the initial model, view function, and update function. An event loop process $(T \mid F)$ consists of an active thread $T$ and function state $F$ comprising the view and update functions. The thread can either be $\text{idle } V_m$, meaning the process has current model $V_m$ and is waiting for another message to process, or evaluating a term $M$. An event handler process $((M))$ is spawned to generate a message in response to an event.
Meta-level definitions

\[
\begin{align*}
\text{handle}(m, (v, u, msg)) & \triangleq \text{handlers}(v, \text{attrEmpty}) = \epsilon \\
& \quad \text{handlers}(v, V \cdot W) = \text{handlers}(ev, V) \cdot \text{handlers}(ev, W) \\
& \quad \text{handlers}(ev, \text{attr at } V) = \epsilon \\
& \quad \text{handlers}(ev, \text{attr } h V) = \begin{cases} 
V & \text{if handler}(ev) = h \\
\epsilon & \text{otherwise}
\end{cases}
\end{align*}
\]

Process reduction

\[
\begin{align*}
P \longrightarrow P'
\end{align*}
\]

Configuration reduction

\[
\begin{align*}
\text{E-Run} & \quad P[\text{run}(V_m, V_v, V_u)] D \longrightarrow P[\text{run}(V_m, V_v, V_u)] D \\
\text{E-Update} & \quad P[(V_m, U | F)] D \longrightarrow P[(\text{idle } V_m | F)] D' \quad \text{where diff}(U, D) = D' \\
\text{E-Interact} & \quad P \triangleright D[\text{domTag}(\overrightarrow{V}) \ t U D] \longrightarrow P \triangleright D[\text{domTag}(\overrightarrow{V} \cdot \text{ev}(V)) \ t U D] \\
& \quad \text{for some } ev, V \text{ such that } \vdash \text{ev}(V) \\
\text{E-Ent} & \quad P \triangleright D[\text{domTag}(\text{ev}(W) \cdot \overrightarrow{V}) \ t U D] \longrightarrow P \parallel (V_1 W) \parallel \cdots \parallel (V_n W) \parallel D[\text{domTag}(\overrightarrow{V}) \ t U D] \\
& \quad \text{where } \text{handlers}(ev, U) = \overrightarrow{V} \\
\text{E-Struct} & \quad C \longrightarrow C' \quad \text{if } C \equiv C_1, C_1 \longrightarrow C_2, \text{ and } C_2 \equiv C' \\
\text{E-LiftP} & \quad P \triangleright D \longrightarrow P' \triangleright D \quad \text{if } P \longrightarrow P'
\end{align*}
\]

Figure 4 Reduction rules for \(\lambda_{\text{MVU}}\) terms and configurations

Configurations. Concurrent and event-driven reduction happens in the context of a system configuration \(P \triangleright D\), where \(P\) is the concurrent fragment of the system and \(D\) is the current DOM page. An MVU program as written by a user is a term \(M\) specifying the initial model, view function, and update function, of type \((A \times (A \rightarrow \text{Html}(B))) \times ((B \times A) \rightarrow A)\). A program is evaluated in the context of an initial configuration:

Definition 1 (Initial configuration). An initial configuration for a term \(M\) is of the form run \(M \triangleright \text{domEmpty}\).

Evaluation contexts. Term evaluation contexts \(E\) (omitted) are set up for call-by-value, left-to-right evaluation. Process contexts \(P\) allow reduction under parallel composition. Thread contexts \(T\) allow reduction inside threads. DOM contexts \(D\) allow us to focus on each element of a DOM forest; note that they deliberately allow non-unique decomposition in order to support nondeterministic reduction.

2.2.2 Reduction Rules

Figure 4 shows the reduction rules for \(\lambda_{\text{MVU}}\) processes and configurations; reduction on terms is standard \(\beta\)-reduction. Reduction on configurations is defined modulo the associativity and commutativity of parallel composition.

Differing. As DOM pages include event queues, they contain strictly more information than HTML. To avoid losing pending events, we require a differencing operation. Define \(\text{erase}(D)\) as the operation \(\text{erase}(\text{domTag}(\overrightarrow{V}) \ t U D) = \text{htmlTag} \ t U (\text{erase}(D))\), with the other cases defined recursively. DOM pages can be modified by adding a node with an empty queue, removing a node, or updating a node’s attributes. We define operation \(\text{diff}(U, D) = D'\) if \(\text{erase}(D') = U\), and \(D'\) is obtained from \(D\) by the minimum number of insertions and deletions.

Semantics by example. Let us return to our original example from §1: a box and a text node displaying the reversed box contents. We reuse the view and update functions and let \(V_m =
(contents = ""), V0 = view, and Vu = update. We extend the HTML syntactic sugar to pages, letting [−→] be a desugaring function and \([\langle t \rightarrow a @ e \rangle \rightarrow D_H] = domTag(a) t [\a] [D_H].\]

We write \(\mathcal{R}^+\) for the transitive closure of a relation \(\mathcal{R}\). We begin by supplying the model, view, and update parameters to an initial configuration. By E-RUN, we get an event loop process, and then term \(V_0 V_{m} \) reduces to the initial rendered HTML. By diffing against the empty page, we display the initial DOM page (E-UPDATE).

\[
\text{run} (V_m, V_v, V_u) : \text{domEmpty} \\
\rightarrow (\text{E-RUN}) \quad \langle (V_m, V_v, V_u) \rangle (V_v, V_u) : \text{domEmpty} \\
\rightarrow^+ (\text{E-INTERACT}) \quad \langle \text{idle} V_m | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ \text{click}() \cdot \text{keyDown}(T5) \cdot \text{keyUp}(T5) \cdot \text{input}("k") \langle /input > \langle div @ e > \langle /div > \\
\rightarrow^+ (\text{E-EVT}) \quad \langle \text{idle} V_m | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ input("k") \langle /input > \langle div @ e > \langle /div > \\
\rightarrow (\text{E-EVT}) \quad \langle \text{idle} V_m | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ e \langle /input > \langle div @ e > \langle /div > \\
\]

The system now does not reduce until a user interacts with the text box and presses the \(k\) key, modelled by E-INTERACT. At this point, the event queue for the input box receives four events: click, keyDown, keyUp, and input, which are processed by rule E-EVT. The input element does not have handlers for the click, keyDown, and keyUp events, so no processes are spawned, but \(does\) contain an onInput handler, which handles the input event by spawning (UpdateBox("k")).

\[
\rightarrow^+ (\text{E-INTERACT}) \quad \langle \text{idle} V_m | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ \text{click}() \cdot \text{keyDown}(T5) \cdot \text{keyUp}(T5) \cdot \text{input}("k") \langle /input > \langle div @ e > \langle /div > \\
\rightarrow^+ (\text{E-EVT}) \quad \langle \text{idle} V_m | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ input("k") \langle /input > \langle div @ e > \langle /div > \\
\rightarrow (\text{E-EVT}) \quad \langle \text{idle} V_m | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ e \langle /input > \langle div @ e > \langle /div > \\
\]

