Proof Through a Probabilistic Argument

• Compute

\[ \sum_{i=0}^{n} i \binom{n}{i} \left( \frac{1}{2} \right)^n \]
Proof Through a Probabilistic Argument

• Compute

\[ \sum_{i=0}^{n} i \binom{n}{i} \left( \frac{1}{2} \right)^n \]

• Let \( X \sim B(n, 1/2) \),

• \( X_i \) independent r.v. with \( Pr(X_i = 1) = Or(X_i = 0) = 1/2 \).

\[ \sum_{i=0}^{n} i \binom{n}{i} \left( \frac{1}{2} \right)^n = E[X] = E[\sum_{i=1}^{n} X_i] = \sum_{i=1}^{n} E[X_i] = \frac{n}{2} \]

• We prove a deterministic statement using a probabilistic argument!
The Probabilistic Method

1. If $E[X] = C$, then there are values $c_1 \leq C$ and $c_2 \geq C$ such that $Pr(X = c_1) > 0$ and $Pr(X = c_2) > 0$.

2. If a random object in a set satisfies some property with positive probability then there is an object in that set that satisfies that property.
Theorem

Given any graph $G = (V, E)$ with $n$ vertices and $m$ edges, there is a partition of $V$ into two disjoint sets $A$ and $B$ such that at least $m/2$ edges connect vertex in $A$ to a vertex in $B$.

Proof.

Construct sets $A$ and $B$ by randomly assign each vertex to one of the two sets. The probability that a given edge connect $A$ to $B$ is $1/2$, thus the expected number of such edges is $m/2$. Thus, there exists such a partition.
Maximum Satisfiability

Given \( m \) clauses in CNF (Conjunctive Normal Form), assume that no clause contains a variable and its complement.

**Theorem**

*For any set of \( m \) clauses there is a truth assignment that satisfy at least \( m/2 \) of the clauses.*

**Proof.**

Assign random values to the variables. The probability that a given clause (with \( k \) literals) is not satisfied is bounded by

\[
1 - 2^{-k} \geq \frac{1}{2}.
\]
Monochromatic Complete Subgraphs

Given a complete graph on 1000 vertices, can you color the edges in two colors such that no clique of 20 vertices is monochromatic?

**Theorem**

If \( n \leq 2^{(k-1)/2} \) then it is possible to edge color the edges of a complete graph on \( n \) points \((K_n)\), such that is has no monochromatic \( K_k \) subgraph.
Proof.

Consider a random coloring. For a given set of $k$ vertices, the probability that the clique defined by that set is monochromatic is bounded by

$$2 \times 2^{-\binom{k}{2}}.$$

There are $\binom{n}{k}$ such cliques, thus the probability that any clique is monochromatic is bounded by

$$\binom{n}{k}2 \times 2^{-\binom{k}{2}} \leq \frac{n^k}{k!}2 \times 2^{-\binom{k}{2}} \leq 2^{(k-1)^2/2-k(k-1)/2+1} \frac{1}{k!} < 1.$$

Thus, there is a coloring with the required property. □
Sample and Modify

An independent set in a graph $G$ is a set of vertices with no edges between them. Finding the largest independent set in a graph is an NP-hard problem.

**Theorem**

Let $G = (V, E)$ be a graph on $n$ vertices with $dn/2$ edges. Then $G$ has an independent set with at least $n/2d$ vertices.

**Algorithm:**

1. Delete each vertex of $G$ (together with its incident edges) independently with probability $1 - 1/d$.
2. For each remaining edge, remove it and one of its adjacent vertices.
\[ X = \text{number of vertices that survive the first step of the algorithm.} \]

\[ E[X] = \frac{n}{d}. \]

\[ Y = \text{number of edges that survive the first step.} \]
An edge survives if and only if its two adjacent vertices survive.

\[ E[Y] = \frac{nd}{2} \left(\frac{1}{d}\right)^2 = \frac{n}{2d}. \]

The second step of the algorithm removes all the remaining edges, and at most \( Y \) vertices.
Size of output independent set:

\[ E[X - Y] = \frac{n}{d} - \frac{n}{2d} = \frac{n}{2d}. \]
**Conditional Expectation**

### Definition

\[
E[Y \mid Z = z] = \sum_y y \Pr(Y = y \mid Z = z),
\]

where the summation is over all \( y \) in the range of \( Y \).

