PROBABILISTIC METHOD
Theorem 1

Let $A_1, A_2, \ldots, A_n$ be subsets of $A$ and $|A_i| = k$ for $1 \leq i \leq n$. If $n < 2^{k-1}$ then there exists a partition $A = R \cup B$ such that

$$A_i \cap R \neq \emptyset \text{ and } A_i \cap B \neq \emptyset \quad 1 \leq i \leq n.$$

[R = Red elements and B = Blue elements.]

Proof

Randomly colour $A$.

$$\Omega = \{R, B\}^A = \{f : A \rightarrow \{R, B\}\},$$ uniform distribution.

$$BAD = \{\exists i : A_i \subseteq R \text{ or } A_i \subseteq B\}.$$

Claim: $P(BAD) < 1$.

Thus $\Omega \setminus BAD \neq \emptyset$ and this proves the theorem.
\[ \text{BAD}(i) = \{ A_i \subseteq R \text{ or } A_i \subseteq B \} \]

\[ \text{BAD} = \bigcup_{i=1}^{n} \text{BAD}(i). \]

\[ \mathbb{P}(\text{BAD}) \leq \sum_{i=1}^{n} \mathbb{P}(\text{BAD}(i)) \]

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

\[ = \frac{n}{2^{k-1}} \]

\[ < 1. \]
Example of system which is not 2-colorable.

Let \( n = \binom{2k-1}{k} \) and \( A = [2k - 1] \) and

\[
\{A_1, A_2, \ldots, A_n\} = \binom{[2k - 1]}{k}.
\]

Then in any 2-coloring of \( A_1, A_2, \ldots, A_n \) there is a set \( A_i \) all of whose elements are of one color.

Suppose \( A \) is partitioned into 2 sets \( R, B \). At least one of these two sets is of size at least \( k \) (since \( (k - 1) + (k - 1) < 2k - 1 \)). Suppose then that \( R \geq k \) and let \( S \) be any \( k \)-subset of \( R \). Then there exists \( i \) such that \( A_i = S \subseteq R \).
De-randomising the coloring procedure.

We describe how we can **deterministically** color the elements of $A$ one at a time so that we end up with a coloring satisfying $A_i \cap R \neq \emptyset$ and $A_i \cap B \neq \emptyset$, $1 \leq i \leq n$.

We need some notation: Suppose that we have only colored a subset $C$ of $A$ and $C = R \cup B$ defines the colors of the elements in $C$. (Abusing notation, $R, B$ now refer to a partial coloring of $A$).

Let $Z(R, B)$ be the number of sets among the $A_i$ that will be mono-colored if we randomly color the remaining elements in $A \setminus (R \cup B)$.
\[
Z(R, B) = \sum_{i=1}^{n} Z_i(R, B)
\]

where

\[
E(Z_i(R, B)) = \begin{cases}
1 & A_i \subseteq R \text{ or } A_i \subseteq B \\
0 & A_i \cap R \neq \emptyset \text{ and } A_i \cap B \neq \emptyset \\
2^{1-k} & A_i \cap C = \emptyset \\
2^{-|A_i \setminus C|} & A_i \cap R \neq \emptyset \text{ and } A_i \cap B = \emptyset \\
2^{-|A_i \setminus C|} & A_i \cap R = \emptyset \text{ and } A_i \cap B \neq \emptyset
\end{cases}
\]

Initially we have \(E(Z(\emptyset, \emptyset)) < 1\).

Not also that we can compute \(E(Z(R, B))\) in \(O(n|A|)\) time.
Suppose now that we have managed to color some of the elements of $A$ and $E(Z(R, B)) < 1$.

Suppose that $x$ is an arbitrary element of $A \setminus C$. Then if we consider the random color $c$ for $x$ then

$$1 > E(Z(R, B)) = E(Z(R, B) \mid c = \text{Red}) \Pr(c = \text{Red}) + E(Z(R, B) \mid c = \text{Blue}) \Pr(c = \text{Blue}) = E(Z(R \cup \{x\}, B)) + E(Z(R, B \cup \{x\}))$$

$$2$$

It follows that at least one of $E(Z(R \cup \{x\}, B)), E(Z(R, B \cup \{x\})$ is less than 1.
If $\mathbf{E}(Z(R \cup \{x\}, B)) < 1$ then we color $x$ Red, otherwise we color it Blue.

We continue in this way until we find $R, B$ such that

$$R \cup B = A \text{ and } \mathbf{E}(Z(R, B)) < 1.$$ 

Now if $R \cup B = A$ then there are no more random choices and $\mathbf{E}(Z(R, B)) = Z(R, B)$ is the number of mono-colored sets.

Since $Z(R, B) < 1$, this number is zero.
Tournaments

$n$ players in a tournament each play each other i.e. there are $\binom{n}{2}$ games.

Fix some $k$. Is it possible that for every set $S$ of $k$ players there is a person $w_S$ who beats everyone in $S$?
Suppose that the results of the tournament are decided by a random coin toss.

Fix $S$, $|S| = k$ and let $\mathcal{E}_S$ be the event that nobody beats everyone in $S$.

The event

$$\mathcal{E} = \bigcup_S \mathcal{E}_S$$

is that there is a set $S$ for which $w_S$ does not exist.

We only have to show that $\Pr(\mathcal{E}) < 1$. 

Probabilistic Method
\[
\Pr(\mathcal{E}) \leq \sum_{|S|=k} \Pr(\mathcal{E}_S)
\]
\[
= \binom{n}{k}(1-2^{-k})^{n-k}
\]
\[
< n^k e^{-(n-k)2^{-k}}
\]
\[
= \exp\{k \ln n - (n - k)2^{-k}\}
\]
\[
\rightarrow 0
\]

since we are assuming here that \(k\) is fixed independent of \(n\).
A binary tree consists of a set of nodes, one of which is the root. Each node is connected to 0, 1 or 2 nodes below it and every node other than the root is connected to exactly one node above it. The root is the highest node. The depth of a node is the number of edges in its path to the root. The depth of a tree is the maximum over the depths of its nodes.
Starting with a tree $T_0$ consisting of a single root $r$, we grow a tree $T_n$ as follows:

The $n$’th *particle* starts at $r$ and flips a fair coin. It goes left (L) with probability 1/2 and right (R) with probability 1/2.

It tries to move along the tree in the chosen direction. If there is a node below it in this direction then it goes there and continues its random moves. Otherwise it creates a new node where it wanted to move and stops.
Let $D_n$ be the depth of this tree.

**Claim:** for any $t \geq 0$,

$$P(D_n \geq t) \leq \left(n2^{-(t-1)/2}\right)^t.$$

**Proof** The process requires at most $n^2$ coin flips and so we let

$$\Omega = \{L, R\}^{n^2}$$

– most coin flips will not be needed most of the time.

$$DEEP = \{D_n \geq t\}.$$

For $P \in \{L, R\}^t$ and $S \subseteq [n], |S| = t$ let

$$DEEP(P, S) = \{\text{the particles } S = \{s_1, s_2, \ldots, s_t\} \text{ follow } P \text{ in the tree i.e. the first } i \text{ moves of } s_i \text{ are along } P, 1 \leq i \leq t\}.$$

$$DEEP = \bigcup_P \bigcup_S DEEP(P, S).$$
S={4,8,11,13,17}

t=5 and DEEP(P,S) occurs if
4 goes L...
8 goes LR...
17 goes LRR...
11 goes LRRL...
13 goes LRRLR...
\[ P(DEEP) \leq \sum_{P} \sum_{S} P(DEEP(P, S)) \]
\[ = \sum_{P} \sum_{S} 2^{-(1+2+\cdots+t)} \]
\[ = \sum_{P} \sum_{S} 2^{-t(t+1)/2} \]
\[ = 2^t \binom{n}{t} 2^{-t(t+1)/2} \]
\[ = 2^t n^t 2^{-t(t+1)/2} \]
\[ \leq 2^t n^t 2^{-(t-1)/2} \]
\[ = (n2^{-(t-1)/2})^t. \]

So if we put \( t = A \log_2 n \) then

\[ P(D_n \geq A \log_2 n) \leq (2n^{1-A/2})^{A \log_2 n} \]

which is very small, for \( A > 2 \).
Secretary Problem

There are $n$ applicants for a secretarial position and CEO Pat will interview them in random order. The rule is that Pat must decide on the spot whether to hire the current applicant or interview the next one. Pat is an excellent judge of quality, but she does not know the set of applicants a priori. She wants to give herself a good chance of hiring the best.