Since UpdateBox("k") is already a value and the event loop process is idle, we can process the message (E-HANDLE). The handle meta-function calculates a new model \(m'\) by applying the update function to a pair of the previous model and the message, calculates a new HTML value \(v'\) by applying the view function to \(m'\), and returns the pair \((m', v')\). Finally, the page is diffed against the previous DOM page to generate a new DOM page \(D'\), and the event loop process reverts to being idle:

\[
\rightarrow (\text{EP-HANDLE}) \quad \langle \text{handle}(V_m, (V_v, V_u), \text{UpdateBox("k")}) | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ e \langle /input > \langle div @ e > \langle /div > \\
\rightarrow^+ (\text{contents = "k")} \quad \langle \text{idle} (\text{contents = "k") | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ e \langle /input > \langle div @ e > \langle /div > \\
\rightarrow (\text{E-UPDATE}) \quad \langle \text{idle} (\text{contents = "k") | (V_v, V_u) \rangle : \text{onInput} = \{\lambda str:UpdateBox(str)\} @ e \langle /input > \langle div @ e > \langle /div > \\
\]


We can now prove that well-typed if process has type $A$ and message type $B$. An idle thread $\text{idle} V_m$ has type $\text{EvtLoop}(A, B)$ if $V_m$ has type $A$ (TS-IDLE). An active thread $M$ currently processing a message has type $\text{EvtLoop}(A, B)$ if $M$ has type $(A \times \text{Html}(B))$, i.e., computes a pair of a new model with type $A$ and HTML which produces messages of type $B$ (TS-PRESEvation).

Judgement $\vdash \phi$ states that process $P$ is well typed and produces or consumes messages of type $A$. The parallel composition of two processes $P_1 \parallel P_2$ has message type $A$ if both $P_1$ and $P_2$ have message type $A$ (TP-PAR). An event handler process $(\langle M \rangle)$ has message type $A$ if term $M$ has type $A$ (TP-THREAD).

An initialisation process $\text{run} M$ is well-typed if $M$ is a product type where each component has the correct model, view, and update types. An event loop process $(T \mid (V_e, V_i))$ has message type $B$ if its active thread $T$ has model type $A$ and message type $B$; its view function $V_e$ has type $A \rightarrow \text{Html}(B)$; and its update function has type $(B \times A) \rightarrow A$ (TP-EVENTLoop).

Thread flags $\phi$ ensure that there is precisely one initialisation process or event loop process in a process typeable under flag $\bullet$.

Judgement $\vdash C$ states that configuration $C$ is well-typed: a system configuration $P \vdash D$ is well-typed if process $P$ has precisely one event loop process with message type $A$ and page $D$ has type $\text{Page}(A)$. The omitted typing rules for pages (of shape $\vdash D : \text{Page}(A)$) are similar to those for terms of type $\text{Html}(A)$.

Note that we consider only closed configurations and processes since it makes little sense for DOM pages $D$ to contain free variables, and because processes do not bind variables.

We are now well-placed to state some formal results. We omit proofs in the main body of the paper; full proofs can be found in the extended version [23].

**Preservation.** Reduction preserves typing.
Theorem 2 (Preservation). If $\vdash C$ and $C \rightarrow C'$, then $\vdash C'$.

Progress. The system vacuously satisfies a progress property as it can always reduce by E-INTERACT due to user input. It is more interesting to consider the event progress property enjoyed by the system without E-INTERACT: either there are no events to process and the system is idle, or the system can reduce. Functional reduction satisfies progress.

Lemma 3 (Progress (Terms)). If $\cdot \vdash M : A$, then either $M$ is a value, or there exists some $N$ such that $M \rightarrow E M N$.

Let $\rightarrow_E$ be the relation $\rightarrow$ without rule E-INTERACT. The concurrent fragment of the language will reduce until all event handler threads have finished evaluating, and there are no more messages to process. By appeal to Lemma 3, we can show event progress.

Theorem 4 (Event Progress). If $\vdash C$, either:
1. there exists some $C'$ such that $C \rightarrow_E C'$; or
2. $C = (idle V_m | (V_v, V_u)) \vdash D$ where $D$ cannot be written $D[\text{domTag}(\overline{e})] t V W$ for some non-empty $\overline{e}$.

3. $\lambda_{MVU}$ with Session Types

In this section, we extend $\lambda_{MVU}$ to support session types. We require three extensions: commands, to perform side-effects; linearity, to implement session types safely; and transitions, to allow multiple model and message types. We begin by showing each extension by example, and show the extended formalism in §3.4.

3.1 Commands

Real-world applications require side-effects. To this end, Elm supports commands which describe side-effects to be performed in the event loop. Although commands in Elm are more general, for our purposes, it is particularly useful to be able to spawn a process which will run concurrently and eventually return a message. As an example, we may want to await the result of an expensive computation, and display the result when the computation completes. Letting $\text{naiveFib}(x)$ be the naïve Fibonacci function and assuming an $\text{intToString}$ function, we can write:

```haskell
Model ≜ Maybe(Int)  Message ≜ StartComputation | Result(Int)
view = \lambda model.html
   <html>
   <body>
     (case model { 
      Just(result) → htmlText intToString(result); 
      Nothing → htmlText "waiting ..." } )
   </body>
   <html>

update : (Message × Model) → (Model, Cmd(Message))
update = \lambda (message, model).
   case message { 
    StartComputation → (Nothing, cmdSpawn Result(\text{naiveFib}(1000)))
    Result(x) → (Just(x), cmdEmpty)
   }
```

The model is of type $\text{Maybe}(\text{Int})$, with value $\text{Just}(V)$ for some integer value $V$ if the result has been computed, or $\text{Nothing}$ if the application is awaiting the result. The Message type is
a variant type consisting of \texttt{StartComputation} which is sent to start the computation, and \texttt{Result(Int)}, which is sent to return a result. The \texttt{view} function renders either the result, or “waiting…” if no result is available.

The type of the \texttt{update} function is changed to return a \textit{pair} of an updated model and a command. In our case, the \texttt{StartComputation} message results in a pair of \texttt{Nothing} and \texttt{cmdSpawn Result(naiveFib(1000))}, which spawns \texttt{Result(naiveFib(1000))} to evaluate in a separate thread. When the function (eventually) completes, the thread will have evaluated to a \texttt{Result} message, which can be processed by the \texttt{update} function to update the model and display the result.

### 3.2 Linearity

As we showed in §1, safely implementing session types requires linearity: we therefore require linear model and message types. Linearity would also prove useful for other linear resources such as functional arrays with in-place update [50]. Unfortunately, $\lambda_{MVU}$ as defined so far does not support linearity. Consider \texttt{handle}:

\[
\texttt{handle}(m, (v, u), \texttt{msg}) \triangleq \texttt{let } m' = u(\texttt{msg}, m) \texttt{ in } (m', v m')
\]

The updated model, $m'$, is used non-linearly as it is returned for use in subsequent requests, and also used to render the model as HTML.

