Higher-Order Constrained Horn Clauses (and Refinement Types)

Toby Cathcart Burn, Luke Ong and Steven Ramsay
University of Oxford

```
let add x y = x + y
let rec iter f m n =
  if n ≤ 0 then m else f n (iter f m (n-1))
in fun n → assert (n ≤ iter add 0 n)
```

```
let add x y = x + y
let rec iter f m n =
  if n ≤ 0 then m else f n (iter f m (n-1))
in fun n → assert (n ≤ iter add 0 n)
```

$$\forall xyz.\; z = x + y \Rightarrow \mathbf{Add}\; x\; y\; z$$

$$\forall fmn.\; n \leq 0 \Rightarrow \mathbf{Iter}\; f\; m\; n\; m$$

$$\forall fmnrp.\; n > 0 \land \mathbf{Iter}\; f\; m\; (n-1)\; p \land f\; n\; p\; r \Rightarrow \mathbf{Iter}\; f\; m\; n\; r$$

$$\forall nr.\; \mathbf{Iter}\; \mathbf{Add}\; 0\; n\; r \Rightarrow n \leq r$$

Higher-order "unknown" relations:

$$Iter : (\text{int} \to \text{int} \to \text{int} \to \text{bool}) \to \text{int} \to \text{int} \to \text{int} \to \text{bool}$$

$$\forall xyz.\ z = x + y \Rightarrow Add\ x\ y\ z$$

$$\forall fmn.\ n \leq 0 \Rightarrow Iter\ f\ m\ n\ m$$

$$\forall fmnrp.\ n > 0 \wedge Iter\ f\ m\ (n-1)\ p \wedge f\ n\ p\ r \Rightarrow Iter\ f\ m\ n\ r$$

$$\forall nr.\ Iter\ Add\ 0\ n\ r \Rightarrow n \leq r$$

Quantification at higher-sorts:

$\forall$ at sort $\text{int} \to \text{int} \to \text{int} \to \text{bool}$

Literals headed by variables:

$f\ n\ p\ r : \text{bool}$

Standard
semantics of sorts

$S[\![\text{int}]\!]$ All of the integers

$S[\![\text{bool}]\!]$ Two truth values, $F \subseteq T$

$S[\![\sigma \rightarrow \tau]\!]$ All functions from $S[\![\sigma]\!]$ to $S[\![\tau]\!]$

$$\mathcal{M} \vDash_S \exists x\colon (\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}.\, G$$

There is some predicate on sets of integers that makes G true in $\mathcal{M}$

Least models

and the monotone semantics

Theorem

Satisfiable systems of higher-order constrained Horn clauses do not necessarily possess least models.

(Least with respect to inclusion of relations)

Theorem

Satisfiable systems of higher-order constrained Horn clauses do not necessarily possess least models.
(Least with respect to inclusion of relations)

$$S[\![\text{one}]\!] = \{\star\}$$

$$\boldsymbol{Q} : \text{one} \to \text{bool}$$
$$\boldsymbol{P} : \big((\text{one} \to \text{bool}) \to \text{bool}\big) \to \text{bool}$$

