Towards the Compression of First-Order Resolution Proofs by Lowering Unit Clauses

J. Gorzny[1] B. Woltzenlogel Paleo[2]

[1]University of Victoria

[2]Vienna University of Technology

6 August 2015

Proof Compression Motivation

- The best, most efficient provers, do not generate the best, least redundant proofs.
- Many compression algorithms for propositional proofs; few for first-order proofs.

(Propositional) Proofs

Definition (Proof)

A directed acyclic graph $\langle V, E, \Gamma \rangle$, where

- V is a set of nodes
- E is a set of edges labeled by literals
- Γ (the proof clause) is inductively constructible using *axiom* and *resolution* nodes

Definition (Axiom)

A proof with a single node (so $E = \emptyset$)

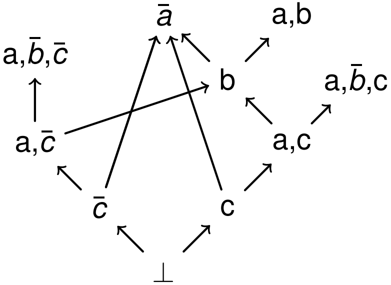
(Propositional) Resolution

Definition (Resolution)

Given two proofs ψ_L and ψ_R with conclusions Γ_L and Γ_R with some literal l such that $\bar{l} \in \Gamma_L$ and $l \in \Gamma_R$, the resolution proof ψ of ψ_L and ψ_R on l, denoted $\psi = \psi_L \psi_R$ is such that:

- ψ's nodes are the union of the nodes of ψ_L and ψ_R, and a new root node
- there is an edge from $\rho(\psi)$ to $\rho(\psi_L)$ labeled with $\bar{l}$
- there is an edge from $\rho(\psi)$ to $\rho(\psi_R)$ labeled with l
- ψ's conclusion is $(\Gamma_L \setminus \{\bar{l}\}) \cup (\Gamma_R \setminus \{l\})$

A Propositional Proof



LowerUnits

Definition (Unit)

A unit is a subproof with a conclusion having exactly 1 literal

Theorem

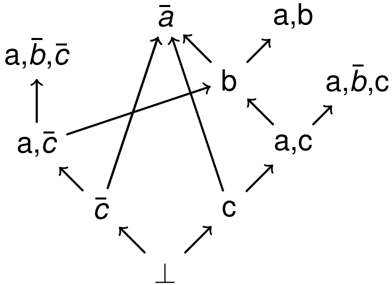
A unit can always be lowered

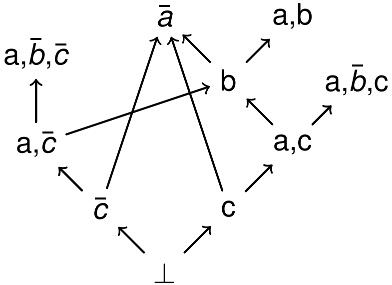
Compression is achieved by delaying resolution with unit subproofs.

Two Traversals

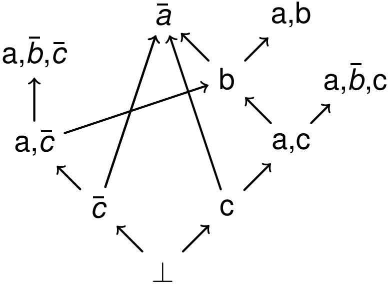
- $\uparrow$ Collect units with more than one resolvent
- $\downarrow$ Delete units and reintroduce them at the bottom of the proof