**Extraction.** Linear resources are needed only when updating the model—not when rendering the webpage—as we will not need to communicate on session channels when rendering. If the developer implements a function:

\[
\texttt{extract} : A \rightarrow (A \times B)
\]

where $A$ is the type of a model, and $B$ is the \textit{unrestricted} fragment of the model, we can restore linear usage of the model (letting $e$ be the extraction function):

\[
\texttt{handle}(m, (v, u, e), \texttt{msg}) \triangleq \texttt{let } m' = u(\texttt{msg}, m) \texttt{ in } (m', v m')
\]

An alternative approach would be to assign the view function type $A \rightarrow (A \times \texttt{Html}(B))$, returning the linear model and allowing it to be re-bound. We would need to modify \texttt{handle}:

\[
\texttt{handle}(m, (v, u), \texttt{msg}) \triangleq \texttt{let } m' = u(\texttt{m}, \texttt{msg}) \texttt{ in } v m'
\]

A key disadvantage of this approach is that rendering is no longer a read-only operation, breaking an important abstraction barrier.

**Example.** We can now write our first session-typed $\lambda_{MVU}$ application. Our web client consists of a button which, when clicked, triggers the sending of a \texttt{Ping} message to the server. Once clicked, the button is disabled. The server then receives the \texttt{Ping} message and responds with a \texttt{Pong} message; upon receiving the response, the client then re-enables the button.

**Simply-typed channels.** Before considering a session-typed version of the application, it is instructive to consider a version \textit{without} session typing, shown in Figure 6. Let \texttt{Chan}(A) be the type of a simply-typed channel over which one can send and receive values of type $A$. The model is a 3-tuple containing a Boolean value which is true when waiting for the user to click the “Send Ping!” button, and false when waiting for a response; a channel for
Ping messages; and a channel for Pong messages. There are two types of UI message: Click
denotes that the button has been clicked, and Ponged denotes that a Pong message has been
received along the Pong channel.

The view function displays the page, adding the disabled attribute to the button if we are
waiting for a Pong message. The update function case-splits on the UI message: in the case
of a Click message raised by the button, the model is updated to set the pinging flag to false,
and the function creates a command to send a Ping message along pingCh, receive a Pong
message from pongCh, and return a Ponged UI message. In the case of a Ponged message,
the model is updated to set the pinging flag to true, enabling the button again. The server
function models a server thread, which repeatedly receives Ping messages from pingCh and
sends Pong messages to pongCh.

Even in this simple example, it is very easy to communicate incorrectly: if the client
neglected to send a Ping message before trying to receiving a Pong message along pongCh,
then the command would hang forever and the GUI would never re-enable the button. A
similar situation would arise if the server received the Ping message but failed to respond.

Session types. Session types $S$ range over output $!A.S$, input $?A.S$, the completed session
End, recursive session types $\mu t.S$, and (possibly dualised) recursive type variables $t$. We take
an equi-recursive treatment of recursive session types, identifying a recursive session type
with its unfolding. We omit types and constructs for branching and selection as they can be
encoded [15, 33]. The send constant sends a value of type $A$ over an endpoint of type
$!A.S$ and returns the continuation of the session, $S$. The close constant closes a completed
session endpoint. The receive constant takes an endpoint of type $?A.S$ and receives a pair
of a value of type $A$ and endpoint of type $S$. The cancel constant allows an endpoint to be
discarded safely [25, 41]; an exception is raised when trying to read from an endpoint whose
peer has been cancelled.

$$
\text{Session types } S ::= \!A.S \mid ?A.S \mid \mu t.S \mid t \mid \text{End}
$$

$$
\text{send : } (A \times !A.S) \to S \quad \text{receive : } ?A.S \to (A \times S) \quad \text{close : } \text{End} \to 1 \quad \text{cancel : } S \to 1
$$

Figure 7 shows the PingPong client written in $\lambda_{\text{MVU}}$. We can encode the PingPong
protocol as a session type, $\mu t.!(Ping.?Pong.t)$. The Model type encodes the two states of the
application: Pinging(c) is the state where the “Send Ping!” button is enabled and the user

\begin{center}
\begin{figure}
\begin{verbatim}
Model $\triangleq (\text{Bool} \times \text{Chan}(\text{Ping}) \times \text{Chan}(\text{Pong}))$
view $\triangleq \lambda (\text{pinging}, \_, \_).$
let attr =
  if pinging then
    attrEmpty
  else
    attr "disabled" "true" in
html
  <html>
  <body>
    <button {attr} onClick = {\lambda().Click}>
      Send Ping!
    </button>
  </body>
  </html>

Message $\triangleq \text{Click \mid Ponged}$
update $\triangleq \lambda (msg, \_, pingCh, pongCh)$.  
  case msg =
    Click $\rightarrow$
      let cmd =
        cmdSpawn ( send (Ping, pingCh);
                          let Pong = receive pongCh in
                          Ponged in
                          ((false, pingCh, pongCh), cmdEmpty)
                          )
    in

server(pingCh, pongCh) $\triangleq$
  (rec f() .
    let Ping = receive pingCh in
    send (Pong, pongCh); f())
\end{verbatim}
\end{figure}
\end{center}
PingPong ≜ μU!Ping.?Pong.t  
UModel ≜ UPinging | UWaiting  
Model ≜ Pinging(PingPong) | Waiting  
Message ≜ Click | Ponged(PingPong)

view ≜ λuModel.  
let attr =  
  case uModel {  
    UPinging → attrEmpty  
    UWaiting → attr "disabled" "true"  
  } in  
<html>  
  <body>  
    <button {attr} onClick = {λ().Click}> 
      Send Ping!  
    </button>  
  </body>  
</html>

handleClick(model) ≜  
  case model {  
    Pinging(c) →  
      let cmd =  
        cmdSpawn (  
          let c = send (Ping(c)) in  
          let pong = receive c in  
          Ponged(c)) in  
      (Waiting, cmd)  
    Waiting → (Waiting, cmdEmpty)  
  }

update ≜ λ(msg, model).  
  case msg {  
    Click →  
      handleClick(model)  
    Ponged(c) →  
      handlePonged(model, c)  
  }

extract ≜ λmodel.  
  case model {  
    Pinging(c) → (Pinging(c), UPinging)  
    Waiting → (Waiting, UWaiting)  
  }

handlePonged(model, c) ≜  
  case model {  
    Pinging(c') →  
      cancel c';  
      (Pinging(c), cmdEmpty)  
    Waiting → (Pinging(c), cmdEmpty)  
  }

Figure 7 PingPong application

can send a Ping message along session channel c, whereas Waiting is the state where the button is disabled and awaiting a Pong message from the other party. The UModel type is the unrestricted model type which does not include the session channel. Again, Message type encodes the UI messages in the application: the Click UI message is produced when the button is pressed, whereas the Ponged(PingPong) UI message is produced when a Pong session message has been received. Note that the Ponged UI message now contains a session channel of type PingPong as a parameter.

The view function takes an unrestricted model and displays a button, which is disabled in the Waiting state but enabled in the Pinging state. The extract function pairs the linear model with the associated unrestricted model.

The update function case-splits on the message. The handleClick function handles the Click message, and case-splits on the model. If the model is in the Pinging(c) state, then the function creates a command to spawn a process which will send a Ping message along c, receive a Pong message along c, and generate a Ponged UI message when the Pong message is received. The function finally updates the model to the Waiting state. If the model is in the Waiting state—which should not occur, since the button is disabled—then the model remains the same and no command is created.

