Compression of Propositional Resolution Proofs by Lowering Subproofs

Joseph Boudou[1] Bruno Woltzenlogel Paleo[2]

[1]Université Paul Sabatier, Toulouse

[2]Vienna University of Technology

SMT Workshop, 2013

Why compressing propositional resolution proofs?

Proof as a tree

$$\cfrac{\cfrac{\cfrac{\bar{b}, c \qquad \bar{a}, b}{\bar{a}, c}\;b \qquad \cfrac{\bar{a}, b \qquad \bar{a}, \bar{b}, \bar{c}}{\bar{a}, \bar{c}}\;\bar{b}}{\bar{a}}\;\bar{c} \qquad a}{\bot}\;a$$

Proof as a directed acyclic graph (DAG)

$$\begin{tikzcd}
\bar{b},c & & \bar{a},b & & \bar{a},\bar{b},\bar{c} \\
& \bar{a},c \arrow[ul] \arrow[ur] & & \bar{a},\bar{c} \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Proof

Definition (Proof)

A proof ψ is a directed acyclic graph

- having a root noted $\rho(\psi)$;
- with nodes labeled with clauses;
- with edges oriented from the resolvent to the premise;
- with edges labeled with the premise's literal removed in the resolvent;
- which is either an axiom or a resolution proof.

Definition (Axiom)

An axiom is a proof with only one node.

Resolution

Given two proofs φ_L and φ_R with conclusion Γ_L and Γ_R and a literal ℓ s.t. $\bar{\ell} \in \Gamma_L$ and $\ell \in \Gamma_R$, the resolution proof ψ of φ_L and φ_R on ℓ, noted $\psi = \varphi_L \odot_\ell \varphi_R$, is such that:

- ψ's nodes are the union of φ_L and φ_R nodes plus a new root node;
- there is an edge from $\rho(\psi)$ to $\rho(\varphi_L)$ labeled with $\bar{\ell}$;
- there is an edge from $\rho(\psi)$ to $\rho(\varphi_R)$ labeled with ℓ;
- ψ's conclusion is $\left(\Gamma_L \setminus \{\bar{\ell}\}\right) \cup (\Gamma_R \setminus \{\ell\})$.

$$
\begin{tikzcd}
\mathrm{a1} & & \mathrm{low} \\
& \mathrm{r1} \arrow[ul] \arrow[ur] &
\end{tikzcd}
\odot_{\bar{c}}
\begin{tikzcd}
\mathrm{low} & & \mathrm{a2} \\
& \mathrm{r2} \arrow[ul] \arrow[ur] &
\end{tikzcd}
=
\begin{tikzcd}
\mathrm{a1} & & \mathrm{low} & & \mathrm{a2} \\
& \mathrm{r1} \arrow[ul] \arrow[ur] & & \mathrm{r2} \arrow[ul] \arrow[ur] & \\
& & \mathrm{r0} \arrow[ul] \arrow[ur] & &
\end{tikzcd}
$$

Deletion

Deletion of an edge

- The resolvent is replaced by the other premise.
- Some subsequent resolutions may have to be deleted too.

Deletion of a subproof φ

- Deletion of every edge coming to $\rho(\varphi)$.
- The operation is commutative and associative.

Notation

$\psi \setminus (\varphi_1, \ldots, \varphi_n)$ denotes the deletions of subproofs $\varphi_1, \ldots, \varphi_n$ from the proof ψ.

Regular proof

Definition (Tseitin 1970)

A proof is regular iff on every path from its root to any of its axiom, any literal appears at most once as edge label.

Theorem (Goerdt 1990)

Given a set of axioms and a clause Γ*, the smallest regular proof of* Γ *might be exponentially bigger than the smallest irregular proof of* Γ*.*

RecyclePivotsWithIntersection (RPI)

Partial Regularization

- Delete an outgoing edge labeled with ℓ iff $\bar{\ell}$ appears on **every** path from the root to the node.