### Lemma

*For any random variables \( X \) and \( Y \),*

\[
E[X] = \sum_y \Pr(Y = y)E[X \mid Y = y],
\]

*where the sum is over all values in the range of \( Y \).*
Given a graph $G = (V, E)$ with $n$ vertices and $m$ edges, we showed that there is a partition of $V$ into $A$ and $B$ such that at least $m/2$ edges connect $A$ to $B$.
How do we find such a partition?
\(C(A, B) = \) number of edges connecting \(A\) to \(B\).
If \(A, B\) is a random partition \(E[C(A, B)] = \frac{m}{2}\).

**Algorithm:**

1. Let \(v_1, v_2, \ldots, v_n\) be an arbitrary enumeration of the vertices.
2. Let \(x_i\) be the set where \(v_i\) is placed \((x_i \in \{A, B\})\).
3. For \(i = 1\) to \(n\) do:
   1. Place \(v_i\) such that
      
      \[
      E[C(A, B) \mid x_1, x_2, \ldots, x_i] \\
      \geq E[C(A, B) \mid x_1, x_2, \ldots, x_{i-1}] \geq \frac{m}{2}.
      \]
Lemma

For all $i = 1, \ldots, n$ there is an assignment of $v_i$ such that

$$E[C(A, B) \mid x_1, x_2, \ldots, x_i] \geq E[C(A, B) \mid x_1, x_2, \ldots, x_{i-1}] \geq m/2.$$
Proof.

By induction on $i$.

For $i = 1$, $E[C(A, B) \mid x_1] = E[C(A, B)] = m/2$.

For $i > 1$, if we place $v_i$ randomly in one of the two sets,

\[
E[C(A, B) \mid x_1, x_2, \ldots, x_{i-1}] = \frac{1}{2} E[C(A, B) \mid x_1, x_2, \ldots, x_i = A] + \frac{1}{2} E[C(A, B) \mid x_1, x_2, \ldots, x_i = B].
\]

\[
\max(E[C(A, B) \mid x_1, x_2, \ldots, x_i = A], E[C(A, B) \mid x_1, x_2, \ldots, x_i = B]) \geq E[C(A, B) \mid x_1, x_2, \ldots, x_{i-1}] \geq m/2
\]
How do we compute

$$\max(E[C(A, B) \mid x_1, x_2, \ldots, x_i = A], E[C(A, B) \mid x_1, x_2, \ldots, x_i = B]) \geq E[C(A, B) \mid x_1, x_2, \ldots, x_{i-1}] \geq m/2$$

We just need to consider edges between $v_j$ and $v_1, \ldots, v_{i-1}$.

**Simple Algorithm:**

1. Place $v_1$ arbitrarily.
2. For $i = 2$ to $n$ do
   1. Place $v_i$ in the set with smaller number of neighbors.
Perfect Hashing

Goal: Store a static disctionary of $n$ items in a table of $O(n)$ space such that any search takes $O(1)$ time.
Definition

Let $U$ be a universe with $|U| \geq n$ and $V = \{0, 1, \ldots, n-1\}$. A family of hash functions $\mathcal{H}$ from $U$ to $V$ is said to be $k$-universal if, for any elements $x_1, x_2, \ldots, x_k$, when a hash function $h$ is chosen uniformly at random from $\mathcal{H}$,

$$\Pr(h(x_1) = h(x_2) = \ldots = h(x_k)) \leq \frac{1}{n^{k-1}}.$$
Example of 2-Universal Hash Functions

Universe $U = \{0, 1, 2, \ldots, m - 1\}$
Table keys $V = \{0, 1, 2, \ldots, n - 1\}$, with $m \geq n$.
A family of hash functions obtained by choosing a prime $p \geq m$,

$$h_{a,b}(x) = ((ax + b) \mod p) \mod n,$$

and taking the family

$$\mathcal{H} = \{h_{a,b} \mid 1 \leq a \leq p - 1, 0 \leq b \leq p\}.$$

Lemma

$\mathcal{H}$ is 2-universal.
Lemma

\( \mathcal{H} \) is 2-universal.

Proof.

