The Method of Multiplicities

Madhu Sudan
Microsoft New England/MIT

Based on joint works with:
- V. Guruswami ‘98
- S. Saraf ‘08
- Z. Dvir, S. Kopparty, S. Saraf ‘09

Agenda

- A technique for combinatorics, via algebra:
  - Polynomial (Interpolation) Method + Multiplicity method
    - List-decoding of Reed-Solomon Codes
    - Bounding size of Kakeya Sets
    - Extractor constructions

Part I: Decoding Reed-Solomon Codes

- Reed-Solomon Codes:
  - Commonly used codes to store information (on CDs, DVDs etc.)
    - Message: $C_0, C_1, \ldots, C_d \in F$ (finite field)
    - Encoding:
      - View message as polynomial: $M(x) = \sum_{i=0}^{d} C_i x^i$
      - Encoding = evaluations: $\{ M(\alpha) \}$_$\{ \alpha \in F \}$
- Decoding Problem:
  - Given: $(x_1,y_1) \ldots (x_n,y_n) \in F \times F$; integers t,d;
  - Find: deg. d poly through t of the n points.

List-decoding?

- If #errors ($n-t$) very large, then several polynomials may agree with t of n points.
  - List-decoding problem:
    - Report <u>all</u> such polynomials.
  - Combinatorial obstacle:
    - There may be too many such polynomials.
    - Hope – can't happen.
    - To analyze: Focus on polynomials $P_1, \ldots, P_L$ and set of agreements $S_1 \ldots S_L$.
- Combinatorial question: Can $S_1, \ldots S_L$ be large, while $n = | \cup_j S_j |$ is small?

List-decoding of Reed-Solomon codes

- Given L polynomials $P_1,\ldots,P_L$ of degree d; and sets $S_1,\ldots,S_L \subset F \times F$ s.t.
    - $|S_i| = t$
    - $S_i \subset \{(x,P_i(x)) \mid x \in F\}$
  - How small can $n = |S|$ be, where $S = \cup_i S_i$?
- Algebraic analysis from [S. '96, GuruswamiS '98] basis of decoding algorithms.

List-decoding analysis [S '96]

- Construct $Q(x,y) \neq 0$ s.t.
    - $\mathrm{Deg}_y(Q) < L$
    - $\mathrm{Deg}_x(Q) < n/L$
    - $Q(x,y) = 0$ for every $(x,y) \in S = \cup_i S_i$
- Can Show:
    - Such a Q exists (interpolation/counting).
    - Implies: $t > n/L + dL \Rightarrow (y - P_i(x)) \mid Q$
- Conclude: $n \geq L \cdot (t - dL)$.
    - (Can be proved combinatorially also; using inclusion-exclusion)
    - If $L > t/(2d)$, yield $n \geq t^2/(4d)$

Focus: The Polynomial Method

- To analyze size of "algebraically nice" set S:
  - Find polynomial Q vanishing on S;
    - (Can prove existence of Q by counting coefficients … degree Q grows with |S|.)
  - Use "algebraic niceness" of S to prove Q vanishes at other places as well.
    - (In our case whenever $y = P_i(x)$).
  - Conclude Q zero too often (unless S large).

… (abstraction based on [Dvir]'s work)

Improved L-D. Analysis [G.+S. '98]

- Can we improve on the inclusion-exclusion bound? One that works when $n > t^2/(4d)$?
- Idea: Try fitting a polynomial Q that passes through each point with "multiplicity" 2.
  - Can find with $\mathrm{Deg}_y < L$, $\mathrm{Deg}_x < 3n/L$.
  - If $2t > 3n/L + dL$ then $(y-P_i(x)) \mid Q$.
  - Yields $n \geq (L/3).(2t - dL)$
  - If $L>t/d$, then $n \geq t^2/(3d)$.
- Optimizing Q; letting mult. $\to \infty$, get $n \geq t^2/d$

Aside: Is the factor of 2 important?

- Results in some improvement in [GS] (allowed us to improve list-decoding for codes of high rate) …

- But crucial to subsequent work
  - [Guruswami-Rudra] construction of rate-optimal codes: Couldn't afford to lose this factor of 2 (or any constant > 1).

Focus: The <u>Multiplicity</u> Method

- To analyze size of "algebraically nice" set S:
  - Find poly Q zero on S (<u>w. high multiplicity</u>);
    - (Can prove existence of Q by counting coefficients … degree Q grows with |S|.)
  - Use "algebraic niceness" of S to prove Q vanishes at other places as well.
    - (In our case whenever $y = P_i(x)$).
  - Conclude Q zero too often (unless S large).

