Bounds for Polynomial Calculus

Jori Dubrovin

Presentation Outline

- Polynomial calculus in Boolean basis for CNF.
- Polynomial calculus in Fourier basis.
- Gaussian calculus for linear equations (XOR).
- Relationships of the above.
- Degree lower bound for polynomial calculus using expansive linear equation systems.

Polynomial Calculus

- Translate formulas to polynomials in $F[\mathbf{x}]$.
- Inference rules:

$$\frac{p(\mathbf{x}) = 0}{x_i p(\mathbf{x}) = 0} \qquad \frac{p_1(\mathbf{x}) = 0 \quad p_2(\mathbf{x}) = 0}{a_1 p_1(\mathbf{x}) + a_2 p_2(\mathbf{x}) = 0}$$

- If $P \subseteq F[\mathbf{x}]$ is a set of polynomials with no common zero point, then a **PC refutation** is a derivation of $1 = 0$ from P.
- The **degree** of a refutation is the *maximal* degree of a polynomial.
- $\deg(P) :=$ minimal degree of a refutation of P.

Gaussian Calculus over GF(2)

- Translate xor formulas to linear equations.
- Inference rule:

$$\frac{\sum_{i\in S} x_i + a = 0 \qquad \sum_{i\in T} x_i + b = 0}{\sum_{i\in S} x_i + a + \sum_{i\in T} x_i + b = 0}$$

- If L is an unsatisfiable system of linear equations, then a **GC refutation** is a derivation of $1 = 0$ from L.
- The **width** of a refutation is the *maximal* number of variables in an equation.
- $w_G(L) :=$ minimal width of a refutation of L.

Where Are We Going To?

- Resolution refutation of width w

  $$\Rightarrow$$

  PC refutation of degree $\leq 2w$
- Some CNF problems that are hard for resolution are also hard for polynomial calculus in Boolean basis.

Binomial Calculus

- Restriction of polynomial calculus to binomials.
- Theorem 5.5.13. If a set of binomials P has a PC refutation of degree d, it also has a BC refutation of degree d.
- Correspondence (not one-to-one) between linear equations over GF(2) and binomials in Fourier basis with coefficients in $\{-1, 1\}$.

Binomial Degree vs. Gaussian Width

- If l is a linear equation $x_{i_1} + \cdots + x_{i_k} + a = 0$, its balanced Fourier representation is

$$P_F(l) = \prod_{r=1}^{\lfloor k/2 \rfloor} y_{i_r} + (-1)^{1-a} \prod_{r=\lfloor k/2 \rfloor + 1}^{k} y_{i_r}.$$

- Corollary 5.5.5. Let L be a minimal unsatisfiable set of linear equations of width at most k. Then

$$\frac{w_G(L)}{2} \leq \deg(P_F(L)) \leq \max\left\{k, \left\lceil \frac{w_G(L)}{2} \right\rceil + 1\right\}.$$

Expansion

- The **boundary** of a set of equations L, denoted ∂L, is the set of variables x such that the truth value of exactly one equation in L depends on x.
- Let L be an unsatisfiable set of equations and let s denote the least size of an unsatisfiable subset of L. The **expansion** of L is defined as

$$e(L) = \min\left\{ |\partial L'| \;:\; L' \subseteq L,\ \frac{s}{3} < |L'| \leq \frac{2s}{3} \right\}.$$

Thus, every medium-size subset of L has a boundary of at least $e(L)$ variables.

High Expansion Yields High Degree

- Theorem 5.5.18. Let L be an unsatisfiable set of linear equations over GF(2), each equation of width at most k. Then

$$\deg(P_F(L)) \geq \max\left\{k, \frac{e(L)}{2} + \Theta(1)\right\}.$$

- Proof idea:
  - In every Gaussian refutation of L, there is an intermediate equation l that is implied by a medium-size subset L' of L.
  - l depends on $\partial L'$, therefore l has $\geq e(L)$ variables.
  - Approximate $w_G(L)$ by $e(L)$ in Corollary 5.5.5.

Equations from Expander Graphs

- We get unsatisfiable linear equation systems with high expansion from Tseitin's odd-charged graphs.
  - L contains n equations, each of width k.
  - $nk/2$ variables.
  - $e(L) = \Omega(n)$.
  - By Thm. 5.5.18, $\deg(P_F(L)) = \Omega(n)$.
- $\Rightarrow$ No low-degree PC refutation in Fourier basis.
- How about PC refutations for CNF formulas in Boolean basis?
  - Same lower bound (next slide).

Clausification Keeps Degree High

- Let L be an unsatisfiable set of linear equations of width k.
- Let $C(L)$ be the clausification of L where each equation is expressed as 2^{k-1} clauses of width k.
- Let $Q(C(L))$ be the set of canonical polynomials of $C(L)$ in Boolean basis along with the polynomials $x_i^2 - x_i$.
- Theorem 5.5.16.

$$\deg(Q(C(L))) \geq \max\{\deg(P_F(L)), k+1\}.$$

Summary

- Polynomial calculus for refuting CNF formulas.
- Binomial calculus in Fourier basis and Gaussian calculus for refuting linear equation systems.
- Tight connection between Gaussian width and BC refutation degree.
- Linear lower bound on the degree of PC refutations using linear equation systems with high expansion.
- PC refutation length or size?