Algebraic PS. Nss

Translating CNF into polynomials.. C satisfied iff f has a root.

$C = x \vee y \vee \bar{z}$ $\qquad$ $f = (1-x)(1-y)z$

$\Gamma = \{C_i\}$ sat iff $F = \{f_i\}$ has a common root

use negated variables $\bar{x}_i = (1-x_i)$, o/w size blows up.

cf. "Power of negative reasoning".

doesn't matter for degree.

work modulo $\{x_i^2 = x_i,\ \bar{x}_i = 1 - x_i\}$.

draw 200.

Nullstellensatz proof.

s'p we have g_i st $\sum f_i g_i = 1$. then no common root.

$\{g_i\}$ are a Nss proof. sound and complete.

↳ by Hilbert's Nss

can sim tree-like res.

e.g. proof of Tseitin on $\mathbb{F}_2$.

if PC: CNF $\rightsquigarrow \sum x_e = \chi_v$. then $0 = \sum_v \sum_e x_e = \sum \chi_v = 1$.

e.g. $x_1 + x_2 + x_3 = 1 \equiv x_1 \vee x_2 \vee x_3 \wedge x_1 \vee \bar{x}_2 \vee \bar{x}_3 \wedge \bar{x}_1 \vee x_2 \vee \bar{x}_3 \wedge \bar{x}_1 \vee \bar{x}_2 \vee x_3 \equiv$

$\equiv \overline{x_1 x_2 x_3} \wedge \bar{x}_1 x_2 x_3 \wedge x_1 \bar{x}_2 x_3 \wedge x_1 x_2 \bar{x}_3 \equiv$

$\equiv x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + x_3 + 1 \ \wedge$

$x_1x_2x_3 + x_2x_3 \ \wedge$

$x_1x_2x_3 + x_1x_3 \ \wedge$

$x_1x_2x_3 + x_1x_2$.

sum, get

$x_1 + x_2 + x_3 + 1$.

$\bar{x}_1 x_2 x_3 + (x_1 + \bar{x}_1 + 1) x_2 x_3$

$x_1 \bar{x}_2 x_3 + (x_2 + \bar{x}_2 + 1) x_1 x_3$

$x_1 x_2 \bar{x}_3 + (x_3 + \bar{x}_3 + 1) x_1 x_2$

$\bar{x}_1 \bar{x}_2 \bar{x}_3 + (x_1 + \bar{x}_1 + 1)\, \overline{x_2 x_3} + (x_2 + \bar{x}_2 + 1)(x_1 \bar{x}_3 + \bar{x}_3)$

$+ (x_3 + \bar{x}_3 + 1)(x_1 x_2 + x_1 + x_2 + 1)$

Nullstellensatz can solve ofPHP.

PC. size – degree relation.

th proof size $s \to$ degree $k + O(\sqrt{n \log s})$. [CEI96, IPS99]

obs not the same refutation, exist formulas with poly size, deg c^{ε},

but deg $< c$ requires size $\exp(c^{\Omega(\varepsilon)})$ [LNSS20]

R operator. $\mathbb{F}[x_1 - x_n] \to \mathbb{F}[x_1 - x_n]$. [BGIP00, AR01]

$\to$ linear

$\to R(1) = 1$

$\to R(xm) = R(xR(m))$.

$\to R(\text{axiom}) = 0$

sp PC proof. induction. $R(\text{axiom}) = 0$.

$R(p+q) = R(p) + R(q) = 0$.

$R(xp) = R(x \cdot 0) = R(0) = 0$.

hence $R(1) = 0 \to$!!.

Tseitin: $\sum_{e \ni v} x_e = 1$. rewrite as $\prod_{e \ni v} y_e = -1 \leftarrow$ lb for this.

obs can write $y_e = 1 - 2x_e \iff x_e = (y_e - 1)/2$.

sp short proof of x version.

then derive x from y in same degree; done.

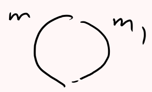
sp G expander, i.e. $|S| \le n/2 \to |\delta S| \geq \varepsilon |S|$ — unique boundary.

def $R(m) = (\min\ m'$ st $\exists S,\ |S| < n/2,\ \delta S = mm') \cdot (-1)^{|S|}$ — works for $d \le \varepsilon n/8$.

$\hookrightarrow$ deglex order.

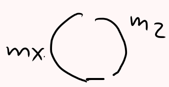
$R(1) = 1$: ok: — obs using $|S|$ small; o/w can take $S = V$.

