# Compression of Propositional Resolution Proofs by Lowering Subproofs [*Presentation-Only*]

Joseph Boudou[1] *and Bruno Woltzenlogel Paleo[2] †

[1] Université Paul Sabatier, Toulouse
joseph.boudou@matabio.net
[2] Vienna University of Technology
bruno@logic.at

**Abstract**

This paper describes a generalization of the `LowerUnits` algorithm [7] for the compression of resolution proofs. The generalized algorithm, called `LowerUnivalents`, is able to lower not only units but also subproofs of non-unit clauses, provided that they satisfy some additional conditions. This new algorithm is particularly suited to be combined with the `RecyclePivotsWithIntersection` algorithm [7]. A formal proof that `LowerUnivalents` always compresses more than `LowerUnits` is shown, and both algorithms are empirically compared on thousands of proofs produced by the SMT-Solver veriT.

## 1 Introduction

The resolution calculus provides the foundation for propositional reasoning in SMT-solvers. Resolution refutations can be output by SMT-solvers with an acceptable efficiency overhead [3] and are detailed enough to allow easy implementation of efficient proof checkers. Therefore, they can be used as certificates of correctness for the answers provided by these tools.

However, as the refutations found by SMT-solvers are often redundant, techniques for compressing and improving resolution proofs in a post-processing stage have flourished. Algebraic properties of the resolution operation that might be useful for compression were investigated in [6]. Compression algorithms based on rearranging and sharing chains of resolution inferences have been developed in [1] and [11]. Cotton [5] proposed an algorithm that compresses a refutation by repeteadly splitting it into a proof of a heuristically chosen literal $\ell$ and a proof of $\overline{\ell}$, and then resolving them to form a new refutation. The `Reduce&Reconstruct` algorithm [10] searches for locally redundant subproofs that can be rewritten into subproofs of stronger clauses and with fewer resolution steps. In [2] two linear time compression algorithms are introduced. One of them is a partial regularization algorithm called `RecyclePivots`. An enhanced version of this latter algorithm, called `RecyclePivotsWithIntersection` (`RPI`), is proposed in [7], along with a new linear time algorithm called `LowerUnits`. These two last algorithms are complementary and better compression can easily be achieved by sequentially composing them (i.e. executing one after the other).

In this paper, the new algorithm `LowerUnivalents`, generalizing `LowerUnits`, is described. Its achieved goals are to compress more than `LowerUnits` and to allow fast *non-sequential* combination with `RPI`. While in a sequential combination one algorithm is simply executed after the other, in a non-sequential combination, both algorithms are executed simultaneously when the proof is traversed. Therefore, fewer traversals are needed.

*Supported by the Google Summer of Code 2012 program.
†Supported by the Austrian Science Fund, project P24300.

The next section introduces the propositional resolution calculus along with the notations, operations and some theoretical results used in the paper. Section 3 briefly describes the `LowerUnits` algorithm. In Sect. 4 the new algorithm `LowerUnivalents` is introduced and it is proved that it always compresses more than `LowerUnits`. Experimental results are discussed in Sect. 5. Appendix A describes the non-sequential combination of `LowerUnivalents` and `RPI`. *A longer version of this paper containing proofs of all theorems and propositions is available at:* `https://github.com/Paradoxika/Skeptik/tree/develop/doc/papers/LUniv`.

## 2 Propositional Resolution Calculus

A *literal* is a propositional variable or the negation of a propositional variable. The *dual* of a literal $\ell$ is denoted $\overline{\ell}$ (i.e. for any propositional variable $p$, $\overline{p} = \neg p$ and $\overline{\neg p} = p$). The set of all literals is denoted $\mathcal{L}$. A *clause* is a set of literals. $\bot$ denotes the *empty clause*.

**Definition 1** (Proof)**.** *A directed acyclic graph $\langle V, E, \Gamma\rangle$, where $V$ is a set of nodes and $E$ is a set of edges labeled by literals (i.e. $E \subset V \times \mathcal{L} \times V$ and $v_1 \xrightarrow{\ell} v_2$ denotes an edge from node $v_1$ to node $v_2$ labeled by $\ell$), is a proof of a clause $\Gamma$ iff it is inductively constructible according to the following cases:*

1. *If $\Gamma$ is a clause, $\widehat{\Gamma}$ denotes some proof $\langle\{v\}, \varnothing, \Gamma\rangle$, where $v$ is a new node.*
2. *If $\psi_L$ is a proof $\langle V_L, E_L, \Gamma_L\rangle$ and $\psi_R$ is a proof $\langle V_R, E_R, \Gamma_R\rangle$ and $\ell$ is a literal such that $\overline{\ell} \in \Gamma_L$ and $\ell \in \Gamma_R$, then $\psi_L \odot_\ell \psi_R$ denotes a proof $\langle V, E, \Gamma\rangle$ s.t.*

$$
\begin{aligned}
V &= V_L \cup V_R \cup \{v\} \\
E &= E_L \cup E_R \cup \left\{ v \xrightarrow{\overline{\ell}} \rho(\psi_L), v \xrightarrow{\ell} \rho(\psi_R) \right\} \\
\Gamma &= \left(\Gamma_L \setminus \left\{\overline{\ell}\right\}\right) \cup (\Gamma_R \setminus \{\ell\})
\end{aligned}
$$

