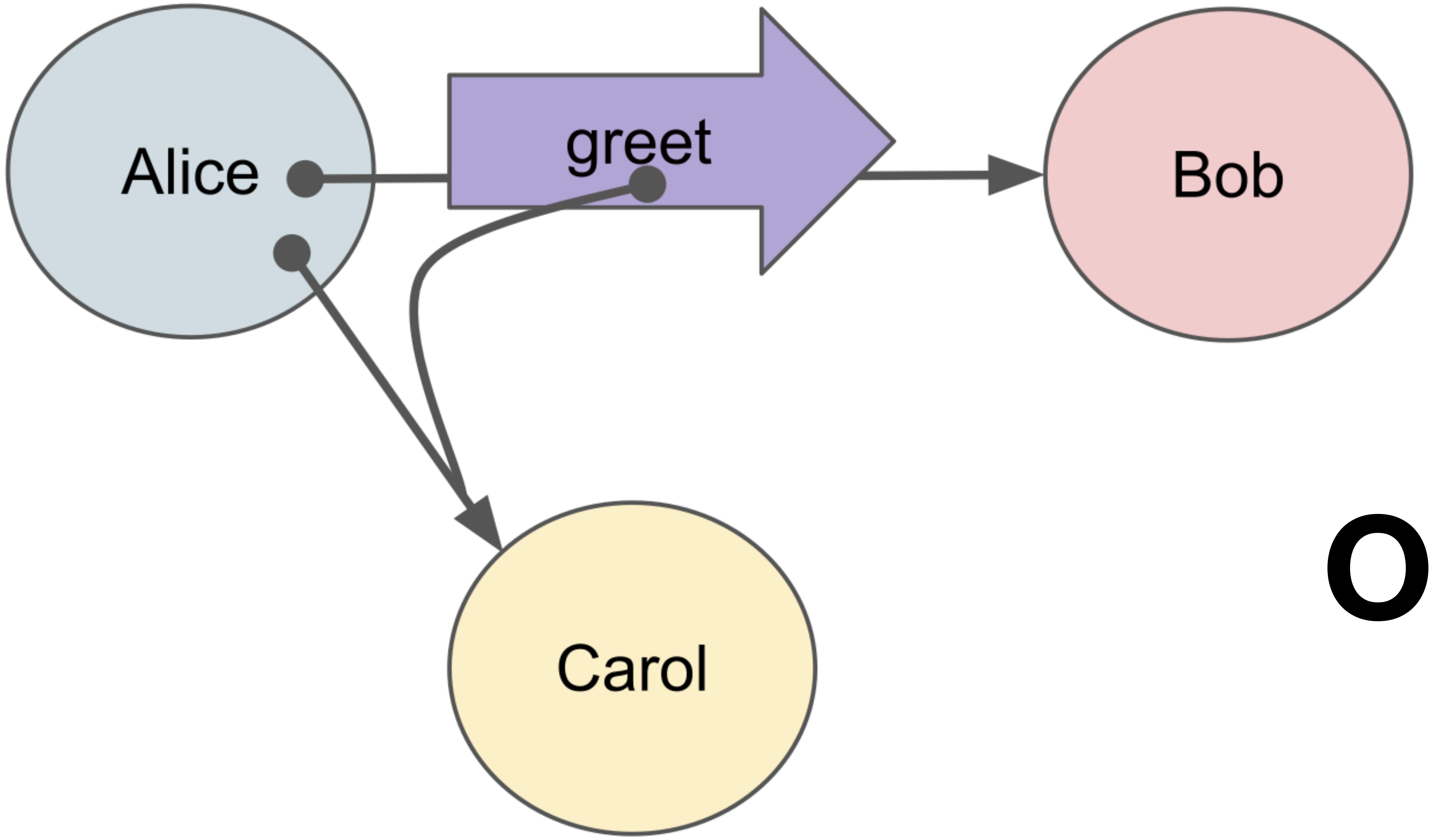


Reasoning with Object Capabilities

POCL 2024

James Noble

Susan Eisenbach

Julian Mackay

and in earlier works

Mark Miller

Toby Murray

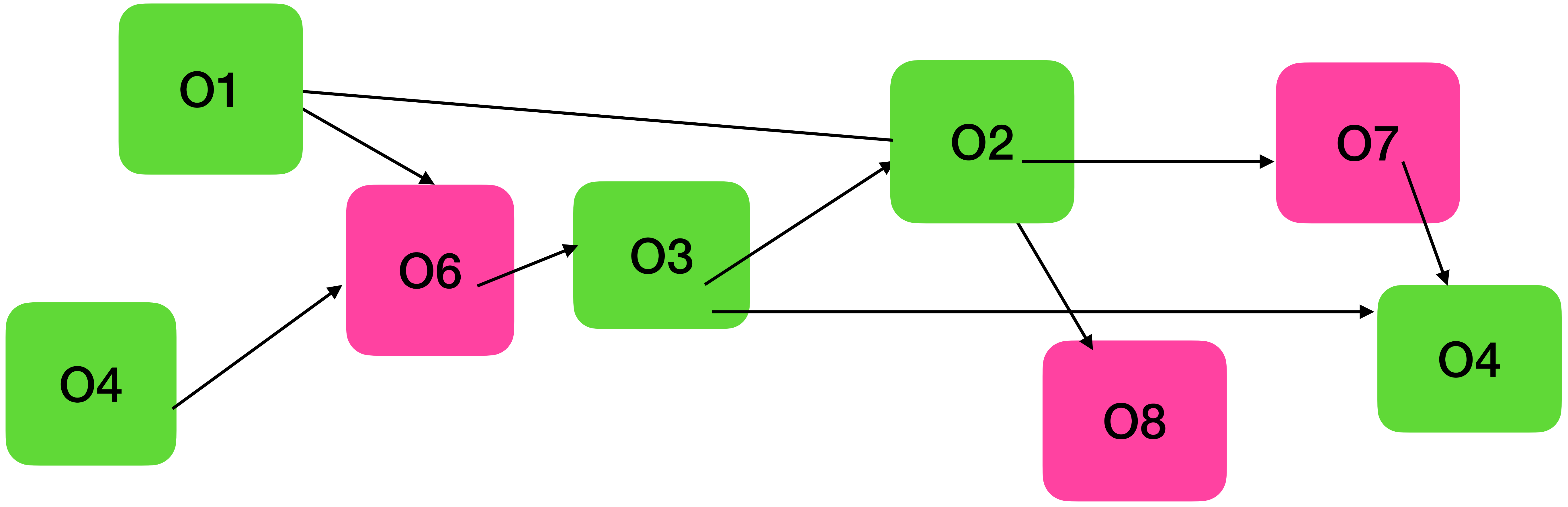
Our research Question

Reason about how our, internal, trusted objects can interact securely with the
external, untrusted, potentially malicious, objects. using object capabilities.

Literature:

*"A **capability** describes a transferable right to perform one (or more) operations."*

"References cannot be forged.
Capability transferred only through messages or through creation."



Literature:

“A capability describes a transferable right to perform one (or more) operations.”

“References cannot be forged. Capability transferred only through messages or through creation.”

Our Insights:

Capabilities are necessary conditions for *effects* (not operations)

Tracking access to capabilities is paramount.

