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 \( n \leq 0 \) then \( m \) else \( f \ n \ (\text{iter} \ f \ m \ (n-1)) \)

in fun \( n \rightarrow \text{assert} \ (n \leq \text{iter} \ add \ 0 \ n) \)
let \textit{add} x y \equiv x + y \\
let \textit{rec iter} f m n = \\
\quad \text{if } n \leq 0 \text{ then } m \text{ else } f n (\textit{iter} f m (n-1)) \\
in \text{fun } n \rightarrow \text{assert } (n \leq \textit{iter add} 0 n)

\forall xyz \; z = x + y \Rightarrow \text{Add } x \; y \; z \\
\forall fmn \; n \leq 0 \Rightarrow \text{Iter } f \; m \; n \; m \\
\forall fmrnp \; n > 0 \land \text{Iter } f \; m \; (n-1) \; p \land f \; n \; p \; r \Rightarrow \text{Iter } f \; m \; n \; r \\
\forall nr \; \text{Iter Add } 0 \; n \; r \Rightarrow n \leq r
Higher-order “unknown” relations:

\[ \text{Iter} : (\text{int} \to \text{int} \to \text{int} \to \text{bool}) \to \text{int} \to \text{int} \to \text{int} \to \text{bool} \]

\[ \forall xyz \quad z = x + y \quad \Rightarrow \quad \text{Add} \; x \; y \; z \]

\[ \forall fmn \quad n \leq 0 \quad \Rightarrow \quad \text{Iter} \; f \; m \; n \; m \]

\[ \forall fmpn \quad n > 0 \land \text{Iter} \; f \; m \; (n - 1) \; p \land f \; n \; p \; r \quad \Rightarrow \quad \text{Iter} \; f \; m \; n \; r \]

\[ \forall nr \quad \text{Iter} \; \text{Add} \; 0 \; n \; r \quad \Rightarrow \quad n \leq r \]

Quantification at higher sorts:

\[ \forall \text{at sort} \quad \text{int} \to \text{int} \to \text{int} \to \text{bool} \]

Literals headed by variables:

\[ f \; n \; p \; r : \text{bool} \]
Standard semantics of sorts

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

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

\[ S[\sigma \rightarrow \tau] \quad \text{All functions from } S[\sigma] \text{ to } S[\tau] \]

\[ \mathcal{M} \models_S \exists x : (\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}. \, G \]

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)

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

\[ Q : \text{one} \to \text{bool} \]
\[ P : ((\text{one} \to \text{bool}) \to \text{bool}) \to \text{bool} \]

\[ \forall x. \ x \ Q \Rightarrow P \ x \]
\[ S[\text{one}] = \{ \star \} \]

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

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

\[ \left\{ \begin{array}{c}
(0 \to F) \\
(1 \to T)
\end{array} \right\} \cup \left\{ \begin{array}{c}
(0 \to F) \\
(1 \to T)
\end{array} \right\} \cup \left\{ \begin{array}{c}
(0 \to F) \\
(1 \to T)
\end{array} \right\} \cup \left\{ \begin{array}{c}
(0 \to F) \\
(1 \times F)
\end{array} \right\} \]
\( Q : \text{one} \to \text{bool} \)
\( P : ((\text{one} \to \text{bool}) \to \text{bool}) \to \text{bool} \)

\[ \forall x. x \ Q \Rightarrow P \ x \]

\( \alpha(Q) = 0 \)

\( \alpha(P) \begin{pmatrix} 0 & \xrightarrow{F} \\ 1 & \xrightarrow{T} \end{pmatrix} = F \)

\( \alpha(P) \begin{pmatrix} 0 & \xrightarrow{F} \\ 1 & \xrightarrow{T} \end{pmatrix} = T \)

\( \alpha(P) \begin{pmatrix} 0 & \xrightarrow{T} \\ 1 & \xrightarrow{F} \end{pmatrix} = F \)

\( \alpha(P) \begin{pmatrix} 0 & \xrightarrow{T} \\ 1 & \xrightarrow{F} \end{pmatrix} = T \)
\( Q : \text{one} \to \text{bool} \)

