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

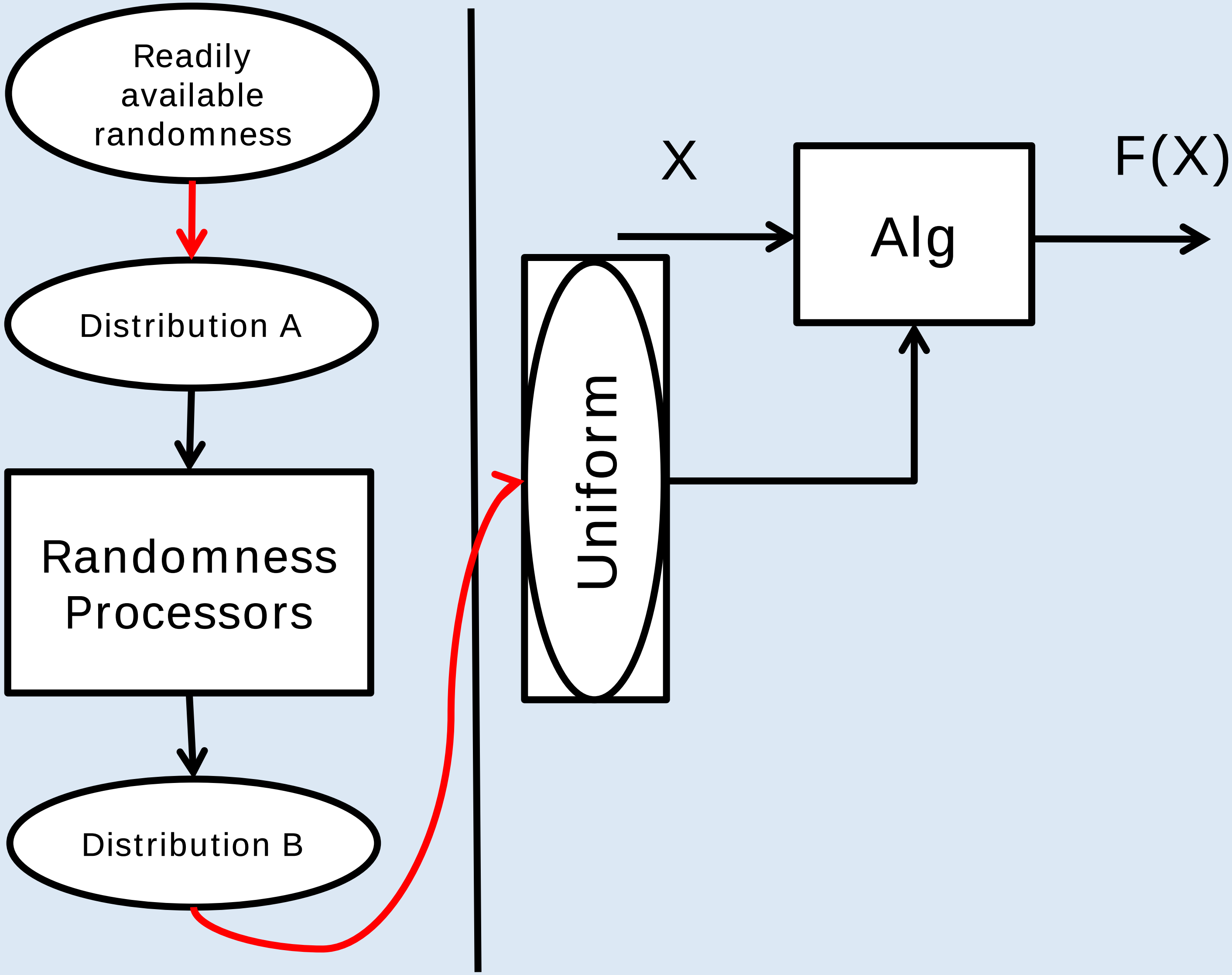
Kakeya Sets

- $K \subset F^n$ 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].

Randomness in Computation

Support industry:



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

Randomness Extractors and Mergers

- Extractors: Physical randomness (correlated, biased) + small pure seed -> Pure randomness (for use in algorithms).

- Mergers: General primitive useful in the context of manipulating randomness.
  - Given: k (possibly dependent) random variables $X_1 \ldots X_k$, such that one is uniform over its domain,
  - Add: small seed s (Additional randomness)
  - Output: a uniform random variable Y.

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 $F \to F^n$

  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.

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 $S = \cup_i S_i$?

- Problem arises in "List-decoding of RS codes"
  - Algebraic analysis from [S. '96, GuruswamiS'98] basis of decoding algorithms.

What is common?

- Given a set in F_q^n with nice algebraic properties, want to understand its size.
  - Kakeya Problem:
    - The Kakeya Set.
  - Merger Problem:
    - Any set $T \subset F^n$ that contains ϵ-fraction of points on ϵ-fraction of merger curves.
    - If T small, then output is non-uniform; else output is uniform.
  - List-decoding problem:
    - The union of the sets.

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: $t > n/L + dL \Rightarrow (y - P_i(x)) \mid Q$
- Conclude: $n \geq L \cdot (t - dL)$.
  - (Can be proved combinatorially also; using inclusion-exclusion)
  - If $L > t/(2d)$, yield $n \geq t^2/(4d)$

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 $|K| \geq q^n/n!$.

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

- Can we improve on the inclusion-exclusion bound? Working when $t < dL$?

- 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. $\rightarrow \infty$, 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).

Multiplicity = ?

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

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

Multiplicities in Kakeya [Saraf,S '08]

- Back to $K \subset F^n$. Fit Q that vanishes often?
  - Works!
  - Can find $Q \neq 0$ of individual degree $< q$, that vanishes at each point 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?
- Improve Merger Analysis?

Concerns from Merger Analysis

- Recall 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 curve s.t. $f(i) = X_i$.
- [DW08] Say X_1 random; Let K be such that ϵ fraction of choices of $X_1,\ldots,X_k$ lead to "bad" curves such that ϵ fraction of s's such that Merger outputs value in K with high probability.
- Build low-deg. poly Q vanishing on K; Prove for "bad" curves, Q vanishes on curve; and so Q vanishes on ϵ-fraction of X_1's (and so ϵ-fraction of domain).
- Apply Schwartz-Zippel. ><

Concerns from Merger Analysis

- [DW] Analysis: Works 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 $O(\log k)$).
- Multiplicty technique: Seems to allow $q < n$.
  - But doesn't seem to help …
  - Degrees of polynomials at most qn;
  - Limits multiplicities.

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 Q can be shown to vanish with high multiplicity at each point in F^n.
    - (Technical question: How?)
  - Perhaps vanishing of Q with high multiplicity at each point shows higher degree polynomials (deg

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

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?

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't remember)

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).

Conclusions

- Method of multiplicities
  - Extends power of algebraic techniques beyond "low-degree" polynomials.
  - Key ingredient: Extended Schwartz-Zippel lemma.
  - Gives applications to
    - Kakeya Sets: Near tight bounds
    - Extractors: State of the art constructions
    - RS List-decoding: Best known algorithm [GS '98] + algebraic proofs of known bounds [DKSS '09].
- Open:
  - Other applications? Why does it work?

Thank You