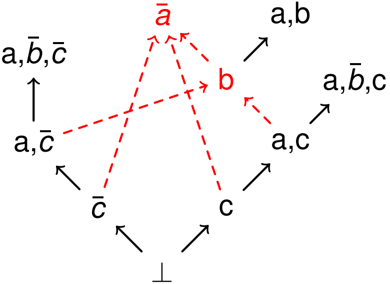
Propositional Example



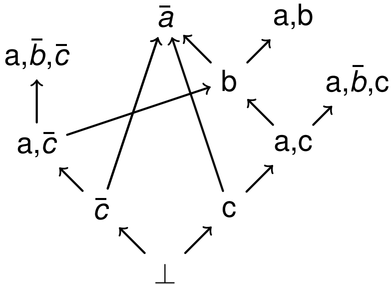


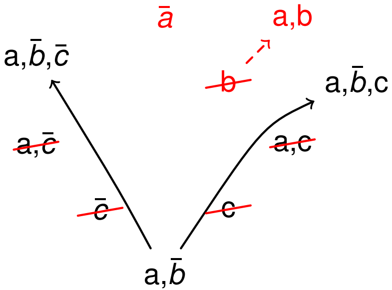
Propositional Example



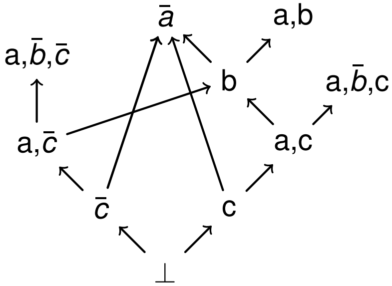


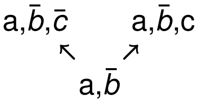
Propositional Example



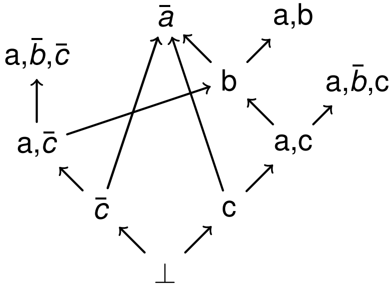


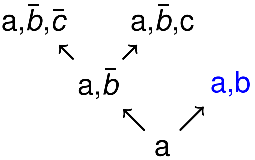
Propositional Example



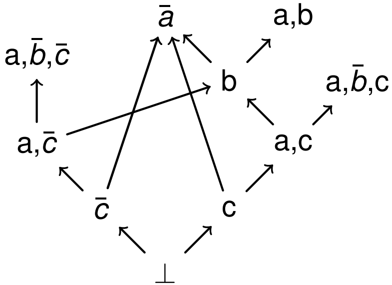


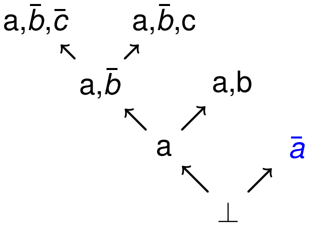
Propositional Example



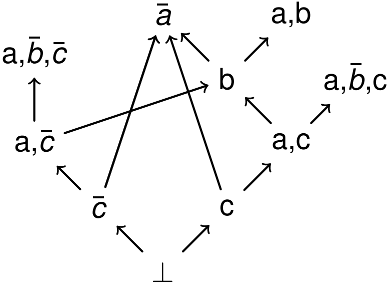


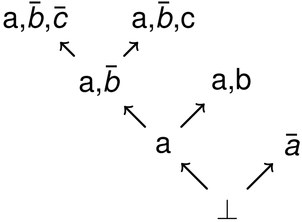
Propositional Example





Propositional Example





First-Order Change: Helpful Contractions

$$
\begin{tikzcd}
\eta_2\colon \vdash p(Y) & & \eta_1\colon p(W) \vdash q(Z) & \\
& \eta_3\colon \vdash q(Z) \arrow[ul] \arrow[ur] & & \eta_4\colon p(X), q(Z) \vdash \\
& & \eta_5\colon p(X) \vdash \arrow[ul] \arrow[ur] & \\
& \bot \arrow[uuul, bend left] \arrow[ur] & &
\end{tikzcd}
$$