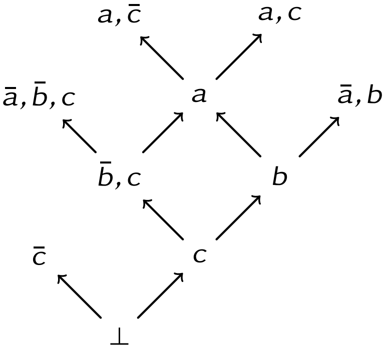
Definition (Safe literal)

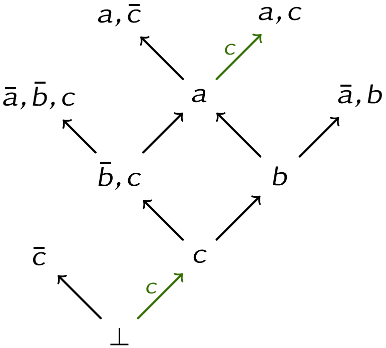
A literal is safe for a node η if it can be added to η's clause without changing proof's conclusion.

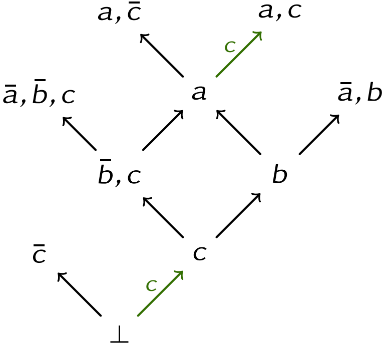
Two traversals

↑ Collect safe literals and mark edges to be deleted.

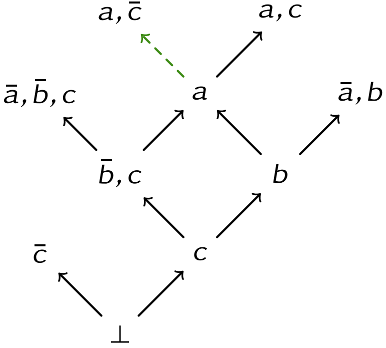
↓ Delete edges.


$a, \bar{c}$
a, c
$\bar{a}, \bar{b}, c$
a
$\bar{a}, b$
$\bar{b}, c$
b
$\bar{c}$
c
$\perp$

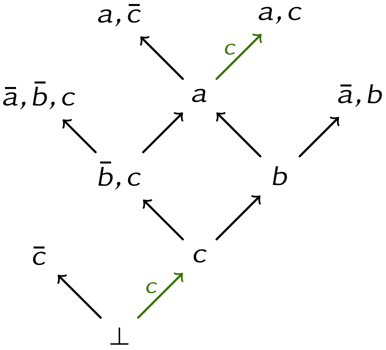

$a, \bar{c}$
a, c
c
$\bar{a}, \bar{b}, c$
a
$\bar{a}, b$
$\bar{b}, c$
b
$\bar{c}$
c
c
$\perp$



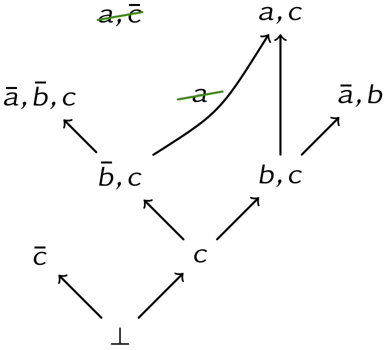
Original proof



Compressed proof



Original proof
4 resolutions



Compressed proof
3 resolutions

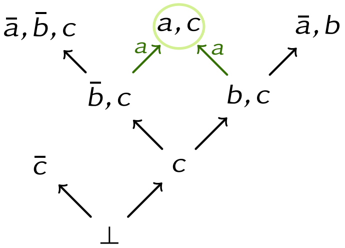
Definition

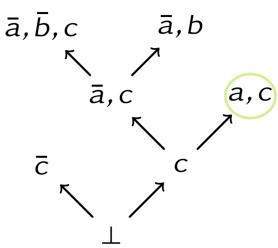
A node is an horizontal redundancy iff it has at least two incoming edges labeled with the same literal.

