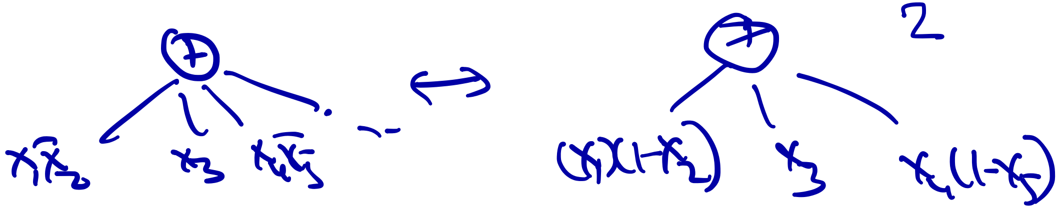
Today: Algebraic Proof Complexity

$AC_0[2]$ - Frege proofs

Razborov Smolensky : analogous result
in circuit complexity $\forall$ prime p, q $p \neq q$
mod p function $f(x_1 \dots x_n) = 1$ iff
$$\sum x_i \bmod p = 1$$
requires expl size $AC_0[q]$ circuits

2

'87



Hilbert's Nullstellensatz (weak version)

over some algebraically closed field $\mathbb{F}$

polynomials

$p_1(\bar{x}) = 0 \ldots p_m(\bar{x}) = 0$ are

unsolvable iff $\exists q_1(\bar{x}) \ldots \exists q_m(\bar{x})$ s.t.

$$\sum p_i(\bar{x})\, q_i(\bar{x}) = 1$$

identically ~~0~~ as a formal poly

proof of unsolvability of p_i's

$0 = 0$ ~~Ff~~

Our situation CNFs over $\{0,1\}$

$\underbrace{F = C_1 \wedge \ldots \wedge C_m}$ C_i: clause (3-clause)

$C_i = (x_1 \vee \bar{x}_2 \vee x_3) \rightsquigarrow p_i(\bar{x}) = 0$

$p_i: (1-x_1)(x_2)(1-x_3) = 0$ $\underbrace{x_i^2 - x_i = 0}$

Start with p_i's coming from 3CNF F
plus $\{x_i^2 - x_i = 0, \; i = 1 \ldots n\}$

$\mathbb{F}$ can be an ordinary field

HN's says F are unsolvable over $\{0,1\}$ iff

$\underbrace{\exists q_1 \ldots q_m}$ s.t. $\sum p_i q_i = 1$

$(x_1 \vee x_2)(\bar{x}_1)(\bar{x}_2) \qquad x_2 = 0$

$(1-x_1)(1-x_2)=0$

$x_1 = 0$

$x_2 = 0$

x_2

$1-x_2=0$

ϕ

$(1-x_1)(1-x_2)=0 \qquad x_1 = 0$

$(1-x_2)x_1 = 0$

$1-x_2=0 \qquad x_2=0$

$1=0$

Hilbert's Nullsatz Pf System over $\mathbb{F}$

$F = C_1 \ldots C_m$

$q_1 \ldots$

s.t $\sum q_i p_i = 1$

~~size~~

typical measure ~~of~~ max degree of q_i's

Can show degree is never more than n

(because $\underbrace{x_i^2 - x_i = 0}$)

Size = # of monomials altogether in all of the q_i's

Poly Calculus (PC)

Same pf system but you measure degree differently.

$(x_1)(\bar{x}_1 \vee x_2)(\bar{x}_2 \vee x_3) \ldots (\bar{x}_7 \vee x_8)(\bar{x}_8)$

$(1-x_2)(1-x_1) = 0$ $\quad (x_1)(1-x_2) = 0$ $\quad x_2(1-x_3) = 0$

$(1-x_3)(1-x_2) = 0$

$(1-x_3)(1-x_3) = 0$

$\ldots$

$(1-x_8) = 0$ $\quad x_8 = 0$

$1 = 0$

Nullsatz degree is linear

PC degree is $O(1)$

Really Nice Property of Nullsatz + PC

They are automatizable

If ~~$\mathcal{F}$~~ $F = C_1 \ldots C_m$ has a degree d
PC / Nullsatz refutation

there is an alg that finds it in
time $n^{O(d)}$

Clegg - Edmonds
Impagliazzo

Hilbert's System (Algebraic Proof System)

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

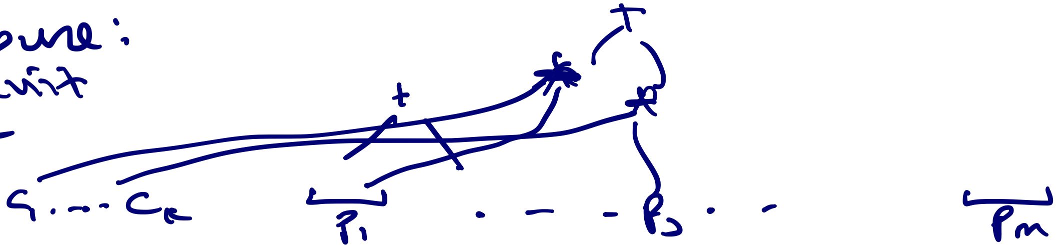
$\mathcal{P} = \{ p_i = 0$, includes $x_i^2 - x_i = 0 \}$

Hilbert Ref of $\mathcal{P}$ is a sequence of polynomials. Final poly $1 = 0$

1. $p_i = 0 \quad p_j = 0 \qquad \alpha_i p_i + \beta_i p_j = 0$

2. $p_i = 0 \quad (1 - x_i) p_i = 0 \quad x_i \cdot p_i = 0$

Measure: is circuit size



Hilbert's system can p-simulate EF

$\{P_1 \dots P_m\}$ $\quad q_1 \dots q_m$

Josh Grochow

Ideal Proof System

An IPS proof of $P_1=0, \dots, P_m=0$ is a algebraic circuit $C(\bar{x}, \bar{y})$ new vars $y_1 \dots y_m$

original vars in P_i's

s.t.

