CIRCULAR (YET SOUND) PROOFS

Albert Atserias
Universitat Politècnica de Catalunya
Barcelona

Joint work with
Massimo Lauria

What is this talk about?

Tree Resolution

Regular Resolution

General Resolution

Circular Resolution

NEW!

exponentially stronger!

Inference rules

Standard rules:

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

Inference rules

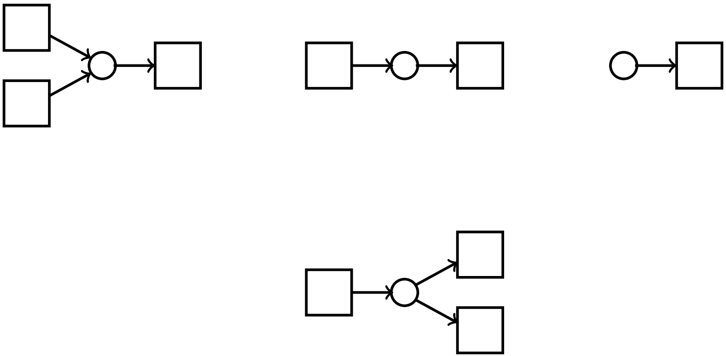
Standard rules:

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

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 proofs



Circular arguments

Want: $E, F \vdash A$

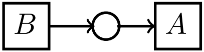
Circular arguments

Want: $E, F \vdash A$

$\boxed{A}$

Circular arguments

Want: $E, F \vdash A$

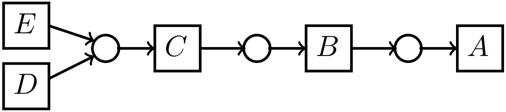


Circular arguments

Want: $E, F \vdash A$

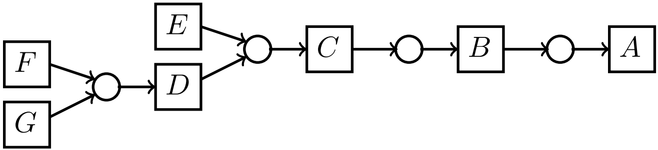
Circular arguments

Want: $E, F \vdash A$



Circular arguments

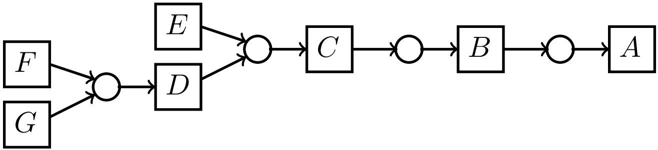
Want: $E, F \vdash A$



Circular arguments

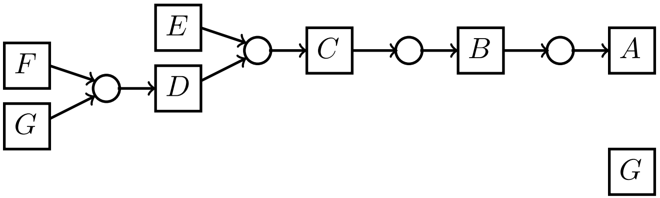
Want: $E, F \vdash A$

Subgoal: $E, F \vdash G$



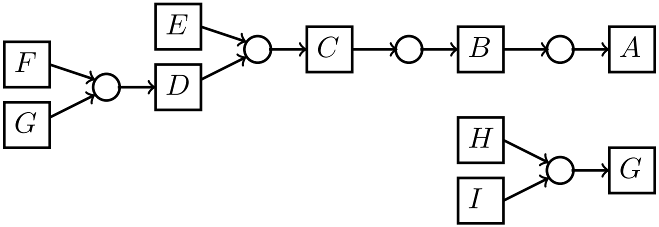
Circular arguments