Reducing horizontal redundancy

- postponing resolution until resolvents are resolved.

Example





LowerUnits (LU)

Definition (Unit)

A unit is a subproof with a conclusion clause having exactly one literal.

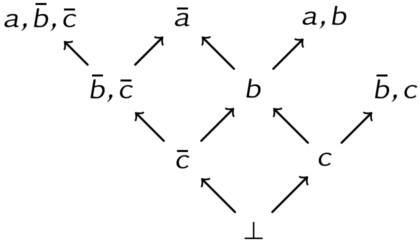
Theorem

A unit can always be lowered.

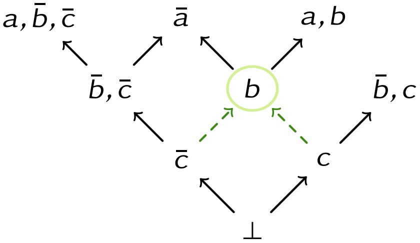
Two traversals

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

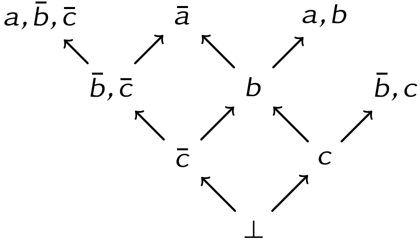
$$
\begin{tikzcd}
a,\bar{b},\bar{c} & & \bar{a} & & a,b & \\
& \bar{b},\bar{c} \arrow[ul] \arrow[ur] & & b \arrow[ul] \arrow[ur] & & \bar{b},c \\
& & \bar{c} \arrow[ul] \arrow[ur] & & c \arrow[ul] \arrow[ur] & \\
& & & \bot \arrow[ul] \arrow[ur] & &
\end{tikzcd}
$$



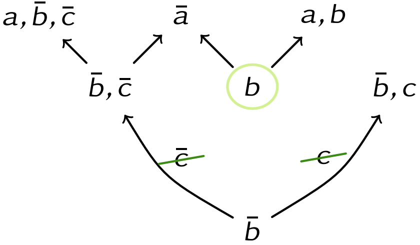
Original proof



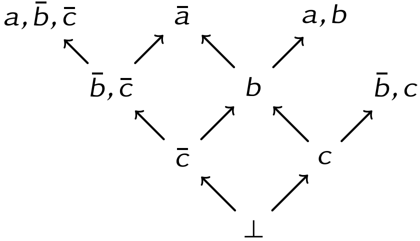
Compressed proof



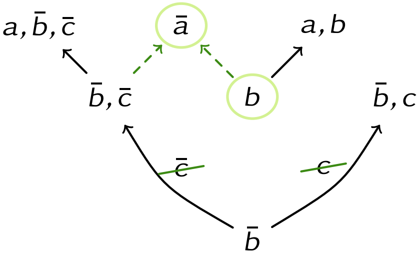
Original proof



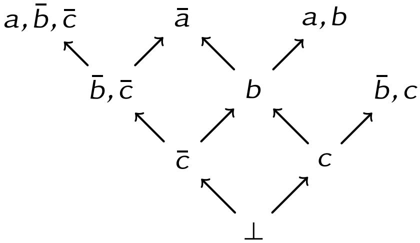
Compressed proof



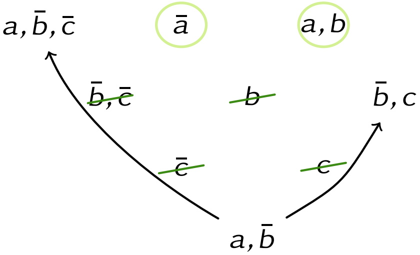
Original proof



Compressed proof



Original proof



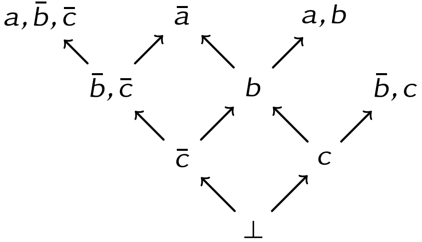
Compressed proof

$$\begin{tikzcd}
a, \bar{b}, \bar{c} & & \bar{a} & & a, b & \\
& \bar{b}, \bar{c} \arrow[ul] \arrow[ur] & & b \arrow[ul] \arrow[ur] & & \bar{b}, c \\
& & \bar{c} \arrow[ul] \arrow[ur] & & c \arrow[ul] \arrow[ur] & \\
& & & \bot \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