The handlePonged function handles a Ponged(c) message. Again, we must case split on the model. If the model is in the Waiting state, then we can change to the Pinging state, given endpoint c. However, if the model is in the Pinging(c') state and a Ponged message is received—which should not occur, since according to the session type, there is no way for the peer to send a Pong message while we are waiting to send a Ping—we now have two linear resources. We choose to discard c' using cancel, and change the model to Pinging(c'), but this is an arbitrary choice to satisfy a code path that must exist, but should never be used.
3.3 Model transitions

Our proposal is still not quite satisfactory: as we saw with the PingPong example, we need to include cases in the update function which cannot arise. We highlight these in red. This is even more pronounced when dealing with linear resources, such as needing to handle a Ponged message when waiting to send a Ping.

The problem is that we are encoding the Model type using a sum type, whereas in fact we require multiple model types, and a way to transition between them.

Example. Figure 8 shows how we can modify PingPong to use multiple model types. The left-hand side of the figure shows the Pinging state: the model type consists of the singleton variant tag Pinging(PingPong) containing an endpoint of type PingPong, the unrestricted model is the unit type, and the only message that the Pinging state can receive is Click. The pView function is similar to before, and the pExtract function returns a pair of the current state and the unit value. The pUpdate function is more interesting. Given the current state and a Click message, the function constructs a command which will send the Ping session message, receive the Pong session message, and then generate a Ponged(c) UI message containing the session channel. The function transitions into the Waiting state using the transition primitive, which allows the developer to specify new model, view, update, extract functions, and a command to evaluate. The functions for the Waiting state follow a similar pattern. Session types rule out the communication errors besetting the example in Figure 6, and model transitions eliminate the redundant code paths arising due to illegal states.

3.4 \(\lambda_{MVU}\) with Commands, Linearity, and Transitions

Commands, linearity, and transitions are the three key ingredients needed to extend MVU to support models which include session-typed channels. In this section, we introduce a calculus which combines all three extensions, and prove that the extended calculus is sound.

3.4.1 Syntax and Typing

Figure 9 shows the syntax of \(\lambda_{MVU}\) extended with commands, linearity, and transitions.
Kinds \( \kappa ::= \mathsf{L} | \mathsf{U} \)

Types \[ A, B, C ::= \mathsf{l} | A \to^\ast B | A \times B | A + B | \text{String} | \text{Int} | S | \text{Html}(A) | \text{Attr}(A) | \text{Cmd}(A) | \text{Transition}(A, B) \]

Session types \[ S ::= !A.S | ?A.S | \mu t.S | t | \top | \text{End} \]

Terms \[ L, M, N ::= x | \lambda x. M | M \cdot N | K.M | () | s | n | (M, N) | \text{let} \ (x, y) = M \text{ in } N | \text{inl} \ x | \text{inr} \ x | \text{case} \ L \ { \text{inl} \ x \mapsto M; \text{inr} \ y \mapsto N } | \text{htmlTag} \ t \ M \ N | \text{htmlText} \ M | \text{attr} \ ak \ M | \text{attrEmpty} | \text{cmdSpawn} \ M | \text{cmdEmpty} | M \ast N | \text{transition} \ M_m \ M_v \ M_u \ M_c | \text{noTransition} \ M_m \ M_c | \text{raise} | \text{try} \ L \text{ as } x \text{ in } M \text{ otherwise } N \]

Constants \[ K ::= \text{send} | \text{receive} | \text{new} | \text{cancel} | \text{close} \]

**Figure 9** Syntax of extended calculus

**Types and kinds.** To support linearity, types are assigned kinds, ranged over by \( \kappa \). Types can either be *linear* (L) or *unrestricted* (U). A value of linear type must be used precisely once, whereas a value of unrestricted type can be used many times.

We modify function types to include a kind annotation: linear functions may close over kinds of their type parameters. The reflexive kinds of product, sum, command and transition types are determined unrestricted. The kind of a function type is determined by its kind annotation. Session formulation is inspired by that of Padovani [44]. Base types and HTML and attribute types are linear. The kinding subsumption rule states that if a value can be used many times, then it can also be treated as only being used once. We write \( \Gamma ::= \kappa \) if \( A : \kappa \) for each \( x : A \in \Gamma \).

**Terms.** Term \( \text{cmdSpawn} \ M \) is a command which can spawn term \( M \) as a thread, and is monoidally composable using \( \ast \) and \( \text{cmdEmpty} \).

There are two terms for transitions: the \( \text{noTransition} \ M_m \ M_c \) term denotes that no transition is to occur, and that the model should be updated to \( M_m \) and command \( M_c \) should be evaluated; and \( \text{transition} \ M_m \ M_v \ M_u \ M_c \) denotes that a transition should occur, with new model \( M_m \), view function \( M_v \), update function \( M_u \), extraction function \( M_c \), and command \( M_c \) to be run once the transition has taken place.

To support session typing, we introduce session typing constants, ranged over by \( K \), as described in §3.2. We also introduce an application form for constants, \( K.M \).

Finally, as discussed in §3.2, it is useful to be able to explicitly discard (or cancel) a session channel. In particular, cancellation is crucial in order to handle the interplay between linearity and transitions, as all unprocessed messages (which may contain linear resources) must be safely discarded when a transition occurs.

Following Mostrous and Vasconcelos [41] and Exceptional GV (EGV) by Fowler et al. [25], if a thread tries to receive from an endpoint whose peer has been cancelled, an exception is raised (\( \text{raise} \)). Exceptions can be handled using the \( \text{try} \ L \text{ as } x \text{ in } M \text{ otherwise } N \) construct, which tries to evaluate term \( L \), and binds the result to \( x \) in \( M \) if the term evaluates to a value, and evaluates \( N \) if the term raises an exception.

**Kinding and subkinding.** The kinding relation \( A :: \kappa \) assigns kind \( \kappa \) to type \( A \); our formulation is inspired by that of Padovani [44]. Base types and HTML and attribute types are unrestricted. The kind of a function type is determined by its kind annotation. Session types are linear. The kinds of product, sum, command and transition types are determined by the kinds of their type parameters. The reflexive subkinding rule \( U \leq L \) combined with the kinding subsumption rule states that if a value can be used many times, then it can also be treated as only being used once. We write \( \Gamma :: \kappa \) if \( A :: \kappa \) for each \( x : A \in \Gamma \).
Definition 5 (Kinding and subkinding). We define the subkinding relation as the reflexive relation on kinds ≤ such that U ≤ L. We define the kinding relation A :: k as the largest relation between types and kinds such that:

- A :: k' if A :: k and k ≤ k'
- S :: L
- A :: U if A ∈ {1, String, Int, Html(B), Attr(B)}
- A →^k B :: k
- Cmd(A) :: k if A :: k
- C :: k if C ∈ {A × B, A + B, Transition(A, B)} and both A :: k and B :: k

Term typing. Figure 10 shows the typing rules for the extended calculus. The splitting relation Γ = Γ1 + Γ2 [9] splits a typing context Γ into two subcontexts which may share only unrestricted variables. We support linearity by changing T-VAR to only type a variable in an unrestricted context, and by using the context splitting judgement when typing subterms. The adaptation of the remaining rules to use context splitting is standard, so we omit them.

