Recalling a Witness

Foundations and Applications of Monotonic State

Danel Ahman

Prosecco Team at Inria Paris

joint work with

Cătălin Hrițcu and Kenji Maillard @ Inria Paris

Cédric Fournet, Aseem Rastogi, and Nikhil Swamy @ MSR

HOPE 2017

September 3, 2017

Outline

- Monotonic state and program verification by example
- Overview of our solution (a simple, general interface)
- Extending F* with our monotonic state interface
- Example uses of monotonicity
- A glimpse of the meta-theory

Outline

- Monotonic state and program verification by example
- Overview of our solution (a simple, general interface)
- Extending F* with our monotonic state interface
- Example uses of monotonicity
- A glimpse of the meta-theory

Monotonic state and program verification

- Consider a program operating on **set-valued state**

$$\texttt{insert v; complex\_procedure(); assert (v} \in \texttt{get())}$$

- To prove the assertion (say, in a Floyd-Hoare style logic), we could prove that the code maintains a **stateful invariant**

$$\{\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}\}\ \texttt{complex\_procedure()}\ \{\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}\}$$

  - likely that we have to **carry** $\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}$ **through** the proof of c_p
    - sensitive to proving that c_p maintains $\lambda\, \texttt{s}\,.\, \texttt{w} \in \texttt{s}$ for some other w
    - does not guarantee that $\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}$ holds at every point in c_p

- However, if c_p **only inserts**, then $\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}$ is **stable**, and we would like the program logic to give us $\texttt{v} \in \texttt{get()}$ "**for free**"

Monotonic state and program verification

- Consider a program operating on **set-valued state**

$$\texttt{insert v; complex\_procedure(); assert } (\texttt{v} \in \texttt{get()})$$

- To prove the assertion (say, in a Floyd-Hoare style logic),
  we could prove that the code maintains a **stateful invariant**

$$\{\lambda\, \texttt{s}\, .\, \texttt{v} \in \texttt{s}\}\ \texttt{complex\_procedure()}\ \{\lambda\, \texttt{s}\, .\, \texttt{v} \in \texttt{s}\}$$

  - likely that we have to **carry** $\lambda\, \texttt{s}\, .\, \texttt{v} \in \texttt{s}$ **through** the proof of c_p
    - sensitive to proving that c_p maintains $\lambda\, \texttt{s}\, .\, \texttt{w} \in \texttt{s}$ for some other $\texttt{w}$
    - does not guarantee that $\lambda\, \texttt{s}\, .\, \texttt{v} \in \texttt{s}$ holds at every point in c_p

- However, if c_p **only inserts**, then $\lambda\, \texttt{s}\, .\, \texttt{v} \in \texttt{s}$ is **stable**, and
  we would like the program logic to give us $\texttt{v} \in \texttt{get()}$ "**for free**"

Monotonic state and program verification

- Consider a program operating on **set-valued state**

$$\texttt{insert v; complex\_procedure(); assert} \; (\texttt{v} \in \texttt{get()})$$

- To prove the assertion (say, in a Floyd-Hoare style logic), we could prove that the code maintains a **stateful invariant**

$$\{\lambda\,\texttt{s}\,.\,\texttt{v} \in \texttt{s}\}\ \texttt{complex\_procedure()}\ \{\lambda\,\texttt{s}\,.\,\texttt{v} \in \texttt{s}\}$$

  - likely that we have to **carry** $\lambda\,\texttt{s}\,.\,\texttt{v} \in \texttt{s}$ **through** the proof of c_p
    - sensitive to proving that c_p maintains $\lambda\,\texttt{s}\,.\,\texttt{w} \in \texttt{s}$ for some other w
    - does not guarantee that $\lambda\,\texttt{s}\,.\,\texttt{v} \in \texttt{s}$ holds at every point in c_p

- However, if c_p **only inserts**, then $\lambda\,\texttt{s}\,.\,\texttt{v} \in \texttt{s}$ is **stable**, and we would like the program logic to give us $\texttt{v} \in \texttt{get()}$ "**for free**"

Monotonic state and program verification

- Consider a program operating on **set-valued state**

$$\texttt{insert v; complex\_procedure(); assert (v} \in \texttt{get())}$$

- To prove the assertion (say, in a Floyd-Hoare style logic), we could prove that the code maintains a **stateful invariant**

$$\{\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}\}\ \texttt{complex\_procedure()}\ \{\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}\}$$

  - likely that we have to **carry** $\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}$ **through** the proof of c_p
    - sensitive to proving that c_p maintains $\lambda\, \texttt{s}\,.\, \texttt{w} \in \texttt{s}$ for some other w
    - does not guarantee that $\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}$ holds at every point in c_p

- However, if c_p **only inserts**, then $\lambda\, \texttt{s}\,.\, \texttt{v} \in \texttt{s}$ is **stable**, and we would like the program logic to give us $\texttt{v} \in \texttt{get()}$ "**for free**"

Other, more substantial examples

- To come later in this talk
  - reasoning about **monotonic counters**
  - using monotonicity to implement **typed** and **untyped references**
  - more flexibility with **monotonic references**
- For other examples of the usefulness of monotonicity,

  Recalling a Witness:
  Foundations and Applications of Monotonic State

  (arXiv:1707.02466)

  which includes
  - a secure **file-transfer** application
  - Ariadne **state continuity** protocol [Strackx, Piessens 2016]
  - pointers to works using monotonicity in **crypto** and **TLS verif.**

Other, more substantial examples

- To come later in this talk
  - reasoning about **monotonic counters**
  - using monotonicity to implement **typed** and **untyped references**
  - more flexibility with **monotonic references**

- For other examples of the usefulness of monotonicity,

  Recalling a Witness:
  Foundations and Applications of Monotonic State
  (arXiv:1707.02466)

  which includes
  - a secure **file-transfer** application
  - Ariadne **state continuity** protocol [Strackx, Piessens 2016]
  - pointers to works using monotonicity in **crypto** and **TLS verif.**

Other, more substantial examples

- To come later in this talk
  - reasoning about **monotonic counters**
  - using monotonicity to implement **typed** and **untyped references**
  - more flexibility with **monotonic references**

- For other examples of the usefulness of monotonicity,

  Recalling a Witness:
  Foundations and Applications of Monotonic State

  (arXiv:1707.02466)

  which includes

  - a secure **file-transfer** application
  - Ariadne **state continuity** protocol [Strackx, Piessens 2016]
  - pointers to works using monotonicity in **crypto** and **TLS verif.**

Outline

- Monotonic state and program verification by example
- Overview of our solution (a simple, general interface)
- Extending F* with our monotonic state interface
- Example uses of monotonicity
- A glimpse of the meta-theory

Overview of our solution

- We focus on **monotonic** programs and **stable** predicates
  - per verification task, we choose a **preorder** `rel` on states
    - set inclusion, heap inclusion, increasing counters, ...
  - a program e is **monotonic** (wrt. `rel`) when

$$(s, e) \rightsquigarrow^* (s', e') \implies \mathtt{rel}\ s\ s'$$

  - a predicate p on states is **stable** (wrt. `rel`) when

$$\forall\, s\, s'.\ p\ s\ \wedge\ \mathtt{rel}\ s\ s' \implies p\ s'$$

- **Our solution:** extend Hoare-style program logics (e.g., F*) with
  - means for turning a p into a **state-independent proposition**
  - operation to **witness** the validity of p s in some state s
  - operation to **recall** the validity of p s′ in a future state s′
- Gives a **general account** of examples already in use in F*

Overview of our solution

- We focus on **monotonic** programs and **stable** predicates
  - per verification task, we choose a **preorder** `rel` on states
    - set inclusion, heap inclusion, increasing counters, ...
  - a program e is **monotonic** (wrt. `rel`) when

$$(\mathrm{s}, \mathrm{e}) \leadsto^* (\mathrm{s}', \mathrm{e}') \implies \texttt{rel}\ \mathrm{s}\ \mathrm{s}'$$

  - a predicate p on states is **stable** (wrt. `rel`) when

$$\forall\, \mathrm{s}\, \mathrm{s}'.\ \mathtt{p}\ \mathrm{s}\ \wedge\ \texttt{rel}\ \mathrm{s}\ \mathrm{s}' \implies \mathtt{p}\ \mathrm{s}'$$

- **Our solution:** extend Hoare-style program logics (e.g., F*) with
  - means for turning a p into a **state-independent proposition**
  - operation to **witness** the validity of p s in some state s
  - operation to **recall** the validity of p s′ in a future state s′
- Gives a **general account** of examples already in use in F*

