Karlsruhe Institute of Technology

# Probability & Computing

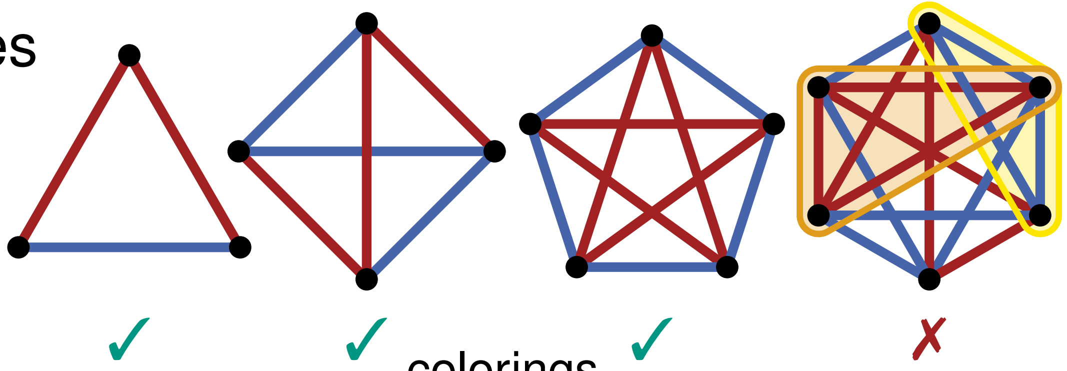
## Probabilistic Method

# Complete Coloring

Karlsruhe Institute of Technology

## The Problem

- Let $G$ be the complete graph on $n$ vertices (every vertex is adjacent to every other vertex)
- A $k$-clique is a complete subgraph with $k$ vertices
- A coloring of the graph assigns each edge one of two colors: red or blue
- In a graph with $n$ vertices, does there *exist* a coloring with *no* monochromatic $k$-clique?




colorings
$k = 3$

## The Solution?

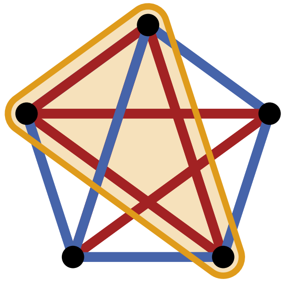
- Brute-force algorithm?
  - $n = 6 \Rightarrow 2^{n(n-1)} = 2^{30} = 1{,}073{,}741{,}824$ possible colorings
  - $k = 3 \Rightarrow \binom{6}{3} = 20$ triangles to check $\Rightarrow$ 60 edges per coloring
  - What about $n = 1000$ and $k = 20$?

  naive implementation: 20min
  no coloring exists
- Randomized algorithm?
  - How often shall we try before assuming that no coloring exists?

# Randomized Coloring

## Algorithm

- For each edge independently, choose one of the colors with probability $1/2$
- Let $X$ be the indicator variable with $X = 1$ if and only if the resulting coloring contains a monochromatic $k$-clique
- Let $H_1, \dots, H_{\binom{n}{k}}$ be all the different $k$-cliques
- Let $X_i$ be the indicator variable with $X_i = 1$ if and only if $H_i$ is monochromatic



$H_i$

- What is $\Pr[X_i = 1]$?
  - Consider the first edge that gets colored (we do not care which color it is, but...)
  - The $\binom{k}{2} - 1$ remaining edges need to get the same color

$$\Pr[X_i = 1] = \left(\tfrac{1}{2}\right)^{\binom{k}{2}-1}$$

$$= 2^{-\binom{k}{2}+1}$$

- What is $\Pr[X = 1]$?

$$\Pr[X = 1] = \Pr\left[\exists_{i \in [\binom{n}{k}]} : X_i = 1\right] \overset{\text{union bound}}{\le} \sum_{i=1}^{\binom{n}{k}} \Pr[X_i = 1]$$

$$= \binom{n}{k} 2^{-\binom{k}{2}+1} \le \frac{n^k}{k!} 2^{-\frac{k(k-1)}{2}+1} = \frac{n^k}{k!} 2 \cdot 2^{-\frac{k^2-k}{2}} = \frac{n^k}{k!} 2 \cdot \left(2^{-\frac{k}{2}}\right)^k \cdot 2^{\frac{k}{2}}$$

simplify by assuming $k \ge 2\log(n)$

$$\Rightarrow 2^{-\frac{k}{2}} \le \frac{1}{n}$$

$$\le \frac{1}{k!} 2\sqrt{2}^k \le \frac{2\sqrt{2}^k}{e\left(\frac{k}{e}\right)^k} = \underbrace{\frac{2}{e}}_{<1} \underbrace{\left(\frac{\sqrt{2}e}{k}\right)^k}_{<1} < 1$$