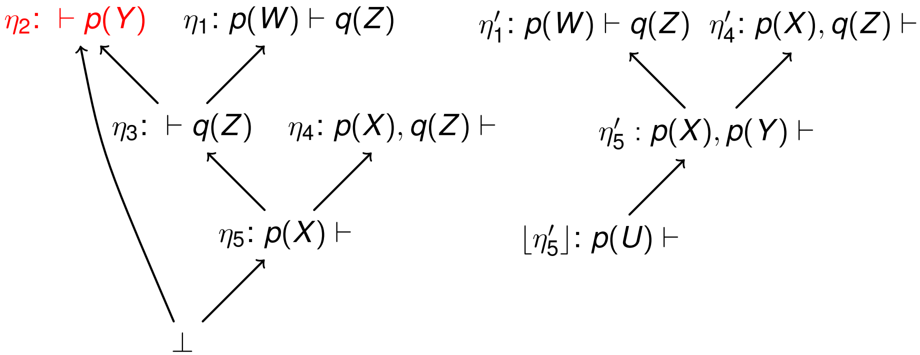
First-Order Change: Helpful Contractions

$$
\begin{tikzcd}
\color{red}{\eta_2\colon \vdash p(Y)} & & \eta_1\colon p(W) \vdash q(Z) & \\
& \eta_3\colon \vdash q(Z) \arrow[ul] \arrow[ur] & & \eta_4\colon p(X), q(Z) \vdash \\
& & \eta_5\colon p(X) \vdash \arrow[ul] \arrow[ur] & \\
& \bot \arrow[uuul, bend left] \arrow[ur] & &
\end{tikzcd}
$$

First-Order Change: Helpful Contractions

$$\begin{tikzcd}[column sep=small]
{\color{red}\eta_2\colon \vdash p(Y)} & & \eta_1\colon p(W) \vdash q(Z) & \\
& \eta_3\colon \vdash q(Z) \arrow[ul] \arrow[ur] & & \eta_4\colon p(X), q(Z) \vdash \\
& & \eta_5\colon p(X) \vdash \arrow[ul] \arrow[ur] & \\
& \bot \arrow[ur] \arrow[uuul, bend left] & &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
\eta_1'\colon p(W) \vdash q(Z) & & \eta_4'\colon p(X), q(Z) \vdash \\
& \eta_5'\colon p(X), p(Y) \vdash \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

First-Order Change: Helpful Contractions



First-Order Change: Helpful Contractions

$$
\begin{tikzcd}
{\color{red}\eta_2 \colon \vdash p(Y)} & & \eta_1 \colon p(W) \vdash q(Z) & \\
& \eta_3 \colon \vdash q(Z) \arrow[ul] \arrow[ur] & & \eta_4 \colon p(X), q(Z) \vdash \\
& & \eta_5 \colon p(X) \vdash \arrow[ul] \arrow[ur] & \\
& \bot \arrow[ur] \arrow[uuul, bend left] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
\eta'_1 \colon p(W) \vdash q(Z) & & \eta'_4 \colon p(X), q(Z) \vdash \\
& \eta'_5 \colon p(X), p(Y) \vdash \arrow[ul] \arrow[ur] & \\
\lfloor \eta'_5 \rfloor \colon p(U) \vdash \arrow[ur] & & \eta'_2 \colon \vdash p(Y) \\
& \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

First-Order Challenge: Pre-Deletion Check

$$
\begin{tikzcd}[column sep=small]
\eta_5\colon q(Y) \vdash p(a) & & \eta_4\colon p(X) \vdash & & \eta_3\colon \vdash p(b), q(Y) \\
& \eta_1\colon q(Y) \vdash \arrow[ul] \arrow[ur] & & \eta_2\colon \vdash q(Y) \arrow[ul] \arrow[ur] & \\
& & \bot \arrow[ul] \arrow[ur] & &
\end{tikzcd}
$$

First-Order Challenge: Pre-Deletion Check

$$\begin{tikzcd}[column sep=small]
\eta_5\colon q(Y) \vdash p(a) & & \eta_4\colon p(X) \vdash & & \eta_3\colon \vdash p(b), q(Y) \\
& \eta_1\colon q(Y) \vdash \arrow[ul] \arrow[ur] & & \eta_2\colon \vdash q(Y) \arrow[ul] \arrow[ur] & \\
& & \bot \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