*where $v$ is a new node and $\rho(\varphi)$ denotes the root node of $\varphi$.* □

If $\psi = \varphi_L \odot_\ell \varphi_R$, then $\varphi_L$ and $\varphi_R$ are *direct subproofs* of $\psi$ and $\psi$ is a *child* of both $\varphi_L$ and $\varphi_R$. The transitive closure of the direct subproof relation is the *subproof* relation. A subproof which has no direct subproof is an *axiom* of the proof. Contrary to the usual graph and proof theoretic conventions but following the actual implementation of the data structures used by `LowerUnivalents`, edges are directed from children (resolvents) to their parents (premises). $V_\psi$, $E_\psi$ and $\Gamma_\psi$ denote, respectively, the nodes, edges and proved clause (conclusion) of $\psi$.

**Definition 2** (Active literals)**.** *Given a proof $\psi$, the set of active literals $A_\psi(\varphi)$ of a subproof $\varphi$ are the labels of edges coming into $\varphi$'s root:*

$$A_\psi(\varphi) = \{\ell \mid \exists \varsigma \in V_\psi.\ \varsigma \xrightarrow{\ell} \rho(\varphi)\}$$

Two operations on proofs are used in this paper: the resolution operation $\odot_\ell$ introduced above and the deletion of a set of subproofs from a proof, denoted $\psi \setminus (\varphi_1 \dots \varphi_n)$ where $\psi$ is the whole proof and $\varphi_i$ are the deleted subproofs. Algorithm 1 describes the deletion operation, with $\psi \setminus (\varphi_1 \dots \varphi_n)$ being the result of `delete(`$\psi$`,`$\{\varphi_1, \dots, \varphi_n\}$`)`. Both the resolution and deletion operations are considered to be left associative.

The basic idea of the deletion algorithm is to traverse the proof in a top-down manner, replacing each subproof having one of its premises marked for deletion (i.e. in $D$) by its other

**Input**: a proof $\varphi$
**Input**: $D$ a set of subproofs
**Output**: a proof $\varphi'$ obtained by deleting the subproofs in $D$ from $\varphi$

1 **if** $\varphi \in D$ *or* $\rho(\varphi)$ *has no premises* **then**
2  **return** $\varphi$ ;
3 **else**
4  **let** $\varphi_L$, $\varphi_R$ *and* $\ell$ be such that $\varphi = \varphi_L \odot_\ell \varphi_R$ ;
5  **let** $\varphi'_L$ = `delete`($\varphi_L$,$D$) ;
6  **let** $\varphi'_R$ = `delete`($\varphi_R$,$D$) ;
7  **if** $\varphi'_L \in D$ **then**
8  **return** $\varphi'_R$ ;
9  **else if** $\varphi'_R \in D$ **then**
10  **return** $\varphi'_L$ ;
11  **else if** $\overline{\ell} \notin \Gamma_{\varphi'_L}$ **then**
12  **return** $\varphi'_L$ ;
13  **else if** $\ell \notin \Gamma_{\varphi'_R}$ **then**
14  **return** $\varphi'_R$ ;
15  **else**
16  **return** $\varphi'_L \odot_\ell \varphi'_R$ ;

**Algorithm 1:** `delete`

direct subproof. The special case when both $\varphi'_L$ and $\varphi'_R$ belong to $D$ is treated rather implicitly and deserves an explanation: in such a case, one might intuitively expect the result $\varphi'$ to be undefined and arbitrary. Furthermore, to any child of $\varphi$, $\varphi'$ ought to be seen as if it were in $D$, as if the deletion of $\varphi'_L$ and $\varphi'_R$ propagated to $\varphi'$ as well. Instead of assigning some arbitrary proof to $\varphi'$ and adding it to $D$, the algorithm arbitrarily returns (in line 8) $\varphi'_R$ (which is already in $D$) as the result $\varphi'$. In this way, the propagation of deletion is done automatically and implicitly. For instance, the following hold:

$$\varphi_1 \odot_\ell \varphi_2 \setminus (\varphi_1, \varphi_2) = \varphi_2 \tag{1}$$

$$\varphi_1 \odot_\ell \varphi_2 \odot_{\ell'} \varphi_3 \setminus (\varphi_1, \varphi_2) = \varphi_3 \setminus (\varphi_1, \varphi_2) \tag{2}$$

A side-effect of this clever implicit propagation of deletion is that the actual result of deletion is only meaningful if it is not in $D$. In the example (1), as $\varphi_1 \odot_\ell \varphi_2 \setminus (\varphi_1, \varphi_2) \in \{\varphi_1, \varphi_2\}$, the actual resulting proof is meaningless. Only the information that it is a deleted subproof is relevant, as it suffices to obtain meaningful results as shown in (2).