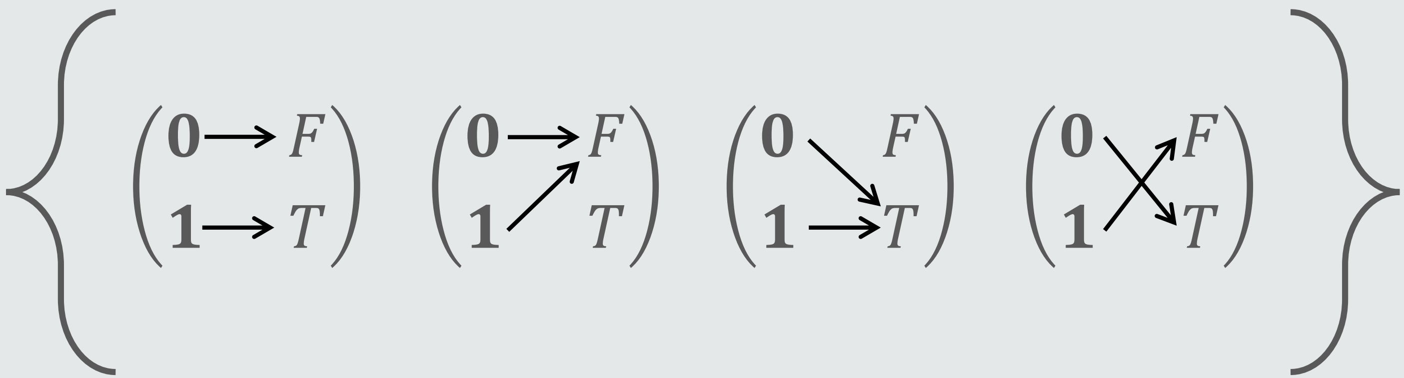
$$\forall x.\, x\; \boldsymbol{Q} \Rightarrow \boldsymbol{P}\; x$$

$$S[\![\text{one}]\!] = \{\star\}$$

0 1

$$S[\![\text{one} \to \text{bool}]\!] = \{\ (\star \to F)\ \ (\star \to T)\ \}$$

$$S[\![(\text{one} \to \text{bool}) \to \text{bool}]\!] =$$



$\boldsymbol{Q}$: one → bool

$\boldsymbol{P}$: ((one → bool) → bool) → bool

$$\forall x.\, x\,\boldsymbol{Q} \Rightarrow \boldsymbol{P}\,x$$

$$\alpha(\boldsymbol{Q}) = \mathbf{0}$$

$$\alpha(\boldsymbol{P})\begin{pmatrix}\mathbf{0} \mapsto F \\ \mathbf{1} \mapsto T\end{pmatrix} = F \qquad \alpha(\boldsymbol{P})\begin{pmatrix}\mathbf{0} \mapsto T \\ \mathbf{1} \mapsto T\end{pmatrix} = T$$

$$\alpha(\boldsymbol{P})\begin{pmatrix}\mathbf{0} \mapsto F \\ \mathbf{1} \mapsto F\end{pmatrix} = F \qquad \alpha(\boldsymbol{P})\begin{pmatrix}\mathbf{0} \mapsto T \\ \mathbf{1} \mapsto F\end{pmatrix} = T$$

$\boldsymbol{Q} : \text{one} \to \text{bool}$

$\boldsymbol{P} : \big((\text{one} \to \text{bool}) \to \text{bool}\big) \to \text{bool}$

$$\forall x.\, x\ \boldsymbol{Q} \Rightarrow \boldsymbol{P}\ x$$

$$\beta(\boldsymbol{Q}) = \mathbf{1}$$

$$\beta(\boldsymbol{P})\begin{pmatrix}\mathbf{0} \mapsto F \\ \mathbf{1} \mapsto T\end{pmatrix} = T \qquad \beta(\boldsymbol{P})\begin{pmatrix}\mathbf{0} \mapsto T \\ \mathbf{1} \mapsto T\end{pmatrix} = T$$

$$\beta(\boldsymbol{P})\begin{pmatrix}\mathbf{0} \mapsto F \\ \mathbf{1} \mapsto F\end{pmatrix} = F \qquad \beta(\boldsymbol{P})\begin{pmatrix}\mathbf{0} \mapsto T \\ \mathbf{1} \mapsto F\end{pmatrix} = F$$

$\forall x.\, x\ \boldsymbol{Q} \Rightarrow \boldsymbol{P}\ x$

$$\alpha(\boldsymbol{Q}) = \mathbf{0} \qquad\qquad \beta(\boldsymbol{Q}) = \mathbf{1}$$