Multiplicity = ?

- Over reals: $Q(x,y)$ has root of multiplicity $m+1$ at (a,b) if every partial derivative of order up to m vanishes at 0.

- Over finite fields?
  - Derivatives don't work; but "Hasse derivatives" do. What are these? Later…
  - There are $\{m+n \text{ choose } n\}$ such derivatives, for n-variate polynomials;
    - Each is a linear function of coefficients of f.

Part II: Kakeya Sets

Kakeya Sets

- $K \subset F^n$ is a Kakeya set if it has a line in every direction.
  - I.e., $\forall\, y \in F^n\ \exists\, x \in F^n$ s.t. $\{x + t.y \mid t \in F\} \subset K$
  - F is a field (could be Reals, Rationals, Finite).

- Our Interest:
  - $F = F_q$ (finite field of cardinality q).
  - Lower bounds.
  - Simple/Obvious: $q^{n/2} \leq K \leq q^n$
  - Do better? Mostly open till [Dvir 2008].

Kakeya Set analysis [Dvir '08]

- Find $Q(x_1,\ldots,x_n) \neq 0$ s.t.
  - Total deg. of $Q < q$ (let deg. $= d$)
  - $Q(x) = 0$ for every $x \in K$. (exists if $|K| < q^n/n!$)
- Prove that (homogenous deg. d part of) Q vanishes on y, if there exists a line in direction y that is contained in K.
  - Line $L \subset K \Rightarrow Q|_L = 0$.
  - Highest degree coefficient of $Q|_L$ is homogenous part of Q evaluated at y.
- Conclude: homogenous part of $Q = 0$. ><.
- Yields $|K| \geq q^n/n!$.

Multiplicities in Kakeya [Saraf, S '08]

- Fit Q that vanishes often?
  - Good choice: #multiplicity $m = n$
  - Can find $Q \neq 0$ of individual degree $< q$, that vanishes at each point in K with multiplicity n, provided $|K|\ 4^n < q^n$
  - $Q|_L$ is of degree $< qn$.
  - But it vanishes with multiplicity n at q points!
  - So it is identically zero $\Rightarrow$ its highest degree coeff. is zero. $><$
- Conclude: $|K| \geq (q/4)^n$

Comparing the bounds

- Simple: $|K| \geq q^{n/2}$
- [Dvir]: $|K| \geq q^n/n!$
- [SS]: $|K| \geq q^n/4^n$

- [SS] improves Simple even when q (large) constant and $n \to \infty$ (in particular, allows $q < n$)
- [MockenhauptTao, Dvir]:

  $\exists$ K s.t. $|K| \leq q^n/2^{n-1} + O(q^{n-1})$

- Can we do even better?