Example
and
Four Challenges

Three Modules

.. assuming all methods are public, and fields are private

```
module Mod_good
  class Account
    field balance:int
    field pwd: Password
    method transfer(dest:Account, pwd':Password) -> void
      if this.pwd==pwd'
        this.balance-=100
        dest.balance+=100
     method init(pwd':Password) -> void
      if this.pwd==null
        this.pwd=pwd'
  class Password
```

```
module Mod_bad
  class Account
    field balance:int
    field pwd: Password
    method transfer(..) ...
      ... as earlier ...
    method init(...) ...
       ... as earlier ...
    method set(pwd': Password)
      this.pwd=pwd'

  class Password
```

```
module Mod_better
  class Account
    field balance:int
    field pwd: Password
    method transfer(..)
      ... as earlier ...

    method set(pwd',pwd'': Password)
      if (this.pwd==pwd')
        this.pwd=pwd''
  class Password
```

```
module Mod_good
  class Account
    field balance:int
    field pwd: Password
    method transfer(dest:Account, pwd':Password) ->
      if this.pwd==pwd'
        this.balance-=100
        dest.balance+=100
     method init(pwd':Password) -> void
      if this.pwd==null
        this.pwd=pwd'
  class Password
```

Challenge_1: A module spec S, such that

$$M_{good} \models S$$
$$M_{bad} \not\models S$$
$$M_{better} \models S$$

```
module Mod_bad
  class Account
    field balance:int
    field pwd: Password
    method transfer(..) ...
      ... as earlier ...
    method init(...) ...
       ... as earlier ...
    method set(pwd': Password)
      this.pwd=pwd'

  class Password
```

```
module Mod_better
  class Account
    field balance:int
    field pwd: Password
    method transfer(..)
      ... as earlier ...

    method set(pwd',pwd'': Password)
      if (this.pwd==pwd')
        this.pwd=pwd''
  class Password
```

```
module Mod_good
  class Account
    field balance:int
    field pwd: Password
    method transfer(dest:Account, pwd':Password) ->
      if this.pwd==pwd'
        this.balance-=100
        dest.balance+=100
     method init(pwd':Password) -> void
      if this.pwd==null
        this.pwd=pwd'
  class Password
```

Challenge_2: An inference system, such that

$$M_{good} \vdash S$$
$$M_{bad} \nvdash S$$
$$M_{better} \vdash S$$

```
module Mod_bad
  class Account
    field balance:int
    field pwd: Password
    method transfer(..) ...
      ... as earlier ...
    method init(...) ...
       ... as earlier ...
    method set(pwd': Password)
      this.pwd=pwd'

  class Password
```

```
module Mod_better
  class Account
    field balance:int
    field pwd: Password
    method transfer(..)
      ... as earlier ...


    method set(pwd',pwd'': Password)
      if (this.pwd==pwd')
        this.pwd=pwd''
  class Password
```

```
module Mod_good
  class Account
    field balance:int
    field pwd: Password
    method transfer(dest:Account, pwd':Password) ->
      if this.pwd==pwd'
        this.balance-=100
        dest.balance+=100
     method init(pwd':Password) -> void
      if this.pwd==null
        this.pwd=pwd'
  class Password
```

Challenge_3: Inference system should be algorithmic

```
module Mod_bad
  class Account
    field balance:int
    field pwd: Password
    method transfer(..) ...
      ... as earlier ...
    method init(...) ...
       ... as earlier ...
    method set(pwd': Password)
      this.pwd=pwd'

  class Password
```

```
module Mod_better
  class Account
    field balance:int
    field pwd: Password
    method transfer(..)
      ... as earlier ...

    method set(pwd',pwd'': Password)
      if (this.pwd==pwd')
        this.pwd=pwd''
  class Password
```

External call

```
class Shop

  fld myAccount : Account
  fld inventory : Inventory

  void buy(buyer: Object, anItem: Item)
    int price = anItem.price
    int oldBalance = this.myAccount.balance
    buyer.payMe(myAccount,price)
    if (this.myAccount.balance == oldBalance+price)
       this.send(buyer,anItem)
    else
       buyer.tell("you have not paid me")
```

Challenge_4: An inference system, such that we can prove **external** calls.

If `Account` comes from a "good" module,
and upon call, `buyer` has no eventual access to `myAccount.password`,

then
the balance of `myAccount` does not decrease by the call `payMe`.

Challenge_1: A module spec S, such that

$$M_{good} \models S$$
$$M_{bad} \not\models S$$
$$M_{better} \models S$$

Challenge_1: A module spec S, such that

$$M_{good} \models S$$
$$M_{bad} \not\models S$$
$$M_{better} \models S$$

Motto:
Capability is a *necessary* condition for some effect

Remember: A capability represents a transferable right to perform one or more operations on a given object

~~*So*: "The password enables withdrawal from the account"?~~

~~*Or*: "Without the password call of withdraw will fail"?~~

Or: "Without the password no reduction of the balance of the account"?

So: $\forall$ s:Statement. {without a.password $\wedge$ a.balance=b} s { a.balance >= b }

Challenge_1: A module spec S, such that …

So: $\forall$ s:Statement {without a.password $\wedge$ a.balance=b} s { a.balance >= b }

So: $\forall$ a: Account. $\forall$ n: Num. (| a.password **prt** $\wedge$ a.balance=b |) (| a.balance>=b |)

In general: $\forall$ x1:C1,x2:C2… (| A |) (| A’ |)

Challenge_1_a : Meaning of x **prt**

Challenge_1_b : Meaning of $\forall$ x1:C1,x2:C2… (| A |) (| A’ |)

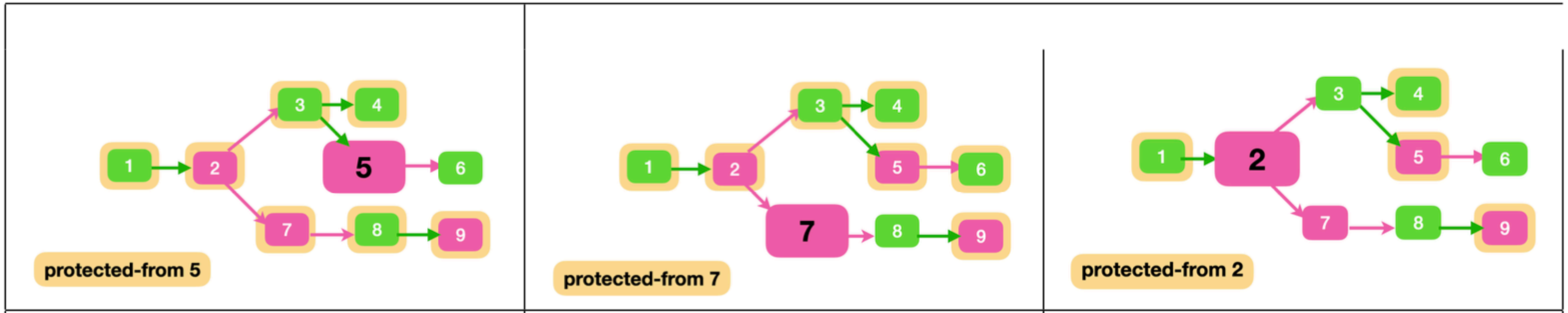
Challenge_1_a : Meaning of x **prt**

Remember:

…how our, internal, trusted objects will interact securely with the external, untrusted, potentially malicious, objects.

Def: **o prt-frm o’** Iff o=/=o’ and the penultimate object on any path from o’ to o is internal.

