CSE 5995 Proof Complexity & Applications

Lecture 9 28 October 2020

Last time:

Gaussian Proofs: inference on linear equations

$\mathcal{L}$ given

1. $x_1 + 2x_2 - x_3 = 1$
2. $x_2 + x_3 = 0$
3. $x_1 - 3x_2 = 1$
4. $x_2 = 5$

5. $x_1 + 3x_2 = 1$ 1+2

6. $x_1 = 1$ $\frac{1}{2}3 + \frac{1}{2}5$

7. $x_2 = 2/3$ $-\frac{1}{3}3 + 1\,6$

8. $0 = 1$ $4 - \cancel{6}\ 7$

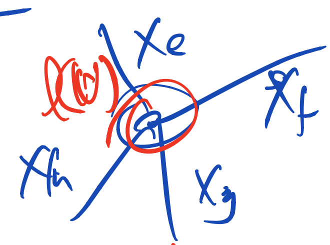
width = max # vars per line

Gaussian Width $w_G(\mathcal{L})$ max # of vars need per line

minimal width Gaussian proofs

Tseitin formulas

parity at $\oplus$ of



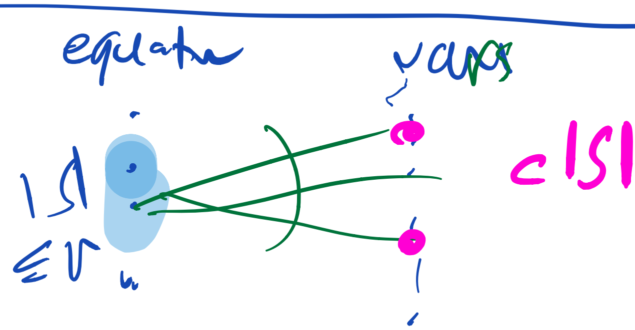
$$x_e + x_f + x_g + x_h \equiv \ell(v) \bmod 2$$

$$\sum_{e \ni v} x_e \equiv \ell(v) \bmod 2$$

linear equation over $\mathbb{F}_2$

E_v for each $v \in G$

$G_{\mathcal{L}}$



Thm If $G_{\mathcal{L}}$ is an (r,c)-boundary expander then $w_G(\mathcal{L}) > \frac{rc}{2}$

Also If G is an (r,c)-edge expander then $\mathcal{L} =$ Tseitin on G. is an (r,c)-boundary expander

---

PC lower bounds using Gaussian width over $\mathbb{F}_2$

Size-degree relationship

$\exists$ enough to prove degree lower bounds

$\boxed{\text{Today}}$ Assume we are doing PC proofs <u>not</u> over $\mathbb{F}_2$

$\mathrm{char}(\mathbb{F}) \neq 2$

$\Rightarrow +1 \neq -1$

x vars $\Rightarrow$ z vars

$0, 1 \qquad 1, -1$

$b \Rightarrow (-1)^b$

$0 \mapsto 1$

$1 \mapsto -1$

$x_1 \mapsto z_1 = (-1)^{x_1}$

$x_2 \mapsto z_2 = (-1)^{x_2}$

$(x_1 + x_2) \bmod 2 \mapsto (-1)^{(x_1+x_2) \bmod 2}$

$= (-1)^{x_1+x_2}$

$= z_1 \cdot z_2$

$PC^{\pm}_{\mathbb{F}}$ proofs

1, -1 $\quad z^2 - 1 = 0$

multilinear

0, 1 $\quad x^2 - x = 0$

multilinear

old

PC $\qquad\qquad PC^{\pm}$

$x_e \longmapsto z_e$

$2^{d(v)-1}$ clauses

$\sum_{e \ni v} x_e \equiv b \bmod 2 \longmapsto \prod_{e \ni v} z_e = (-1)^b$

$\Downarrow$

$2^{d(v)-1}$ equations

PC

concise

(*) Claim: Degree of $PC^{\pm}$ proofs $=$ Degree of PC proofs

Proof

$\phi: x \longmapsto z$

$b \longmapsto (-1)^b \qquad b \in \{0,1\}$

Claim: ϕ is a linear map (invertible)

$z = 1 - \frac{x}{2}$

$0 \longmapsto 1$

$1 \longmapsto -1$

$\phi(b) = 1 - 2b$

$\phi^{-1}(c) = \frac{1-c}{2} \qquad c \in \{+1,-1\}$

$\phi(x^2 - x) = \frac{z^2 - 1}{4}$

PC proof $\qquad\qquad$ $PC^{\pm}$ proof

$P \xmapsto{\ \phi\ } \phi(P)$ $\qquad$ preserves degree

$P_c \qquad\qquad P'_c$

$C = x_1 \vee \bar{x}_2 \vee x_3 \longmapsto \left(\frac{1+z_1}{2}\right)\left(\frac{1-z_2}{2}\right)\left(\frac{1+z_3}{2}\right)$

