# Randomized Algorithms

Michal Dvořák

November 19, 2021

## 1 Probabilistic method

**Definition 1.** For tournament $T = (V, E)$ define the property $p_k$ as follows. $T$ has a property $p_k$ if for each subset $S$ of size $k$ there is a vertex $p_S \notin S$ s.t. $(p_S, w) \in E$ for all $w \in S$ (we call such vertex a beater for $S$).

**Theorem 1.** *For each $k \in \mathbb{N}$ there exists a tournament $G$ on $n = n(k)$ vertices s.t. it has property $p_k$.*

**Lemma 1.1.** *If $n^k(1-2^{-k})^{n-k} < 1$, then there exists $n$-vertex tournament with the property $p_k$.*

*Proof.* Let $T$ be random tournament on $n$ in following sense. Fix $n$ vertices and for each pair $u, v$ flip a fair coin and either orient the edge from $u$ to $v$ or vice versa. Let $S \subseteq V$ be a set of size $k$. Probability that a vertex outside of $S$ is a beater for $S$ is $2^{-k}$. Thus the probability that a vertex is not a beater is $1-2^{-k}$. There are $n-k$ independent such vertices, thus the probability that $S$ violates the property $p_S$ is $(1-2^{-k})^{n-k}$. Let $W_S$ denote the event that $S$ does not have a beater. Then $P(\exists S : W_S) = P(\bigcup_{S \subseteq V, |S|=k} W_S) \leq \sum P(W_S) = \binom{n}{k}(1-2^{-k})^{n-k} \leq n^k(1-2^{-k})^{n-k}$ which is $< 1$ by assumption. So the probability of existence of such set is less than one. Thus the probability that in random tournament no such $S$ will exists is nonzero, so some tournament must satisfy the property $p_k$. ■

*Proof of the Theorem.* It suffices to show that for each $k$ there is $n := f(k)+k$ s.t. it satisfies $n^k(1-2^{-k})^{n-k}$. Instead, let's solve

$$n^k e^{-2^{-k}(n-k)} < 1$$

by inequality $1 - x \leq e^{-x}$. Taking logarithm of both sides, this can be rewritten to

$$k \log n < 2^{-k}(n-k)$$

we can upper bound $n$ by $n = f(k)+k \leq f(k)^2$ since $f(k) \in \Omega(2^k)$. Set $f(k) = 10 \cdot 2^k k^2$. Then the inequality becomes:

$$2k^2 + 4k \log k + \log 10 < 10k^2$$

which is true. ■

**Fact 1.** *For $k$ large enough, every tournament on $\Theta(k2^k)$ vertices does not have the property $p_k$.*

**Theorem 2.** *Let $G$ be a graph on $n$ vertices and let $\delta = \delta(G)$. Then $G$ has a dominating set $D$ of size $|D| \leq n\frac{1+\ln(\delta+1)}{\delta+1}$*

*Proof.* Pick $X \subseteq V$ at random where each vertex $v \in V$ is in $X$ with probability $p$. Let $|X|$ denote random variable with value corresponding to the size of $X$. Clearly $|X|$ has binomial distribution with parameters $n, p$. Thus $E|X| = np$. Probability that a vertex $v$ is not dominated by $X$ is $(1-p)^{\deg v} \leq (1-p)^{\deg v}$. Also, the probability that $v$ is outside of $X$ is $1-p$. So for any vertex, the probability that it is not dominated by $X$ is at most $(1-p)^{\delta+1}$. Let $Y$ denote the set of vertices not dominated by $X$. By the above, $E|Y| \leq n(1-p)^{\delta+1}$. Let $Z = X \cup Y$. Clearly $Z$ is a dominating set and $E|Z| = E|X| + E|Y|$ because $X$ and $Y$ are disjoint. But

$$E|Z| = E|X| + E|Y| \leq np + n(1-p)^{\delta+1}$$

In particular, there is some dominating set $Z$ for which $|Z| \leq n(p + (1-p)^{\delta+1})$. It remains to minimalize function $f(p) = p + (1-p)^{\delta+1}$. It suffices to minimize relaxation $p + e^{-p(\delta+1)}$. It is a straightforward calculus exercise to show that $p = \frac{\ln(\delta+1)}{\delta+1}$ is the optimum solution for the above. Thus

$$|Z| \leq n\frac{1 + \ln(\delta+1))}{\delta+1}$$

■

**Lemma 2.1.** *Let $G$ be a graph and $D$ inclusion-wise minimal dominating set for $G$. Then $\overline{D}$ is a dominating set for $G$.*