$$\Rightarrow \Pr[X = 0] = 1 - \Pr[X = 1] > 0$$

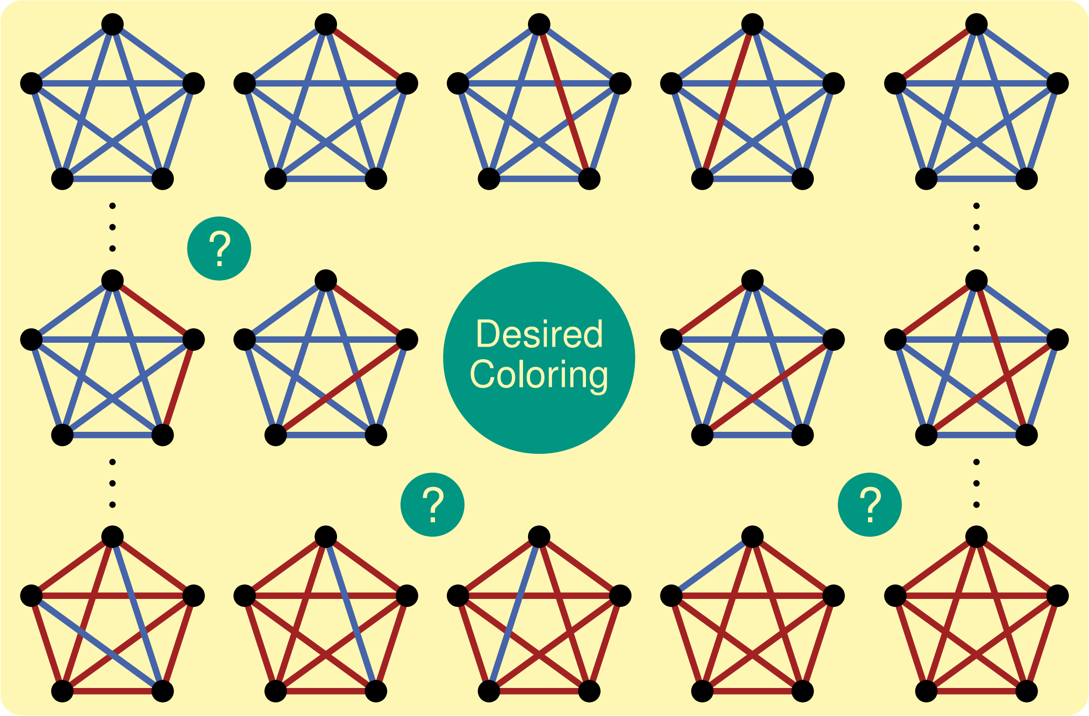
It may happen that the algorithm returns a coloring with the desired property!

not very confident...

# What did we just show?!

## The Probability Space

- What is the sample space of the algorithm?
  - Each edge is red or blue with prob. $1/2$
  - $\binom{n}{2}$ edges $\Rightarrow 2^{\binom{n}{2}}$ possible colorings
- Each occurs with equal probability $1/2^{\binom{n}{2}}$




## Just Shown

- $X = 0 \Rightarrow$ coloring returned by algorithm contains *no* monochromatic $k$-clique
- $\Pr[X = 0] > 0$
- Consequence: At least one such coloring in the sample space! Unclear where. But we know *deterministically* that it exists!

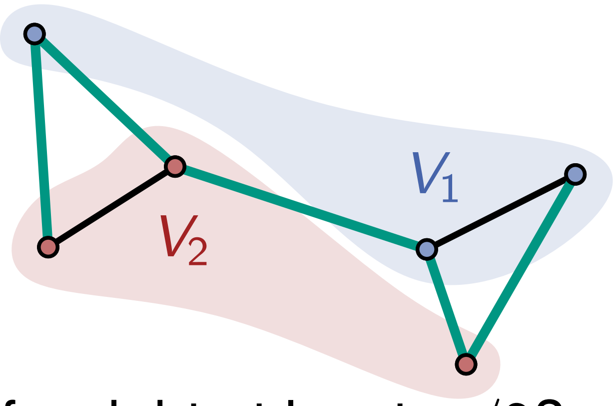
No need to actually run the algorithm to find it!

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process. (pioneered by Paul Erdős)

# Application: Cuts

## Recap

- $G = (V, E)$ an unweighted, undirected, connected graph
- *Cut*: partition of $V$ into $V_1$, $V_2$ s.t. $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$
- *Cut-set*: set of edges with one endpoint in $V_1$ and the other in $V_2$
- *Weight*: size of the cut-set
- Question now: In a graph with $m$ edges, does there *exist* a cut of weight at least $m/2$?




## Random Process

- Add each vertex to one of the two sets with equal prob. $\frac{1}{2}$

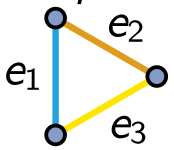
**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.

## Positive Probability

- Consider edges $e_1, \dots, e_m$ and let $X_i$ be the indicator that is 1 iff $e_i$ is in the cut-set
- $X = \sum_{i=1}^{m} X_i$ is the weight of the cut
- To show: $\Pr[X \geq \frac{m}{2}] > 0$

$\Pr[X \geq \frac{m}{2}] = \Pr\left[\sum_{i=1}^{m} X_i \geq \frac{m}{2}\right] = ???$

- Depends on the graph?
- The $X_i$ are not even independent...




$X_2 = X_3 = 1 \Rightarrow X_1 = 1$

# Probabilistic Method: The Expectation Argument

**Theorem**: Let $X$ be a random variable taking values in a set $S$. Then, $\Pr[X \geq \mathbb{E}[X]] > 0$ and $\Pr[X \leq \mathbb{E}[X]] > 0$.