We first observe that for \( x_1, x_2 \in \{0, \ldots, p - 1\}, x_1 \neq x_2, \)

\[ ax_1 + b \neq ax_2 + b \mod p. \]

Thus, if \( h_{a,b}(x_1) = h_{a,b}(x_2) \) there is a pair \((s, r)\) such that \( s \neq r, \)
\( s = r \mod n, \) and

\[ (ax_1 + b) \mod p = r \]
\[ (ax_2 + b) \mod p = s \]

For each \( r \) there are \( \leq \lceil \frac{p}{n} \rceil - 1 \) values \( s \neq r \) such that \( s = r \mod n. \) There are \( p \) choices of \( r, \) and for each pair \((r, s)\) there is only one pair \((a, b)\) that satisfies the relation.

Thus, the probability of a collision is \( \leq \frac{p(\lceil \frac{p}{n} \rceil - 1)}{p(p-1)} \leq \frac{1}{n}. \)

\hfill \Box
Lemma

Assume that \( m \) elements are hashed into an \( n \) bin chain hashing table, using a hash function \( h \) chosen uniformly at random from a 2-universal family. For an arbitrary element \( x \), let \( X \) be the number of items at the bin \( h(x) \).

\[
E[X] \leq \begin{cases} 
\frac{m}{n} & \text{if } x \notin S \\
1 + \frac{m-1}{n} & \text{if } x \in S.
\end{cases}
\]

Proof.

Let \( X_i = 1 \) if the \( i \)-th element of \( S \) is in the same bin as \( x \) and 0 otherwise. \( \Pr(X_i = 1) \leq 1/n \)

If \( x \notin S \), \( E[X] = E[\sum_{i=1}^{m} X_i] = \sum_{i=1}^{m} E[X_i] \leq m/n \),

If \( x \in S \) (assume \( x \) is \( s_1 \)),

\[
E[X] = E[\sum_{i=1}^{m} X_i] = 1 + \sum_{i=2}^{m} E[X_i] \leq 1 + (m - 1)/n.
\]

\( \square \)
Lemma

If \( h \in \mathcal{H} \) is chosen uniformly at random from a 2-universal family of hash functions mapping the universe \( U \) to \([0, n - 1]\), then for any set \( S \subset U \) of size \( m \), with probability \( \geq 1/2 \) the number of collisions is bounded by \( m^2/n \).

Proof.

Let \( s_1, s_2, \ldots, s_m \) be the \( m \) items of \( S \). Let \( X_{ij} \) be 1 if the \( h(s_i) = h(s_j) \) and 0 otherwise. Let \( X = \sum_{1 \leq i < j \leq n} X_{ij} \).

\[
E[X] = E \left[ \sum_{1 \leq i < j \leq n} X_{ij} \right] = \sum_{1 \leq i < j \leq m} E[X_{ij}] \leq \left( \frac{m}{2} \right) \frac{1}{n} < \frac{m^2}{2n},
\]

Markov’s inequality yields

\[
\Pr(X \geq m^2/n) \leq \Pr(X \geq 2E[X]) \leq \frac{1}{2}.
\]
Definition

A hash function is perfect for a set $S$ if it maps $S$ with no collisions.

Lemma

If $h \in H$ is chosen uniformly at random from a 2-universal family of hash functions mapping the universe $U$ to $[0, n - 1]$, then for any set $S \subseteq U$ of size $m$, such that $m^2 \leq n$ with probability $\geq 1/2$ the hash function is perfect.
Theorem

The two-level approach gives a perfect hashing scheme for $m$ items using $O(m)$ bins.

Level I: use a hash table with $n = m$. Let $X$ be the number of collisions,

$$\Pr(X \geq m^2/n) \leq \Pr(X \geq 2\mathbb{E}[X]) \leq \frac{1}{2}.$$ 

When $n = m$, there exists a choice of hash function from the 2-universal family that gives at most $m$ collisions.
Level II: Let $c_i$ be the number of items in the $i$-th bin. There are $\binom{c_i}{2}$ collisions between items in the $i$-th bin, thus

$$\sum_{i=1}^{m} \binom{c_i}{2} \leq m.$$ 

For each bin with $c_i > 1$ items, we find a second hash function that gives no collisions using space $c_i^2$. The total number of bins used is bounded above by

$$m + \sum_{i=1}^{m} c_i^2 \leq m + 2 \sum_{i=1}^{m} \binom{c_i}{2} + \sum_{i=1}^{m} c_i \leq m + 2m + m = 4m.$$ 

Hence the total number of bins used is only $O(m)$. 
Complexity is usually studied in terms of resources, \textbf{TIME} and \textbf{SPACE}.
We add a new resource, \textbf{RANDOMNESS}, measured by the number of independent random bits used by the algorithm (\(=\) the entropy of the random source).
We proved:

**Theorem**

There is an algorithm for permutation routing on an $N = 2^n$-cube that uses a total of $O(nN)$ random bits and terminates with high probability in $cn$ steps, for some constant $c$.

Can we achieve the same result with fewer random bits?

**Theorem**

There is an algorithm for permutation routing on an $N = 2^n$-cube that uses a total of $O(n)$ random bits and terminates with high probability in $cn$ steps, for some constant $c$. 
Proof

Let $A(\pi)$ be a randomized algorithm with input $\pi$ that uses (up to) $s$ random bits.

We can replace $A(\pi)$ with a deterministic algorithm $D(\pi, r)$ that takes two inputs, $\pi$ and a random string $r \in \{0, \ldots, 2^s - 1\}$.

We can write $A(\pi)$ as

1. Choose $r$ uniformly at random in $[0, 2^s - 1]$.
2. Run $D(\pi, r)$. 

In the two phase routing algorithm $s = \log(N^N) = nN$ (it chooses a random destination independently for each packet).

Let $\mathcal{D}(\pi) = \{D(\pi, r) \mid r = 0, \ldots, 2^s - 1\}$ be the a collection of $m = 2^s$ deterministic algorithms $D(\pi, r)$.

We proved:

**Lemma**

*For a given input permutation $\pi$ and a deterministic algorithm $D(\pi, r)$ chosen uniformly at random from $\mathcal{D}$, the probability that $D(\pi, r)$ fails to route $\pi$ in $cn$ steps is bounded by $1/N$.***
Using a Smaller Collection of Deterministic Algorithms

Choose a random subset $R \subset \{0, \ldots, 2^s - 1\}$ of $m = N^3$ $s$-bits sequences $r_1, \ldots, r_m$.
Let $X^\pi_i = 1$ if algorithm $D(\pi, r_i)$ does NOT route permutation $\pi$ in $cn$ steps, else $X^\pi_i = 0$

$$E\left[\sum_{i=1}^{N^3} X^\pi_i\right] \leq N^2$$

$$\text{Prob}\left(\sum_{i=1}^{N^3} X^\pi_i \geq 2N^2\right) \leq e^{-N^2/3}$$

$$\text{Prob}(\exists \pi \sum_{i=1}^{N^3} X^\pi_i \geq 2N^2) \leq N!e^{-N^2/3} < 1$$
Theorem

There exists a set $\mathcal{D}$ of $N^3$ deterministic algorithms, such that for any given permutation $\pi$ and an algorithm $D$ chosen uniformly at random from $\mathcal{D}$, algorithm $D$ routes $\pi$ in $cn$ steps with probability $1 - 1/N$. The random choice requires $O(n)$ random bits.
Can we do better?

Do we need any random bits?

**Definition**

A routing algorithm is **oblivious** if the path taken by one packet is independent of the source and destinations of any other packets in the system.

**Theorem**

*Given an \( N \)-node network with maximum degree \( d \) the routing time of any deterministic oblivious routing scheme is*

\[
\Omega\left(\sqrt{\frac{N}{d^3}}\right).
\]
Theorem

For any deterministic oblivious algorithm for permutation routing on the $N = 2^n$ cube there is an input permutation that requires $\Omega(\sqrt{N}/n^3)$ steps.

Theorem

Any randomized oblivious routing algorithm for permutation routing on the $N = 2^n$ cube must use $\Omega(n)$ random bits to route an arbitrary permutation in $O(n)$ expected time.
Assume that the algorithm uses $k$ random bits. It can choose between no more than $2^k$ possible deterministic executions. There is a deterministic execution $\tilde{A}$ that is chosen with probability $\geq 1/2^k$. Let $\pi$ be an input permutation that requires $\Omega(\sqrt{N}/n^3)$ steps in $\tilde{A}$. The expected running time of this input permutation on the randomized algorithm is $\Omega(\sqrt{N}/(2^k n^3))$.
The First and Second Moment

<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>For an integer random variable $X$,</td>
</tr>
<tr>
<td>• $Pr(X &gt; 0) = Pr(X \geq 1) \leq E[X]$</td>
</tr>
<tr>
<td>• $Pr(X = 0) \leq Pr(</td>
</tr>
</tbody>
</table>
Let $G_{n,p} = (V, E)$ be a random graph generated as follows:
- The graph has $n$ nodes.
- Each of the $\binom{n}{2}$ pairs of vertices are connected by an edge with probability $p$ independently of any other edge in the graph.

A node is isolated if it is adjacent to no edges.

If $p = 0$ all vertices are isolated (have no edges). If $p = 1$ no vertex is isolated. What can we say for $0 < p < 1$?
Application: Number of Isolated Nodes

Let $G_{n,p} = (V, E)$ be a random graph generated as follows:

- The graph has $n$ nodes.
- Each of the $\binom{n}{2}$ pairs of vertices are connected by an edge with probability $p$ independently of any other edge in the graph.

A node is isolated if it has no edges.

Theorem

For any function $w(n) \to \infty$

- If $p = \frac{\log n - w(n)}{n}$, then whp the graph has isolated nodes.
- If $p = \frac{\log n + w(n)}{n}$, then whp the graph has no isolated nodes.
Proof

For \( i = 1, \ldots, n \), let \( X_i = 1 \) if node \( i \) is isolated, otherwise \( X_i = 0 \). Let \( X = \sum_{i=1}^{n} X_i \).

\[ E[X] = n(1 - p)^{n-1} \]

For \( p = \frac{\log n + w(n)}{n} \)

\[ E[X] = n(1 - p)^{n-1} \leq e^{\log n - (n-1)p} \leq e^{-w(n)} \to 0 \]

Thus, for \( p = \frac{\log n + w(n)}{n} \),

\[ Pr(X > 0) \leq E[X] \to 0 \]
To use the second moment method we need to bound $\text{Var}[x]$. 

$$\text{Var}[X_i] \leq E[X_i^2] = E[X_i] = (1 - p)^{n-1}$$

$$\sum_{i \neq j} \text{Cov}(X_i, X_j) = (1 - p)^{2n-3} - (1 - p)^{2n-2}$$

$$\text{Var}[X] \leq \sum_{i=1}^{n} \text{Var}[X_i] + \sum_{i \neq j} \text{Cov}(X_i, X_j)$$

$$= n(1 - p)^{n-1} + n(n - 1)(1 - p)^{2n-3} - n(n - 1)(1 - p)^{2n-2}$$

$$= n(1 - p)^{n-1} + n(n - 1)p(1 - p)^{2n-3}$$
\[
\begin{align*}
\text{Var}[X] & = \sum_{i=1}^{n} \text{Var}[X_i] + \sum_{i \neq j} \text{Cov}(X_i, X_i) \\
& = n(1 - p)^{n-1} + n(n - 1)p(1 - p)^{2n-3}
\end{align*}
\]

\[
\begin{align*}
\text{Pr}(X = 0) & \leq \frac{\text{Var}[X]}{(E[X])^2} \\
& = \frac{n(1 - p)^{n-1} + n(n - 1)p(1 - p)^{2n-3}}{n^2(1 - p)^{2n-2}} \\
& = \left(1 - \frac{1}{n}\right) \frac{p}{1 - p} + \frac{1}{n(1 - p)^{n-1}}
\end{align*}
\]
For \( p = \frac{\log n - w(n)}{n} \),

\[
Pr(X = 0) \leq \frac{\text{Var}[X]}{(E[X])^2} = \left(1 - \frac{1}{n}\right) \frac{p}{1 - p} + \frac{1}{n(1 - p)^{n-1}} \to 0
\]

Since

\[
n(1 - p)^{n-1} \geq ne^{-p(n-1)}(1 - \frac{p^2}{n}) \geq \frac{1}{2}e^{w(n)}
\]

We use: for \(|X| \leq 1\)

\[
e^{x} \left(1 - \frac{x^2}{n}\right) \leq \left(1 + \frac{x}{n}\right)^n \leq e^x
\]