*Proof.* Assume, for the sake of contradiction, that there is a vertex $x$ not dominated by $\overline{D}$. Then $N[x] \subseteq D$. But then $D \setminus x$ is still a dominating set since $x$ can be dominated by one of his neighbours (he has atleast 1 because $\delta(G) \geq 1$) and he was not dominating anyone else because all his neighbours were in $D$. But $D \setminus x$ being a dominating set is a contradiction with the assumption that $D$ was inclusion-wise minimal. ■

**Corollary 1.** *In every graph $G$ with $\delta(G) \geq 1$ there is a dominating set of size at most $n/2$.*

*Proof.* Let $D$ be a inclusion-wise minimal dominating set. By the previous lemma, $\overline{D}$ is a dominating set. Now, one of $D, \overline{D}$ must have at most $n/2$ vertices. ■

**Theorem 3.** *Given a graph $G = (V, E)$, then $\alpha(G) \geq \sum_{v \in V} \frac{1}{\deg v + 1}$*

*Proof.* Consider graph $G$ and permute its vertices randomly. For each vertex in the permutation, if no vertex from its closed neighbourhood is included, then add him to the set $X$. The probability that a vertex was seen in the permutation before anyone else from his neighbours is $\frac{1}{\deg v+1}$. Thus the expected size of $X$ is $\sum_{v \in V} \frac{1}{\deg v+1}$. Therefore, there exists some independent set $I$ satisfying $|I| \geq \sum_{v \in V} \frac{1}{\deg v+1}$. The claim follows. ■

**Corollary 2** (Turán)**.** *For each $k$ an $n$-vertex graph which is $K_{k+1}$-free satisfies $|E(G)| \leq \frac{n^2(k-1)}{2k}$.*

*Proof.* TODO ■

**Theorem 4.** *There exists an $n$-vertex tournament with atleast $n!2^{-n+1}$ Hamiltonian paths.*

*Proof.* Consider random tournament $T$ in the sense that for each edge we flip a fair coin and decide its orientation. For any permutation of the vertices, probability that the given permutation forms a Hamiltonian path is $2^{-(n-1)} = 2^{-n+1}$. Summing up the probability over all permutations of the vertices yields the expected number of Hamiltonian paths $n!2^{-n+1}$. In particular, there is a tournament with atleast as many Hamiltonian paths. ■

**Theorem 5.** *Every graph admits a max-cut of size atleast $m/2$.*

*Proof.* Fix a graph on $n$ vertices and flip a fair coin for each vertex $v$ whether it belongs to $A$ or to $B$. For each edge, the probability that both of its ends are not both in $A$ or both in $B$ is $1/2$. So the expected number of edges in between $A$ and $B$ is $m/2$. In particular, there is a cut with atleast $m/2$ edges, so the claim follows. ■

## 2 Method of conditional expectations

Algorithm for max cut. Set $A = B = \emptyset$ at the beginning. Go over each $v \in V$ and if number of edges to $A$ is larger than number of edges to $B$ (in current step), add $v$ to $B$, otherwise to $A$.

**Theorem 6.** *The algorithm above always yields a cut of size atleast $m/2$.*

*Proof.* We show that at each step $k$ with current split $(A_k, B_k)$ there are completions $\overline{A}, \overline{B}$ s.t. $\overline{A}, \overline{B}$ is a bipartition of $V$ and edges in between $\overline{A}, \overline{B}$ is atleast $m/2$ and the number of edges going in between $(A_k, B_k)$ is atleast $\frac{1}{2}|E(A_k) \cup E(B_k)|$. It will follow that for $k = n$, the desired output of the algorithm is a cut of size atleast $m/2$.

