Validating QBF Validity in HOL4

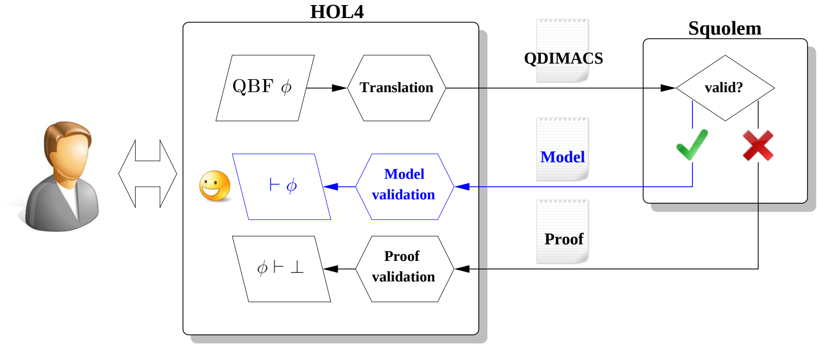
Ramana Kumar and Tjark Weber

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

ITP 2011 (Berg en Dal)

August 25, 2011

Introduction

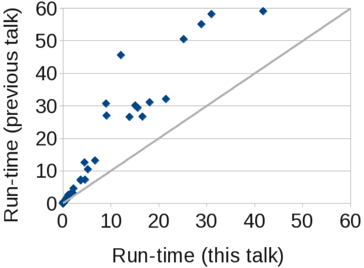


Comparison to Kunčar's Approach

- We happen to use HOL4 instead of HOL Light.

Comparison to Kunčar's Approach

- We happen to use HOL4 instead of HOL Light.
- Our solution is often twice as fast.



Comparison to Kunčar's Approach

- We happen to use HOL4 instead of HOL Light.
- Our solution is often twice as fast.
- Our solution is simpler.

$$\begin{tikzcd}
\vdash \mathcal{M} \implies \phi \arrow[d] \\
\vdash \mathbf{Q}\mathcal{M} \implies \mathbf{Q}\phi \\
\vdash \mathbf{Q}\mathcal{M} \arrow[u]
\end{tikzcd}$$

$$\begin{tikzcd}
\vdash \mathcal{M} \implies \phi \arrow[d] \\
\mathcal{M} \vdash \phi \arrow[d] \\
\vdash \mathbf{Q}\phi
\end{tikzcd}$$

Valid QBF and Models

QBF

$$\forall x\, \exists y\, \exists z.\; (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (\neg x \vee y \vee z) \wedge \\ (\neg x \vee \neg y \vee \neg z) \wedge (\neg y \vee z)$$

Model

$$y \mapsto f_y, \quad f_y(x) = \bot \qquad\qquad z \mapsto f_z, \quad f_z(x, y) = x$$

Valid QBF and Models

QBF

$$\forall x\, \exists y\, \exists z.\ (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z) \wedge (\neg y \vee z)$$

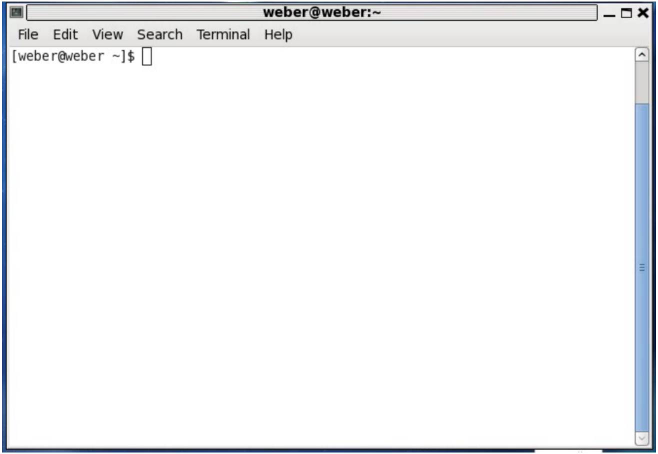
Model

$$y \mapsto f_y, \quad f_y(x) = \bot \qquad\qquad z \mapsto f_z, \quad f_z(x, y) = x$$

Propositional Tautology

$$(x \vee \bot \vee \neg x) \wedge (x \vee \top \vee x) \wedge (\neg x \vee \bot \vee x) \wedge (\neg x \vee \top \vee \neg x) \wedge (\top \vee x)$$