Overview of our solution

- We focus on **monotonic** programs and **stable** predicates
  - per verification task, we choose a **preorder** `rel` on states
    - set inclusion, heap inclusion, increasing counters, ...
  - a program $\mathtt{e}$ is **monotonic** (wrt. `rel`) when

$$(\mathtt{s}, \mathtt{e}) \rightsquigarrow^* (\mathtt{s}', \mathtt{e}') \implies \mathtt{rel}\ \mathtt{s}\ \mathtt{s}'$$

  - a predicate $\mathtt{p}$ on states is **stable** (wrt. `rel`) when

$$\forall\, \mathtt{s}\, \mathtt{s}'.\ \mathtt{p}\ \mathtt{s}\ \wedge\ \mathtt{rel}\ \mathtt{s}\ \mathtt{s}' \implies \mathtt{p}\ \mathtt{s}'$$

- **Our solution:** extend Hoare-style program logics (e.g., F*) with
  - means for turning a $\mathtt{p}$ into a **state-independent proposition**
  - operation to **witness** the validity of $\mathtt{p}\ \mathtt{s}$ in some state $\mathtt{s}$
  - operation to **recall** the validity of $\mathtt{p}\ \mathtt{s}'$ in a future state $\mathtt{s}'$
- Gives a **general account** of examples already in use in F*

Overview of our solution

- We focus on **monotonic** programs and **stable** predicates
  - per verification task, we choose a **preorder** `rel` on states
    - set inclusion, heap inclusion, increasing counters, ...
  - a program e is **monotonic** (wrt. `rel`) when

$$(\mathtt{s}, \mathtt{e}) \rightsquigarrow^* (\mathtt{s}', \mathtt{e}') \implies \mathtt{rel}\ \mathtt{s}\ \mathtt{s}'$$

  - a predicate p on states is **stable** (wrt. `rel`) when

$$\forall\, \mathtt{s}\ \mathtt{s}'.\ \mathtt{p}\ \mathtt{s}\ \wedge\ \mathtt{rel}\ \mathtt{s}\ \mathtt{s}' \implies \mathtt{p}\ \mathtt{s}'$$

- **Our solution:** extend Hoare-style program logics (e.g., F*) with
  - means for turning a p into a **state-independent proposition**
  - operation to **witness** the validity of p s in some state s
  - operation to **recall** the validity of p s′ in a future state s′
- Gives a **general account** of examples already in use in F*

Overview of our solution

- We focus on **monotonic** programs and **stable** predicates
  - per verification task, we choose a **preorder** `rel` on states
    - set inclusion, heap inclusion, increasing counters, ...
  - a program e is **monotonic** (wrt. `rel`) when

$$(\mathtt{s}, \mathtt{e}) \rightsquigarrow^* (\mathtt{s}', \mathtt{e}') \implies \mathtt{rel}\ \mathtt{s}\ \mathtt{s}'$$

  - a predicate p on states is **stable** (wrt. `rel`) when

$$\forall\, \mathtt{s}\, \mathtt{s}'.\ \mathtt{p}\ \mathtt{s}\ \wedge\ \mathtt{rel}\ \mathtt{s}\ \mathtt{s}' \implies \mathtt{p}\ \mathtt{s}'$$

- **Our solution:** extend Hoare-style program logics (e.g., F*) with
  - means for turning a p into a **state-independent proposition**
  - operation to **witness** the validity of p s in some state s
  - operation to **recall** the validity of p s′ in a future state s′
- Gives a **general account** of examples already in use in F*

Overview of our solution

- We focus on **monotonic** programs and **stable** predicates
  - per verification task, we choose a **preorder** $\texttt{rel}$ on states
    - set inclusion, heap inclusion, increasing counters, ...
  - a program $\mathtt{e}$ is **monotonic** (wrt. $\texttt{rel}$) when

$$(\mathtt{s}, \mathtt{e}) \rightsquigarrow^* (\mathtt{s}', \mathtt{e}') \implies \texttt{rel}\ \mathtt{s}\ \mathtt{s}'$$

  - a predicate $\texttt{p}$ on states is **stable** (wrt. $\texttt{rel}$) when

$$\forall\, \mathtt{s}\, \mathtt{s}'.\ \texttt{p}\ \mathtt{s}\ \wedge\ \texttt{rel}\ \mathtt{s}\ \mathtt{s}' \implies \texttt{p}\ \mathtt{s}'$$

- **Our solution:** extend Hoare-style program logics (e.g., F*) with
  - means for turning a $\texttt{p}$ into a **state-independent proposition**
  - operation to **witness** the validity of $\texttt{p}\ \mathtt{s}$ in some state $\mathtt{s}$
  - operation to **recall** the validity of $\texttt{p}\ \mathtt{s}'$ in a future state $\mathtt{s}'$
- Gives a **general account** of examples already in use in F*

Overview of our solution

- We focus on **monotonic** programs and **stable** predicates
  - per verification task, we choose a **preorder** `rel` on states
    - set inclusion, heap inclusion, increasing counters, . . .
  - a program e is **monotonic** (wrt. `rel`) when
    $$(\mathtt{s}, \mathtt{e}) \leadsto^* (\mathtt{s}', \mathtt{e}') \implies \mathtt{rel}\ \mathtt{s}\ \mathtt{s}'$$
  - a predicate `p` on states is **stable** (wrt. `rel`) when
    $$\forall\, \mathtt{s}\, \mathtt{s}'.\ \mathtt{p}\ \mathtt{s}\ \wedge\ \mathtt{rel}\ \mathtt{s}\ \mathtt{s}' \implies \mathtt{p}\ \mathtt{s}'$$
- **Our solution:** extend Hoare-style program logics (e.g., F*) with
  - means for turning a `p` into a **state-independent proposition**
  - operation to **witness** the validity of `p` s in some state s
  - operation to **recall** the validity of `p` s′ in a future state s′
- Gives a **general account** of examples already in use in F*

Outline

- Monotonic state and program verification by example
- Overview of our solution (a simple, general interface)
- Extending F* with our monotonic state interface
- Example uses of monotonicity
- A glimpse of the meta-theory

Reasoning about ordinary state in F*

- An ML-like dependently typed language, aimed at verification

- F* supports Hoare-style reasoning about state via the **comp. type**

  $$\mathtt{ST}\ \mathtt{t}\ (\mathtt{requires}\ \mathtt{pre})\ (\mathtt{ensures}\ \mathtt{post})$$

  where

  $$\mathtt{t} : \mathtt{Type} \qquad \mathtt{pre} : \mathtt{state} \to \mathtt{Type} \qquad \mathtt{post} : \mathtt{state} \to \mathtt{t} \to \mathtt{state} \to \mathtt{Type}$$

  (formally, this type is derived from a WP calculus for state)

- The **get** and **put** actions are typed as follows

$$\mathtt{get} : \mathtt{unit} \to \mathtt{ST}\ \mathtt{state}\ (\mathtt{requires}\ (\lambda\, \_ \,.\, \top))\ (\mathtt{ensures}\ (\lambda\, \mathtt{s}_0\, \mathtt{s}\, \mathtt{s}_1 \,.\, \mathtt{s}_0 = \mathtt{s} = \mathtt{s}_1))$$

$$\mathtt{put} : \mathtt{s}{:}\mathtt{state} \to \mathtt{ST}\ \mathtt{unit}\ (\mathtt{requires}\ (\lambda\, \_ \,.\, \top))\ (\mathtt{ensures}\ (\lambda\, \_\, \_\, \mathtt{s}_1 \,.\, \mathtt{s}_1 = \mathtt{s}))$$

Reasoning about ordinary state in F*

- An ML-like dependently typed language, aimed at verification
- F* supports Hoare-style reasoning about state via the **comp. type**

$$\mathtt{ST}\ \mathtt{t}\ (\mathtt{requires}\ \mathtt{pre})\ (\mathtt{ensures}\ \mathtt{post})$$

  where

  $\mathtt{t} : \mathtt{Type} \qquad \mathtt{pre} : \mathtt{state} \to \mathtt{Type} \qquad \mathtt{post} : \mathtt{state} \to \mathtt{t} \to \mathtt{state} \to \mathtt{Type}$

  (formally, this type is derived from a WP calculus for state)

- The **get** and **put** actions are typed as follows

$$\mathtt{get} : \mathtt{unit} \to \mathtt{ST}\ \mathtt{state}\ (\mathtt{requires}\ (\lambda\,\_\,.\top))\ (\mathtt{ensures}\ (\lambda\,\mathtt{s}_0\ \mathtt{s}\ \mathtt{s}_1\,.\,\mathtt{s}_0 = \mathtt{s} = \mathtt{s}_1))$$

$$\mathtt{put} : \mathtt{s}{:}\mathtt{state} \to \mathtt{ST}\ \mathtt{unit}\ (\mathtt{requires}\ (\lambda\,\_\,.\top))\ (\mathtt{ensures}\ (\lambda\,\_\,\_\,\mathtt{s}_1\,.\,\mathtt{s}_1 = \mathtt{s}))$$