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



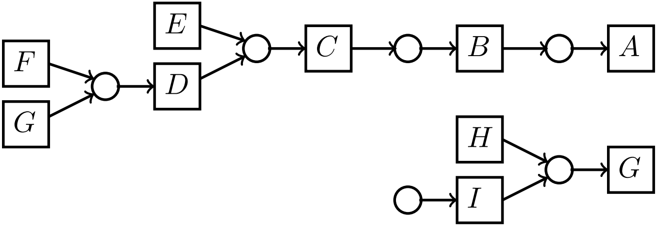
Circular arguments

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



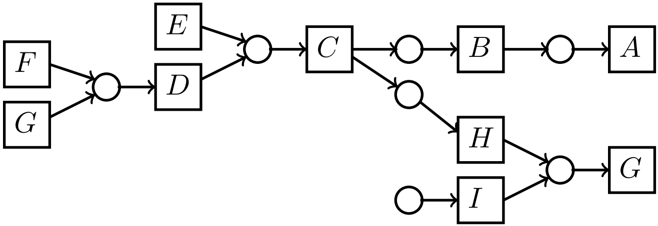
Circular arguments

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



Circular arguments

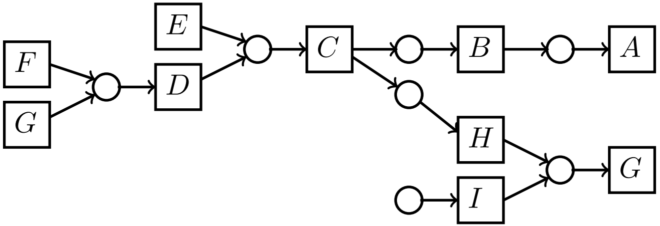
Want: $E, F \vdash A$
Subgoal: $E, F \vdash G$



Circular arguments

Want: $E, F \vdash A$

Subgoal: $E, F \vdash G$

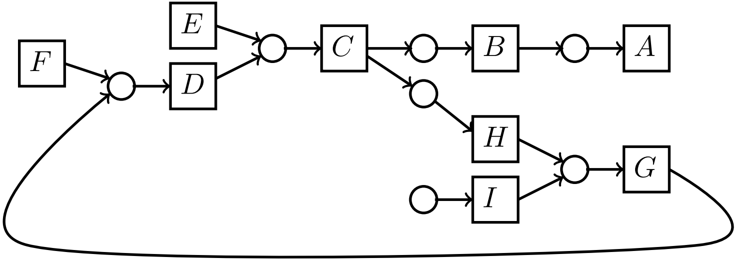


...???...

Circular arguments

Want: $E, F \vdash A$

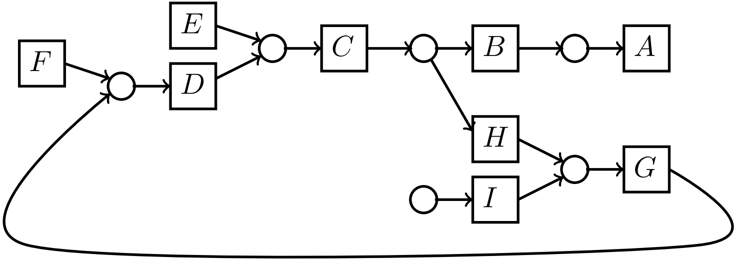
Subgoal: $E, F \vdash G$



...???...

Circular arguments

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



...???...

Circular Pre-proofs

Definition: A pre-proof is a pair (Π, B) where:

- Π is an ordinary proof $C_1, C_2, \ldots, C_m$,
- B is a set of backedges; i.e. pairs (i, j) s.t. $j < i$ and $C_j = C_i$.

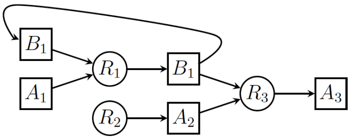
Circular Pre-proofs

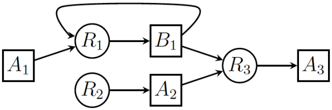
Definition: A pre-proof is a pair (Π, B) where:

- Π is an ordinary proof $C_1, C_2, \ldots, C_m$,
- B is a set of backedges; i.e. pairs (i, j) s.t. $j < i$ and $C_j = C_i$.