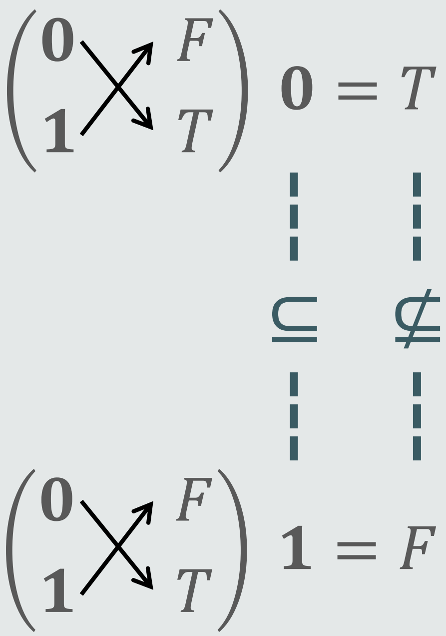
$$\alpha(\boldsymbol{P})\begin{pmatrix} \mathbf{0} & \longrightarrow & F \\ \mathbf{1} & \longrightarrow & T \end{pmatrix} = F \qquad\qquad \beta(\boldsymbol{P})\begin{pmatrix} \mathbf{0} & \longrightarrow & F \\ \mathbf{1} & \longrightarrow & T \end{pmatrix} = T$$

$$\alpha(\boldsymbol{P})\begin{pmatrix} \mathbf{0} & \longrightarrow & F \\ \mathbf{1} & \nearrow & T \end{pmatrix} = F \qquad\qquad \beta(\boldsymbol{P})\begin{pmatrix} \mathbf{0} & \longrightarrow & F \\ \mathbf{1} & \nearrow & T \end{pmatrix} = F$$

$$\alpha(\boldsymbol{P})\begin{pmatrix} \mathbf{0} & \searrow & F \\ \mathbf{1} & \longrightarrow & T \end{pmatrix} = T \qquad\qquad \beta(\boldsymbol{P})\begin{pmatrix} \mathbf{0} & \searrow & F \\ \mathbf{1} & \longrightarrow & T \end{pmatrix} = T$$

$$\alpha(\boldsymbol{P})\begin{pmatrix} \mathbf{0} & \searrow & F \\ \mathbf{1} & \nearrow & T \end{pmatrix} = T \qquad\qquad \beta(\boldsymbol{P})\begin{pmatrix} \mathbf{0} & \searrow & F \\ \mathbf{1} & \nearrow & T \end{pmatrix} = F$$

$x\ Q$



Monotone
semantics of sorts

$M[\![\text{int}]\!]$ All of the integers, ordered discretely

$M[\![\text{bool}]\!]$ Two truth values, $F \subseteq T$

$M[\![\sigma \to \tau]\!]$ All *monotone* functions from $M[\![\sigma]\!]$ to $M[\![\tau]\!]$

$$\mathcal{M} \vDash_M \exists x : (\text{int} \to \text{bool}) \to \text{bool}. G$$

There is some <u>monotone</u> predicate on sets of integers that makes G true in $\mathcal{M}$

$M[\![\text{int} \to \text{bool}]\!]$ All sets of integers

$M[\![(\text{int} \to \text{bool}) \to \text{bool}]\!]$ All upward closed sets of sets of integers

$M[\![\big((\text{int} \to \text{bool}) \to \text{bool}\big) \to \text{bool}]\!]$ All upward closed sets of upward closed sets of sets of integers

$$x \mapsto \{\,\{\,1\,\}\,\} \quad \not\models \quad \exists yz.\ x\ y \wedge y\ z$$

Standard
semantics

Completely standard satisfiability problem (modulo background theory) in higher-order logic.

No least model

Monotone
semantics

Bespoke satisfiability problem with highly restricted class of models.

Least model arising in the usual way

Theorem

Given set of higher-order constrained horn clauses *H:*

- For each (standard) model β of the standard semantics of *H* there is a (monotone) model $U(\beta)$ of the monotone semantics of *H*.
- For each (monotone) model α of the monotone semantics of *H*, there is a (standard) model $I(\alpha)$ of the standard semantics of *H*.

