Randomized Algorithms
The Probabilistic Method
Thomas Kesselheim  Kurt Mehlhorn

June, 2016
The Probabilistic Method in a Nutshell

Color the edges of $K_n$ with two colors so that it has no monochromatic $K_k$?

- In order to show the existence of an object with certain properties, demonstrate a sample space of objects in which the probability is positive that a randomly selected object has the property.
- Since we work with finite sample spaces, the existence proofs are, in principle, algorithmic. An object with the desired properties can be found by exhaustive search.
- Sometimes, the existence proofs can be converted into efficient randomized or even deterministic algorithms.

Lecture is based on Chapter 6 in Mitzenmacher/Upfal. The definitive book on the subject is “The Probabilistic Method” by Noga Alon and Joel Spencer.
The Basic Counting Argument

**Theorem**

If \( \binom{n}{k} < 2^{\binom{k}{2}}^{-1} \), then it is possible to color the edges of \( K_n \) with two colors so that it has no monochromatic \( K_k \).

- There are \( 2^{\binom{n}{2}} \) possible colorings. We pick each one with probability \( 2^{-\binom{n}{2}} \).
- There are \( \binom{n}{k} \) different \( k \)-vertex cliques in \( K_n \). Number them. Let \( A_i \) be the event that the \( i \)-th clique is monochromatic. Then \( \Pr[A_i] = 2^{-\binom{k}{2}}^{-1} \).
- By union bound, \( \Pr\left[A_1 \lor \ldots \lor A_{\binom{n}{k}}\right] \leq \binom{n}{k} 2^{-\binom{k}{2}}^{-1} < 1 \).
- Thus \( \Pr\left[\overline{A_1} \land \ldots \land \overline{A_{\binom{n}{k}}}\right] > 0 \).

\[ n = 1000, \quad k = 20. \quad \binom{n}{k} \leq \left(\frac{en}{k}\right)^k \leq 150^{20} \leq 2^{160}, \quad 2^{\binom{k}{2}}^{-1} = 2^{20 \cdot 19/2 - 1} = 2^{189} \]
Finding a Large Cut

**Theorem**

*In an undirected graph $G$ with $m$ edges there is always a cut of size at least $m/2$.*

- We construct a random cut by assigning the vertices randomly to the two sides of the cut.
- For an edge $e$, let $X_e = 1$ if the endpoints are assigned to different sides, and $0$ otherwise. Then $\mathbb{E}[X_e] = 1/2$.
- Let $X = \sum_{e \in E} X_e$ be the expected size of the cut. Then $\mathbb{E}[X] = \sum_{e \in E} \mathbb{E}[X_e] = m/2$.
- Thus there exists a cut $(A, B)$ of size $m/2$. 
A Las Vegas Algorithm for Finding a Large Cut

- For a partition \((A, B)\) of the vertices, let \(C(A, B)\) be the capacity of the cut (= number of edges with one endpoint on both sides). Clearly, \(C(A, B) \leq m\) always.

- Let \(p = \Pr [C(A, B) \geq m/2]\). Then

\[
\frac{m}{2} = E[C(A, B)] = \sum_{i \leq m/2} i \cdot \Pr [C(A, B) = i] + \sum_{i \geq m/2} i \cdot \Pr [C(A, B) = i]
\]

\[
\leq (1 - p) \left( \frac{m}{2} - \frac{1}{2} \right) + pm,
\]

which implies \(p \geq 1/(m + 1)\).

- The algorithm is now clear: Generate a random cut and determine its capacity. Repeat until a cut of capacity at least \(m/2\) has been found.

- The expected number of repetitions is \(1/p = O(m)\).
Derandomization (Method of Conditional Expectations)

- Number the vertices $v_1, v_2$ to $v_n$.
- $E[C(A, B) \mid x_1, \ldots, x_k] =$ conditional expectation of $C(A, B)$ given that we place vertex $v_i$ on side $x_i \in \{A, B\}$ for $1 \leq i \leq k$.

To show: can efficiently find $x_1$ to $x_n$ such that $E[C(A, B)] \leq E[C(A, B) \mid x_1, \ldots, x_k]$ for all $k$.

- $k = 1$: $E[C(A, B)] = E[C(A, B) \mid x_1]$ since RHS does not depend on $x_1$.