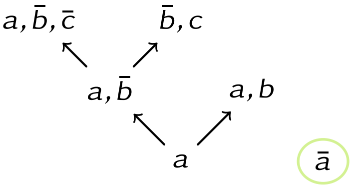
Original proof

$$\begin{tikzcd}
a, \bar{b}, \bar{c} & & \bar{b}, c & & \\
& a, \bar{b} \arrow[ul] \arrow[ur] & & a, b & \\
& & & & \bar{a}
\end{tikzcd}$$

Compressed proof



Original proof



Compressed proof

$$
\begin{tikzcd}[column sep=small]
a,\bar{b},\bar{c} & & \bar{a} & & a,b & \\
& \bar{b},\bar{c} \arrow[ul] \arrow[ur] & & b \arrow[ul] \arrow[ur] & & \bar{b},c \\
& & \bar{c} \arrow[ul] \arrow[ur] & & c \arrow[ul] \arrow[ur] & \\
& & & \bot \arrow[ul] \arrow[ur] & &
\end{tikzcd}
$$

Original proof
5 resolutions

$$
\begin{tikzcd}[column sep=small]
a,\bar{b},\bar{c} & & \bar{b},c & & \\
& a,\bar{b} \arrow[ul] \arrow[ur] & & a,b & \\
& & a \arrow[ul] \arrow[ur] & & \bar{a} \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Compressed proof
3 resolutions

Introduction

Redundancies and corresponding algorithms

LowerUnivalents
- Principles
- Algorithm and implementation
- Experiments

Conclusion

Goals

- Lower more subproofs.
- Allow fast combination after RPI.

Idea

- If a unit with conclusion clause $\{a\}$ is already marked for lowering, a subproof with conclusion clause $\{\bar{a}, b\}$ may be lowered too.

Definition (Valent literal)

In a proof ψ, a literal ℓ is *valent* for the subproof φ iff $\bar{\ell}$ belongs to the conclusion of $\psi \setminus (\varphi)$ but not to the conclusion of ψ.

Definition (Univalent subproof)

A subproof φ with conclusion Γ is *univalent* w.r.t. a set Δ of literals iff φ has exactly one valent literal ℓ, $\ell \notin \Delta$ and $\Gamma \subseteq \Delta \cup \{\ell\}$. ℓ is called the *univalent literal* of φ w.r.t. Δ.

Theorem

Given a proof ψ, if there is a sequence $U = (\varphi_1 \ldots \varphi_n)$ of ψ's subproofs and a sequence $(\ell_1 \ldots \ell_n)$ of literals such that $\forall i \in [1 \ldots n], \ell_i$ is the univalent literal of φ_i w.r.t. $\Delta_{i-1} = \{\bar{\ell}_1 \ldots \bar{\ell}_{i-1}\}$, then the conclusion of

$$\psi' = \psi \setminus (U) \odot_{\ell_n} \varphi_n \ldots \odot_{\ell_1} \varphi_1$$

subsumes the conclusion of ψ.

Input: a proof ψ
Output: a compressed proof ψ'

Univalents $\leftarrow \emptyset$;
$\Delta \leftarrow \emptyset$;

for *every subproof* φ*, in a top-down traversal* **do**
    $\psi' \leftarrow \varphi \backslash$Univalents ;
    if ψ' *is univalent w.r.t.* Δ **then**
        let ℓ be the univalent literal ;
        push $\bar{\ell}$ onto Δ ;
        push ψ' onto Univalents ;