For example:



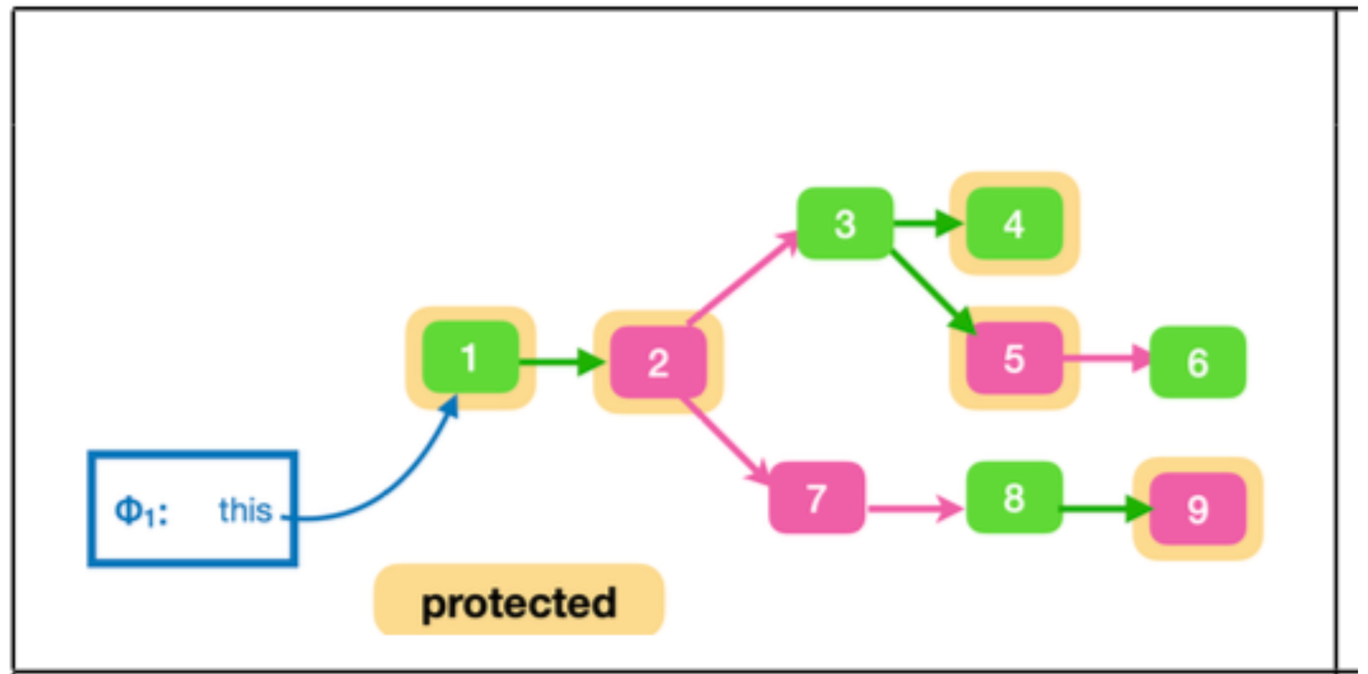
protected from o_5	protected from o_7	protected from o_2

Challenge_1_a : Meaning of x **prt**

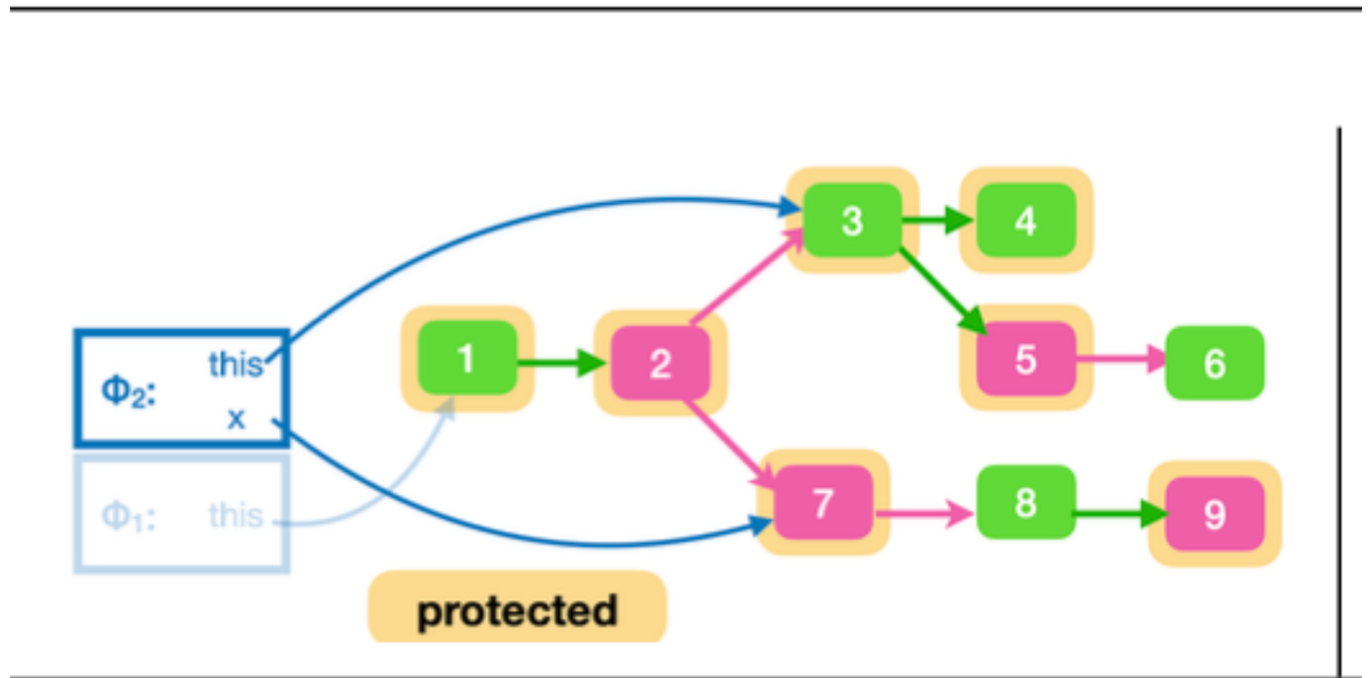
Def: o **prt-frm o'**, if **extr** o' and any path from o' to o goes through an internal object.