Reasoning about ordinary state in F*

- An ML-like dependently typed language, aimed at verification
- F* supports Hoare-style reasoning about state via the **comp. type**

$$\mathtt{ST}\ \mathtt{t}\ (\mathtt{requires}\ \mathtt{pre})\ (\mathtt{ensures}\ \mathtt{post})$$

where

$$\mathtt{t} : \mathtt{Type} \qquad \mathtt{pre} : \mathtt{state} \to \mathtt{Type} \qquad \mathtt{post} : \mathtt{state} \to \mathtt{t} \to \mathtt{state} \to \mathtt{Type}$$

(formally, this type is derived from a WP calculus for state)

- The **get** and **put** actions are typed as follows

$$\mathtt{get} : \mathtt{unit} \to \mathtt{ST}\ \mathtt{state}\ (\mathtt{requires}\ (\lambda\,\_.\top))\ (\mathtt{ensures}\ (\lambda\,\mathtt{s}_0\,\mathtt{s}\,\mathtt{s}_1\,.\,\mathtt{s}_0 = \mathtt{s} = \mathtt{s}_1))$$

$$\mathtt{put} : \mathtt{s}{:}\mathtt{state} \to \mathtt{ST}\ \mathtt{unit}\ (\mathtt{requires}\ (\lambda\,\_.\top))\ (\mathtt{ensures}\ (\lambda\,\_\,\_\,\mathtt{s}_1\,.\,\mathtt{s}_1 = \mathtt{s}))$$

Reasoning about monotonic state in F*

- We capture monotonic state with a new **computation type**

$$\texttt{MST}\ \texttt{rel}\ \texttt{t}\ (\texttt{requires}\ \texttt{pre})\ (\texttt{ensures}\ \texttt{post})$$

  where t, pre, and post are typed as in ST

- The **get** action is typed as in ST

- To ensure **monotonicity**, the **put** action is typed as follows

$$\begin{aligned}\texttt{put} : \texttt{s}{:}\texttt{state} \to \texttt{MST}\ \texttt{unit}\ &(\texttt{requires}\ (\lambda\, \texttt{s}_0\, .\, \texttt{rel}\ \texttt{s}_0\ \texttt{s}))\\ &(\texttt{ensures}\ (\lambda\, \_\, \_\, \texttt{s}_1\, .\, \texttt{s}_1 = \texttt{s}))\end{aligned}$$

  - thus MST is a bit like an **update monad** [A., Uustalu'14]

Reasoning about monotonic state in F*

- We capture monotonic state with a new **computation type**

$$\texttt{MST rel t (requires pre) (ensures post)}$$

where t, pre, and post are typed as in ST

- The **get** action is typed as in ST

- To ensure **monotonicity**, the **put** action is typed as follows

$$\begin{aligned}\texttt{put} : \texttt{s:state} \rightarrow \texttt{MST unit } & (\texttt{requires } (\lambda\, \texttt{s}_0 \,.\, \texttt{rel s}_0\ \texttt{s})) \\ & (\texttt{ensures } (\lambda\, \_\, \_\, \texttt{s}_1 \,.\, \texttt{s}_1 = \texttt{s}))\end{aligned}$$

  - thus MST is a bit like an **update monad** [A., Uustalu'14]

Reasoning about monotonic state in F*

- We capture monotonic state with a new **computation type**

$$\texttt{MST rel t (requires pre) (ensures post)}$$

where `t`, `pre`, and `post` are typed as in `ST`

- The **get** action is typed as in `ST`

- To ensure **monotonicity**, the **put** action is typed as follows

$$\begin{aligned}\texttt{put} : \texttt{s:state} \to \texttt{MST unit } &(\texttt{requires } (\lambda\, \texttt{s}_0\, .\, \texttt{rel s}_0\ \texttt{s}))\\ &(\texttt{ensures } (\lambda\, \_\, \_\, \texttt{s}_1\, .\, \texttt{s}_1 = \texttt{s}))\end{aligned}$$

  - thus `MST` is a bit like an **update monad** [A., Uustalu'14]

Reasoning about monotonic state in F*

- We capture monotonic state with a new **computation type**

$$\texttt{MST}\ \texttt{rel}\ \texttt{t}\ (\texttt{requires}\ \texttt{pre})\ (\texttt{ensures}\ \texttt{post})$$

  where t, pre, and post are typed as in ST

- The **get** action is typed as in ST

- To ensure **monotonicity**, the **put** action is typed as follows

$$\begin{aligned}\texttt{put} : \texttt{s}{:}\texttt{state} \rightarrow \texttt{MST}\ \texttt{unit}\ &(\texttt{requires}\ (\lambda\, \texttt{s}_0\, .\, \texttt{rel}\ \texttt{s}_0\ \texttt{s}))\\ &(\texttt{ensures}\ (\lambda\, \_\, \_\, \texttt{s}_1\, .\, \texttt{s}_1 = \texttt{s}))\end{aligned}$$

  - thus MST is a bit like an **update monad** [A., Uustalu'14]

Reasoning about monotonic state in F*

- We introduce a **logical capability**

$$\texttt{witnessed} : \texttt{pred state} \rightarrow \texttt{Type}$$

  together with a **weakening** principle

$$\begin{aligned}\texttt{wk} : \texttt{p,q:pred state} \rightarrow \texttt{Lemma}\ &(\texttt{requires}\ (\forall\, \texttt{s}\,.\,\texttt{p s} \implies \texttt{q s}))\\ &(\texttt{ensures}\ (\texttt{witnessed p} \implies \texttt{witnessed q}))\end{aligned}$$

- We introduce an operation for **witnessing** stable predicates

$$\begin{aligned}\texttt{witness} : \texttt{p:pred state} \rightarrow \texttt{MST unit}\ &(\texttt{requires}\ (\lambda\, \texttt{s}_0\,.\,\texttt{p s}_0 \wedge \texttt{stable p}))\\ &(\texttt{ensures}\ (\lambda\, \texttt{s}_0\, \_\, \texttt{s}_1\,.\,\texttt{s}_0 = \texttt{s}_1 \wedge\\ &\qquad\qquad \texttt{witnessed p}))\end{aligned}$$

- We introduce an operation for **recalling** validity of predicates

$$\begin{aligned}\texttt{recall} : \texttt{p:pred state} \rightarrow \texttt{MST unit}\ &(\texttt{requires}\ (\lambda\, \texttt{s}_0\,.\,\texttt{witnessed p}))\\ &(\texttt{ensures}\ (\lambda\, \texttt{s}_0\, \_\, \texttt{s}_1\,.\,\texttt{s}_0 = \texttt{s}_1 \wedge \texttt{p s}_1))\end{aligned}$$

Reasoning about monotonic state in F*

- We introduce a **logical capability**

$$\mathtt{witnessed} : \mathtt{pred}\ \mathtt{state} \to \mathtt{Type}$$

together with a **weakening** principle

$$\mathtt{wk} : \mathtt{p},\mathtt{q}{:}\mathtt{pred}\ \mathtt{state} \to \mathtt{Lemma}\ (\mathtt{requires}\ (\forall\, \mathtt{s}\,.\, \mathtt{p}\ \mathtt{s} \implies \mathtt{q}\ \mathtt{s}))$$
$$(\mathtt{ensures}\ (\mathtt{witnessed}\ \mathtt{p} \implies \mathtt{witnessed}\ \mathtt{q}))$$

- We introduce an operation for **witnessing** stable predicates

$$\mathtt{witness} : \mathtt{p}{:}\mathtt{pred}\ \mathtt{state} \to \mathtt{MST}\ \mathtt{unit}\ (\mathtt{requires}\ (\lambda\, \mathtt{s}_0\,.\, \mathtt{p}\ \mathtt{s}_0 \wedge \mathtt{stable}\ \mathtt{p}))$$
$$(\mathtt{ensures}\ (\lambda\, \mathtt{s}_0\ \_\ \mathtt{s}_1\,.\, \mathtt{s}_0 = \mathtt{s}_1 \wedge \mathtt{witnessed}\ \mathtt{p}))$$