Here is her strategy: She chooses a number $m < n$, interviews the first $m$ and then hires the first person in $m + 1, \ldots, n$ who is the best so far. (There is a chance that she will not hire anyone).
Let $S$ be the event that Pat chooses the best person and let $P_i$ be the event that the best person is the $i$th applicant. Then

$$
Pr(S) = \sum_{i=1}^{n} Pr(S \mid P_i) Pr(P_i) = \frac{1}{n} \sum_{i=1}^{n} Pr(S \mid P_i).
$$

Now Pat’s strategy implies that $Pr(S \mid P_i) = 0$ for $1 \leq i \leq m$. If $P_i$ occurs for $i > m$ then Pat will succeed iff the best of the first $i - 1$ applicants ($j$ say) is one of the first $m$, otherwise Pat will mistakenly hire $j$. Thus, for $i > m$, $Pr(S \mid P_i) = \frac{m}{i-1}$ and hence

$$
Pr(S) = \frac{m}{n} \sum_{i=m+1}^{n} \frac{1}{i-1}.
$$
Now assume that $n$ is large and that $m = \alpha n$. Then

$$\Pr(S) \sim \alpha (\ln n - \ln \alpha n) = \alpha \ln 1/\alpha.$$ 

Pat will want to choose the value of $\alpha$ that maximises $f(\alpha) = \alpha \ln 1/\alpha$. But $f'(\alpha) = \ln 1/\alpha - 1$ and so the optimum choice for $\alpha$ is $1/e$. In which case,

$$\Pr(S) \sim e^{-1}.$$
A problem with hats

There are $n$ people standing a circle. They are blind-folded and someone places a hat on each person’s head. The hat has been randomly colored Red or Blue.

They take off their blind-folds and everyone can see everyone else’s hat. Each person then simultaneously declares (i) my hat is red or (ii) my hat is blue or (iii) or I pass.

They win a big prize if the people who opt for (i) or (ii) are all correct. They pay a big penalty if there is a person who incorrectly guesses the color of their hat.

Is there a strategy which means they will win with probability better than 1/2?
Suppose that we partition $Q_n = \{0, 1\}^n$ into 2 sets $W, L$ which have the property that $L$ is a cover i.e. if $x = x_1x_2 \cdots x_n \in W = Q_n \setminus L$ then there is $y_1y_2 \cdots y_n \in L$ such that $h(x, y) = 1$ where

$$h(x, y) = |\{j : x_j \neq y_j\}|.$$

Hamming distance between $x$ and $y$.

Assume that $0 \equiv \text{Red}$ and $1 \equiv \text{Blue}$. Person $i$ knows $x_j$ for $j \neq i$ (color of hat $j$) and if there is a unique value $\xi$ of $x_i$ which places $x$ in $W$ then person $i$ will declare that their hat has color $\xi$.

The people assume that $x \in W$ and if indeed $x \in W$ then there is at least one person who will be in this situation and any such person will guess correctly.

Is there a small cover $L$?
Let $p = \frac{\ln n}{n}$. Choose $L_1$ randomly by placing $y \in Q_n$ into $L_1$ with probability $p$.

Then let $L_2$ be those $z \in Q_n$ which are not at Hamming distance $\leq 1$ from some member of $L_1$.

Clearly $L = L_1 \cup L_2$ is a cover and
\[
\mathbb{E}(|L|) = 2^n p + 2^n (1 - p)^{n+1} \leq 2^n (p + e^{-np}) \leq 2^{n \frac{2\ln n}{n}}.
\]

So there must exist a cover of size at most $2^{n \frac{2\ln n}{n}}$ and the players can win with probability at least $1 - \frac{2 \ln n}{n}$.
First Moment Method

Let $X$ be a random variable that takes values in $\{0, 1, 2, \ldots\}$. Then

$$\Pr(X \geq 1) \leq E(X)$$

Proof

$$E(X) = E(X | X = 0)\Pr(X = 0) + E(X | X \geq 1)\Pr(X \geq 1) \geq \Pr(X \geq 1).$$
Intersection Safe Families

Let $\mathcal{A}$ be a family of sub-sets of $[n]$. We say that $\mathcal{A}$ is Intersection Safe if for distinct $A, B, C \in \mathcal{A}$ we have $C \not\supseteq A \cap B$. We use the probabilistic method to show the existence of an Intersection Safe family of exponential size.

Suppose that $\mathcal{A}$ consists of $p$ randomly and independently chosen sets $X_1, X_2, \ldots, X_p$. Let $Z$ denote the number of 3-tuples $i, j, k$ such that $X_i \cap X_j \subseteq X_k$. Then

$$E(Z) = p(p-1)(p-2) \Pr(X_i \cap X_j \subseteq X_k) = p(p-1)(p-2) \left(\frac{7}{8}\right)^n.$$ 

(Observe that $\Pr(x \in (X_i \cap X_j) \setminus X_k = 1/8).$)
So if $p \leq (8/7)^{n/3}$ then

$$\Pr(Z \geq 1) \leq \mathbb{E}(Z) < p^3 \left(\frac{7}{8}\right)^n \leq 1$$

implying that there exists a union free family of size $p$.

There is a small problem here in that we might have repetitions $X_i = X_j$ for $i \neq j$. Then our set will not be of size $p$.

But if $Z_1$ denotes the number of pairs $i, j$ such that $X_i = X_j$ then

$$\Pr(Z_1 \neq 0) \leq \mathbb{E}(Z_1) = \binom{p}{2} 2^{-n}$$

and so we should really choose $p$ so that

$$\Pr(Z + Z_1 \neq 0) \leq \mathbb{E}(Z) + \mathbb{E}(Z_1) < p^3 \left(\frac{7}{8}\right)^n + p^2 \left(\frac{1}{2}\right)^n \leq 1.$$
Application: Suppose that we have a central storage containing \( n \) keys \( \{k_1, k_2, \ldots, k_n\} \).

We must distribute sets of keys to \( p \) people. Person \( i \) will get the set \( K_i = \{k_j : j \in X_i\} \). The sets \( X_1, X_2, \ldots, X_p \) are public knowledge.

If person \( r \) wishes to communicate with person \( s \) then he/she will send them \( \{k_j : j \in X_r \cap X_s\} \) as a means of proving their identity.

If the sets \( X_1, X_2, \ldots, X_p \) are intersection safe, then person \( t \) cannot pretend to be person \( r \).