(1) $C(x_1 \dots x_n, \bar{0}) = 0$ final poly in Ideal generated by $P_1 \dots P_m$

(2) $C(x_1 \dots x_n, P_1 \dots P_m) = 1$

such a circuit really tells us $P_1 \dots P_m$ unsolvable

size: circuit size of C

Still can check ~~E~~ pf in rand. polytime

Theorem Hilbert + IPS are equivalent

(Forbes, Tzameret, Shpilka, Wigderson)

EF ~~IPS / Hilbert~~ can p-sim ~~EF~~ IPS / Hilbert

iff certain set of axioms

that define "polynomial identity testing"

have small EF proofs

$\boxed{\text{Thm}}$ superpoly LBs for IPS

imply VP ≠ VNP

algebraic P   algebraic NP

VP : a poly $(f_m)_{m=1}^{\infty}$ of formal polys with poly(n) variables of poly(n) degree and is computed by alg circuit (over $\mathbb{R}$) of poly size

<u>VNP</u> : class of polys g_n, g_n has poly(n) variables, poly(n) degree and

$$g_n(x_1 \ldots x_{poly(n)}) = \sum_{\bar{e} \in \{0,1\}^{poly(n)}} f_n(\bar{e}, \bar{x})$$

poly in VP

Thm LBs for IPS $\Rightarrow$ VP $\neq$ VNP

Pf let F be 3CNF

1. Let F be any UNSAT formula
then F has VNP - IPS pfs

$$g = \sum_{e \in \{0,1\}^r} f(e, \bar{y}, \bar{x})$$

$$\underbrace{C(\bar{x}, \bar{y})}$$

VNP-IPS

$$C(\bar{x}, \bar{y}, \ldots)$$

$$\sum_{e \in \{0,1\}^{p(n)}} \underbrace{f(\bar{x}, \bar{y}, \bar{e})}$$

2

Let $\overline{(f_n)}$ be UNSAT formulas s.t. we've shown expl LBs for IPS

Let $g_n(x,y)$ be VNP circuit

So g_n not in VP

Pf that any f_n has VNP-certificate

$(x_1 \vee x_2)(\bar{x}_1 \vee x_3 \vee x_4)(\bar{x}_2 \vee x_3)(\bar{x}_3)(\bar{x}_4)$

$\underset{c_1}{(1-x_1)(1-x_2)}$ $\quad \underset{c_2}{x_1(1-x_3)(1-x_4)}$ $\quad \underset{c_3}{x_2(1-x_3)}$ $\quad \underset{c_4}{x_3}$ $\quad \underset{c_5}{x_4}$

High level: $1 = x_1x_2x_3x_4 + x_1x_2x_3(1-x_4) + \ldots$ (*)

partition all ta's into $A_1 \ldots A_5$

A_1: falsify c_1 $\{0000, 0001, 0010, 0011\}$ $00**$

A_2: $1*00$ $\{1000, 1100\}$

A_3: $\{0100, 0101, 1101\}$

$\vdots$

rewrite * as

$1 = c_1 \cdot [(1-x_3)(1-x_4) + (1-x_3)x_4 + x_3(1-x_4) + x_3x_4] +$

Let $b(e,x) = ex + (1-e)(1-x)$

$1 - x_i = b(0, x_i)$

$x_i = b_i(1, x_i)$

the previous equality can be rewritten as

$$1 = c_1 \Big[\sum_{e \in A_1} \prod_{\substack{j : x_j \text{ not} \\ \text{in clause } 1}} b(e_j, x_j) \Big] +$$

$$c_2 \Big[\sum_{e \in A_2} \prod_{\substack{j : x_j \\ \text{not in} \\ \text{clause } 2}} b(e_j, x_j) \Big] + \cdots \; c_5 [\quad]$$

$$= \sum_{i=1}^{m} c_i \Big[\sum_{e \in \{0,1\}^n} \underbrace{c(\bar{e}) \prod_{j<i} (1 - c_j(\bar{e}))} \prod_{\substack{j : x_j \text{ not} \\ \text{in clause } i}} b(e_j, x_j)$$

$$= \sum_{e \in \{0,1\}^n} \sum_{i=1}^{m} \underbrace{e_i}_{y_i} \underbrace{c_i(\bar{e}) \Big(\prod_{j<i} (1 - c_j(\bar{e})) \Big)} \prod_{\substack{j : x_j \text{ not} \\ \text{in clause } i}} b(e_j, x_j)$$