\( P : (\text{one} \to \text{bool}) \to \text{bool} \)

\( \forall x. x \ Q \Rightarrow P \ x \)

\[ \beta(Q) = 1 \]

\[
\begin{align*}
\beta(P) \left( \begin{array}{c}
0 \\
1
\end{array} \rightarrow \begin{array}{c}
F \\
T
\end{array} \right) &= T \\
\beta(P) \left( \begin{array}{c}
0 \\
1
\end{array} \rightarrow \begin{array}{c}
F \\
T
\end{array} \right) &= F
\end{align*}
\]

\[
\begin{align*}
\beta(P) \left( \begin{array}{c}
0 \\
1
\end{array} \rightarrow \begin{array}{c}
F \\
T
\end{array} \right) &= T \\
\beta(P) \left( \begin{array}{c}
0 \\
1
\end{array} \rightarrow \begin{array}{c}
F \\
T
\end{array} \right) &= F
\end{align*}
\]
\[
\forall x. x \ Q \Rightarrow P \ x
\]

\[
\begin{align*}
\alpha(Q) &= 0 \\
\alpha(P) \begin{pmatrix} 0 & \rightarrow & F \\ 1 & \rightarrow & T \end{pmatrix} &= F \\
\alpha(P) \begin{pmatrix} 0 & \rightarrow & F \\ 1 & \rightarrow & T \end{pmatrix} &= F \\
\alpha(P) \begin{pmatrix} 0 & \rightarrow & F \\ 1 & \rightarrow & T \end{pmatrix} &= T \\
\alpha(P) \begin{pmatrix} 0 & \rightarrow & F \\ 1 & \rightarrow & T \end{pmatrix} &= T \\
\beta(Q) &= 1 \\
\beta(P) \begin{pmatrix} 0 & \rightarrow & F \\ 1 & \rightarrow & T \end{pmatrix} &= T \\
\beta(P) \begin{pmatrix} 0 & \rightarrow & F \\ 1 & \rightarrow & T \end{pmatrix} &= F \\
\beta(P) \begin{pmatrix} 0 & \rightarrow & F \\ 1 & \rightarrow & T \end{pmatrix} &= T \\
\beta(P) \begin{pmatrix} 0 & \rightarrow & F \\ 1 & \rightarrow & T \end{pmatrix} &= F
\end{align*}
\]
\( x \in Q \)

\[
\begin{pmatrix}
0 & F \\
1 & T \\
\end{pmatrix}
\]

\( 0 = T \)

\[
\begin{pmatrix}
0 & F \\
1 & T \\
\end{pmatrix}
\]

\( 1 = F \)
Monotone semantics of sorts

\( M[\text{int}] \) All of the integers, ordered discretely

\( M[\text{bool}] \) Two truth values, \( F \subseteq T \)

\( M[\sigma \rightarrow \tau] \) All monotone functions from \( M[\sigma] \) to \( M[\tau] \)

\[ M \models \exists x : (\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}. \ G \]

There is some monotone predicate on sets of integers that makes \( G \) true in \( M \)
\[ M[\text{int} \rightarrow \text{bool}] \quad \text{All sets of integers} \]

\[ M[(\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}] \quad \text{All upward closed sets of sets of integers} \]

\[ M[(\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}] \quad \text{All upward closed sets of upward closed sets of sets of integers} \]

\[ x \mapsto \{ \{ 1 \} \} \quad \nmid \quad \exists yz. \ x \ y \land y \ z \]
| Standard semantics | Monotone semantics |
|--------------------|--------------------|
| Completely standard satisfiability problem (modulo background theory) in higher-order logic. | Bespoke satisfiability problem with highly restricted class of models. |
| No least model | Least model arising in the usual way |
Theorem

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

- For each (standard) model $\beta$ of the standard semantics of $H$ there is a (monotone) model $U(\beta)$ of the monotone semantics of $H$.
- For each (monotone) model $\alpha$ of the monotone semantics of $H$, there is a (standard) model $I(\alpha)$ of the standard semantics of $H$. 
Mapping models means mapping relations:

\[ M \left[ \left( \text{int} \to \text{bool} \right) \to \text{bool} \right] \]

\[ S \left[ \left( \text{int} \to \text{bool} \right) \to \text{bool} \right] \]
Mapping models means mapping relations:

\[ M[(\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}] \]

\[ S[(\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}] \]

From monotone to standard: inclusion?