**Proposition 1.** *For any proof $\psi$ and any sets $A$ and $B$ of $\psi$'s subproofs, either $\psi \setminus (A \cup B) \in A \cup B$ and $\psi \setminus (A) \setminus (B) \in A \cup B$, or $\psi \setminus (A \cup B) = \psi \setminus (A) \setminus (B)$.*

**Definition 3** (Valent literal)**.** *In a proof $\psi$, a literal $\ell$ is* valent *for the subproof $\varphi$ iff $\overline{\ell}$ belongs to the conclusion of $\psi \setminus (\varphi)$ but not to the conclusion of $\psi$.*

**Proposition 2.** *In a proof $\psi$, every valent literal of a subproof $\varphi$ is an active literal of $\varphi$.*

**Proposition 3.** *Given a proof $\psi$ and a set $D = \{\varphi_1 \dots \varphi_n\}$ of $\psi$'s subproofs, $\forall \ell \in \mathcal{L}$ s.t. $\ell$ is in the conclusion of $\psi \setminus (D)$ but not in $\psi$'s conclusion, then $\exists i$ s.t. $\overline{\ell}$ is a valent literal of $\varphi_i$ in $\psi$.*

**Input**: a proof $\psi$
**Output**: a compressed proof $\psi'$

```
1 Units ← ∅ ;
2 for every subproof φ in a bottom-up traversal do
3     if φ is a unit and has more than one child then
4         Enqueue φ in Units;
5 ψ' ← delete(ψ,Units) ;
6 for every unit φ in Units do
7     let {ℓ} = Γ_φ ;
8     if ℓ̄ ∈ Γ_ψ' then ψ' ← ψ' ⊙_ℓ φ ;
```

**Algorithm 2:** `LowerUnits`

# 3 LowerUnits

When a subproof $\varphi$ has more than one child in a proof $\psi$, it may be possible to *factor* all the corresponding resolutions: a new proof is constructed by removing $\varphi$ from $\psi$ and reintroducing it later. The resulting proof is smaller because $\varphi$ participates in a single resolution inference in it (i.e. it has a single child), while in the original proof it participates in as many resolution inferences as the number of children it had. Such a factorization is called *lowering* of $\varphi$, because its delayed reintroduction makes $\varphi$ appear at the bottom of the resulting proof.

Formally, a subproof $\varphi$ in a proof $\psi$ can be lowered if there exists a proof $\psi'$ and a literal $\ell$ such that $\psi' = \psi \setminus (\varphi) \odot_\ell \varphi$ and $\Gamma_{\psi'} \subseteq \Gamma_\psi$. It has been noted in [7] that $\varphi$ can always be lowered if it is a *unit*: its conclusion clause has only one literal. This led to the invention of the `LowerUnits` algorithm, which lowers every unit with more than one child, taking care to reintroduce units in an order corresponding to the subproof relation: if a unit $\varphi_2$ is a subproof of a unit $\varphi_1$ then $\varphi_2$ has to be reintroduced later than (i.e. below) $\varphi_1$.

A possible presentation of `LowerUnits` is shown in Algorithm 2. Units are collected during a first traversal. As this traversal is bottom-up, units are stored in a queue. The traversal could have been top-down and units stored in a stack. Units are effectively deleted during a second, top-down traversal. The last for-loop performs the reintroduction of units.

# 4 LowerUnivalents

`LowerUnits` does not lower every lowerable subproof. In particular, it does not take into account the already lowered subproofs. For instance, if a unit $\varphi_1$ proving $\{a\}$ has already been lowered, a subproof $\varphi_2$ with conclusion $\{\neg a, b\}$ may be lowered as well and reintroduced above $\varphi_1$. The posterior reintroduction of $\varphi_1$ will resolve away $\neg a$ and guarantee that it does not occur in the resulting proof's conclusion. But care must also be taken not to lower $\varphi_2$ if $\neg a$ is a valent literal of $\varphi_2$, otherwise $a$ will undesirably occur in the resulting proof's conclusion.

**Definition 4** (Univalent subproof)**.** *A subproof $\varphi$ in a proof $\psi$ is* univalent *w.r.t. a set $\Delta$ of literals iff $\varphi$ has exactly one valent literal $\ell$ in $\psi$, $\ell \notin \Delta$ and $\Gamma_\varphi \subseteq \Delta \cup \{\ell\}$. $\ell$ is called the* univalent literal *of $\varphi$ in $\psi$ w.r.t. $\Delta$.*

The principle of `LowerUnivalents` is to lower all univalent subproofs. Having only one valent literal makes them behave essentially like units w.r.t. the technique of lowering. $\Delta$ is