- We introduce an operation for **recalling** validity of predicates

$$\mathtt{recall} : \mathtt{p}{:}\mathtt{pred}\ \mathtt{state} \to \mathtt{MST}\ \mathtt{unit}\ (\mathtt{requires}\ (\lambda\, \mathtt{s}_0\,.\, \mathtt{witnessed}\ \mathtt{p}))$$
$$(\mathtt{ensures}\ (\lambda\, \mathtt{s}_0\ \_\ \mathtt{s}_1\,.\, \mathtt{s}_0 = \mathtt{s}_1 \wedge \mathtt{p}\ \mathtt{s}_1))$$

Reasoning about monotonic state in F*

- We introduce a **logical capability**

$$\mathtt{witnessed} : \mathtt{pred\ state} \to \mathtt{Type}$$

  together with a **weakening** principle

$$\mathtt{wk} : \mathtt{p,q{:}pred\ state} \to \mathtt{Lemma}\ (\mathtt{requires}\ (\forall\, \mathtt{s}\,.\, \mathtt{p\ s} \implies \mathtt{q\ s}))$$
$$(\mathtt{ensures}\ (\mathtt{witnessed\ p} \implies \mathtt{witnessed\ q}))$$

- We introduce an operation for **witnessing** stable predicates

$$\mathtt{witness} : \mathtt{p{:}pred\ state} \to \mathtt{MST\ unit}\ (\mathtt{requires}\ (\lambda\, \mathtt{s}_0\,.\, \mathtt{p\ s}_0 \wedge \mathtt{stable\ p}))$$
$$(\mathtt{ensures}\ (\lambda\, \mathtt{s}_0\ \_\ \mathtt{s}_1\,.\, \mathtt{s}_0 = \mathtt{s}_1 \wedge \mathtt{witnessed\ p}))$$

- We introduce an operation for **recalling** validity of predicates

$$\mathtt{recall} : \mathtt{p{:}pred\ state} \to \mathtt{MST\ unit}\ (\mathtt{requires}\ (\lambda\, \mathtt{s}_0\,.\, \mathtt{witnessed\ p}))$$
$$(\mathtt{ensures}\ (\lambda\, \mathtt{s}_0\ \_\ \mathtt{s}_1\,.\, \mathtt{s}_0 = \mathtt{s}_1 \wedge \mathtt{p\ s}_1))$$

Reasoning about monotonic state in F*

- We introduce a **logical capability**

$$\texttt{witnessed} : \texttt{pred state} \rightarrow \texttt{Type}$$

  together with a **weakening** principle

$$\begin{aligned}\texttt{wk} : \texttt{p,q:pred state} \rightarrow \texttt{Lemma}\ &(\texttt{requires}\ (\forall\, \texttt{s}\,.\,\texttt{p s} \implies \texttt{q s}))\\ &(\texttt{ensures}\ (\texttt{witnessed p} \implies \texttt{witnessed q}))\end{aligned}$$

- We introduce an operation for **witnessing** stable predicates

$$\begin{aligned}\texttt{witness} : \texttt{p:pred state} \rightarrow \texttt{MST unit}\ &(\texttt{requires}\ (\lambda\, \texttt{s}_0\,.\,\texttt{p}\ \texttt{s}_0 \wedge \texttt{stable p}))\\ &(\texttt{ensures}\ (\lambda\, \texttt{s}_0\,\_\,\texttt{s}_1\,.\,\texttt{s}_0 = \texttt{s}_1 \wedge\\ &\qquad \texttt{witnessed p}))\end{aligned}$$

- We introduce an operation for **recalling** validity of predicates

$$\begin{aligned}\texttt{recall} : \texttt{p:pred state} \rightarrow \texttt{MST unit}\ &(\texttt{requires}\ (\lambda\, \texttt{s}_0\,.\,\texttt{witnessed p}))\\ &(\texttt{ensures}\ (\lambda\, \texttt{s}_0\,\_\,\texttt{s}_1\,.\,\texttt{s}_0 = \texttt{s}_1 \wedge \texttt{p}\ \texttt{s}_1))\end{aligned}$$

Outline

- Monotonic state and program verification by example
- Overview of our solution (a simple, general interface)
- Extending F* with our monotonic state interface
- Example uses of monotonicity
- A glimpse of the meta-theory

The motivating example revisited

- Recall the program operating on **set-valued state**

$$\texttt{insert v};\ \texttt{complex\_procedure}();\ \texttt{assert}\ (\mathtt{v} \in \mathtt{get}())$$

  - We pick **set inclusion** $\subseteq$ as our preorder on states
  - We **prove the assertion** by adding a `witness` and a `recall`

$$\texttt{insert v};\ \texttt{witness}\ (\lambda\, \mathtt{s} \,.\, \mathtt{v} \in \mathtt{s});\ \mathtt{c\_p}();\ \texttt{recall}\ (\lambda\, \mathtt{s} \,.\, \mathtt{v} \in \mathtt{s});\ \texttt{assert}\ (\mathtt{v} \in \mathtt{get}())$$

  - For any other `w`, wrapping

$$\texttt{insert w};\ [\ \ ];\ \texttt{assert}\ (\mathtt{w} \in \mathtt{get}())$$

    around the program is handled similarly easily

- **Monotonic counters** are analogous, with $\mathbb{N}$ and $\leq$

$$\texttt{create 0};\ \texttt{incr}();\ \texttt{witness}\ (\lambda\, \mathtt{c} \,.\, \mathtt{c} > 0);\ \mathtt{c\_p}();\ \texttt{recall}\ (\lambda\, \mathtt{c} \,.\, \mathtt{c} > 0)$$

The motivating example revisited

- Recall the program operating on **set-valued state**

$$\texttt{insert v};\ \texttt{complex\_procedure}();\ \texttt{assert}\ (\texttt{v} \in \texttt{get}())$$

  - We pick **set inclusion** $\subseteq$ as our preorder on states
  - We **prove the assertion** by adding a `witness` and a `recall`

$$\texttt{insert v};\ \texttt{witness}\ (\lambda\,\texttt{s}\,.\,\texttt{v} \in \texttt{s});\ \texttt{c\_p}();\ \texttt{recall}\ (\lambda\,\texttt{s}\,.\,\texttt{v} \in \texttt{s});\ \texttt{assert}\ (\texttt{v} \in \texttt{get}())$$

  - For any other `w`, wrapping

$$\texttt{insert w};\ [\ \ ];\ \texttt{assert}\ (\texttt{w} \in \texttt{get}())$$

    around the program is handled similarly easily

- **Monotonic counters** are analogous, with $\mathbb{N}$ and $\leq$

$$\texttt{create 0};\ \texttt{incr}();\ \texttt{witness}\ (\lambda\,\texttt{c}\,.\,\texttt{c} > 0);\ \texttt{c\_p}();\ \texttt{recall}\ (\lambda\,\texttt{c}\,.\,\texttt{c} > 0)$$

The motivating example revisited

- Recall the program operating on **set-valued state**

$$\mathtt{insert}\ \mathrm{v};\ \mathtt{complex\_procedure}();\ \mathtt{assert}\ (\mathrm{v} \in \mathrm{get}())$$

  - We pick **set inclusion** $\subseteq$ as our preorder on states
  - We **prove the assertion** by adding a `witness` and a `recall`

$$\mathtt{insert}\ \mathrm{v};\ \mathtt{witness}\ (\lambda\, \mathrm{s}\,.\, \mathrm{v} \in \mathrm{s});\ \mathrm{c\_p}();\ \mathtt{recall}\ (\lambda\, \mathrm{s}\,.\, \mathrm{v} \in \mathrm{s});\ \mathtt{assert}\ (\mathrm{v} \in \mathrm{get}())$$

  - For any other w, wrapping

$$\mathtt{insert}\ \mathrm{w};\ [\ \ ];\ \mathtt{assert}\ (\mathrm{w} \in \mathrm{get}())$$

    around the program is handled similarly easily

- **Monotonic counters** are analogous, with $\mathbb{N}$ and $\leq$

$$\mathtt{create}\ 0;\ \mathtt{incr}();\ \mathtt{witness}\ (\lambda\, \mathrm{c}\,.\, \mathrm{c} > 0);\ \mathrm{c\_p}();\ \mathtt{recall}\ (\lambda\, \mathrm{c}\,.\, \mathrm{c} > 0)$$

The motivating example revisited

- Recall the program operating on **set-valued state**

$$\texttt{insert v; complex\_procedure(); } \texttt{assert } (\texttt{v} \in \texttt{get()})$$

  - We pick **set inclusion** $\subseteq$ as our preorder on states
  - We **prove the assertion** by adding a `witness` and a `recall`

$$\texttt{insert v; } \texttt{witness } (\lambda\, \texttt{s} \,.\, \texttt{v} \in \texttt{s})\texttt{; c\_p(); } \texttt{recall } (\lambda\, \texttt{s} \,.\, \texttt{v} \in \texttt{s})\texttt{; } \texttt{assert } (\texttt{v} \in \texttt{get()})$$