We will show this by induction. For $k = 0$ the result follows from theorem 5. At time $k \geq 1$, we constructed $(A_{k-1}, B_{k-1})$ and are about to place $v_k$ in the algorithm. At $k$-th step we add atleast $1/2$ of all the edges between $v_k$ and $A_{k-1} \cup B_{k-1}$. By induction, the number of edges in between $(A_{k-1}, B_{k-1})$ is atleast $1/2|E(A_{k-1}) \cup E(B_{k-1})|$. Let $F$ be the edges inside $A_k \cup B_k$. For edges $E \setminus F$ a simillar argument as in 5 shows that there is a bipartite splitting with atleast $|E \setminus F|/2$ edges, thus the claim holds for the step $k$. ■

**Theorem 7.** *There is a deterministic algorithm which finds an independent set in given graph of size atleast* $\sum_{v \in V} \frac{1}{\deg v + 1}$.

*Proof.* We will iteratively build an independent set $I$, starting with $I = \emptyset$. Denote $G_0 = G$ – the input graph. We will consider graphs $G_1, \ldots, G_k$ in each step. In $i$-th step, we add one vertex from $G_{i-1}$ to $I$ and construct graph $G_i$. For each step $i$ and each vertex $v$, define a potential function $\varphi_i : v \mapsto \frac{1}{\deg_{G_i} v + 1}$.

In each step we choose a vertex $v$ with some potential $\varphi(v)$ ■

There are two types of randomized algorithms. *Las-Vegas* is a type of randomized algorithm where the result is correct and the expected running time should be good, while the worst-case might not. Example of such is QuickSort with expected running time $\Theta(n \log n)$ but $O(n^2)$ the worst case.

In *Monte-Carlo* algorithm, we allow the algorithm to produce a wrong answer but we bound the probability that this happens.

Every Las-Vegas algorithm $A$ with expected running time $T(n)$ can be turned into following Monte-Carlo algorithm. Run $A$ for $cT(n)$ steps and then stop it and if it didnt finish, output something random (maybe 42) or the result of $A$ if it did. Then probability that $A$ runs for more than $cT(n)$ steps is at most $1/c$ by Markov inequality which says for nonnegative random variable $T$

$$P(T \geq a) \leq \frac{E(T)}{a}$$

substituting $a = cE(T)$.

Now, we design a randomized Monte-Carlo algorithm for min-cut (Karger's algorithm). Let $\mathrm{mc}(G)$ denote the size of minimum cut in $G$. In the following, edge contractions will be preserving multi-edges and the input graph is generally a multigraph. Let $G/e$ denote the contraction of $e$ in $G$.

**Observation 1.** $\mathrm{mc}(G) \leq \mathrm{mc}(G/e)$

*Proof.* Every mincut of $G/e$ can be turned into a mincut of $G$ with the same size. ■

If $|V| = 2$, then the only cut in the graph is all the edges in between the two vertices, so output the edges in between the two vertices. Otherwise if $|V| \geq 3$, pick edge $e$ uniformly at random and let $G := G/e$ and repeat.

**Theorem 8.** *The probability that the above algorithm outputs correct answer is atleast* $p \geq 2/n^2$.

*Proof.* Let $\ell = \mathrm{mc}(G)$ and $C = \{c_1, \ldots, c_\ell\}$ the corresponding mincut in $G$. Let $E' = \{e_1, \ldots, e_{n-2}\}$ denote the set of randomly chosen edges by the algorithm. Then the algorithm outputs $C$ as a result if and only if $C \cap E' = \emptyset$. Because $\delta(G) \geq \mathrm{mc}(G)$. By the handshaking lemma $|E| \geq \frac{n\delta(G)}{2} \geq \frac{n\ell}{2} = \frac{n|C|}{2}$.

