Circular (Yet Sound) Proofs

Massimo Lauria (joint work with Albert Atserias)

SAT 2019, Lisbon - July, 10th

Sapienza - Università di Roma

Further generalization of resolution proof graphs

Tree Resolution	(trees)
Regular Resolution	(read-once dags)
Resolution	(dags)

Further generalization of resolution proof graphs

Tree Resolution		(trees)
Regular Resolution		(read-once dags)
Resolution		(dags)
Circular Resolution	(NEW!)	**(cycles)**

Cycles in proof???

Cycles in proof???

We introduce cycles while retaining **soundness**

We get **exponential gain** over resolution

I. What is a circular proof?

Inference rules

Standard rules:

$$\frac{C \vee X \qquad D \vee \overline{X}}{C \vee D} \qquad\qquad \frac{C}{C \vee D} \qquad\qquad \frac{}{X \vee \overline{X}}$$

Inference rules

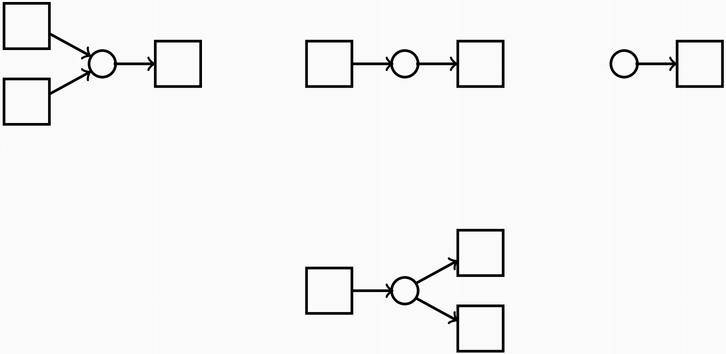
Standard rules:

$$\frac{C \vee X \qquad D \vee \overline{X}}{C \vee D} \qquad\qquad \frac{C}{C \vee D} \qquad\qquad \frac{}{X \vee \overline{X}}$$

Symmetric rules:

$$\frac{C \vee X \qquad C \vee \overline{X}}{C} \qquad\qquad \frac{C}{C \vee X \qquad C \vee \overline{X}} \qquad\qquad \frac{}{X \vee \overline{X}}$$