Demo



```
[weber@weber ~]$ 
```

Selected HOL4 Inference Rules

$$\frac{}{\{\phi\} \vdash \phi}\ \textsc{Assume}_{\phi} \qquad \frac{\Gamma \vdash \phi}{\Gamma\,\theta \vdash \phi\,\theta}\ \textsc{Inst}_{\theta} \qquad \frac{}{\vdash t = t}\ \textsc{Refl}_{t}$$

$$\frac{\Gamma \vdash \psi}{\Gamma \setminus \{\phi\} \vdash \phi \implies \psi}\ \textsc{Disch}_{\phi} \qquad \frac{\Gamma \vdash \phi \implies \psi \qquad \Delta \vdash \phi}{\Gamma \cup \Delta \vdash \psi}\ \mathrm{MP}$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \forall x.\, \phi}\ \textsc{Gen}_{x}\ (x \text{ not free in } \Gamma) \qquad \frac{\Gamma \vdash \phi[t]}{\Gamma \vdash \exists x.\, \phi[x]}\ \textsc{Exists}_{(\exists x.\, \phi[x],t)}$$

Validating Squolem's Certificates in HOL4

QBF

$$\forall x\, \exists y\, \exists z.\ \phi, \text{ where } \phi = (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z) \wedge (\neg y \vee z)$$

Validating Squolem's Certificates in HOL4

QBF

$$\forall x\,\exists y\,\exists z.\ \phi,\ \text{where}\ \phi = (x \lor y \lor \neg z) \land (x \lor \neg y \lor z) \land (\neg x \lor y \lor z) \land (\neg x \lor \neg y \lor \neg z) \land (\neg y \lor z)$$

Model

$v_1 \Leftrightarrow \bot, \quad v_2 \Leftrightarrow x, \quad y \Leftrightarrow v_1, \quad z \Leftrightarrow v_2$

Validating Squolem's Certificates in HOL4

QBF

$$\forall x\, \exists y\, \exists z.\ \phi\text{, where } \phi = (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z) \wedge (\neg y \vee z)$$

Model

$v_1 \Leftrightarrow \bot, \quad v_2 \Leftrightarrow x, \quad y \Leftrightarrow v_1, \quad z \Leftrightarrow v_2$

1. MiniSat proves $\vdash (v_1 \Leftrightarrow \bot) \implies (v_2 \Leftrightarrow x) \implies (y \Leftrightarrow v_1) \implies (z \Leftrightarrow v_2) \implies \phi$

Validating Squolem's Certificates in HOL4

QBF

$\forall x\, \exists y\, \exists z.\ \phi$, where $\phi = (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z) \wedge (\neg y \vee z)$

Model

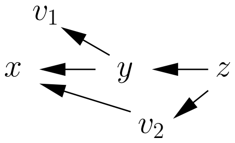
$v_1 \Leftrightarrow \bot, \quad v_2 \Leftrightarrow x, \quad y \Leftrightarrow v_1, \quad z \Leftrightarrow v_2$

1. MiniSat proves $\vdash (v_1 \Leftrightarrow \bot) \implies (v_2 \Leftrightarrow x) \implies (y \Leftrightarrow v_1) \implies (z \Leftrightarrow v_2) \implies \phi$
2. $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:

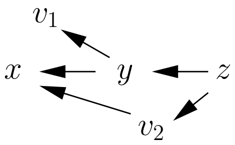


e.g., $z < v_2 < y < x < v_1$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

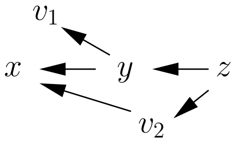
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\qquad \{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3 Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

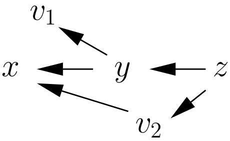
4 Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \exists z.\ \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

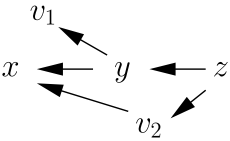
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, v_2 \Leftrightarrow v_2\} \vdash \exists z.\ \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\qquad\qquad$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

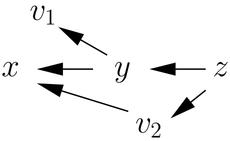
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1\} \vdash \exists z.\ \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\,\exists y\,\exists z.\ \phi$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

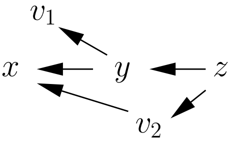
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot, x \Leftrightarrow x, y \Leftrightarrow v_1\} \vdash \exists z.\ \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