Part III:
Randomness Mergers & Extractors

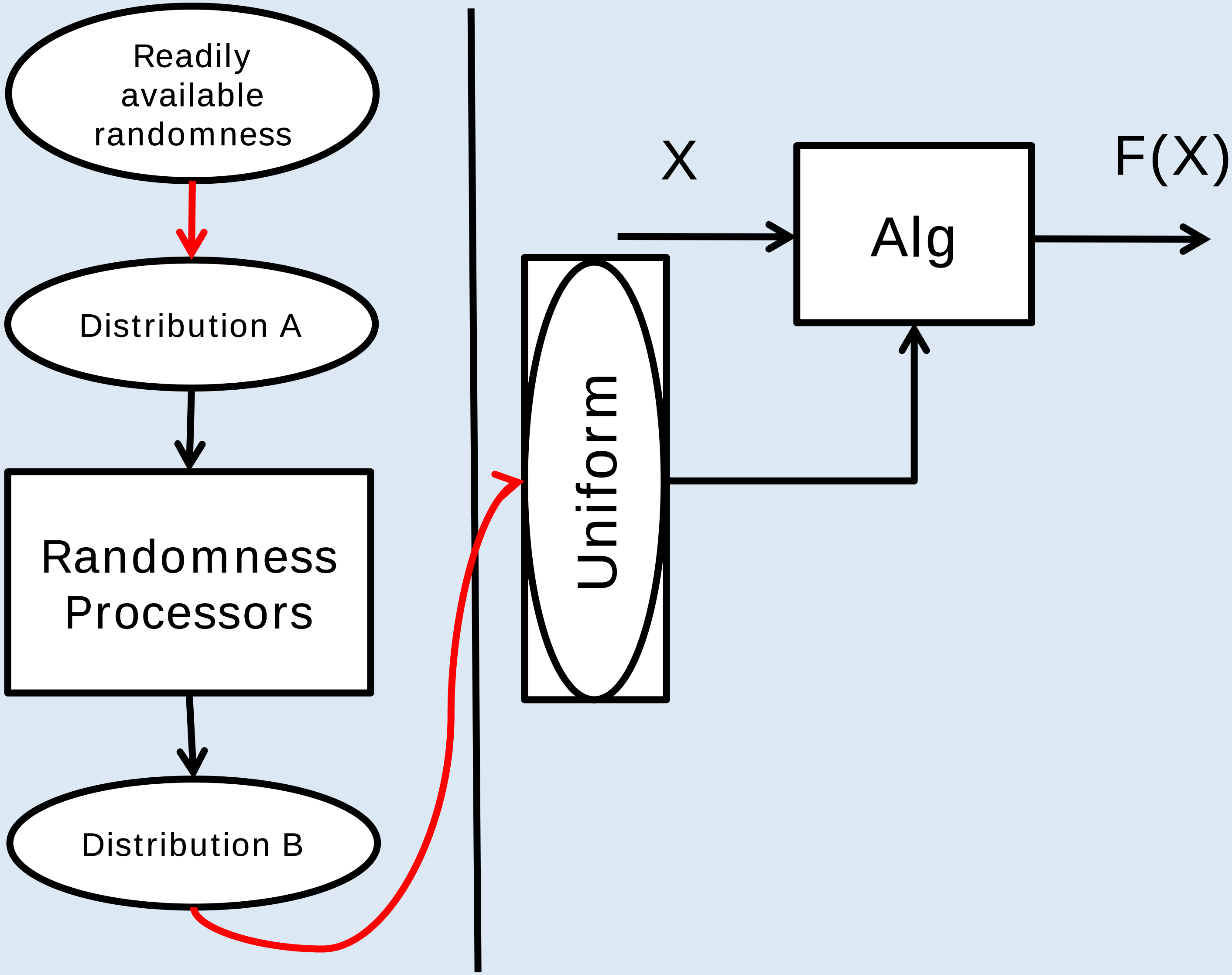
Context

- One of the motivations for Dvir's work:
  - Build better "randomness extractors"
  - Approach proposed in [Dvir-Shpilka]
  - Following [Dvir] , new "randomness merger" and analysis given by [Dvir-Wigderson]
  - Led to "extractors" matching known constructions, but not improving them …

- What are Extractors? Mergers? … can we improve them?

Randomness in Computation

Support industry:



Prgs, (seeded) extractors, limited independence generators, epsilon-biased generators, Condensers, mergers,

Randomness Extractors and Mergers

- Extractors:
  - Dirty randomness $\rightarrow$ Pure randomness

    (Biased, correlated) (Uniform, independent … nearly)

    + small pure seed

- Mergers: General primitive useful in the context of manipulating randomness.
  - k random variables $\rightarrow$ 1 random variable

    (One of them uniform) (high entropy)

    (Don't know which, others potentially correlated)

    + small pure seed

Merger Analysis Problem

- Merger($X_1,\ldots,X_k$; s) = f(s),
  where $X_1, \ldots, X_k \in F_q^n$; $s \in F_q$
  and f is deg. k-1 function mapping $F \rightarrow F^n$
  s.t. $f(i) = X_i$.
  (f is the curve through $X_1,\ldots,X_k$)

- Question: For what choices of q, n, k is Merger's output close to uniform?

- Arises from [DvirShpilka'05, DvirWigderson'08].
  - "Statistical high-deg. version" of Kakeya problem.

Concerns from Merger Analysis

- [DW] Analysis: Worked only if $q > n$.
  - So seed length $= \log_2 q > \log_2 n$
  - Not good enough for setting where $k = O(1)$, and $n \to \infty$.
  - (Would like seed length to be $O(\log k)$).
- Multiplicity technique:
  - seems bottlenecked at mult $= n$.

General obstacle in multiplicity method

- Can't force polynomial Q to vanish with too high a multiplicity. Gives no benefit.

- E.g. Kakeya problem: Why stop at mult $= n$?
  - Most we can hope from Q is that it vanishes on all of q^n;
  - Once this happens, $Q = 0$, if its degree is $< q$ in each variable.
  - So $Q|_L$ is of degree at most qn, so mult n suffices. Using larger multiplicity can't help!
  - Or can it?