**Input**: a proof $\psi$
**Output**: a compressed proof $\psi'$

1 Univalents $\leftarrow \varnothing$ ;
2 $\Delta \leftarrow \varnothing$ ;
3 **for** *every subproof* $\varphi$*, in a top-down traversal* **do**
4 $\quad \psi' \leftarrow$ `delete(`$\varphi$`,`Univalents`)` ;
5 $\quad$ **if** $\psi'$ *is univalent w.r.t.* $\Delta$ **then**
6 $\quad\quad$ **let** $\ell$ be the univalent literal ;
7 $\quad\quad$ **push** $\overline{\ell}$ onto $\Delta$ ;
8 $\quad\quad$ **push** $\psi'$ onto Univalents ;
`// At this point,` $\psi' = \psi \setminus$ (Univalents)
9 **while** Univalents $\neq \varnothing$ **do**
10 $\quad \varphi \leftarrow$ **pop** from Univalents;
11 $\quad \ell \leftarrow$ **pop** from $\Delta$ ;
12 $\quad$ **if** $\ell \in \Gamma_{\psi'}$ **then** $\psi' \leftarrow \varphi \odot_\ell \psi'$ ;

**Algorithm 3:** Simplified `LowerUnivalents`

initialized to the empty set. Then the duals of the univalent literals are incrementally added to $\Delta$. Proposition 4 ensures that the conclusion of the resulting proof subsumes the conclusion of the original one.

**Proposition 4.** *Given a proof* $\psi$*, if there is a sequence* $U = (\varphi_1 \dots \varphi_n)$ *of* $\psi$*'s subproofs and a sequence* $(\ell_1 \dots \ell_n)$ *of literals such that* $\forall i \in [1 \dots n]$*,* $\ell_i$ *is the univalent literal of* $\varphi_i$ *w.r.t.* $\Delta_{i-1} = \{\overline{\ell_1} \dots \overline{\ell_{i-1}}\}$*, then the conclusion of*

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

*subsumes the conclusion of* $\psi$*.*

For this principle to lead to proof compression, it is important to take care of the mutual inclusion of univalent subproofs. Suppose, for instance, that $\varphi_i, \varphi_j, \varphi_k \in U$, $i < j < k$, $\varphi_j$ is a subproof of $\varphi_i$ but not a subproof of $\psi \setminus (\varphi_i)$, and $\overline{\ell_j} \in \Gamma_{\varphi_k}$. In this case, $\varphi_j$ will have one more child in

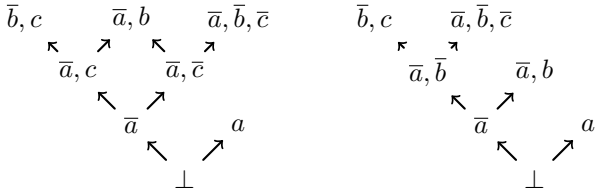
$$\psi \setminus (U) \odot_{\ell_n} \varphi_n \dots \odot_{\ell_k} \varphi_k \dots \odot_{\ell_j} \varphi_j \dots \odot_{\ell_i} \varphi_i \dots \odot_{\ell_1} \varphi_1$$

than in the original proof $\psi$. The additional child is created when $\varphi_j$ is reintroduced. All the other children are reintroduced with the reintroduction of $\varphi_i$, because $\varphi_j$ was not deleted from $\varphi_i$.

To solve this issue, `LowerUnivalents` traverses the proof in a top-down manner and simultaneously deletes already collected univalent subproofs, as sketched in Algorithm 3.

Figure 1 shows an example proof and the result of compressing it with `LowerUnivalents`. The top-down traversal starts with the leaves (axioms) and only visits a child when all its parents have already been visited. Assuming the unit with conclusion $\{a\}$ is the first visited leaf, it passes the univalent test in line 5, is marked for lowering (line 8) and the dual of its univalent literal is pushed onto $\Delta$ (line 7). When the subproof with conclusion $\{\overline{a}, b\}$ is considered, $\Delta = \{\overline{a}\}$. As this subproof has only one valent literal $b \notin \Delta$ and $\{\overline{a}, b\} \subseteq \Delta \cup \{b\}$, it is marked for lowering as well. At this point, $\Delta = \{\overline{a}, \overline{b}\}$, `Univalents` contains the two subproofs marked for lowering and $\psi'$ is the subproof with conclusion $\{\overline{a}, \overline{b}\}$ shown in Subfig. (b) (i.e. the

result of deleting the two marked subproofs from the original proof in Subfig. (a)). No other subproof is univalent; no other subproof is marked for lowering. The final compressed proof (Subfig. (b)) is obtained by reintroducing the two univalent subproofs that had been marked (lines 9 – 12). It has one resolution less than the original. This is so because the subproof with conclusion $\{\overline{a}, b\}$ had been used (resolved) twice in the original proof, but lowering delays its use to a point where a single use is sufficient.




(a) Original proof (b) Compressed proof

Figure 1: Example of proof crompression by `LowerUnivalents`

Although the call to `delete` inside the first loop (line 3 to 8) suggests quadratic time complexity, this loop (line 3 to 8) can be (and has been) actually implemented as a recursive function extending a recursive implementation of `delete`. With such an implementation, `LowerUnivalents` has a time complexity linear w.r.t. the size of the proof, assuming the univalent test (at line 5) is performed in constant bounded time.