Induction step: place $v_{k+1}$ randomly. Then

$$E[C(A, B) \mid x_1, \ldots, x_k] = \frac{1}{2} E[C(A, B) \mid x_1, \ldots, x_k, A] + \frac{1}{2} E[C(A, B) \mid x_1, \ldots, x_k, B].$$

- Compute both expectations on the right and fix $x_{k+1}$ to choose the larger one.
Derandomization, Continued

- How to compute $\mathbb{E}[C(A, B) \mid x_1, \ldots, x_k, A]$.
- for edges having both endpoints among $v_1$ to $v_{k+1}$ contribution is clear.
- other edges contribute with probability $1/2$.
- contribution by other edges is the same for both placements.
- So we place $v_{k+1}$ such that we cut at least half of the edges connecting it to vertices $v_1$ to $v_k$.
- direct analysis of deterministic algorithm: Let $d'_{k+1}$ be the number of edges connecting $v_{k+1}$ to $\{v_1, \ldots, v_k\}$.
- Place $v_1$ arbitrarily and $v_{k+1}$, $k \geq 1$, such that at least $d'_{k+1}/2$ edges are cut. Then total number of edges cut is at least $\sum_{1 \leq k \leq n} d'_{k}/2 = m/2$. 
Independent Sets

Theorem

A graph $G = (V, E)$ with $n$ vertices and $m$ edges has an independent set of size at least $n^2/(4m)$.

- Let $d = 2m/n$ be the average degree of the vertices.
  - Delete each vertex independently with probability $1 - 1/d$.
  - For each remaining edge, remove it and one of its adjacent vertices.

- Let $X$ be the number of vertices surviving the first step. Then $E[X] = n/d$. Let $Y$ be the number of edges surviving the first step. Then $E[Y] = nd/2 \cdot \left(\frac{1}{d}\right)^2 = \frac{n}{2d}$.

- The second step removes the surviving edges and at most $Y$ vertices. Thus alg outputs an independent set of size at least $X - Y$ and

$$E[X - Y] = \frac{n}{d} - \frac{n}{2d} = \frac{n}{2d} = \frac{n^2}{4m}.$$
Graphs with Large Girth

**Theorem**

For every $k \geq 3$ and large $n$, there is a graph with $n$ vertices, $\frac{1}{4}n^{1+1/k}$ edges, and girth (length of a shortest cycle) at least $k$.

- Sample a random graph $G \in \mathcal{G}_{n,p}$ with $p = n^{1/(k-1)}$. Let $X = \#$ of edges. Then $E[X] = \binom{n}{2} \cdot p = \frac{1}{2} \left(1 - \frac{1}{n}\right) n^{1+1/k}$.
- Let $Y = \text{number of cycles in } G \text{ of length at most } k - 1$.
- There are at most $\binom{n}{i} \frac{(i-1)!}{2}$ candidate cycles of length $i$ and each one is present with probability $p^i$. Thus

  $$E[Y] = \sum_{i=3}^{k-1} \binom{n}{i} \frac{(i-1)!}{2} p^i \leq \sum_{i=3}^{k-1} n^i p^i = \sum_{i=3}^{k-1} n^{i/k} < kn^{(k-1)/k}.$$  

- For each cycle of length $\leq k - 1$ in $G$, we remove one of its edges. The expected number of edges remaining is

  $$E[X - Y] \geq \frac{1}{2} \left(1 - \frac{1}{n}\right) n^{1+1/k} - kn^{(k-1)/k} \geq \frac{1}{4} n^{1+1/k}.$$
The Lovasz Local Lemma

Let $E_1$ to $E_n$ be a set of “bad events” in a probability space. We want to show that the probability that no bad event occurs is positive. This is easy if the events are mutually independent, i.e., for any $I \subseteq \{1, \ldots, n\}$

$$\Pr[\bigcap_{i \in I} E_i] = \prod_{i \in I} \Pr[E_i].$$

Then the events $\overline{E}_i$ are also independent (prove it) and hence

$$\Pr[\bigcap_{1 \leq i \leq n} \overline{E}_i] = \prod_{1 \leq i \leq n} \Pr[\overline{E}_i] = \prod_{1 \leq i \leq n} (1 - \Pr[E_i]) > 0$$

provided that $\Pr[E_i] < 1$ for all $i$.

Lovasz showed that less than mutual independence suffices to show that the probability of no bad event happening is positive.
The Dependency Graph

An event $E$ is mutually independent of the events $E_1$ to $E_n$ if for any subset $I \subseteq \{1, \ldots, n\}$, $\Pr[E | \cap_{i \in I}E_i] = \Pr[E]$.

Dependency Graph

A dependency graph for a set of events $E_1$ to $E_n$ is a graph $G = (V, E)$ on vertex set $\{1, \ldots, n\}$ such that for all $i$, $E_i$ is mutually independent of the events $\{E_j | (i, j) \not\in E\}$.

Example (Edge Disjoint Paths)

$n$ pairs of users need to communicate in a graph. Each pair $i \in \{1, \ldots, n\}$ can choose from a collection $F_i$ of paths.

For $i \neq j$, let $E_{\{i,j\}}$ be the event that the paths chosen by pairs $i$ and $j$ share an edge; this is a bad event. Then $E_{i,j}$ is independent of all events $E_{\{i',j'\}}$ when $\{i, j\} \cap \{i', j'\} = \emptyset$. So each event has $< 2n$ neighbors in the dependency graph.

