Behavioural Type-Based Static Verification Framework for GO
Us ∈ Mobility Research Group

http://mrg.doc.ic.ac.uk/
• **TCS’16**: Monitoring Networks through Multiparty Session Types. Laura Bocchi, Tzu-Chun Chen, Romain Demangeon, Kohei Honda, Nobuko Yoshida
• **LMCS’16**: Multiparty Session Actors. Rumyana Neykova, Nobuko Yoshida
• **FMSD’15**: Practical interruptible conversations: Distributed dynamic verification with multiparty session types and Python. Romain Demangeon, Kohei Honda, Raymond Hu, Rumyana Neykova, Nobuko Yoshida
• **TGC’13**: The Scribble Protocol Language. Nobuko Yoshida, Raymond Hu, Rumyana Neykova, Nicholas Ng
Scribble: Describing Multi Party Protocols

Scribble is a language to describe application-level protocols among communicating systems. A protocol represents an agreement on how participating systems interact with each other. Without a protocol, it is hard to do meaningful interaction: participants simply cannot communicate effectively, since they do not know when to expect the other parties to send data, or whether the other party is ready to receive data. However, having a description of a protocol has further benefits. It enables verification to ensure that the protocol can be implemented without resulting in unintended consequences, such as deadlocks.
module examples;

global protocol HelloWorld(role Me, role World) {
    hello() from Me to World;
    choice at World {
        goodMorning1() from World to Me;
    } or {
        goodMorning2() from World to Me;
    }
}
End-to-End Switching Programme by DCC

1. All design work takes place in ABACUS, DCC’s enterprise architecture tool. This can export standard XMI files (an open standard for UML5)

2. XMI is converted into OpenTracing format for consumption by managed service

3. OpenTracing files are combined to build a model in Scribble

4. Model holds types rather than instances to understand behaviour

5. Scribble compiler identifies inconsistency, change & design flaws

6. Issues highlighted graphically in Eclipse

7. Generate exception report and send back to DCC

www.estafet.com

Estafet Managed Service
Caveats:
1. Using earlier implementation of Scribble (CDL), because we already have those tools
2. Using earlier plugin to Eclipse - we’d want to improve this
3. We’re not going via OpenTracing - this is part of the bid costs

3. OpenTracing files are combined to build a model in Scribble
4. Model holds types rather than instances to understand behaviour
5. Scribble compiler identifies inconsistency, change & design flaws
6. Issues highlighted graphically in Eclipse
7. Generate exception report and send back to DCC

Scope of the demo

Estafet Managed Service
Interactions with Industries

Strange Loop
SEPTEMBER 15-17 2016 / PEABODY OPERA HOUSE / ST. LOUIS, MO

Adam Bowen @adammbowen · Sep 15
I didn’t even know that session types existed an hour ago, but thanks to Nobuko Yoshida’s great talk at #pwiconf, I want to learn more.

DoC researcher to speak at Golang UK conference
by Vicky Kapogianni
20 July 2016

@nicholascwng rocking on @GolangUKconf about static deadlock detection in #golang #gouk16

The Golang UK Conference
Interactions with Industries

F#unctional Londoners Meetup Group

6 days ago · 6:30 PM
Session Types with Fahd Abdeljallal

43 Members

Synopsis: Session types are a formalism to codify the structure of a communication, using types to specify the communication protocol used. This formalism provides the...

Distributed Systems vs. Compositionality

Dr. Roland Kuhn
@rolandkuhn — CTO of Actyx

Current State

• behaviors can be composed both sequentially and concurrently
• effects are not yet tracked
• Scribble generator for Scala not yet there
• theoretical work at Imperial College, London (Prof. Nobuko Yoshida & Alceste Scalas)
Selected Publications 2016/2017

• [CC’16] Nicholas Ng, NY: Static Deadlock Detection for Concurrent Go by Global Session Graph Synthesis.
• [POPL’16] Dominic Orchard, NY: Effects as sessions, sessions as effects.
Selected Publications 2016/2017

- [CC’16] Nicholas Ng, NY: Static Deadlock Detection for Concurrent Go by Global Session Graph Synthesis.
HOW to

- derive theories to practices
- make theories understandable
- meet theoretical challenges (concurrency, distributions)
- communicate people
Behavioural Type-Based Static Verification Framework for GO

Julian Lange  Nicholas Ng  Bernardo Toninho  Nobuko Yoshida
Go concurrency verification research at DoC grabs headline

A paper by DoC researchers at POPL on Go concurrency verification was featured in a tech blog and generates a buzz outside of the research community.