Example:

$$\Pi' : (\Pi = (B_1, A_1, B_1, A_2, A_3), B = \{(3, 1)\})$$





Some terminology and notation

$$\Pi' : ((C_1, C_2, \ldots, C_m), B)$$

Terminology and notation:

- $G(\Pi)$: the graph representation of Π.
- $N^+(u)$: the set of out-neighbours of u.
- $N^-(u)$: the set of in-neighbours of u.
- F: the set of formula vertices (the squares) of $G(\Pi)$.
- I: the set of inference vertices (the circles) of $G(\Pi)$.

Some terminology and notation

$$\Pi' : ((C_1, C_2, \ldots, C_m), B)$$

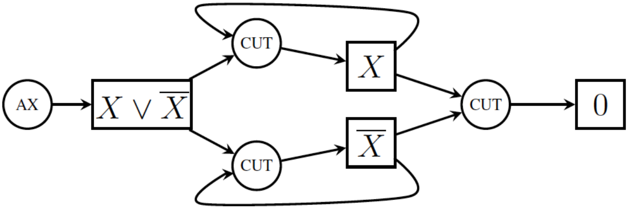
Terminology and notation:

- $G(\Pi)$: the graph representation of Π.
- $N^+(u)$: the set of out-neighbours of u.
- $N^-(u)$: the set of in-neighbours of u.
- F: the set of formula vertices (the squares) of $G(\Pi)$.
- I: the set of inference vertices (the circles) of $G(\Pi)$.

Observe:

- $u \in F$ implies $N^-(u) \subseteq I$ and $N^+(u) \subseteq I$.
- $u \in I$ implies $N^-(u) \subseteq F$ and $N^+(u) \subseteq F$.

Severe unsoundness of pre-proofs



Flow assignments and balance

$$\Pi' : ((C_1, C_2, \ldots, C_m), B)$$

More terminology and notation:

Flow assignments and balance

$$\Pi' : ((C_1, C_2, \ldots, C_m), B)$$

More terminology and notation:

- a flow assignment is a mapping $W : I \to \mathbb{R}^+$.

Flow assignments and balance

$$\Pi' : ((C_1, C_2, \ldots, C_m), B)$$

More terminology and notation:

- a flow assignment is a mapping $W : I \to \mathbb{R}^+$.

- $W^-(u) := \sum_{v \in N^-(u)} W(u)$ for $u \in F$; the in-flow of u.
- $W^+(u) := \sum_{v \in N^+(u)} W(u)$ for $u \in F$; the out-flow of u.
- $B(u) := W^-(u) - W^+(u)$ for $u \in F$; the balance of $u \in F$.

Flow assignments and balance

$$\Pi' : ((C_1, C_2, \ldots, C_m), B)$$

More terminology and notation:

- a flow assignment is a mapping $W : I \to \mathbb{R}^+$.

- $W^-(u) := \sum_{v \in N^-(u)} W(u)$ for $u \in F$; the in-flow of u.
- $W^+(u) := \sum_{v \in N^+(u)} W(u)$ for $u \in F$; the out-flow of u.
- $B(u) := W^-(u) - W^+(u)$ for $u \in F$; the balance of $u \in F$.

- if $B(u) < 0$, then C_u is called a hypothesis.
- if $B(u) > 0$, then C_u is called a conclusion.

Circular Proofs

Definition: A circular proof of A from $A_1, \ldots, A_m$ is a pre-proof for which there exists a flow-assignment such that, for each formula vertex $u \in F$, the following hold:

1. $B(u) < 0$ if $C_u \in \{A_1, \ldots, A_m\}$,
2. $B(u) \geq 0$ if $C_u \notin \{A_1, \ldots, A_m\}$,
3. $B(u) > 0$ if $C_u = A$.

Circular Proofs

Definition: A circular proof of A from $A_1, \ldots, A_m$ is a pre-proof for which there exists a flow-assignment such that, for each formula vertex $u \in F$, the following hold:

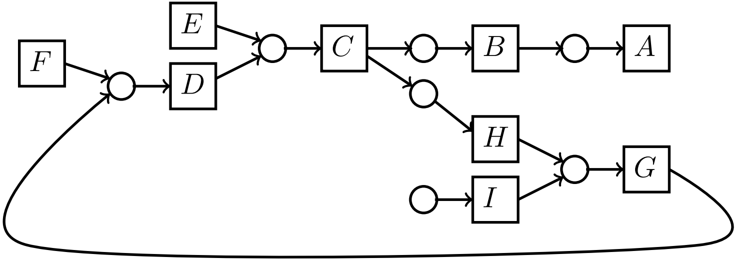
1. $B(u) < 0$ if $C_u \in \{A_1, \ldots, A_m\}$,
2. $B(u) \geq 0$ if $C_u \notin \{A_1, \ldots, A_m\}$,
3. $B(u) > 0$ if $C_u = A$.