Determining whether a literal is valent is expensive. But thanks to Proposition 2, subproofs with one active literal which is not in $\Gamma_\psi$ can be considered instead of subproofs with one valent literal. If the active literal is not valent, the corresponding subproof will simply not be reintroduced later (i.e. the condition in line 28 of Algorithm 4 will fail).

While verifying if a subproof could be univalent, some edges might be deleted. If a subproof $\varphi_i$ has already been collected as univalent subproof with univalent literal $\ell_i$ and the subproof $\varphi'$ being considered now has $\ell_i$ as active literal, the corresponding incoming edges can be removed. Even if $\ell_i$ is valent for $\varphi'$, only $\overline{\ell_i}$ would be introduced, and it would be resolved away when reintroducing $\varphi_i$. The `delete` operation can be easily modified to remove both nodes and edges.

Algorithm 4 sums up the previous remarks on how to efficiently implement `LowerUnivalents`. As noticed above, sometimes this algorithm may consider a subproof as univalent when it is actually not. But as care is taken when reintroducing subproofs (at line 28), the resulting conclusion still subsumes the original. The test that $\ell \in \Gamma_\varphi$ at line 20 is mandatory since $\ell$ might have been deleted from $\Gamma_\varphi$ by the deletion of previously collected subproofs.

Every node in a proof $\langle V, E, \Gamma \rangle$ has exactly two outgoing edges unless it is the root of an axiom. Hence the number of axioms is $|V| - \frac{1}{2}|E|$ and because there is at least one axiom, the average number of active literals per node is strictly less than two. Therefore, if `LowerUnivalents` is implemented as an improved recursive `delete`, its time complexity remains linear, assuming membership of literals to the set $\Delta$ is computed in constant time.

**Proposition 5.** *Given a proof $\psi$, `LowerUnits`$(\psi)$ has at least as many nodes as `LowerUnivalents`$(\psi)$ if there are no two units in $\psi$ with the same conclusion.*

In the case where there are at least two units with the same conclusion in $\psi$, the compressed proof depends on the order in which the units are collected. For both algorithms, only one of these units appears in the compressed proof.

**Data**: a proof $\psi$, compressed in place
**Input**: a set $D_V$ of subproofs to delete
**Input**: a set $D_E$ of edges to delete

```
1  Univalents ← ∅ ;
2  Δ ← ∅ ;
3  for every subproof φ, in a top-down traversal of ψ do
       // The deletion part.
4      if φ is not an axiom then
5          let φ = φ_L ⊙_ℓ φ_R ;
6          if φ_L ∈ D_V or ρ(φ) -ℓ̄-> ρ(φ_L) ∈ D_E then
7              if ρ(φ) -ℓ-> ρ(φ_R) ∈ D_E then
8                  add φ to D_V ;
9              else
10                 replace φ by φ_R ;
11         else if φ_R ∈ D_V or ρ(φ) -ℓ̄-> ρ(φ_R) ∈ D_E then
12             if ρ(φ) -ℓ-> ρ(φ_L) ∈ D_E then
13                 add φ to D_V ;
14             else
15                 replace φ by φ_L ;
           // Test whether φ is univalent.
16     ActiveLiterals ← ∅ ;
17     for each incoming edge e = v -ℓ-> ρ(φ), e ∉ D_E do
18         if ℓ̄ ∈ Δ then
19             add e to D_E ;
20         else if ℓ ∉ Δ, ℓ ∈ Γ_φ and ℓ ∉ Γ_ψ then
21             add ℓ to ActiveLiterals;
22     if ActiveLiterals = {ℓ} and Γ_φ ⊆ Δ ∪ {ℓ} then
23         push ℓ̄ onto Δ ;
24         push φ onto Univalents;
   // Reintroduce lowered subproofs.
25 while Univalents ≠ ∅ do
26     φ ← pop from Univalents;
27     ℓ ← pop from Δ ;
28     if ℓ ∈ Γ_ψ then
29         replace ψ by φ ⊙_ℓ ψ ;
```

**Algorithm 4:** Optimized `LowerUnivalents` as an enhanced `delete`

# 5 Experiments

`LowerUnivalents` and `LUnivRPI` have been implemented in the functional programming language Scala[1] as part of the Skeptik library[2]. `LowerUnivalents` has been implemented as a recursive `delete` improvement.

The algorithms have been experimented on 5 059 proofs (QF_UF: 3907, QF_IDL: 475, QF_LIA: 385, QF_UFIDL: 156, QF_UFLIA: 106, QF_RDL : 30) produced by the SMT-solver veriT[3] on unsatisfiable benchmarks from the SMT-Lib[4].