- There always exists at least one sample that yields $X \geq \mathbb{E}[X]$ ($X \leq \mathbb{E}[X]$)

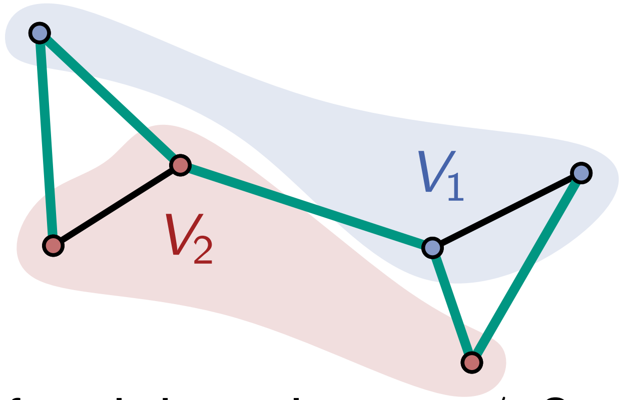
**Proof** ($\Pr[X \geq \mathbb{E}[X]] > 0$, the other works analogous)

- Towards a contradiction assume $\Pr[X \geq \mathbb{E}[X]] = 0$

$$\begin{aligned}
\mathbb{E}[X] = \sum_{x \in S} x \cdot \Pr[X = x] &= \sum_{x \in S, x < \mathbb{E}[X]} x \cdot \Pr[X = x] \\
&\lightning < \sum_{x \in S, x < \mathbb{E}[X]} \mathbb{E}[X] \cdot \Pr[X = x] \\
&= \mathbb{E}[X] \cdot \sum_{x \in S, x < \mathbb{E}[X]} \Pr[X = x] \\
&\leq \mathbb{E}[X]
\end{aligned}$$

# Application: Cuts – Second Try

## Recap




- $G = (V, E)$ an unweighted, undirected, connected graph
- *Cut*: partition of $V$ into $V_1$, $V_2$ s.t. $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$
- *Cut-set*: set of edges with one endpoint in $V_1$ and the other in $V_2$
- *Weight*: size of the cut-set
- Question now: In a graph with $m$ edges, does there *exist* a cut of weight at least $m/2$?

## Random Process

- Add each vertex to one of the two sets with equal prob. $\frac{1}{2}$

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.

## Positive Probability

- Consider edges $e_1, \ldots, e_m$ and let $X_i$ be the indicator that is 1 iff $e_i$ is in the cut-set
- $X = \sum_{i=1}^m X_i$ is the weight of the cut
- To show: $\Pr[X \geq \frac{m}{2}] > 0$ ✓

$\Pr[X \geq \mathbb{E}[X]] > 0$

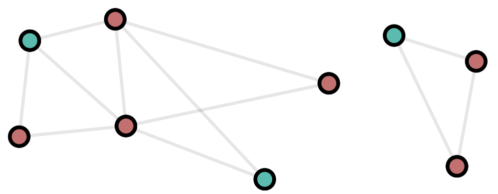
$$\mathbb{E}[X] = \mathbb{E}[\textstyle\sum_{i=1}^m X_i] = \sum_{i=1}^m \mathbb{E}[X_i]$$
$$= m \cdot \Pr[X_i = 1] = \frac{m}{2}$$

| $e_i$ | | | | | | |
|---|---|---|---|---|---|---|
| Pr | | $\frac{1}{4}$ | $\frac{1}{4}$ | $\frac{1}{4}$ + | $\frac{1}{4}$ | $= \frac{1}{2}$ |

# Application: Independent Sets

## The Problem

- Two vertices in a graph are *independent*, if they are not adjacent
- An *independent set* of a graph is a subgraph whose vertices are pairwise independent
- Let $\alpha(G)$ denote the size of a largest independent set in $G$ (in general, determining $\alpha(G)$ is NP-complete)



$d = \frac{24}{9} \Rightarrow$ Survival rate: $\frac{3}{8}$

**Theorem**: Let $G$ be a graph with $n$ vertices and $m \geq n/2$ edges. Then $\alpha(G) \geq n^2/(4m)$.

## Proof

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.

*Random Process*

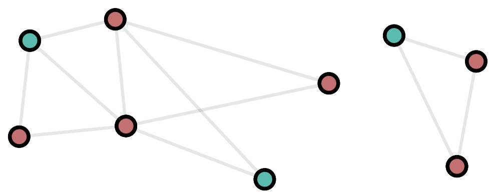
- Let $d = 2m/n$ be the average degree of $G$
- Independently, delete each vertex with probability $1 - \frac{1}{d}$
- Afterwards, for each remaining edge, delete one endpoint chosen uniformly at random
- Note that the remaining vertices form an independent set

# Application: Independent Sets

Karlsruhe Institute of Technology

## The Problem

- Two vertices in a graph are *independent*, if they are not adjacent
- An *independent set* of a graph is a subgraph whose vertices are pairwise independent
- Let $\alpha(G)$ denote the size of a largest independent set in $G$ (in general, determining $\alpha(G)$ is NP-complete)



$d = \frac{24}{9} \Rightarrow$ Survival rate: $\frac{3}{8}$

**Theorem**: Let $G$ be a graph with $n$ vertices and $m \geq n/2$ edges. Then $\alpha(G) \geq n^2/(4m)$.

## Proof

*Positive Probability*

$\mathbb{E}$**-Argument**: $\Pr[X \geq \mathbb{E}[X]] > 0$

*Random Process*: $d = 2m/n$
Step 1: Delete $v$ with prob. $1 - \frac{1}{d}$
Step 2: Delete one endpoint of each $e$

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.