Notes:

- efficient verification: linear programming techniques,
- weights may be assumed small rationals: by LP techniques,
- and even small integers: by flow techniques,

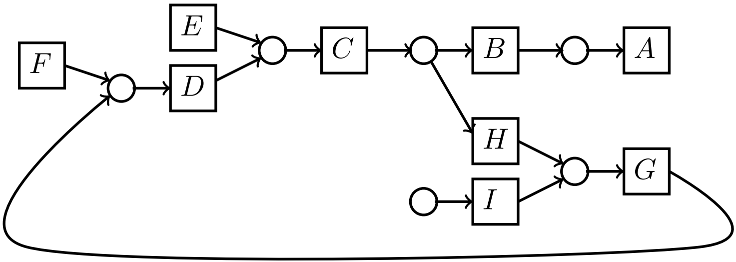
The examples again

Want: $E, F \vdash A$

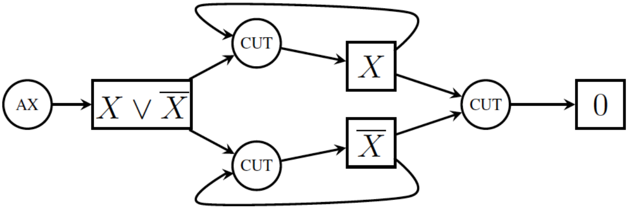


The examples again

Want: $E, F \vdash A$



The examples again

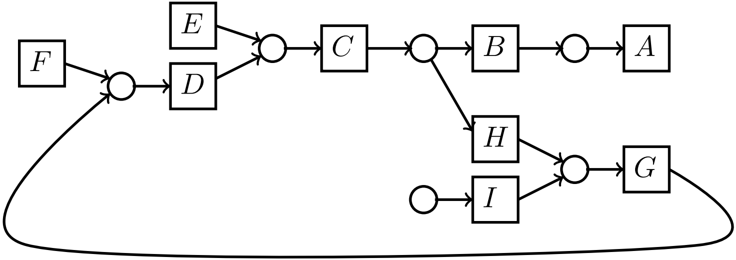


Soundness

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.

1st proof of soundness: by example

$$E, F \vdash A \quad \Longrightarrow \quad E, F \models A$$

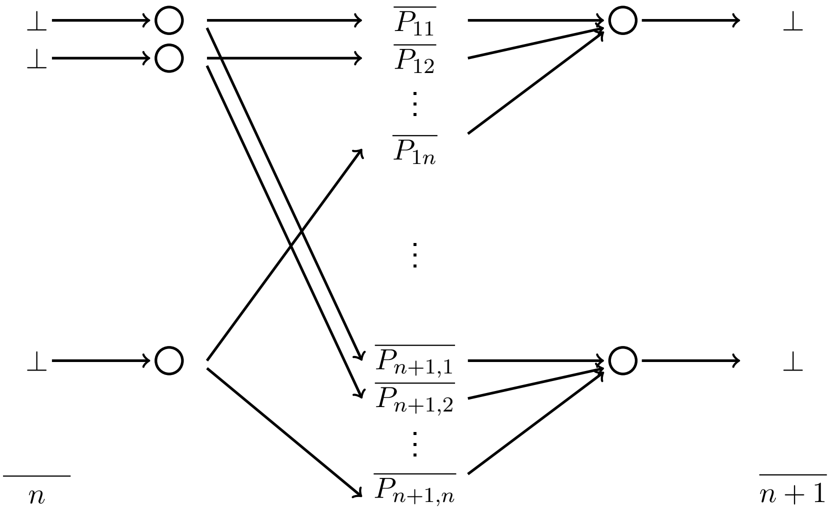


Poly-size circular resolution proof of PHP

Theorem:

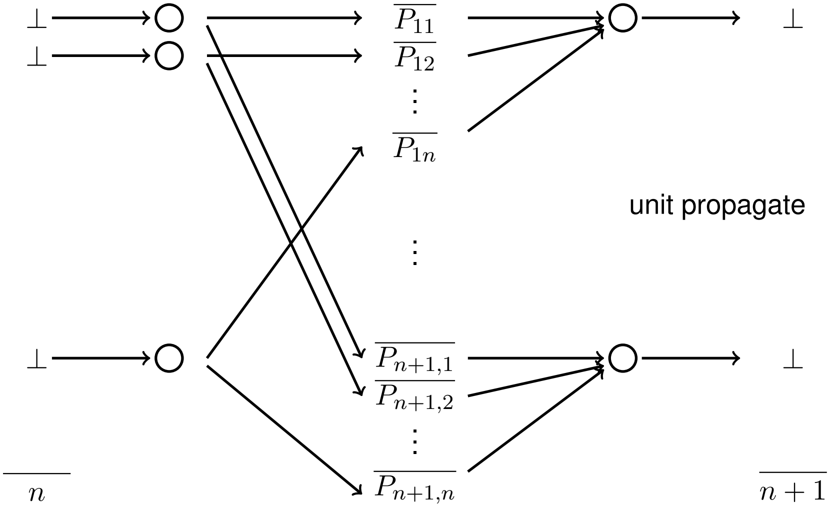
PHP_n^{n+1} has poly-size circular resolution refutations.

Proof of PHP



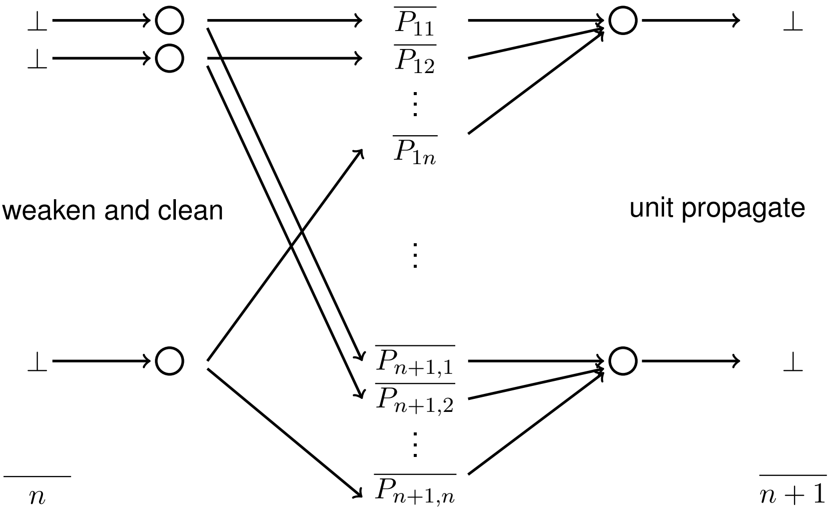
$\perp$
$\perp$
$\perp$
$\overline{P_{11}}$
$\overline{P_{12}}$
$\overline{P_{1n}}$
$\overline{P_{n+1,1}}$
$\overline{P_{n+1,2}}$
$\overline{P_{n+1,n}}$
$\perp$
$\perp$
$\overline{n}$
$\overline{n+1}$

Proof of PHP



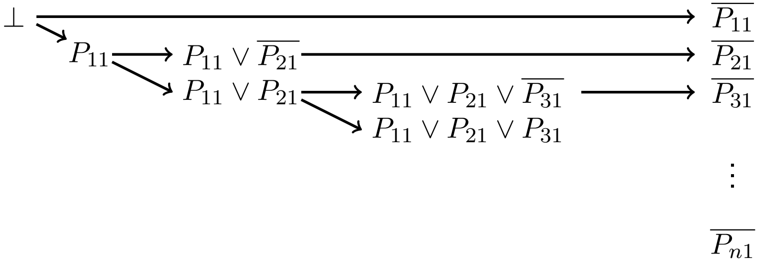
$\perp$
$\perp$
$\perp$
$\overline{P_{11}}$
$\overline{P_{12}}$
$\overline{P_{1n}}$
$\overline{P_{n+1,1}}$
$\overline{P_{n+1,2}}$
$\overline{P_{n+1,n}}$
$\perp$
$\perp$
unit propagate
$\overline{n}$
$\overline{n+1}$