A paper by researchers at the department was recently featured in the morning paper, a blog by venture capitalist Adrian Colye, which summarises an important, influential, topical or otherwise interesting paper in the field of computer science every weekday in an easily digestible way by non-researchers. On the 2 Feb 2017 issue of the morning paper, it was highlighted as "the true spirit of POPL (Principles of Programming Languages)".
GO programming language @ Google (2009)

- Message-Passing based multicore PL, successor of C

- Do not communicate by shared memory; instead, share memory by communicating

  Go Lang Proverb

- Explicit channel-based concurrency
  - Buffered I/O communication channels
  - Lightweight thread spawning — goroutines
  - Selective send/receive

Fun

Dropbox, Netflix, Docker, CoreOS
- Go has a runtime deadlock detector
- How can we detect *partial* deadlock and channel errors for *realistic* programs?
- Use *behavioural types* in process calculi
  e.g. [ACM Survey, 2016] 185 citations, 6 pages

- Dynamic channel creations, unbounded thread creations, recursions, ...

- *Scalable* (synchronous/asynchronous) · Modular, Refinable
- **GO** has a runtime deadlock detector.

- How can we detect **partial deadlock and channel errors for realistic programs**?

- Use **behavioural types** in process calculi; e.g., [ACM Survey, 2016] 185 citations, 6 pages.

- Dynamic channel creations, unbounded thread creations, recursions, ...

- **Scalable** (synchronous/asynchronous) · Modular, Refinable
- **Go** has a runtime deadlock detector.
- How can we detect partial deadlock and channel errors for realistic programs?
- Use behavioural types in process calculi.
  - e.g. [ACM Survey, 2016] 185 citations, 6 pages.
- Dynamic, unbounded thread creations, recursions, ...
- **Scalable** (synchronous/asynchronous), Modular, Refinable.
- **GO** has a **runtime deadlock detector**

- **How can we detect** **partial deadlock and channel errors** for **realistic programs**?

- **Use** **behavioural types in process calculi**
  
  e.g. **[ACM Survey, 2016]** 185 citations, 6 pages

- **Channel creations, unbounded thread creations, recursions**...

- **Scalable** (**synchronous/asynchronous**) **Modular, Refinable**
- **Go** has a runtime deadlock detector.
- How can we detect partial deadlock and channel errors for realistic programs?
- Use behavioural types in process calculi.
  - e.g. [ACM Survey, 2016] 185 citations, 6 pages.
- Dynamic channel creations, unbounded thread creation, etc.
- **Scalable** (synchronous/asynchronous) Modular, retrainable, understandable.
Our Framework

**STEP 1** Extract Behavioural Types
- (Most) Message passing features of **GO**
- Tricky primitives: selection, channel creation

**STEP 2** Check Safety/Liveness of Behavioural Types
- Model-Checking (Finite Control)

**STEP 3**
- Relate Safety/Liveness of Behavioural Types and **GO Programs**
  - 3 Classes [POPL’17]
  - Termination Check
Our Framework

**STEP 1** Extract Behavioural Types
- (Most) Message passing features of **GO**
- Tricky primitives: selection, channel creation

**STEP 2** Check Safety/Liveness of Behavioural Types
- Model-Checking (Finite Control)

**STEP 3**
- Relate Safety/Liveness of Behavioural Types and **GO** Programs
  - 3 Classes [POPL’17]
  - Termination Check
Verification framework for Go