  - For any other `w`, wrapping

$$\texttt{insert w; [ ]; } \texttt{assert } (\texttt{w} \in \texttt{get()})$$

    around the program is handled similarly easily

- **Monotonic counters** are analogous, with $\mathbb{N}$ and $\leq$

$$\texttt{create 0; incr(); } \texttt{witness } (\lambda\, \texttt{c} \,.\, \texttt{c} > 0)\texttt{; c\_p(); } \texttt{recall } (\lambda\, \texttt{c} \,.\, \texttt{c} > 0)$$

The motivating example revisited

- Recall the program operating on **set-valued state**

$$\texttt{insert v; complex\_procedure(); } \texttt{assert } (\texttt{v} \in \texttt{get}())$$

  - We pick **set inclusion** $\subseteq$ as our preorder on states
  - We **prove the assertion** by adding a `witness` and a `recall`

$$\texttt{insert v; } \texttt{witness } (\lambda\, \texttt{s} \,.\, \texttt{v} \in \texttt{s}); \texttt{ c\_p(); } \texttt{recall } (\lambda\, \texttt{s} \,.\, \texttt{v} \in \texttt{s}); \texttt{ assert } (\texttt{v} \in \texttt{get}())$$

  - For any other `w`, wrapping

$$\texttt{insert w; [ ]; } \texttt{assert } (\texttt{w} \in \texttt{get}())$$

    around the program is handled similarly easily

- **Monotonic counters** are analogous, with $\mathbb{N}$ and $\leq$

$$\texttt{create 0; incr(); } \texttt{witness } (\lambda\, \texttt{c} \,.\, \texttt{c} > 0); \texttt{ c\_p(); } \texttt{recall } (\lambda\, \texttt{c} \,.\, \texttt{c} > 0)$$

References: both typed and untyped

- We define **local state** using monotonicity and global state
- We define **heaps** as maps

  $\mathtt{type\ heap} =$

  $\mid \mathtt{H} : \mathtt{h}{:}(\mathbb{N} \to \mathtt{cell}) \to \mathtt{ctr}{:}\mathbb{N}\{\forall\,\mathtt{n}\,.\,\mathtt{ctr} \leq \mathtt{n} \implies \mathtt{h}\ \mathtt{n} = \mathtt{Unused}\} \to \mathtt{heap}$

  where

  $\mathtt{type\ cell} = \mathtt{Unused} : \mathtt{cell} \mid \mathtt{Used} : \mathtt{a}{:}\mathrm{Type} \to \mathtt{v}{:}\mathtt{a} \to \mathtt{t}{:}\mathtt{tag} \to \mathtt{cell}$

  $\mathtt{type\ tag} \ \ = \mathtt{Typed} : \mathtt{tag} \mid \mathtt{Untyped} : \mathtt{live}{:}\mathrm{bool} \to \mathtt{tag}$

- The **preorder** on heaps is given by

  $\mathtt{let\ rel}\ (\mathtt{H}\ \mathtt{h}_0\ \_)\ (\mathtt{H}\ \mathtt{h}_1\ \_) = \forall\,\mathtt{id}\,.\,\mathtt{match}\ \mathtt{h}_0\ \mathtt{id}, \mathtt{h}_1\ \mathtt{id}\ \mathtt{with}$

  $\mid \mathtt{Used}\ \mathtt{a}\ \_\ \mathtt{Typed}, \mathtt{Used}\ \mathtt{b}\ \_\ \mathtt{Typed} \to \mathtt{a} = \mathtt{b}$

  $\mid \mathtt{Used}\ \_\ \_\ (\mathtt{Untyped}\ \mathtt{l}_0), \mathtt{Used}\ \_\ \_\ (\mathtt{Untyped}\ \mathtt{l}_1) \to \neg(\mathtt{l}_0) \implies \neg(\mathtt{l}_1)$

  $\mid \_, \_ \to \bot$

References: both typed and untyped

- We define **local state** using monotonicity and global state

- We define **heaps** as maps

```
type heap =
  | H : h:(ℕ → cell) → ctr:ℕ{∀ n . ctr ≤ n ⟹ h n = Unused} → heap
```

  where

```
    type cell = Unused : cell | Used : a:Type → v:a → t:tag → cell
    type tag  = Typed : tag | Untyped : live:bool → tag
```

- The **preorder** on heaps is given by

```
let rel (H h0 _) (H h1 _) = ∀ id . match h0 id, h1 id with
  | Used a _ Typed, Used b _ Typed → a = b
  | Used _ _ (Untyped l0), Used _ _ (Untyped l1) → ¬(l0) ⟹ ¬(l1)
  | _, _ → ⊥
```

References: both typed and untyped

- We define **local state** using monotonicity and global state
- We define **heaps** as maps

$$\texttt{type heap} =$$
$$\mid \texttt{H} : \texttt{h}{:}(\mathbb{N} \rightarrow \texttt{cell}) \rightarrow \texttt{ctr}{:}\mathbb{N}\{\forall\,\texttt{n}\,.\,\texttt{ctr} \leq \texttt{n} \implies \texttt{h n} = \texttt{Unused}\} \rightarrow \texttt{heap}$$

where

$$\texttt{type cell} = \texttt{Unused} : \texttt{cell} \mid \texttt{Used} : \texttt{a}{:}\mathrm{Type} \rightarrow \texttt{v}{:}\texttt{a} \rightarrow \texttt{t}{:}\texttt{tag} \rightarrow \texttt{cell}$$
$$\texttt{type tag} = \texttt{Typed} : \texttt{tag} \mid \texttt{Untyped} : \texttt{live}{:}\mathrm{bool} \rightarrow \texttt{tag}$$

- The **preorder** on heaps is given by

$$\texttt{let rel (H } \texttt{h}_0 \texttt{ \_) (H } \texttt{h}_1 \texttt{ \_)} = \forall\,\texttt{id}\,.\,\texttt{match } \texttt{h}_0 \texttt{ id}, \texttt{h}_1 \texttt{ id with}$$
$$\mid \texttt{Used a \_ Typed}, \texttt{Used b \_ Typed} \rightarrow \texttt{a} = \texttt{b}$$
$$\mid \texttt{Used \_ \_ (Untyped } \texttt{l}_0\texttt{)}, \texttt{Used \_ \_ (Untyped } \texttt{l}_1\texttt{)} \rightarrow \neg(\texttt{l}_0) \implies \neg(\texttt{l}_1)$$
$$\mid \texttt{\_}, \texttt{\_} \rightarrow \bot$$

References: both typed and untyped

- We define **local state** using monotonicity and global state

- We define **heaps** as maps

  $$\texttt{type heap} =$$
  $$\mid \texttt{H} : \texttt{h}{:}(\mathbb{N} \to \texttt{cell}) \to \texttt{ctr}{:}\mathbb{N}\{\forall\, \texttt{n}\,.\, \texttt{ctr} \leq \texttt{n} \implies \texttt{h n} = \texttt{Unused}\} \to \texttt{heap}$$

  where

  $$\texttt{type cell} = \texttt{Unused} : \texttt{cell} \mid \texttt{Used} : \texttt{a}{:}\mathrm{Type} \to \texttt{v}{:}\texttt{a} \to \texttt{t}{:}\texttt{tag} \to \texttt{cell}$$
  $$\texttt{type tag} = \texttt{Typed} : \texttt{tag} \mid \texttt{Untyped} : \texttt{live}{:}\texttt{bool} \to \texttt{tag}$$

- The **preorder** on heaps is given by

  $$\texttt{let rel (H } \texttt{h}_0\ \_\texttt{) (H } \texttt{h}_1\ \_\texttt{)} = \forall\, \texttt{id}\,.\,\texttt{match } \texttt{h}_0\ \texttt{id}, \texttt{h}_1\ \texttt{id with}$$
  $$\mid \texttt{Used a \_ Typed}, \texttt{Used b \_ Typed} \to \texttt{a} = \texttt{b}$$
  $$\mid \texttt{Used \_ \_ (Untyped } \texttt{l}_0\texttt{)}, \texttt{Used \_ \_ (Untyped } \texttt{l}_1\texttt{)} \to \neg(\texttt{l}_0) \implies \neg(\texttt{l}_1)$$
  $$\mid \_, \_ \to \bot$$

References: both typed and untyped ctd.