Graphical representation of proof inferences



Formula vertices: □ Inference vertices: ○

First example

Want: $E, F \vdash A$

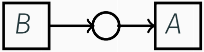
First example

Want: $E, F \vdash A$

$\boxed{A}$

First example

Want: $E, F \vdash A$

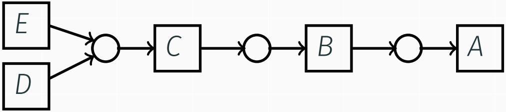


First example

Want: $E, F \vdash A$

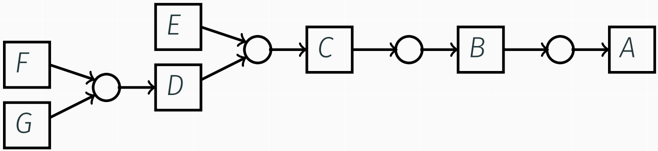
First example

Want: $E, F \vdash A$



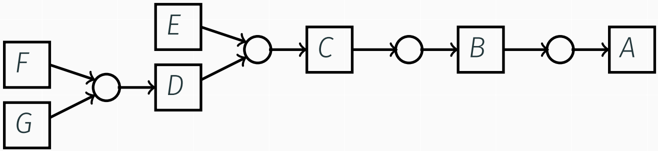
First example

Want: $E, F \vdash A$



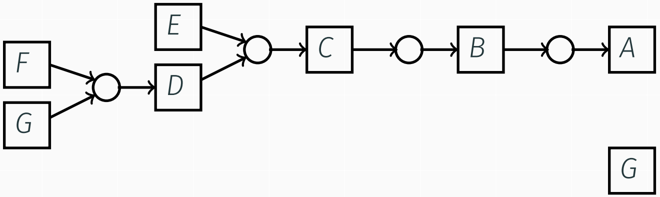
First example

Want: $E, F \vdash A$
Subgoal: $E, F \vdash G$



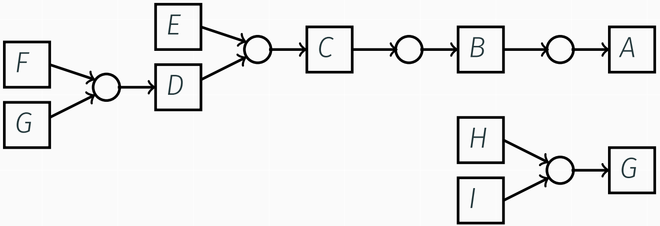
First example

Want: $E, F \vdash A$
Subgoal: $E, F \vdash G$



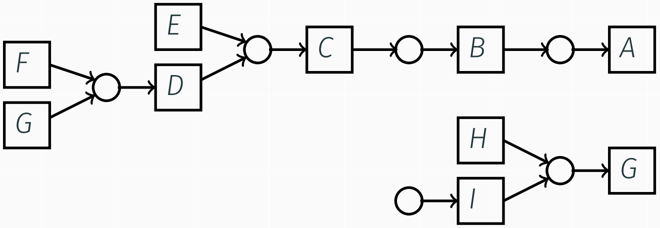
First example

Want: $E, F \vdash A$
Subgoal: $E, F \vdash G$



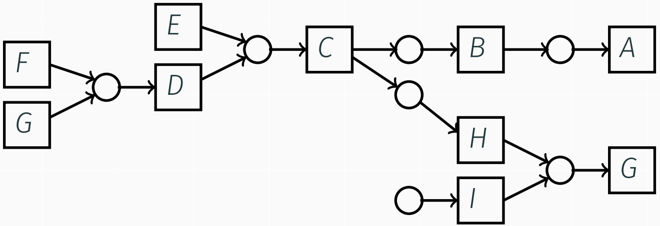
First example

Want: $E, F \vdash A$
Subgoal: $E, F \vdash G$

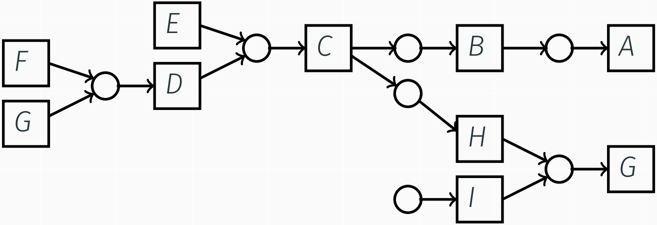


First example

Want: $E, F \vdash A$
Subgoal: $E, F \vdash G$



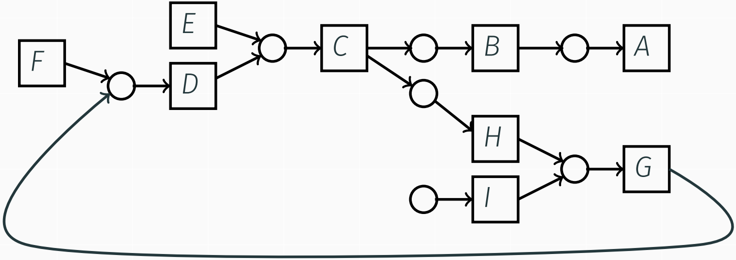
Want: $E, F \vdash A$
Subgoal: $E, F \vdash G$



...WHAT?...