First-Order Challenge: Pre-Deletion Check

$$
\begin{tikzcd}
\eta_5\colon q(Y) \vdash p(a) & & \color{red}{\eta_4\colon p(X) \vdash} & & \eta_3\colon \vdash p(b), q(Y) \\
& \eta_1\colon q(Y) \vdash \arrow[ul] \arrow[ur] & & \eta_2\colon \vdash q(Y) \arrow[ul] \arrow[ur] & \\
& & \bot \arrow[ul] \arrow[ur] & & \\
& \eta'_5\colon q(Y) \vdash p(a) & & \eta'_3\colon \vdash p(b), q(Y) & \\
& & \eta\colon \vdash p(a), p(b) \arrow[ul] \arrow[ur] & &
\end{tikzcd}
$$

First-Order Challenge: Pre-Deletion Check

$$
\begin{tikzcd}[column sep=small]
\eta_5\colon q(Y) \vdash p(a) & & \color{red}{\eta_4\colon p(X) \vdash} & & \eta_3\colon \vdash p(b), q(Y) \\
& \eta_1\colon q(Y) \vdash \arrow[ul] \arrow[ur] & & \eta_2\colon \vdash q(Y) \arrow[ul] \arrow[ur] & \\
& & \bot \arrow[ul] \arrow[ur] & & \\
& \eta_5'\colon q(Y) \vdash p(a) & & \eta_3'\colon \vdash p(b), q(Y) & \\
& & \eta\colon \vdash p(a), p(b) \arrow[ul] \arrow[ur] & & \\
& & \color{red}{\cancel{\lfloor \eta \rfloor}} \arrow[u] & &
\end{tikzcd}
$$

First-Order Challenge: Pre-Deletion Check

$$
\begin{tikzcd}
\eta_5 \colon q(Y) \vdash p(a) & & {\color{red}\eta_4 \colon p(X) \vdash} & & \eta_3 \colon \vdash p(b), q(Y) \\
& \eta_1 \colon q(Y) \vdash \arrow[ul] \arrow[ur] & & \eta_2 \colon \vdash q(Y) \arrow[ul] \arrow[ur] & \\
& & \bot \arrow[ul] \arrow[ur] & &
\end{tikzcd}
$$

Definition (Pre-Deletion Property)

η unit, $l \in \eta$, such that l is resolved with literals $l_1, \ldots, l_n$ in a proof ψ. η satisfies the *pre-deletion unifiability* property in ψ if $l_1, \ldots, l_n$ and $\bar{l}$ are unifiable.

First-Order Challenge: Post-Deletion Check

$$\eta_1\colon r(Y), p(X, q(Y, b)), p(X, Y) \vdash \qquad\qquad \eta_2\colon \vdash p(U, V)$$

$$\eta_4\colon \vdash r(W) \qquad\qquad \eta_3\colon r(V), p(U, q(V, b)) \vdash$$

$$\eta_5\colon p(U, q(W, b)) \vdash$$

$$\bot$$

First-Order Challenge: Post-Deletion Check

$$
\begin{tikzcd}
 & \color{red}{\eta_1\colon r(Y), p(X, q(Y, b)), p(X, Y) \vdash} & & \eta_2\colon \vdash p(U, V) \\
\eta_4\colon \vdash r(W) & & \eta_3\colon r(V), p(U, q(V, b)) \vdash \arrow[ul] \arrow[ur] & \\
 & \eta_5\colon p(U, q(W, b)) \vdash \arrow[ul] \arrow[ur] & & \\
 & & \perp \arrow[ul] \arrow[uuur, bend right] &
\end{tikzcd}
$$

First-Order Challenge: Post-Deletion Check

$$
\begin{tikzcd}
 & {\color{red}\eta_1 : r(Y), p(X, q(Y, b)), p(X, Y) \vdash} & & \eta_2 : \vdash p(U, V) \\
\eta_4 : \vdash r(W) & & \eta_3 : r(V), p(U, q(V, b)) \vdash \arrow[ul] \arrow[ur] & \\
 & \eta_5 : p(U, q(W, b)) \vdash \arrow[ul] \arrow[ur] & & \\
 & & \bot \arrow[ul] \arrow[uuur, bend right] &
\end{tikzcd}
$$

$$
\begin{tikzcd}
\eta'_1 : r(Y), p(X, q(Y, b)), p(X, Y) \vdash & & \eta'_4 : \vdash r(W) \\
 & \eta'_5 : p(X, q(W, b)), p(X, W) \vdash \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