The constant application rule T-APPK types term KM and makes use of the type schema function Σ(K) to ensure that the argument M is of the correct type. Rule T-CMDSPAWN
assigns term \texttt{cmdSpawn}~\texttt{M} type \texttt{Cmd(A)} if term \texttt{M} has type \texttt{A}, and rules \texttt{T-CmdEmpty} and \texttt{T-CmdAppend} allow commands to be composed monoidally.

Rule \texttt{T-Transition} types a \texttt{transition} term. The typing rule ensures that the types of the new model, and view, update and extract functions are compatible. Note that the type parameters of the \texttt{Transition}(\texttt{A}', \texttt{B}') need not match the types of the new model and functions. Rule \texttt{T-NoTransition} assigns term \texttt{noTransition~\texttt{M}~\texttt{N}} type \texttt{Transition(\texttt{A},\texttt{B})} if new model \texttt{M} has type \texttt{A}, and \texttt{N} is a command of type \texttt{Cmd(B)}. Note that in this way, the \texttt{noTransition~\texttt{M}~\texttt{N}} term replaces the standard result of the \texttt{update} function.

Rule \texttt{T-Try} types an exception handler: the continuations share a typing environment, but the success continuation is augmented with the a variable of the type of the possibly-failing continuation. Finally, \texttt{raise} can have any type as it does not return (\texttt{T-Raise}).

The type and kinding system ensures that the kind of type \texttt{A} determines the kind of the typing environment needed to type a term of type \texttt{A}.

\begin{lemma}
If \( \Gamma \vdash M : A \) and \( A :: \kappa \), then \( \Gamma :: \kappa \).
\end{lemma}

\textbf{Duality.} The duality relation for session types is standard: output types are dual to input types; we use a self-dual \texttt{End} type; and we use the formulation of the duality of recursive session types advocated by Lindley and Morris [37].
3.4.2 Operational Semantics

Runtime syntax. Figure 11 shows the runtime syntax for the combined calculus. We introduce runtime names \(c, d\) which identify session channel endpoints.

The biggest departure is that we require a richer structure on active threads, which form a state machine based on whether a model transition occurs. The idle state is as before, and the updating state evaluates the update function. If there is no model transition, then the thread moves to the extracting state to extract the unrestricted model, and the rendering state to render the new HTML. If there is a model transition, then the thread moves to the extracting\(T\) state followed by the transitioning state to calculate the new HTML to be displayed after the transition. Each state records values which are required in later states: for example, the rendering\([V_m, V_c]\) \(M\) state records the new model \(V_m\) and the command to be executed upon updating the page \(V_c\).

We introduce four new types of process. To model client-server communication, we introduce server processes \(\lfloor M \rfloor\) to model a process \(M\) running on the server; the thread to spawn is given as an argument to \(\text{run}\). As an example, we could write a Ponger server process for the PingPong example, which immediately responds with a Pong message:

\[
\begin{align*}
\text{let } (c, s) &= \text{new } () \text{ in } \\
&\quad \text{Pinging}(c), \text{pView}, \text{pUpdate}, \text{pExtract}, \text{cmdEmpty}, \text{ponger}(s)) \\
\text{ponger}(s) &\triangleq \lambda(). \\
\text{(rec } f(s) . \\
\text{let } (\text{Ping}, s) &= \text{receive } s \text{ in } \\
\text{let } s &= \text{send } (\text{Pong}, s) \text{ in } f s) s
\end{align*}
\]

A name restriction \((\nu cd)P\) binds runtime names \(c\) and \(d\) in process \(P\), following the double-binder formulation due to Vasconcelos [49]. A zapper thread \(\bullet c\) denotes an endpoint \(c\) that has been cancelled and cannot be used in future communications; we write \(\bullet c_1 \parallel \cdots \parallel \bullet c_n\) for \(c_i \in \text{fn}(V)\), where \(\text{fn}(V)\) enumerates the free runtime names in a value \(V\), and extend this sugar to evaluation contexts. The halt process denotes that the event loop process has terminated due to an unhandled exception.

We extend evaluation contexts in the standard way, and introduce a class of pure contexts \(E_P\), which are evaluation contexts which do not contain any exception handling frames. We extend thread contexts with the additional thread states.

Versions. Versions \(\iota\), realised as natural numbers, ensure that threads spawned in a previous state do not deliver incompatible messages. We annotate event loop processes and event handler threads with versions: given an event loop \(\langle T \mid F \rangle_\iota\), a thread \(\langle (M) \rangle_\iota\) where \(\iota \neq \iota'\) can be of arbitrary type as it will be discarded. We write \(\text{version}(P) = \iota\) if \(P\) contains a subprocess \(\langle T \mid F \rangle_\iota\).

Reduction. Figures 12 and 13 show the extended process equivalence and reduction rules. Rule E-Try handles evaluation of the success continuation of an exception handler, and the proc meta-definition returns a sequence of processes to be spawned by a command. Process equivalence is extended to allow commutativity of name restrictions, reordering of names in a binder, and scope extrusion. The final “garbage collection” equivalences \((\nu cd)\langle \xi c \parallel \xi d \parallel P \equiv P\text{ and } \langle \rangle \parallel P \equiv P\) allow us to discard a channel where both endpoints have been cancelled, and a completed server thread, respectively.

Figure 12 details the extended MVU process reduction rules. We split the reduction rules into four categories: MVU reduction rules, session reduction rules, exception reduction rules, and administrative reduction rules.

MVU reduction. MVU reduction rules are specific to MVU. Central to safely integrating linearity and transitions are rules E-Discard, E-DiscardHalt, and E-Handle. Rule
### Additional term reduction rule

$$M \rightarrow_{\text{A}} N$$

### Additional meta-level definitions

- $\operatorname{proc}(\text{cmdEmpty}) = \epsilon$
- $\operatorname{proc}(\text{cmdSend} M) = M$
- $\operatorname{proc}(V \times W) = \operatorname{proc}(V) \cdot \operatorname{proc}(W)$

#### Equivalence of processes

$$P \equiv P'$$

#### Reduction of processes

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Discard</td>
<td>$(T</td>
</tr>
<tr>
<td>E-DiscardHalt</td>
<td>$\parallel V \rightarrow \parallel V$</td>
</tr>
<tr>
<td>E-Handle</td>
<td>$(\text{idle } V_m</td>
</tr>
<tr>
<td>E-Extract</td>
<td>(extracting $V_c (V_c, V_u)</td>
</tr>
<tr>
<td>E-ExtractT</td>
<td>(extracting $T(V_m, V_c, V_c, V_u)</td>
</tr>
<tr>
<td>E-Render</td>
<td>$\parallel \langle\text{rendering}</td>
</tr>
<tr>
<td>E-RenderT</td>
<td>$\parallel \langle\text{transitional}</td>
</tr>
</tbody>
</table>

