Block-symmetric polynomials correlate with parity better than symmetric

November 2012

Emanuele Viola

Northeastern University

Joint work with

Frederic Green (Clark University)

Daniel Kreymer (Northeastern University Undergraduate)

Correlation between

polynomial f, n variables modulo p, degree d

and mod q function

$$\gamma = E_x [\, \zeta_p^{\,f(x)} \, \zeta_q^{\,|x|} \,]$$

where $|x| = \sum_i x_i$, ζ_p = p-th primitive root of unity $e^{2\pi i/p}$

Long-standing challenge ($\forall$ co-prime p,q)

Prove $|\gamma| \leq \exp(n^{-\Omega(1)})$, for $d = n^{0.01}$

Open even $|\gamma| \leq 1/n$, for $d = \log_2 n$

Surveyed in [V]

About challenge:

- $|\gamma| \leq \exp(-n/2^d)$ [Babai Nisan Szegedy] (cf. [V] for Nisan's proof of [Bourgain] from [BNS])

  $|\gamma| \leq d/\sqrt{n}$ [Razborov, Smolensky]

- So-called "barriers" not known to apply

- Progress (some distribution)
  $\Leftrightarrow$ long-sought lower bounds against Maj AC^0 mod p

Question by many, including Alon and Beigel in 2001:

Is maximum correlation achieved by symmetric polynomials?

Symmetric: invariant under permutation of variables,
value depends only on Hamming weight of input

- Block-symmetric polynomials (symmetric in each block)

- Theorem [This work] Polynomials mod odd p vs. parity

  $\forall$ degree $d \in [\,0.995\, p^t - 1\,,\, p^t - 1]$, $\forall\, t \geq 1$

$$\frac{\text{max block-symmetric correlation}}{\text{max symmetric correlation}} \geq (1.01)^{n/d^2 \log d}$$

- Only previous case known: $d = 2$, $p = 3$ [Green '02]

Partial complements

- Theorem [This work] Symmetric correlate better than block-symmetric with large blocks if

- $d = p^t$

(previous result: $d \in [\, 0.995\, p^t - 1 \,,\, p^t - 1]$)

- Or if polynomials p = 2, vs. the Mod q = odd function

(previously nothing suggested different results for different moduli)

We develop a theory we call
spectral analysis of symmetric correlation

Originates in [Cai Green Thierauf]

Our results follow from a fine result about symmetric:
correlation established up to exponentially small relative error

Spectral analysis

Correlation of symmetric polynomial f mod p with Mod q

$= \sum \alpha_i^n \ \ \beta_i$

where $\alpha_1 > \alpha_2 > \ldots > 0$, independent from polynomial
β take finitely many values

➔ $\forall$ f, $\exists$ $\beta = \beta_1$: correlation $\to \alpha_1^n \beta$

This work: tight bound on β

How does this matter for block-symmetric vs. symmetric?

Correlation of symmetric = $\alpha_1^n \beta$

Divide up n variables in n/b blocks of b each

Correlation = $(\alpha_1^b \beta)^{n/b} = \alpha_1^n \beta^{n/b}$

➔ block-symmetric beat symmetric if $\beta > 1$

Unexpected, first observed using computer search

We advocate further use of computer search
Lack of progress provides excellent terrain

This work: Analytic proof that $\beta > 1$ for $d \in [0.995\, p^t - 1, p^t - 1]$

$\beta < 1$ for $d = p^t$

Proof sketch when $d = p^t - 1$, case of smaller d reduced to it

Lemma: $\beta = \sum_{k \le d} \zeta_p^{r(k)} (-1)^k \cos(\pi (n-2k) / 2 p^t)$,

where $r(k)$ = value of polynomials at inputs of weight k

Fact: $\forall d+1$ values $r(k)$, $\exists$ symmetric polynomial achieving'em

How do we maximize $| \beta |$?

Proof sketch when $d = p^t - 1$, case of smaller d reduced to it

Lemma: $\beta = \sum_{k \le d} \zeta_p^{r(k)} (-1)^k \cos(\pi (n-2k) / 2 p^t)$,

where r(k) = value of polynomials at inputs of weight k

Fact: $\forall$d+1 values r(k), $\exists$ symmetric polynomial achieving'em

Define polynomial that agrees in sign with
$X := (-1)^k \cos(\pi (n-2k) / 2 p^t)$ as much as possible:

$r(k) = 0$	if	$X > 0$
$r(k) = (p-1)/2$	if	$X < 0$

Some trigonometric sums later...

Theorem: For this choice of the polynomial, $\beta > 1$

Also, $\beta \to 2\sqrt{3} / \pi = 1.102...$ for large d

And this is best possible

More results and open problems

- Switch-symmetric polynomials sometimes beat symm. too

- Challenge: Are symmetric polys modulo $p = 2$ optimal?

  We verified this for Mod 3 when $d = 2$, $\forall\ n \leq 10$
  $d = 3$, $\forall\ n \leq 6$

Bonus material

[Razborov V] "Real advantage"

Consider real-valued polynomials f vs. boolean function, where $f(x) \notin \{0,1\}$ always counts as a mistake

Challenge: Prove 1/n correlation with parity for degree $\log_2 n$

Prerequisite for correlation mod p, and for sign correlation

… and what do we do about it? (Spoiler: not much)

[Razborov V] “Real advantage”

Consider real-valued polynomials f vs. boolean function, where $f(x) \notin \{0,1\}$ always counts as a mistake

Challenge: Prove 1/n correlation with parity for degree $\log_2 n$

Prerequisite for correlation mod p, and for sign correlation

- **Theorem**: Correlation ≤ 0 for degree $d \leq \log \log n$

Based on anti-concentration by [Costello Tao Vu]
False for modulo p, and sign

Challenge: $d=\sqrt{n}$ is smallest we know with correlation > 0

[Servedio V] “On a special case of rigidity”

Valiant's '77 rigidity: Construct matrices far from low-rank.

Candidate: Hadamard, corresponding to Inner Product (IP)

Challenge: Prove the special case where low-rank matrices are given by sparse polynomials

Recall rank(M) = R $\leftrightarrow$ M = sum of R rank-1 matrixes.
In challenge, rank-1 matrices given by monomials.

Next: specific challenge and some new facts

- Challenge:

$\forall$ real-valued polynomial f in 2n variables (x,y) with R terms:

$$\Pr_{x,y}[f(x,y) \neq IP] >> 1/R$$

Note: log(R)/R follows from known rigidity results

- Theorem:

Challenge ➔ IP $\not\in$ AC^0 with a layer of parity gates at the input

(not known !!??)

- Theorem:

$\forall$ real-valued polynomial f in 2n variables (x,y) with R terms:

$$\Pr_{x,y}[\mathrm{sign}(f(x,y)) \neq IP] \geq \Omega(1/R)$$

Not known for rigidity

Proof by extension of [Aspnes Beigel Furst Rudich]