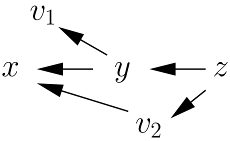
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot, y \Leftrightarrow v_1\} \vdash \exists z.\ \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\,\exists y\,\exists z.\ \phi$ $\quad\quad$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

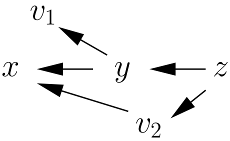
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot, y \Leftrightarrow v_1\} \vdash \exists y\,\exists z.\ \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

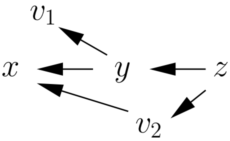
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot, v_1 \Leftrightarrow v_1\} \vdash \exists y\, \exists z.\ \phi$$

Validating Squolem's Certificates in HOL4

$\forall x \, \exists y \, \exists z. \; \phi$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

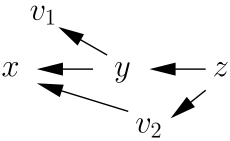
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot\} \vdash \exists y \, \exists z. \; \phi$$

Validating Squolem's Certificates in HOL4

$\forall x \, \exists y \, \exists z. \; \phi$ $\qquad$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

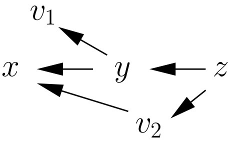
4. Eliminate hypotheses, introduce quantifiers:

$$\{v_1 \Leftrightarrow \bot\} \vdash \forall x \, \exists y \, \exists z. \; \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

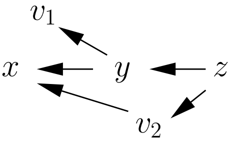
4. Eliminate hypotheses, introduce quantifiers:

$$\{\bot \Leftrightarrow \bot\} \vdash \forall x\, \exists y\, \exists z.\ \phi$$

Validating Squolem's Certificates in HOL4

$\forall x\, \exists y\, \exists z.\ \phi$ $\qquad$ $\{v_1 \Leftrightarrow \bot, v_2 \Leftrightarrow x, y \Leftrightarrow v_1, z \Leftrightarrow v_2\} \vdash \phi$

3. Topologically sort all variables:



e.g., $z < v_2 < y < x < v_1$

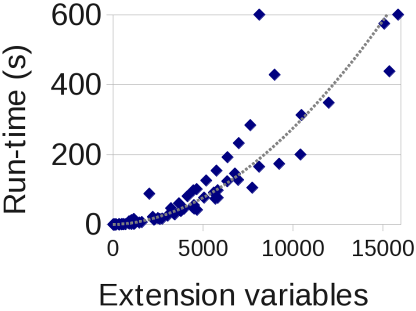
4. Eliminate hypotheses, introduce quantifiers:

$$\emptyset \vdash \forall x\, \exists y\, \exists z.\ \phi$$

Evaluation

Evaluation on 100 valid QBF problems from the *2005 fixed instance* and *2006 preliminary QBF-Eval* data sets

up to 133 alternating quantifiers, 11,570 variables, 131,072 clauses



Evaluation

Evaluation on 100 valid QBF problems from the *2005 fixed instance* and *2006 preliminary QBF-Eval* data sets

up to 133 alternating quantifiers, 11,570 variables, 131,072 clauses

Success rate: 87% (at 600 s)

- Average run-times: 134 s (de Bruijn), 163 s (name-carrying)
- Essentially quadratic in the number of extension variables
- 18 times slower than Squolem
- 16 times slower than non-LCF-style validation

Conclusions

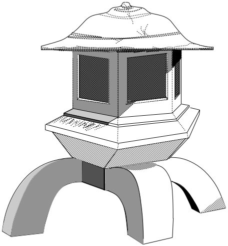
Integration of a QBF solver with HOL4

- Improved automation for QBF in HOL4
- High correctness assurances for Squolem's results

- LCF-style proof checking for QBF validity is often feasible.
- HOL4: `http://hol.sourceforge.net/`

Future Work

- Applications, case studies
- Other ITPs/QBF solvers
- Different approaches (e.g., reflection)



Future Work

- Applications, case studies
- Other ITPs/QBF solvers
- Different approaches (e.g., reflection)

Thank You!