- $X_V$: number of *vertices* that survive the first step
- $X_E$: number of *edges* that survive the first step
- Step 2: each of the $X_E$ edges removes $\leq 1$ vertex
- Size of resulting independent set $S$ is $\geq X_V - X_E$
- $\Pr[|S| \geq n^2/(4m)] \geq \Pr[X_V - X_E \geq n^2/(4m)] > 0$ ✓

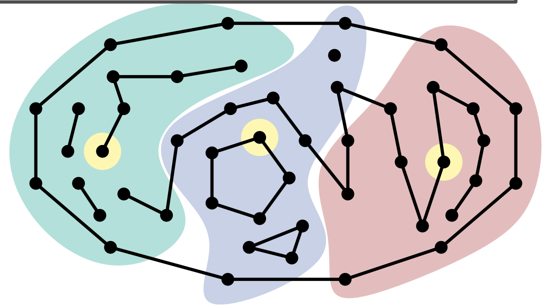
- $\mathbb{E}[X_V] = n \cdot \frac{1}{d}$ (since each vertex survives with prob. $\frac{1}{d}$)
- Edge $\{u, v\}$ survives if both $u, v$ do
- $\mathbb{E}[X_E] = m \cdot \frac{1}{d^2} = \frac{nd}{2} \cdot \frac{1}{d^2} = \frac{n}{2d}$
- $\mathbb{E}[X_V - X_E] = \mathbb{E}[X_V] - \mathbb{E}[X_E] = \frac{n}{d} - \frac{n}{2d}$
  $= \frac{n}{2d} = \frac{n}{2(2m/n)} = n^2/(4m)$

# Application: Dependent Independent Set

**Theorem**: Let $G = (V, E)$ be a graph with max-degree $\Delta$. For any partition $V_1 \cup \ldots \cup V_t = V$ such that $|V_i| \geq 8\Delta$, there exists an independent set containing one vertex from each $V_i$.

## Proof

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.



$\Delta = 2 \Rightarrow 8\Delta = 16$

*Random Process*

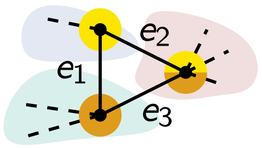
- Assume $|V_i| = k = 8\Delta$ for all $i$ (otherwise remove vertices from too large $V_i$)
- Let $S$ be the set obtained by independently choosing one vertex uniformly at random from each $V_i$

*Positive Probability*

- To show: $\Pr[\text{“}S\text{ independent”}] > 0$
- $S$ is independent iff no edge $e = \{u, v\}$ has $\overbrace{e \subseteq S}^{\text{(both endpoints in } S)}$, Let $A_e$ be the event that $e \subseteq S$

$$\Pr[\text{“}S\text{ independent”}] = \Pr\Big[\bigcap_{e\in E} \neg A_e\Big] \cancel{=} \prod_{e\in E} \Pr[\neg A_e] = \prod_{e\in E}\big(1 - \underbrace{\Pr[A_e]}_{\leq \frac{1}{k}\cdot\frac{1}{k}}\big) \geq \prod_{e\in E}\Big(1 - \frac{1}{k^2}\Big) \underset{k>1}{>} 0 \ \checkmark$$

The events are not independent!




$\Pr[A_{e_1}] = \frac{1}{k^2}$

$\Pr[A_{e_1} \mid A_{e_2} \cap A_{e_3}] = 1$ The probability of an event is affected by the outcomes of other events. Dependence...

# To be or not to be... independent

## Independence

**Definition**: Event $A$ is **independent of an event** $B$ if $\Pr[A \mid B] = \Pr[A]$. $(\Pr[A \cap B] = \Pr[A]\Pr[B])$

**Definition**: Event $A$ is **independent of a set of events** $\mathcal{E}$ if for all subsets $\mathcal{E}' = \{B_1, B_2, \dots, B_k\} \subseteq \mathcal{E}$ we have $\Pr[A \mid \bigcap_{i \in [k]} B_i] = \Pr[A]$.

## Example

- Triangle, independently color each vertex red/blue with prob. $\frac{1}{2}$
- Let $A_{ij}$ for $i < j$ be the event that $i$ and $j$ have the same color
- $A = A_{12}$, $B = A_{23}$:

  $\Pr[A_{12}] = \boxed{\frac{1}{2}}$

  $\Pr[A_{12} \mid A_{23}] = \frac{\Pr[A_{12} \cap A_{23}]}{\Pr[A_{23}]} = \frac{1/4}{1/2} = \frac{1}{2}$

  (same holds for all choices of $A$ and $B$)
- All $A_{ij}$ are *pairwise* independent

- $A = A_{12}$, $\mathcal{E} = \{A_{13}, A_{23}\}$:

  $\Pr[A_{12} \mid A_{13} \cap A_{23}]$

  $= \frac{\Pr[A_{12} \cap A_{13} \cap A_{23}]}{\Pr[A_{13} \cap A_{23}]} = \frac{1/4}{1/4} = \boxed{1}$
- $A_{ij}$ not independent of the other events

| Pr | Graph | 1 | 2 | 3 | $A_{12}$ | $A_{13}$ | $A_{23}$ |
|---|---|---|---|---|---|---|---|
| $\frac{1}{8}$ | | red | red | red | ✓ | ✓ | ✓ |
| $\frac{1}{8}$ | | red | red | blue | ✓ | ✗ | ✗ |
| $\frac{1}{8}$ | | red | blue | red | ✗ | ✓ | ✗ |
| $\frac{1}{8}$ | | red | blue | blue | ✗ | ✗ | ✓ |
| $\frac{1}{8}$ | | blue | red | red | ✗ | ✗ | ✓ |
| $\frac{1}{8}$ | | blue | red | blue | ✗ | ✓ | ✗ |
| $\frac{1}{8}$ | | blue | blue | red | ✓ | ✗ | ✗ |
| $\frac{1}{8}$ | | blue | blue | blue | ✓ | ✓ | ✓ |

# Lovász Local Lemma (LLL)

Karlsruhe Institute of Technology

**Theorem**: Let $E_1, \ldots, E_n$ be events such that each $E_i$ for $i \in [n]$ is independent of all but at most $d > 0$ of the other events. Let $p = \max_{i \in [n]} \Pr[E_i]$. If $4dp \leq 1$, then $\Pr[\bigcap_{i \in [n]} \neg E_i] > 0$.

