Lovász Local Lemma

Oriol Serra

Univ. Politècnica de Catalunya
Barcelona

Cargèse Fall School on Random Graphs, September 2015

Outline

- The Local Lemma. Examples. Lopsided version.
- Counting with the Local Lemma: the device of Lu and Székely. Examples
- Algorithmic version of LLL by Moser and Tardos

The Lovász Local Lemma

Theorem (LLL, Erdős-Lovász, 1975)

Let $A_1, \ldots, A_n$ be events in a probability space. Let $C_1, \ldots, C_n \subset [n]$ such that A_i is independent of $\{A_j : j \in C_i\}$ for each i.
If there are numbers $x_1, \ldots, x_n \in (0,1)$ such that

$$\Pr(A_i) \leq x_i \prod_{j \in [n] \setminus C_j} (1 - x_j), \; i = 1, \ldots, n,$$

then

$$\Pr(\cap_i \overline{A_i}) \geq \prod_{j \in [n]} (1 - x_j).$$

The Lovász Local Lemma

Theorem (LLL, Erdős-Lovász, 1975)

Let $A_1, \ldots, A_n$ be events in a probability space. Let $C_1, \ldots, C_n \subset [n]$ such that A_i is independent of $\{A_j : j \in C_i\}$ for each i.
If there are numbers $x_1, \ldots, x_n \in (0,1)$ such that

$$\Pr(A_i) \le x_i \prod_{j \in [n] \setminus C_j} (1 - x_j), \; i = 1, \ldots, n,$$

then

$$\Pr(\cap_i \overline{A_i}) \ge \prod_{j \in [n]} (1 - x_j).$$

- If the events $A_1, \ldots, A_n$ are independent then the statement is obvious. The LLL is useful when dependencies are rare.
- The directed graph $G = ([n], E)$ with $(i,j) \in E$ iff $j \in [n] \setminus C_i$ is a dependency graph for the events $A_1, \ldots, A_n$.
- The LLL has been used in many applications of the probabilistic method, including graph coloring, Ramsey theory, combinatorial number theory.

First examples

Theorem (Erdős-Lovász, 1975)

For $k \geq 9$ every k–uniform and k–regular hypergraph H admits a 2–coloring with no monochromatic edges.

First examples

Theorem (Erdős-Lovász, 1975)

For $k \geq 9$ every k–uniform and k–regular hypergraph H admits a 2–coloring with no monochromatic edges.

- Define a random 2–coloring of H by giving each vertex the color red or blue with probability $p = 1/2$ independently.

First examples

Theorem (Erdős-Lovász, 1975)

For $k \geq 9$ every k–uniform and k–regular hypergraph H admits a 2–coloring with no monochromatic edges.

- Define a random 2–coloring of H by giving each vertex the color red or blue with probability $p = 1/2$ independently.
- For each edge $e \in E(H)$ define A_e the event that e is monochromatic. $\Pr(A_e) = 2^{-(k-1)}$.

First examples

Theorem (Erdős-Lovász, 1975)

For $k \geq 9$ every k–uniform and k–regular hypergraph H admits a 2–coloring with no monochromatic edges.

- Define a random 2–coloring of H by giving each vertex the color red or blue with probability $p = 1/2$ independently.
- For each edge $e \in E(H)$ define A_e the event that e is monochromatic. $\Pr(A_e) = 2^{-(k-1)}$.
- The events $A_e, A_{e'}$ are independent if $e \cap e' = \emptyset$: each A_e is independent with all but at most $k(k-1)$ events.

First examples

Theorem (Erdős-Lovász, 1975)

For $k \geq 9$ every k–uniform and k–regular hypergraph H admits a 2–coloring with no monochromatic edges.

- Define a random 2–coloring of H by giving each vertex the color red or blue with probability $p = 1/2$ independently.
- For each edge $e \in E(H)$ define A_e the event that e is monochromatic. $\Pr(A_e) = 2^{-(k-1)}$.
- The events $A_e, A_{e'}$ are independent if $e \cap e' = \emptyset$: each A_e is independent with all but at most $k(k-1)$ events.
- By setting $x = x_1 = \cdots = x_m$, $m = |E(H)|$, if $2^{-(k-1)} \leq x(1-x)^{k(k-1)}$ then (LLL) the probability that no edge is monochromatic is at least $(1-x)^{k(k-1)}$.

LLL: Symmetric version

Theorem (LLL, Erdős-Lóvasz, 1975)

Let $A_1, \ldots, A_n$ *be events in a probability space. Let* $C_1, \ldots, C_n \subset [n]$ *such that* A_i *is independent of* $\{A_j : j \in C_i\}$ *for each* i*.*
If there are numbers $x_1, \ldots, x_n \in (0,1)$ *such that*

$$\Pr(A_i) \leq x_i \prod_{j \in [n] \setminus C_j} (1 - x_j), \ i = 1, \ldots, n, \tag{1}$$

then

$$\Pr(\cap_i \overline{A_i}) \geq \prod_{j \in [n]} (1 - x_j).$$

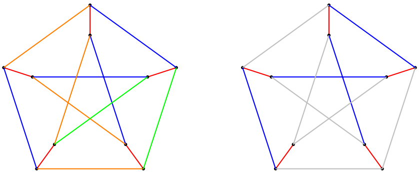
If $\Pr(A_i) \leq p$, $i = 1, \ldots, n$, and every event is independent with all but at most d events, then (1) can be replaced by

$$ep(d+1) \leq 1$$

and the conclusion by $\Pr(\cap_i \overline{A_i}) \geq e^{-nx(1+o(1))}$ by setting $x_i = 1/(d+1)$. The constant e is best possible [Shearer, 1981]

Acyclic edge–coloring

A proper edge–coloring of a graph G is acyclic if every two colors induce a forest.



$a(G)$ acyclic chromatic number

G Δ–regular, $a(G) \geq \Delta(G) + 1$, $a(K_{2n}) \geq \Delta(K_{2n}) + 2$.

Conjecture (Alon, Sudakov, Zaks)

$a(G) \leq \Delta(G) + 2$ *for all graphs* G

Acyclic edge–coloring

Theorem (Alon, Sudakov, Zaks)

There is a constant c such that $g(G) \geq c\Delta \log \Delta$ implies $a(G) \leq \Delta(G) + 2$.

- Take a proper edge–coloring of G with $\leq \Delta + 1$ colors (Vizing)

Acyclic edge–coloring

Theorem (Alon, Sudakov, Zaks)

There is a constant c such that $g(G) \geq c\Delta \log \Delta$ implies $a(G) \leq \Delta(G) + 2$.

- Take a proper edge–coloring of G with $\leq \Delta + 1$ colors (Vizing)
- Change the color of each edge independently with probability p to a new color $\Delta + 2$

Acyclic edge–coloring

Theorem (Alon, Sudakov, Zaks)

There is a constant c such that $g(G) \geq c\Delta \log \Delta$ *implies* $a(G) \leq \Delta(G) + 2$.

- Take a proper edge–coloring of G with $\leq \Delta + 1$ colors (Vizing)
- Change the color of each edge independently with probability p to a new color $\Delta + 2$
- Define 'bad' events
  - A_B: the incident edges $B = \{e, e'\}$ receive color $\Delta + 2$,
  - A_C: the bichromatic cycle C gets no $\Delta + 2$ color,
  - A_D: the cycle D with half the edges monochromatic gets the other half with color $\Delta + 2$,

Acyclic edge–coloring

Theorem (Alon, Sudakov, Zaks)

There is a constant c such that $g(G) \geq c\Delta \log \Delta$ implies $a(G) \leq \Delta(G) + 2$.

- Take a proper edge–coloring of G with $\leq \Delta + 1$ colors (Vizing)
- Change the color of each edge independently with probability p to a new color $\Delta + 2$
- Define 'bad' events
  - A_B: the incident edges $B = \{e, e'\}$ receive color $\Delta + 2$, $Pr(A_{e,e'}) = p^2$
  - A_C: the bichromatic cycle C gets no $\Delta + 2$ color, $Pr(A_C) = (1 - p)^{l(C)}$
  - A_D: the cycle D with half the edges monochromatic gets the other half with color $\Delta + 2$, $Pr(A_D) \leq 2p^{l(D)/2}$
- A_X is independent with all A_Y with $X \cap Y = \emptyset$: all but at most $2x\Delta$ 'A_B's, $x\Delta$ 'A_C's and $2x\Delta^{l(D)/2-1}$ 'A_D's. $(x = |X|)$

Acyclic edge–coloring

Theorem (Alon, Sudakov, Zaks)

There is a constant c such that $g(G) \geq c\Delta \log \Delta$ implies $a(G) \leq \Delta(G) + 2$.

- Take a proper edge–coloring of G with $\leq \Delta + 1$ colors (Vizing)
- Change the color of each edge independently with probability p to a new color $\Delta + 2$
- Define ‘bad’ events
  - A_B: the incident edges $B = \{e, e'\}$ receive color $\Delta + 2$, $Pr(A_{e,e'}) = p^2$
  - A_C: the bichromatic cycle C gets no $\Delta + 2$ color, $Pr(A_C) = (1 - p)^{l(C)}$
  - A_D: the cycle D with half the edges monochromatic gets the other half with color $\Delta + 2$, $Pr(A_D) \leq 2p^{l(D)/2}$
- A_X is independent with all A_Y with $X \cap Y = \emptyset$: all but at most $2x\Delta$ ‘A_B’s, $x\Delta$ ‘A_C’s and $2x\Delta^{l(D)/2-1}$ ’A_D’s. ($x = |X|$)
- Choose appropriate p and x_i’s (here large girth is used) and apply LLL

Acyclic edge–coloring

Theorem (Alon, Sudakov, Zaks)

There is a constant c such that $g(G) \geq c\Delta \log \Delta$ implies $a(G) \leq \Delta(G) + 2$.

The best current result is

Theorem (Cai, Perarnau, Reed, Watts (2015))

For every $\epsilon > 0$ there are $\Delta_0 = \Delta_0(\epsilon)$ and $g = g(\epsilon)$ such that a graph G with girth g and maximum degree $\delta \geq \delta_0$ has acyclic chromatic number at most

$$a(G) \leq (1+\epsilon)\Delta.$$

Proof of LLL

If there are numbers $x_1, \ldots, x_n$ such that

$$\Pr(A_i) \leq x_i \prod_{j \in [n] \setminus C_i} (1 - x_j),\ i = 1, \ldots, n,$$

then

$$\Pr(\cap_i \overline{A_i}) \geq \prod_{j \in [n]} (1 - x_j).$$

- $\Pr(\cap_{i=1}^n \overline{A_i}) = \Pr(\overline{A_1}) \Pr(\overline{A_2} | \overline{A_1}) \Pr(\overline{A_3} | \overline{A_2} \cap \overline{A_1}) \cdots \Pr(\overline{A_n} | \cap_{i=1}^{n-1} \overline{A_i})$.
- For each $J \subset [n]$ and $i \notin J$, $\Pr(A_i | \cap_{j \in J} \overline{A_j}) \leq x_i$.
  By induction on $j = |J|$. Set $J_1 = J \setminus C_i$ and $J_2 = J \cap C_i$

$$\Pr(A_i | \cap_{j \in J} \overline{A_j}) = \frac{\Pr(A_i \cap (\cap_{j \in J_1} \overline{A_j}) | \cap_{j \in J_2} \overline{A_j})}{\Pr(\cap_{j \in J_1} \overline{A_j} | \cap_{j \in J_2} \overline{A_j})} \leq \frac{\Pr(A_i)}{\prod_{j \in [n] \setminus C_i} (1 - x_i)}$$

  To bound the denominator use induction: $J_1 = \{j_1, \ldots, j_r\}$

$$\Pr(\cap_{j \in J_1} \overline{A_j} | \cap_{j \in J_2} \overline{A_j}) = \Pr(\overline{A_{j_1}} | \cap_{j \in J_2} \overline{A_j}) \Pr(\overline{A_{j_2}} | \overline{A_{j_1}} \cap_{j \in J_2} \overline{A_j}) \cdots \Pr(\overline{A_{j_r}} | \cap_{s=1}^{r-1} \overline{A_s} \cap_{j \in J_2}$$

Proof of LLL

If there are numbers $x_1, \dots, x_n$ such that

$$\Pr(A_i | \cap_{j\in J} \overline{A_j}) \le x_i \prod_{j\in[n]\setminus C_i} (1-x_j),\ i = 1,\dots,n,\ J\subset C_i$$

then

$$\Pr(\cap_i \overline{A_i}) \ge \prod_{j\in[n]} (1-x_j).$$

- $\Pr(\cap_{i=1}^n \overline{A_i}) = \Pr(\overline{A_1}) \Pr(\overline{A_2}|\overline{A_1}) \Pr(\overline{A_3}|\overline{A_2}\cap\overline{A_1}) \cdots \Pr(\overline{A_n}| \cap_{i=1}^{n-1} \overline{A_i})$.
- For each $J \subset [n]$ and $i \notin J$, $\Pr(A_i| \cap_{j\in J} \overline{A_j}) \le x_i$.
  By induction on $j = |J|$. Set $J_1 = J \setminus C_i$ and $J_2 = J \cap C_i$

$$\Pr(A_i| \cap_{j\in J} \overline{A_j}) = \frac{\Pr(A_i \cap (\cap_{j\in J_1}\overline{A_j})| \cap_{j\in J_2} \overline{A_j})}{\Pr(\cap_{j\in J_1}\overline{A_j}| \cap_{j\in J_2} \overline{A_j})} \le \frac{\Pr(A_i)}{\prod_{j\in[n]\setminus C_i}(1-x_i)}$$

To bound the denominator use induction: $J_1 = \{j_1, \dots, j_r\}$

$$\Pr(\cap_{j\in J_1}\overline{A_j}|\cap_{j\in J_2}\overline{A_j}) = \Pr(\overline{A_{j_1}}|\cap_{j\in J_2}\overline{A_j}) \Pr(\overline{A_{j_2}}|\overline{A_{j_1}}\cap_{j\in J_2}\overline{A_j}) \cdots \Pr(\overline{A_{j_r}}|\cap_{s=1}^{r-1}\overline{A_s}\cap_{j\in J_2}$$

Lopsided LLL

Theorem (Erdős, Spencer, 1991)

Let $A_1, \dots, A_n$ *be events in a probability space. Let* $C_1, \dots, C_n \subset [n]$ *and* $x_1, \dots, x_n \in (0,1)$ *such that*

$$\Pr(A_i | \cap_{j\in J} \overline{A_j}) \le x_i \prod_{j\in J} (1-x_j), \; i = 1, \dots, n, \; J \subset [n] \setminus C_i$$

then

$$\Pr(\cap_i \overline{A_i}) \ge \prod_{j\in[n]} (1-x_j).$$

- A graph G with vertex set $\{A_1, \dots, A_n\}$ is a negative dependence graph if

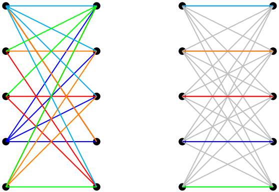
$$\Pr(A_i | \cap_{j\in J} \overline{A_j}) \le \Pr(A_i), \; i = 1, \dots, n, \; J \subset N[A_i]$$

- Independency can be replaced by negative correlation.

Rainbow matchings

Theorem (Erdős, Spencer, 1991)

Every edge–coloring of $K_{n,n}$ in which every color is used at most $k \leq n/4e$ times contains a rainbow matching.

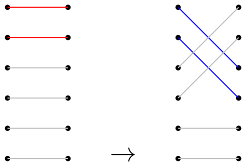


Rainbow matchings

Theorem (Erdős, Spencer, 1991)

Every edge–coloring of $K_{n,n}$ in which every color is used at most $k \leq n/4e$ times contains a rainbow matching.

- Choose a random matching M
- $A_{e,e'}$: the monochromatic pair $\{e, e'\}$ of independent edges is in M.
- Define a graph G on these events where $A_{e,e'}$ is adjacent to $A_{u,u'}$ whenever $\{e, e'\} \cap \{u, u'\} = \emptyset$: its maximum degree is at most $4nk$.
- $\Pr(A_{e,e'} | \cap_{\{u,u'\} \in J} \overline{A_{u,u'}}) \leq 1/n(n-1)$ for all set J of pairs nonincident with e, e'.



- G is a negative dependency graph and probabilities of bad events are small enough: aply LLLL (symmetric version)

Rainbow matchings

Theorem (Erdős, Spencer, 1991)

Every edge–coloring of $K_{n,n}$ in which every color is used at most $k \leq n/4e$ times contains a rainbow matching.

- A Latin transversal in a Latin square is equivalent to a rainbow matching of a proper edge–coloring of $K_{n,n}$ ($k = n$) (Ryser, Brualdi–Stein conjectures for Latin squares)
- Every proper edge–coloring of $K_{n,n}$ contains a rainbow matching of size $n - c\log^2 n$ (Hatami-Shor, 2008).
- Every graph which is the union of n edge–disjoint matchings with size $n + o(n)$ has a rainbow matching (Prokovsky 2015; Haggkvist-Johansson 2008) (Aharoni-Berger conjecture is that size $n + 1$ is enough)

Part 2: A counting device with LLLL

LLL provides a lower bound

$$\Pr(\cap_i \overline{A_i}) \geq \prod_i (1 - x_i).$$

A graph G on $\{A_1, \ldots, A_n\}$ is an ϵ–near positive dependency graph if

- $\Pr(A_i \cap A_j) = 0$ for $ij \in E(G)$ and
- $\Pr(A_i | \cap_{j \in S} \overline{A_j}) \geq (1 - \epsilon) \Pr(A_i), \ \forall S \subset V \setminus N[A_i]$.

Theorem (Lu, Székely)

If G is an ϵ–near positive dependency graph on $A_1, \ldots, A_k$ then

$$\Pr(\cap_i \overline{A_i}) \leq \prod_i (1 - (1 - \epsilon) \Pr(A_i)).$$

Combination of the two bounds give tight asymptotic enumeration of derangements, latin rectangles,...

A counting device with LLLL

Theorem (Lu, Székely, 2009)

If G is an ϵ–near positive dependency graph on $A_1, \dots, A_k$ then

$$\Pr(\cap_i \overline{A_i}) \geq \prod_i (1 - (1-\epsilon)\Pr(A_i)).$$

- $\Pr(\cap_{i=1}^n \overline{A_i}) = \Pr(\overline{A_1})\Pr(\overline{A_2}|\overline{A_1})\Pr(\overline{A_3}|\overline{A_2}\cap\overline{A_1})\cdots\Pr(\overline{A_n}|\cap_{i=1}^{n-1}\overline{A_i})$.
- For each $J \subset [n]$ and $i \notin J$, $\Pr(A_i|\cap_{j\in J}\overline{A_j}) \geq (1-\epsilon)\Pr(A_i)$.
  Set $J_1 = J \cap N(A_i)$ and $J_2 = J \setminus N(A_i)$

$$\Pr(A_i|\cap_{j\in J}\overline{A_j}) = \frac{\Pr(A_i \cap (\cap_{j\in J_1}\overline{A_j})|\cap_{j\in J_2}\overline{A_j})}{\Pr(\cap_{j\in J_1}\overline{A_j}|\cap_{j\in J_2}\overline{A_j})} \geq \Pr(A_i|\cap_{j\in J_2}\overline{A_j})$$

Example: Enumeration of rainbow matchings

$K_{n,n}$ edge–colored, each color appears at most n/k times.

G graph with vertex set $\mathcal{M} = \{A_{e,e'} : \{e, e'\}$ monochromatic pair$\}$ and eges $A_{e,e'}, A_{u,u'}$ whenever $\{e, e'\} \cap \{u, u'\} \neq \emptyset$.

- G is a negative dependency graph.
  - $\Pr(\cap_{i=1}^{n} \overline{A_i}) \geq e^{-(1+16/k)\mu}$, $\mu = \sum_{(e,e')\in\mathcal{M}} \Pr(A_{e,e'})$.
  - Actually, for $I \cap J = \emptyset$, $\Pr(\cap_{i\in I} \overline{A_i} | \cap_{j\in J} \overline{A_j}) \geq \prod_{i\in I}(1 - x_i)$.
- G is an ϵ–near positive dependence graph with $\epsilon = 1 - e^{-(2/k+32/k^2+o(1))}$.
  - $\Pr(A_{e,e'} \cap A_{u,u'}) = 0$ for adjacent events.
  - With $B = \cap_{j\in J} \overline{A_j}$,

$$\Pr(A_i|B) \geq (1-\epsilon)\Pr(A_i) \Leftrightarrow \Pr(B|A_i) \geq (1-\epsilon)\Pr(B)$$

  - $\Pr(B|A_i) = \Pr(B')$, B' an event in $K_{n-2,n-2}$.
    Use LLLL to in it to get the desired lower bound.

Example: Enumeration of rainbow matchings

Theorem (Perarnau, Serra, 2013)

The number $z_{n,k}$ of rainbow perfect matchings in a proper edge coloring of $K_{n,n}$ which uses each color at most n/k times, $k \geq 12$, $n \geq 200$, satisfies

$$c_1^n n! \leq z_{n,k} \leq c_2^n n!.$$

for some $0 < c_1 < c_2 < 1$ which depend only on k.

- Vardi Conjecture: The number z_n of latin transversals of the cyclic group of order n satisfies

$$c_1^n n! < z_n < c_2^n n!$$

  for some constants $0 < c_1 < c_2 < 1$.

- (McKay, McLeod, Wanless, 2006; Cavenagh, Greenhill, Wanless, 2008)

$$a^n < z_n < b^n \sqrt{n} n!$$

  where $a = 3.246$ and $b = 0.614$.

Counting with LLL: A general framework for matchings

- $\mathcal{M}$ a collection of (partial) matchings of K_{2n} or $K_{n,n}$
- A_M denotes the family of matchings extending $M \in \mathcal{M}$.
- $G_{\mathcal{M}}$ graph with vertex set $\{A_M : M \in \mathcal{M}\}$ and A_M adjacent to $A_{M'}$ whenever $M \cup M'$ is not a matching (conflicting).

Theorem (Lu and Székely, 2009)

$G_{\mathcal{M}}$ is a negative dependence graph.

- $\mathcal{M}$ is δ–sparse, $\delta < 1/16r$, $r = \max_{M \in \mathcal{M}} |M|$ if
  - $\mathcal{M}$ is an antichain (by inclusion)
  - $\sum_i \Delta_i p(n,i) \leq 1/8r - \delta$, Δ_i max degree of the hypergraph of matchings with i edges.
  - For each F, $\sum_{M \in N(F) \cap C} q(n,M) \leq \delta$, C set of nonconflicting with F.

Theorem (Lu and Székely, 2009)

$G_{\mathcal{M}}$ is an ϵ–near–positive dependence graph for some (specific) $\epsilon = \epsilon(\delta, r, d_i)$.

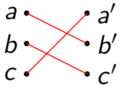
Counting with LLL: A general framework for matchings

Theorem (Lu and Székely, 2009)

Let $\mathcal{M}$ be a regular familiy of matchings of K_{2n} or $K_{n,n}$ and $\mu = \sum_M \Pr(A_M)$. If $\mathcal{M}$ is δ–sparse, $\delta = o(\mu^{-1})$ and $\mu = o(\sqrt{n} r^{-3/2})$ then

$$\Pr(\cap \overline{A_M}) = (1 + o(1))e^{-\mu}.$$

- Derangements: $\mathcal{M}$ the edges (i, i) of $K_{n,n}$. $r = \mu = 1$.
- k–cicle free permutations: $\mathcal{M}$ k–matchings sending K to K' which are minimal with this property. $r = k, \mu = 1/k$, one can choose $\delta = 1/n$.

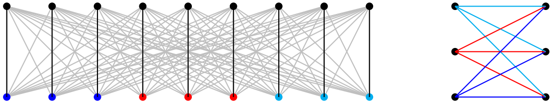


- Latin rectangles, enumeration of d–regular graphs, ...

(A pause) Rainbow matchings with random colorings

Random edge–coloring of $K_{n,n}$ with $s = kn$ colors, $k \geq 1$.

- Uniform model: Choose randomly and independently one of s colors for each edge of $K_{n,n}$
  All edge–colorings of $K_{n,n}$ with at most s colors appear with the same probability.
- Regular model: Choose a perfect matching in K_{n^2,n^2}. Identify one stable set with $E(K_{n,n})$ and partition the other one in s parts (colors) with n/k elements each.
  All equitable edge–colorings of $K_{n,n}$ using each of s colors n/k times appear with the same probability.



(A pause) Rainbow matchings with random colorings

Theorem (Perarnau, Serra, 2013)

Every random edge–coloring of $K_{n,n}$ in the uniform or regular models has a rainbow matching whp.

Uniform model

- X_M indicator function that M is rainbow. $X = \sum_M X_M$.

$$\mathbb{E}(X) = n!\mathbb{E}(X_M) = n!\Pr(X_M = 1) = \prod_{i=1}^{n}\left(1 - \frac{i}{s}\right) = n!e^{-(c(k)+o(1))n},$$

- $\Pr(X = 0) \le \mathbb{E}(|X - \mu_X| \ge \mu_X) \le \sigma_X^2/\mu_X^2 = O(n^{-1})$ (second moment method)

$$\mathbb{E}(X_M X_N) = \Pr(X_M = 1)\Pr(X_N = 1|X_M = 1) = e^{\frac{\alpha(z)z^2}{2s}}\Pr(X_M = 1).$$

$z = |M \cap N|$, and upper bound the number of pairs M, N with $z = |M \cap N|$.

(A pause) Rainbow matchings with random colorings

Theorem (Perarnau, Serra, 2013)

Every random edge–coloring of $K_{n,n}$ in the uniform or regular models has a rainbow matching whp.

- One gets $\Pr((K_{n,n},c)$ has a rainbow matching$) = e^{-(c(k)+o(1))n/k}$.
- Unfortunately Pr(random edge coloring is proper) $\sim e^{-n^2}$: too small for an a.a.s. to Ryser conjecture.
- There are more than $(n/2)^{n^2}$ edge–colorings of $K_{n,n}$ with n colors which do not contain rainbow matchings:

$$\Pr((K_{n,n},c) \text{ has no rainbow matching}) \geq 1/2^{n^2}.$$

- There is no good model for random Latin squares.

Part 3: Algorithmic version of LLL

Lóvasz proof is nonconstructive:
can we find an element in $\cap_i \overline{A_i}$ (which has small probability)

- Beck (1991) proposes an algorithm with certain constrains.
- Particular examples (e.g. acyclic coloring) have been worked out.
- Moser (2008) finds an elegant simple solution to the algorithmic issue.

Theorem (Moser, Tardos (2010))

Let $X_1, \ldots, X_m$ be independent random variables.
Let $A_1, \ldots, A_n$ be events such that A_i is determined by $\{X_i : i \in C_i\}$ (but is independent of the remaining variables). Set the dependency graph with edge $A_i A_j$ whenever $C_i \cap C_j \neq \emptyset$.
If there are numbers $x_1, \ldots, x_n \in (0,1)$ such that $\Pr(A_i) \le x_i \prod_{j \in N[A_i]} (1 - xj)$ then $\Pr(\cap_i \overline{A_i}) > 0$.
Moreover a point in $\cap_i \overline{A_i}$ can be found by a randomized algorithm in expected time at most $\sum_i x_i/(1-x_i)$.

Algorithmic version of LLL

The proof of the theorem consists of an algorithm which finds a point in $\cap_i \overline{A_i}$.

MT Algorithm

for all $j = 1, \ldots, m$
    $v_j \leftarrow$ a random evaluation of X_j
while some A_i occurs
    choose A_i occurring
    for all $X_j \in C_i$
        $v_j \leftarrow$ a new random evaluation of X_j
return $(v_1, \ldots, v_m)$

Algorithmic version of LLL

for all $j = 1, \ldots, m$
    $v_j \leftarrow$ a random evaluation of X_j
while some A_i occurs
    choose A_i occurring
    for all $X_j \in C_i$
        $v_j \leftarrow$ a new random evaluation of X_j
return $(v_1, \ldots, v_m)$

Analysis of the algorithm

- $C = (E_1, E_2, \cdots, E_t, \cdots)$ the log of the algorithm, $E_t \in \{A_1, \ldots, A_n\}$ the event resampled at step t.

Algorithmic version of LLL

for all $j = 1, \ldots, m$
  $v_j \leftarrow$ a random evaluation of X_j
while some A_i occurs
  choose A_i occurring
  for all $X_j \in C_i$
    $v_j \leftarrow$ a new random evaluation of X_j
return $(v_1, \ldots, v_m)$

Analysis of the algorithm

- $C = (E_1, E_2, \cdots, E_t, \cdots)$ the log of the algorithm, $E_t \in \{A_1, \ldots, A_n\}$ the event resampled at step t.
- Construct a witness rooted tree $\tau(C, t)$ recursively (backwards) as follows:

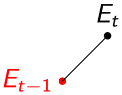
Place E_t at the root.

Algorithmic version of LLL

for all $j = 1, \ldots, m$
  $v_j \leftarrow$ a random evaluation of X_j
while some A_i occurs
  choose A_i occurring
  for all $X_j \in C_i$
    $v_j \leftarrow$ a new random evaluation of X_j
return $(v_1, \ldots, v_m)$

Analysis of the algorithm

- $C = (E_1, E_2, \cdots, E_{t-1}, E_t, \cdots)$ the log of the algorithm, $E_t \in \{A_1, \ldots, A_n\}$ the event resampled at step t.
- Construct a witness rooted tree $\tau(C, t)$ recursively (backwards) as follows:



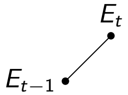
Look for the neighbour of E_{t-1} in the dependency graph deepest in the tree and add E_{t-1} as a child to it.

Algorithmic version of LLL

for all $j = 1, \dots, m$
  $v_j \leftarrow$ a random evaluation of X_j
while some A_i occurs
  choose A_i occurring
  for all $X_j \in C_i$
    $v_j \leftarrow$ a new random evaluation of X_j
return $(v_1, \dots, v_m)$

Analysis of the algorithm

- $C = (E_1, E_2, \cdots, E_{t-2}, E_{t-1}, E_t, \cdots)$ the log of the algorithm, $E_t \in \{A_1, \dots, A_n\}$ the event resampled at step t.
- Construct a witness rooted tree $\tau(C, t)$ recursively (backwards) as follows:



Look for the neighbour of E_{t-1} in the dependency graph deepest in the tree and add E_{t-1} as a child to it.
If no neighbour of E_{t-2} is in the tree then leave the tree untouched.

Algorithmic version of LLL

for all $j = 1, \ldots, m$
    $v_j \leftarrow$ a random evaluation of X_j
while some A_i occurs
    choose A_i occurring
    for all $X_j \in C_i$
        $v_j \leftarrow$ a new random evaluation of X_j
return $(v_1, \ldots, v_m)$

Analysis of the algorithm

- Such a labeled rooted tree τ appears in the (random) C if $\tau = \tau(C, t)$ for some t. $\mathcal{T}_A$ is the family of trees rooted at A.
- If the event A is resampled N_A times, then there are N_A distinct trees occurring in C rooted at A.
- the probability that τ appears in C is at most $\prod_{E \in V(\tau)} \Pr(E)$. (We assume we pick evaluations of variables from a sequence)

$$\mathbb{E}(N_A) = \sum_{\tau \in \mathcal{T}_A} \Pr(\tau \text{ appears in } C) = \sum_{\tau \in \mathcal{T}_A} \prod_{E \in V(\tau)} \Pr(E).$$

Algorithmic version of LLL

for all $j = 1, \ldots, m$
    $v_j \leftarrow$ a random evaluation of X_j
while some A_i occurs
    choose A_i occurring
    for all $X_j \in C_i$
        $v_j \leftarrow$ a new random evaluation of X_j
return $(v_1, \ldots, v_m)$

Analysis of the algorithm

- For a given tree $\tau \in \mathcal{T}_A$ we consider the Galton-Watson tree rooted at A where at each step we add a child $A_j \in N[B]$ to each vertex B independently with probability x_j.
- The probability that the resulting tree is τ is

$$p_\tau = \frac{x_i}{1 - x_i} \prod_{A_j \in V(\tau)} \left(x_j \prod_{A_r \in N[A_j]} (1 - x_r) \right).$$

Algorithmic version of LLL

for all $j = 1, \ldots, m$
    $v_j \leftarrow$ a random evaluation of X_j
while some A_i occurs
    choose A_i occurring
    for all $X_j \in C_i$
        $v_j \leftarrow$ a new random evaluation of X_j
return $(v_1, \ldots, v_m)$

Analysis of the algorithm

- From the assumptions on $\Pr(A_j) \leq x_j \prod_{A_r \in N[A_j]}(1 - x_r)$, if $A = A_i$

$$\mathbb{E}(N_A) = \sum_{\tau \in \mathcal{T}_A} \prod_{E \in V(\tau)} \Pr(E) \leq \frac{x_i}{1 - x_i} \sum_{\tau \in \mathcal{T}_A} p_\tau \leq \frac{x_i}{1 - x_i}.$$

- The algorithm terminates in expected time at most $\sum_{i=1}^{n} \frac{x_i}{1-x_i}$

Acyclic coloring again

Theorem (Esperet, Parreau (2013), Giotis. Kirousis, Psaromiligkos, Thillikos (2015))

The acyclic chromatic number of a graph G with maximum degree Δ is at most

$$a(G) \leq 4\Delta - 4.$$

- G can be edge–colored with $2\Delta - 1$ colors to obtain a proper coloring with no bichromatic 4–cycles.
- Order the edges of G, $e_1, \ldots, e_n$, and the even cycles. Use $K = \lceil (2+\gamma)(\Delta - 1) \rceil + 1$ colors.
- At step i color e_i randomly subject to preserve 4–acyclicity.
- If a bichromatic $2k$–cycle appears, choose C the smallest such one and Recolor(C)

Recolor(C)

- Recolor the edges of C preserving 4–acyclicity
- While some edge of C belongs to a bichromatic cycle, choose C' the smallest one and Recolor(C').

Algorithmic version of LLL

- The MT algorithm can be derandomized. For the symmetric case it provides a linear time algorithm.
- Several versions have been proposed. In particular for eliminating the condition on independent random variables.
- In applications explicit procedures for sampling the variables must be made explicit.
- By implementing the algorithm in particular problems some improvements may be obtained from known results.