Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols

Emanuele Viola, IAS

(Work partially done during postdoc at Harvard)

Joint work with Avi Wigderson

June 2007

Basic questions

- Computational model M
  - E.g. M = circuits, GF(2) polynomials, multiparty protocols
- Lower bound: $\exists$ explicit $f : \{0,1\}^n \to \{0,1\}$ not in M?
- [This talk] Correlation bound: $\exists$ explicit $f : Cor(f,M) \leq \varepsilon$?

  $Cor(f,M) := \max_{p \in M} \left| E_x \left[(-1)^{f(x) + p(x)} \right] \right| \in [0,1]$
  - Want $\varepsilon = \varepsilon(|x|)$ small
- Motivation: Correlation bound $\Rightarrow$
  pseudorandom generator [Yao,Nisan Wigderson]
  lower bound for M' $\supset$ M [Razborov, Hajnal et al.]

XOR lemma

- Generic way to boost correlation bound

- $f^{\oplus k}(x_1,\ldots, x_k) := f(x_1) \oplus \cdots \oplus f(x_k)$

  Hope: $Cor(f^{\oplus k},M) \leq Cor(f,M)^{\Omega(k)}$

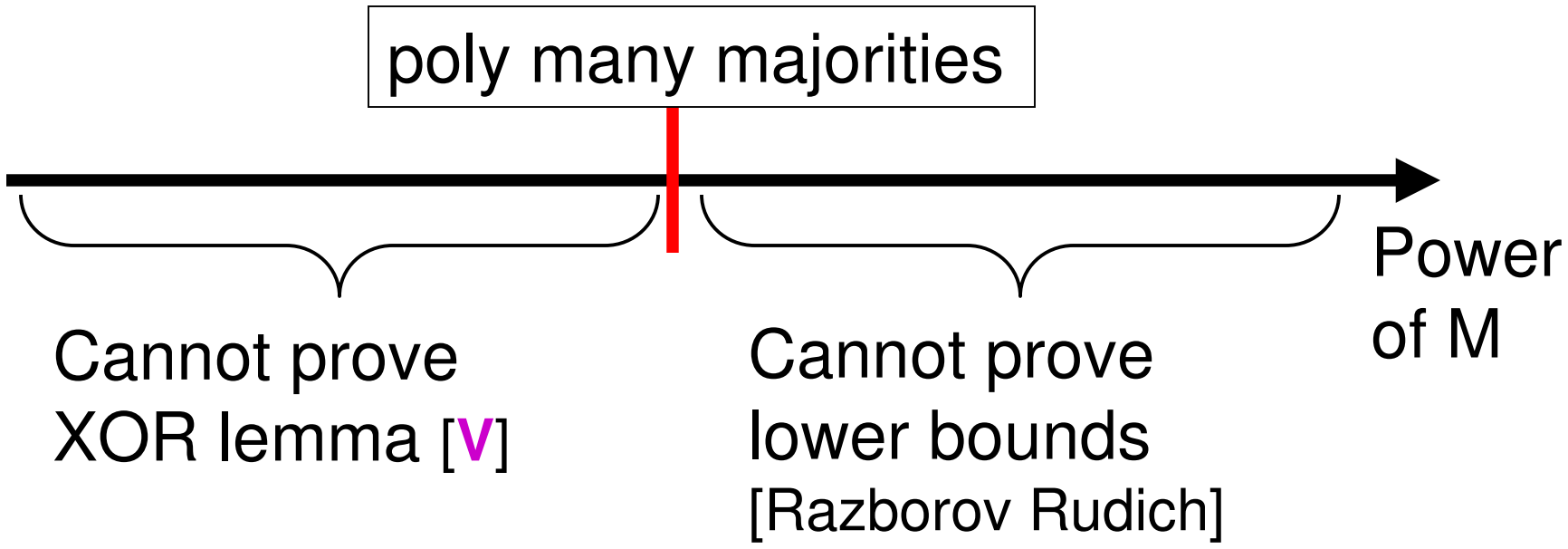
- Theorem[Yao, Levin, Goldreich Nisan Wigderson, Impagliazzo,…]

  XOR lemma for M = circuits

Problem with XOR lemma

- Proofs of the XOR lemma [Y,L,GNW,…] don't work in any model M for which we have lower bounds!

- Conjecture[V]: Black-box proof of XOR lemma for M $\Rightarrow$ M closed under polynomially many majorities



Overview of our results

- Study two fundamental models
  1) GF(2) polynomials
  2) multiparty protocols

- Prove new XOR lemmas

- Improve or simplify correlation bounds

Main technique

- Use norm $N(f) \in [0,1]$:
  (I) $Cor(f,M) \approx N(f)$
  (II) $N(f^{\oplus k}) = N(f)^k$

- Proof of the XOR lemma:
  $Cor(f^{\oplus k},M) \approx N(f^{\oplus k}) = N(f)^k \approx Cor(f,M)^k$ Q.e.d.