- If $d = 0$, everything is independent and we can just compute the probability as the product
- For each $i \in [n]$ let $D_i \subseteq [n]$ be the such that $E_i$ is independent of $\{E_1, \ldots, E_n\} \setminus (\bigcup_{j \in \{i\} \cup D_i} E_j)$, then $|D(i)| \leq d$.

(Remove events defined by $D_i$ to make $E_i$ independent of the rest.)

Notation: For $S \subseteq [n]$ write $\mathcal{I}(S) = \bigcap_{i \in S} \neg E_i$

**Conditional Probability**: $\Pr[A \cap B] = \Pr[A \mid B] \cdot \Pr[B]$

**Proof**

$$\underbrace{\Pr[\overbrace{\textstyle\bigcap_{i \in [n]} \neg E_i}^{\mathcal{I}([n])}]} \overset{\text{“Chain Rule”}}{=} \prod_{i \in [n]} \Pr[\neg E_i \mid \mathcal{I}([i-1])]$$

$$= \Pr[\neg E_n \cap (\neg E_{n-1} \cap \neg E_{n-2} \cap \ldots \cap \neg E_1)]$$

$$= \Pr[\neg E_n \mid (\neg E_{n-1} \cap \neg E_{n-2} \cap \ldots \cap \neg E_1)] \cdot \Pr[(\neg E_{n-1} \cap \neg E_{n-2} \cap \ldots \cap \neg E_1)]$$

$$= \Pr[\neg E_n \mid \underbrace{(\neg E_{n-1} \cap \neg E_{n-2} \cap \ldots \cap \neg E_1)}_{\mathcal{I}([n-1])}] \cdot \Pr[\neg E_{n-1} \mid \underbrace{(\neg E_{n-2} \cap \ldots \cap \neg E_1)}_{\mathcal{I}([n-2])}] \cdot \Pr[(\neg E_{n-2} \cap \ldots \cap \neg E_1)]$$

# Lovász Local Lemma (LLL)

Karlsruhe Institute of Technology

**Theorem**: Let $E_1, \dots, E_n$ be events such that each $E_i$ for $i \in [n]$ is independent of all but at most $d > 0$ of the other events. Let $p = \max_{i \in [n]} \Pr[E_i]$. If $4dp \leq 1$, then $\Pr[\bigcap_{i \in [n]} \neg E_i] > 0$.

- If $d = 0$, everything is independent and we can just compute the probability as the product
- For each $i \in [n]$ let $D_i \subseteq [n]$ be the such that $E_i$ is independent of $\{E_1, \dots, E_n\} \setminus (\bigcup_{j \in \{i\} \cup D_i} E_j)$, then $|D(i)| \leq d$.

(Remove events defined by $D_i$ to make $E_i$ independent of the rest.)

Notation: For $S \subseteq [n]$ write $\mathcal{I}(S) = \bigcap_{i \in S} \neg E_i$

**Conditional Probability**: $\Pr[A \cap B] = \Pr[A \mid B] \cdot \Pr[B]$

**Proof**

$$
\begin{aligned}
\Pr[\overbrace{\textstyle\bigcap_{i \in [n]} \neg E_i}^{\mathcal{I}([n])}] &\overset{\text{“Chain Rule”}}{=} \prod_{i \in [n]} \Pr[\neg E_i \mid \mathcal{I}([i-1])] \\
&= \prod_{i \in [n]} (1 - \underbrace{\Pr[E_i \mid \mathcal{I}([i-1])]}_{\text{Claim: } \leq 2p}) \\
&\geq \prod_{i \in [n]} (1 - 2p) \\
&\geq \prod_{i \in [n]} 1/2
\end{aligned}
$$

- Since $d > 0$ and $4dp \leq 1$, we have $4p \leq 1$ and thus $2p \leq 1/2$

# LLL – Proof of Claim

Karlsruhe Institute of Technology

**Claim**: For all $S_i \subseteq \{1, ..., n\} \setminus \{i\}$, $\Pr[E_i \mid \mathcal{I}(S_i)] \leq 2p$.

**Proof** (via induction over the size $s = |S_i|$)

*Start*: $s = 0 \rightarrow S_i = \emptyset \rightarrow \Pr[E_i \mid \mathcal{I}(S_i)] = \Pr[E_i] \leq p \leq 2p$ ✓

