Small pool resolution proofs of stone tautologies

Leszek Kołodziejczyk
University of Warsaw

(joint work with Sam Buss)

Limits of Theorem Proving
Rome, September 2012

Introduction

Pool resolution: a subsystem of resolution designed to correspond to DPLL with clause learning but no restarts. Original definition was by van Gelder 2005.

We use versions defined in terms of resolution trees with lemmas (Buss-Hoffman-Johannsen 2008).

regWRTL proofs

- proofs are ordered binary trees, each line is a clause,
- leaves are either axiom clauses or lemmas, i.e. clauses derived (learned) earlier in the proof, in the sense of the tree postorder,
- the rule is w-resolution: given A and B, w-resolution on x derives $(A \setminus \{x\}) \cup (B \setminus \{\bar{x}\})$, where $\bar{x} \notin A, x \notin B$.

regWRTL proofs

- proofs are ordered binary trees, each line is a clause,
- leaves are either axiom clauses or lemmas, i.e. clauses derived (learned) earlier in the proof, in the sense of the tree postorder,
- the rule is w-resolution: given A and B, w-resolution on x derives $(A \setminus \{x\}) \cup (B \setminus \{\bar{x}\})$, where $\bar{x} \notin A, x \notin B$.
- the proof is regular, meaning no variable is resolved on twice along the same branch.

Some variants of regWRTL

- regWRTI: only clauses derived by input subderivations are learned and can be used as lemmas, where a proof is input if in each inference at least one premise is a leaf,
- regRTL: all inferences have to be non-degenerate, meaning the resolution variable is present in both premises.
- regRTI: combines both restrictions.

regWRTI corresponds exactly to non-greedy DPLL with clause learning but no restarts (BHJ 2008).

Strength of pool-style systems

- regWRTI is strictly stronger than all proper subsystems of resolution closed under restrictions (proved in BKS 2004 in terms of DPLL with clause learning).
- Already regRTI is strictly stronger than regular resolution (BBJ 2012).
- Open problem: separate the pool-style systems from full resolution.

Candidates for separation?

Two main kinds of tautologies separating regular from full resolution:

- guarded versions of simple combinatorial tautologies (AJPU 2002, Urquhart 2011),

  Example: the usual "finite linear order has a least element" tautology, but with each transitivity clause $\overline{p}_{i,j}, \overline{p}_{j,k}, p_{i,k}$ replaced by two clauses: $\overline{p}_{i,j}, \overline{p}_{j,k}, p_{i,k}, p_{r,s}$ and $\overline{p}_{i,j}, \overline{p}_{j,k}, p_{i,k}, \overline{p}_{r,s}$.

- the stone tautologies (AJPU 2002).

The stone tautologies

$G = (V, E)$ dag with N vertices, where vertices $n+1, \ldots, N$ are sources; $1, \ldots, n$ have indegree 2; and 1 is the unique sink. All edges are from higher- to lower-numbered vertices. Let $m \geq N$.

Stone(G, m) has variables $p_{i,j}$, r_j, for $i \leq N$, $j \leq m$, and clauses:

- $p_{i,1}, \ldots, p_{i,m}$, for each i,
- $\overline{p}_{i,j}, r_j$, for $n+1 \leq i \leq N$, each j,
- $\overline{p}_{1,j}, \overline{r}_j$, for each j,
- $\overline{p}_{i',j'}, \overline{r}_{j'}, \overline{p}_{i'',j''}, \overline{r}_{j''}, \overline{p}_{i,j}, r_j$, for i', i'' the two predecessors of i, and each j, j', j'' such that $j \notin \{j', j''\}$. (induction clause)

Candidates for separation???

Guarded tautologies known to be hard for regular resolution do have short proofs in regRTI (BBJ 2012).

Intuitively, finding short pool proofs for stone tautologies should be harder, as their "canonical" resolution proofs are highly non-regular.

Candidates for separation???

Guarded tautologies known to be hard for regular resolution do have short proofs in regRTI (BBJ 2012).