It is possible therefore to have a “secure“ system with \( p \) people that requires each person to get \( O(\ln p) \) keys.
Average case of Quicksort

Quicksort is an algorithm for sorting numbers. Given distinct \( x_1, x_2, \ldots, x_n \) we

1. Randomly choose an integer \( p \) between 1 and \( n \) — the pivot.
2. Divide the remaining numbers into 2 sets \( L, R \) where
   \[
   L = \{ x_j : x_j < x_p \} \quad \text{and} \quad R = \{ x_j : x_j > x_p \}.
   \]
3. Recursively sort \( L, R \).

Let \( T_n \) be the expected number of comparisons taken by Quicksort.
We have $T_0 = 0$ and for $n \geq 1$

$$T_n = \sum_{i=1}^{n} E(\text{No. comparisons } | \text{ } p \text{ is } i^{th} \text{ largest}) \Pr(p \text{ is } i^{th} \text{ largest}) =$$

$$= \sum_{i=1}^{n} (n - 1 + T_{i-1} + T_{n-i}) \times \frac{1}{n}$$

$$= n - 1 + \frac{2}{n} \sum_{i=0}^{n-1} T_i$$

or

$$nT_n = n(n - 1) + 2 \sum_{i=0}^{n-1} T_i.$$
Let \( T(x) = \sum_{n=0}^{\infty} T_n x^n \) be the generating function for \( T_n \).

We note that

\[
\sum_{n=1}^{\infty} nT_n x^n = xT'(x).
\]

\[
\sum_{n=1}^{\infty} n(n-1)x^n = \frac{2x^2}{(1-x)^3}.
\]

\[
\sum_{n=1}^{\infty} \left( \sum_{i=0}^{n-1} T_i \right) x^n = \frac{xT(x)}{1-x}.
\]
Thus,

\[ T'(x) = \frac{2x}{(1-x)^3} + \frac{2T(x)}{1-x} \]

or

\[ (1-x)^2 T'(x) - 2(1-x)T(x) = \frac{2x}{1-x} \]

or

\[ \frac{d}{dx}((1-x)^2 T(x)) = \frac{2x}{1-x} \]

and so

\[ (1-x)^2 T(x) = C - 2x - 2\ln(1-x). \]
\[(1 - x)^2 T(x) = C - 2x - 2 \ln(1 - x).\]

Now \(T(0) = 0\) implies that \(C = 0\) and so

\[
T(x) = -\frac{2x}{(1 - x)^2} - \frac{2 \ln(1 - x)}{(1 - x)^2}
\]

\[
= -2 \sum_{n=0}^{\infty} nx^n + 2 \sum_{n=0}^{\infty} \left( \sum_{k=1}^{n} \frac{n - k + 1}{k} \right) x^n
\]

So

\[
T_n = -4n + 2(n + 1) \sum_{k=1}^{n} \frac{1}{k}
\approx 2n \ln n.
\]
Hashing

Let $U = \{0, 1, \ldots, N - 1\}$ and $H = \{0, 1, \ldots, n - 1\}$ where $n$ divides $N$ and $N \gg n$. $f : U \rightarrow H$, $f(u) = u \mod n$.

($H$ is a hash table and $U$ is the universe of objects from which a subset is to be stored in the table.)

Suppose $u_1, u_2, \ldots, u_m$, $m = \alpha n$, are a random subset of $U$. A copy of $u_i$ is stored in “cell” $f(u_i)$ and $u_i$’s that “hash” to the same cell are stored as a linked list.

Questions: $u$ is chosen uniformly from $U$.

(i) What is the expected time $T_1$ to determine whether or not $u$ is in the table?

(ii) If it is given that $u$ is in the table, what is the expected time $T_2$ to find where it is placed?

Time = The number of comparisons between elements of $U$ needed.
Let $M = N/n$, the average number of $u's$ that map to a cell. Let $X_k$ denote the number of $u_i$ for which $f(u_i) = k$. Then

$$E(T_1) = \sum_{k=1}^{n} E(T_1 \mid f(u) = k) \cdot P(f(u) = k)$$

$$= \frac{1}{n} \sum_{k=1}^{n} E(T_1 \mid f(u) = k)$$

$$\leq \frac{1}{n} \sum_{k=1}^{n} E(X_k)$$

$$= \frac{1}{n} E \left( \sum_{k=1}^{n} X_k \right)$$

$$= \alpha.$$
Let $X$ denote $X_1, X_2, \ldots, X_n$ and let $\mathcal{X}$ denote the set of possible values for $X$. Then

$$E(T_2) = \sum_{X \in \mathcal{X}} E(T_2 \mid X)P(X)$$

$$= \sum_{X \in \mathcal{X}} \sum_{k=1}^{n} E(T_2 \mid f(u) = k, X)P(f(u) = k)P(X)$$

$$= \sum_{X \in \mathcal{X}} \sum_{k=1}^{n} E(T_2 \mid f(u) = k, X) \frac{X_k}{m} P(X)$$

$$= \sum_{X \in \mathcal{X}} \sum_{k=1}^{n} \left( \frac{1 + X_k}{2} \right) \frac{X_k}{m} P(X)$$

$$= \frac{1}{2m} \sum_{X \in \mathcal{X}} \sum_{k=1}^{n} X_k(1 + X_k)P(X)$$
\[ E(T_2) = \frac{1}{2} + \frac{1}{2M} \mathbb{E}(X_1^2 + \cdots + X_n^2) \]

\[ = \frac{1}{2} + \frac{1}{2\alpha} \mathbb{E}(X_1^2) \]

\[ = \frac{1}{2} + \frac{1}{2\alpha} \sum_{t=1}^{m} t^2 \frac{M}{t} \frac{(N-M)}{(m-t)} \frac{(N)}{(m)} \]

Probabilistic Method
If $\alpha$ is small and $t$ is small then we can write

$$\binom{M}{t} \binom{N-M}{m-t} \frac{(N)_m}{(m)_t} \approx \frac{M^t (N - M)^{m-t}}{t! (m - t)!} \frac{m!}{N^m}$$

$$\approx \left(1 - \frac{1}{n}\right)^m \frac{m^t}{t! n^t}$$

$$\approx \alpha^t e^{-\alpha} \frac{m^t}{t!}.$$

Then we can further write

$$E(T_2) \approx \frac{1}{2} + \frac{1}{2\alpha} \sum_{t=1}^\infty t^2 \frac{\alpha^t e^{-\alpha}}{t!} = 1 + \frac{\alpha}{2}$$
Finding Minimum

Consider the following program which computes the minimum of the \( n \) numbers \( x_1, x_2, \ldots, x_n \).

\begin{verbatim}
begin
\hspace{1em}min := \infty;
\hspace{1em}for \ i = 1 \ to \ n \ do
\hspace{2em}begin
\hspace{3em}if \ x_i < min \ then \ min := x_i
\hspace{2em}end
\hspace{1em}output min
end
\end{verbatim}

If the \( x_i \) are all different and in random order, what is the expected number of times that that the statement \( min := x_i \) is executed?