Note that there are $n(n - 1)/2$ events.
Statement of Lovasz Local Lemma

**Theorem**

Let \( d \in \mathbb{N} \) and \( p \in \mathbb{R} \) with \( 4dp \leq 1 \). Let \( E_1, \ldots, E_n \) be events. If

1. \( \Pr[E_i] \leq p \) for all \( i \), and
2. the degree of their dependency graph is bounded by \( d \), then

\[
\Pr[\bigcap_{1 \leq i \leq n} \overline{E_i}] > 0.
\]

**Disjoint Paths:** Assume each \( F_i \) consists of \( m \) paths. For \( i \) and \( j \): a path in \( F_i \) intersects with at most \( k \) paths in \( F_j \). Then

\[
\Pr[E_{\{i,j\}}] \leq \frac{k}{m} \quad \text{and} \quad d < 2n \quad \text{and hence} \quad 4dp < \frac{8nk}{m}.
\]

So if \( 8nk/m \leq 1 \), there is a choice of paths such that the \( n \) paths are disjoint.
Application: $k$-Satisfiability

**Theorem**

Let $\varphi = C_1 \land \ldots \land C_m$, where each $C_i$ has exactly $k$ literals. If no variable appears in more than $T = 2^k / (4k)$ clauses, $\varphi$ is satisfiable.

- We assign random truth values to the variables.
- Let $E_i$ be the event that $i$-th clause is false. Then $\Pr[E_i] = 2^{-k}$. Thus $p = 2^{-k}$.
- $C_i$ is independent of $C_j$ if they do not share a variable.
- Each of the $k$ variables of a clause can appear in $T$ other clauses. Hence $d \leq k \cdot T \leq 2^k / 4$.
- Thus $4pd \leq 1$ and hence a satisfying assignment exists.

Under somewhat stronger assumptions, this can be turned into an algorithm.
Proof of Local Lemma

**Claim**
For all $S \subseteq \{1, \ldots, n\}$ and $k \not\in S$

$$\Pr \left[ E_k \mid \bigcap_{i \in S} \overline{E_i} \right] \leq 2p.$$ 

**Claim $\rightarrow$ Local Lemma**

$$\Pr \left[ \bigcap_{1 \leq i \leq n} \overline{E_i} \right] = \prod_{1 \leq i \leq n} \Pr \left[ E_i \mid \bigcap_{1 \leq j < i} \overline{E_j} \right]$$

$$= \prod_{1 \leq i \leq n} \left( 1 - \Pr \left[ E_i \mid \bigcap_{1 \leq j < i} \overline{E_j} \right] \right)$$

$$\geq \prod_{1 \leq i \leq n} \left( 1 - 2p \right) > 0$$
Proof of Claim

For all $S \subseteq \{1, \ldots, n\}$ and $k \notin S$: $\Pr [E_k \mid \cap_{i \in S} E_i] \leq 2p$.

Show $\Pr [\cap_{i \in S} E_i] > 0$ as in Claim $\Rightarrow$ Local Lemma.

Use induction on $s = |S|$. $s = 0$ is trivial. Split $S$ into $S_1 = \{i \mid k$ and $i$ are connected in dependency graph$\}$ and $S_2 = S \setminus S_1$. If $S_1$ is empty, full independence. So assume $|S_2| < |S|$. Let $F_{S_1} = \cap_{i \in S_1} E_i$. Similarly, $F_{S_2}, F_S$. Note $|S_1| \leq d$.

$$\Pr [E_k \mid F_S] = \frac{\Pr [E_k \cap F_S]}{\Pr [F_S]} = \frac{\Pr [E_k \cap F_{S_1} \mid F_{S_2}] \Pr [F_{S_2}]}{\Pr [F_{S_1} \mid F_{S_2}] \Pr [F_{S_2}]}$$

$$\Pr [E_k \cap F_{S_1} \mid F_{S_2}] \leq \Pr [E_k \mid F_{S_2}] \leq p \quad E_k \text{ indep of } S_2$$

$$\Pr [F_{S_1} \mid F_{S_2}] = \Pr [\cap_{i \in S_1} E_i \mid F_{S_2}] \geq 1 - \sum_{i \in S_1} \Pr [E_i \mid F_{S_2}]$$

$$\geq 1 - \sum_{i \in S_1} 2p \geq 1 - 2pd \geq 1/2.$$
In order to show the existence of an object with certain properties, demonstrate a sample space of objects in which the probability is positive that a randomly selected object has the property.

Since we work with finite sample spaces, the existence proofs are, in principle, algorithmic. An object with the desired properties can be found be exhaustive search.

Sometimes, the existence proofs can be converted into efficient randomized or even deterministic algorithms.

Lecture is based on Chapter 6 in Mitzenmacher/Upfal. The definitive book on the subject is “The Probabilistic Method” by Noga Alon and Joel Spencer.