Intuitively, finding short pool proofs for stone tautologies should be harder, as their "canonical" resolution proofs are highly non-regular. However...

Theorem

- *Stone*(G, m) *has a regWRTL refutation of size* $O(Nm^3)$,
- *Stone*(G, m) *has a regRTI refutation of size* $O(N^3m^4)$.

The proof: high-level view

Intuition (not quite right): building proof bottom-up, first resolve on the $p_{i,j}$'s, then on the problematic r_j's.

Structure:

n-th segment

$n-1$-st segment

$\vdots$

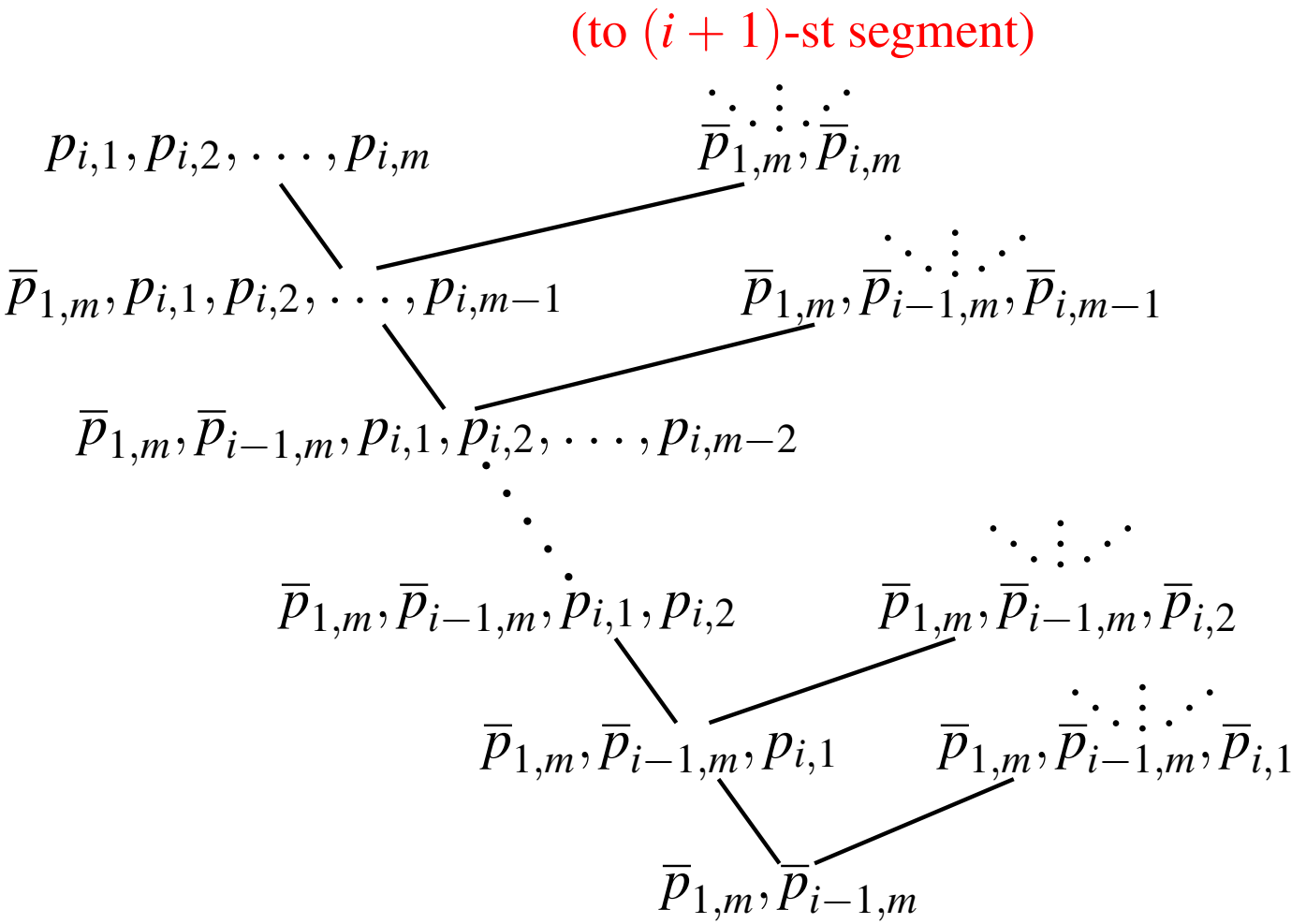