Def: o **prt** , if o **prt-from** any external object

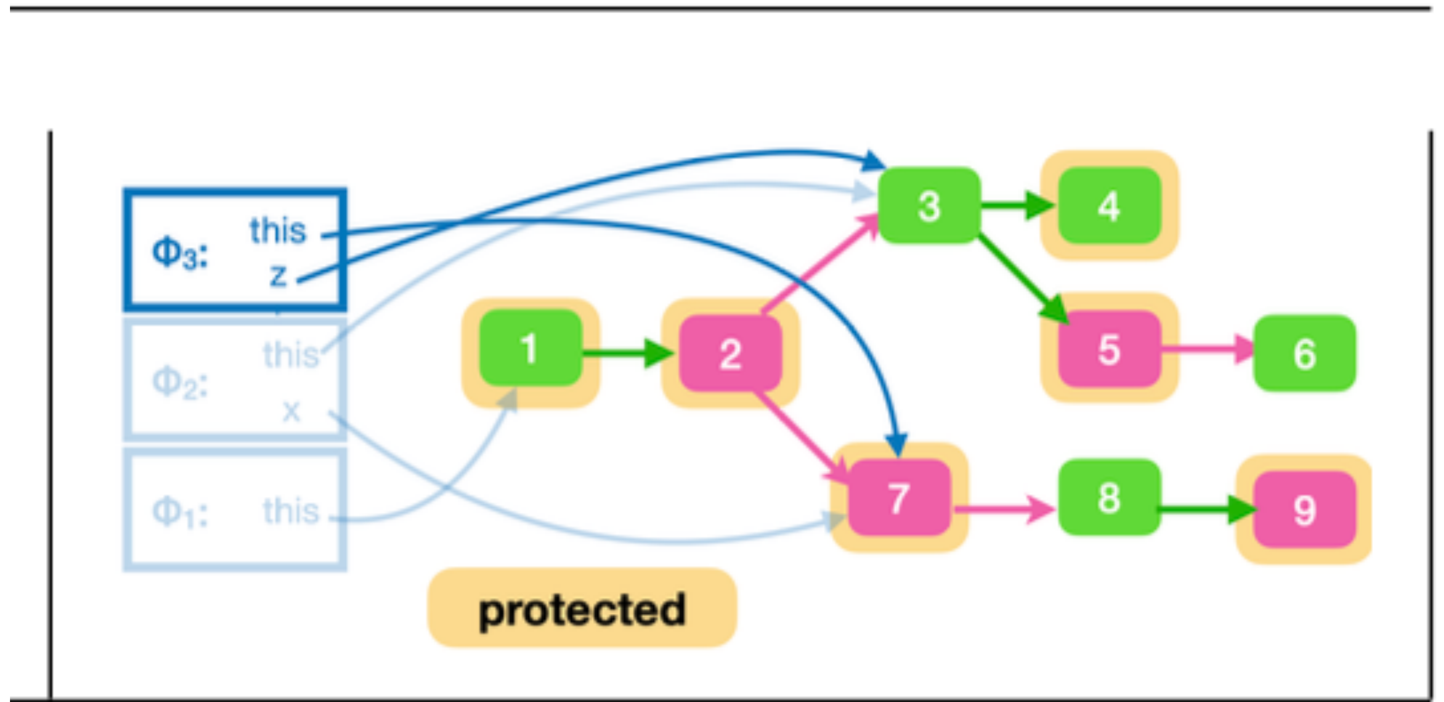
Motto:
Tracking access to Capabilities



protected with top frame ϕ_1



protected with top frame ϕ_2



protected with top frame ϕ_3

Challenge_1_b : Meaning of $\forall$ x1:C1,x2:C2… (| A |) (| A’ |)

Definition

M $\models$ $\forall$ x1:C1,x2:C2… (| A |) (| A’ |)

iff

For all modules M’,
For all states σ arising from execution of (M, M’) $\wedge$
For all objects o1, .. on globally accessible at σ of class C1, … Cn,
For all states σ’ in the future from σ whithout returning from σ ’s top frame,

If

M, σ $\models$ o1:C1 $\wedge$ … $\wedge$ on:Cn $\wedge$ A[o1/x1,… on/xn]

then

M, σ’ $\models$ A’[o1/x1,… on/xn]

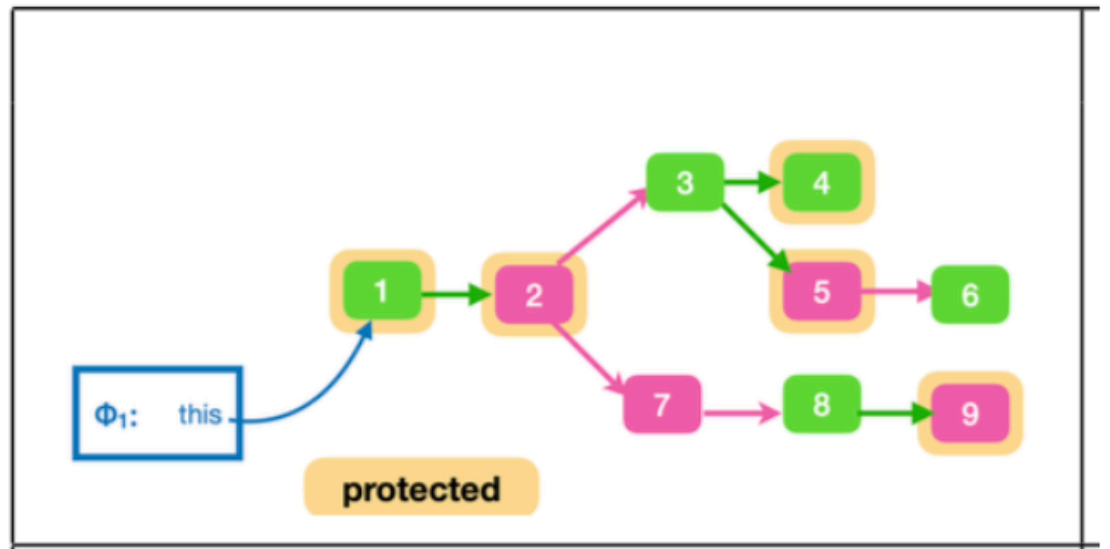
Putting it together

Therefore,

$$\forall\ x: \text{Object}\ (|\ \mathbf{prt}\ x\ \wedge A(x)\ |)\ (|\ A(x)\ |)$$

guarantees that

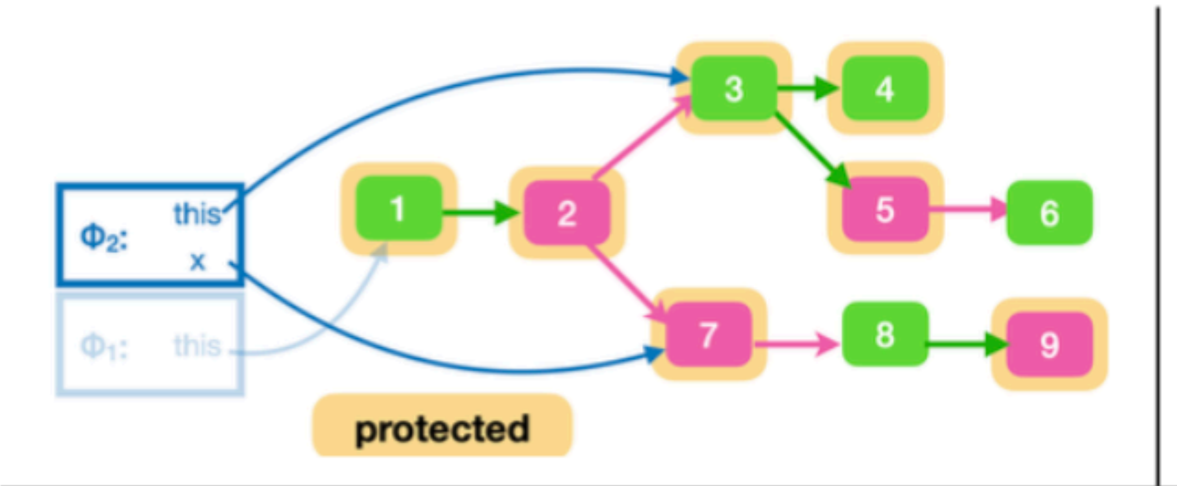
if we start below,



protected with top frame ϕ_1

then
A(o1), A(o2), A(o4),
A(o5), A(o9)
will be preserved

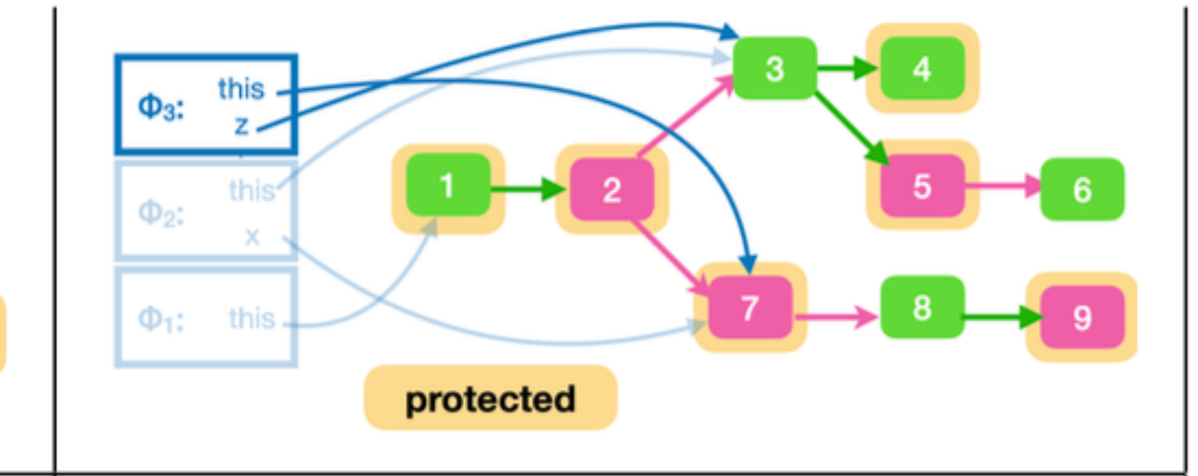
And if we start below,



protected with top frame ϕ_2

then
A(o1), A(o2), A(o3), A(o4),
A(o5), A(o7), A(o9)
will be preserved

And if we start below,



protected with top frame ϕ_3

then
A(o1), A(o2), A(o4),
A(o5), A(o7), A(o9)
will be preserved

Challenge_1: A module spec S, such that

$M_{good} \models S$

$M_{bad} \not\models S$

$M_{better} \models S$

API - agnostic:
a.balance, a.password can be ghost

Talks about effects

S = ∀ a:Account (| **prt** a |) (| **prt** a |)