#### Session reduction rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-New</td>
<td>$T [\text{new}] \rightarrow (vcd) (T [\text{c, d}]$ where $c, d$ fresh</td>
</tr>
<tr>
<td>E-Comm</td>
<td>$(vcd) (T [\text{send } V_c] \parallel T' [\text{receive } d]) \rightarrow (vcd) (T [\text{c}] \parallel T' [\text{V, d}]$</td>
</tr>
<tr>
<td>E-Close</td>
<td>$(vcd) (T [\text{close } c] \parallel T' [\text{close } d]) \rightarrow T [\text{c}] \parallel T' [\text{d}]$</td>
</tr>
<tr>
<td>E-Cancel</td>
<td>$T [\text{cancel } c] \rightarrow T [\text{c}]$</td>
</tr>
<tr>
<td>E-SendZap</td>
<td>$(vcd) (T [\text{send } V_c] \parallel c) \rightarrow (vcd) (T [\text{raise }] \parallel c \parallel V</td>
</tr>
<tr>
<td>E-RecvZap</td>
<td>$(vcd) (T [\text{recv } c] \parallel d) \rightarrow (vcd) (T [\text{raise }] \parallel c \parallel d)$</td>
</tr>
<tr>
<td>E-CloseZap</td>
<td>$(vcd) (T [\text{close } c] \parallel d) \rightarrow (vcd) (T [\text{raise }] \parallel c \parallel d)$</td>
</tr>
</tbody>
</table>

#### Exception reduction rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-RaiseH</td>
<td>$T [\text{try } E_p [\text{raise } x in M otherwise } N] \rightarrow T [N] \parallel E_p$</td>
</tr>
<tr>
<td>E-RaiseURun</td>
<td>$\text{run } E_p [\text{raise }] \rightarrow \parallel E_p$</td>
</tr>
<tr>
<td>E-RaiseUMain</td>
<td>$\langle T_p [\text{raise }]</td>
</tr>
<tr>
<td>E-RaiseUThread</td>
<td>$(E_p [\text{raise }])_i, \rightarrow E_p$</td>
</tr>
<tr>
<td>E-RaiseUSeq</td>
<td>$E_p [\text{raise }], \rightarrow E_p$</td>
</tr>
</tbody>
</table>

#### Administrative reduction rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-LiftT</td>
<td>$T [M] \rightarrow T [N]$ if $M \rightarrow N$</td>
</tr>
<tr>
<td>E-Nu</td>
<td>$(vab) P \rightarrow (vab) P'$ if $P \rightarrow P'$</td>
</tr>
<tr>
<td>E-Par</td>
<td>$P_1 \parallel P_2 \rightarrow P_1 \parallel P_2$ if $P_1 \rightarrow P_1'$</td>
</tr>
</tbody>
</table>

### Figure 12 Reduction rules for extended calculus (1)

E-HANDLE is modified so that the event loop process only handles a message if the message has the same version. If the versions do not match, then E-Discard safely discards any channel endpoints in the discarded message by generating zapper threads. Rules E-Extract, E-ExtractT, E-Render, and E-RenderT handle the state machine transitions described in Figure 11 and are used to calculate the new model and HTML.

### Session reduction

Session reduction rules encode session-typed communication and are mostly standard: E-New generates a name restriction and returns two fresh endpoints; E-Comm handles synchronous communication; and E-Close discards the endpoints of a completed session. The remaining session communication rules handle session cancellation, and are a synchronous variant of Exceptional GV described by Fowler et al. [25]. Rule E-Cancel discards an endpoint. Rules E-SendZap, E-RecvZap, and E-CloseZap raise an exception if a thread tries to communicate along an endpoint whose peer is cancelled, ensuring resources are discarded safely.
We write \( \Psi_1, \Psi_2 \) for the disjoint union of environments \( \Psi_1 \) and \( \Psi_2 \).

We modify the shape of the process typing judgement to \( \Psi \vdash^\phi P : A \), which can be read “under typing environment \( \Psi \) and thread flag \( \phi \), process \( P \) has type \( A \) and version \( \psi \)”. We modify rule TP-EVENTLOOP to include the extraction function, and mandate that the unrestricted model type \( C \) has kind \( U \). We modify rule T-THREAD to state that type of an
event handler thread \( \langle M \rangle \), has type \( A \) if term \( M \) has type \( A \) and the version matches that of the event handler process. We also add a rule TP-OLDTHREAD which allows a thread to have a mismatching type to the event handler process if the versions are incompatible; this is safe as the message will be discarded by E-DISCARD. Finally, TP-ZAP and TP-HALT type zapper threads and the halt thread, and TP-Nu types a name restriction \( (vcd)P \) by adding \( c \) and \( d \) with dual session types into the typing environment.

**Properties.** The extended calculus satisfies preservation.

> **Theorem 7** (Preservation). If \( \vdash C \) and \( C \rightarrow C' \), then \( \vdash C' \).

Although session types rule out deadlock within a single session, without imposing a tree-like structure on processes [36, 51] (which is too inflexible for our purposes) or using techniques such as channel priorities [34, 43, 45], it is not possible to rule out deadlocks when considering multiple sessions. Since communication over multiple sessions can introduce deadlocks, we begin by proving an error-freedom property, similar to that of Gay and

---

### Figure 14: Runtime typing for extended calculus

<table>
<thead>
<tr>
<th>Typing rules for names, events, and function state</th>
<th>( \Gamma \vdash M : A )</th>
<th>( \vdash c : \Psi )</th>
<th>( \Psi \vdash F : State(A, B, C) )</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>T-NAME</strong> ( \Gamma : U )</td>
<td>( \vdash V : ty(ev) ) ( ty(ev) : U )</td>
<td>( \vdash ev(V) )</td>
<td></td>
</tr>
<tr>
<td>( \Gamma, c : S \vdash c : S )</td>
<td>( \vdash ev(V) )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Typing rules for active threads</th>
<th>( \Psi \vdash T : EvtLoop(A, B, C) )</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TT-IDLE</strong></td>
<td>( \Psi \vdash \text{idle} ) ( V, \text{EvtLoop}(A, B, C) )</td>
</tr>
<tr>
<td><strong>TT-RENDERING</strong></td>
<td>( \Psi \vdash \text{rendering}(V_m, V_c) ) ( M : \text{EvtLoop}(A, B, C) )</td>
</tr>
<tr>
<td><strong>TT-EXTRACTING</strong></td>
<td>( \Psi \vdash \text{extracting}(V_c) ) ( M : \text{EvtLoop}(A, B, C) )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Typing rules for processes</th>
<th>( \Psi \vdash^* P : A )</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TP-RUN</strong></td>
<td>( \Psi \vdash M : (A \times (A \rightarrow U \text{Html}(B))) \times ((B \times A) \rightarrow U \text{Transition}(A, B)) \times C : U )</td>
</tr>
<tr>
<td><strong>TP-EVENTLOOP</strong></td>
<td>( \Psi \vdash T : \text{EvtLoop}(A, B, C) )</td>
</tr>
<tr>
<td><strong>TP-THREAD</strong></td>
<td>( \Psi \vdash M : A )</td>
</tr>
<tr>
<td><strong>TP-OLDTHREAD</strong></td>
<td>( \Psi \vdash M : B )</td>
</tr>
<tr>
<td><strong>TP-SERVERTHREAD</strong></td>
<td>( \Psi \vdash M : 1 )</td>
</tr>
<tr>
<td><strong>TP-PAR</strong></td>
<td>( \Psi \vdash P_1 : A )</td>
</tr>
<tr>
<td><strong>TP-ZAP</strong></td>
<td>( \Psi \vdash P_1 : A )</td>
</tr>
<tr>
<td><strong>TP-HALT</strong></td>
<td>( \Psi \vdash P_1 : A )</td>
</tr>
<tr>
<td><strong>TP-Nu</strong></td>
<td>( \Psi \vdash c : S )</td>
</tr>
</tbody>
</table>

---

*Note: The table above represents the typing rules for names, events, and function state, as well as the rules for active threads and processes.*
Vasconcelos [26]. An error process involves a communication mismatch.