2-nd segment

1-st segment

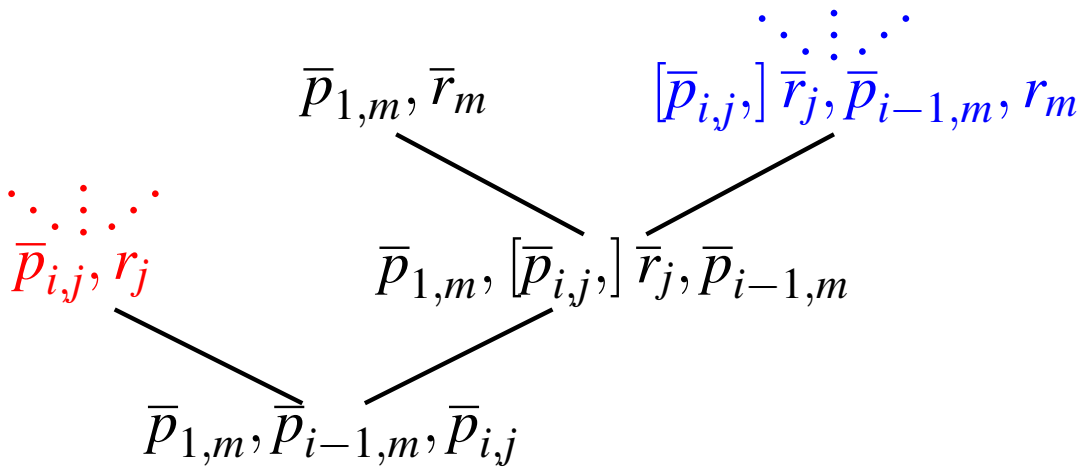
$\bot$

The i_0-th segment resolves on $p_{i_0,j}$'s (plus some other variables) and learns clauses $\overline{p}_{i_0,j}$, r_j.

The "skeleton" of the i-th segment



The proof above $\overline{p}_{1,m}, \overline{p}_{i-1,m}, \overline{p}_{i,j}$



On l.h.s., we want to learn $\overline{p}_{i,j}, r_j$.

On r.h.s., we just want a valid proof, without trying to learn anything. The literal $\overline{p}_{i,j}$ is present iff $(i, i-1) \in E$.

