Correlation bounds for polynomials,

and the disproof of a conjecture on Gowers' norm using Ramsey theory

Emanuele Viola

Northeastern University

May 2011

Polynomials

- Polynomials: degree d, n variables over $F_2 = \{0,1\}$

E.g.,	$p = x_1 + x_5 + x_7$	degree d = 1
	$p = x_1 \cdot x_2 + x_3$	degree d = 2

- Computational model: $p : \{0,1\}^n \rightarrow \{0,1\}$

  Sum (+) = XOR, Product $(\cdot)$ = AND

  $x^2 = x$ over $F_2 \Rightarrow$ multilinear

- Complexity = degree

Importance of model

- Coding theory

  Hadamard, Reed-Muller codes based on polynomials

- Circuit lower bounds [Razborov ’87; Smolensky ’87]

  Lower bound on polynomials $\Rightarrow$ circuit lower bound

- Pseudorandomness [Naor Naor ‘90, Bogdanov V.]

  Useful for algorithms, PCP, expanders, learning…

Outline

- Correlation bounds
- Gowers' norm
- Disproof of a conjecture using Ramsey theory

Lower bound

- Question: Are there explicit functions that cannot be computed by low-degree polynomials?

- Answer:

$x_1 \cdot x_2 \cdots x_d$ requires degree d

Majority$(x_1,\ldots,x_n) := 1 \Leftrightarrow \sum x_i > n/2$

requires degree n/2

Correlation bound

- Question: Which functions do not correlate with low-degree polynomials?

- Cor(f, degree d) := $\max_{\text{degree-d } p}$ Bias(f+p) $\in [0,1]$

  Bias(f+p) := $| \Pr_X [f(X)=p(X)] - \Pr_X [f(X)\neq p(X)] |$

  X distribution on $\{0,1\}^n$; often uniform; won't specify

  E.g. Cor(deg d, deg d) = 1; Cor(random f, deg. d) ~ 0

- More challenging. Surveyed in [V.]

A sample of correlation bounds

- Want: Explicit **f**: Cor(**f**, degree $n^{\Omega(1)}$) ≤ exp($-n^{\Omega(1)}$)
  Equivalent to long-standing circuit lower bounds

- Candidate **f**: sum of input bits **mod 3**

- [Babai Nisan Szegedy '92] [Bourgain] … [V.]
  Cor(**f**, degree d) ≤exp(-n/2^d)   (good if d ≤0.9 log n)

- [Razborov '87] [Smolensky]: Cor(**f**, degree $n^{\Omega(1)}$) ≤ 1/√n

- Barrier: Cor(**f**, degree log n) ≤ 1/n ?

Exact correlation

- Exact bounds: find polynomial maximing correlation

  [Green '04]

- [Kreymer V.] ongoing computer search

  E.g.: Up to $n = 10$, Cor(mod 3, degree 2) maximized

  by symmetric polynomial =

  sum of elementary symmetric polynomials

  $S_1 := \sum_i x_i \qquad S_2 := \sum_{i<j} x_i \cdot x_j$

- Challenge: prove it for every n

Outline

- Correlation bounds
- Gowers' norm
- Disproof of a conjecture using Ramsey theory

Gowers norm

[Gowers '98; Alon Kaufman Krivelevich Litsyn Ron '03]

- Measure correlation with degree-d polynomials: check if random d-th derivative is biased

- Derivative in direction $y \in \{0,1\}^n$: $D_y f(x) := f(x+y) - f(x)$
  - E.g. $D_{y_1\, y_2\, y_3}(x_1 x_2 + x_3) = y_1 x_2 + x_1 y_2 + y_1 y_2 + y_3$

- Norm $N_d(f) := E_{Y^1 \ldots Y^d \in \{0,1\}^n} \mathrm{Bias}_U[D_{Y^1 \ldots Y^d} f(U)] \in [0,1]$

(Bias [Z] := | Pr[Z = 0] - Pr[Z = 1] |)

$N_d(f) = 1 \Leftrightarrow f$ has degree d

Using Gowers norm

- Lemma [Babai Nisan Szegedy] [Gowers] [Green Tao]

  Cor(**f**, degree d) < $N_d(\mathbf{f})^{1/2^d}$

- Theorem [V.]

  Cor(**mod 3**, degree d) < $\exp(n/4^d)$

  Explicit **f** : Cor(**f**, degree d) < $\exp(n/2^d)$

– Best-known bounds for d < 0.9 log n.
  Slight improvement over [Babai Nisan Szegedy] [Bourgain]

Outline

- Correlation bounds
- Gowers' norm
- Disproof of a conjecture using Ramsey theory

A conjecture on Gowers' norm

- Conjecture [Green Tao] [Samorodnitsky] '07:
  For every function **f**,
  $N_d(\mathbf{f}) = \Omega(1) \Leftrightarrow \mathrm{Cor}(\mathbf{f}, \text{degree } d) = \Omega(1)$

- [GT] [Lovett Meshulam Samorodnitsky]
  False for d = 4

Counterexample: $\mathbf{f} = S_4 := \sum_{h< i< j< k} x_h \cdot x_i \cdot x_j \cdot x_k$

$N_3(S_4) = \Omega(1)$ (not difficult)

$\mathrm{Cor}(S_4, \text{degree } 3) = o(1)$ (complicated)

Developments

- Remark: An inverse conjecture can be saved going to non-classical polynomials [Green Tao]

- After announcement of counterexample, [GT] and [V.]

  noted simple proof of Cor(S_4, degree 3) = o(1)

  using [Alon Beigel], in turn based on Ramsey Theory

Simple proof [Alon Beigel]

- Theorem $\mathrm{Cor}(S_4$, degree $d=3) = o(1)$
- Proof for $d = 2$: Let p be degree-2 polynomial.
- Easy if p = Linear + b S_2 $\quad b \in \{0,1\}$
- Reduce to this case:

  Graph $V := \{1,2,\ldots,n\}$, $E := \{ \{i,j\} : x_i \cdot x_j$ monomial of $p \}$

  Ramsey: $\exists$ clique (or indep. set) of size $\Omega(\log n)$

  Fix other variables arbitrarily. ♦

Conclusion

- Model: degree-d polynomials over {0,1}

- Correlation bounds

  Barrier: correlation 1/n for degree log n

  Computer search reveals symmetry [Kreymer V.]

- Gowers' norm

  Gives best known correlation bounds d < 0.9 log n [V.]

  A false conjecture [Green Tao] [Lovett Meshulam Samorodnitsky]

  simple proof [GT] [V.] via Ramsey theory [Alon Beigel]

- ∑∏√∩∉∪⊃⊇⊄⊂⊆∈⇓⇒⇑⇐⇔∨∧≥≤∀∃Ωαβεγδ→⇒
- ≠≈TAΘω
- ∈ ∉
-
-
- ∑∏√∩∉∪⊃⊇⊄⊂⊆∈⇓⇒⇑⇐⇔∨∧≥≤∀∃Ωαβεγδ→
- ≠≈TAΘ
-
- Recall: edit style changes ALL settings.
- Click on “line” for just the one you highlight