First-Order Challenge: Post-Deletion Check

$$\begin{tikzcd}
 & {\color{red}\eta_1\colon r(Y), p(X, q(Y, b)), p(X, Y) \vdash} & & \eta_2\colon \vdash p(U, V) \\
\eta_4\colon \vdash r(W) & & \eta_3\colon r(V), p(U, q(V, b)) \vdash \arrow[ul] \arrow[ur] & \\
 & \eta_5\colon p(U, q(W, b)) \vdash \arrow[ul] \arrow[ur] & & \\
 & & \bot \arrow[ul] \arrow[uuur, bend right] &
\end{tikzcd}$$

$$\begin{tikzcd}
\eta'_1\colon r(Y), p(X, q(Y, b)), p(X, Y) \vdash & & \eta'_4\colon \vdash r(W) \\
 & \eta'_5\colon p(X, q(W, b)), p(X, W) \vdash \arrow[ul] \arrow[ur] & \\
 & \lfloor \cancel{\eta'_5} \rfloor \arrow[u] &
\end{tikzcd}$$

First-Order Challenge: Post-Deletion Check

$$
\begin{tikzcd}
 & \color{red}{\eta_1\colon r(Y), p(X, q(Y, b)), p(X, Y) \vdash} & & \eta_2\colon \vdash p(U, V) \\
\eta_4\colon \vdash r(W) & & \eta_3\colon r(V), p(U, q(V, b)) \vdash \arrow[ul] \arrow[ur] & \\
 & \eta_5\colon p(U, q(W, b)) \vdash \arrow[ul] \arrow[ur] & & \\
 & & & \bot \arrow[ull] \arrow[uuu, bend right]
\end{tikzcd}
$$

Definition (Post-Deletion Property)

η unit, $l \in \eta$, such that l is resolved with literals $l_1, \ldots, l_n$ in a proof ψ. η satisfies the *post-deletion unifiability* property in ψ if $l_1^{\dagger\downarrow}, \ldots, l_n^{\dagger\downarrow}$ and $\overline{l^\dagger}$ are unifiable, where $l^\dagger$ is the literal in $\psi' = \psi \setminus \{\eta\}$ corresponding to l in ψ, and $l^{\dagger\downarrow}$ is the descendant of $l^\dagger$ in the roof of ψ'.

First-Order Lower Units Challenges

- Deletion changes literals
- Unit collection depends on if contraction is possible after propagation down the proof

Deletion of units require knowledge of proof after deletion, and deletion depends on what will be lowered.

- $O(n^2)$ solution to have full knowledge
- Difficult bookkeeping required for implementation

Greedy First-Order Lower Units - A Quicker Alternative

- Ignore post-deletion satisfaction
- Focus on pre-deletion satisfaction
- Greedy contraction

Faster run-time (linear; one traversal)
Easier to implement

- Doesn't always compress (returns original proof sometimes)

Greedy First-Order Lower Units - A Quicker Alternative

- Ignore post-deletion satisfaction
- Focus on pre-deletion satisfaction
- Greedy contraction

Faster run-time (linear; one traversal)
Easier to implement

- Doesn't always compress (returns original proof sometimes)

