Probabilistic Method and Random Graphs

Lecture 10. Second Moment Method and Lovász Local Lemma

Xingwu Liu

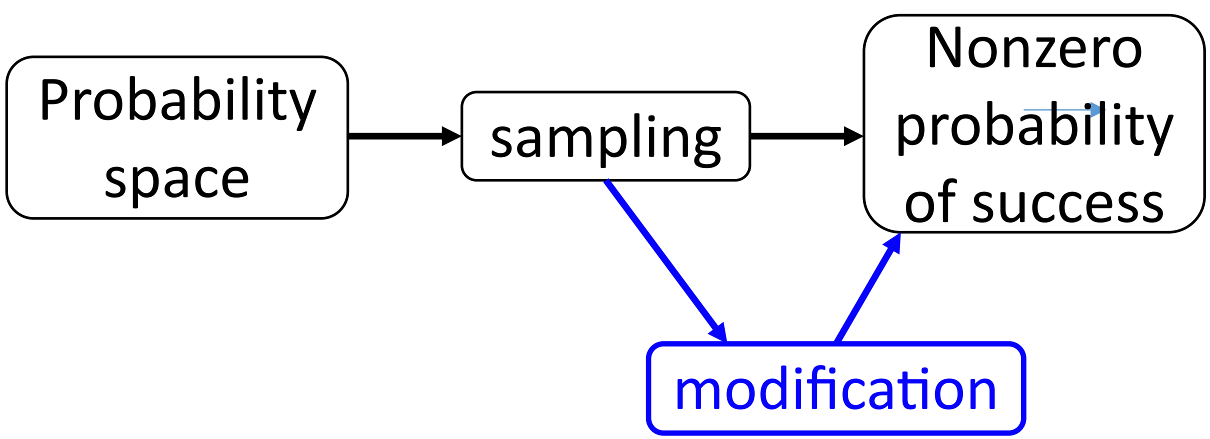
Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China

[1]The slides are mainly based on Chapter 6 of Probability and Computing.

Comments, questions, or suggestions?

Recap of Lecture 9

- Derive a deterministic algorithm from expectation argument
- Markov's Ine.: graphs with arbitrarily big girth and chro. number



First Moment method

Recap of Lecture 9

- Chebyshev's Ine.: $\Pr(|X - \mathbb{E}[X]| \geq a) \leq \frac{\mathrm{Var}[X]}{a^2}$
- $\Pr(X = 0) \leq \Pr(|X - \mathbb{E}[X]| \geq \mathbb{E}[X]) \leq \frac{Var[X]}{\mathbb{E}[X^2]} \leq \frac{\mathrm{Var}[X]}{(\mathbb{E}[X])^2}$
  - When $X \geq 0$, $\Pr(X > 0) > \frac{(\mathbb{E}[X])^2}{\mathbb{E}[X^2]}$
  - $\Pr(X > \theta\mathbb{E}[X]) \geq \frac{(1-\theta)^2(\mathbb{E}[X])^2}{\mathrm{Var}[X]+(1-\theta)^2(\mathbb{E}[X])^2}$

$$\geq (1-\theta)^2 \frac{(\mathbb{E}[X])^2}{\mathbb{E}[X^2]}, \theta \in (0,1)$$

Second moment method

- Application: Distinct Subset sum problem

Main Probabilistic Methods

- Counting argument
- First-moment method
- Second-moment method
- Lovasz local lemma

Application: threshold function

- Consider a property P of random graph $G_{n,p}$
- Threshold function $t(n)$ for P is such that

$$\lim_{n\to\infty} \Pr\big(G_{n,p} \text{ has } P\big) = \begin{cases} 0 \text{ if } p = o(t(n)) \\ 1 \text{ if } p = \omega(t(n)) \end{cases}$$

- Example (clique number $c(G)$: max clique size)
  - P: $c(G) \geq 4$
  - $t(n) = n^{-\frac{2}{3}}$ is its threshold function

Proof: when $p = o(n^{-\frac{2}{3}})$

- S: a 4-subset of the n vertices
- X_S: indicator of whether S spans a clique
- $X = \sum_S X_S$: the number of 4-cliques
- $\mathbb{E}[X] = \binom{n}{4} p^6 < \frac{n^4 p^6}{24}$
- By Markov's inequality

$$\Pr(c(G) \geq 4) = \Pr(X > 0)$$
$$\leq \mathbb{E}[X] < \frac{n^4 p^6}{24} = o(1)$$

Proof: when $p = \omega(n^{-\frac{2}{3}})$

- To derive $\Pr(X > 0) \to 1$
  - By Chebychev's Ineq.: $\Pr(X = 0) \leq \frac{\mathrm{Var}[X]}{(\mathbb{E}[X])^2}$
  - Try to show $\mathrm{Var}[X] = o(\mathbb{E}[X])^2$
- Recall $\mathrm{Var}[X] = \sum \mathrm{Var}[X_S] + \sum_{S \neq T} \mathrm{Cov}(X_S, X_T)$
- X_S is an indicator $\Rightarrow \mathrm{Var}[X_S] \leq \mathbb{E}[X_S]$
- $\mathrm{Cov}(X_S, X_T) \leq \mathbb{E}[X_S X_T] = \Pr(X_S = 1, X_T = 1)$

  $= \mathbb{E}[X_S]\Pr(X_T = 1 | X_S = 1)$

  And $\mathrm{Cov}(X_S, X_T)$=0 if independent

Proof: estimating the variance

- $\mathrm{Var}[X] \le \mathbb{E}[X] + \sum \mathbb{E}[X_S] \sum_{T\sim S} \Pr(X_T = 1 | X_S = 1)$
  $= \sum \mathbb{E}[X_S] \Delta_S$
- $\Delta_S = 1 + \sum_{|T\cap S|=2} \Pr(X_T = 1 | X_S = 1)$
  $+ \sum_{|T\cap S|=3} \Pr(X_T = 1 | X_S = 1)$
  $= 1 + \binom{n-4}{2}\binom{4}{2} p^5 + \binom{n-4}{1}\binom{4}{3} p^3$
  $= o(n^4 p^6) = o(\mathbb{E}[X])$
- $\mathrm{Var}[X] = o(\mathbb{E}[X]^2) \Rightarrow \Pr(X = 0) \le \frac{\mathrm{Var}[X]}{\mathbb{E}[X]^2} = o(1)$
  $\Rightarrow \Pr(X > 0) \to 1$

Main Probabilistic Methods

- Counting argument
- First-moment method
- Second-moment method
- Lovász local lemma

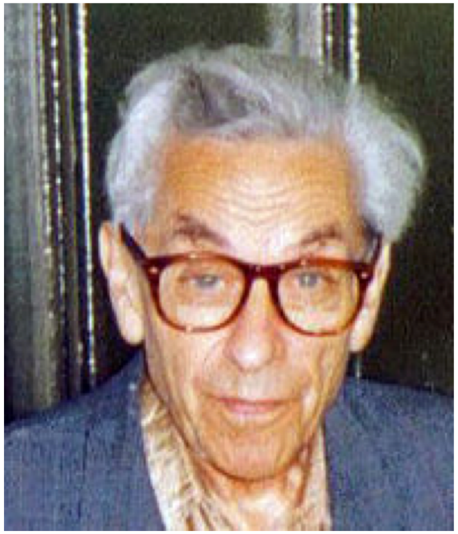
Lovász local lemma: motivation

- Can we avoid all bad events?
- Given bad events $A_1, A_2, \ldots A_n$, is $\Pr(\cap_i \overline{A_i}) > 0$?
  - Applicable to SAT, coloring, Ramsey theory…
- Two special cases
  - $\sum_i \Pr(A_i) < 1 \Rightarrow \Pr(\cap_i \overline{A_i}) \geq 1 - \sum_i \Pr(A_i) > 0$
  - Independent $\Rightarrow \Pr(\cap_i \overline{A_i}) = \prod(1 - \Pr(A_i)) > 0$
- What if *almost* independent?

Lovász local lemma: symmetric version

- Dependency graph
  - Undirected simple graph on $S = \{A_1, A_2, \ldots A_n\}$
  - A_i is independent of its non-neighborhood $S \backslash \Gamma^+(A_i)$
    - $\Gamma(A_i) \triangleq \Gamma^+(A_i) \backslash \{A_i\}$
- **Theorem**: $\Pr(\cap_i \overline{A_i}) > 0$ if
  1. $\forall i, \Pr(A_i) \leq p, |\Gamma(A_i)| \leq d$ and
  2. $4pd \leq 1$
- By Erdös&Lovász in 1973 to Erdös 60$^{\text{th}}$ birthday

Lovász



Erdos

Lovász local lemma: proof

- Standard trick
  - Chain rule: $\Pr(\cap_i \overline{A_i}) = \prod_{i=1}^{n} \Pr(\overline{A_i} | \cap_{j=1}^{i-1} \overline{A_j})$
    - Valid only if each $\cap_{j=1}^{i-1} \overline{A_j}$ has nonzero probability
  - Hold if each term $\Pr\left(\overline{A_i} \middle| \cap_{j=1}^{i-1} \overline{A_j}\right) > 0$
- **Claim**: for any $t \geq 0$ and $A, B_1, B_2, \dots B_t \in S$,

  1. $\Pr(\cap_{j=1}^{t} \bar{B}_j) > 0$

  2. $\Pr\left(A \middle| \cap_{j=1}^{t} \bar{B}_j\right) < \frac{1}{2d}$

Inductive proof of the claim

- **Basis**: $t = 0$. Both 1 and 2 of the claim hold
- **Hypothesis**: the claim holds for all $t' < t$
- **Induction**
  - For **1**, $\Pr\left(\bigcap_{j=1}^{t} \overline{B_j}\right)$
    $$= \Pr\left(\overline{B_t} \mid \bigcap_{j=1}^{t-1} \overline{B_j}\right) \Pr\left(\bigcap_{j=1}^{t-1} \overline{B_j}\right) > 0$$
  - For **2**, let $\{C_1, \ldots C_x\} = \{B_1, \ldots B_t\} \cap \Gamma(A)$, and
    $$\{D_1, \ldots D_y\} = \{B_1, \ldots B_t\} \backslash \Gamma(A)$$
    - $x \leq d, x + y = t$

Proof: induction for 2

- If $x = 0$, A is independent of $\{B_1, \dots B_t\}$ and $\Pr\left(A \middle| \cap_{j=1}^{t} \overline{B_j}\right) = \Pr(A) < \frac{1}{2d}$
- Assume $x > 0$. Then $y < t$.
  - $\Pr\left(A \middle| \cap_{j=1}^{t} \overline{B_j}\right) = \frac{\Pr(A \cap (\cap_{j=1}^{t} \overline{B_j}))}{\Pr(\cap_{j=1}^{t} \overline{B_j})}$

$$\leq \frac{\Pr\left(A \cap (\cap \overline{D_j})\right)}{\Pr\left((\cap \overline{C_j}) \cap (\cap \overline{D_j})\right)} = \frac{\Pr\left(A | \cap \overline{D_j}\right)}{\Pr\left((\cap \overline{C_j}) | \cap \overline{D_j}\right)}$$

$$= \frac{\Pr(A)}{1 - \Pr\left((\cup C_j) | \cap \overline{D_j}\right)} < \frac{p}{1 - \frac{d}{2d}} \leq \frac{1}{2d}$$

General case

Application to (k,s)-SAT

- (k,s)-CNF
  - Any clause has k literals
  - Any literal appears in at most s clauses
- Theorem: Any (k,s)-CNF is satisfiable if $s \leq \frac{1}{4}\frac{2^k}{k}$
  - Randomly assign values to the Boolean variables
  - A_i: the event that the ith clause is not satisfied
  - $\Pr(\bigcap \overline{A_i}) > 0 \Leftrightarrow$ satisfiable
  - $p = \Pr(A_i) = 2^{-k}, \;\; d \leq ks$
  - $s \leq \frac{1}{4}\frac{2^k}{k} \Rightarrow 4pd \leq 1 \Rightarrow \Pr(\bigcap \overline{A_i}) > 0 \Rightarrow$ satisfiable

Application to Ramsey Number $R(k)$

- Counting argument: $R(k) \geq k2^{\frac{k}{2}}\left[\frac{1}{e\sqrt{2}} + o(1)\right]$ [1947]
- Best result: $R(k) \geq k2^{\frac{k}{2}}\left[\frac{\sqrt{2}}{e} + o(1)\right]$ [1975, Spencer]
  - Randomly color edges of K_n in red/blue
  - S: a k-subset of the vertices
  - A_S: S is monochromatic
  - $p = \Pr(A_S) = 2^{1-\binom{k}{2}}$, $d \leq \binom{k}{2}\binom{n}{k-2}$
  - By Stirling's formula, $4pd \leq 1$ if $n \leq k2^{\frac{k}{2}}\left[\frac{\sqrt{2}}{e} + o(1)\right]$
- Can we say something about $R(k,t)$?

Non-symmetric LLL

- **Theorem**: $\Pr(\cap_i \overline{A_i}) > 0$ if $\forall i, \sum_{j\in\Gamma(A_i)} \Pr(A_j) < \frac{1}{4}$
  - [Spencer, 1975]
  - The sense of "local"
- Follow the proof of symmetric LLL, with induction on m to show that $\Pr\left(A \middle| \cap_{j=1}^{m} \bar{B}_j\right) < 2\Pr(A)$
- Application to $R(k,t)$:

$$R(k,t) > t^{\frac{\binom{k}{2}-2}{k-2}+o(1)}$$ with k fixed and $t \to \infty$

Proof: $R(k,t) > t^{\frac{\binom{k}{2}-2}{k-2}+o(1)}$

- Randomly color edges of K_n, p in red, $(1-p)$ in blue
- S: a k-set of the vertices; T: a t-set of the vertices
- A_S: S is a red clique; B_T: T is a blue clique
- $\Pr(A_S) = p^{\binom{k}{2}}$,$\Pr(B_T) = (1-p)^{\binom{t}{2}}$
- Any event has at most $\binom{t}{2}\binom{n}{k-2}$ neighbors being A_S,

  at most $\binom{n}{t}$ neighbors being B_T
- Let $p = n^{-\epsilon-\beta+\delta}$, $t = n^{\beta+\epsilon}$, $\beta = \frac{k-2}{\binom{k}{2}-2}$, $0 < \delta < \epsilon$,

  we have $\binom{t}{2}\binom{n}{k-2}p^{\binom{k}{2}} + \binom{n}{t}(1-p)^{\binom{t}{2}} < \frac{1}{4}$

Open problem

A stronger non-symmetric LLL

- $\Pr(\cap \overline{A_i}) > 0$ if there are $x_1, x_2, \dots, x_n \in (0,1)$ s.t. $\forall i, \Pr(A_i) \leq x_i \prod_{j \in \Gamma(A_i)} (1 - x_j)$
  - Similar proof, but
    - Prove $\Pr\left(A_i \middle| \cap_{j=1}^{t} \overline{B_j}\right) \leq x_i$
    - Use chain rule to lower-bound the numerator $\Pr\left(\cap \overline{C_j} \mid \cap \overline{D_j}\right)$ by $\prod_{j \in \Gamma(A_i)} (1 - x_j)$
  - Spencer, 1977

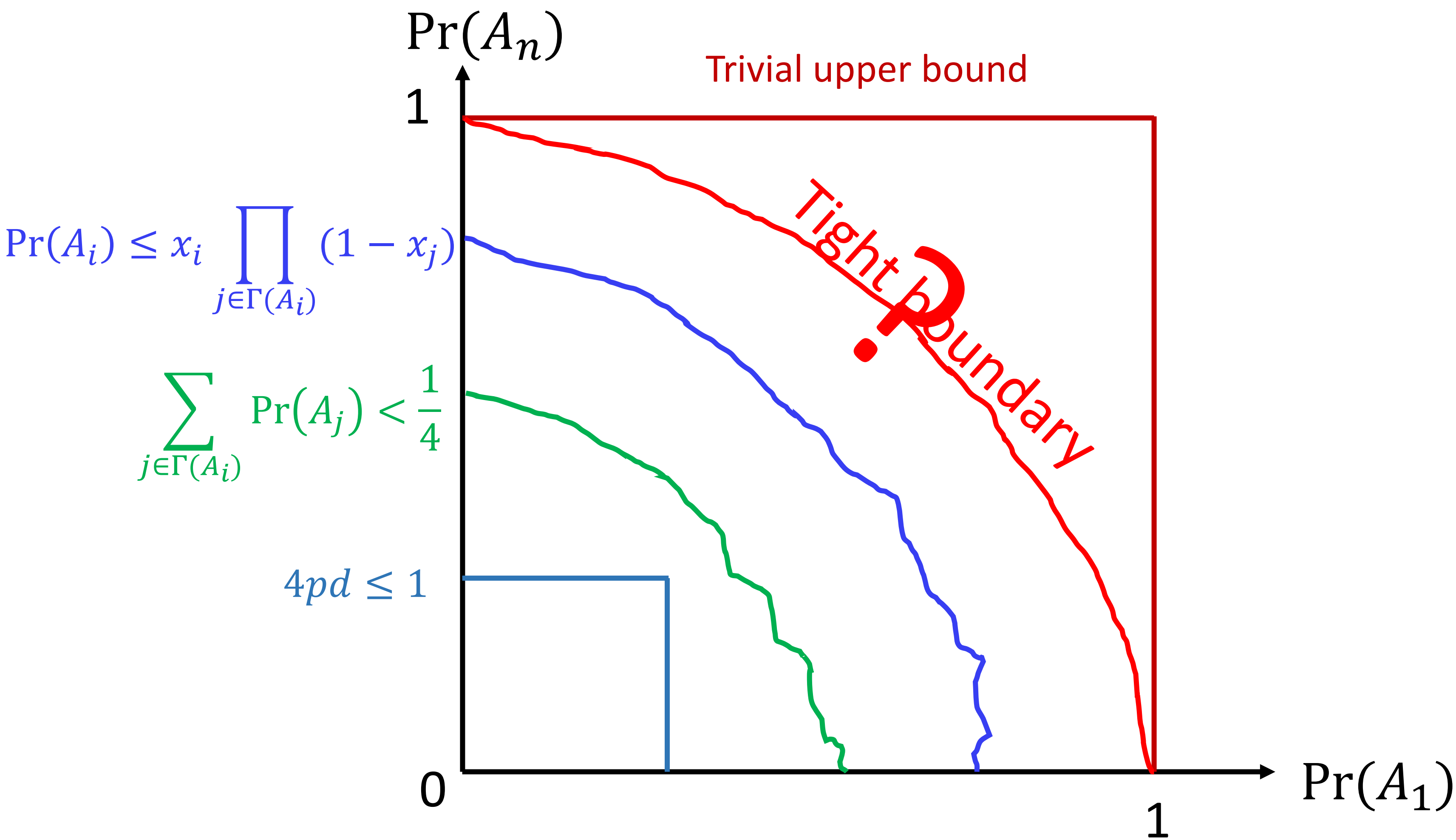
$$R(k,t) \geq c\left(\frac{t}{\ln t}\right)^{\frac{k+1}{2}}(1-o(1))$$

- Follow the proof of $R(k,t) > t^{\frac{\binom{k}{2}-2}{k-2}+o(1)}$
  - Define events A_S and B_T for any k-set S and t-set T
  - Let $p = c_1 n^{-\beta}$, $t = c_2 n^{\beta} \ln n$, $x_S = (1+\epsilon)\Pr(A_s)$
    $x_T = e^{c_3 n^{\beta} \ln^2 n} \Pr(A_s)$, with $\beta = \frac{2}{k+1}$, $\epsilon > 0$
  - Apply LLL
- Best until 2010
  - Bohman&Keevash: $R(k,t) \geq c\left(\frac{t}{\ln t}\right)^{\frac{k+1}{2}}(\ln t)^{\frac{1}{k-2}}$

Major open problem

- Determine $\alpha(k)$ s.t. $R(k,t) = t^{\alpha(k)+o(1)}$
- Spencer 1975: $\alpha(k) \geq \frac{\binom{k}{2}-2}{k-2}$
- Spencer 1977: $\alpha(k) \geq \frac{k+1}{2} = \frac{\binom{k}{2}-1}{k-2}$
  - Best for 40+ years
  - How tight is it?
- $\alpha(k) \leq k-1$ since $R(k,t) \leq \binom{k+t-2}{k-1}$
- Conjecture: $\alpha(k) = k-1$
  - Yes for $k = 3$
  - Unknown for larger k

- This local lemma is so strong. Is it ultimate?



Local lemma is to determine a curve surrounding a *safe zone.*

Safe: $\Pr(\cap_i \overline{A_i}) > 0$ any set of events with the probabilities

Tight Bound of Lovász local lemma

- General (Non-symmetrical) case
- $\Pr(\cap \overline{A_i}) > 0$ if

$\forall S \in \mathrm{ind}(G),\ \sum_{\substack{T \supseteq S \\ T \in \mathrm{ind}(G)}} (-1)^{|T \setminus S|} \prod_{i \in T} p_i > 0$

- By James B. Shearer @IBM in 1985

James Shearer

Tight Bound of Lovász local lemma

- Symmetrical case
- $\Pr(\cap \overline{A_i}) > 0$ if

$$p < \begin{cases} \dfrac{(d-1)^{d-1}}{d^d} & \text{when } d > 1 \\ \dfrac{1}{2} & \text{when } d = 1 \end{cases}$$

- Corollary: $\Pr(\cap \overline{A_i}) > 0$ if $edp \leq 1$

Application

- Any (k,s)-CNF is satisfiable if $s \leq \frac{1}{e}\frac{2^k}{k}$
  - Known: satisfiable if $s \leq \frac{1}{4}\frac{2^k}{k}$
  - Tight bound of s: $\left(\frac{2}{e} + o\left(\frac{1}{\sqrt{k}}\right)\right)\frac{2^k}{k}$ [Gebauer et al. 2011]
  - Can we efficiently find a satisfying assignment?

Algorithmic aspects

- **Like** other probabilistic methods, LLL proves existence non-constructively
- **Unlike** other probabilistic methods, LLL doesn't lead to efficient algorithms
  - Directly sampling has an *exponentially small* lower bound of success probability
  - Say, $\Pr(\cap \overline{A_i}) \geq \prod(1 - x_i)$ for general version
- Is there an efficient, constructive proof?

Constructive Lovász Local Lemma

- Initiated by Joszef Beck in 1991
  - Under strong conditions on neighborhood size
  - In terms of coloring, SAT …
- Breakthrough by Robin Moser&Gabor Tardos in 2009, Kashyap Kolipaka and Mario Szegedy in 2011
  - Events are generated by independent random variables
  - If Shearer's condition is met, an assignment s.t. none events occurs can be found in linear time

Joszef Beck

Gabor Tardos

Mario Szegedy

The assignment algorithm

For $X \in \mathcal{X}$ do

  $v_X \leftarrow$ a random evaluation of X

EndFor

While (some A occurs) do

  Arbitrarily pick an event A that occurs

  For $X \in \mathrm{vbl}(A)$ do

    $v_X \leftarrow$ a random evaluation of X

  EndFor

EndWhile

Return $(v_X)_{X \in \mathcal{X}}$

- $\mathrm{vbl}\ (A) \subset \Upsilon$: the set of variables determining A

Directions of LLL research

- Local conditions
  - Cluster LLL
  - Random walk
- Algorithms (Inspired by Moser&Tardos)
  - Efficient beyond Shearer's bound?
  - Efficient for abstract events?

Comparing probabilistic methods

- All dependent vs almost independent
  - Counting (union bound): mutually exclusive
  - First moment: linearity doesn’t care dependence
  - Second moment: pairwise dependence
  - LLL: global dependence

References

- Spencer. Ramsey's theorem-A new lower bound. 1975
- Spencer. Asymptotic lower bounds for Ramsey functions. 1977
- James B. Shearer. On a Problem of Spencer. 1985
- Robin Moser and Gabor Tardos. A constructive proof of the general Lovasz Local Lemma. 2009
- Polipaka and Szegidy. Moser and Tardos Meet Lovász. 2011

- http://www.openproblemgarden.org/

Thank you