- We define **local state** using monotonicity and global state
- We define **heaps** as maps

  $$\mathtt{type}\ \mathtt{heap} =$$
  $$\mid \mathtt{H} : \mathtt{h}{:}(\mathbb{N} \rightarrow \mathtt{cell}) \rightarrow \mathtt{ctr}{:}\mathbb{N}\{\forall\, \mathtt{n}\,.\, \mathtt{ctr} \leq \mathtt{n} \implies \mathtt{h}\ \mathtt{n} = \mathtt{Unused}\} \rightarrow \mathtt{heap}$$

  where

  $$\mathtt{type}\ \mathtt{cell} = \mathtt{Unused} : \mathtt{cell} \mid \mathtt{Used} : \mathtt{a}{:}\mathrm{Type} \rightarrow \mathtt{v}{:}\mathtt{a} \rightarrow \mathtt{t}{:}\mathtt{tag} \rightarrow \mathtt{cell}$$
  $$\mathtt{type}\ \mathtt{tag} = \mathtt{Typed} : \mathtt{tag} \mid \mathtt{Untyped} : \mathtt{live}{:}\mathtt{bool} \rightarrow \mathtt{tag}$$

- **Typed references** are defined as

  $$\mathtt{abstract}\ \mathtt{type}\ \mathtt{ref}\ \mathtt{t} = \mathtt{id}{:}\mathbb{N}\{\mathtt{witnessed}\ (\lambda\, \mathtt{h}\,.\, \mathtt{has\_used\_typed}\ \mathtt{id}\ \mathtt{t}\ \mathtt{h})\}$$

- **Untyped references** are defined as

  $$\mathtt{abstract}\ \mathtt{type}\ \mathtt{uref} = \mathtt{id}{:}\mathbb{N}\{\mathtt{witnessed}\ (\lambda\, \mathtt{h}\,.\, \mathtt{has\_used\_untyped\_live}\ \mathtt{id}\ \mathtt{h})\}$$

- In F*, we also support more sophisticated heap models

References: both typed and untyped ctd.

- We define **local state** using monotonicity and global state
- We define **heaps** as maps

  $\texttt{type heap} =$

  $\quad \mid \texttt{H} : \texttt{h}{:}(\mathbb{N} \to \texttt{cell}) \to \texttt{ctr}{:}\mathbb{N}\{\forall\, \texttt{n}\,.\, \texttt{ctr} \leq \texttt{n} \implies \texttt{h n} = \texttt{Unused}\} \to \texttt{heap}$

  where

  $\texttt{type cell} = \texttt{Unused} : \texttt{cell} \mid \texttt{Used} : \texttt{a}{:}\texttt{Type} \to \texttt{v}{:}\texttt{a} \to \texttt{t}{:}\texttt{tag} \to \texttt{cell}$

  $\texttt{type tag} = \texttt{Typed} : \texttt{tag} \mid \texttt{Untyped} : \texttt{live}{:}\texttt{bool} \to \texttt{tag}$

- **Typed references** are defined as

  $\texttt{abstract type ref t} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed}\ (\lambda\, \texttt{h}\,.\, \texttt{has\_used\_typed id t h})\}$

- **Untyped references** are defined as

  $\texttt{abstract type uref} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed}\ (\lambda\, \texttt{h}\,.\, \texttt{has\_used\_untyped\_live id h})\}$

- In F*, we also support more sophisticated heap models

References: both typed and untyped ctd.

- We define **local state** using monotonicity and global state
- We define **heaps** as maps

$$\texttt{type heap} =$$
$$\mid \texttt{H} : \texttt{h}{:}(\mathbb{N} \rightarrow \texttt{cell}) \rightarrow \texttt{ctr}{:}\mathbb{N}\{\forall\, \texttt{n}\,.\, \texttt{ctr} \leq \texttt{n} \implies \texttt{h n} = \texttt{Unused}\} \rightarrow \texttt{heap}$$

where

$$\texttt{type cell} = \texttt{Unused} : \texttt{cell} \mid \texttt{Used} : \texttt{a}{:}\mathrm{Type} \rightarrow \texttt{v}{:}\texttt{a} \rightarrow \texttt{t}{:}\texttt{tag} \rightarrow \texttt{cell}$$
$$\texttt{type tag} = \texttt{Typed} : \texttt{tag} \mid \texttt{Untyped} : \texttt{live}{:}\texttt{bool} \rightarrow \texttt{tag}$$

- **Typed references** are defined as

$$\texttt{abstract type ref t} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed}\ (\lambda\, \texttt{h}\,.\, \texttt{has\_used\_typed id t h})\}$$

- **Untyped references** are defined as

$$\texttt{abstract type uref} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed}\ (\lambda\, \texttt{h}\,.\, \texttt{has\_used\_untyped\_live id h})\}$$

- In F*, we also support more sophisticated heap models

References: both typed and untyped ctd.

- We define **local state** using monotonicity and global state
- We define **heaps** as maps

$$\texttt{type heap} = $$
$$\mid \texttt{H} : \texttt{h}{:}(\mathbb{N} \to \texttt{cell}) \to \texttt{ctr}{:}\mathbb{N}\{\forall\, \texttt{n}\,.\, \texttt{ctr} \leq \texttt{n} \implies \texttt{h n} = \texttt{Unused}\} \to \texttt{heap}$$

where

$$\texttt{type cell} = \texttt{Unused} : \texttt{cell} \mid \texttt{Used} : \texttt{a}{:}\mathrm{Type} \to \texttt{v}{:}\texttt{a} \to \texttt{t}{:}\texttt{tag} \to \texttt{cell}$$
$$\texttt{type tag} = \texttt{Typed} : \texttt{tag} \mid \texttt{Untyped} : \texttt{live}{:}\texttt{bool} \to \texttt{tag}$$

- **Typed references** are defined as

$$\texttt{abstract type ref t} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed}\ (\lambda\, \texttt{h}\,.\, \texttt{has\_used\_typed id t h})\}$$

- **Untyped references** are defined as

$$\texttt{abstract type uref} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed}\ (\lambda\, \texttt{h}\,.\, \texttt{has\_used\_untyped\_live id h})\}$$

- In F*, we also support more sophisticated heap models

References: typed and untyped ctd.

- The state actions for **typed references** use **witness** and **recall**
  - `let alloc t (v:t) : MST (ref t) ... = ...`
    - **get** the current heap (using global state `get`)
    - **create** a fresh ref., and **add** it to the heap
    - **put** the updated heap back (using global state `put`)
    - **witness** that the created ref. is in the heap
  - `let read t (r:ref t) : MST t ... = ...`
    - **recall** that the given ref. is in the heap
    - **get** the current heap (using global state `get`)
    - **select** the given reference from the heap
  - `let write t (r:ref t) (v:t) : MST unit ... = ...`
    - **recall** that the given ref. is in the heap
    - **get** the current heap (using global state `get`)
    - **update** the heap with the given value at the given ref.
    - **put** the updated heap back (using global state `put`)
- The actions for **untyped references** involve liveness preconditions

References: typed and untyped ctd.

- The state actions for **typed references** use **witness** and **recall**
  - `let alloc t (v:t) : MST (ref t) ... = ...`
    - **get** the current heap (using global state `get`)
    - **create** a fresh ref., and **add** it to the heap
    - **put** the updated heap back (using global state `put`)
    - **witness** that the created ref. is in the heap
  - `let read t (r:ref t) : MST t ... = ...`
    - **recall** that the given ref. is in the heap
    - **get** the current heap (using global state `get`)
    - **select** the given reference from the heap
  - `let write t (r:ref t) (v:t) : MST unit ... = ...`
    - **recall** that the given ref. is in the heap
    - **get** the current heap (using global state `get`)
    - **update** the heap with the given value at the given ref.
    - **put** the updated heap back (using global state `put`)
- The actions for **untyped references** involve liveness preconditions

References: typed and untyped ctd.