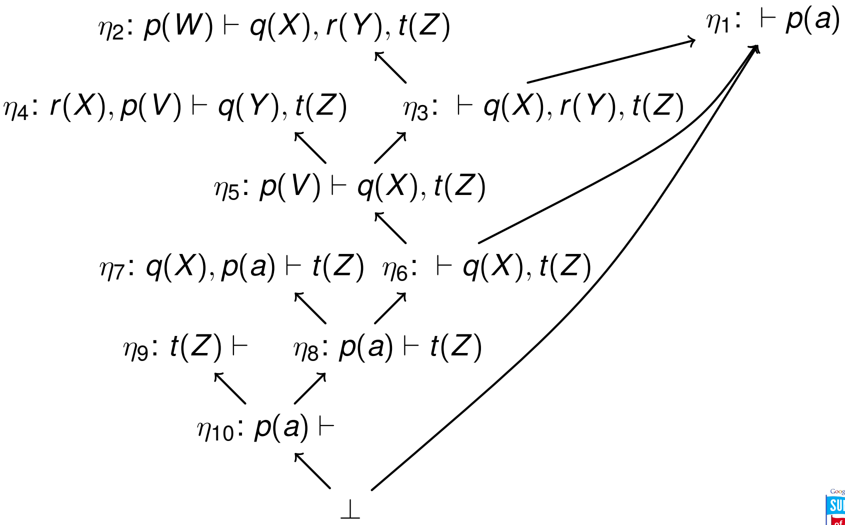
Greedy First-Order Lower Units - A Quicker Alternative

- Ignore post-deletion satisfaction
- Focus on pre-deletion satisfaction
- Greedy contraction

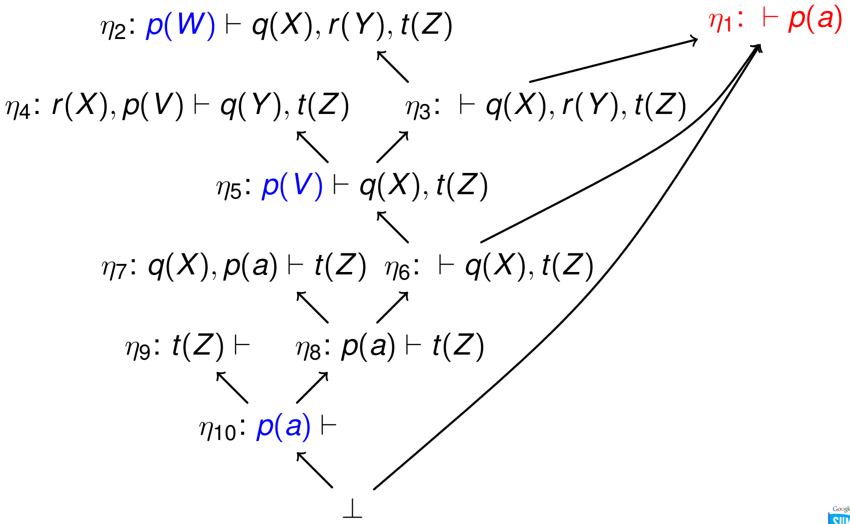
Faster run-time (linear; one traversal)
Easier to implement

- Doesn't always compress (returns original proof sometimes)

First-Order Example



First-Order Example



$$\sigma = \{W \to a, V \to a\}$$

First-Order Example

$\eta_2\colon p(W) \vdash q(X), r(Y), t(Z)$ $\qquad$ $\eta_1\colon \vdash p(a)$

$\{W \to a\}$

$\eta_4\colon r(X), p(V) \vdash q(Y), t(Z)$ $\qquad$ $\eta_3\colon \vdash q(X), r(Y), t(Z)$

$\eta_5\colon p(V) \vdash q(X), t(Z)$

$\eta_7\colon q(X), p(a) \vdash t(Z)$ $\qquad$ $\eta_6\colon \vdash q(X), t(Z)$

$\eta_9\colon t(Z) \vdash$ $\qquad$ $\eta_8\colon p(a) \vdash t(Z)$

$\eta_{10}\colon p(a) \vdash$

$\perp$

First-Order Example

$$
\begin{tikzcd}[column sep=small]
 & & & & & \eta_1\colon\ \vdash p(a) \\
 & \eta_4\colon r(X), p(V) \vdash q(Y), t(Z) & & \eta_3'\colon p(a) \vdash q(X), r(Y), t(Z) & & \\
 & & \eta_5'\colon p(V), p(a) \vdash q(X), t(Z) \arrow[ul] \arrow[ur] & & & \\
 & \eta_7\colon q(X), p(a) \vdash t(Z) & & \eta_6\colon\ \vdash q(X), t(Z) \arrow[ul] \arrow[uuurr, bend right] & & \\
 \eta_9\colon t(Z) \vdash & & \eta_8\colon p(a) \vdash t(Z) \arrow[ul] \arrow[ur] & & & \\
 & \eta_{10}\colon p(a) \vdash \arrow[ul] \arrow[ur] & & & & \\
 & & \bot \arrow[ul] \arrow[uuuuuurrr, bend right] & & &
\end{tikzcd}
$$