$R(\text{axiom}) = R(m_v) + 1 = (-1)^1 + 1 = 0$ — $S = \{v\}$



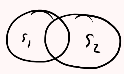
$R(m) = m_1 \rightsquigarrow$ witness S_1

$R(xm) = m_2 \rightsquigarrow$ witness S_2



$R(xm_1) = m_2$

$\hookrightarrow$ pick witness $S_1 \oplus S_2$.



has $\delta(S_1 \oplus S_2)$
$\quad\ \ ||$
$\quad x m_1 m_2$.

$\delta(S_1) = m m_1$

$\delta(S_2) = x m m_2$

$\delta(S_1 \oplus S_2) =$

$\delta(S_1) \oplus \delta(S_2)$

$= m m_1 \oplus x m m_2$

$= x m_1 m_2$.

and why not smaller?

b/c then $R(xm)$ would also be smaller.

and why is $S_1 \oplus S_2$ small?

b/c $\delta(S_1)$ is $\le 2d$ and $|S_1| \le n/2$, $|S_1| \le n/4$ actually.

Algebraic PS: semialgebraic.

Fix $\mathbb{F}=\mathbb{R}$.

sup write $\sum f_i g_i = 1 + h$ where $h \geq 0$. that's also a proof.

if h is $\sum \alpha_i$ monomial, we have SA.

if h is $\sum h_i^2$, we have SoS.

These are also degree-automatable.

Degree lower bounds exist

And we have size $\to$ degree relation. $\rightsquigarrow$ (wait, what about PHP)

Fun: SA $\equiv$ circular resolution

SA simulates resolution, but big coefficients required

SoS simulates PC, (but what about coeffs?).

Lower bounds for SA, SoS for e.g. random 3XOR, Tseitin

SA can prove PHP.

proof: pick h to be the following:

* $\{\overline{x_{ij}} \vee x_{ij+1} \vee \dots \vee x_{ik-1} \vee \overline{x_{ik}}\}$ for all i, for $1 \leq j < k \leq n$. // pigeon i into ≤ 1 hole
* $\{x_{1j} \vee \dots x_{nj}\}$ for all j // some pigeon goes to hole j
* $\{\overline{x_{ij}} \vee x_{i+1j} \vee \dots \vee x_{k-1j} \vee \overline{x_{kj}} \vee \overline{x_{\ell j}}\}$ for all j, for $1 \leq j < k < \ell \leq n+1$ // hole $j \leq 2$ pigeons.

ΔPHP

claim: $\sum \text{PHP} = 1 + \sum \Delta\text{PHP}$

intuition: $\sum$PHP is counting how many clauses are violated.

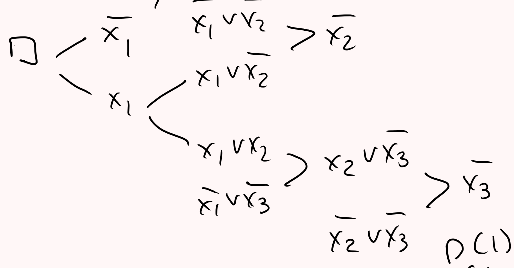
$\sum \Delta$PHP is the "residual" and takes care of all assignments that violate ≥ 2 clauses.

talk about GPHP

weighted resolution proof of PHP.

for each hole: axioms $+ \square \to \neg x_{ij}$ (see for $n=3$)

for each pigeon: axiom $+ \neg x_{ij} \to \square$ (clear)



talk about pseudoexpectations: $D(1)=1$, $D(f \cdot \text{axiom}) = 0$, $D(\text{monom}) \geq 0$

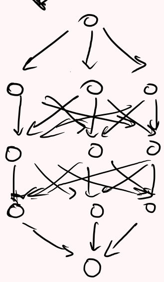
Algebraic PS : IPS

$\sum f_i g_i = 1$, but who says g_i must be expanded?
represent with algebraic ckts instead.
obs not Cook-Reckhow b/c we can't do PIT in P.

what we know:

-> exist some formula st IPS lbs imply lbs for permanent
(so VP $\neq$ VNP)
-> if VP $\neq$ VNP then exist some formula w/ IPS lbs.

-> unconditional lbs known for fragments of IPS
(which)
-> unconditional lbs recently proven for IPS where ckts are restricted to ro ABP (read-once, oblivious)
where inputs are CNFs.
[HLT 26]



edges : x poly in x_i
nodes : Σ incoming

proof is through feasible interpolation.
object we interpolate into is span program.

span program: have bunch of vectors, with a clause attached.
given input, evaluate clauses and pick vectors whose
clause is 1. if $1^m \in$ span (vectors), output 1.

span program stronger than comm cplex.