Definition 8 (Error process). A process $P$ is an error process if it contains one of the following processes as a subprocess:

1. $(\nu_{\text{cd}})(T[\text{send}(V,c)] \parallel T'[\text{send}(W,d)])$
2. $(\nu_{\text{cd}})(T[\text{send}(V,c)] \parallel T'[\text{close}])$
3. $(\nu_{\text{cd}})(T[\text{receive} c] \parallel T'[\text{receive} d])$
4. $(\nu_{\text{cd}})(T[\text{receive} c] \parallel T'[\text{close}])$

Configuration typing ensures error-freedom.

Theorem 9 (Error-freedom). If $\Psi \vdash_? P : A$, then $P$ is not an error process.

Error-freedom shows that session typing ensures the absence of communication mismatches. What remains is to show that, apart from the possibility of deadlock, the additional features do not interfere with the progress property enjoyed by $\lambda_{MVU}$. We begin by classifying the notion of a blocked thread, which is a thread blocked on a communication action.

Definition 10 (Blocked thread). We say a thread $T[M]$ is blocked if either $M = \text{send}(V,W)$, $M = \text{receive} V$, or $M = \text{close} V$.

Let us refer to halt, $(T | F)_i$, and run $M$ as main threads, and $(M)_i$, $[M]$, and $\emptyset c$ as auxiliary threads. Each well-typed configuration has precisely one main thread.

We can now classify the notion of progress enjoyed by the extended calculus. Either the configuration can reduce; is waiting for an event; has halted due to an unhandled exception; or is deadlocked. Again, let $\rightarrow E$ be the $\rightarrow$ relation without E-Interact.

Theorem 11 (Weak Event Progress). Suppose $\vdash C$. Either there exists some $C'$ such that $C \rightarrow C'$, or there exists some $C'$ such that $C \equiv C'$ and:

1. $D$ cannot be written $D[\text{domTag}(\vec{c}) \text{ t V D}]$ for a non-empty $\vec{c}$.
2. If the main thread of $C'$ is halt, then all auxiliary threads are blocked or zapper threads.
3. If the main thread of $C'$ is run $M$, then $M$ is blocked, and all auxiliary threads are either blocked, values, or zapper threads.
4. If the main thread of $C'$ is $(T | F)_i$, then:
   a. if $T = \text{idle} V_m$, then each auxiliary thread is either blocked or a zapper thread; or
   b. if $T = T_A[L]$ then $L$ is blocked, and each auxiliary thread is either blocked, a value, or a zapper thread.

4 Implementation and Example Application

We have implemented an MVU library for the Links tierless web programming language, which includes all extensions in the paper; Links already has a linear type system and distributed session types, so is an ideal fit.

We now describe a chat application, extending the application presented by Fowler et al. [25]. The application (Figure 15) has two main stages shown to the user: on the first, the user is presented with a list of rooms, and enters a username and selects a room. If a user with the given nickname is not already in the selected room, then the user joins the room, receiving the current topic, a list of other nicknames, and a channel used to receive messages from the server. The user can then send chat messages, change the topic, and leave the room. If the user is the first user in the room, then they join as a moderator and receive an additional channel which can be used to kick, mute, or promote other users to moderators. Users can receive incoming chat messages, and system messages detailing changes such as a new topic or a user joining the room.
**Model-View-Update-Communicate**

**Client session types**

- **typename ClientConnect**: \(?[RoomName]\).ClientSelect;
- **typename ClientSelect**: \(![RoomName, Nickname]\).
  - JoinedOK: ?[Topic, [Nickname], ClientReceive] . ClientSend,
  - JoinedOKAsModerator: ?[Topic, [Nickname], ClientReceive, ModeratorSend],
  - Nope: ?ConnectError.End |&|

- **typename ClientReceive**: [&|\n  - IncomingChatMessage: ?[Nickname, Message].ClientReceive,
  - NewUser: ?[Nickname].ClientReceive,
  - NewTopic: ?[Topic].ClientReceive,
  - UserLeft: ?[Nickname].ClientReceive,
  - UserMuted: ?[Nickname].ClientReceive,
  - UserUnmuted: ?[Nickname].ClientReceive,
  - BecomeModerator: ?ModeratorSend.ClientReceive,
  - Kick: End |&|

- **typename ClientSend**: [+|\n  - ChatMessage: !(Message).ClientSend,
  - ChangeTopic: ![Topic].ClientSend,
  - Leaving: End [+];

- **typename ModeratorSend**: [+|\n  - KickUser: !(Nickname).ModeratorSend,
  - MuteUser: !(Nickname).ModeratorSend,
  - MakeModerator: ![Nickname].ModeratorSend [+];

**Figure 15** Chat server application

**Session types.** We can encode these interaction patterns using session types. Links session type notation for offering a choice is [&]|...|&|, and making a choice is [+]|...|+|. Type ClientConnect describes the client receiving the room list. Type ClientSelect describes the client sending the room name and nickname, and receiving the response from the server: either joining as a regular user (JoinedOK); joining as a moderator (JoinedOKAsModerator); or an error (Nope). Types ClientSend and ClientReceive detail the messages that the client can send to, and receive from the server, respectively. Type ModeratorSend details privileged moderator actions.

**Server.** Although the original version of Links [11] ran as a CGI script, modern Links applications run as a persistent webserver.

Upon execution, the chat application creates an access point for sessions of type ClientConnect, which supports session establishment, and spawns an acceptor thread to accept incoming requests on the access point. Each chat room is represented as a process on the server.

When an HTTP request is made, the response contains the MVU application and the access point ID which can be used to establish a session of type ClientConnect. After the initial HTTP response, further communication between the client and server happens over a WebSocket [20].
Client. The application has three states: connection, chatting, and a “waiting” state shown while waiting for a response. For the purposes of the paper, we consider the connection state.

\[
\text{typename SelectedRoom = NewRoom | SelectedRoom: String;}
\]

\[
\text{typename NotConnectedModel = nickname: String, rooms: [RoomName], selectedRoom: SelectedRoom, newRoomText: RoomName, error: Maybe(Error);}
\]

\[
\text{typename NCModel = (ClientSelect, NotConnectedModel);}
\]

\[
\text{typename NCMessage = UpdateNickname: Nickname | UpdateSelectedRoom: SelectedRoom | UpdateNewRoom: RoomName | SubmitJoinRoom |;}
\]

The NotConnectedModel is the unrestricted part of the model, and contains the current nickname (nickname), list of rooms (rooms), selected room (selectedRoom), value of the “new room” text box (newRoomText), and an optional error message to display (error). The model, NCModel, is a pair of a session endpoint of type ClientSelect and a NotConnectedModel. The UI messages are described by the NCMessage type: for example, the UpdateNickname message is generated by the onInput event of the nickname input box.