Proof of PHP



⊥
⊥
⊥
$\overline{P_{11}}$
$\overline{P_{12}}$
$\overline{P_{1n}}$
$\overline{P_{n+1,1}}$
$\overline{P_{n+1,2}}$
$\overline{P_{n+1,n}}$
weaken and clean
unit propagate
⊥
⊥
$\overline{n}$
$\overline{n+1}$

Proof of PHP: weaken and clean for hole 1



Next question

WHAT IS CIRCULAR RESOLUTION?

Sherali-Adams proofs on Boolean variables

Variables:

$$X_1, \ldots, X_n \text{ and } \overline{X_1}, \ldots, \overline{X_n}$$

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

$$\sum_{j=1}^{m} P_j Q_j + Q_0 = -1$$

where each Q_i has the form

$$\sum_{j \in K} c_j^2 \prod_{i \in I_j} X_i \prod_{i \in J_j} \overline{X_i}.$$

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

Equivalence: Circular Resolution $\equiv$ 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:

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

Theorem:

Circular Resolution $\equiv_p$ Sherali-Adams.

(for both encodings)

Equivalence: Circular Resolution $\equiv$ 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:

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

Theorem:

Circular Resolution $\equiv_p$ Sherali-Adams.

(for both encodings)

Proof:

Equivalence: Circular Resolution $\equiv$ 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:

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

Theorem:

Circular Resolution $\equiv_p$ Sherali-Adams.

(for both encodings)

Proof:

$\leq_p$: essentially [Dantchev 2007] (reused in [ALN16]).

Equivalence: Circular Resolution $\equiv$ 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:

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

Theorem:

Circular Resolution $\equiv_p$ Sherali-Adams.

(for both encodings)

Proof:

$\leq_p$: essentially [Dantchev 2007] (reused in [ALN16]).

$\geq_p$: a normal form result for Sherali-Adams proofs.

2nd proof of soundness: via LP

Assume: α satisfies all the hypotheses.
Define: $Z_u = 1 - \alpha(C_u)$ for each $u \in F$.
Note:

$-Z_u \geq 0$	for each axiom vertex
$Z_u + Z_v - Z_w \geq 0$	for each cut vertex
$Z_u - Z_v - Z_w \geq 0$	for each weakening vertex

Therefore:

$$\sum_{v \in I} W(v) \left(\sum_{u \in N^-(v)} Z_u - \sum_{u \in N^+(v)} Z_u \right) \geq 0.$$

Equivalently:

$$-\sum_{u \in F} B(u) Z_u \geq 0$$

Proof of Circular Resolution $\leq_p$ Sherali-Adams

Define: $M_u =$ "multiplicative encoding of C_u" for each $u \in F$.
Note:

$$\begin{array}{rcll} M_u & = & -X\overline{X} & \text{for axiom } \vdash u \\ -M_u - M_v + M_w & = & (-X - \overline{X} + 1)M_w & \text{for cut } u, v \vdash w \\ -M_u + M_v + M_w & = & (-1 + X + \overline{X})M_u & \text{for weakening } u \vdash v, w \end{array}$$

Therefore:

$$\sum_{v \in I} W(v) \left(\sum_{u \in N^-(v)} M_u - \sum_{u \in N^+(v)} M_u \right) = -\sum_{u \in F} B(u) M_u$$

Now: Add positive multiples of

$$\prod_i X_i \prod_j \overline{X_j} = -M_u \qquad \text{for each } u \text{ s.t. } C_u \neq 0.$$

Get: $M_0 = -1$.

Take-home messages

1- Circular proofs are not always meaningless.

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

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

Acknowledgments

ERC-2014-CoG 648276 (AUTAR) EU.