Mapping models means mapping relations:

$$M[\![((\mathrm{int} \to \mathrm{bool}) \to \mathrm{bool}) \to \mathrm{bool}]\!]$$

$$S[\![((\mathrm{int} \to \mathrm{bool}) \to \mathrm{bool}) \to \mathrm{bool}]\!]$$

Mapping models means mapping relations:

$$M[\![((\text{int} \to \text{bool}) \to \text{bool}) \to \text{bool}]\!]$$

$$S[\![((\text{int} \to \text{bool}) \to \text{bool}) \to \text{bool}]\!]$$

From monotone to standard: inclusion?

$$\alpha(\boldsymbol{P}) = \{X \in \mathcal{P}(\mathcal{P}(\mathbb{Z})) : X \text{ upward closed }\}$$

$$\alpha \quad \vDash_M \quad \forall x\colon (\text{int} \to \text{bool}) \to \text{bool}. \quad \mathit{true} \Rightarrow \boldsymbol{P}\, x$$

$$\alpha \quad \nvDash_S \quad \forall x\colon (\text{int} \to \text{bool}) \to \text{bool}. \quad \mathit{true} \Rightarrow \boldsymbol{P}\, x$$

$$M[\![((\text{int} \to \text{bool}) \to \text{bool}) \to \text{bool}]\!]$$

J

$$S[\![((\text{int} \to \text{bool}) \to \text{bool}) \to \text{bool}]\!]$$

Inclusion: constructs relations that are typically too small

$$S[\![((\text{int} \to \text{bool}) \to \text{bool}) \to \text{bool}]\!]$$

$$J(r)(t) = \begin{cases} r(t) & \text{if } t \in M[\![(\text{int} \to \text{bool}) \to \text{bool}]\!] \\ F & \text{otherwise} \end{cases}$$

$$S[\![(\text{int} \to \text{bool}) \to \text{bool}]\!]$$

$$M[\![((\text{int} \to \text{bool}) \to \text{bool}) \to \text{bool}]\!]$$

$$J^c$$

$$S[\![((\text{int} \to \text{bool}) \to \text{bool}) \to \text{bool}]\!]$$

Complementary inclusion: constructs relations that are typically too large

$$S[\![((\text{int} \to \text{bool}) \to \text{bool}) \to \text{bool}]\!]$$

$$J^c(r)(t) = \begin{cases} r(t) & \mathit{if}\ t \in M[\![(\text{int} \to \text{bool}) \to \text{bool}]\!] \\ T & \mathit{otherwise} \end{cases}$$

$$S[\![(\text{int} \to \text{bool}) \to \text{bool}]\!]$$

Determine the value of standard relation $J(r)$ on non-(hereditarily) monotone input t by considering the value of r on:

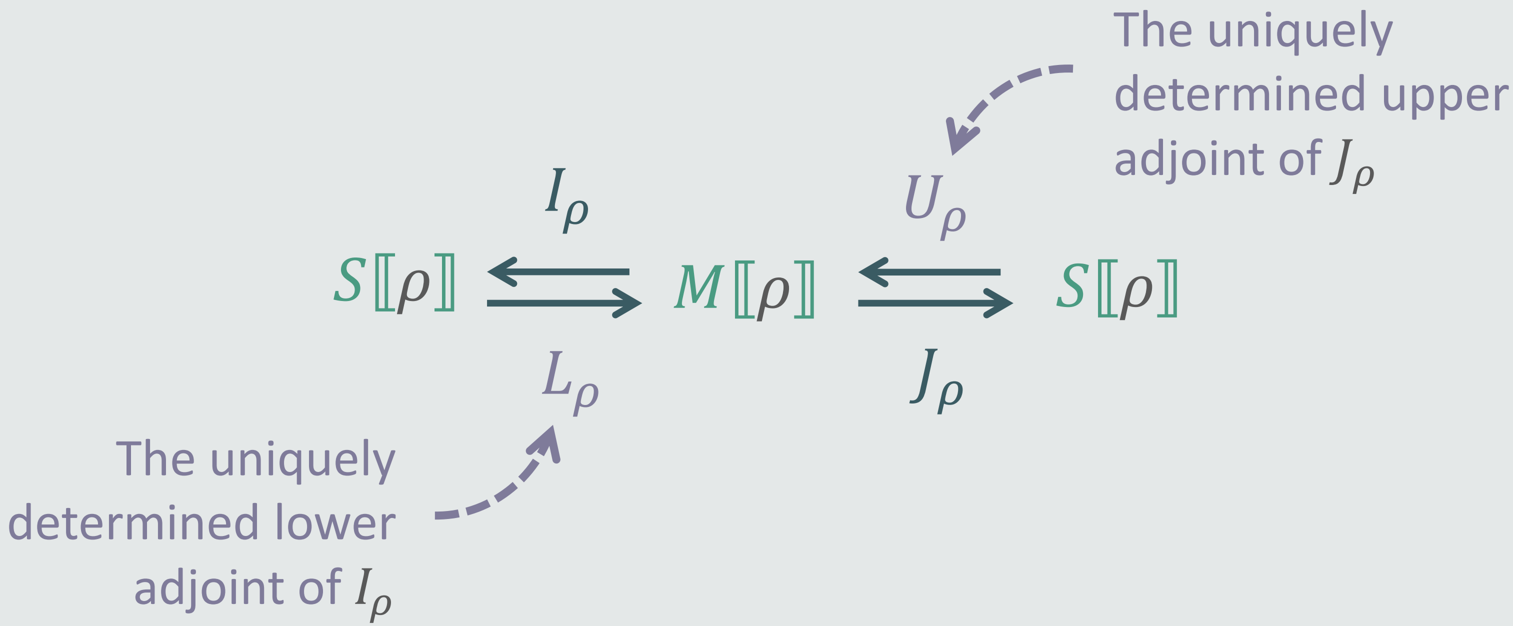
The largest (hereditarily) monotone relation of at most t

$$J(r)\big(\{\{\,1\,\}\}\big) = r\,(\emptyset)$$

The smallest (hereditarily) monotone relation of at least t

$$I(r)\big(\{\{\,1\,\}\}\big) = r\,\big(\{\{1\},\{1,2\},\{1,2,3\},\ldots\}\big)$$

For each sort of relations ρ:



$$I_{bool}(b) = b \qquad J_{bool}(b) = b$$

$$I_{int\to\rho}(r) = I_\rho \circ r \qquad J_{int\to\rho}(r) = J_\rho \circ r$$

$$I_{\rho_1\to\rho_2}(r) = I_{\rho_2} \circ r \circ L_{\rho_1} \qquad J_{\rho_1\to\rho_2}(r) = J_{\rho_2} \circ r \circ U_{\rho_1}$$

$$S[\![\rho]\!] \;\overset{I_\rho}{\underset{L_\rho}{\leftrightarrows}}\; M[\![\rho]\!] \;\overset{U_\rho}{\underset{J_\rho}{\leftrightarrows}}\; S[\![\rho]\!]$$

Theorem

Given set of higher-order constrained horn clauses *H:*

- For each (standard) model β of the standard interpretation of *H* there is a (monotone) model $U(\beta)$ of the monotone interpretation of *H*.
- For each (monotone) model α of the monotone interpretation of *H*, there is a (standard) model $I(\alpha)$ of the standard interpretation of *H*.