Overview

(1) Type inference
(2) Model checking
(3) Termination checking

Transform and verify

Behavioural types

Check safety and liveness

Create input model and formula

Address type and process gap

Pass to termination prover

SSA IR

Go source code

Nobuko Yoshida
Open Problems of Session Types
mrg.doc.ic.ac.uk
Concurrent in Go

```
func main() {
    ch, done := make(chan int), make(chan int)
    go send(ch) // Spawn as goroutine.
    go func() {
        for i := 0; i < 2; i++ {
            print("Working...")
        }
    }()
    go recv(ch, done)
    go recv(ch, done) // Who is ch receiving from?
    print("Done:", <-done, <-done) // 2 receivers, 2 replies
}
```

```
func send(ch chan int) { ch <- 1 } // Send to channel.
func recv(in, out chan int) { out <- <-in } // Fwd in to out.
```

- Send/receive blocks goroutines if channel full/empty resp.
- Close a channel `close(ch)`
- Guarded choice `select { case <-ch; case <-ch2; }`
Concurrency in Go
Deadlock detection

```go
func main() {
    ch, done := make(chan int), make(chan int)
    go send(ch) // Spawn as goroutine.
    go func() {
        for i := 0; i < 2; i++ {
            print("Working...")
        }
    }()
    go recv(ch, done)
    go recv(ch, done) // Who is ch receiving from?
    print("Done:", <-done, <-done) // 2 receivers, 2 replies
}
func send(ch chan int) { ch <- 1 } // Send to channel.
func recv(in, out chan int) { out <- <-in } // Fwd in to out.

Run program:

$ go run main.go
fatal error: all goroutines are asleep - deadlock!
```

Nobuko Yoshida
Open Problems of Session Types
mrg.doc.ic.ac.uk
func main() {
    ch, done := make(chan int), make(chan int)
    go send(ch) // Spawn as goroutine.
    go func() {
        for i := 0; ; i++ { // infinite
            print("Working...")
        }
    }()
    go recv(ch, done)
    go recv(ch, done) // Who is ch receiving from?
    print("Done:", <-done, <-done) // 2 receivers, 2 replies
}
func send(ch chan int) { ch <- 1 } // Send to channel.
func recv(in, out chan int) { out <- <-in } // Fwd in to out.
**Concurrency in Go**

**Deadlock detection**

```go
cfunc main() {
    ch, done := make(chan int), make(chan int)
    go send(ch) // Spawn as goroutine.
    go func() {
        for i := 0; ; i++ { // infinite
            print("Working...")
        }
    }()
    go recv(ch, done)
    go recv(ch, done) // Who is ch receiving from?
    print("Done:", <-done, <-done) // 2 receivers, 2 replies
}
cfunc send(ch chan int) { ch <- 1 } // Send to channel.
cfunc recv(in, out chan int) { out <- <-in } // Fwd in to out.
```

Deadlock **NOT** detected (some goroutines are running)
Concurrency in Go
Deadlock detection

- Go has a runtime deadlock detector, panics (crash) if deadlock
- Deadlock if all goroutines are blocked
- Some packages (e.g. net for networking) disables it

```go
import "net" // Load "net" package
func main() {
    ch := make(chan int)
    send(ch)
    print(<-ch)
}
func send(ch chan int) { ch <- 1 }
```

Add benign import
Concurrency in Go
Deadlock detection

- Go has a runtime deadlock detector, panics (crash) if deadlock
- Deadlock if all goroutines are blocked
- Some packages (e.g. `net` for networking) **disables** it

```go
import _ "net" // Load "net" package

func main() {
    ch := make(chan int)
    send(ch)
    print(<-ch)
}

func send(ch chan int) { ch <- 1 }
```

Deadlock **NOT** detected
Go Programs as Processes

<table>
<thead>
<tr>
<th>Go Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P, Q := \pi; P$</td>
</tr>
<tr>
<td>$\pi := u!\langle e \rangle</td>
</tr>
</tbody>
</table>
Go Programs as Processes

Go Program

\[
P, Q \; ::= \; \pi; P \\
\quad | \quad \text{close } u; P
\]

\[
\pi \; ::= \; u!\langle e \rangle \mid u?(y) \mid \tau
\]
Go Programs as Processes