First-Order Example

$\eta_1\colon\ \vdash p(a)$

$\eta_4\colon r(X), p(V) \vdash q(Y), t(Z) \qquad \eta_3\colon p(a) \vdash q(X), r(Y), t(Z)$

$\eta_5'\colon p(V), p(a) \vdash q(X), t(Z)$

$\{V \to a\}$

$\eta_7\colon q(X), p(a) \vdash t(Z) \qquad \eta_6\colon\ \vdash q(X), t(Z)$

$\eta_9\colon t(Z) \vdash \qquad \eta_8\colon p(a) \vdash t(Z)$

$\eta_{10}\colon p(a) \vdash$

$\perp$

First-Order Example

$$
\begin{tikzcd}
 & & & & & & \eta_1\colon \vdash p(a) \\
 & & \eta_4\colon r(X), p(V) \vdash q(Y), t(Z) & & & \eta_3\colon p(a) \vdash q(X), r(Y), t(Z) & \\
 & & & & & \eta_6'\colon p(a), p(a) \vdash q(X), t(Z) \arrow[ulll] \arrow[u] & \\
 & & \eta_7\colon q(X), p(a) \vdash t(Z) & & & \lfloor \eta_6' \rfloor\colon p(a) \vdash q(X), t(Z) \arrow[u] & \\
 \eta_9\colon t(Z) \vdash & & & & \eta_8\colon p(a) \vdash t(Z) \arrow[ull] \arrow[ur] & & \\
 & \eta_{10}\colon p(a) \vdash \arrow[ul] \arrow[urrr] & & & & & \\
 & & & \bot \arrow[ull] \arrow[uuuuuurrr, bend right] & & &
\end{tikzcd}
$$

First-Order Example

$$\eta_1\colon\ \vdash p(a)$$

$$\eta_4\colon r(X), p(V) \vdash q(Y), t(Z) \qquad \eta_3\colon p(a) \vdash q(X), r(Y), t(Z)$$

$$\eta_6'\colon p(a), p(a) \vdash q(X), t(Z)$$

$$\eta_7\colon q(X), p(a) \vdash t(Z) \qquad \lfloor \eta_6' \rfloor\colon p(a) \vdash q(X), t(Z)$$

$$\eta_9\colon t(Z) \vdash \qquad \eta_8\colon p(a) \vdash t(Z)$$

$$\eta_{10}\colon p(a) \vdash$$

$$\emptyset$$

$$\bot$$

First-Order Example

$\eta_1\colon \vdash p(a)$

$$
\begin{tikzcd}[column sep=small]
\eta_4\colon r(X), p(V) \vdash q(Y), t(Z) & & \eta_3\colon p(a) \vdash q(X), r(Y), t(Z) \\
& & \eta_6'\colon p(a), p(a) \vdash q(X), t(Z) \arrow[ull] \arrow[u] \\
\eta_7\colon q(X), p(a) \vdash t(Z) & & \lfloor \eta_6' \rfloor\colon p(a) \vdash q(X), t(Z) \arrow[u] \\
\eta_9\colon t(Z) \vdash & \eta_8\colon p(a) \vdash t(Z) \arrow[ul] \arrow[ur] & \\
& \eta_{10}\colon p(a) \vdash \arrow[ul] \arrow[u] &
\end{tikzcd}
$$