*Step*: $s > 0$

- Case 1: $D'_i = S_i \cap D_i = \emptyset$
  - $E_i$ is independent of $\{E_j \mid j \in S_i\} \rightarrow \Pr[E_i \mid \mathcal{I}(S_i)] = \Pr[E_i] \leq p \leq 2p$ ✓
- Case 2: $D'_i = S_i \cap D_i \neq \emptyset$

$$\Pr[E_i \mid \mathcal{I}(S_i)] = \frac{\Pr[E_i \cap \mathcal{I}(S_i)]}{\Pr[\mathcal{I}(S_i)]} = \frac{\Pr[E_i \cap \mathcal{I}(D'_i) \cap \mathcal{I}(S_i \setminus D'_i)]}{\Pr[\mathcal{I}(S_i)]} = \frac{\Pr[E_i \cap \mathcal{I}(D'_i) \cap \mathcal{I}(S_i \setminus D'_i)]}{\Pr[\mathcal{I}(D'_i) \cap \mathcal{I}(S_i \setminus D'_i)]}$$

$$S_i = (S_i \setminus D'_i) \cup D'_i$$

$$\begin{aligned} \mathcal{I}(S_i) &= \bigcap_{j \in S_i} \neg E_j \\ \rightarrow &= \bigcap_{j \in S_i \setminus D'_i} \neg E_j \cap \bigcap_{j \in D'_i} \neg E_j \\ &= \mathcal{I}(S_i \setminus D'_i) \cap \mathcal{I}(D'_i) \end{aligned}$$

**LLL**: Events $E_1, ..., E_n$

- $p = \max_{i \in [n]} \Pr[E_i]$
- $E_i$ independent of $\{E_1, ..., E_n\} \setminus \bigcup_{j \in \{i\} \cup D_i} E_j$ with $|D_i| \leq d$
- $4dp \leq 1$

Notation: For $S \subseteq [n]$ write $\mathcal{I}(S) = \bigcap_{i \in S} \neg E_i$

**Conditional Probability**: $\Pr[A \cap B] = \Pr[A \mid B] \cdot \Pr[B]$

# LLL – Proof of Claim

Karlsruhe Institute of Technology

**Claim**: For all $S_i \subseteq \{1, ..., n\} \setminus \{i\}$, $\Pr[E_i \mid \mathcal{I}(S_i)] \leq 2p$.

**Proof** (via induction over the size $s = |S_i|$)

*Start*: $s = 0 \rightarrow S_i = \emptyset \rightarrow \Pr[E_i \mid \mathcal{I}(S_i)] = \Pr[E_i] \leq p \leq 2p$ ✓

*Step*: $s > 0$

- Case 1: $D_i' = S_i \cap D_i = \emptyset$
  - $E_i$ is independent of $\{E_j \mid j \in S_i\} \rightarrow \Pr[E_i \mid \mathcal{I}(S_i)] = \Pr[E_i] \leq p \leq 2p$ ✓
- Case 2: $D_i' = S_i \cap D_i \neq \emptyset$

$$\Pr[E_i \mid \mathcal{I}(S_i)] = \frac{\Pr[E_i \cap \mathcal{I}(S_i)]}{\Pr[\mathcal{I}(S_i)]} = \frac{\Pr[E_i \cap \mathcal{I}(D_i') \cap \mathcal{I}(S_i \setminus D_i')]}{\Pr[\mathcal{I}(S_i)]} = \frac{\Pr[E_i \cap \mathcal{I}(D_i') \cap \mathcal{I}(S_i \setminus D_i')]}{\Pr[\mathcal{I}(D_i') \cap \mathcal{I}(S_i \setminus D_i')]}$$

$$= \frac{\Pr[E_i \cap \mathcal{I}(D_i') \mid \mathcal{I}(S_i \setminus D_i')] \cdot \cancel{\Pr[\mathcal{I}(S_i \setminus D_i')]}}{\Pr[\mathcal{I}(D_i') \mid \mathcal{I}(S_i \setminus D_i')] \cdot \cancel{\Pr[\mathcal{I}(S_i \setminus D_i')]}} \leq \frac{\Pr[E_i \mid \mathcal{I}(S_i \setminus D_i')]}{\Pr[\mathcal{I}(D_i') \mid \mathcal{I}(S_i \setminus D_i')]}$$

$$= \frac{\Pr[E_i]}{\Pr[\mathcal{I}(D_i') \mid \mathcal{I}(S_i \setminus D_i')]} \leq \frac{p}{\underbrace{\Pr[\mathcal{I}(D_i') \mid \mathcal{I}(S_i \setminus D_i')]}_{\text{remains to show } \geq \frac{1}{2}}}$$

Removing the $D_i'$ makes $E_i$ independent of the remaining events.

**LLL**: Events $E_1, ..., E_n$

- $p = \max_{i \in [n]} \Pr[E_i]$
- $E_i$ independent of $\{E_1, ..., E_n\} \setminus \bigcup_{j \in \{i\} \cup D_i} E_j$ with $|D_i| \leq d$
- $4dp \leq 1$

Notation: For $S \subseteq [n]$ write $\mathcal{I}(S) = \bigcap_{i \in S} \neg E_i$

**Conditional Probability**: $\Pr[A \cap B] = \Pr[A \mid B] \cdot \Pr[B]$

$\Pr[A \cap B] \leq \Pr[A]$

# LLL – Proof of Claim

**Claim**: For all $S_i \subseteq \{1, ..., n\} \setminus \{i\}$, $\Pr[E_i \mid \mathcal{I}(S_i)] \leq 2p$.

**Proof** (via induction over the size $s = |S_i|$)

*Start*: $s = 0 \rightarrow S_i = \emptyset \rightarrow \Pr[E_i \mid \mathcal{I}(S_i)] = \Pr[E_i] \leq p \leq 2p$ ✓

*Step*: $s > 0$

- Case 1: $D'_i = S_i \cap D_i = \emptyset$
  - $E_i$ is independent of $\{E_j \mid j \in S_i\} \rightarrow \Pr[E_i \mid \mathcal{I}(S_i)] = \Pr[E_i] \leq p \leq 2p$ ✓
- Case 2: $D'_i = S_i \cap D_i \neq \emptyset$

$$\Pr[E_i \mid \mathcal{I}(S_i)] \leq \frac{p}{\Pr[\mathcal{I}(D'_i) | \mathcal{I}(S_i \setminus D'_i)]}$$ } remains to show $\geq \frac{1}{2}$

$$\Pr[\mathcal{I}(D'_i) \mid \mathcal{I}(S_i \setminus D'_i)] = \Pr[\textstyle\bigcap_{j \in D'_i} \neg E_j \mid \mathcal{I}(S_i \setminus D'_i)]$$

$$= 1 - \Pr[\textstyle\bigcup_{j \in D'_i} E_j \mid \mathcal{I}(S_i \setminus D'_i)]$$

(via union bound) $\geq 1 - \sum_{j \in D'_i} \Pr[E_j \mid \mathcal{I}(\overbrace{S_i \setminus D'_i}))]$ $\rightarrow \subsetneq S_i$, since $S_i \cap D'_i \neq \emptyset$

$\Rightarrow |S_i \setminus D'_i| < s$ and we can apply induction hypothesis

$|D'_i| \leq |D_i|$ $\geq 1 - \sum_{j \in D'_i} 2p \geq 1 - d \cdot 2p \geq \frac{1}{2}$ ✓

**LLL**: Events $E_1, ..., E_n$

- $p = \max_{i \in [n]} \Pr[E_i]$
- $E_i$ independent of $\{E_1, ..., E_n\} \setminus \bigcup_{j \in \{i\} \cup D_i} E_j$ with $|D_i| \leq d$
- $4dp \leq 1$

Notation: For $S \subseteq [n]$ write $\mathcal{I}(S) = \bigcap_{i \in S} \neg E_i$

**Conditional Probability**: $\Pr[A \cap B] = \Pr[A \mid B] \cdot \Pr[B]$

$\Pr[A \cap B] \leq \Pr[A]$

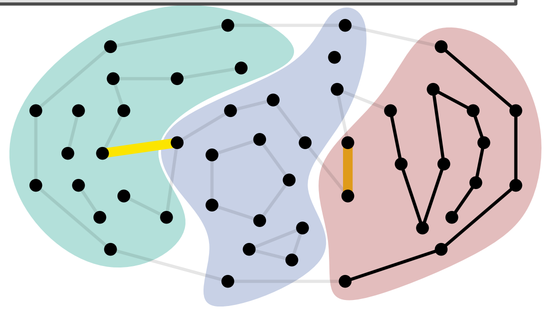
$\Pr[\neg A \cap \neg B] = \Pr[\neg(A \cup B)]$

# Application: Dependent Independent Set (2nd Try)

**Theorem**: Let $G = (V, E)$ be a graph with max-degree $\Delta$. For any partition $V_1 \cup \ldots \cup V_t = V$ such that $|V_i| \geq 8\Delta$, there exists an independent set containing one vertex from each $V_i$.

## Proof

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.



*Random Process*

- Assume $|V_i| = k = 8\Delta$ for all $i$ (otherwise remove vertices from too large $V_i$)
- Obtain $S$ by ind. choosing one vertex unif. at random from each $V_i$

*Positive Probability*

- To show: $\Pr[\text{“}S \text{ independent”}] > 0$
- $S$ is independent iff no edge $e = \{\underset{V_i}{\underset{\downarrow}{u}}, \underset{V_j}{\underset{\downarrow}{v}}\}$ has $\overbrace{e \subseteq S}^{\text{(both endpoints in } S\text{)}}$,

  Let $A_e$ be the event that $e \subseteq S$

  $\Pr[\text{“}S \text{ independent”}] = \Pr[\bigcap_{e \in E} \neg A_e]$

  $\Pr[A_e] \leq \frac{1}{k^2} =: p$

  $D_e = \{A_{e'} \mid e' \cap (V_i \cup V_j) \neq \emptyset\}$

This is like isolating $V_i, V_j$ from the remainder of the graph

No matter the outcome of $A_f$ for $f \in E \setminus D_e$, the probability for a node in $V_i$ or $V_j$ to be chosen remains the same $\Rightarrow A_e$ is independent of all events but $D_e$

**LLL**: Events $E_1, \ldots, E_n$

- $p = \max_{i \in [n]} \Pr[E_i]$
- $E_i$ independent of $\{E_1, \ldots, E_n\} \setminus \bigcup_{j \in \{i\} \cup D_i} E_j$ with $|D_i| \leq d$
- $4dp \leq 1$

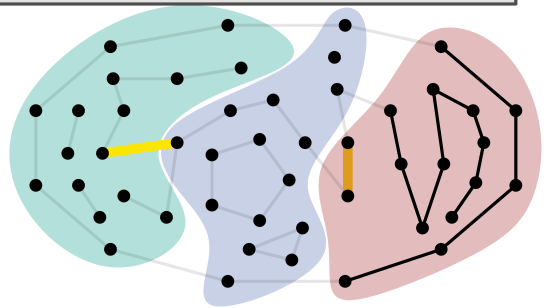
Then, $Pr[\bigcap_{i \in [n]} \neg E_i] > 0$.

# Application: Dependent Independent Set (2nd Try)

**Theorem**: Let $G=(V,E)$ be a graph with max-degree $\Delta$. For any partition $V_1 \cup \ldots \cup V_t = V$ such that $|V_i| \geq 8\Delta$, there exists an independent set containing one vertex from each $V_i$.

**Proof**

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.