Go Program

\[
P, Q \quad ::= \quad \pi; P \quad \pi \quad ::= \quad u!\langle e \rangle \mid u?(y) \mid \tau
\]

| \quad close u; P | select\{\pi; P\}_{i\in I} |
Go Programs as Processes

**Go Program**

\[
P, Q ::= \pi; P \quad \pi ::= u!\langle e \rangle \mid u?(y) \mid \tau
\]

- close \( u \); \( P \)
- select\{\( \pi_i; P_i \)\}_{i \in I}
- if \( e \) then \( P \) else \( Q \)
Go Programs as Processes

Go Program

\[
P, Q \quad ::= \quad \pi; P \\
\quad \quad \text{close } u; P \\
\quad \quad \text{select}\{\pi_i; P_i\}_{i \in I} \\
\quad \quad \text{if } e \text{ then } P \text{ else } Q \\
\quad \quad \text{newchan}(y: \sigma); P
\]

\[
\pi \quad ::= \quad u!(e) \mid u?(y) \mid \tau
\]
Go Programs as Processes

<table>
<thead>
<tr>
<th>Go Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P, Q ::= \pi; P$</td>
</tr>
<tr>
<td>close $u; P$</td>
</tr>
<tr>
<td>select{$\pi_i; P_i$}$_{i \in I}$</td>
</tr>
<tr>
<td>if $e$ then $P$ else $Q$</td>
</tr>
<tr>
<td>newchan($y: \sigma$); $P$</td>
</tr>
<tr>
<td>$P \mid Q \mid 0 \mid (\nu c)P$</td>
</tr>
</tbody>
</table>

$\pi ::= u!\langle e \rangle \mid u?(y) \mid \tau$
Go Programs as Processes

Go Program

\[\begin{align*}
P, Q & := \pi; P & \pi & := u!\langle e \rangle \mid u?(y) \mid \tau \\
& \mid \text{close } u; P \\
& \mid \text{select}\{\pi_i; P_i\}_{i \in I} \\
& \mid \text{if } e \text{ then } P \text{ else } Q \\
& \mid \text{newchan}(y:\sigma); P \\
& \mid P \mid Q \mid 0 \mid (\nu c)P \\
& \mid X\langle \tilde{e}, \tilde{u} \rangle \\
D & := X(\tilde{x}) = P \\
P & := \{D_i\}_{i \in I} \text{ in } P
\end{align*}\]
## Go Programs as Processes

### Go Program

| $P, Q$ | $\pi; P$ | $\pi : u!\langle e \rangle | u?\langle y \rangle | \tau$ |
|-------|---------|------------------|
|       | close $u; P$ |                 |
|       | select${\pi_i; P_i}_{i \in I}$ |                 |
|       | if $e$ then $P$ else $Q$ |                 |
|       | newchan($y:\sigma$); $P$ |                 |
| $P \mid Q \mid 0 \mid (\nu c)P$ |                 |
|       | $X\langle \tilde{e}, \tilde{u} \rangle$ |                 |
| $D$   | $X(\tilde{x}) = P$ |                 |
| $P$   | ${D_i}_{i \in I}$ in $P$ |                 |
Abstracting Go with Behavioural Types

Types

\[
\alpha := \overline{u} \mid u \mid \tau
\]

\[
T, S := \alpha; T \mid T \oplus S \mid \&\{\alpha_i; T_i\}_{i \in I} \mid (T \mid S) \mid 0
\]

\[
T := \{t(\tilde{y}_i) = T_i\}_{i \in I} \text{ in } S
\]

- Types of a CCS-like process calculus
- Abstracts Go concurrency primitives
  - Send/Recv, new (channel), parallel composition (spawn)
  - Go-specific: Close channel, Select (guarded choice)
MiGo Liveness / Safety

Channel Safety

- Channel is closed at most once.
- Can only input from a closed channel (default value).
- Others raise an error and crash.
Channel Safety

- Channel is closed at most once.
- Can only input from a closed channel (default value).
- Others raise an error and crash.

\[ P \text{ is channel safe if } P \xrightarrow{*} (r \leftarrow) Q \text{ and } Q \downarrow \text{ close}(a) \]

\[ \neg(Q \downarrow \text{end}(a)) \land \neg(Q \downarrow \overline{a}) \]