- The state actions for **typed references** use **witness** and **recall**
  - `let alloc t (v:t) : MST (ref t) ... = ...`
    - **get** the current heap (using global state `get`)
    - **create** a fresh ref., and **add** it to the heap
    - **put** the updated heap back (using global state `put`)
    - **witness** that the created ref. is in the heap
  - `let read t (r:ref t) : MST t ... = ...`
    - **recall** that the given ref. is in the heap
    - **get** the current heap (using global state `get`)
    - **select** the given reference from the heap
  - `let write t (r:ref t) (v:t) : MST unit ... = ...`
    - **recall** that the given ref. is in the heap
    - **get** the current heap (using global state `get`)
    - **update** the heap with the given value at the given ref.
    - **put** the updated heap back (using global state `put`)
- The actions for **untyped references** involve liveness preconditions

Monotonic references: more flexibility

- The heap now associates a **local preorder** with each reference

```
type tag a = Typed : rel:preorder a → tag a | Untyped : live:bool → tag a
```

- The **global preorder** is a point-wise lifting of the individual ones

```
let rel (H h₀ _) (H h₁ _) = ∀ id . match h₀ id, h₁ id with
  | Used a₀ v₀ (Typed rel₀),
    Used a₁ v₁ (Typed rel₁) → a₀ = a₁ ∧ rel₀ = rel₁ ∧ rel₀ v₀ v₁
  | ...
```

- **Monotonic references** are then given as

```
abstract type mref t rel = id:ℕ{witnessed (λ h . has_mref id t rel h)}
```

- State actions
  - The **write** action is constrained by `rel` of the given mref.
  - The **witness** and **recall** actions are given reference-wise

Monotonic references: more flexibility

- The heap now associates a **local preorder** with each reference

```
type tag a = Typed : rel:preorder a → tag a | Untyped : live:bool → tag a
```

- The **global preorder** is a point-wise lifting of the individual ones

```
let rel (H h₀ _) (H h₁ _) = ∀ id . match h₀ id, h₁ id with
  | Used a₀ v₀ (Typed rel₀),
    Used a₁ v₁ (Typed rel₁) → a₀ = a₁ ∧ rel₀ = rel₁ ∧ rel₀ v₀ v₁
  | ...
```

- **Monotonic references** are then given as

```
abstract type mref t rel = id:ℕ{witnessed (λ h . has_mref id t rel h)}
```

- State actions
  - The **write** action is constrained by `rel` of the given mref.
  - The **witness** and **recall** actions are given reference-wise

Monotonic references: more flexibility

- The heap now associates a **local preorder** with each reference

$\texttt{type tag a} = \texttt{Typed} : \texttt{rel:preorder a} \rightarrow \texttt{tag a} \mid \texttt{Untyped} : \texttt{live:bool} \rightarrow \texttt{tag a}$

- The **global preorder** is a point-wise lifting of the individual ones

$$
\begin{array}{l}
\texttt{let rel } (\texttt{H } \texttt{h}_0 \ \_) \ (\texttt{H } \texttt{h}_1 \ \_) = \forall \texttt{id}\,.\,\texttt{match } \texttt{h}_0 \texttt{ id}, \texttt{h}_1 \texttt{ id with} \\
\quad \mid \texttt{Used } \texttt{a}_0 \ \texttt{v}_0 \ (\texttt{Typed } \texttt{rel}_0), \\
\quad \ \ \ \texttt{Used } \texttt{a}_1 \ \texttt{v}_1 \ (\texttt{Typed } \texttt{rel}_1) \rightarrow \texttt{a}_0 = \texttt{a}_1 \wedge \texttt{rel}_0 = \texttt{rel}_1 \wedge \texttt{rel}_0 \ \texttt{v}_0 \ \texttt{v}_1 \\
\quad \mid \ \ldots
\end{array}
$$

- **Monotonic references** are then given as

$\texttt{abstract type mref t rel} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed } (\lambda\,\texttt{h}\,.\,\texttt{has\_mref id t rel h})\}$

- State actions
  - The **write** action is constrained by `rel` of the given mref.
  - The **witness** and **recall** actions are given reference-wise

Monotonic references: more flexibility

- The heap now associates a **local preorder** with each reference

$\texttt{type tag a} = \texttt{Typed} : \texttt{rel:preorder a} \rightarrow \texttt{tag a} \mid \texttt{Untyped} : \texttt{live:bool} \rightarrow \texttt{tag a}$

- The **global preorder** is a point-wise lifting of the individual ones

$$
\begin{aligned}
&\texttt{let rel } (\texttt{H } \texttt{h}_0 \ \_)\ (\texttt{H } \texttt{h}_1 \ \_) = \forall\, \texttt{id}\,.\, \texttt{match } \texttt{h}_0 \texttt{ id}, \texttt{h}_1 \texttt{ id with} \\
&\quad \mid \texttt{Used } \texttt{a}_0\ \texttt{v}_0\ (\texttt{Typed } \texttt{rel}_0), \\
&\quad\ \ \ \texttt{Used } \texttt{a}_1\ \texttt{v}_1\ (\texttt{Typed } \texttt{rel}_1) \rightarrow \texttt{a}_0 = \texttt{a}_1 \wedge \texttt{rel}_0 = \texttt{rel}_1 \wedge \texttt{rel}_0\ \texttt{v}_0\ \texttt{v}_1 \\
&\quad \mid \ldots
\end{aligned}
$$

- **Monotonic references** are then given as

$\texttt{abstract type mref t rel} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed } (\lambda\, \texttt{h}\,.\, \texttt{has\_mref id t rel h})\}$

- State actions
  - The **write** action is constrained by `rel` of the given mref.
  - The **witness** and **recall** actions are given reference-wise

Monotonic references: more flexibility

- The heap now associates a **local preorder** with each reference

$\texttt{type tag a} = \texttt{Typed} : \texttt{rel:preorder a} \rightarrow \texttt{tag a} \mid \texttt{Untyped} : \texttt{live:bool} \rightarrow \texttt{tag a}$

- The **global preorder** is a point-wise lifting of the individual ones

$$
\begin{aligned}
&\texttt{let rel } (\texttt{H } \texttt{h}_0 \ \_) \ (\texttt{H } \texttt{h}_1 \ \_) = \forall\, \texttt{id}\,.\, \texttt{match } \texttt{h}_0 \texttt{ id}, \texttt{h}_1 \texttt{ id with} \\
&\quad \mid \texttt{Used } \texttt{a}_0 \ \texttt{v}_0 \ (\texttt{Typed } \texttt{rel}_0), \\
&\quad\ \ \texttt{Used } \texttt{a}_1 \ \texttt{v}_1 \ (\texttt{Typed } \texttt{rel}_1) \rightarrow \texttt{a}_0 = \texttt{a}_1 \wedge \texttt{rel}_0 = \texttt{rel}_1 \wedge \texttt{rel}_0 \ \texttt{v}_0 \ \texttt{v}_1 \\
&\quad \mid \ \ldots
\end{aligned}
$$

- **Monotonic references** are then given as

$\texttt{abstract type mref t rel} = \texttt{id}{:}\mathbb{N}\{\texttt{witnessed } (\lambda\, \texttt{h}\,.\, \texttt{has\_mref id t rel h})\}$

- State actions
  - The **write** action is constrained by `rel` of the given mref.
  - The **witness** and **recall** actions are given reference-wise

Outline

- Monotonic state and program verification by example
- Overview of our solution (a simple, general interface)
- Extending F* with our monotonic state interface
- Example uses of monotonicity
- A glimpse of the meta-theory

A glimpse of the meta-theory

- We formalize `MST` in a small dependently typed CBV calculus

$$
\begin{aligned}
t &::= \mathsf{state} \mid x{:}t_1 \to \textbf{Tot}\ t_2 \mid x{:}t_1 \to \textbf{MST}\ t_2\ (s.\varphi_{\mathsf{pre}})\ (s.y.s'.\varphi_{\mathsf{post}}) \\
e &::= \mathsf{get} \mid \mathsf{put}\ v \mid \mathsf{witness}\ s.\varphi \mid \mathsf{recall}\ s.\varphi \mid \ldots \\
\varphi &::= \mathsf{rel}\ v_1\ v_2 \mid \mathsf{witnessed}\ s.\varphi \mid \ldots
\end{aligned}
$$

  - **Consistency** and **props. of the logic** via seq. calc. and cut-adm.