Extended method of multiplicities

- (In Kakeya context):
  - Perhaps vanishing of Q with high multiplicity at each point shows higher degree polynomials (deg > q in each variable) are identically zero?
    - (Needed: Condition on multiplicity of zeroes of multivariate polynomials .)
  - Perhaps Q can be shown to vanish with high multiplicity at each point in F^n.
    - (Technical question: How?)

Vanishing of high-degree polynomials

- Mult(Q,a) = multiplicity of zeroes of Q at a.
- I(Q,a) = 1 if mult(Q,a) > 0 and 0 o.w.

  = min{1, mult(Q,a)}

- Schwartz-Zippel: for any $S \subset F$

  $\sum I(Q,a) \leq d. \, |S|^{n-1}$ where sum is over $a \in S^n$
- Can we replace I with mult above? Would strengthen S-Z, and be useful in our case.
- [DKSS '09]: Yes … (simple inductive proof

  … that I can never remember)

Multiplicities?

- $Q(X_1,\ldots,X_n)$ has zero of mult. m at $a = (a_1,\ldots,a_n)$ if all (Hasse) derivatives of order $< m$ vanish.
- Hasse derivative = ?
  - Formally defined in terms of coefficients of Q, various multinomial coefficients and a.
  - But really …
    - The $i = (i1,\ldots, in)$th derivative is the coefficient of $z_1^{i1}\ldots z_n^{in}$ in $Q(z + a)$.
  - Even better … coeff. of z^i in $Q(z+x)$
    - (defines ith derivative Q_i as a function of x; can evaluate at $x = a$).

Key Properties

- Each derivative is a linear function of coefficients of Q. [Used in [GS'98], [SS'09] .] $(Q+R)_i = Q_i + R_i$
- Q has zero of mult m at a, and S is a curve that passes through a, then $Q|_S$ has zero of mult m at a. [Used for lines in prior work.]
- Q_i is a polynomial of degree $\deg(Q) - \sum_j i_j$ (not used in prior works)
- $(Q_i)_j \neq Q_{i+j}$, but $Q_{i+j}(a) = 0 \Rightarrow (Q_i)_j(a) = 0$
- Q vanishes with mult m at a

  $\Rightarrow Q_i$ vanishes with mult $m - \sum_j i_j$ at a.

Propagating multiplicities (in Kakeya)

- Find Q that vanishes with mult m on K
- For every i of order $m/2$, Q_i vanishes with mult $m/2$ on K.
- **Conclude:** Q, as well as all derivatives of Q of order $m/2$ vanish on F^n

  $\Rightarrow$ Q vanishes with multiplicity $m/2$ on F^n

- **Next Question:** When is a polynomial (of deg $> qn$, or even q^n) that vanishes with high multiplicity on q^n identically zero?

Back to Kakeya

- Find Q of degree d vanishing on K with mult m. (can do if $(m/n)^n\,|K| < (d/n)^n \;\Leftrightarrow\; d^n > m^n\,|K|$)
- Conclude Q vanishes on F^n with mult. $m/2$.
- Apply Extended-Schwartz-Zippel to conclude

$$(m/2)\, q^n < d\, q^{n-1}$$
$$\Leftrightarrow \quad (m/2)\, q < d$$
$$\Leftrightarrow (m/2)^n\, q^n < d^n = m^n\,|K|$$

- Conclude: $|K| \geq (q/2)^n$
- Tight to within $2+o(1)$ factor!

Consequences for Mergers

- Can analyze [DW] merger when $q > k$ very small, n growing;
  - Analysis similar, more calculations.
  - Yields: Seed length $\log q$ (independent of n).

- By combining it with every other ingredient in extractor construction:
  - Extract all but vanishing entropy ($k - o(k)$ bits of randomness from (n,k) sources) using $O(\log n)$ seed (for the first time).

Other applications

- [Woodruff-Yekhanin '05]: An elegant construction of novel "LDCs (locally decodable codes)". [Outclassed by more recent Yekhanin/Efremenko constructions.]

- [Kopparty-Lev-Saraf-S. '09]: Higher dimensional Kakeya problems.

- [Kopparty-Saraf-Yekhanin 'yesterday]: Locally decodable codes with Rate $\rightarrow$ 1.

Conclusions

- New (?) technique in combinatorics …
- Polynomial method + Multiplicity method
  - Supporting evidence:
    - List decoding
    - Kakeya sets
    - Extractors/Mergers
    - Locally decodable codes …

Thank You