There is atleast one such minimum cut $C$. The probability that $e_1$ is in $C$ is

$$P[e_1 \in C] = \frac{|C|}{|E|} \leq \frac{2}{n}$$

so

$$P[e_1 \notin C] \geq 1 - \frac{2}{n} = \frac{n-2}{n}$$

$$P[e_2 \in C \mid e_1 \notin C] = \frac{|C|}{|E(G_1)|} \leq \frac{2}{n-1}$$

$$P[e_2 \notin C \mid e_1 \notin C] \geq \frac{n-3}{n-1}$$

$$P[e_3 \in C \mid e_1, e_2 \notin C] = \frac{|C|}{|E(G_2)|} \leq \frac{2}{n-2}$$

$$P[e_3 \notin C \mid e_1, e_2 \notin C] \geq \frac{n-4}{n-2}$$

up to

$$P[e_{n-2} \notin C \mid e_1, \ldots, e_{n-3} \notin C] \geq 1/3$$

Probability of success (i.e. outputing $C$) is atleast

$$\prod_{i=0}^{n-3} \frac{n-i-2}{n-i} = \frac{2}{n(n-1)} = \frac{1}{\binom{n}{2}}$$

We could express it exactly with conditional probabilities, but the bound holds for the i-th graph too: $|E_i| \geq (n-i)\delta(G_i)/2$ ■

The real Monte-Carlo algorithm will repeat the above algorith $n^2$ times independently and return the minimum from all the runs. Then the probability that the algorithms fails is at most $(1-\frac{2}{n^2})^{n^2} \leq e^{-2n^2/n^2} = 1/e^2 < 1/2$.

**Corollary 3.** *Every multigraph $G$ has at most $\binom{n}{2}$ min cuts.*

*Proof.* If $G$ has $\ell$ different mincuts $c_1, \ldots, c_\ell$ then by the analysis of the Karger's algorithm the probability that the algorithm outputs some mincut is atleast $\frac{\ell}{\binom{n}{2}}$. But as probability is always at most 1, so the claim follows. ■

Cycle $C_n$ shows that the bound is tight.

Let's improve the algorithm (also called Karger-Stein). The probability that this algorithm will be atleast $\theta(\frac{1}{\log n})$. Instead of iterating while $|V| \geq 3$, we will now iterate while $|V| \geq t$ for some $t$. Then the huge probability that the algorithm succeeded, was atleast

$$\frac{n-2}{n} \cdot \frac{n-3}{n-1} \cdots \frac{t-2}{t}$$

now, we set $t = \frac{n}{\sqrt{2}}$.

In each iteration, if the number of vertices is $O(1)$, then solve by bruteforce. Otherwise call a contraction with $t = |V(G)|/\sqrt{2}+2$ on $G$ twice independently - resulting in $G_1$ and $G_2$ and then recurse on the contracted parts and return the better solution. Plugging the $t$ in the formula above gives that the probability of one contraction succeeds is atleast $1/2$.

The probability that K-S fails is the probability that both branches fail (they are ran independently). That is

$$P(Fail_n) \leq \left(1 - \frac{1}{2}P(Fail_{\frac{n}{\sqrt{2}}+1})\right)^2$$

The parameter $t$ said that the threshold at which the contraction should stop and the iteration was done while $|V| \geq t$. So the number of vertices in the recursive call is $t-1$. So, the probability of success is:

$$P(Win_n) \geq 1 - \left(1 - \frac{1}{2}P(Fail_{\frac{n}{\sqrt{2}}+1})\right)^2$$

$$p(n) \geq 1 - \left(1 - \frac{1}{2}p\left(\frac{n}{\sqrt{2}}+1\right)\right)$$

Solve $=$ instead and set $k = \Theta(\log n)$. Then

$$q(k+1) = 1 - \left(1 - \frac{1}{2}q(k)\right)^2 = q(k) - \frac{q(k)^2}{4}$$

finally, let $q(k) = \frac{4}{r(k)+1}$

$$\frac{4}{r(k+1)+1} = \frac{4}{r(k)+1} - \frac{4}{(r(k)+1)^2}$$

$$\frac{1}{r(k+1)+1} = \frac{r(k)}{(r(k)+1)^2}$$

$$r(k+1) = \frac{r(k)^2 + r(k) + 1}{r(k)}$$

$$r(k+1) = r(k) + 1 + \frac{1}{r(k)}$$

induction on $\ell$: $\ell \leq r(\ell) \leq \ell + H_{\ell-1} + 3$ shows that $r(\ell) = \Theta(\ell)$. So $q(k) = \Theta(\frac{1}{k})$. So $\tilde{p} = \Theta(\frac{1}{\log n})$. TODOdo

# 3 Lovász Local Lemma

The aim is to show an existence of a 'good' object avoiding some bad properties $B_1, \ldots, B_m$. The probability that a random object will satisfy some $B_i$ (i.e.) some bad event will occur, i.e. $P(\bigcup B_i) < 1$ if and only if the probability that none of the $B_i$ occured, is $> 0$. If all the events are independent and $P(B_i) < 1$ for all $B_i$. Then the probability that noone of them happening is:

$$P\left(\bigcap_{i=1}^{n} \overline{B_i}\right) = \prod_{i=1}^{m}(P(\overline{B_i})) = \prod_{i=1}^{m}(1 - P(B_i)) > 0$$

Stated differently, the probability that some of the bad events will occur is

$$P\left(\bigcup_{i=1}^{m} B_i\right) = 1 - P\left(\bigcap_{i=1}^{n} \overline{B_i}\right) = \ldots < 0$$

On the other hand, if the events are not independent, we could use union-bound:

$$P\left(\bigcup_{i=1}^{m} B_i\right) \leq \sum_{i=1}^{m} P(B_i)$$

So it would suffice, if $\sum_{i=1}^{m} P(B_i) < 1$. Then

$$P\left(\bigcap_{i=1}^{n} \overline{B_i}\right) = P\left(\overline{\bigcup_{i=1} B_i}\right) = 1 - P\left(\bigcup_{i=1}^{m} B_i\right) > 0$$

Let's state the technical things used in the Lovász Local Lemma.

**Definition 2.** We say that an event $B$ in some probability space is mutually independent of some set of events $A_1, \ldots, A_n$ if $P(B \mid \bigcap_{i=1}^n A_i) = P(B)$

In other words, whether $B$ occured or not, does not depend on whether all of $A_i$'s happened.

**Lemma 8.1.** *If $B$ is mutually independent of events $A_1, \ldots, A_n$, then $B$ is mutually independent of events $\overline{A_1}, \ldots, \overline{A_n}$.*

*Proof.*

$$P\left(B \middle| \bigcap_{i=1}^{n} \overline{A_i}\right)$$

■

**Definition 3.** Given events $B_1, \ldots, B_m$ in some probability space, we say that $B_i$ has a *local-lemma degree* or *LL-degree* $d_i$ if and only if there is $J_i \subseteq \{1, \ldots, m\} \setminus \{i\}, |J_i| = d_i$ s.t. $B_i$ is mutually independent of events $\{B_j \mid j \notin J_i \cup \{i\}\}$.

**Theorem 9** (Lovász Local Lemma, symmetric version)**.** *Let $B_1, \ldots, B_m$ be events in some probability space. If*

1. *for all $i \in \{1, \ldots, m\}$ $d_i \leq D$*
2. *for all $i \in \{1, \ldots, m\}$ $P(B_i) \leq p$*
3. *$(D+1)p \leq \frac{1}{e}$*

*then the probability that all of $B_i$'s did not happen is nonzero, i.e. $P(\bigcap_{i=1}^m)\overline{B_i} > 0$.*

Let's show a trivial use of LLL.

**Theorem 10.** *Let $M = \{1, \ldots, m\}, N = \{1, \ldots n\}$, then for each $m$ there is $n$ s.t. there is injective map $f$ from $M$ to $N$.*

*Proof.* Set $m = n$ and take $f = \text{id}$. ■

*Proof using the probabilistic method.* Take a map $f : M \to N$ uniformly at random. For each $i \neq j$, the probability that $f(i) = f(j)$ is $1/n$. Call such event $B_{ij}$. $P(B_{ij}) = \frac{1}{n}$. Function $f$ is injective if $B_{ij}$ did not happen for every $i, j$. The probability that none of these events occured is

$$P\left(\bigcap_{i,j} \overline{B_{ij}}\right) = P\left(\overline{\bigcup_{i,j} B_{ij}}\right) = 1 - P\left(\bigcup_{i,j} B_{ij}\right) \geq 1 - \sum_{i,j} P(B_{ij}) = 1 - \frac{\binom{m}{2}}{n}$$

Now, if $n > \binom{m}{2} = \frac{m(m-1)}{2}$, then the above probability is strictly greater than zero, so the probability of picking a injective function is nonzero, so in particular, one such function must exist. Thus, it suffices to set (for example) $n = m^2$. ■

*Proof using Lovász Local Lemma.* ■

Given $i \in \{1, \ldots, m\}$ $B_i$ is having (local-lemma)-degree (LL-degree) $d_i$ iff $\exists J \subseteq \{1, \ldots, m\}, |J| = d_i$ s.t. $\{B_k \mid k \notin J_i\}$ are mutually independent.

In other words. $J$ is the set of indices that has to be deleted s.t. $B_i$ with all the others forms set of mutually independent events.

**Theorem 11** (Lovász Local Lemma (LLL), symmetric version)**.** *If $d_i \leq D$ for all $i \in \{1, \ldots, m\}$ and $P(B_i) \leq \tilde{p}$ and $(D+1)\tilde{p} \leq \frac{1}{e}$ then the probability that a random object avoids all $B_i$'s is nonzero.*

**Theorem 12.** *Let $M = \{1, \dots, m\}$, $N = \{1, \dots, n\}$. For each $m$ there is $n$ s.t. there is injective map from $M$ to $N$.*

*Proof.* Take a map $f : M \to N$ uniformly at random. For each $i \neq j$, the probability that $f(i) = f(j)$ is $1/n$. Call such event $B_{ij}$. $P(B_{ij}) = \frac{1}{n}$. Function $f$ is injective if $B_{ij}$ did not happen for every $i, j$. The probability that none of these events occured is

$$P\left(\bigcap_{i,j} \overline{B_{ij}}\right) = P\left(\overline{\bigcup_{i,j} B_{ij}}\right) = 1 - P\left(\bigcup_{i,j} B_{ij}\right) \geq 1 - \sum_{i,j} P(B_{ij}) = 1 - \frac{\binom{m}{2}}{n}$$

Now, if $n > \binom{m}{2} = \frac{m(m-1)}{2}$, then the above probability is strictly greater than zero, so the probability of picking a injective function is nonzero, so in particular, one such function must exist. Thus, it suffices to set (for example) $n = m^2$. ■

*Proof.* Take $n = f(m) = m$ and the identity. ■

*Proof using Lovász Local Lemma.* Take a map $h : M \to N$ uniformly at random. The bad event is that for some $i, j$ $h(i) = h(j)$. Index this with $B_{ij}$. There are $\binom{m}{2}$ such bad events. $P(B_{ij}) = 1/n$. By union-bound, if $\binom{m}{2}/n < 1$, then there is a map avoiding all $B_{ij}$'s.

It is true that $P(\overline{B_{ij}}) \cap \overline{B_{kl}}) = P(\overline{B_i}) \cdot P(\overline{B_{kl}})$. So $J_{ij} = \{\{i,k\}, k \in \{1, \dots, m\}, k \neq j\} \cup \{\{j,k\}, k \in \{1, \dots m\}, k \neq i\}$. $J_{ij} = 2m - 2$. That's the bound $D$ in LLL. So by LLL if $e \cdot \frac{2m-1}{n} < 1$, then a random map is injective with nonzero probability so we can choose $n = 2em$. ■

## 3.1 Coloring of hypergraphs

**Definition 4.** $k$-coloring of a hypergraph $(V, \mathcal{E})$ is a map $c : V \to \{1, \dots, k\}$ such that no hyperedge is monochromatic. In other words, for each hyperedge $F \in \mathcal{E}$ there are two vertices $x, y \in F$ s.t. $c(x) \neq c(y)$.

**Definition 5.** A hypergraph $(V, \mathcal{E})$ is $\ell$-uniform if for all $F \in \mathcal{E}$, $|F| = \ell$.

The problem of deciding whether given $\ell$-uniform graph is 2-colorable is NP-hard (Easy reduction from Nae $k$-Sat for $k = \ell$).

**Theorem 13.** *Let $G = (V, \mathcal{E})$ be $\ell$-uniform hypergraph with $|\mathcal{E}| < 2^{\ell-1}$. Then $G$ is 2-colorable.*

*Proof.* Color the vertices at random. For each vertex flip a fair coin and color it either red or blue. The probability that a given edge $F \in \mathcal{E}$ is monochromatic is $\frac{2}{2^\ell} = 2^{-\ell+1}$, because either the edge is all-red of all-blue. $P(F \text{ is monochromatic}) = 2^{-\ell+1}$. The probability that some edge is monochromatic is

$$P(\exists F : F \text{ is monochromatic}) = P(\bigcup_{F \in \mathcal{E}} F \text{ is monochromatic}) \leq \sum_{F \in \mathcal{E}} P(F \text{ is monochromatic}) < 2^{-\ell+1} \cdot 2^{\ell-1} = 1$$

So a random coloring has a nonzero probability that no edge will be monochromatic. In particular, some such coloring must exist. ■

**Definition 6.** In hypergraph $G = (V, \mathcal{E})$ *degree* of a vertex $v$ is the number of hyperedges $F \in \mathcal{E}$ s.t. $v \in F$.

**Theorem 14.** *Let $G = (V, \mathcal{E})$ be $\ell$-uniform hypergraph with $\deg(v) \leq \frac{2^\ell}{e \cdot \ell} := \Delta$. Then $G$ is 2-colorable.*

*Proof.* Color the vertices at random. For each vertex flip a fair coin and color it either red of blue. The probabilityt that a given edge $F \in \mathcal{E}$ is monochromatic is $2^{-\ell+1}$. Given a hyperedge $F$ there are at most $\ell \cdot (\Delta - 1)$ other hyperedges $F'$ intersecting $F$. Now

$$\ell(\Delta - 1) \leq \ell\Delta - 1 \leq \frac{2^{\ell-1}}{e} - 1$$

So the LLL-degree of the event that a given hyperedge $F$ is monochromatic is $D = \frac{2^{\ell-1}}{e} - 1$. Applying local lemma yields $\frac{1}{2^{\ell-1}} \cdot \frac{2^{\ell-1}}{e} = 1/e$, so the probability that no edge is monochromatic is nonzero, i.e. one such coloring exists. ■

**Theorem 15** (Lovász Local Lemma, general version)**.** *Given events $B_1, \ldots, B_m$ in some probability space. Let the following hold:*

1. *for each $i \in \{1, \ldots, m\}$ there is $w_i, 0 \leq w_i < 1$,*
2. *for each $i \in \{1, \ldots, m\}$ there is $J_i \subseteq \{1, \ldots, m\} \setminus \{i\}$, s.t. $B_i$ is mutually independent of*[1] *any set $\mathcal{B} \subseteq \{B_j \mid j \notin J_i \cup \{i\}\}$, i.e. for all such $\mathcal{B}$ $P(B_i \mid \bigwedge_{C \in \mathcal{B}} C) = P(B_i)$.*
3. *for each $i \in \{1, \ldots, m\}$ $P(B_i) \leq w_i \prod_{j \in J_i}(1 - w_j)$*

*then $P(\bigcap_{i=1}^m \overline{B_i}) \geq \prod_{i=1}^m (1 - w_i) > 0$.*

*Proof.* We will be proving by induction, that for any $S \subseteq \{1, \ldots, m\}$ and $i \notin S$, the probability $P(B_i \mid \bigcap_{j \in S} \overline{B_j}) \leq w_i$. The base case is trivial, this follows from the third assumption. $P(B_i) \leq w_i \prod_{j \in J_i}(1 - w_j) \leq w_i$. Assume the claim holds for some $k = |S| \geq 1$. Split $S$ into $S_1, S_2$. We set $S_1 = S \cap J_i, S_2 = S \setminus S_1$. Now

CONTINUE ON PAPER

Now, it follows ... (td: write it down) ■

**Claim 16.** The general version of local lemma implies the symmetric version.

*Proof.* Without loss of generality, $D \geq 1$. If not, i.e. the events $B_i$ are all mutually independent, then since $p(d+1) = p \leq 1/e < 1$, i.e. $P(B_i) \leq 1/e < 1$ then $P(\bigcap_{i=1}^m \overline{B_i}) = \prod_{i=1}^m (1 - P(B_i)) > 0$. Otherwise, we apply the general version of the local lemma. Set $w_i = \frac{1}{D+1} < 1$. We now want to show that

$$P(B_i) \leq w_i \prod_{j \in J_i} (1 - w_j)$$

From the asusmption of the symmetric lemma, we have

$$P(B_i) \leq p \leq \frac{1}{e(D+1)}$$

From the other way around

$$w_i \prod_{j \in J_i} (1 - w_j) = \frac{1}{D+1} \left(1 - \frac{1}{D+1}\right)^{J_i} \geq \frac{1}{D+1} \left(1 - \frac{1}{D+1}\right)^{D}$$

TODO: finish it ■

**Example 17** (Acyclic colorings)**.** Assume we want to proper-color a graph and moreover we want no cycle to be bichromatic.

Prove that if $G$ has max degree $\Delta$, then there exists acyclic coloring with at most $o(\Delta^2)$ colors.

Prove that there exists a graph with max degree $\Delta$ that cannot be acyclicly $c$-colored for $c = \omega(\Delta)$.

In fact, there is some $f$ s.t. $c_L = f / \log^k \Delta$ and $c_U = f \cdot \log^k \Delta$.

palete with $c$ colors - bad edge $1/c$, bad even cycle with length $\ell$ - $1/c^{\ell-2}$

[1] There is no 'dependency' between $B_i$ and any other events that are not (indices) in $J_i$ (and are not $i$). We don't say that the set of all the events together is mutually independent. It might hold that maybe two from $\mathcal{B}$ may not be independent, but really, what we care about is, whether knowing anything from $\mathcal{B}$, tells us anything about the probability $P(B_i)$ (and it must not).

### 3.2 Algorithmic local lemma

Not only that with local lemma can show an existence of an object avoiding some bad properties. There is an algorithmic version which, in polynomial time, finds such object. There are technical assumptions:

Firstly, the probability space must be a product space $P = \prod_{i=1}^{n} P_i$, $X = (X_1, \ldots, X_n)$ and each $X_i \sim P_i$ and $P_i$ independent on $P_j$ for each $i \neq j$.

For bad events $B_1, \ldots, B_m$, we assume that each $B_i$ can be verified (whether it happened or not). Also, we want $m \in O(\text{poly}(n))$.

Algorithm for LLL: Start with random assignment $X_i \sim P_i$. Each $B_j$ depends on some set $V_j \subseteq \{1, \ldots, n\}$ of indices in While there exists $B_i$ satisfied. Let $X_{i_1}, \ldots, X_{i_j}$ be variables which $B_i$ depends on. Resample these from the corresponding probability distributions $P_{i_1}, \ldots, P_{i_j}$.

**Theorem 18** (Moser-Tardos)**.** *If there are $w_i \in [0, 1)$ s.t. $P(B_i) \leq w_i \prod_{j \in J_i} (1 - w_j)$. $J_i = \{j \mid V_i \cap V_j \neq \emptyset\}$. Then ALLL runs in expected polynomial time.*

We have $J_i = \{j : V_i \cap V_j \neq \emptyset\}$ - the event $B_i$ is really "dependent" on those, which share a variable with $B_i$.