  - **Operational semantics** on configurations (e, σ, W)

$$
\begin{aligned}
(\mathsf{witness}\ s.\varphi, \sigma, W) &\rightsquigarrow (\mathsf{return}\ (), \sigma, W \cup \{s.\varphi\}) \\
(\mathsf{recall}\ s.\varphi, \sigma, W) &\rightsquigarrow (\mathsf{return}\ (), \sigma, W)
\end{aligned}
$$

  - **Total correctness** via progress, preservation, and SN

$$
\begin{array}{c}
\vdash e : \textbf{MST}\ t\ (s.\varphi_{\mathsf{pre}})\ (s.x.s'.\varphi_{\mathsf{post}}) \\
\mathsf{witnessed}\ W \vdash \varphi_{\mathsf{pre}}[\sigma/s]
\end{array}
\implies
\begin{array}{c}
(e, \sigma, W) \rightsquigarrow^* (\mathsf{return}\ v, \sigma', W') \quad \vdash v : t \\
W \subseteq W' \quad \mathsf{witnessed}\ W' \vdash \mathsf{rel}\ \sigma\ \sigma' \\
\mathsf{witnessed}\ W' \vdash \varphi_{\mathsf{post}}[\sigma/s, v/x, \sigma'/s']
\end{array}
$$

A glimpse of the meta-theory

- We formalize MST in a small dependently typed CBV calculus

$$
\begin{aligned}
t &::= \mathsf{state} \mid x{:}t_1 \to \textbf{Tot}\ t_2 \mid x{:}t_1 \to \textbf{MST}\ t_2\ (s.\varphi_{\mathsf{pre}})\ (s.y.s'.\varphi_{\mathsf{post}}) \\
e &::= \mathsf{get} \mid \mathsf{put}\ v \mid \mathsf{witness}\ s.\varphi \mid \mathsf{recall}\ s.\varphi \mid \ \ldots \\
\varphi &::= \mathsf{rel}\ v_1\ v_2 \mid \mathsf{witnessed}\ s.\varphi \mid \ \ldots
\end{aligned}
$$

  - **Consistency** and **props. of the logic** via seq. calc. and cut-adm.

  - **Operational semantics** on configurations (e, σ, W)

$$
\begin{aligned}
(\mathsf{witness}\ s.\varphi, \sigma, W) &\rightsquigarrow (\mathsf{return}\ (), \sigma, W \cup \{s.\varphi\}) \\
(\mathsf{recall}\ s.\varphi, \sigma, W) &\rightsquigarrow (\mathsf{return}\ (), \sigma, W)
\end{aligned}
$$

  - **Total correctness** via progress, preservation, and SN

$$
\begin{array}{c} \vdash e : \textbf{MST}\ t\ (s.\varphi_{\mathsf{pre}})\ (s.x.s'.\varphi_{\mathsf{post}}) \\ \mathsf{witnessed}\ W \vdash \varphi_{\mathsf{pre}}[\sigma/s] \end{array}
\implies
\begin{array}{c} (e, \sigma, W) \rightsquigarrow^* (\mathsf{return}\ v, \sigma', W') \quad \vdash v : t \\ W \subseteq W' \quad \mathsf{witnessed}\ W' \vdash \mathsf{rel}\ \sigma\ \sigma' \\ \mathsf{witnessed}\ W' \vdash \varphi_{\mathsf{post}}[\sigma/s, v/x, \sigma'/s'] \end{array}
$$

A glimpse of the meta-theory

- We formalize `MST` in a small dependently typed CBV calculus

$$
\begin{aligned}
t &::= \mathsf{state} \mid x{:}t_1 \to \textbf{Tot}\ t_2 \mid x{:}t_1 \to \textbf{MST}\ t_2\ (s.\varphi_{\mathsf{pre}})\ (s.y.s'.\varphi_{\mathsf{post}}) \\
e &::= \mathsf{get} \mid \mathsf{put}\ v \mid \mathsf{witness}\ s.\varphi \mid \mathsf{recall}\ s.\varphi \mid \ \ldots \\
\varphi &::= \mathsf{rel}\ v_1\ v_2 \mid \mathsf{witnessed}\ s.\varphi \mid \ \ldots
\end{aligned}
$$

  - **Consistency** and **props. of the logic** via seq. calc. and cut-adm.

  - **Operational semantics** on configurations (e, σ, W)

$$
\begin{aligned}
(\mathsf{witness}\ s.\varphi, \sigma, W) &\quad\rightsquigarrow\quad (\mathsf{return}\ (), \sigma, W \cup \{s.\varphi\}) \\
(\mathsf{recall}\ s.\varphi, \sigma, W) &\quad\rightsquigarrow\quad (\mathsf{return}\ (), \sigma, W)
\end{aligned}
$$

  - **Total correctness** via progress, preservation, and SN

$$
\begin{array}{c}
\vdash e : \textbf{MST}\ t\ (s.\varphi_{\mathsf{pre}})\ (s.x.s'.\varphi_{\mathsf{post}}) \\
\mathsf{witnessed}\ W \vdash \varphi_{\mathsf{pre}}[\sigma/s]
\end{array}
\quad\Longrightarrow\quad
\begin{array}{c}
(e, \sigma, W) \rightsquigarrow^* (\mathsf{return}\ v, \sigma', W') \quad \vdash v : t \\
W \subseteq W' \quad \mathsf{witnessed}\ W' \vdash \mathsf{rel}\ \sigma\ \sigma' \\
\mathsf{witnessed}\ W' \vdash \varphi_{\mathsf{post}}[\sigma/s, v/x, \sigma'/s']
\end{array}
$$

A glimpse of the meta-theory

- We formalize `MST` in a small dependently typed CBV calculus

$$
\begin{aligned}
t &::= \mathsf{state} \mid x{:}t_1 \to \mathbf{Tot}\ t_2 \mid x{:}t_1 \to \mathbf{MST}\ t_2\ (s.\varphi_{\mathsf{pre}})\ (s.y.s'.\varphi_{\mathsf{post}}) \\
e &::= \mathsf{get} \mid \mathsf{put}\ v \mid \mathsf{witness}\ s.\varphi \mid \mathsf{recall}\ s.\varphi \mid \ \ldots \\
\varphi &::= \mathsf{rel}\ v_1\ v_2 \mid \mathsf{witnessed}\ s.\varphi \mid \ \ldots
\end{aligned}
$$

- **Consistency** and **props. of the logic** via seq. calc. and cut-adm.

- **Operational semantics** on configurations (e, σ, W)

$$
\begin{aligned}
(\mathsf{witness}\ s.\varphi, \sigma, W) &\rightsquigarrow (\mathsf{return}\ (), \sigma, W \cup \{s.\varphi\}) \\
(\mathsf{recall}\ s.\varphi, \sigma, W) &\rightsquigarrow (\mathsf{return}\ (), \sigma, W)
\end{aligned}
$$

- **Total correctness** via progress, preservation, and SN

$$
\begin{array}{c}
\vdash e : \mathbf{MST}\ t\ (s.\varphi_{\mathsf{pre}})\ (s.x.s'.\varphi_{\mathsf{post}}) \\
\mathsf{witnessed}\ W \vdash \varphi_{\mathsf{pre}}[\sigma/s]
\end{array}
\implies
\begin{array}{c}
(e, \sigma, W) \rightsquigarrow^* (\mathsf{return}\ v, \sigma', W') \quad \vdash v : t \\
W \subseteq W' \quad \mathsf{witnessed}\ W' \vdash \mathsf{rel}\ \sigma\ \sigma' \\
\mathsf{witnessed}\ W' \vdash \varphi_{\mathsf{post}}[\sigma/s, v/x, \sigma'/s']
\end{array}
$$

Conclusion

- In conclusion
  - making use of monotonicity is quite useful in verification
  - using monotonicity can be distilled into a simple interface
  - useful for both programming (refs.) and verification (crypto,TLS)
- Not in this talk (see the draft paper on arXiv)
  - temporarily **escaping the preorder** via snapshots
  - **revealing the representation** via selective monadic reification
- Future work
  - indexed effects in F*
  - combining preorders (e.g., ala graded monads)
  - modal aspects of `witnessed p`
  - connections with update monads (revealing the representation)
  - connections with other works, e.g., Iris and [Pilkiewicz,Pottier'11]

Conclusion

- In conclusion
  - making use of monotonicity is quite useful in verification
  - using monotonicity can be distilled into a simple interface
  - useful for both programming (refs.) and verification (crypto,TLS)
- Not in this talk (see the draft paper on arXiv)
  - temporarily **escaping the preorder** via snapshots
  - **revealing the representation** via selective monadic reification
- Future work
  - indexed effects in F*
  - combining preorders (e.g., ala graded monads)
  - modal aspects of `witnessed p`
  - connections with update monads (revealing the representation)
  - connections with other works, e.g., Iris and [Pilkiewicz,Pottier'11]

Conclusion

- In conclusion
  - making use of monotonicity is quite useful in verification
  - using monotonicity can be distilled into a simple interface
  - useful for both programming (refs.) and verification (crypto,TLS)
- Not in this talk (see the draft paper on arXiv)
  - temporarily **escaping the preorder** via snapshots
  - **revealing the representation** via selective monadic reification
- Future work
  - indexed effects in F*
  - combining preorders (e.g., ala graded monads)
  - modal aspects of `witnessed p`
  - connections with update monads (revealing the representation)
  - connections with other works, e.g., Iris and [Pilkiewicz,Pottier'11]

Thank you!

Questions?

Recalling a Witness:
Foundations and Applications of Monotonic State

(arXiv:1707.02466)