`// At this point,` $\psi' = \psi \setminus$ Univalents
while Univalents $\neq \emptyset$ **do**
    $\varphi \leftarrow$ **pop** from Univalents;
    $\ell \leftarrow$ **pop** from Δ ;
    if ℓ *in the conclusion of* ψ' **then** $\psi' \leftarrow \varphi \odot_\ell \psi'$;

$$\Delta = \varnothing$$

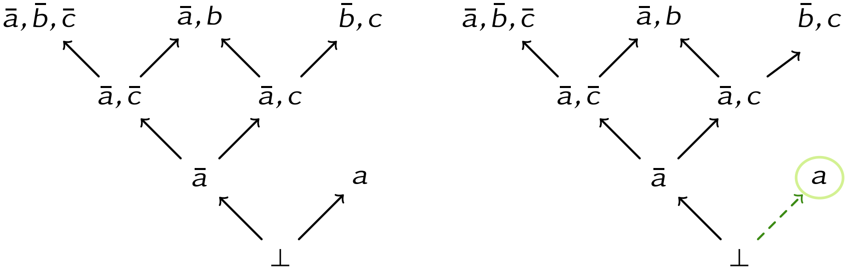
$$\begin{tikzcd}[column sep=small]
\bar{a},\bar{b},\bar{c} & & \bar{a},b & & \bar{b},c \\
& \bar{a},\bar{c} \arrow[ul] \arrow[ur] & & \bar{a},c \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Original proof

$$\begin{tikzcd}[column sep=small]
\bar{a},\bar{b},\bar{c} & & \bar{a},b & & \bar{b},c \\
& \bar{a},\bar{c} \arrow[ul] \arrow[ur] & & \bar{a},c \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