The experiment compared the following algorithms: **LU**, the `LowerUnits` algorithm from [7]; **LUniv**, the `LowerUnivalents` algorithm; **RPI**, the `RecyclePivotsWithIntersection` from [7]; **RPILU**, a non-sequential combination of `RPI` after `LowerUnits`; **RPILUniv**, a non-sequential combination of `RPI` after `LowerUnivalents`; **LU.RPI**, the sequential composition of `LowerUnits` after `RPI`; **LUnivRPI**, the non-sequential combination of `LowerUnivalents` after `RPI` as described in Sect. A; **Split**, Cotton's `Split` algorithm ([5]); **RedRec**, the `Reduce&Reconstruct` algorithm from [10]; **Best RPILU/LU.RPI**, which performs both `RPILU` and `LU.RPI` and chooses the smallest resulting compressed proof; **Best RPILU/LUnivRPI**, which performs `RPILU` and `LUnivRPI` and chooses the smallest resulting compressed proof.

For each of these algorithms, the time needed to compress the proof along with the number of nodes and the number of axioms (i.e. *unsat core* size) have been measured. Raw data of the experiment can be downloaded from Skeptik's repository[5].

The experiments were executed on the Vienna Scientific Cluster[6] VSC-2. Each algorithm was executed in a single core and had up to 16 GB of memory available. This amount of memory has been useful to compress the biggest proofs (with more than $10^6$ nodes).

The overall results of the experiments are shown in Table 1. The compression ratios in the second column are computed according to formula (3), in which $\psi$ ranges over all the proofs in the benchmark and $\psi'$ ranges over the corresponding compressed proofs.

$$1 - \frac{\sum |V_{\psi'}|}{\sum |V_{\psi}|} \tag{3}$$

The unsat core compression ratios are computed in the same way, but using the number of axioms instead of the number of nodes. The speeds on the fourth column are computed according to formula (4) in which $d_\psi$ is the duration in milliseconds of $\psi$'s compression by a given algorithm.

$$\frac{\sum |V_{\psi}|}{\sum d_{\psi}} \tag{4}$$

For the `Split` and `RedRec` algorithms, which must be repeated, a timeout has been fixed so that the speed is about 3 nodes per millisecond.

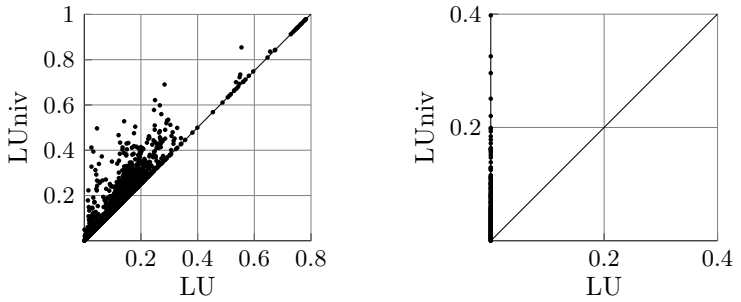
Figure 2 shows the comparison of `LowerUnits` with `LowerUnivalents`. Subfigures (a) and (b) are scatter plots where each dot represents a single benchmark proof.

As expected, `LowerUnivalents` always compresses more than `LowerUnits` (subfigure (a)) at the expense of a longer computation (subfigure (d)). And even if the compression gain is low on average (as noticeable in Table 1), subfigure (a) shows that `LowerUnivalents` compresses some proofs significantly more than `LowerUnits`.

[1] `http://www.scala-lang.org/`
[2] `https://github.com/Paradoxika/Skeptik`
[3] `http://www.verit-solver.org/`
[4] `http://www.smtlib.org/`
[5] `https://raw.github.com/Paradoxika/Skeptik/master/doc/papers/LUniv/all-final.csv`
[6] `http://vsc.ac.at/`

Table 1: Total compression ratios

| Algorithm | Compression | Unsat Core Compression | Speed |
|---|---|---|---|
| LU | 7.5 % | 0.0 % | 22.4 n/ms |
| LUniv | 8.0 % | 0.8 % | 20.4 n/ms |
| RPILU | 22.0 % | 3.6 % | 7.4 n/ms |
| RPILUniv | 22.1 % | 3.6 % | 6.5 n/ms |
| LU.RPI | 21.7 % | 3.1 % | 15.1 n/ms |
| LUnivRPI | 22.0 % | 3.6 % | 17.8 n/ms |
| RPI | 17.8 % | 3.1 % | 31.3 n/ms |
| Split | 21.0 % | 0.8 % | 2.9 n/ms |
| RedRec | 26.4 % | 0.4 % | 2.9 n/ms |
| Best RPILU/LU.RPI | 22.0 % | 3.7 % | 5.0 n/ms |
| Best RPILU/LUnivRPI | 22.2 % | 3.7 % | 5.2 n/ms |




(a) Compression ratio (b) Unsat core compression ratio

Figure 2: Comparison between LU and LUniv

It has to be noticed that veriT already does its best to produce compact proofs. In particular, a forward subsumption algorithm is applied, which results in proofs not having two different subproofs with the same conclusion. This results in `LowerUnits` being unable to reduce unsat core. But as `LowerUnivalents` lowers non-unit subproofs and performs some partial regularization, it achieves some unsat core reduction, as noticeable in subfigure (b).