First example

Want: $E, F \vdash A$
Subgoal: $E, F \vdash G$

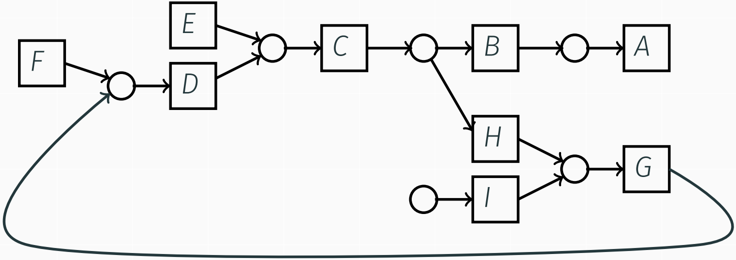


...WHAT?...

First example

Want: $E, F \vdash A$

Subgoal: $E, F \vdash G$

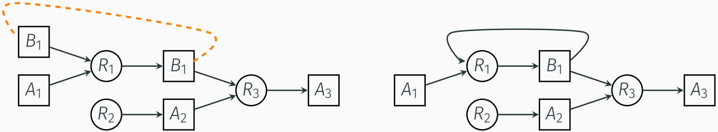


...WHAT?...

Circular Pre-proofs

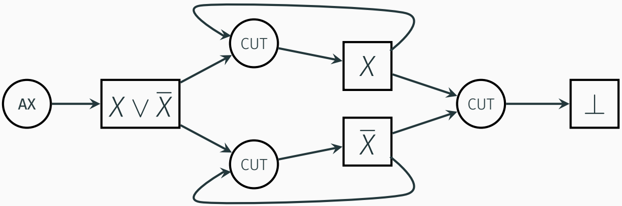
Definition: A pre-proof is

- a graph of a resolution proof with the symmetric rules,
- where occurrences of the same formula can be identified (potentially creating cycles)



Remark. formula and inference vertices form a bipartition.

Guess what? Circular arguments may be unsound



How to make them sound?

Need to keep track of how many times a formula vertex $\square$ is

used as a premise

vs

deduced as a consequence

How to make them sound?

Need to keep track of how many times a formula vertex □ is

used as a premise

vs

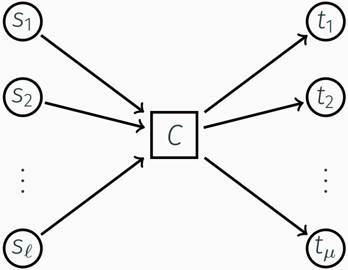
deduced as a consequence

Solution.

We assign a flow in $\mathbb{R}^+$ to each inference vertex ○.

Flow and balance

Flow is a positive real assigned to each inference vertex.



We define the balance of a formula vertex $\boxed{C}$ as

$$\mathsf{Bal}_{\boxed{C}} = \sum_{i=1}^{\ell} \mathrm{flow}(s_i) - \sum_{i=1}^{\mu} \mathrm{flow}(t_i)$$

Circular proof

Definition: A circular resolution proof of A from $A_1, \ldots, A_m$ is a pre-proof for which we can assign a flow to each inference vertex so that

- when **Bal** $_{\boxed{C}} < 0$, then $C \in \{A_1, \ldots, A_m\}$,
- there is a formula vertex $\boxed{A}$ with **Bal** $_{\boxed{A}} > 0$.

Circular proof

Definition: A circular resolution proof of A from $A_1, \ldots, A_m$ is a pre-proof for which we can assign a flow to each inference vertex so that

- when $\mathbf{Bal}_{\boxed{C}} < 0$, then $C \in \{A_1, \ldots, A_m\}$,
- there is a formula vertex $\boxed{A}$ with $\mathbf{Bal}_{\boxed{A}} > 0$.

Notes:

- efficient verification: linear programming techniques.

Soundness

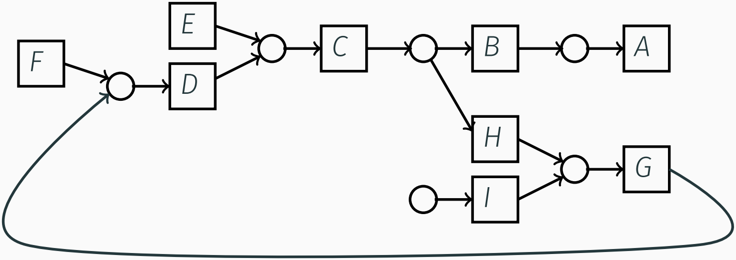
Theorem:
If there is a circular proof of A from $A_1, \ldots, A_m$,
then every assignment that satisfies $A_1, \ldots, A_m$ also satisfies A.