Refinement Types

in the rest of the paper

A refinement type system for solving the monotone satisfiability problem:

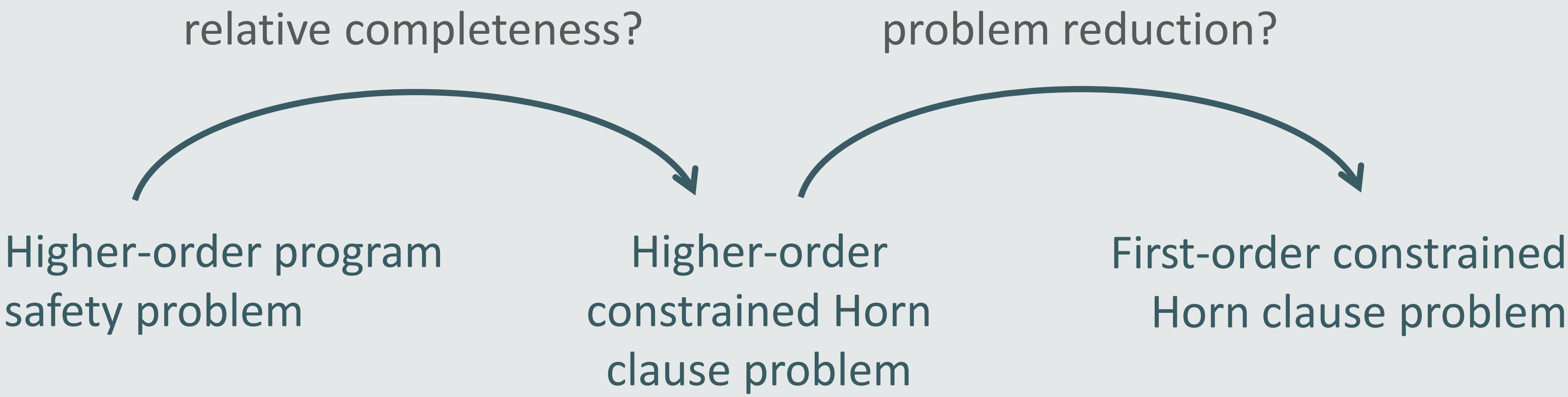
$$\Gamma \vdash G : bool\langle\phi\rangle$$

In models satisfying Γ … … the truth of goal G … … is bounded above by constraint ϕ

Typability reduces to first-order constrained Horn clause solving

Given any refinement type T and any goal term G, $G : T$ can be expressed as a higher-order constrained Horn clause.

Future
work



Refinements of type constructors:

$$int \text{ refined by } P : int \to bool$$

$$List \text{ refined by } P : (\alpha \to bool) \to List\ \alpha \to bool$$

Thanks.

Atom
e.g. *Iter f m (n-1) p*
e.g. *f n p r*

Constraint
e.g. *x > 3*

$$G \;::= A \mid G \wedge G \mid G \vee G \mid \phi \mid \exists x{:}\,\sigma.\, G$$

$$D \;::= true \mid G \Rightarrow X y_1 \ldots y_k \mid D \wedge D \mid \forall x{:}\,\sigma.\, D$$

Relational "unknown"
e.g. *Iter*

$$J_{bool}(b) = b$$
$$J_{int\to\rho}(r) = J_\rho \circ r$$
$$J_{\rho_1\to\rho_2}(r) = J_{\rho_2} \circ r \circ U_{\rho_1}$$

At $bool$: $M[\![bool]\!] = S[\![bool]\!]$

J_{bool} is the identity with upper adjoint U_{bool} also the identity

At $int \to bool$: $M[\![int \to bool]\!] = S[\![int \to bool]\!]$

$J_{int\to bool}(r) = J_{bool} \circ r = r$ is the identity
with upper adjoint $U_{int\to bool}$ also the identity

At $(int \to bool) \to bool$: $M[\![(int \to bool) \to bool]\!] \subseteq S[\![(int \to bool) \to bool]\!]$

$J_{(int\to bool)\to bool}(r) = J_{bool} \circ r \circ U_{int\to bool} = r$ is an inclusion

$$U_{(int\to bool)\to bool}(s) = \bigcup\left\{t \in M[\![(int \to bool) \to bool]\!] \,\middle|\, J_{(int\to bool)\to bool}(t) \subseteq s\right\}$$
$$= \bigcup\{t \in M[\![(int \to bool) \to bool]\!] \mid t \subseteq s\}$$