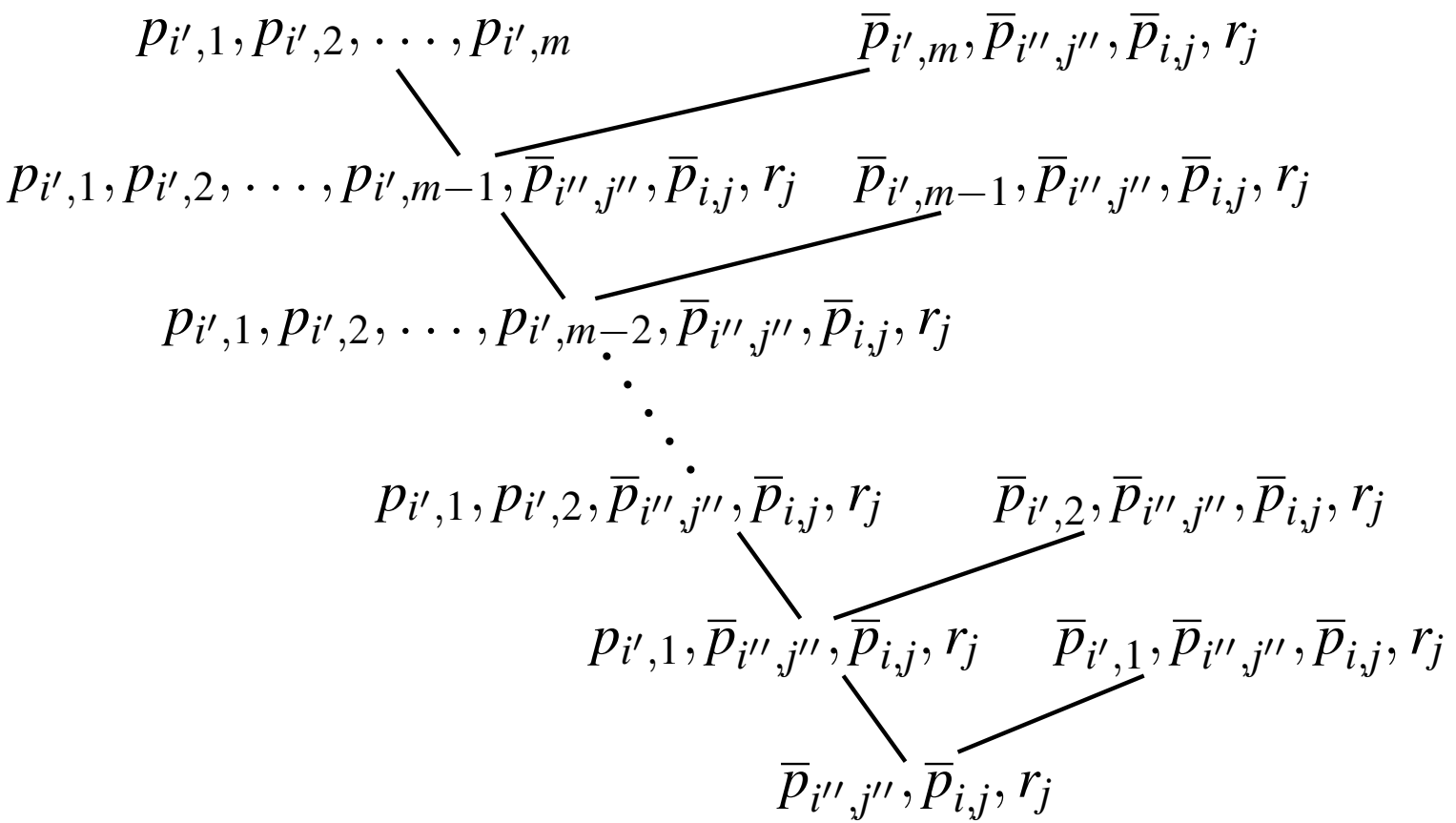
Learning $\overline{p}_{i,j}$, r_j, take one

$$\dfrac{\dfrac{\overline{p}_{i',j'}, \overline{r}_{j'}, \overline{p}_{i'',j''}, \overline{r}_{j''}, \overline{p}_{i,j}, r_j \qquad \overline{p}_{i',j'}, r_{j'}}{\overline{p}_{i',j'}, \overline{p}_{i'',j''}, \overline{r}_{j''}, \overline{p}_{i,j}, r_j} \qquad \overline{p}_{i'',j''}, r_{j''}}{\overline{p}_{i',j'}, \overline{p}_{i'',j''}, \overline{p}_{i,j}, r_j}$$

The vertices i', i'' are the predecessors of i.