- never closing
- never send

Barb
[Milner 87; Sangiorgi 92]
Migo  Liveness / Safety

> Liveness

All reachable actions are eventually performed

\[ P \text{ is live if } P \xrightarrow{\varphi} Q \]

\[ Q \downarrow a \Rightarrow Q \downarrow \tau \text{ at } a \]

\[ Q \downarrow \overline{a} \Rightarrow Q \downarrow \tau \text{ at } a \]

Reduction (tau) at a
Select

\[ P_1 = \text{select} \{ a!, \ b? \}, \ 2. \ P \} \]

\[ P_2 = \text{select} \{ a!, \ b? \} \quad R_1 = a? \]

Time Out

\begin{align*}
& \text{if } P \text{ is live} \\
& \text{P}_1 \text{ is live} \\
& \text{P}_2 \text{ is not live} \\
& \text{P}_2 | R_2 \text{ is}
\end{align*}
Select

\[ P_1 = \text{select } \{ a!, b?, z \cdot P \} \]

\[ P_2 = \text{select } \{ a!, b? \} \]

Barb \( \downarrow \bar{a} \)

Time Out

if \( P \) is live
\( P_1 \) is live

P2 is not live
\( P_2 \mid R_2 \) is

\[ R_1 = a? \]

\[ \pi_i \downarrow Q_i \]

\[ \text{select } \{ \pi_i. P_i \} \downarrow \bar{a} \]

\[ P \downarrow \bar{a} \]
\[ Q \downarrow \bar{a} \]

Liveness \( Q \downarrow \bar{a} \Rightarrow Q \downarrow z \) at ai
Verification framework for Go
Model checking with mCRL2

Generate LTS model and formulae from types

- Finite control (no parallel composition in recursion)

- Properties (formulae for model checker):
  - Global deadlock
  - Channel safety (no send/c\texttt{lose} on closed channel)
  - Liveness (partial deadlock)
  - Eventual reception

  - Require additional guarantees
the $\mu$-calculus encoding properties with barbs

Global Deadlock

Channel Safety

Liveness

$\forall a \in C \ (\downarrow a \lor \downarrow \bar{a}) \Rightarrow \langle \alpha \rangle T$

$\forall a \in C \ \downarrow \text{close } a \Rightarrow \neg (\downarrow \bar{a} \lor \downarrow \text{close } a)$

$\forall a \in C \ (\downarrow a \lor \downarrow \bar{a}) \Rightarrow \Phi (\langle [a] \rangle T) \land$

$\forall \bar{a} \in C \ ^m \downarrow \bar{a} \Rightarrow \Phi (\forall a \in \bar{a} \langle [a] \rangle T)$

[Lange & NY TACAS '17]
Verification framework for Go
Termination checking with KITTeL

- Extracted types do not consider data in process
- Type liveness $\neq$ program liveness
  - Especially when involving iteration
  - Check for loop termination
- Properties:
  - ✓ Global deadlock
  - ✓ Channel safety (no send/close on closed channel)
  - ✓ Liveness (partial deadlock)
  - ✓ Eventual reception

```go
def main() {
    ch := make(chan int)
    go func() {
        for i := 0; i < 10; i++ {
            // Does not terminate
        }
        ch <- 1
    }()
    <-ch
}
```

- Type: Live
- Program: NOT live

Nobuko Yoshida
Open Problems of Session Types
mrg.doc.ic.ac.uk
Tool demo
Conclusion

Verification framework based on **Behavioural Types**

- Behavioural types for Go concurrency
- Infer types from Go source code
- Model check types for safety/liveness
- + termination for iterative Go code

Diagram:
- Go source code → Type inference
- SSA IR
- Behavioural types
- Transform and verify
- Model checking
- Termination checking

Nobuko Yoshida
Open Problems of Session Types
mrg.doc.ic.ac.uk
Future work

- Extend framework to support more properties
- Unlimited possibilities!
  - Different verification techniques
    - e.g. [POPL’17], Choreography synthesis [CC’15]
  - Different concurrency issues
    - Other synchronisation mechanisms
    - Race conditions