Proofs:

- 1st proof: combinatorial
- 2nd proof: via linear programming
- 3rd proof: equivalence with another proof system

Sound example

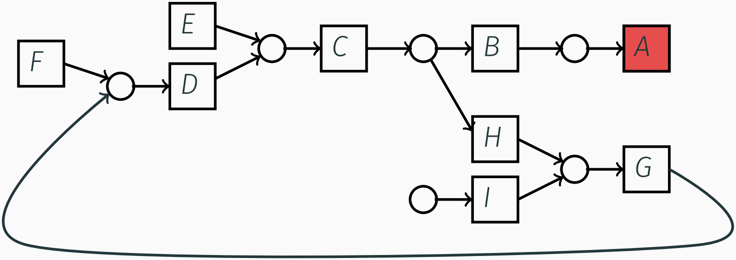
Want: $E, F \vdash A$



Flow assignment: all 1's.

Sound example

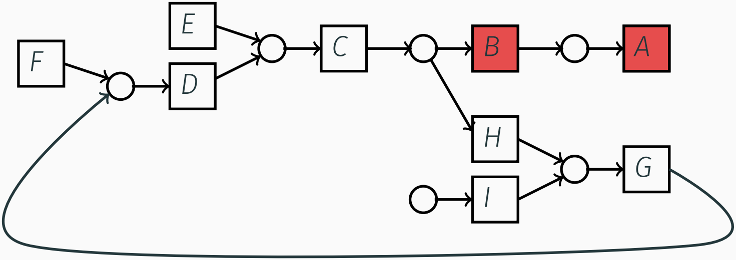
Want: $E, F \vdash A$



Flow assignment: all 1's.

Sound example

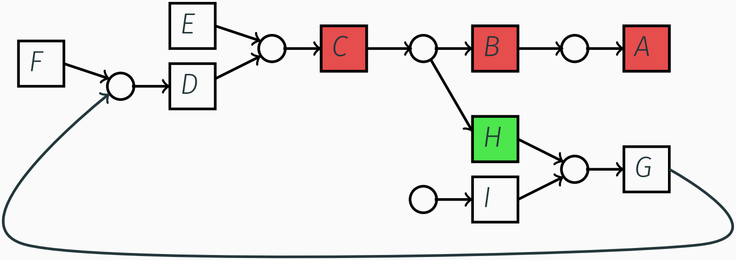
Want: $E, F \vdash A$



Flow assignment: all 1's.

Sound example

Want: $E, F \vdash A$

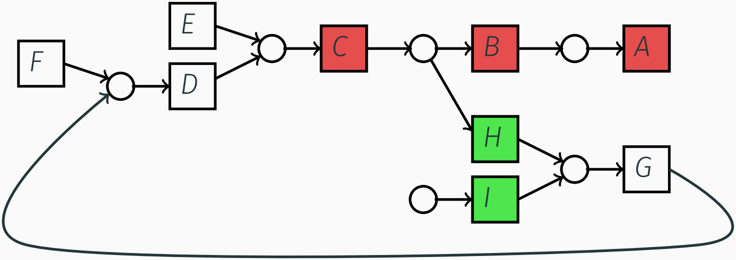


Flow assignment: all 1's.

Important. in split rule at most one consequence false.