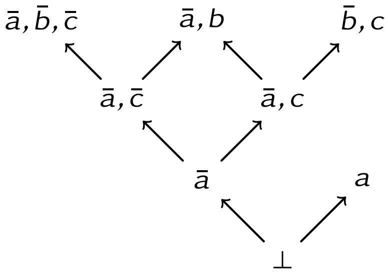
Compressed proof

$$\Delta = \{\bar{a}\}$$

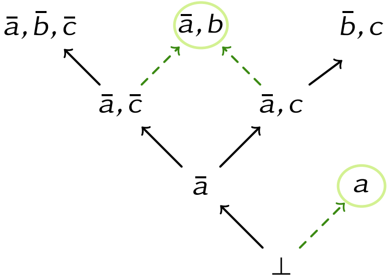


Original proof Compressed proof

$$\Delta = \{\bar{a}, \bar{b}\}$$

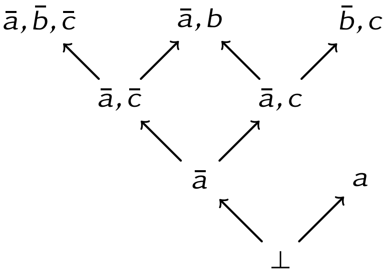


Original proof

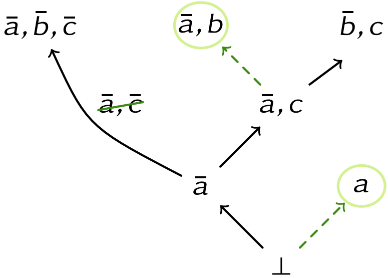


Compressed proof

$$\Delta = \{\bar{a}, \bar{b}\}$$

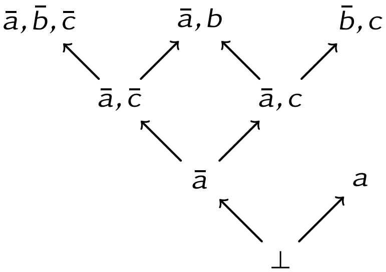


Original proof

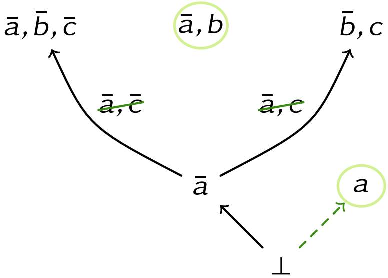


Compressed proof

$$\Delta = \{\bar{a}, \bar{b}\}$$

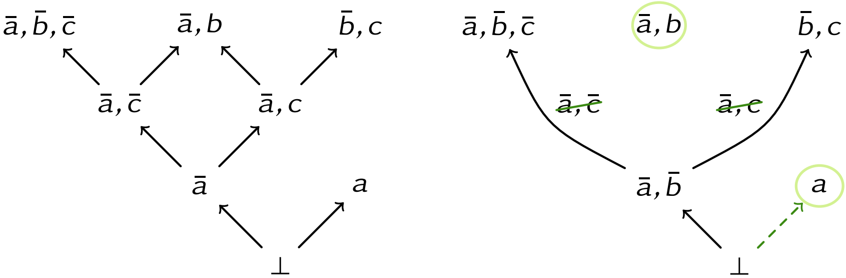


Original proof



Compressed proof

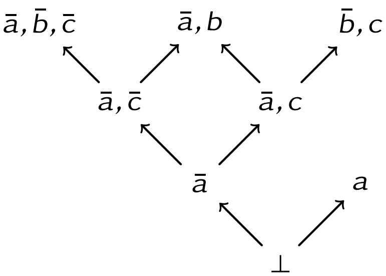
$$\Delta = \{\bar{a}, \bar{b}\}$$



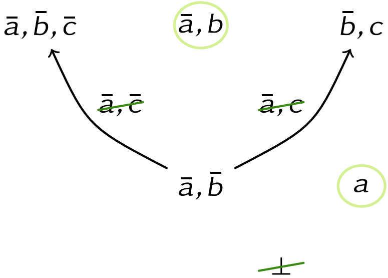
Original proof

Compressed proof

$$\Delta = \{\bar{a}, \bar{b}\}$$



Original proof



Compressed proof

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}
\bar{a},\bar{b},\bar{c} & & \bar{a},b & & \bar{b},c \\
& \bar{a},\bar{c} \arrow[ul] \arrow[ur] & & \bar{a},c \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Original proof

$$\begin{tikzcd}
\bar{a},\bar{b},\bar{c} & & \bar{b},c & & \\
& \bar{a},\bar{b} \arrow[ul] \arrow[ur] & & \bar{a},b & \\
& & & & a
\end{tikzcd}$$

Compressed proof

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}
\bar{a},\bar{b},\bar{c} & & \bar{a},b & & \bar{b},c \\
& \bar{a},\bar{c} \arrow[ul] \arrow[ur] & & \bar{a},c \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Original proof

$$\begin{tikzcd}
\bar{a},\bar{b},\bar{c} & & \bar{b},c & & \\
& \bar{a},\bar{b} \arrow[ul] \arrow[ur] & & \bar{a},b & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a
\end{tikzcd}$$

Compressed proof

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{a}, b & & \bar{b}, c \\
& \bar{a}, \bar{c} \arrow[ul] \arrow[ur] & & \bar{a}, c \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Original proof
4 resolutions

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{b}, c & & \\
& \bar{a}, \bar{b} \arrow[ul] \arrow[ur] & & \bar{a}, b & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Compressed proof
3 resolutions

Configuration

- Algorithms implemented in Scala for the Skeptik library.
- 5 000 SMT proofs produced by the VeriT solver.
- Experiments performed on the Vienna Scientific Cluster.

Results

Algorithm	Compression	Speed
LowerUnits	7.5 %	22.4 n/ms
LowerUnivalents	8.0 %	20.4 n/ms
LU composed after RPI	21.7 %	15.1 n/ms
LUniv combined after RPI	22.0 %	17.8 n/ms

Goals achieved

- LowerUnivalents compresses more than LowerUnits.
- LowerUnivalents combines efficiently after RPI.

Future works

- Combine LowerUnivalents after other algorithms.
- Get rid of order dependency.
- Lower subproofs just until resolvents are all resolved.
- Explore other kind of redundancies.

Thank you for your attention.

Any question ?

Skeptik

- http://github.com/Paradoxika/Skeptik