∧

∀ a:Account (| **prt** a.password |) (| **prt** a.password |)

∧

∀ a:Account. ∀ b:Num (| **prt** a ∧ a.balance = b |) (| a.balance = b |)

∧

∀ a:Account. ∀ b:Num (| **prt** a.password ∧ a.balance = b |) (| a.balance ≥ b |)

Talks about emergent behaviour

Challenge_1: A module spec S, such that

$M_{good} \models S$

$M_{bad} \not\models S$

$M_{better} \models S$

$M_{better} \models \forall$ a:Account (| **prt** a |) (| **prt** a |)

$M_{better} \models \forall$ a:Account (| **prt** a.password |) (| **prt** a.password |)

$M_{better} \models \forall$ a:Account. $\forall$ b:Num (| **prt** a $\wedge$ a.balance = b |) (| a.balance = b |)

$M_{better} \models \forall$ a:Account. $\forall$ b:Num (| **prt** a.password $\wedge$ a.balance = b |) (| a.balance $\geq$ b |)

$M_{bad} \models \forall$ a:Account (| **prt** a |) (| **prt** a |)

$M_{bad} \not\models \forall$ a:Account (| **prt** a.password |) (| **prt** a.password |)

$M_{bad} \models \forall$ a:Account. $\forall$ b:Num (| **prt** a $\wedge$ a.balance = b |) (| a.balance = b |)

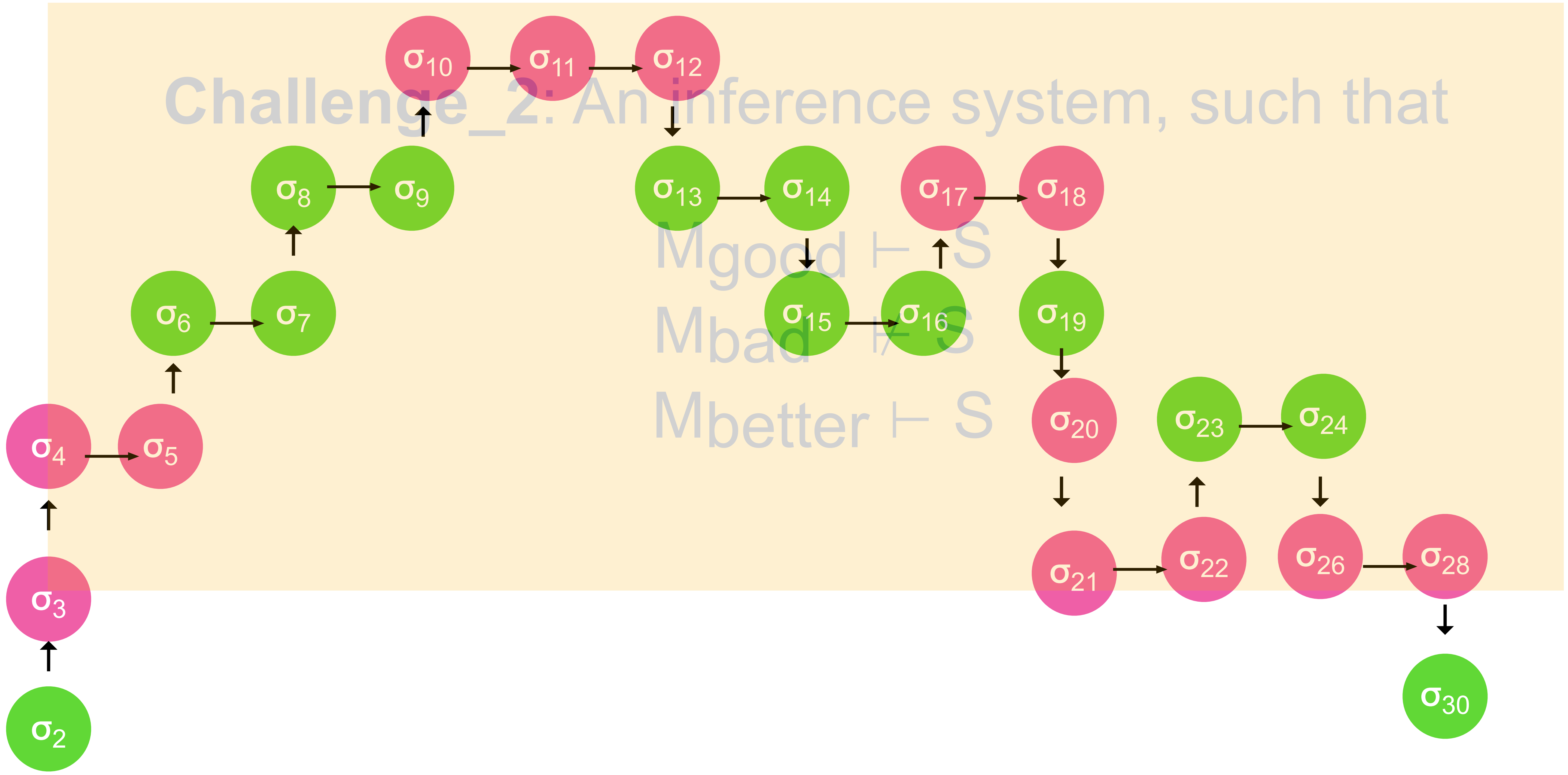
$M_{bad} \not\models \forall$ a:Account. $\forall$ b:Num (| **prt** a.password $\wedge$ a.balance = b |) (| a.balance $\geq$ b |)

Challenge_2: An inference system, such that

$$M_{good} \vdash S$$
$$M_{bad} \nvdash S$$
$$M_{better} \vdash S$$

Challenge_4: An inference system, such that we can prove external calls

In the context of arbitrary, unlimited calls from internal to external, and arbitrary, unlimited calls from external to internal,



Challenge_2/4: An inference system, such that …

An assertion A is **encapsulated** by module M, if
it can only be invalidated through calls to methods from M.

For example:

$$\texttt{Mod}_{\texttt{bad}} \models \mathit{Encaps}(\texttt{a}:\texttt{Account} \ \land \texttt{a.balance} = \texttt{bal})$$

$$\texttt{Mod}_{\texttt{better}} \models \mathit{Encaps}(\texttt{a}:\texttt{Account} \ \land \texttt{a.balance} = \texttt{bal})$$

Assume two further modules, Mod_{ul} and Mod_{pl}, which use ledgers to keep a map between accounts and their balances, which export functions that allow the update of this map. In Mod_{ul} the ledger is *not* protected, while in Mod_{pl} the ledger *is* protected.

$$Mod_{ul} \not\models \mathit{Encaps}(\texttt{a}:\texttt{Account} \ \land \texttt{a.balance} = \texttt{bal})$$

$$Mod_{pl} \models \mathit{Encaps}(\texttt{a}:\texttt{Account} \ \land \texttt{a.balance} = \texttt{bal})$$

Challenge_2/4: An inference system, such that …

$$\textsc{Module\_Well\_Formed}$$

$$\dfrac{\begin{array}{l}\forall D \in M, m \textit{ with } \texttt{mBody}(m, D, M) = \overline{y : D}\{\ s\ \} \\ \quad m \textit{ private} \\ \qquad \textit{for all its specs } A_{pre}, A_{post}: \\ \qquad\qquad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \} \\ \quad m \textit{ public} \\ \qquad\qquad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge \quad ??? \quad \}\ s\ \{\quad ??? \quad \} \\ \qquad \textit{and for all its specs } A_{pre}, A_{post}: \\ \qquad\qquad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge \quad ??? \quad \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \}\end{array}}{\vdash M}$$