Sound example

Want: $E, F \vdash A$

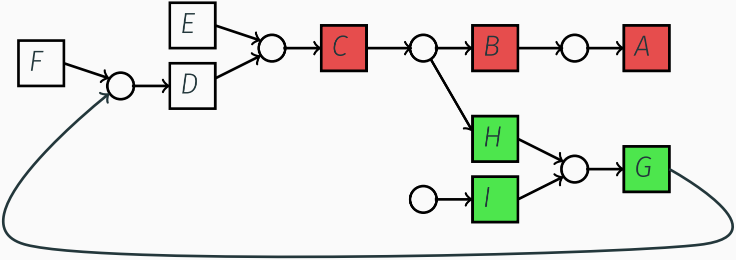


Flow assignment: all 1's.

Important. in split rule at most one consequence false.

Sound example

Want: $E, F \vdash A$

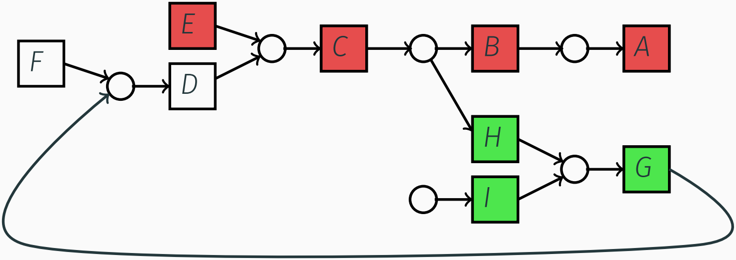


Flow assignment: all 1's.

Important. in split rule at most one consequence false.

Sound example

Want: $E, F \vdash A$

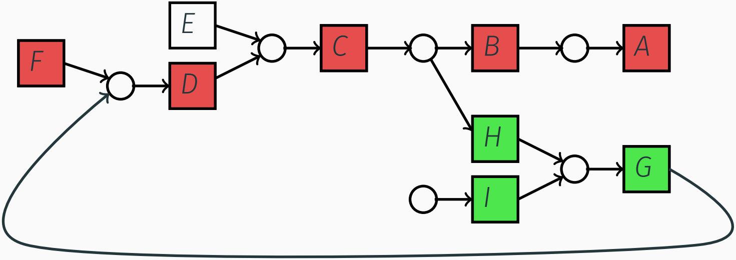


Flow assignment: all 1's.

Important. in split rule at most one consequence false.

Sound example

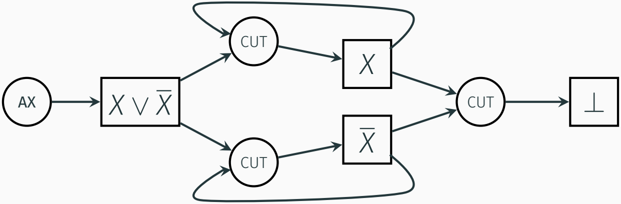
Want: $E, F \vdash A$



Flow assignment: all 1's.

Important. in split rule at most one consequence false.

Unsound example



Impossible to assign flow

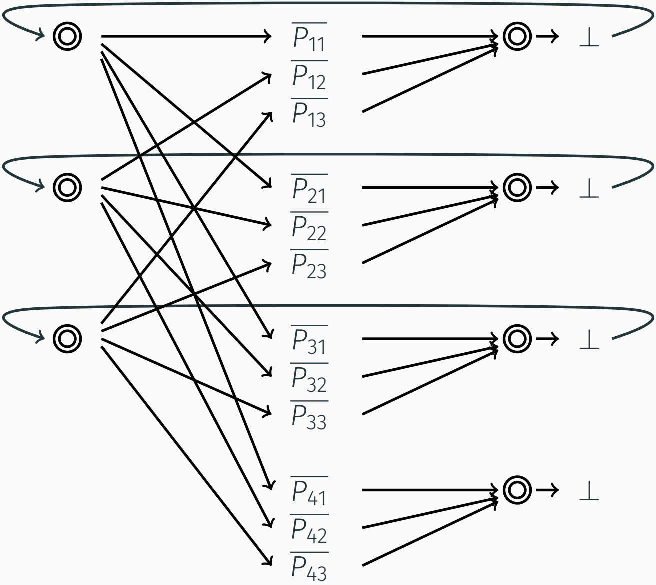
II. Strength of Circular Resolution

Poly-size circular resolution proof of PHP

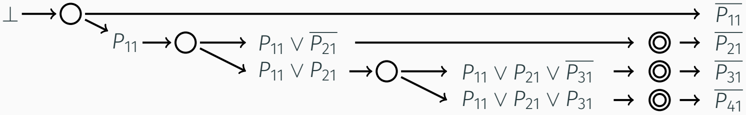
Theorem:

PHP_n^{n+1} has poly-size circular resolution refutations.

