Second Moment Lower Bounds for K-SAT

Cristopher Moore
Univ. New Mexico
Santa Fe Institute

Joint work with
Dimitris Achlioptas

Random Formulas

- In analogy with the $G(n,m)$ model of random graphs, let $F_k(n,m)$ denote a formula with *n* variables and *m* clauses, where the clauses are chosen uniformly (with replacement) from the $2^k\binom{n}{k}$ possible clauses:

$$(x_{37} \vee \overline{x_{12}} \vee x_{42}) \wedge \cdots$$

- When is $F_k(n, m = rn)$ probably satisfiable?

The Threshold Conjecture

- We believe that for each $k \geq 2$, there is a constant r_k such that

$$\lim_{n\to\infty} \Pr[F_k(n, m = rn) \text{ is satisfiable}] = \begin{cases} 1 & \text{if } r < r_k \\ 0 & \text{if } r > r_k \end{cases}$$

- Known for $k = 2$ [Chvátal & Reed, de la Vega, Goerdt]

- A non-uniform threshold [Friedgut] implies that positive probability ⇒ high probability

Upper and Lower Bounds

- A first moment argument gives [Franco & Paull]

$$r_k < 2^k \ln 2$$

- Analyzing simple algorithms with differential equations [Chao & Franco, Frieze & Suen] gives

$$r > 2^k / k$$

- This asymptotic gap persisted for 10 years until [Achlioptas and Moore, FOCS 2002] showed

$$r > 2^{k-1} \ln 2 - O(1)$$

The Second Moment Method

- Let X be the number of satisfying assignments. We will try to show that $F_k(n, m)$ is satisfiable with positive probability using

$$\Pr[X > 0] \geq \frac{\mathrm{E}[X]^2}{\mathrm{E}[X^2]}$$

- True for any non-negative random variable X; proof by Cauchy-Schwartz

Overlaps and Correlations

- For any truth assignment, the probability it satisfies a random clause *c* is $p = 1 - 2^{-k}$, and so $\mathrm{E}[X] = 2^n p^m = (2p^r)^n$.

- $\mathrm{E}[X^2]$ is the expected number of *pairs* of satisfying assignments. If s, t have *overlap* α, the probability they both satisfy *c* is

$$q(\alpha) = 1 - 2 \cdot 2^{-k} + \alpha^k 2^{-k}$$

- Note $q(1/2) = p^2$ (as if s, t were independent)

A Little Asymptotic Combinatorics

- Stirling's approximation gives

$$\mathrm{E}[X^2] = 2^n \sum_{z=0}^{n} \binom{n}{z} q(z/n)^m$$

$$\sim \frac{1}{\sqrt{n}} \sum_{z=0}^{n} g(z/n)^n \sim \sqrt{n} \int_0^1 g(\alpha)^n \,\mathrm{d}\alpha$$