Challenge_2/4: An inference system, such that …

$$\textsc{Module\_Well\_Formed}$$

$$\frac{\begin{array}{l} \forall D \in M, m \textit{ with } \texttt{mBody}(m, D, M) = \overline{y : D}\{\ s\ \} \\ \quad m \textit{ private} \\ \quad\quad \textit{for all its specs } A_{pre}, A_{post} : \\ \quad\quad\quad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \} \\ \quad m \textit{ public} \\ \quad\quad\quad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge \mathscr{I}nvs(M)\ ??\ \}\ s\ \{\ \mathscr{I}nvs(M)\ ??\ \} \\ \quad\quad \textit{and for all its specs } A_{pre}, A_{post} : \\ \quad\quad\quad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge \mathscr{I}nvs(M)\ ??\ \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \} \end{array}}{\vdash\ M}$$

$$\begin{array}{lcl} \mathscr{I}nvs(\forall \overline{x : C}.(\!|\, A \,|\!)) & \triangleq & \forall \overline{x}.[\ \overline{x : C} \to A\ ] \\ \mathscr{I}nvs(\forall \overline{x : C}.(\!|\, A \,|\!)(\!|\, A \,|\!)) & \triangleq & \overline{x : C} \wedge A \\ \mathscr{I}nvs(S_1 \wedge S_2) & \triangleq & \mathscr{I}nvs(S_1)\ \wedge S_2\ \mathscr{I}nvs(S_2) \\ \mathscr{I}nvs(M) & \triangleq & \mathscr{I}nvs(HS(M)) \end{array}$$

Challenge_2/4: An inference system, such that …

$$\textsc{Module\_Well\_Formed}$$

$$\frac{\begin{array}{l} \forall D \in M, m \textit{ with } \texttt{mBody}(m, D, M) = \overline{y : D}\{\, s \,\} \\ \quad m \textit{ private} \\ \quad\quad \textit{for all its specs } A_{pre}, A_{post} : \\ \quad\quad\quad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \} \\ \quad m \textit{ public} \\ \quad\quad\quad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge \mathscr{I}nvs(M) \mathrel{-\!\!\triangledown} \overline{y}\ \}\ s\ \{\ \mathscr{I}nvs(M) \mathrel{-\!\!\triangledown} \overline{y}\ \} \\ \quad\quad \textit{and for all its specs } A_{pre}, A_{post} : \\ \quad\quad\quad M \vdash \{\ \texttt{this} : \texttt{D} \wedge \overline{y : D} \wedge \mathscr{I}nvs(M) \mathrel{-\!\!\triangledown} \overline{y} \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \} \end{array}}{\vdash\ M}$$

$$\begin{array}{rcl} (\,\mathbf{prt}\ e\,) \mathrel{-\!\!\triangledown} \overline{y} & \triangleq & e\ \mathbf{prt\text{–}frm}\ \overline{y} \\ (\,e\ \mathbf{prt\text{–}frm}\ \overline{u}) \mathrel{-\!\!\triangledown} \overline{y} & \triangleq & e\ \mathbf{prt\text{–}frm}\ \overline{u} \\ (\,\mathbf{intl}\ e\,) \mathrel{-\!\!\triangledown} \overline{y} & \triangleq & \mathbf{intl}\ e \\ e \mathrel{-\!\!\triangledown} \overline{y} & \triangleq & e \end{array} \qquad \begin{array}{rcl} (A_1 \wedge A_2) \mathrel{-\!\!\triangledown} \overline{y} & \triangleq & (A_1 \mathrel{-\!\!\triangledown} \overline{y}) \wedge (A_2 \mathrel{-\!\!\triangledown} \overline{y}) \\ (\forall x : C.A) \mathrel{-\!\!\triangledown} \overline{y} & \triangleq & \forall x : C.(A \mathrel{-\!\!\triangledown} \overline{y}) \\ (\neg A) \mathrel{-\!\!\triangledown} \overline{y} & \triangleq & \neg(A \mathrel{-\!\!\triangledown} \overline{y}) \\ (e : C) \mathrel{-\!\!\triangledown} \overline{y} & \triangleq & e : C \end{array}$$

Challenge_2/4: An inference system, such that …

$$\dfrac{\begin{array}{l} \forall D \in M, m \textit{ with } \texttt{mBody}(m, D, M) = \overline{y : D}\{\ s\ \} \\ \quad m \textit{ private} \\ \quad\quad \textit{for all its specs } A_{pre}, A_{post}: \\ \quad\quad\quad M \vdash \{\ \texttt{this}:\texttt{D} \wedge \overline{y : D} \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \} \\ \quad m \textit{ public} \\ \quad\quad\quad M \vdash \{\ \texttt{this}:\texttt{D} \wedge \overline{y : D} \wedge \mathscr{I}nvs(M) \,\neg\nabla \overline{y}\ \}\ s\ \{\ \mathscr{I}nvs(M) \,\neg\nabla \overline{y}\ \} \\ \quad\quad \textit{and for all its specs } A_{pre}, A_{post}: \\ \quad\quad\quad M \vdash \{\ \texttt{this}:\texttt{D} \wedge \overline{y : D} \wedge \mathscr{I}nvs(M) \,\neg\nabla \overline{y} \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \} \end{array}}{\vdash\ M} \ \text{MODULE\_WELL\_FORMED}$$

LEMMA 3.6. *For any states σ, σ', assertion A, addresses $\overline{\alpha}$, variables $\overline{x}$, $\overline{y}$, $\overline{z}$ disjoint with one another, and such that $fv(A) \subseteq \overline{x}$:*

(1) $M, \sigma[\overline{x \mapsto \alpha}] \models A \,\neg\nabla \overline{y} \quad \Longrightarrow \quad M,\ (\sigma[\overline{x \mapsto \alpha}]) \nabla \overline{y} \models A$

(2) $M, ((\sigma[\overline{x \mapsto \alpha}]) \nabla (\overline{y}, \overline{z})) \models A \quad \Longrightarrow \quad M, \sigma[\overline{x \mapsto \alpha}] \models A \,\neg\nabla \overline{y}$

Challenge_2/4: An inference system, such that …

$$\frac{\begin{array}{l}\forall D \in M, m \textit{ with } \mathtt{mBody}(m, D, M) = \overline{y : D}\{\ s\ \} \\ \quad m \textit{ private} \\ \qquad \textit{for all its specs } A_{pre}, A_{post} : \\ \qquad\qquad M \ \vdash \{\ \mathtt{this}:\mathtt{D} \wedge \overline{y : D} \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \} \\ \quad m \textit{ public} \\ \qquad\qquad M \ \vdash \{\ \mathtt{this}:\mathtt{D} \wedge \overline{y : D} \wedge \mathscr{I}nvs(M) \nabla \overline{y}\}\ s\ \{\ \mathscr{I}nvs(M) \nabla \overline{y}\} \\ \qquad \textit{and for all its specs } A_{pre}, A_{post} : \\ \qquad\qquad M \ \vdash \{\ \mathtt{this}:\mathtt{D} \wedge \overline{y : D} \wedge \mathscr{I}nvs(M) \nabla \overline{y} \wedge A_{pre}\ \}\ s\ \{\ A_{post}\ \}\end{array}}{\vdash\ M}\ \textsc{Module\_Well\_Formed}$$

$$\textsc{Weaken}\quad \frac{M \vdash S \qquad M \vdash S \sqsubseteq S'}{M \vdash S'} \qquad\qquad \textsc{Multi}\quad \frac{M \ \vdash\ S \qquad M \ \vdash\ S'}{M \ \vdash\ S \wedge S'}$$

Challenge_2/4: … prove method bodies ….