- Proof for circuits [L,GNW,…] different: “simulation”

Outline

- Overview
- GF(2) polynomials
- Multiparty protocols
- Direct product

GF(2) polynomials

- P_d := polynomials $p : \{0,1\}^n \to \{0,1\}$ of degree d

  E.g., $p = x_1 + x_5 + x_7$ $\quad d = 1$

  $p = x_1 \cdot x_2 + x_3$ $\quad d = 2$

- Recall correlation bound: $Cor(f,P_d) \leq \varepsilon = \varepsilon(n,d)$

  $\Leftrightarrow \forall\, p \in P_d : |\, E_x [e(f(x) + p(x))] \,| \leq \varepsilon$

  $(e(X):=(-1)^X)$

- Note: Fundamental barrier: $d = \log_2 n$, $\varepsilon = 1/n$?

Gowers norm

- Idea: Measure correlation with degree-d polynomials by checking if random (d+1)-th derivative vanishes
  - Other view: perform random parity check

- Derivative $D_y\, p(x) := p(x+y) + p(x)$
  - E.g. $D_y\,(x_1x_2 + x_3) = y_1x_2 + x_1y_2 + y_1y_2 + y_3$
  - p degree d $\Rightarrow$ $D_y\, p(x)$ degree d-1
  - Iterate: $D_{y,y'}\, p(x) := D_y(\, D_{y'}\, p(x))$

- t-th Gowers norm of $f : \{0,1\}^n \to \{0,1\}$: $(t = d+1)$

  $\mathbf{U_t(f) := E_{x,y^1,\ldots,y^t}[e(\, D_{y^1,\ldots,y^t}\, f(x)\,)]}$ $(e(X):=(-1)^X)$

  Note: p degree d $\Leftrightarrow$ $U_{d+1}(p)=1$, and $U_{d+1}(f+p)=U_{d+1}(f)$

Properties of norm

- $U_t(f) := E_{x,y^1,\ldots,y^t}[e(D_{y^1,\ldots,y^t} f(x))]$ $\quad (e(X):=(-1)^X)$

(I) $U_{d+1}(f) \approx Cor(f,P_d)$:

Lemma[Gowers, Green Tao]:
$Cor(f,P_d) \leq U_{d+1}(f)^{1/2^d}$

Lemma[Alon Kaufman Krivelevich Litsyn Ron] (Property testing):
$Cor(f,P_d) \leq 1/2 \Rightarrow U_{d+1}(f) \leq 1\text{-}2^{-O(d)}$

(II) $U(f^{\oplus k}) = U(f)^k$

– Follows from definition

XOR lemma for GF(2) polynomials

(I) $U_{d+1}(f) \approx Cor(f,P_d)$:

Lemma[G, GT]: $Cor(f,P_d) \leq U_{d+1}(f)^{1/2^d}$

Lemma[AKKLR]: $Cor(f,P_d) \leq 1/2 \Rightarrow U_{d+1}(f) \leq 1-2^{-O(d)}$

(II) $U(f^{\oplus k}) = U(f)^k$

- Theorem[This work]:
  $Cor(f,P_d) \leq 1/2 \Rightarrow Cor(f^{\oplus k},P_d) \leq \exp(-k/2^{O(d)})$
- Proof:
  $Cor(f^{\oplus k},P_d) \leq U_{d+1}(f^{\oplus k})^{1/2^d} = U_{d+1}(f)^{k/2^d} \leq (1-2^{-O(d)})^{k/2^d}$

Q.e.d.

Our correlation bound for Mod 3

- Mod $3(x_1,\ldots,x_n) := 1$ iff $3 \mid \sum_i x_i$
- Theorem [Bourgain '05]: $\mathrm{Cor}(\mathrm{Mod}\ 3, P_d) \leq \exp(-n/8^d)$
- Theorem [This work]: $\mathrm{Cor}(\mathrm{Mod}\ 3, P_d) \leq \exp(-n/4^d)$
- New proof (formalize over $\mathbb{C}$):