Circular proof of PHP_3^4



Weakening and cleaning for hole 1



Sherali-Adams proofs on Boolean variables

Variables: $X_1, \ldots, X_n$ and $\overline{X_1}, \ldots, \overline{X_n}$

Axioms:

$$X_i \geq 0 \qquad X_i^2 - X_i \geq 0 \qquad X_i + \overline{X_i} - 1 \geq 0$$
$$1 - X_i \geq 0 \qquad -X_i + X_i^2 \geq 0 \qquad 1 - X_i - \overline{X_i} \geq 0$$

Sherali-Adams proofs on Boolean variables

Variables: $X_1, \ldots, X_n$ and $\overline{X_1}, \ldots, \overline{X_n}$

Axioms:

$$\begin{array}{lll} X_i \geq 0 & X_i^2 - X_i \geq 0 & X_i + \overline{X_i} - 1 \geq 0 \\ 1 - X_i \geq 0 & -X_i + X_i^2 \geq 0 & 1 - X_i - \overline{X_i} \geq 0 \end{array}$$

SA Proofs: A refutation of $P_1 \geq 0, \ldots, P_m \geq 0$ (including the axioms) is a polynomial identity of the form

$$\sum_{j=1}^{m} P_j Q_j + Q_0 = -1 \qquad \text{where } Q_j = \sum_{j \in K} c_j^2 \prod_{i \in I_j} X_i \prod_{i \in J_j} \overline{X_i}.$$

Monomial size: number of monomials in $P_i Q_i$ and Q_0.

Resolution $<_p$ Sherali-Adams

Multiplicative encoding of clauses:

$$\bigvee_{i \in I} X_i \vee \bigvee_{i \in J} \overline{X_i} \quad \mapsto \quad -\prod_{i \in I} \overline{X_i} \prod_{j \in J} X_i \geq 0$$

Additive encoding of clauses:

$$\bigvee_{i \in I} X_i \vee \bigvee_{i \in J} \overline{X_i} \quad \mapsto \quad \sum_{i \in I} X_i + \sum_{j \in J} \overline{X_i} - 1 \geq 0$$

Strength comparison:

- Sherali-Adams refutes PHP easily
- Sherali-Adams efficiently simulates Resolution (see [Dantchev 2007])

Circular Resolution $\equiv_p$ Sherali-Adams

Theorem:

Circular Resolution $\equiv_p$ Sherali-Adams.
(for both multiplicative and additive encodings)

Proof of equivalence:

- $\leq_p$: extension of [Dantchev 2007, ALN16].
- $\geq_p$: a normal form result for Sherali-Adams proofs.

III. Conclusions

Take home message

1- Circular proofs are not always meaningless.

2- PHP has poly-size proofs in Circular Resolution.

3- Indeed Circular Resolution $\equiv_p$ Sherali-Adams.

Circular proofs in Frege

TreeLike Resolution	$<_p$	Resolution	$<_p$	Circular Resolution
TreeLike BD-Frege	$\equiv_p$	BD-Frege	$<_p$	Circular BD-Frege
TreeLike Frege	$\equiv_p$	Frege	$\equiv_p$	Circular Frege

Circular vs Dual Rail Resolution

[IMM-S, SAT 2017] Dual rail encoding for MaxSAT resolution

- stronger than resolution
- *circular Resolution efficiently simulates Dual Rail MaxSAT resolution refutations.* [Vinyals, 2018]

Thank you!