EXTEND

$$\frac{M \vdash_{ul} \{\, A \,\}\; s \;\{\, A' \,\}}{M \;\vdash\; \{\, A \,\}\; s \;\{\, A' \,\}}$$

COMBINE

$$\frac{M \;\vdash\; \{\, A_1 \,\}\; s \;\{\, A_1' \,\} \quad M \;\vdash\; \{\, A_2 \,\}\; s \;\{\, A_2' \,\}}{M \;\vdash\; \{\, A_1 \wedge A_2 \,\}\; s \;\{\, A_1' \wedge A_2' \,\}}$$

SEQU

$$\frac{M \;\vdash\; \{\, A \,\}\; s_1 \;\{\, A'' \,\} \quad M \;\vdash\; \{\, A'' \,\}\; s_2 \;\{\, A' \,\}}{M \;\vdash\; \{\, A \,\}\; s_1;\; s_2 \;\{\, A' \,\}}$$

CONSEQU

$$\frac{M \vdash A \to A'' \quad M \;\vdash\; \{\, A'' \,\}\; s \;\{\, A''' \,\} \quad M \vdash A''' \to A'}{M \;\vdash\; \{\, A \,\}\; s \;\{\, A' \,\}}$$

[IntCall_WithSpec]

$$\frac{M, C, m : (\, A_1,\; A_2 \,) \qquad fv(A_1) = \overline{x}}{M \;\vdash\; \{\;\; \mathbf{intl}\, y_0 \wedge y : C \;\wedge\; A_1[\overline{y}/\mathtt{this}, \overline{x}] \;\;\}\; u := y_0.m(y_1, ..y_n)\; \{\;\; A_2[u/result, \overline{y}/\mathtt{this}, \overline{x}] \;\;\}}$$

Challenge_2/4: …. prove external calls

[CallAndAlias

$$\frac{x \overset{\text{txt}}{\neq} u \overset{\text{txt}}{\neq} x'}{M \vdash \{\ x = x' \ \wedge \ (\,\textbf{extl}\, y_0 \ \longrightarrow \ \mathscr{I}nvs(M) \,\text{-}\nabla \overline{y})\ \}\, u := y_0.m(y_1, ..y_n)\ \{\ x = x'\ \}}$$

[CallNonAlias]

$$\frac{x \overset{\text{txt}}{\neq} u \overset{\text{txt}}{\neq} x'}{M \vdash \{\ x \neq x' \ \wedge \ (\,\textbf{extl}\, y_0 \ \longrightarrow \ \mathscr{I}nvs(M) \,\text{-}\nabla \overline{y})\ \}\, u := y_0.m(y_1, ..y_n))\ \{\ x \neq x'\ \}}$$

Challenge_2/4: …. prove external calls

[ExtCal]

$$\frac{}{M \vdash \{ \ \textbf{extl}\, y_0 \ \wedge \ \mathscr{I}nvs(M) \,\text{-}\!\nabla \overline{y} \ \} \ u := y_0.m(y_1, ..y_n) \ \{ \ \mathscr{I}nvs(M) \,\text{-}\!\nabla \overline{y} \ \}}$$

Challenge_2/4: …. prove external calls

[ExtCall_WithSpec_Weak]

$$\frac{\vdash\ M\ :\ \qquad ???}{M\ \vdash\ \{\ \mathbf{extl}\, y_0\ \wedge\ \overline{x:C}\ \wedge\ \ ???\ \ \wedge\ \mathscr{I}nvs(M) \nabla \overline{y}\ \}\ u := y_0.m(y_1,..y_n)\ \{\ \ ???\ \ \}}$$

Motto:
Capability is a *necessary* condition for some effect

Challenge_2/4: …. prove external calls

[ExtCall_WithSpec_Strong]

$$\dfrac{\vdash \;\; M \; : \; \forall \overline{x : C}.\llparenthesis\, A_1 \,\rrparenthesis \llparenthesis\, A_2 \,\rrparenthesis}{M \;\vdash\; \{\;\; \mathbf{extl}\, y_0 \;\; \wedge \; \overline{x : C} \; \wedge \; A_1 \mathbin{-\!\nabla} \overline{y} \; \wedge \; \text{???} \; \wedge \; \mathscr{I}nvs(M) \mathbin{-\!\nabla} \overline{y} \;\; \} \; u := y_0.m(y_1, ..y_n) \; \{ \;\; A_2 \mathbin{-\!\nabla} \overline{y} \;\;\; \text{???} \;\; \}}$$

Motto:
Capability is a *necessary* condition
for some effect

Challenge_2/4: …. prove external calls

[ExtCall_WithSpec_Strong]

$$\frac{\vdash\ M\ :\ \forall \overline{x:C}.(\!|\, A_1 \,|\!)(\!|\, A_2 \,|\!)}{M\ \vdash\ \{\ \textbf{extl}\, y_0\ \wedge\ \overline{x:C}\ \wedge\ A_1 \mathbin{-\!\nabla} \overline{y}\ \wedge\ A_1\ \wedge\ \mathscr{I}nvs(M) \mathbin{-\!\nabla} \overline{y}\ \}\ u := y_0.m(y_1, ..y_n)\ \{\ A_2 \mathbin{-\!\nabla} \overline{y}\ \wedge\ A_2\ \}}$$

Motto:
Capability is a *necessary* condition
for some effect

Challenge_2/4: …. Revisiting the Shop exam

External call

```
class Shop

   fld myAccount : Account
   fld inventory : Inventory

   void buy(buyer: Object, anItem: Item)
     int price = anItem.price
     int oldBalance = this.myAccount.balance
     buyer.payMe(myAccount,price)
     if (this.myAccount.balance == oldBalance+price)
        this.send(buyer,anItem)
     else
        buyer.tell("you have not paid me")
```

🤔🤔 this spec is implied 🤔🤔

Of course, we have to prove that `buy` preserves `Banking's` spec (as per rule Module_Well_Fomed)

`Shop` part of `Banking` module;
`buy` a public method of `Shop`.

`buy` possible spec

PRE: `myAccount.balance=b && this.inventory = list`
POST: `myAccount.balance=b+anItem.price`
`—> this.inventory = list\anItem`

`buy` satisfies **implicitly**

PRE: `this.myAccount.passdw` **`prt-frm`** `buyer && this.myAccount.balance==b`
POST: `this.myAccount.balance >= b`

This spec *derivable* from the `Banking` spec

Challenge_3: The inference system should be algorithmic

Happy!

Convinced!

Surprised!

Summary

- Distinction between external/internal objects

- Specifications talk about necessary conditions for effect:

  $\forall$ x: Object (| **denial of capability** $\wedge$ A |) (| A |)

  means that **capability** is needed in order to invalidate A

- **prt** x: expresses that capability x is protected from external objects

- Design "Fineties"
  - **prt** x — only protects from *locally-relevant* objects;
  - $\forall$ x: ..(|..|)(|…|) — tallks about *globally-relevant* objects
  - "future is shallow"

- API-agrnositc spec, "Algorithmic" inference system system, open calls

- Hand-written soundness and adherence proof

Happy!

Convinced:

Object capabilities are about necessary conditions for effects caused by external objects.

Surprised!

Happy!

Convinced!