- where $g(\alpha) = 2\mathrm{e}^{h(\alpha)} q(\alpha)^r$

$$[h(\alpha) = -\alpha \ln \alpha - (1-\alpha)\ln(1-\alpha)]$$

Laplace's Method

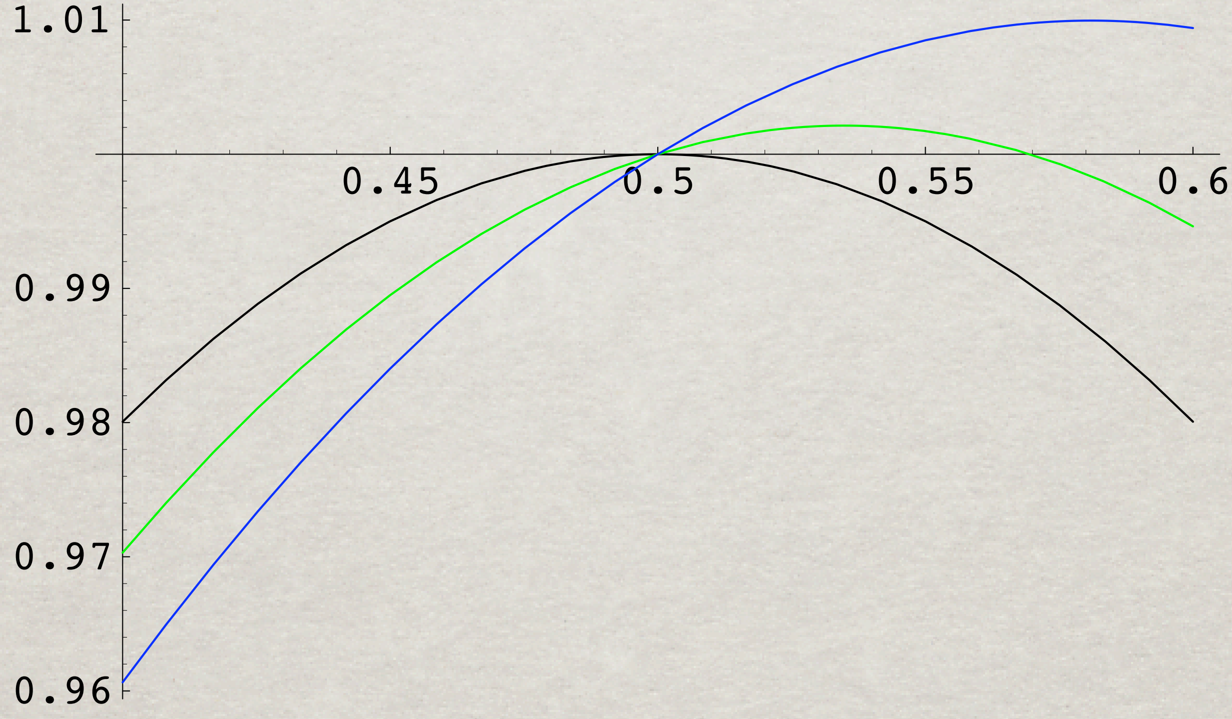
- For any smooth function $g(\alpha)$,

$$\int g(\alpha)^n \, \mathrm{d}\alpha \sim \sqrt{\frac{2\pi}{n} \frac{g_{\max}}{|g''_{\max}|}} \, g_{\max}^n$$

- Approximate the integrand by a Gaussian.
- So, $\mathrm{E}[X^2] = C g_{\max}^n$.
- We have $g(1/2) = (2p^r)^2$, matching $\mathrm{E}[X]^2$.
- If $\alpha = 1/2$ is the max, then $\mathrm{E}[X]^2 / \mathrm{E}[X^2] \geq 1/C$.

A Disturbing Lack of Symmetry

- For 3-SAT, sadly, $g'(1/2) > 0$:



- Failure: $\mathrm{E}[X]^2/\mathrm{E}[X^2]$ is exponentially small unless $k = \log n + \omega(1)$ [Frieze & Wormald]

An Attractive Force

- Where does this asymmetry come from?
- $q(\alpha)$ grows monotonically with α: satisfying assignments s, t have an "attractive force" between them.
- Moreover, both s and t are attracted to the majority assignment.
- How can we cancel this attraction?