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

\[ \alpha \models_M \forall x : (\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}. \quad \text{true} \Rightarrow P \, x \]

\[ \alpha \not\models_S \forall x : (\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}. \quad \text{true} \Rightarrow P \, x \]
Inclusion: constructs relations that are typically too small

\[ J(r)(t) = \begin{cases} r(t) & \text{if } t \in M[(\text{int} \rightarrow \text{bool}) \rightarrow \text{bool}] \\ F & \text{otherwise} \end{cases} \]
Complementary inclusion: constructs relations that are typically too large

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

\[
J(r)(\{\{ 1 \}\}) = r(\emptyset)
\]

The smallest (hereditarily) monotone relation of at least \( t \)

\[
I(r)(\{\{ 1 \}\}) = r(\{\{1\}, \{1,2\}, \{1,2,3\}, \ldots\})
\]
For each sort of relations $\rho$:

$\forall \rho: \begin{align*}
I_{\text{bool}}(b) &= b \\
I_{\text{int} \to \rho}(r) &= I_{\rho} \circ r \\
I_{\rho_1 \to \rho_2}(r) &= I_{\rho_2} \circ r \circ L_{\rho_1}
\end{align*}$

$\forall \rho: \begin{align*}
J_{\text{bool}}(b) &= b \\
J_{\text{int} \to \rho}(r) &= J_{\rho} \circ r \\
J_{\rho_1 \to \rho_2}(r) &= J_{\rho_2} \circ r \circ U_{\rho_1}
\end{align*}$
Given set of higher-order constrained horn clauses $H$:

- For each (standard) model $\beta$ of the standard interpretation of $H$ there is a (monotone) model $U(\beta)$ of the monotone interpretation of $H$.
- For each (monotone) model $\alpha$ 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:

\[ \Gamma \vdash G : \text{bool} \langle \phi \rangle \]

In models satisfying \( \Gamma \) the truth of goal \( G \) is bounded above by constraint \( \phi \)

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` refined by $P : \text{int} \to \text{bool}$
- `List` refined by $P : (\alpha \to \text{bool}) \to \text{List} \alpha \to \text{bool}$
Thanks.
\[
G ::= A \mid G \land G \mid G \lor G \mid \phi \mid \exists x: \sigma. G
\]

\[
D ::= \text{true} \mid G \Rightarrow Xy_1 \ldots y_k \mid D \land D \mid \forall x: \sigma. D
\]
At \textit{bool}: \quad M[\textit{bool}] = S[\textit{bool}]

\( J_{\text{bool}}(b) = b \)

\( J_{\text{int} \to \rho}(r) = J_\rho \circ r \)

\( J_{\rho_1 \to \rho_2}(r) = J_{\rho_2} \circ r \circ U_{\rho_1} \)

\( J_{\text{bool}} \) is the identity with upper adjoint \( U_{\text{bool}} \) also the identity

At \textit{int} \to \textit{bool}: \quad M[\textit{int} \to \textit{bool}] = S[\textit{int} \to \textit{bool}]

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

At \textit{(int} \to \textit{bool}) \to \textit{bool} : \quad M[\textit{(int} \to \textit{bool}) \to \textit{bool}] \subseteq S[\textit{(int} \to \textit{bool}) \to \textit{bool}]$

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

\( U_{\text{(int} \to \text{bool}) \to \text{bool}}(s) = \bigcup \{ t \in M[\text{(int} \to \text{bool}) \to \text{bool}] \mid J_{\text{(int} \to \text{bool}) \to \text{bool}}(t) \subseteq s \} \)

\( = \bigcup \{ t \in M[\text{(int} \to \text{bool}) \to \text{bool}] \mid t \subseteq s \} \)