First-Order Example

$$
\begin{tikzcd}
 & & & \eta_1\colon \vdash p(a) \\
\eta_4\colon r(X), p(V) \vdash q(Y), t(Z) & & \eta_3\colon p(a) \vdash q(X), r(Y), t(Z) & \\
 & & \eta_6'\colon p(a), p(a) \vdash q(X), t(Z) \arrow[ull] \arrow[u] & \\
\eta_7\colon q(X), p(a) \vdash t(Z) & & \lfloor \eta_6' \rfloor\colon p(a) \vdash q(X), t(Z) \arrow[u] & \\
\eta_9\colon t(Z) \vdash & \eta_8\colon p(a) \vdash t(Z) \arrow[ul] \arrow[ur] & & \\
 & \eta_{10}\colon p(a) \vdash \arrow[ul] \arrow[u] & & \\
 & & \bot \arrow[ul] \arrow[uuuuuur, bend right] &
\end{tikzcd}
$$

Experiment Setup

- Simple First-Order Lower units implemented as part of Skeptik (in Scala)
- 308 real first-order proofs generated by SPASS from problems from TPTP Problem Library
    - 2280 initial problems (1032 known unsatisfiable)
    - solver asked to use only resolution and contraction rules
    - 300s timeout
- proofs *generated* on cluster at the University of Victoria
- proofs *compressed* on *this laptop*

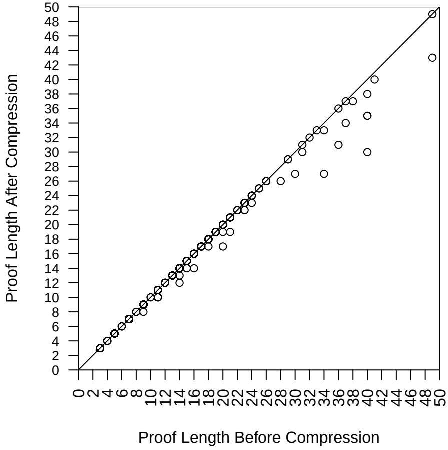
Time to generate proofs: $\approx$ 40 minutes
Time to compress proofs: $\approx$ 5 seconds

Experiment Setup

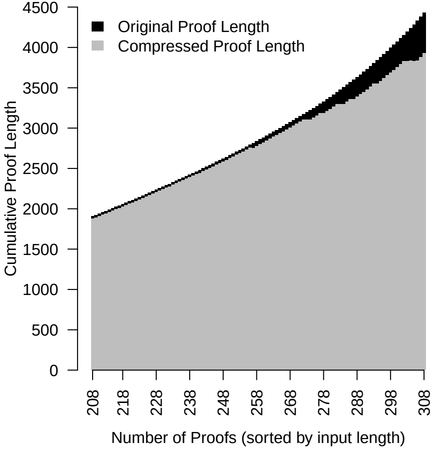
- Simple First-Order Lower units implemented as part of Skeptik (in Scala)
- 308 real first-order proofs generated by SPASS from problems from TPTP Problem Library
  - 2280 initial problems (1032 known unsatisfiable)
  - solver asked to use only resolution and contraction rules
  - 300s timeout
- proofs *generated* on cluster at the University of Victoria
- proofs *compressed* on *this laptop*

Time to generate proofs: $\approx$ 40 minutes
Time to compress proofs: $\approx$ 5 seconds

Results



Proof Length After Compression
Proof Length Before Compression
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50



Original Proof Length
Compressed Proof Length
Cumulative Proof Length
0 500 1000 1500 2000 2500 3000 3500 4000 4500
208 218 228 238 248 258 268 278 288 298 308
Number of Proofs (sorted by input length)

Results

Higher compression in longer proofs: 13/18 proofs with length ≥ 30 nodes successfully compressed.

Total compression ratio 11.3%: 4429 vs. 3929 nodes.

18.4% for 100 longest proofs.

Only 14/308 proofs were returned uncompressed

Conclusion

- Simple First-Order Lower Units is a quick algorithm for first-order proof compression
- Future work:
  - Explore other proof compression algorithms, e.g. Recycle Pivots with Intersection
  - Explore ways of dealing with the post-deletion property quickly

Thank you for your attention.
Any questions?

- Source code: `https://github.com/jgorzny/Skeptik`
- Data: `http://www.math.uvic.ca/~jgorzny/data/`