Probabilistic Method
\[ \Omega = \{\text{permutations of } 1, 2, \ldots, n\} \] – uniform distribution.
Let \( X \) be the number of executions of statement \( \text{min} := x_i \). Let

\[
X_i = \begin{cases} 
1 & \text{statement executed at } i. \\
0 & \text{otherwise}
\end{cases}
\]

Then \( X_i = 1 \) iff \( x_i = \min\{x_1, x_2, \ldots, x_i\} \) and so

\[
P(X_i = 1) = \frac{(i - 1)!}{i!} = \frac{1}{i^i}.
\]

[The number of permutations of \( \{x_1, x_2, \ldots, x_i\} \) in which \( x_i \) is the largest is \((i - 1)!\).]
So

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

\[
= \sum_{i=1}^{n} E(X_i)
\]

\[
= \sum_{i=1}^{n} \frac{1}{i} \quad (= H_n)
\]

\[
\approx \log_e n.
\]
Inequalities

Markov Inequality: let $X : \Omega \rightarrow \{0, 1, 2, \ldots, \}$ be a random variable. For any $t \geq 1$

$$P(X \geq t) \leq \frac{E(X)}{t}.$$ 

Proof

$$E(X) = \sum_{k=0}^{\infty} kP(X = k) \geq \sum_{k=t}^{\infty} kP(X = k) \geq \sum_{k=t}^{\infty} tP(X = k) = tP(X \geq t).$$

In particular, if $t = 1$ then $P(X \neq 0) \leq E(X)$. 

Probabilistic Method
Chebycheff Inequality

Now let $\sigma = \sqrt{\text{Var}(Z)}$.

$$
P(|Z - \mu| \geq t\sigma) = P((Z - \mu)^2 \geq t^2\sigma^2) \\
\leq \frac{E((Z - \mu)^2)}{t^2\sigma^2} \\
= \frac{1}{t^2}.
$$

(1) comes from the Markov inequality applied to the random variable $(Z - \mu)^2$.

Back to Binomial: $\sigma = \sqrt{np(1-p)}$.

$$
P(|B_{n,p} - np| \geq t\sqrt{np(1-p)}) \leq \frac{1}{t^2}
$$

which implies

$$
P(|B_{n,p} - np| \geq \epsilon np) \leq \frac{1}{\epsilon^2 np}
$$

[Law of large numbers.]
Hoeffding’s Inequality – I

Let $X_1, X_2, \ldots, X_n$ be independent random variables taking values such that $\Pr(X_i = 1) = 1/2 = \Pr(X_i = -1)$ for $i = 1, 2, \ldots, n$. Let $X = X_1 + X_2 + \cdots + X_n$. Then for any $t \geq 0$

$$\Pr(|X| \geq t) < 2e^{-t^2/2n}.$$ 

**Proof:** For any $\lambda > 0$ we have

$$\Pr(X \geq t) = \Pr(e^{\lambda X} \geq e^{\lambda t}) \leq e^{-\lambda t} E(e^{\lambda X}).$$

Now for $i = 1, 2, \ldots, n$ we have

$$E(e^{\lambda X_i}) = \frac{e^{-\lambda} + e^{\lambda}}{2} = 1 + \frac{\lambda^2}{2!} + \frac{\lambda^4}{4!} + \cdots < e^{\lambda^2/2}.$$
So, by independence,

$$\mathbb{E}(e^{\lambda X}) = \mathbb{E}\left( \prod_{i=1}^{n} e^{\lambda X_i} \right) = \prod_{i=1}^{n} \mathbb{E}(e^{\lambda X_i}) \leq e^{\lambda^2 n/2}.$$ 

Hence,

$$\Pr(X \geq t) \leq e^{-\lambda t + \lambda^2 n/2}.$$ 

We choose $\lambda = t/n$ to minimise $-\lambda t + \lambda^2 n/2$. This yields

$$\Pr(X \geq t) \leq e^{-t^2/2n}.$$ 

Similarly,

$$\Pr(X \leq -t) = \Pr(e^{-\lambda X} \geq e^{\lambda t}) \leq e^{-\lambda t} \mathbb{E}(e^{-\lambda X}) \leq e^{-\lambda t + \lambda^2 n/2}.$$
Suppose that $|X| = n$ and $\mathcal{F} \subseteq \mathcal{P}(X)$. If we color the elements of $X$ with Red and Blue i.e. partition $X$ in $R \cup B$ then the discrepancy $\text{disc}(\mathcal{F}, R, B)$ of this coloring is defined

$$\text{disc}(\mathcal{F}, R, B) = \max_{F \in \mathcal{F}} \text{disc}(F, R, B)$$

where $\text{disc}(F, R, B) = ||R \cap F| - |B \cap F||$ i.e. the absolute difference between the number of elements of $F$ that are colored Red and the number that are colored Blue.
Claim:

If $|\mathcal{F}| = m$ then there exists a coloring $R, B$ such that $\text{disc}(\mathcal{F}, R, B) \leq (2n \log_e(2m))^{1/2}$.

**Proof** Fix $F \in \mathcal{F}$ and let $s = |F|$. If we color $X$ randomly and let $Z = |R \cap F| - |B \cap F|$ then $Z$ is the sum of $s$ independent $\pm 1$ random variables.

So, by the Hoeffding inequality,

$$\Pr(|Z| \geq (2n \log_e(2m))^{1/2}) < 2e^{-n \log_e(2m)/s} \leq \frac{1}{m}.$$
Switching Game:

We are given an $n \times n$ matrix $A$ where $A(i, j) = \pm 1$. We interpret $A(i, j) = 1$ as the light at $i, j$ is on.

Now suppose that $x, y \in \{\pm 1\}^n$ are switches. The light at $i, j$ is on if $A(i, j)x_iy_j = 1$ and off otherwise.

Let $\sigma(A) = \max_{x,y} \left| \sum_{i,j} A(i, j)x_iy_j \right|$ be the maximum absolute difference between the number of lights which are on and those that are off, obtainable by switching.

**Claim:** There exists $A$ such that $\sigma(A) \leq cn^{3/2}$ where $c = 2(\ln 2)^{1/2}$. 

Probabilistic Method
Fix \( x, y \in \{\pm 1\}^n \) and let \( A \) be a random \( \pm 1 \) matrix. Consider the random variable

\[
Z_{x,y} = \sum_{i,j} A(i,j) x_i y_j.
\]

This is the sum of \( n^2 \) independent random variables \( (A(i,j) x_i y_j) \) taking values in \( \pm 1 \).

It follows from the Hoeffding inequality that

\[
|Z_{x,y}| \geq cn^{3/2} < 2e^{-(cn^{3/2})^2/2n^2} = 2^{-2n}
\]

So

\[
\Pr(\max_{x,y} |Z_{x,y}| \geq cn^{3/2}) < 2^n \times 2^n \times = 2^{-2n} = 1.
\]

Hence there exists \( A \) such that \( \sigma(A) \leq cn^{3/2} \).
Hoeffding’s Inequality – II

Now let $S_n = X_1 + X_2 + \cdots + X_n$ where $X_i, i = 1, \ldots, n$ are independent random variables where $0 \leq X_i \leq 1$ and $E X_i = \mu_i$ for $i = 1, 2, \ldots, n$. Let $\mu = \mu_1 + \mu_2 + \cdots + \mu_n$. Then for $\lambda \geq 0$

$$P(S_n \geq \mu + t) \leq e^{-\lambda(\mu + t)} \prod_{i=1}^{n} E(e^{\lambda X_i})$$

(2)

and for $\lambda \leq 0$

$$P(S_n \leq \mu - t) \leq e^{-\lambda(\mu - t)} \prod_{i=1}^{n} E(e^{\lambda X_i}).$$

(3)

Now the convexity of $e^x$ and $0 \leq X_i \leq 1$ implies that

$$e^{\lambda X_i} \leq 1 - X_i + X_i e^\lambda.$$

Taking expectations we get

$$E(e^{\lambda X_i}) \leq 1 - \mu_i + \mu_i e^\lambda.$$
Equation (2) becomes, for $\lambda \geq 0$,

$$P(S_n \geq \mu + t) \leq e^{-\lambda(\mu+t)} \prod_{i=1}^{n}(1 - \mu_i + \mu_i e^\lambda)$$

$$\leq e^{-\lambda(\mu+t)} \left( \frac{n - \mu + \mu e^\lambda}{n} \right)^n. \quad (4)$$

The second inequality follows from the fact that the geometric mean is at most the arithmetic mean i.e.

$$(x_1 x_2 \cdots x_n)^{1/n} \leq \frac{x_1 + x_2 + \cdots + x_n}{n}$$

for non-negative $x_1, x_2, \ldots, x_n$. The right hand side of (4) attains its minimum, as a function of $\lambda$, at

$$e^\lambda = \frac{(\mu + t)(n - \mu)}{(n - \mu - t)\mu}. \quad (5)$$
Hence, by (4) and (5), assuming that $\mu + t < n$,

$$P(S_n \geq \mu + t) \leq \left(\frac{\mu}{\mu + t}\right)^{\mu + t} \left(\frac{n - \mu}{n - \mu - t}\right)^{n - \mu - t},$$

while for $t > n - \mu$ this probability is zero.

Now let

$$0 \leq \phi(x) = (1 + x) \log(1 + x) - x, \quad x \geq -1,$$

and let $\phi(x) = \infty$ for $x < -1$. Now, for $0 \leq t \leq n - \mu$, we can rewrite the bound (50) as

$$P(S_n \geq \mu + t) \leq \exp\left\{-\mu \phi\left(\frac{t}{\mu}\right) - (n - \mu)\phi\left(-\frac{t}{n - \mu}\right)\right\}.$$

Since $\phi(x) \geq 0$ for every $x \geq -1$, we get

$$\Pr(S_n \geq \mu + t) \leq e^{-\mu \phi(t/\mu)}.$$  \hfill (6)
Similarly, putting $n - S_n$ for $S_n$, or by an analogous argument, using (3), we get for $0 \leq t \leq \mu$,

$$P(S_n \leq \mu - t) \leq \exp \left\{-\mu \phi \left(\frac{-t}{\mu}\right) - (n - \mu) \phi \left(\frac{t}{n - \mu}\right)\right\}.$$  

Hence,

$$P(S_n \leq \mu - t) \leq e^{-\mu \phi(-t/\mu)}. \quad (7)$$
We can simplify the expressions (6) and (7) by observing that

\[ \phi(x) \geq \frac{x^2}{2(1 + \frac{x}{3})}. \]  

(8)

To see this observe that for \( |x| \leq 1 \) we have

\[
\phi(x) - \frac{x^2}{2(1 + \frac{x}{3})} = \sum_{k=2}^{\infty} (-1)^k \left( \frac{1}{k(k-1)} - \frac{1}{2 \cdot 3^{k-2}} \right) x^k.
\]

Equation (8) for \( |x| \leq 1 \) follows from \( \frac{1}{k(k-1)} - \frac{1}{2 \cdot 3^{k-2}} \geq 0 \) for \( k \geq 2 \).

For \( x \geq 1 \) we let \( f(x) = \phi(x) - \frac{x^2}{2(1 + \frac{x}{3})} \) and then check that \( f'(1) \geq 0 \) and

\[
f'(x) = \log(1+x) - 3 + \frac{9}{3 + x} + \frac{3x^2}{(3 + x)^2} \geq \log 2 - 0.75 + \frac{3x^2}{(3 + x)^2} \geq 0
\]

for \( x \geq 1 \).
Taking this into account we arrive at the following theorem,

**Theorem 2**

Suppose that $S_n = X_1 + X_2 + \cdots + X_n$ where (i) $0 \leq X_i \leq 1$ and $E X_i = \mu_i$ for $i = 1, 2, \ldots, n$, (ii) $X_1, X_2, \ldots, X_n$ are independent. Let $\mu = \mu_1 + \mu_2 + \cdots + \mu_n$. Then for $t \geq 0,$

$$P(S_n \geq \mu + t) \leq \exp \left\{ -\frac{t^2}{2(\mu + \frac{t}{3})} \right\}$$

and for $t \leq \mu,$

$$P(S_n \leq \mu - t) \leq \exp \left\{ -\frac{t^2}{2(\mu - \frac{t}{3})} \right\}.$$ (9)
Putting \( t = \epsilon \mu \), for \( 0 < \epsilon < 1 \), one can immediately obtain the following bounds.

**Corollary 3**

Let \( 0 < \epsilon < 1 \), then

\[
P(S_n \geq (1 + \epsilon)\mu) \leq \left( \frac{e^{\epsilon}}{(1 + \epsilon)^{1+\epsilon}} \right)^\mu \leq \exp \left\{ -\frac{\mu \epsilon^2}{3} \right\},
\]

while

\[
P(S_n \leq (1 - \epsilon)\mu) \leq \exp \left\{ -\frac{\mu \epsilon^2}{2} \right\}
\]

The formula (3) follows directly from (9) and (3) follows from (50).
For large deviations we have the following result.

**Corollary 4**

*If* $c > 1$ *then*

$$P(S_n \geq c\mu) \leq \left\{ \frac{e}{ce^{1/c}} \right\}^{c\mu} \leq \left( \frac{e}{c} \right)^{c\mu}. \quad (10)$$

Put $t = (c - 1)\mu$ into (6).
Valiant-Brebner routing algorithm:

Let $Q_n = (V_n = \{0, 1\}^n, E_n)$ be the $n$-cube where $(x, y) \in E_n$ iff

$$h(x, y) = | \{j : x_j \neq y_j\} | = 1.$$ 

Given a permutation $\pi : V_n \rightarrow V_n$ we wish to synchronously send a packet $p_x$ from $x$ to $\pi(x)$ along a path of $Q_n$ for all $x \in V_n$.

At most one packet can cross any edge in one time step. Packets form a queue waiting to cross.
Bit Fixing Path: Given $x, y$ let $z_i = (y_1, y_2, \ldots, y_i, x_{i+1}, \ldots, x_n)$. Let $BFP(x, y)$ be the path $(x, z_1, z_2, \ldots, z_n = y)$.

Step 1: For each $x \in V_n$ choose $\delta(x)$ independently and randomly from $V_n$.

Step 2: Send packet $p_x$ to $\delta(x)$ along the path $P(x) = BFP(x, \delta(x))$.

Step 3: Send packet $p_x$ to $\pi(x)$ along the path $Q(x) = BFP(\delta(x), \pi(x))$.

Note that for a given $x$, $P(x) = (x, x_1, x_2, \ldots, x_n = \delta(x))$ where $x_{i+1}$ is obtained from $x_i$ by flipping the $i + 1$th bit of $x_i$ with probability $1/2$. Note also that the length of $P(x)$ is equal to the number of $i$ such that $x_{i+1} \neq x_i$. 

Probabilistic Method
Let $D(x)$ be the time spent by $p_x$ waiting in a queue. Let

$$S(x) = \{y \neq x : P(x) \cap P(y) \neq \emptyset\}.$$ 

Observation: $D(x) \leq |S(x)|$. This follows from $|P(x) \cap P(y)| \leq 1$ for all $x, y$. This follows from the fact that paths can meet, continue together for a while and diverge. They cannot meet again once they diverge.

We claim that

$$P(|S(x)| \geq 3n) \leq 3^{-n}. \quad (11)$$

It follows from this that

$$P(\exists x : \text{Step 2 takes more than } 4n \text{ time}) \leq 2^n \times 3^{-n} = o(1).$$

Step 3 can be analysed similarly.
**Proof of (11):** We write

\[ |S(x)| = \sum_{y \in V_n \setminus \{x\}} Z_y \]

where

\[ Z_y = 1_{P_y \cap P_x \neq \emptyset}. \]

Observe next that if \( u, v \) are chosen randomly from \( V_n \) then

\[ \sum_{x, y \in V_n} P(P(x) \cap P(y) \neq \emptyset) = 2^{2n} P(P(v) \cap P(u) \neq \emptyset) \]

\[ \leq 2^{2n} \sum_{k=1}^{n} \frac{1}{2^{k+1}} \cdot \frac{1}{2^{n-k}} \]

\[ = 2^{n-1} n. \]

Here \( P(v) \cap P(u) \neq \emptyset \) only if there is some \( k \) such that \( u, v \) agree on the last \( n - k \) components and \( P(u) \) amends the first \( k + 1 \) components of \( u \) so that they agree with the first \( k + 1 \) components of the \( k + 1 \)st vertex of \( P(v) \).
On the other hand, symmetry yields that for any fixed \( x \in V_n \),

\[
\sum_{x, y \in V_n} P(P(x) \cap P(y) \neq \emptyset) = 2^n \sum_{y \in V_n} P(P(x) \cap P(y) \neq \emptyset) \\
\geq 2^n E(|S(x)|).
\]

It follows that

\[ E(|S(x)|) \leq \frac{n}{2}. \]

Applying the Chernoff bound (10) we see that

\[ P(|S(x)| \geq \alpha n) \leq \left( \frac{e}{2\alpha} \right)^{\alpha n} \]

and we obtain (11) by putting \( \alpha = 3 \).
Independent sets and cliques

$S \subseteq V$ is *independent* if no edge of $G$ has both of its endpoints in $S$.

$\alpha(G)$ = maximum size of an independent set of $G$. 

Theorem 5

If graph $G$ has $n$ vertices and $m$ edges then

$$\alpha(G) \geq \frac{n^2}{2m + n}.$$ 

Note that this says that $\alpha(G)$ is at least $\frac{n}{d+1}$ where $d$ is the average degree of $G$.

**Proof** Let $\pi(1), \pi(2), \ldots, \pi(\nu)$ be an arbitrary permutation of $V$. Let $N(\nu)$ denote the set of neighbours of vertex $\nu$ and let

$$I(\pi) = \{ \nu : \pi(w) > \pi(\nu) \text{ for all } w \in N(\nu) \}.$$
Claim 1

$I$ is an independent set.

Proof of Claim 1

Suppose $w_1, w_2 \in I(\pi)$ and $w_1 w_2 \in E$. Suppose $\pi(w_1) < \pi(w_2)$. Then $w_2 \notin I(\pi)$ — contradiction.
\textbf{Probabilistic Method}

\begin{itemize}
\item \(\pi_1\) \textcolor{blue}{\{c, f\}}
\item \(\pi_2\) \textcolor{blue}{\{g, a\}}
\end{itemize}
Claim 2

If \( \pi \) is a random permutation then

\[
E(|I|) = \sum_{v \in V} \frac{1}{d(v) + 1}.
\]

Proof: Let \( \delta(v) = \begin{cases} 
1 & v \in I \\
0 & v \notin I 
\end{cases} \)

Thus

\[
|I| = \sum_{v \in V} \delta(v)
\]

\[
E(|I|) = \sum_{v \in V} E(\delta(v))
\]

\[
= \sum_{v \in V} \Pr(\delta(v) = 1).
\]
Now $\delta(v) = 1$ iff $v$ comes before all of its neighbours in the order $\pi$. Thus

$$\Pr(\delta(v) = 1) = \frac{1}{d(v) + 1}$$

and the claim follows.

Thus there exists a $\pi$ such that

$$|I(\pi)| \geq \sum_{v \in V} \frac{1}{d(v) + 1}$$

and so

$$\alpha(G) \geq \sum_{v \in V} \frac{1}{d(v) + 1}.$$
We finish the proof of the theorem by showing that

\[
\sum_{v \in V} \frac{1}{d(v) + 1} \geq \frac{n^2}{2m + n}.
\]

This follows from the following claim by putting \( x_v = d(v) + 1 \) for \( v \in V \).

**Claim 3**

*If \( x_1, x_2, \ldots, x_k > 0 \) then*

\[
\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} \geq \frac{k^2}{x_1 + x_2 + \cdots + x_k}.
\]
Proof

Multiplying (3) by $x_1 + x_2 + \cdots + x_k$ and subtracting $k$ from both sides we see that (3) is equivalent to

$$\sum_{1 \leq i < j \leq k} \left( \frac{x_i}{x_j} + \frac{x_j}{x_i} \right) \geq k(k - 1).$$

But for all $x, y > 0$

$$\frac{x}{y} + \frac{y}{x} \geq 2$$

and (68) follows. \qed
Corollary 6

If $G$ contains no clique of size $k$ then

$$m \leq \frac{(k - 2)n^2}{2(k - 1)}$$

For example, if $G$ contains no triangle then $m \leq n^2/4$.

**Proof** Let $\bar{G}$ be the complement of $G$ i.e. $G + \bar{G} = K_n$.

By assumption

$$k - 1 \geq \alpha(\bar{G}) \geq \frac{n^2}{n(n - 1) - 2m + n}.$$
Parallel searching for the maximum – Valiant

We have $n$ processors and $n$ numbers $x_1, x_2, \ldots, x_n$. In each round we choose $n$ pairs $i, j$ and compare the values of $x_i, x_j$. The set of pairs chosen in a round can depend on the results of previous comparisons.

**Aim:** find $i^*$ such that $x_{i^*} = \max_j x_j$.

**Claim 4**

*For any algorithm there exists an input which requires at least $\frac{1}{2} \log_2 \log_2 n$ rounds.*
Suppose that the first round of comparisons involves comparing $x_i, x_j$ for edge $ij$ of the above graph and that the arrows point to the larger of the two values. Consider the independent set {1, 2, 5, 8, 9}. These are the indices of the 5 largest elements, but their relative order can be arbitrary since there is no implied relation between their values.
Let $C(a, b)$ be the maximum number of rounds needed for $a$ processors to compute the maximum of $b$ values in this way.

**Lemma 7**

$$C(a, b) \geq 1 + C \left( a, \left\lceil \frac{b^2}{2a+b} \right\rceil \right).$$

**Proof** The set of $b$ comparisons defines a $b$-edge graph $G$ on $a$ vertices where comparison of $x_i, x_j$ produces an edge $ij$ of $G$. Now,

$$\alpha(G) \geq \left\lceil \frac{b}{2a/b + 1} \right\rceil = \left\lceil \frac{b^2}{2a+b} \right\rceil.$$
For any independent set $I$ it is always possible to define values for $x_1, x_2, \ldots, x_a$ such $I$ is the index set of the $|I|$ largest values and so that the comparisons do not yield any information about the ordering of the elements $x_i, i \in I$.

Thus after one round one has the problem of finding the maximum among $\alpha(G)$ elements.

Now define the sequence $c_0, c_1, \ldots$ by $c_0 = n$ and

$$c_{i+1} = \left\lceil \frac{c_i^2}{2n + c_i} \right\rceil.$$

It follows from the previous lemma that

$$c_k \geq 2 \text{ implies } C(n, n) \geq k + 1.$$
Claim 4 now follows from

**Claim 5**

\[ c_i \geq \frac{n}{3^{2^i} - 1}. \]

By induction on \( i \). Trivial for \( i = 0 \). Then

\[
c_{i+1} \geq \frac{n^2}{3^{2^i} - 2} \times \frac{1}{2n + \frac{n}{3^{2^i} - 1}} \]

\[
= \frac{n}{3^{2^i+1} - 1} \times \frac{3}{2 + \frac{1}{3^{2^i} - 1}}
\]

\[
\geq \frac{n}{3^{2^i+1} - 1}.
\]

\[ \square \]
The Local Lemma

We go back to the coloring problem at the beginning of these slides. We now place a different restriction on the sets involved.

Theorem 8

Let $A_1, A_2, \ldots, A_n$ be subsets of $A$ where $|A_i| \geq k$ for $1 \leq i \leq n$. If each $A_i$ intersects at most $2^{k-3}$ other sets then there exists a partition $A = R \cup B$ such that

$$A_i \cap R \neq \emptyset \text{ and } A_i \cap B \neq \emptyset \quad 1 \leq i \leq n.$$
Symmetric Local Lemma: We consider the following situation. 

\( X = \{x_1, x_2, \ldots, x_N\} \) is a collection of independent random variables. Suppose that we have events \( E_i, i = 1, 2, \ldots, m \) where \( E_i \) depends only on the set \( X_i \subseteq X \). Thus if \( X_i \cap X_j = \emptyset \) then \( E_i \) and \( E_j \) are independent.

The dependency graph \( \Gamma \) has vertex set \([m]\) and an edge \((i, j)\) iff \( X_i \cap X_j \neq \emptyset \).

**Theorem 9**

Let

\[
p = \max_i P(E_i) \text{ and let } d \text{ be the maximum degree of } \Gamma.
\]

\[
4dp \leq 1 \text{ implies that } P \left( \bigcap_{i=1}^{m} \bar{E}_i \right) \geq (1 - 2p)^m > 0.
\]
Proof: We prove by induction on $|S|$ that for any $i$,

$$P \left( \mathcal{E}_i \bigg| \bigcap_{j \in S} \bar{\mathcal{E}}_j \right) \leq 2p. \quad (12)$$

Notice that this suffices, since

$$P \left( \bigcap_{i=1}^{m} \bar{\mathcal{E}}_i \right) = \prod_{i=1}^{m} P \left( \mathcal{E}_i \bigg| \bigcap_{j=1}^{i-1} \bar{\mathcal{E}}_j \right)$$

The base case $|S| = 0$ for (12) is trivial.
Inductive Step: Renumber for convenience so that \( i = n, S = [s] \) and \( (i, x) \notin \Gamma \) for \( x > d \). Now

\[
P \left( \mathcal{E}_n \bigg| \bigcap_{i=1}^{s} \bar{\mathcal{E}}_i \right) = \frac{P \left( \mathcal{E}_n \cap \bigcap_{i=1}^{d} \bar{\mathcal{E}}_i \bigg| \bigcap_{i=d+1}^{s} \bar{\mathcal{E}}_i \right)}{P \left( \bigcap_{i=1}^{d} \bar{\mathcal{E}}_i \bigg| \bigcap_{i=d+1}^{s} \bar{\mathcal{E}}_i \right)},
\]

\[
\leq \frac{P \left( \mathcal{E}_n \bigg| \bigcap_{i=d+1}^{s} \bar{\mathcal{E}}_i \right)}{P \left( \bigcap_{i=1}^{d} \bar{\mathcal{E}}_i \bigg| \bigcap_{i=d+1}^{s} \bar{\mathcal{E}}_i \right)},
\]

\[
\leq \frac{P \left( \mathcal{E}_n \bigg| \bigcap_{i=d+1}^{s} \bar{\mathcal{E}}_i \right)}{1 - \sum_{i=1}^{d} P \left( \mathcal{E}_i \bigg| \bigcap_{i=d+1}^{s} \bar{\mathcal{E}}_i \right)}.
\] (13)
Now
\[
P\left(\mathcal{E}_n \middle| \bigcap_{i=d+1}^{s} \bar{\mathcal{E}}_i\right) = P(\mathcal{E}_n) \leq p,
\]
(14)
since \(\mathcal{E}_n\) is independent of \(\mathcal{E}_{d+1}, \ldots, \mathcal{E}_s\).

Furthermore, we can assume that \(d > 0\), else the events \(\mathcal{E}_1, \ldots, \mathcal{E}_m\) are independent and the result is trivial. So, by induction, we have that

\[
1 - \sum_{i=1}^{d} P\left(\mathcal{E}_i \middle| \bigcap_{i=d+1}^{s} \bar{\mathcal{E}}_i\right) \geq 1 - 2dp \geq \frac{1}{2}.
\]
(15)

The induction is now completed by using (14) and (15) in (13).
Proof of Theorem 8: We randomly color the elements of $A$ Red and Blue. Let $E_i$ be the event that $A_i$ is mono-colored. Clearly, $P(E_i) \leq 2^{-(k-1)}$. Thus,

$$p \leq 2^{-(k-1)}.$$ 

The degree of vertex $i$ of $\Gamma$ is the number of $j$ such that $A_i \cap A_j \neq \emptyset$. So, by assumption,

$$d \leq 2^{k-3}.$$ 

Theorem 9 implies that $P(\bigcap_{i=1}^{n} \bar{E}_i) > 0$ and so the required coloring exists.
Theorem 10

Let $G = (V, E)$ be an $r$-regular graph. If $r$ is sufficiently large, then $E$ can be partitioned into $E_1, E_2$ so that if $G_i = (V, E_i), i = 1, 2$ then

$$\frac{r}{2} - (20r \log r)^{1/2} \leq \delta(G_i) \leq \Delta(G_i) \leq \frac{r}{2} + (20r \log r)^{1/2}.$$

Proof: We randomly partition the edges of $G$ by independently placing $e$ into $E_1 E_1$ with probability $1/2$. For $v \in V$, we let $E_v$ be the event that the degree $d_1(v)$ in $G_1$ satisfies

$$d_1(v) \notin \left[ \frac{r}{2} - 3(r \log r)^{1/2}, \frac{r}{2} + 3(r \log r)^{1/2} \right].$$
It follows from Corollary 3 with $\epsilon = \left(\frac{9 \log r}{r}\right)^{1/2}$ that

$$P(\mathcal{E}_v) \leq 2e^{-\epsilon^2 r/6} = 2r^{-3/2}.$$ 

Furthermore, if $\mathcal{E}_v$ is independent of the events $\mathcal{E}_w$ for vertices $w$ at distance 2 or more from $v$ in $G$. Thus,

$$d \leq r.$$ 

Clearly, $4 \cdot 2r^{-3/2} \cdot r \leq 1$ for $r$ large and the result follows from Theorem 9. I.e. $P(\bigcap_{v \in V} \mathcal{E}_v) > 0$ which implies that there exists a partition where none of the events $\mathcal{E}_v, v \in V$ occur.
For the next application, let $D = (V, E)$ be a $k$-regular digraph. By this we mean that each vertex has exactly $k$ in-neighbors and $k$ out-neighbors.

**Theorem 11**

*Every $k$-regular digraph has a collection of $\lfloor k/(4 \log k) \rfloor$ vertex disjoint cycles.*

**Proof:** Let $r = \lfloor k/(4 \log k) \rfloor$ and color the vertices of $D$ with colors $[r]$. For $v \in V$, let $E_v$ be the event that there is a color missing at the out-neighbors of $v$. We will show that $P(\bigcap_{v \in V} \bar{E}_v) > 0$.

Suppose then that none of the events $E_v, v \in V$ occur. Consider the graph $D_j$ induced by a single color $j \in [r]$. Note that $D_j$ is not the empty graph. Let $P_j = (v_1, v_2, \ldots, v_m)$ be a longest directed path in $D_j$. Let $w$ be an out-neighbor of $v_m$ of color $j$. We must have $w \in \{v_1, \ldots, v_m\}$, else $P_j$ is not a longest path in $D_j$. Thus each $D_j, j \in [r]$ contains a cycle and these cycles are vertex disjoint.
We first estimate
\[
P(\mathcal{E}_v) \leq k \left(1 - \frac{1}{r}\right)^k \leq ke^{-k/r} \leq ke^{-4\log{k}} = k^{-3}.
\]

On the other hand, if \( N^+(v) \) denotes the out-neighbors of \( v \) plus \( v \) then \( \mathcal{E}_v \) is independent of all events \( \mathcal{E}_w \) for which \( N^+(v) \cap N^+(w) = \emptyset \). It follows that
\[
d \leq k^2.
\]

To apply Theorem 9 we need to have \( 4k^{-3}k^2 \leq 1 \). This is true for \( k \geq 4 \). For \( k \leq 3 \) we have \( r = 1 \) and the local lemma is not needed.
Constructive version: Moser/Tardos
Suppose now that in the context of Theorem 9 we have
\[ p \frac{d^d}{(d - 1)^{d-1}} \leq 1. \]  \hspace{1cm} (16)
(Notice that this is a weaker assumption than \( 4dp \leq 1 \).)

Algorithm MT:

Step 1. Assign values to \( x_1, x_2, \ldots, x_N \).
Step 2. While \( \exists j : \mathcal{E}_j \) holds do
Step 3. Pick smallest \( j \) such that \( \mathcal{E}_j \) occurs.
Step 4. Randomly re-set \( \{ x \in X_j \} \).
Step 5. od
Theorem 12

Assuming (16) holds, algorithm MT that finds an assignment of values to \( x \in X \) such that \( \bigcap_{i=1}^{m} \bar{E}_i \) holds in \( O(N) \) expected number of iterations.

Let \( j_t \) be the value of \( j \) in Step 3 at the \( t \)th execution of Steps 2–5.

The LOG of the execution is the sequence \( Y_t = X_{j_t}, \ t \geq 1 \).

For \( j \in M \) we let \( \text{COUNT}(j) \) denote the number of times that \( j_t = j \).
Theorem 12 follows from Lemma 13

**Lemma 13**

\[ E(COUNT(j)) \leq \frac{1}{d-1} \text{ for } j \in [m]. \]

It follows that the expected length of LOG is at most \( \frac{m}{d-1} \). Then \( m \leq Nd \) because each \( x \in X \) can be in at most \( d \) of the \( X_i \)'s.

**Proof of Lemma 13:** Given an execution of MT of length at least \( t \) we define a rooted tree \( TREE(t) \) with vertices from \( X_1, X_2, \ldots, X_m \) as follows: Its root is \( Y_t \). Now for \( i = t - 1, t - 2, \ldots, 1 \) we see if there exists \( k \) such that \( i < k \leq t \) and \( Y_i \cap Y_k \neq \emptyset \). If so, choose \( Y_k \) furthest from the root and make \( Y_i \) a child of \( Y_k \). Otherwise do nothing.
We observe the following:

**P1** $s \neq t$ implies that $\text{TREE}(s) \neq \text{TREE}(t)$.
Reason: Suppose not and $Y = Y_s = Y_t$. Then $\text{TREE}(t)$ will have at least one more appearance of $Y$ (its root) than $\text{TREE}(s)$, contradiction.

**P2** If $Y'$, $Y''$ are children of $Y$ in $\text{TREE}(t)$ then $Y' \cap Y'' = \emptyset$.
Reason: Otherwise, $Y''$ is a child of $Y'$ or vice-versa.

**P3** Let $x \in X$ and let $Y_{i_1}, Y_{i_2}, \ldots, Y_{i_s}$ be those $Y_i$ that contain $x$, ordered by their appearance in LOG. Then each value for $x$ comes from a different independent sample.
Reason: Because $Y_{i_a}$ appears in LOG, we re-sample the random variables in $Y_{i_a} \cap Y_{i_{a+1}}$ before $Y_{i_{a+1}}$ appears.
Next let $T$ be a rooted tree with vertices labelled by $X_1, X_2, \ldots, X_m$ such that if $Y'$ is a child of $Y$ then $Y \cap Y' \neq \emptyset$. Let $OCCUR(T)$ be the event that $TREE(t) = T$ for some $t$.

\[ P(OCCUR(T)) \leq p^{|T|}. \quad (17) \]

Let the vertices of $T = TREE(t)$ be $X_{i_1}, X_{i_2}, \ldots, X_{i_s}$ ordered by their appearance in LOG. Then

\[ P(OCCUR(T)) \leq \prod_{j=1}^{s} P\left( E_{i_j} \mid E_{i_1}, \ldots, E_{i_{j-1}} \right) = \prod_{j=1}^{s} P\left( E_{i_j} \right) \leq p^{|T|}. \]

The appearance of $X_{i_j}$ implies that $E_{i_j}$ has occurred and P3 means that the values of $x \in X_{i_j}$ are fresh with respect to $E_{i_1}, \ldots, E_{i_{j-1}}$. 

Probabilistic Method
Next let $\mathcal{T}$ denote an infinite tree with branching factor $d$ rooted at a vertex $\rho$. Then, for each $j$,

$$E(\text{Count}(j)) \leq y = \sum_{T} \rho^{|T|}$$

where $T$ ranges over subtrees of $\mathcal{T}$ that are rooted at $\rho$. This is because each occurrence of $Y_j$ corresponds to a distinct $T \subseteq \mathcal{T}$.

We complete the proof of Theorem 12 by proving

$$\xi \leq \frac{1}{d - 1}.$$  (18)
Let $\mathcal{T}_s$ denote the set of sub-trees of $\mathcal{T}$ that are rooted at $\rho$. Let $y_s = \sum_{T \in \mathcal{T}_s} p^{|T|}$ so that $y = \lim_{s \to \infty} y_s$. Then $y_0 \leq p$ and

$$y_{s+1} \leq p \sum_{i=0}^{d} \binom{d}{i} y^i_s. \quad (19)$$

Note that (19) follows from the fact that if $T \in \mathcal{T}_{s+1}$ then it will contain $\rho$ and $0 \leq i \leq d$ subtrees, each of which is isomorphic to a tree in $\mathcal{T}_s$. The factor $y^i_s$ follows from (17).

All that remains to prove (18) is to prove that $y_s \leq \frac{1}{d-1}$ for $s \geq 0$. We do this by induction on $s$. 

Probabilistic Method
Now for the base case we have

\[ y_0 \leq p \leq \frac{(d - 1)^{d-1}}{d^d} \leq \frac{1}{d - 1}. \]

For the inductive step we have

\[ y_{s+1} \leq p \sum_{i=0}^{d} \binom{d}{i} \frac{1}{(d - 1)^i} = p \left(1 + \frac{1}{d - 1}\right)^d \leq \frac{(d - 1)^{d-1}}{d^d} \cdot \left(\frac{d}{d - 1}\right)^d = \frac{1}{d - 1}. \]

Note that \( y_s \) is monotone increasing and bounded and so has a limit.