Thm (Sokolov) $PC^{\pm}_{\mathbb{F}}$ over any field $char(\mathbb{F}) \neq 2$ 0

Polynomial Calculus over $\{\pm 1\}$-variables requires size $2^{\Omega(n)}$ to refute PHP^m_n.

Also proves a lifting result (Maj^5) and proves the above for random CNFs and other CSPs...

↳ "isolation property"

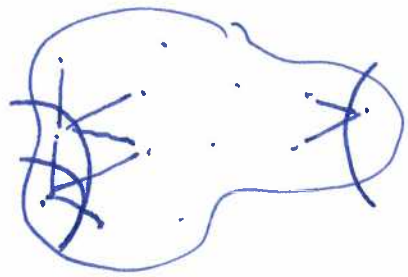
(1) . Tseitin (size) easy for $PC^{\pm}_{\mathbb{F}}$:

an XOR is efficiently represented as $\prod_{i=1}^{n} x_i = -1$.

$\Updownarrow$

odd # of vars is set to -1.

$\rightarrow$ In a graph we can maintain the parity of a cut:



$\rightarrow$ in $O(n)$ steps we are done.

· However we still require large degree.

$\Longrightarrow$ Cannot hope for a degree-size tradeoff for $PC^{+-}_{\mathbb{F}}$.

---

(2) · A restriction of 0/1 variables is useful as it makes monomials $\prod_{i\in A} x_i \prod_{i\in B} \bar{x}_i$ disappear.

· What happens with ± 1 variables?

$$\prod_{i\in A} x_i \prod_{i\in B} (-x_i) = (-1)^{|B|} \cdot \prod_{i\in A\cup B} x_i$$

the monomial will simply change the sign.

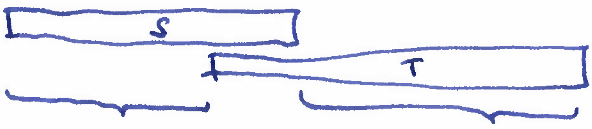
---

(3) · Suppose we have some multilinear polynomial f. $\leftarrow$ everything multilinear going forward

Boolean setting	±-setting
$\deg(f) \le \deg(\underset{\uparrow \text{multilin.}}{x f}) \le \deg(f)+1$	$\deg(f)-1 \le \deg(x\cdot f) \le \deg(f)+1$ $+\ f = x^2 \cdot f$
$\rightsquigarrow$ "stable" invariant	$\rightsquigarrow$ "brittle" invariant

To fix 3 we will introduce a different measure than degree: the diameter of a multilinear polynomial:

$$\mathrm{diam}(p) = \max_{\substack{S,T \in \mathrm{mon}(p) \\ S,T \subseteq [n]}} |S \oplus T| .$$



$\rightsquigarrow$ in some sense a notion of degree <u>stable</u> under multiplication by variables.

$\mathrm{diam}(p) \le 2 \cdot \deg(p)$.

$\mathrm{diam}(\pi) = \max_{p \in \pi} \mathrm{diam}(p)$

<u>Lemma 1</u>: If there is a $PC^{+-}_{\mathbb{F}}$ refutation π of F, then there is a $PC^{+-}_{\mathbb{F}}$ refutation π' of F of degree $(\pi') \leq 2 \cdot \max(\mathrm{diam}(\pi), \deg(F))$.

<u>Def</u>: Let $[p]$ denote all polys $q = z_S \cdot p$ for $S \in \mathrm{mon}(p)$

$\Leftrightarrow$ q "sets" the monomial S to 1.

<u>Claims</u>: (1) $\deg(q) \leq \cancel{\deg(p)}\ \mathrm{diam}(p)$

$\cdot \deg(q) \leq \max\limits_{S,T} |S \oplus T| = \mathrm{diam}(p)$.