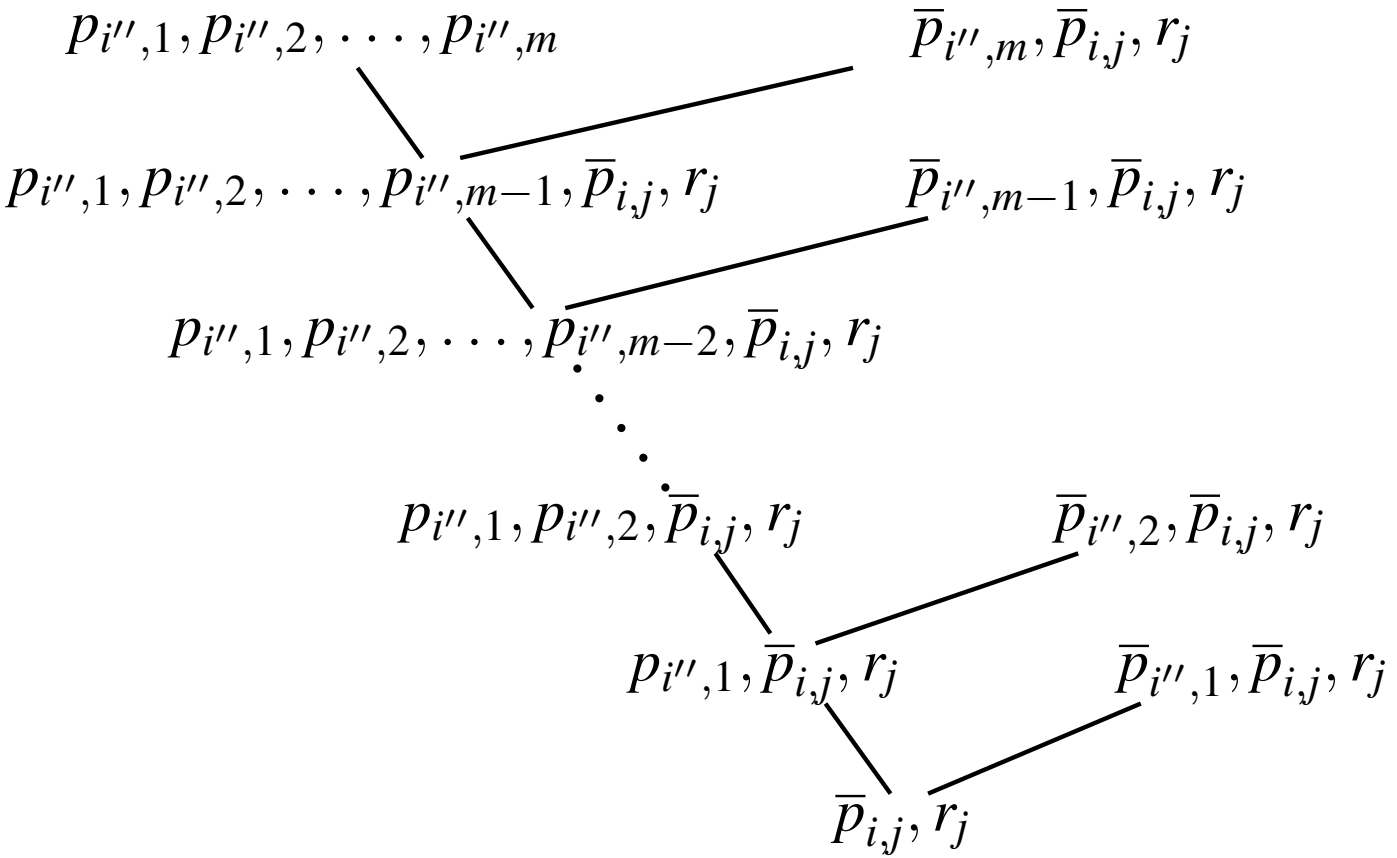
This inference is only needed if j is not among j', j''.

Learning $\overline{p}_{i,j}, r_j$, take two



Clause $\overline{p}_{i',j}, r_j$ is used instead of $\overline{p}_{i',j}, \overline{p}_{i'',j''}, \overline{p}_{i,j}, r_j$.

Learning $\overline{p}_{i,j}, r_j$, take three



Clause $\overline{p}_{i'',j}, r_j$ is used instead of $\overline{p}_{i'',j}, \overline{p}_{i,j}, r_j$.