# 6 Conclusions and Future Work

`LowerUnivalents`, the algorithm presented here, has been shown in the previous section to compress more than `LowerUnits`. This is so because, as demonstrated in Proposition 5, the set of subproofs it lowers is always a superset of the set of subproofs lowered by `LowerUnits`. It might be possible to lower even more subproofs by finding a characterization of (efficiently) lowerable subproofs broader than that of univalent subproofs considered here. This direction for future work promises to be challenging, though, as evidenced by the non-triviality of the optimizations discussed in Section 4 for obtaining a linear-time implementation of `LowerUnivalents`.

As discussed in Appendix A, the proposed algorithm can be embedded in the deletion

traversal of other algorithms. As an example, it has been shown that the combination of `LowerUnivalents` with `RPI`, compared to the sequential composition of `LowerUnits` after `RPI`, results in a better compression ratio with only a small processing time overhead (Figure 3). Other compression algorithms that also have a subproof deletion or reconstruction phase (e.g. `Reduce&Reconstruct`) could probably benefit from being combined with `LowerUnivalents` as well.

**Acknowledgments:** The authors would like to thank Pascal Fontaine for providing veriT's proofs for the experiments, for co-organizing our joint workshops on proof compression[7], and for several interesting and useful discussions on this topic.

# References

[1] Amjad, H.: Compressing propositional refutations. Electr. Notes Theor. Comput. Sci. 185, 3–15 (2007)

[2] Bar-Ilan, O., Fuhrmann, O., Hoory, S., Shacham, O., Strichman, O.: Linear-time reductions of resolution proofs. In: Chockler, H., Hu, A.J. (eds.) Haifa Verification Conference. Lecture Notes in Computer Science, vol. 5394, pp. 114–128. Springer (2008)

[3] Bouton, T., de Oliveira, D.C.B., Déharbe, D., Fontaine, P.: verit: An open, trustable and efficient smt-solver. In: Schmidt, R.A. (ed.) CADE. Lecture Notes in Computer Science, vol. 5663, pp. 151–156. Springer (2009)

[4] Cook, S.A.: The complexity of theorem-proving procedures. In: Harrison, M.A., Banerji, R.B., Ullman, J.D. (eds.) STOC. pp. 151–158. ACM (1971)

[5] Cotton, S.: Two techniques for minimizing resolution proofs. In: Strichman, O., Szeider, S. (eds.) Theory and Applications of Satisfiability Testing SAT 2010, Lecture Notes in Computer Science, vol. 6175, pp. 306–312. Springer (2010)

[6] Fontaine, P., Merz, S., Woltzenlogel Paleo, B.: Exploring and exploiting algebraic and graphical properties of resolution. In: 8th International Workshop on Satisfiability Modulo Theories - SMT 2010. Edinburgh, Royaume-Uni (Jul 2010), `http://hal.inria.fr/inria-00544658`

[7] Fontaine, P., Merz, S., Woltzenlogel Paleo, B.: Compression of propositional resolution proofs via partial regularization. In: Bjørner, N., Sofronie-Stokkermans, V. (eds.) CADE. Lecture Notes in Computer Science, vol. 6803, pp. 237–251. Springer (2011)

[8] Goerdt, A.: Comparing the complexity of regular and unrestricted resolution. In: Marburger, H. (ed.) GWAI. Informatik-Fachberichte, vol. 251, pp. 181–185. Springer (1990)

[9] Järvisalo, M., Le Berre, D., Roussel, O., Simon, L.: The international SAT solver competitions. AI Magazine 33(1), 89–92 (2012)

[10] Rollini, S.F., Bruttomesso, R., Sharygina, N.: An efficient and flexible approach to resolution proof reduction. In: Barner, S., Harris, I., Kroening, D., Raz, O. (eds.) Hardware and Software: Verification and Testing, Lecture Notes in Computer Science, vol. 6504, pp. 182–196. Springer (2011)

[11] Sinz, C.: Compressing propositional proofs by common subproof extraction. In: Moreno-Díaz, R., Pichler, F., Quesada-Arencibia, A. (eds.) EUROCAST. Lecture Notes in Computer Science, vol. 4739, pp. 547–555. Springer (2007)

[12] Tseitin, G.S.: On the complexity of derivation in propositional calculus. In: Siekmann, J., Wrightson, G. (eds.) Automation of Reasoning: Classical Papers in Computational Logic 1967-1970, vol. 2. Springer-Verlag (1983)

[7] `http://www.logic.at/people/bruno/MediaWiki/index.php/Amadeus_Vienna-Nancy_Joint_Project_on_Proof_Compression`

# A Remarks about Combining `LowerUnivalents` with `RPI`

**Definition 5** (Regular proof [12])**.** *A proof $\psi$ is* regular *iff on every path from its root to any of its axioms, each literal labels at most one edge. Otherwise, $\psi$ is* irregular*.*

Any irregular proof can be converted into a regular proof having the same axioms and the same conclusion. But it has been proved [8] that such a total regularization might result in a proof exponentially bigger than the original.