(2) $\mathrm{diam}(q) = \mathrm{diam}(p)$

$$\cdot\ \mathrm{diam}(q) = \max_{T,T' \in \mathrm{mon}(p)} |(S \oplus T) \oplus (S \oplus T')|$$
$$= \max_{T,T' \in \mathrm{mon}(p)} |T \oplus T'| = \mathrm{diam}(p)$$

(3) for <u>any</u> $S \subseteq [n]$: $[z_S \cdot p] = [p]$

$q \in [z_S \cdot p]$ $\quad q = z_{S'} \cdot z_S \cdot p$ $\quad S' \in \mathrm{mon}(z_S \cdot p)$.

$\rightarrow S' \oplus S = T$

$T \in \mathrm{mon}(p)$

$\longrightarrow q = z_T \cdot p$

$q \in [p]$.

(4) there is a $PC^{+-}_{\mathbb{F}}$ derivation of q from p of degree $2 \cdot \deg(p)$. ~~+ diam(p)~~.

<u>Proof of L1:</u>

- $\pi = (f_1, \dots, f_T)$.
- $\pi' = (f_1', \dots, f_T')$ for $f_i' \in [f_i]$

(1) If f_i is an axiom, then $f_i' \in [f_i]$ can be derived in $2 \cdot dg(f_i)$.

(2) $f_i = z_k \cdot f_j \longrightarrow [f_i] = [f_j]$.

- $f_i' = z_R \cdot f_j$ for $R \in mon(f_j)$
- $f_j' = z_S \cdot f_j$ for $S \in mon(f_j)$

$$f_i' = z_R f_j = z_{R \ominus S} \cdot z_S \cdot f_j = z_{R \ominus S} f_j'$$

Since $diam(f_j) \le diam(\pi)$:

- $dg(z_{R \ominus S}) \le diam(\pi)$.
- $dg(f_j') \le diam(\pi)$.

(3) $f_i = a \cdot f_j + b \cdot f_{j'}$

- $f_i' = z_R \cdot f_i$ $\quad R \in mon(f_i)$
- $f_j' = z_S \cdot f_j$ $\quad S \in mon(f_j)$
- $f_{j'}' = z_T f_{j'}$ $\quad T \in mon(f_{j'})$

(i) $Mon(f_j)$ is disjoint of $mon(f_{j'})$

$\rightarrow mon(f_i) = mon(f_j) \,\dot\cup\, mon(f_{j'})$

$$f_i' = z_R \cdot f_i = a \cdot z_{R \ominus S} \cdot z_S f_j + b \cdot z_{R \ominus T} \cdot z_T \cdot f_{j'}$$

$$= a \cdot z_{R \ominus S} f_j' + b \cdot z_{R \ominus T} f_{j'}'.$$

(ii) $U \in mon(f_j) \cap mon(f_{j'})$.

all of low degree. $\le diam(\pi)$.

$$\begin{cases} \text{Derive} \quad p = z_{U \ominus S} f_j' = z_U \cdot f_j \\ \qquad\qquad\; q = z_{U \ominus T} f_{j'}' = z_U \cdot f_{j'} \\ \rightsquigarrow r = a \cdot p + b \cdot q = z_U (a f_j + b \cdot f_{j'}) = z_U \cdot f_i \end{cases}$$

W.l.o.g. suppose that $R \in \mathrm{mon}(f_j)$.

$$\mathrm{diam}(f_j) \le d \rightarrow |R \oplus U| \le d.$$

$$f_i' = z_R \cdot f_i = z_{R \oplus U} \cdot z_U \cdot f_i = z_{R \oplus U} \cdot r \quad \boxtimes$$

What remains?

Argue that a <u>small</u> $PC^{+-}_{\mathbb{F}}$ refutation may be turned into a low diameter refutation.

$$W(\pi, D) := \{ A \subseteq [n] \mid A = R \oplus S \text{ for } R, S \in \mathrm{mon}(f_i) \text{ with } f_i \in \pi \text{ and } |A| \ge D \}$$

be the set of <u>wide</u> symmetric differences in π.