Dealing with the right-hand side

$$\begin{matrix} \ddots & \vdots & \ddots \\ [\overline{p}_{i,j}, & \overline{r}_j, & \overline{p}_{i-1,m}, r_m \end{matrix}$$

This is handled essentially like $\overline{p}_{i-1,m}, r_m$, except that:

- the presence of $\overline{r}_j$ is taken into account,
- if $(i, i-1) \in E$, then some modifications occur.

Comments on proof

- To learn $\overline{p}_{i,m}, r_m$, derive $\overline{p}_{1,m}, \overline{p}_{i-1,m}, \overline{p}_{i,m-1}$ from itself and $\overline{p}_{1,m}, \overline{p}_{i,m}$ by w-resolution on $p_{i,m}$ (this is a degenerate inference!).
- The subderivation leading to $\overline{p}_{i,j}, r_j$ is not input.
- There are some changes in segments 1, 2 and n.
- We never use the assumption $m \geq N$ (more stones than vertices)!

Better properties?

Two things we might do to make the proof better:

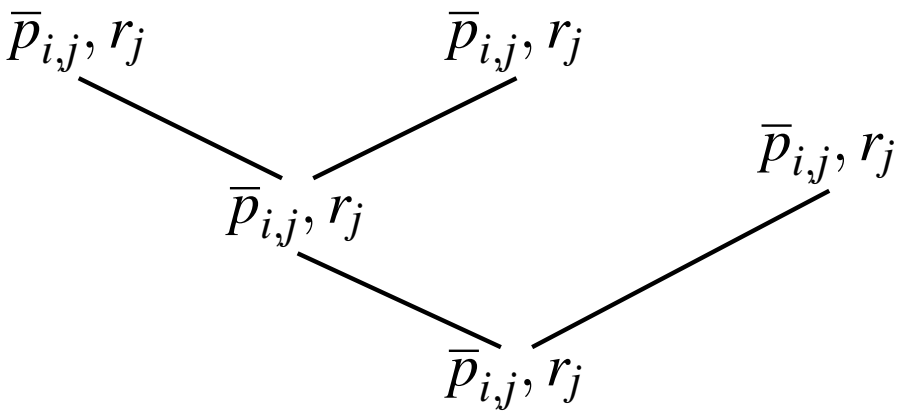
- make all lemmas derived by input subderivations,
- get rid of degenerate inferences.

Inputization

Making the proof become regWRTI is easy.

In the subderivation leading to $\overline{p}_{i,j}, r_j$, each clause is at distance ≤ 3 from a leaf. So, essentially, we just need to derive $\overline{p}_{i,j}, r_j$ thrice.

To do that, use gadgets like:



These are (highly degenerate) w-resolutions on irrelevant variables.

Eliminating degeneracies

Putting the proof into regRTI requires much more work.

The basic idea remains is the same, but the clauses $\overline{p}_{1,m}, \overline{p}_{i-1,m}, \overline{p}_{i,j}$ have to be replaced.

Instead, we use more complicated clauses of $\overline{p}$ literals, taking graph structure into account and making sure every vertex mentioned in the clause "matters".

Eliminating degeneracies (cont'd)

Constructing the proof bottom-up, build clauses of the form

$$\overline{p}_{1,j_1}, \overline{p}_{i_2,j_2}, \ldots, \overline{p}_{i_k,j_k}, \tag{1}$$

by branching on p variables related to "not yet fully learned" predecessors of "relevant" i_ℓ's.
(Sometimes, i_ℓ stops being "relevant" and then $\overline{p}_{i_\ell,j_\ell}$ is dropped.)

Once the clause can no longer be extended in this way, it is derived by a regular derivation, and progress towards learning $\overline{p}_{i_k,j_k}, r_{j_k}$ is made, unless it has been learned already.

Interestingly, the construction makes use of the assumption $m \geq N$.