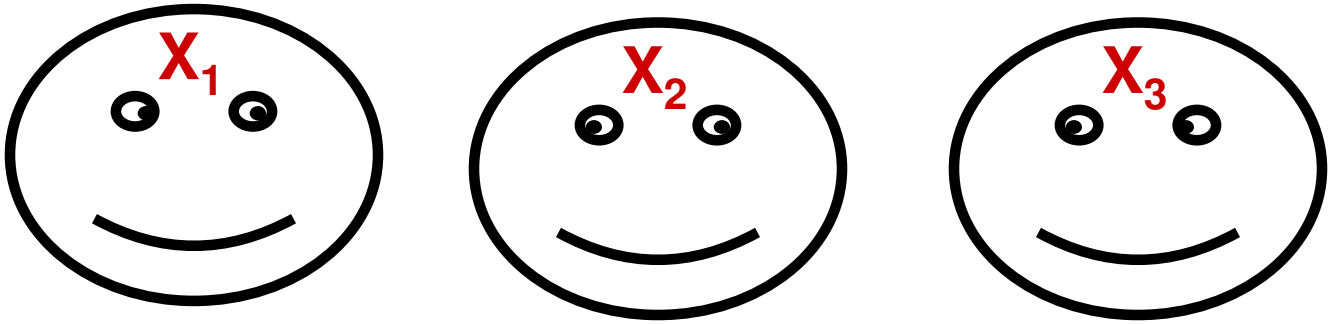
$$\mathrm{Cor}((x_1)^{\oplus n} \bmod 3, P_d) \leq U_{d+1}((x_1)^{\oplus n} \bmod 3)^{1/2^d}$$
$$= U_{d+1}(x_1 \bmod 3)^{n/2^d}$$
$$= \exp(-n/4^d) \qquad \text{Q.e.d.}$$

Outline

- Overview
- GF(2) polynomials
- Multiparty protocols
- Direct product

Multiparty protocols

[Yao,Chandra Furst Lipton]



- d parties wish to compute $f : X_1 \times X_2 \ldots \times X_d \rightarrow \{0,1\}$
  Party i knows all inputs except x_i (on forehead)
  Cost of protocol = communication

- Applications to nearly every area of computer science
  - Circuit/proof complexity, PRGs, TM's, branching programs…

- $\Pi_{d,c}$:= d-party protocols communicating c bits

Multiparty norm

[Babai Nisan Szegedy,Chung Tetali,Raz]

- [This work]: coherent view like GF(2) polynomials

- $\Pi\oplus_d$:= each party sends one bit, output is XOR
  - Note: $P_{d-1} \subseteq \Pi\oplus_d \subseteq \Pi_{d,d}$ [Hastad Goldmann]

- d-party norm of f, captures correlation with $\Pi\oplus_d$

  $\mathbf{R_d(f) := E_{X^0,X^1}[e(\sum_{b \in \{0,1\}^d} f(X^b))]}$ $(e(X):=(-1)^X)$

  where $X^0 = (x_1^0,\ldots,x_d^0)$, $X^1 = (x_1^1,\ldots,x_d^1)$, $X^b = (x_1^{b1},\ldots,x_d^{bd})$
  (Perform random parity check)

- Note: $p \in \Pi\oplus_d \Leftrightarrow R_d(p)=1$, and $R_d(f+p)=R_d(f)$

XOR lemma for protocols

(I) $R_d(f) \approx Cor(f,\Pi_{d,c})$:

Lemma[BNS,CT,R]: $Cor(f,\Pi_{d,c}) \leq 2^c \cdot Cor(f,\Pi\oplus_d)$

Lemma[BNS,CT,R]: $Cor(f,\Pi\oplus_d) \leq R_d(f)^{1/2^d}$

Lemma[This work]: $Cor(f, \Pi\oplus_d) \geq R_d(f)$

(II) $R_d(f^{\oplus k}) = R_d(f)^k$

- Theorem[This work]:
  $Cor(f,\Pi\oplus_d) \leq \varepsilon \Rightarrow Cor(f^{\oplus k}, \Pi_{d,c}) \leq 2^c \cdot \varepsilon^{k/2^d}$
- 2-party case already known [Shaltiel]

Outline

- Overview
- GF(2) polynomials
- Multiparty protocols
- Direct product

Direct product

- Want to compute $f^k(x_1,\ldots,x_k) := (f(x_1),\ldots,f(x_k)) \in \{0,1\}^k$

  $Suc(f,M) := \max_{p \in M} |Pr[f^k(x_1,\ldots,x_k) = p(x_1,\ldots,x_k)]|$

- Lemma[This work]: $Suc(f^k,M) \leq Cor(f^{\oplus k},M)$
  - Easy converse of [Goldreich Levin]; works whenever $\oplus \in M$
  - Simplifies result from [Impagliazzo Wigderson '97]

- XOR lemmas for P_d, $\Pi_{d,c} \Rightarrow$ direct products

- [Parnafes Raz Wigderson] direct product for 2-party
  - Parameters incomparable

Conclusion

- Study two fundamental models:
  - 1) GF(2) polynomials
  - 2) multiparty protocols

- Prove new XOR lemmas, correlation bounds, direct products

- Via norm N : (I) $Cor(f,M) \approx N(f)$, (II) $N(f^{\oplus k}) = N(f)^k$
  - Powerful technique: new PRGs for GF(2) polynomials [BV]

- Questions: Are XOR lemmas tight?
  - [This work] "Ideal" XOR lemma $\varepsilon \Rightarrow \varepsilon^2$ for 2-party false

  Bounds for (log n)-degree polynomials?

Thank you!