<u>Thm:</u> given a $PC^{+-}_{\mathbb{F}}$ refutation π of PHP^m_n, then there is a $PC^{+-}_{\mathbb{F}}$ refutation π' of PHP^{m-1}_{n-2} such that

$$|W(\pi', D)| \le (1 - D/n)\,|W(\pi, D)|.$$

By repeating the above $\varepsilon \cdot n$ times, we get that the final refutation π^* satisfies

$$|W(\pi^*, D)| \le (1 - D/n)^{\varepsilon \cdot n}\,|W(\pi, D)|$$

$$\le \exp(-\varepsilon \cdot D) \cdot |W(\pi, D)|.$$

$\rightarrow$ If $|W(\pi, D)| < \exp(\varepsilon \cdot D)$, then $|W(\pi^*, D)| = \emptyset$;

$\mathrm{diam}(\pi^*) \le D$.

By previous lemma $\exists\, \pi^{*\prime}$:

$\deg(\pi^{*\prime}) \le 2D$.

For $D = n/8$ this contradicts the PHP deg l.b..

Proof of Thm:

intuition: $\Pi' = \Pi|_{x \leftarrow 1} + \Pi|_{x \leftarrow -1}$

is hopefully a "proof" and monomials cancel if they contain x.

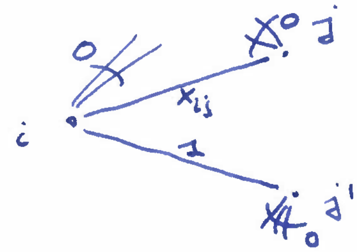
① isolate x so that we can "set" it to ± 1, without affecting the hardness of the formula

② argue that we maintain a valid refutation.

Choose $\cancel{i \in [n]}$ $(i,j) \in [m] \times [n]$ that appears most frequent in $\omega(\Pi, D)$. Since each set $A \in \omega(\Pi, D)$ is of size $|A| \geq D$, we have that i occurs in at least a D/n fraction of $\omega(\Pi, D)$. We want to make these disappear.

① $\cancel{x_i = x}$

$x_{(i,j)}$



let ρ: 1) pick $j' \neq j$.

2) set $x_{(i,j')} = 1$

3) set $x_{(i,j'')} = 0$ for $j'' \neq j, j'$

4) set $x_{i',j} = x_{i',j'} = 0$ for $i' \neq i$.

→ this "isolates x_{ij}": all axioms touched by x_{ij} are satisfied, no matter the value assigned to x_{ij}.

Consider $\Pi|_\rho$: it still contains terms with x_{ij}.

<u>Claim</u>: we can "remove" all these sym-differences: ~~those terms, the proof~~

for $f_t|_\rho \in \Pi|_\rho$ write $f_t|_\rho = x_{ij} \cdot p_{t,1} + p_{t,0}$

$$f_t|_\rho = x_{ij} \cdot p_{t,1} + p_{t,0}$$

Replace $f_t|_\rho$ by two lines $p_{t,1}$ and $p_{t,0}$

$\to$ gives Π'.

- $f_t|_\rho = p_{t,0}$ and $p_{t,1} = 0$ for all axioms.
  aka the axioms are satisfied <u>indep</u> of x_{ij}.
- If $f_t|_\rho = x_{i'j'} \cdot f_{t'}|_\rho$, then $p_{t,b} = x_{i'j'} \cdot p_{t',b}$.
- If $f_t|_\rho = x_{ij} f_{t'}|_\rho$, then $p_{t,b} = p_{t',\bar{b}}$
- If $f_t|_\rho = a \cdot f_{t'}|_\rho + b \cdot f_{t''}|_\rho$, then

$$p_{t,b} = a \cdot p_{t',b} + b \cdot p_{t'',b}.$$

- $p_{T,0} = 1$.

The symmetric difference of monomials in Π' are those of $\Pi|_\rho$ that do not contain the variable x_{ij}.

$\Rightarrow |W(\Pi', D)| \leq (1 - D/n) |W(\Pi, D)|$.