Upon receiving the SubmitJoinRoom UI message when the form is submitted, the application can send the nickname and selected room along the ClientSelect channel, all of which are contained in the model, without requiring ad-hoc messaging or imperative updates.

5 Related work

Flapjax [40] was the first web programming language to use functional reactive programming (FRP) [17] in the setting of web applications. Flapjax provides behaviours, which are variables whose contents change over time, and event streams, which are an infinite stream of discrete events which change a behaviour. ScalaLoci [52] is a multi-tier reactive programming framework written in Scala, where changes in reactive signals are propagated across tiers, rather than using explicit message passing. Ur/Web [10] and WebSharper UI [24] store data in mutable variables, and allow views of the data to be combined using monadic combinators.

Felleisen et al. [19] describe an earlier approach similar to MVU written in the DrScheme [21] system. Similar to the MVU update function, events such as key presses and mouse movements are handled using functions of type (Model × Event) → Model. The approach handles “environment” events rather than events dispatched by individual elements, and the approach is not formalised. Environment events can be handled using subscriptions in Elm, which can be added to \(\lambda\)MVU (see the extended version of the paper [23]).

React [2] is a popular JavaScript UI framework. In React, a user defines data models and rendering functions, and similar to Elm, updates are propagated to the DOM by diffing. Differently to MVU, there is no notion of a message, and a page consists of multiple components rather than being derived from a single model. We expect some technical machinery from \(\lambda\)MVU (e.g., event queues, DOM contexts, and diffing) could be reused when formalising React. Redux [5] is a state container for JavaScript applications: to modify the state, one dispatches an action, and a function takes the previous state and an action and produces a new state. In combination with React, the approach strongly resembles MVU.

Formlets [12] are a web form abstraction based on applicative functors [39]. Bjornson et al. [7] generalise Formlets to support a monadic interface, and Denuzière et al. [16] decouple a form’s data model from its rendering function.

Hop.js [47] is a multi-tier web framework written in JavaScript. Hop.js services allow remote function invocation, and the framework supports client-side message-passing concurrency using Web Workers [27], but there is no cross-tier message-passing concurrency.

Session types were introduced by Honda [28] and were first considered in a linear functional language by Gay and Vasconcelos [26]; Wadler [51] later introduced a session-typed functional
language GV and a logically-grounded session-typed calculus CP (following Caires and Pfenning [8]), and translated GV into CP. Lindley and Morris [36] introduced an operational semantics for GV, and showed type- and semantics-preserving translations between GV and CP. GV inspires FST [38], which is the core calculus for Links’ treatment of session typing.

Fowler et al. [25] extend GV with failure handling, and extend Links with cross-tier session-typed communication. They do not formally consider GUI development, and their approach to frontend web programming using session types (described in Section 1) leads to a disconnect between the state of the page and the application logic. We build upon their approach to session-typed web programming, while also allowing idiomatic GUI development.

King et al. [32] present a toolchain for writing web applications which respect multiparty session types [30]. Protocols are compiled to PureScript [48] using a parameterised monad [6] to guarantee linearity, and the authors integrate their encoding of session types with the Concur UI framework [31]. Each application may only have a single session connecting the client and server, whereas in our system there may be multiple; our approach supports first-class linearity and cross-tier typechecking; our approach is formalised; and our approach supports failure handling. Links does not yet support multiparty session types.

6 Conclusion

Session types allow conformance to protocols to be checked statically. The last few years have seen a flurry of activity in implementing session types in a multitude of programming languages, but linearity—a vital prerequisite for implementing session types safely—is difficult to reconcile with the asynchronous nature of graphical user interfaces. Consequently, the vast majority of implementations using session types are command line applications, and the few implementations which do integrate session types and GUIs do so in an ad-hoc manner.

In this paper, we have addressed this problem by extending the Model-View-Update architecture, pioneered by the Elm programming language. We have presented the first formal study of MVU by introducing a core calculus, $\lambda_{MVU}$, and have proved it sound. Leveraging our formal characterisation of MVU, we have introduced three extensions: commands, linearity, and model transitions, enabling us to present the first formal integration of session-typed communication with a GUI framework. Informed by our formal model, we have implemented our approach in Links, and have shown a larger example of a chat application.

At present, an application can transition freely between any models. As future work, we will investigate how to encode allowed transitions as a behavioural type.

References


25 Simon Fowler, Sam Lindley, J. Garrett Morris, and Sára Decova. Exceptional
asynchronous session types: session types without tiers. PACMPL, 3(POPL):28:1–28:29, 2019. doi:
26 Simon J. Gay and Vasco Thudichum Vasconcelos. Linear type theory for
28 Kohei Honda. Types for dyadic interaction. In CONCUR, volume 715 of Lecture
29 Kohei Honda, Vasco Thudichum Vasconcelos, and Makoto Kubo. Language
primitives and type discipline for structured communication-based programming. In ESOP,
30 Kohei Honda, Nobuko Yoshida, and Marco Carbone. Multiparty asynchronous
32 Jonathan King, Nicholas Ng, and Nobuko Yoshida. Multiparty session type-safe
web development with static linearity. In PLACES@ETAPS, volume 291 of EPTCS, pages
33 Naoki Kobayashi. Type systems for concurrent programs. In 10th Anniversary
Colloquium of UNU/IIST, volume 2757 of Lecture Notes in Computer Science, pages
34 Naoki Kobayashi. A new type system for deadlock-free processes. In CONCUR,
35 Glenn E. Krasner and Stephen T. Pope. A Cookbook for using the Model-view
Controller user interface paradigm in Smalltalk-80. J. Object Oriented Program., 1(3):26–49, August
36 Sam Lindley and J. Garrett Morris. A semantics for propositions as sessions. In ESOP,
37 Sam Lindley and J. Garrett Morris. Talking bananas: structural recursion for session
38 Sam Lindley and J. Garrett Morris. Lightweight functional session types. Behavioural
39 Conor McBride and Ross Paterson. Applicative programming with effects. J. Funct.
40 Leo A. Meyerovich, Arjun Guha, Jacob P. Baskin, Gregory H. Cooper, Michael Greenberg,
Aleks Bronfman, and Shiriram Krishnamurthi. Flapjax: a programming language for
41 Dimitris Mostrous and Vasco T. Vasconcelos. Affine sessions. Logical Methods in
42 Joachim Niehren, Jan Schwinghammer, and Gert Smolka. A concurrent lambda calculus
43 Luca Padovani. Deadlock and lock freedom in the linear \( \pi \)-calculus. In CSL-LICS,
44 Luca Padovani. Context-free session type inference. In ESOP, volume 10201 of Lecture
45 Luca Padovani and Luca Novara. Types for deadlock-free higher-order programs. In