Nevertheless, *partial* regularization algorithms, such as `RecyclePivots` [2] and its improvement `RecyclePivotsWithIntersection` (`RPI`) [7], carefully avoid the worst case of total regularization and do efficiently compress proofs. For any subproof $\varphi$ of a proof $\psi$, `RPI` removes the edge $\rho(\varphi) \xrightarrow{\ell} v$ if $\ell$ is a safe literal for $\varphi$.

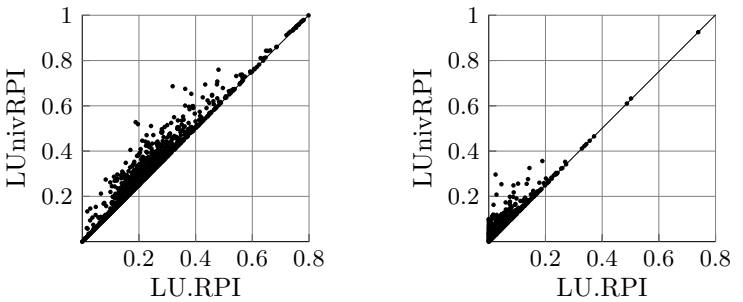
**Definition 6** (Safe literal)**.** *A literal $\ell$ is* safe *for a subproof $\varphi$ in a proof $\psi$ iff $\ell$ labels at least one edge on every path from $\rho(\psi)$ to $\rho(\varphi)$.*

`RPI` performs two traversals. During the first one, safe literals are collected and edges are marked for deletion. The second traversal is the effective deletion similar to the `delete` algorithm.

Both sequential compositions of `LowerUnits` with `RPI` have been shown to achieve good compression ratio [7]. However, the best combination order (`LowerUnits` after `RPI` (`LU.RPI`) or `RPI` after `LowerUnits` (`RPI.LU`)) depends on the input proof. A reasonable solution is to perform both combinations and then to choose the smallest compressed proof, but sequential composition is time consuming. To speed up DAG traversal, it is useful to topologically sort the nodes of the graph first. But in case of sequential composition this costly operation has to be done twice. Moreover, some traversals, like deletion, are identical in both algorithms and might be shared. Whereas implementing a non-sequential combination of `RPI` after `LowerUnits` is not difficult, a non-sequential combination of `LowerUnits` after `RPI` would be complicated. The difficulty is that `RPI` could create some new units which would be visible only after the deletion phase. A solution could be to test for units during deletion. But if units are effectively lowered during this deletion, their deletion would cause some units to become non-units. And postponing deletions of units until a second deletion traversal would prevent the sharing of this traversal and would cause one more topological sorting to be performed, because the deletion phase significantly transforms the structure of the DAG.

Apart from having an improved compression ratio, another advantage of `LowerUnivalents` over `LowerUnits` is that `LowerUnivalents` can be implemented as an enhanced `delete` operation. With such an implementation, a simple non-sequential combination of `LowerUnivalents` after `RPI` can be implemented just by replacing the second traversal of `RPI` by `LowerUnivalents`. After the first traversal of `RPI`, as all edges labeled by a safe literal have been marked for deletion, the remaining active literals are all valent, because for every edge $\rho(\varphi) \xrightarrow{\ell} \rho(\varphi')$, $\ell$ is either a safe literal of $\varphi$ or a valent literal of $\varphi'$. Therefore, in the second traversal of the non-sequential combination (deletion enhanced by `LowerUnivalents`), all univalent subproofs are lowered.

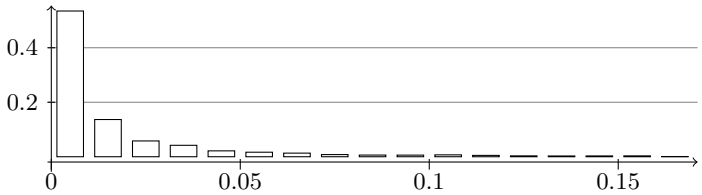
The comparison of the sequential `LU.RPI` with the non-sequential `LUnivRPI` shown in Fig. 3 outlines the ability of `LowerUnivalents` to be efficiently combined with other algorithms. Not only compression ratios are improved but `LUnivRPI` is faster than the sequential composition for more than 80 % of the proofs.



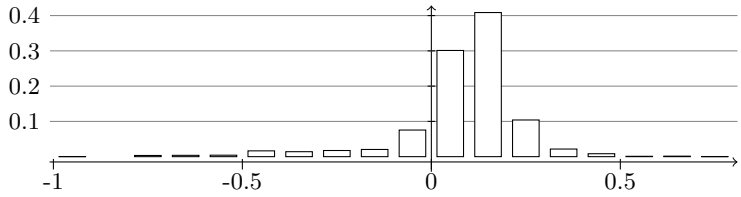

(a) Compression ratio




(b) Unsat core compression ratio




(c) Compression ratio difference




(d) Duration difference

Figure 3: Comparison between LU.RPI and LUnivRPI