$\Downarrow$

$(1-x_1)x_2(1-x_3) \xmapsto{\ \phi\ }$

Lemma: mod 2 equations $\Longleftrightarrow$ binomial poly over ± 1 with ± 1 coeffs.

width 5: $x_1 + x_2 + x_3 \equiv 1 + x_4 + x_5 \mod 2$

$(-1)^{x_1+x_2+x_3} = -1 \cdot (-1)^{x_4+x_5}$

$$z_5 z_4 (z_1 z_2 z_3 + z_4 z_5)$$
$$= z_5 (z_1 z_2 z_3 z_4 + z_5)$$
$$= \underline{z_1 z_2 z_3 z_4 z_5 + 1}$$

$$z_1 z_2 z_3 = -1 \cdot z_4 \cdot z_5$$
$$\Downarrow$$
$$\rightarrow \quad z_1 z_2 z_3 + z_4 z_5 = 0$$

deg 3

2 terms.

Thm $PC^{\pm}$ proofs with binomial input polys.

only require binomial polys (except for monomials at end)

$$z_1 z_2 z_3 \xrightarrow[\times z_1]{} z_2 z_3 \xrightarrow[\times z_2]{} z_3 \xrightarrow[\times z_3]{} \underline{1}$$

Proof V_d vector space of polys of degree $\le d$ in z_i vars

$\binom{n}{\le d}$ monomials

binomials: $0\ 0\ 1\ 0\ 0 \cdots 0\ \pm 1\ 0\ 0\ 0\ 0$ vector of coefficients

Basis B_d for V_d

$\binom{n}{\le d}$

- add an input poly ← binomial
- take linear combination to get a basis so far

Provided degree $\le d$
- take all polys p in basis and add $x_i \cdot p$ (shifted version of p) still binomial
- take linear combos for a basis

Gaussian Elimination

pivot row →

→

1 cause		±1	
1	±1		
−1			1

binomial

1	−1
−1	−1

← monomial

monomial

Cor If we start a $PC^{\pm}$ proof with translation of mod 2 equations, every line can be viewed as a mod 2 equation (except the last part with monomials)

refuting $\mathcal{L}$ system of mod 2 equations

$\text{mon}_1 = \pm \text{ mod } 2$

deg in $PC^{\pm}$ — width in Gaussian proof

$PC^{\pm}$ size — Gaussian size

Vars split between 2 monomials

Degree $\geq \left\lceil \frac{w_G(\mathcal{L})}{2} \right\rceil$

$w_G(\mathcal{L})$

Cor If G is an $(\alpha n, c)$-edge-expander on n vertices of constant degree (4)

then $TS(G, \ell)$ requires $PC^{\pm}$ degree $\Omega(n)$.

$w_G(\mathcal{L}_{TS(\,)}) > \frac{nc}{2}$

PC, PCR degree $= PC^{\pm}$ deg.

$deg \geq w_G(\mathcal{L}_{TS})/2$

$\geq \boxed{\frac{\alpha n c}{4}}$ which is $\Omega(n)$

Cor $TS(G, \ell)$ require PC, PCR proofs of size $2^{\Omega(n)}$

$2^{\frac{(deg)^2}{\sqrt{n}}}$

size deg relationship

Note: need one more thing

PC assumed clause form.

binomial proof assume parity

$PC^{\pm}$ equation form.

Fact: easy conversion between

P^{1}_{C} 2^{d-1} clauses deg d $\Longleftrightarrow$ parity form degree d

$\mathrm{char}(\mathbb{F}) \neq 2$

Reduce to CNF formulas

Idea: F $\qquad$ $F^{augment}$

$x_1 \vee \bar{x}_2 \vee x_3 \longmapsto x_1 + x_2 + x_3 \equiv 0 \pmod 2$ $\quad 1-b$

falsified by

$\begin{matrix} 0 & 1 & 0 \\ x_1 & x_2 & x \end{matrix}$

total parity

$b=1$

add $2^{k-1}-1$ new clauses to represent above parity constraint

$F^{augment}$ is at least as easy to refute as F

$G_{F^{augment}}$ has same expansion properties as G_F does.

G_F is an (an, c)-boundary expander w.h.p.

$\Rightarrow$ $W_G(\mathcal{L}_{F^{\text{augment}}})$ is $\Omega(n)$

$\Rightarrow$ PC$^{\pm}$ degree F^{augment} is $\Omega(n)$

$\Rightarrow$ PC degree $F^{\text{aug.}}$ is $\Omega(n)$

$\Rightarrow$ PCR degree F is $\Omega(n)$

$\Rightarrow$ PC, PCR size of F is $2^{\Omega(n)}$ w.h.p.

This method does not work for PHP^m_n

- can we explicit computation of basis B_d for V_d to get degree $\geq \lceil \frac{n}{2} \rceil$ + random restrictions get $2^{\Omega(n)}$ size l.b.s