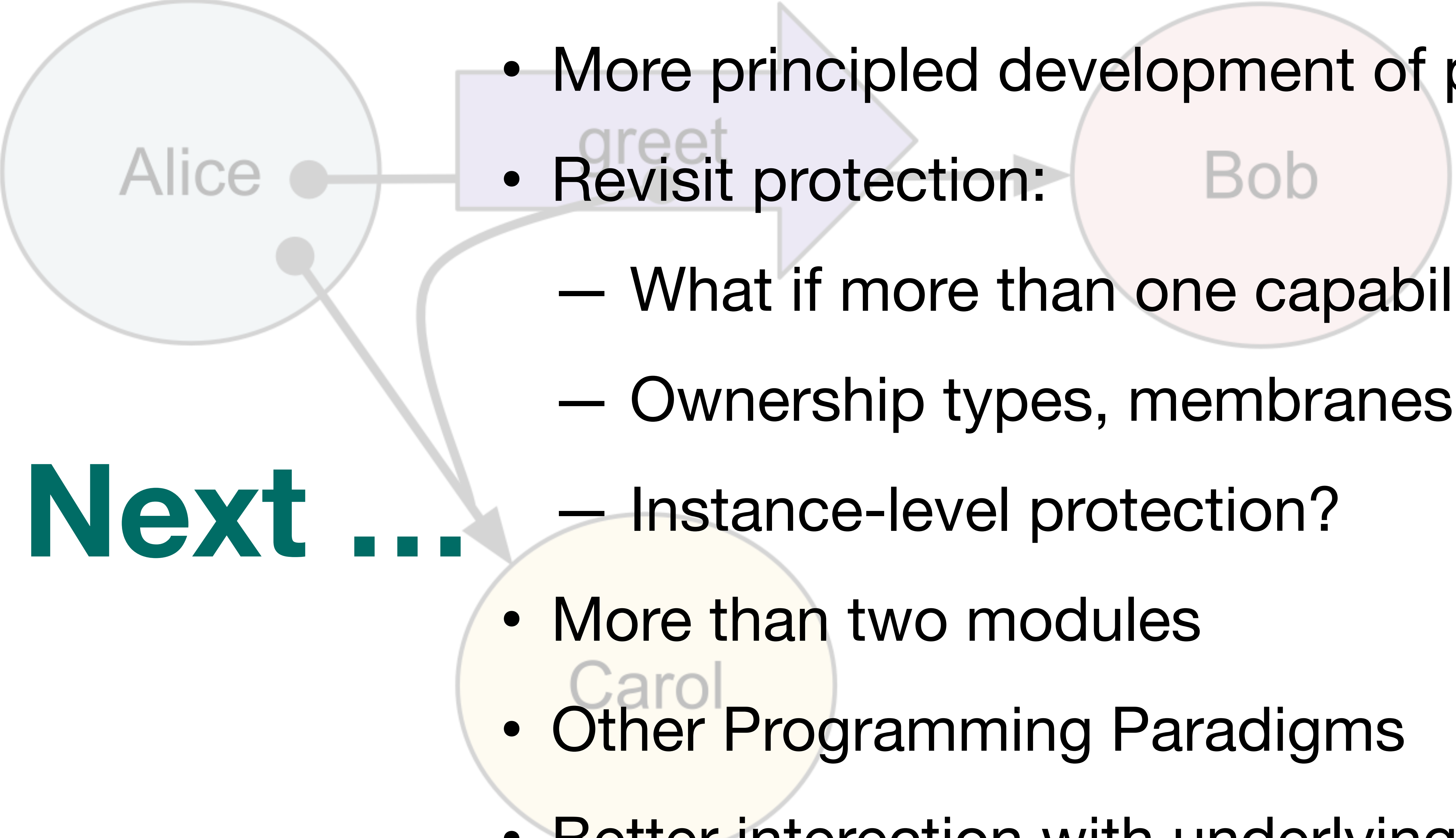
Surprised:

* talk about *necessary* conditions, but reason with *sufficient* conditions.

* No need for temporal logic specifications.

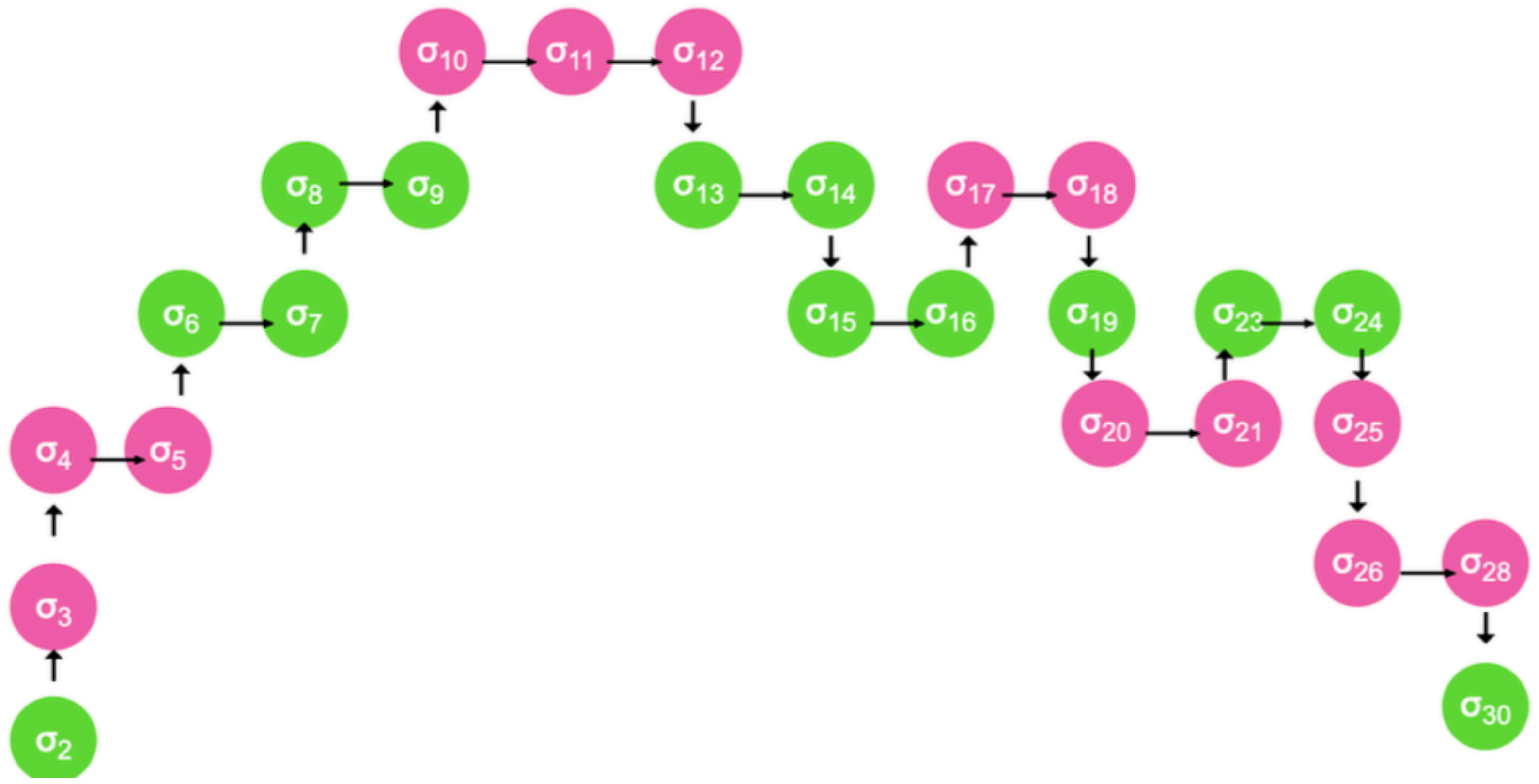
* Hoare-logic extension

Next …



- Smooth the edges
- Mechanize proofs
- Completeness?
- Adversarial logic
- More principled development of ptr-Hoare rules
- Revisit protection:
  — What if more than one capability for an effect?
  — Ownership types, membranes etc?
  — Instance-level protection?
- More than two modules
- Other Programming Paradigms
- Better interection with underlying Hoare logics, esp. “modifies” clauses, *
- Parametric with language and Hoare Logic
- Inference of Classic Specs given Invariants
- Tool

the original execution:



the summarised execution: