CSE 599S Proof Complexity and its Applications

Lecture 12 9 Nov 2020

Clause	Algebraic $\mathbb{F}$	$\mathbb{R}$ Semi-algebraic
$C = x \vee \bar{y} \vee z$	$p_C = (1-x)y(1-z) = 0$	$\ell_C = x + (1-y) + z - 1 \geq 0$

Cutting Planes

$$\frac{\begin{array}{c} a_1x_1 + \cdots + a_nx_n \geq A \\ b_1x_1 + \cdots + b_nx_n \geq B \end{array}}{(a_1+b_1)x_1 + \cdots + (a_n+b_n)x_n \geq A+B}$$

$$\frac{a_1x_1 + \cdots + a_nx_n \geq A}{ca_1x_1 + \cdots + ca_nx_n \geq cA} \qquad c \geq 0$$

Division

$$\frac{ca_1x_1 + \cdots + ca_nx_n \geq A}{\therefore\ a_1x_1 + \cdots + a_nx_n \geq \lceil A/c \rceil} \qquad c > 0$$

Alt Division

$$\frac{a_1x_1 + \cdots + a_nx_n \geq A}{\lceil \frac{a_1}{c} \rceil x_1 + \cdots + \lceil \frac{a_n}{c} \rceil x_n \geq \lceil \frac{A}{c} \rceil} \qquad c > 0$$

$c\lceil \frac{a_i}{c} \rceil \geq a_i$

$x_i \geq 0$

$$\boxed{\underbrace{\left(c\lceil \tfrac{a_i}{c} \rceil - a_i\right)}_{\geq 0} x_i \geq 0}$$

Pseudo Boolean Solvers : Solvers that reason with inequalities in the style of DPLL/CDCL solvers

- Not all PB solvers implement cutting planes
  - some just convert to CNF
  - some just do cardinality constraints + clauses

$$x_1 + \cdots + x_n \geq k$$

  - often implement a different inference rule

Saturation
$$\frac{a_1 x_1 + \cdots + a_n x_n \geq A}{\min(a_1, A) x_1 + \cdots + \min(a_n, A) x_n \geq A}$$

Weakening
$$\frac{a_1 x_1 + \cdots + a_n x_n \geq A}{(a_1 - 1) x_1 + \cdots + a_n x_n \geq A - 1}$$

Analog of unit propagation:

$$\frac{a_1 x_1 + \cdots + a_n x_n \geq A \quad \text{and} \quad a_2 + \cdots + a_n < A}{x_1 = 1}$$

Translation: Dual vars x_i $\overline{x_i}$

Instead of $(1 - x_i)$ use $\overline{x_i}$

$0 \leq \overline{x_i} \leq 1$
$0 \leq x_i \leq 1$

$x_i + \overline{x_i} \geq 1$ — all +ve coeffs.

$(-x_i - \overline{x_i} \geq -1)$

No

$$\boxed{a_1 x_1 + a_1' \bar{x}_1} + a_2 x_u + \cdots + a_n x_n \geq A$$

$$2x_1 + 3\bar{x}_1 + \cdots \geq A$$

$$\boxed{x_1 + \bar{x}_1 = 1}$$

$$2 + \bar{x}_1 + \cdots \geq A$$

$$\Downarrow$$

$$\bar{x}_1 + \cdots \geq A - 2$$

---

eg. $C_1: \; 2x_1 + 2x_2 + 2x_3 + x_4 \geq 4$

$C_2: \; 2\bar{x}_1 + 2\bar{x}_2 + 2\bar{x}_3 \geq 3$

PB solver: Behaves like CDCL

Branches on truth assts

x_1: 0, 1

level 1

$C_2|_{x_1}: 2\bar{x}_2 + 2\bar{x}_3 \geq 1$

$$x_1 \xrightarrow{C_1} x_2 \rightarrow x_3 \xrightarrow{C_2} \bot$$

$C_1|_{x_1 \leftarrow 0}$

$$2x_2 + 2x_3 + x_4 \geq 4$$

$\therefore x_2 = 1$

$\therefore 2x_3 + x_4 \geq 2$

$x_3 = 1$

Learning new constraints on backtracks

Cancelling linear combinations

$$\boxed{2x_1} + 2x_2 + 2x_3 + x_4 \geq 4$$
$$\boxed{2\bar{x}_1} + 2\bar{x}_2 + 2\bar{x}_3 + \geq 3$$

$$a_1 x_i + L \geq A$$
$$b_1 \bar{x}_1 + L' \geq B$$

Choose c, d st $a_1 c = b_1 d$
$= \underline{\text{lcm}(a,b)}$

$$cL + dL' \geq cA + dB - \text{lcm}(a_1, b_1)$$

$$x_4 \geq 1$$

<u>not asserting</u>

Need to iterate constraint learning to get assertion constraints

Big Open question: Best method for learning constraints in PB solvers.

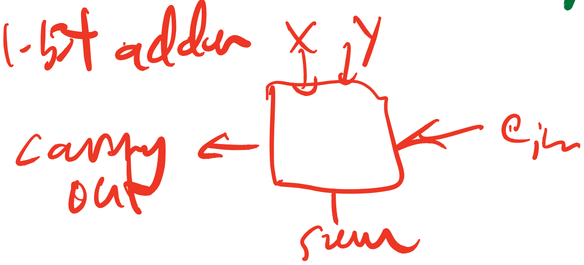
Sat4j
Saturation

RoundingSAT
special form of division
"round to 1"
or general division

Fact: If input is just a translation of clauses and all inferences involve cancelling linear combinations, then PB solvers act like CDCL solvers on original clauses

Better

e.g. 1-bit adder



$$\boxed{\begin{aligned} sum &= X \oplus Y \oplus C_{in} \\ C_{out} &= maj(X, Y, C_{in}) \end{aligned}}$$

Use $x + y + c_{in} = sum + 2c_{out}$

instead of clauses for

Polynomial inequalities over $\mathbb{R}$

01-programming:

$$x_i^2 - x_i = 0$$

Sherali-Adams : Linear programming

extending LP

Sum-of-squares (SoS) : Semi-definite programming

(Lasserre) (SDP)

$\boxed{\text{Both extend Nullstellensatz over } \mathbb{R}}$

Static Nsatz $f_1 = 0, \ldots, f_m = 0$

$$\sum_I g_i f_i = 1$$

Sherali-Adams

Input $h_1 \geq 0, \ldots, h_m \geq 0$; $f_1 = 0, \ldots, f_m = 0$

$F = C_1 \wedge \dots \wedge C_m$

e.g. Input: $(\ell_{C_1} \geq 0, \dots \ell_{C_m} \geq 0;\ )$

or $(;\ P_{C_1} = 0, \dots P_{C_m} = 0)$

SA Proof $\quad g_i$ polys "non-negative sums of juntas"

to derive $h \geq 0$, e_i polys

$$\underbrace{g_0 + \sum_{i=1}^{m} g_i h_i}_{\text{need}} + \sum e_i f_i \equiv_I h$$

degree of proof = $\max_i$ (deg$(g_i h_i)$, deg(g_0), deg$(e_i f_i)$)

non-neg junta

$\binom{n}{\leq d} 2^d \rightarrow \prod_{i \in P_i} x_i \prod_{j \in N_i} (1 - x_j) \geq 0$

each g_i is a sum of expressions with coefficients ≥ 0

Size = total # of monomials

bitsizes = total # of bits including coeffs.

<u>Prop</u>. Can convert $\mathcal{L}_C$ representation to P_C representation in deg $|C|$ and size $O(|C|^2)$.

- can convert P_C representation to $\mathcal{L}_C$ representation in deg $|C|$ and size $O(|C|^2)$

$h_i \geq 0$ $\quad -h_i \geq 0$ $\quad h_i = 0$

$e_i h_i$

<u>Cor</u> If F has an NSATZ proof of deg d over $\mathbb{R}$ and size S then F has an SA proof of degree d and size

$S + |F| \cdot w(F)$

SA proofs and LP

Vertex Cover

$$\min \sum_V x_v \le B$$

0/1-P

$$x_u + x_v \ge 1 \quad \text{for } (u,v) \in E$$

$$x_v \in \{0,1\} \quad \forall v$$

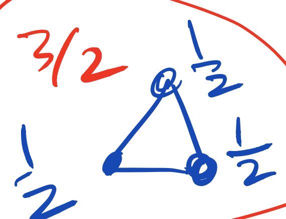
2

LP

$$\min \sum_V x_v$$

$$x_u + x_v \ge 1$$

$$0 \le x_v \le 1$$



add extra vars for each subset of vertices up to a certain size

$\iff$ non-negative juntas.

$X_{S,T}$

$x_u = 1 \ \forall u \in S$

$x_v = 0 \ \forall v \in T$

Finding SA proofs:

$2^d \binom{n}{\leq d}$ possible terms

coefficients,

equality to get h.

non-negativity to get

$A\vec{z}=b$ equality

$\vec{z}$ coefficients of $g_i e_i$

$z \geq 0$ for the coefficients of the term in the g_i

LP polytime solvable

$n^{O(d)}$ $d g$.