Not-All-Equal SAT

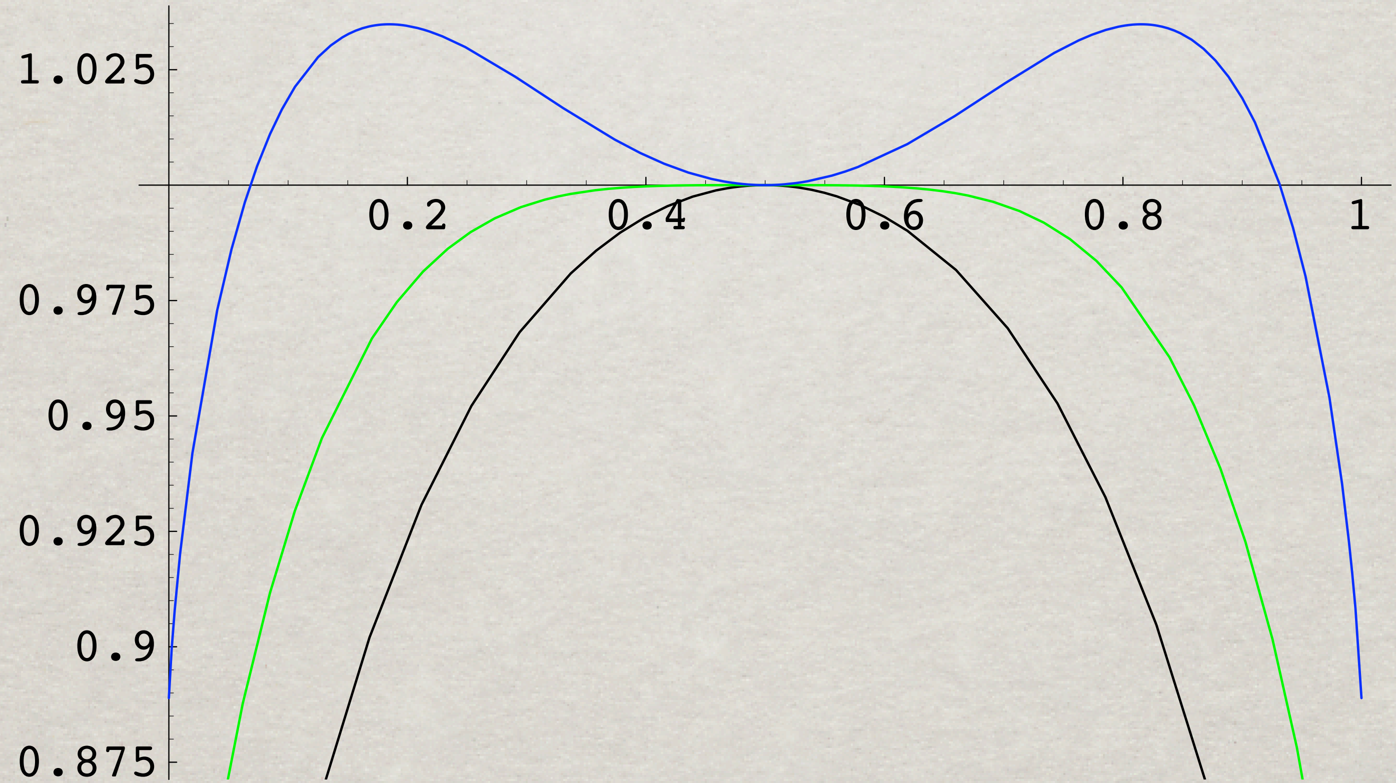
- What if we demand that each clause contain both a true literal and a false one?
- Equivalently, only count the assignments such that both s and $\bar{s}$ satisfy the formula.
- Now the probability s, t both satisfy c is

$$q(\alpha) = 1 - 2 \cdot 2^{1-k} + (\alpha^k + (1-\alpha)^k) 2^{1-k}$$

- This is symmetric around $\alpha = 1/2$.

Symmetry Regained

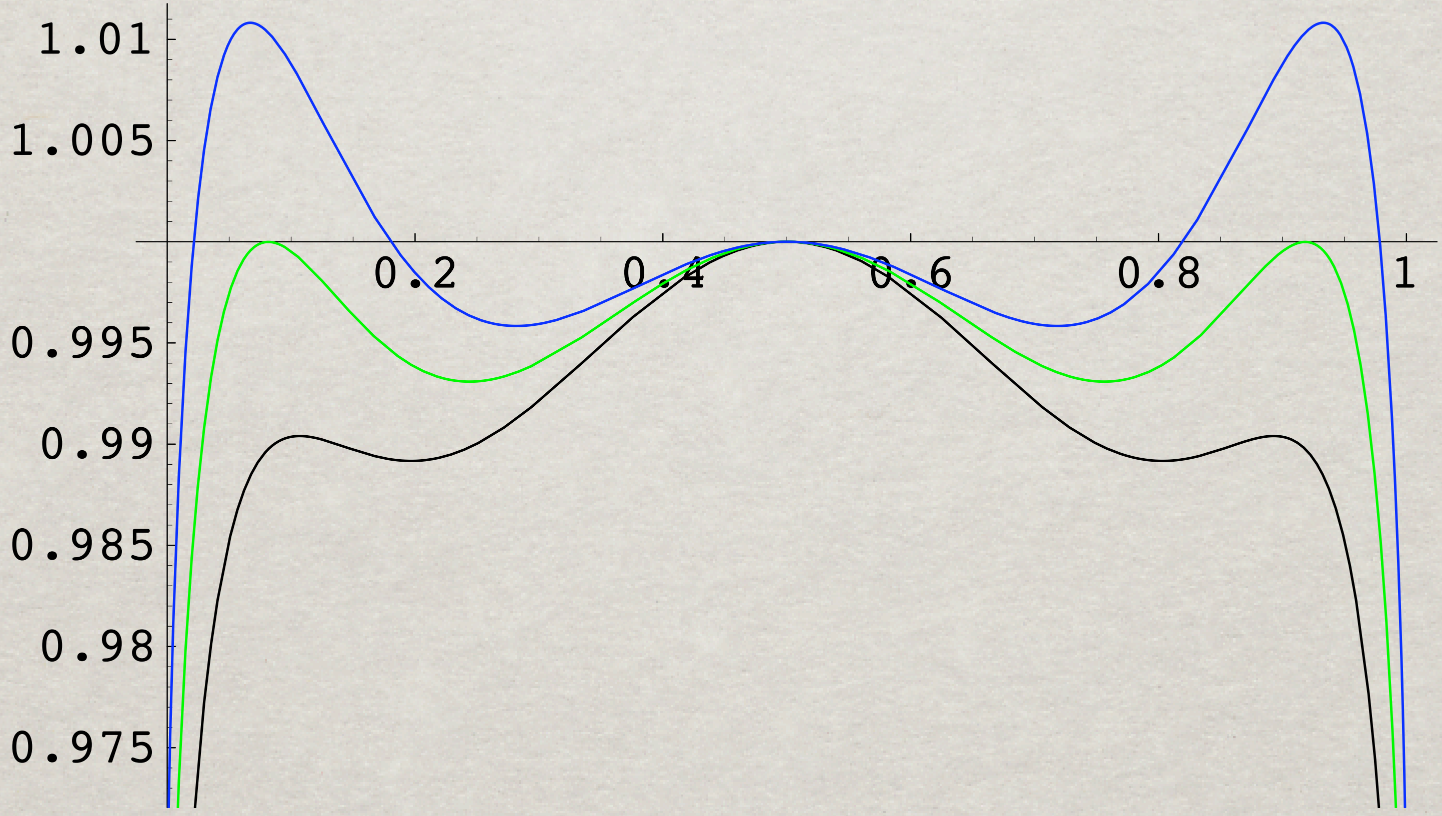
- Now $g'(1/2) = 0$, and for sufficiently small r:



- Thus we have $\mathrm{E}[X]^2/\mathrm{E}[X^2] \geq C$.

Symmetry Regained

- For k-SAT with larger k, side maxima appear:



- These are below $g(1/2)$ for small enough r.

Tight Bounds for NAESAT

- For NAE k-SAT, refined first moment gives

$$r_k < 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1}{4}$$

- And our second moment bound gives

$$r_k > 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1}{2} - o(1)$$

k	3	4	5	6	7	8	9	10
$r_k >$	$3/2$	$49/12$	9.973	21.190	43.432	87.827	176.570	354.027
$r_k <$	2.214	4.969	10.505	21.590	43.768	88.128	176.850	354.295

Closing the Asymptotic Gap

- This brings our upper and lower bounds to within a multiplicative constant:

$$2^{k-1}\ln 2 - O(1) < r_k < 2^k \ln 2$$

- And proves the conjecture that

$$r_k = \Theta(2^k)$$

- Can we narrow the gap even further?

Closing the Factor of 2

- A more fine-tuned way to restore symmetry
  [Achlioptas and Peres, STOC 2003]

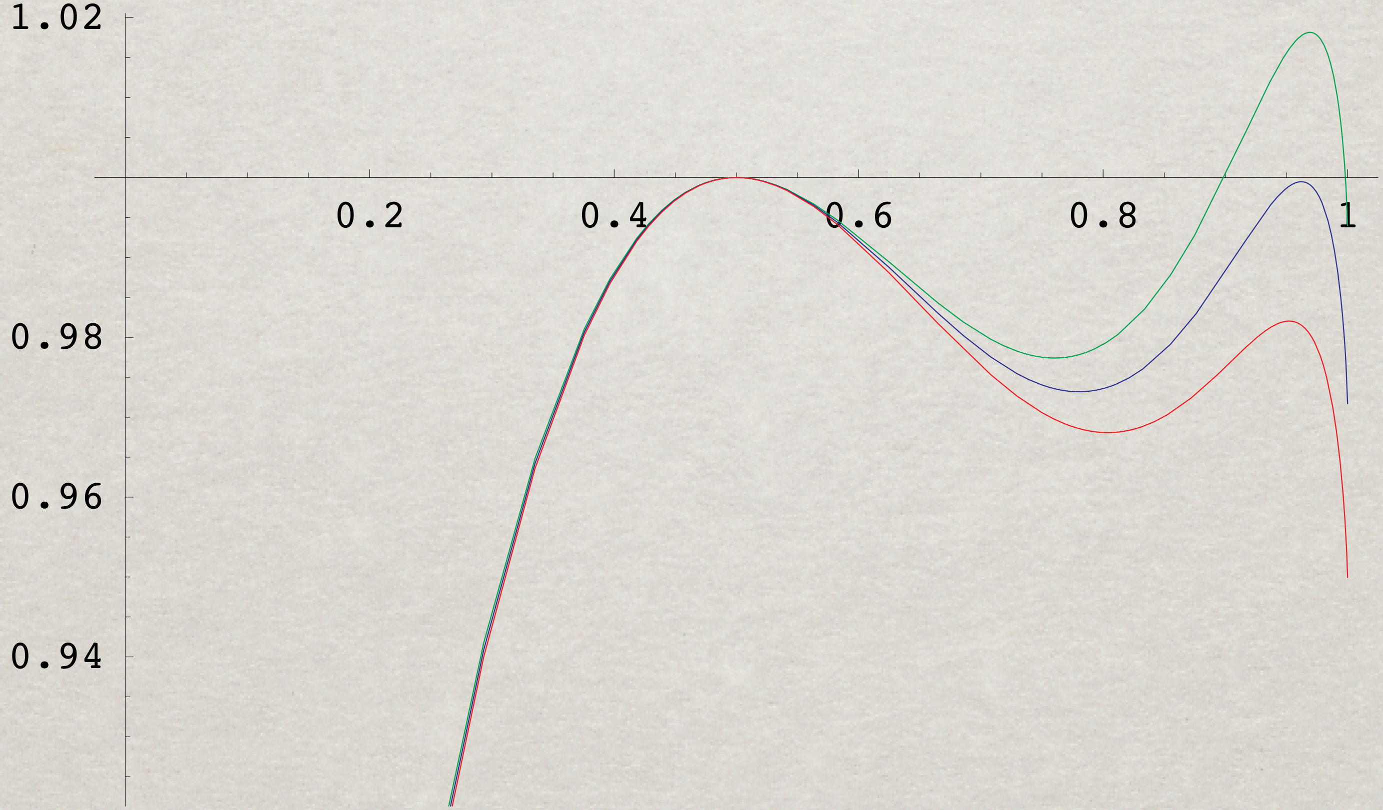
- Let X be the sum over satisfying assignments of

$$\prod_c \eta^{\#\text{ of satisfied literals in } c}$$

- Idea: $\eta < 1$ discourages the majority assignment

Closing the Factor of 2

- The right value of η restores local symmetry:



- Implies $r^k > 2^k \ln 2 - O(k)$: within $1 + o(1)$!

More Applications of the Second Moment

- Hypergraph 2-Coloring, or "Property B" [Achlioptas & Moore]
- MAX k-SAT [Achlioptas, Naor, Peres]
- Graph Coloring on G(n,p) [Achlioptas & Naor] and random regular graphs [Achlioptas & Moore]

A Conjecture About Graph Coloring

- Let $A = (a_{ij})$ be a doubly-stochastic matrix. Is the function

$$\left(1 - \frac{2}{k} + \sum_{ij} a_{ij}^2\right)^{d/2} \exp\left(-\sum_{ij} a_{ij} \ln a_{ij}\right)$$

- maximized by matrices of the form

$$A = b\mathbb{1} + cJ?$$

- This would determine d_k to within $O(1)$.

Acknowledgments