*Random Process*

- Assume $|V_i| = k = 8\Delta$ for all $i$ (otherwise remove vertices from too large $V_i$)
- Obtain $S$ by ind. choosing one vertex unif. at random from each $V_i$

*Positive Probability*

- To show: Pr["$S$ independent"] $> 0$
- $S$ is independent iff no edge $e = \{u, v\}$ has $\overbrace{e \subseteq S}^{\text{(both endpoints in } S)}$, with $u \in V_i$, $v \in V_j$

  Let $A_e$ be the event that $e \subseteq S$

  $\Pr[\text{“}S \text{ independent”}] = \Pr[\bigcap_{e \in E} \neg A_e] > 0$ ✓

  $\Pr[A_e] \leq \frac{1}{k^2} =: p$

  $D_e = \{A_{e'} \mid e' \cap (V_i \cup V_j) \neq \emptyset\} \rightarrow |D_e| \leq \underbrace{k\Delta}_{|V_i|} + \underbrace{k\Delta}_{|V_j|} \leq 2k\Delta =: d$

**LLL**: Events $E_1, \ldots, E_n$

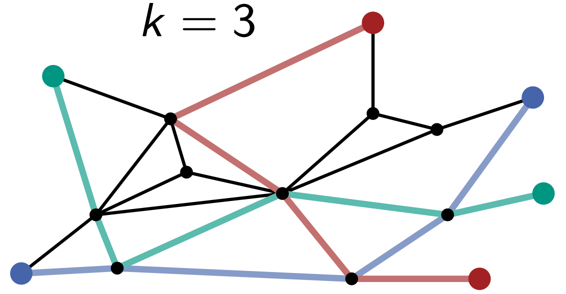
- $p = \max_{i \in [n]} \Pr[E_i]$
- $E_i$ independent of $\{E_1, \ldots, E_n\} \setminus \bigcup_{j \in \{i\} \cup D_i} E_j$ with $|D_i| \leq d$
- $4dp \leq 1$

Then, $Pr[\bigcap_{i \in [n]} \neg E_i] > 0$.

$$4dp = 4 \cdot 2k\Delta \cdot \frac{1}{k^2} = \frac{8\Delta}{k} = 1$$

# Application: Independent Paths

- Given a network and $k$ vertex pairs that want to communicate
- Each $i \in [k]$ has a set $S_i$ of candidate communication paths
- Does there exist a choice of paths (one $P_i$ from each $S_i$) that are pairwise edge-disjoint? (NP-complete to decide)




**Theorem**: Let $m = \min_{i\in[k]}\{|S_i|\}$. Then, there exists a valid choice if any path in $S_i$ shares edges with at most $\ell \leq m/(8k)$ paths in $S_j$ for $i \neq j$.

**Proof**

*Random Process*: Ind., unif. at random choose $P_i$ from $S_i$

*Positive Probability*

- Let $E_{ij}$ be the event that $P_i$ and $P_j$ share an edge

$$\Pr[\bigcap_{i<j} \neg E_{ij}] \overset{?}{>} 0$$

$$\Pr[E_{ij}] \leq \frac{\ell}{m} =: p$$

- $E_{ij}$ independent of every other event but not of *all* others
- If $E_{i1}, \ldots, E_{i\ell}$ occur, then $Pr[E_{ij}] = 0$ for $j > \ell$

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.

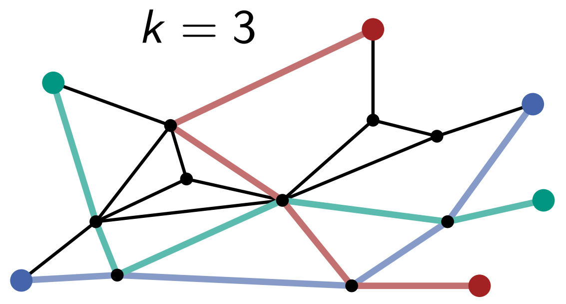
**LLL**: Events $E_1, \ldots, E_n$

- $p = \max_{i\in[n]} \Pr[E_i]$
- $E_i$ independent of $\{E_1, \ldots, E_n\} \setminus \bigcup_{j\in\{i\}\cup D_i} E_j$ with $|D_i| \leq d$
- $4dp \leq 1$

Then, $Pr[\bigcap_{i\in[n]} \neg E_i] > 0$.

# Application: Independent Paths

- Given a network and $k$ vertex pairs that want to communicate
- Each $i \in [k]$ has a set $S_i$ of candidate communication paths
- Does there exist a choice of paths (one $P_i$ from each $S_i$) that are pairwise edge-disjoint? (NP-complete to decide)




**Theorem**: Let $m = \min_{i \in [k]}\{|S_i|\}$. Then, there exists a valid choice if any path in $S_i$ shares edges with at most $\ell \leq m/(8k)$ paths in $S_j$ for $i \neq j$.

**Proof**

*Random Process*: Ind., unif. at random choose $P_i$ from $S_i$

*Positive Probability*

- Let $E_{ij}$ be the event that $P_i$ and $P_j$ share an edge

$$\Pr[\textstyle\bigcap_{i<j} \neg E_{ij}] \overset{?}{>} 0$$

$$\Pr[E_{ij}] \leq \frac{\ell}{m} =: p$$

$$D_{ij} = \{E_{st} \mid \{s,t\} \cap \{i,j\} \neq \emptyset\}$$

Removing $D_{ij}$ is discarding all events that could tell us something about whether $P_i$ and $P_j$ can intersect

**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.

**LLL**: Events $E_1, \dots, E_n$

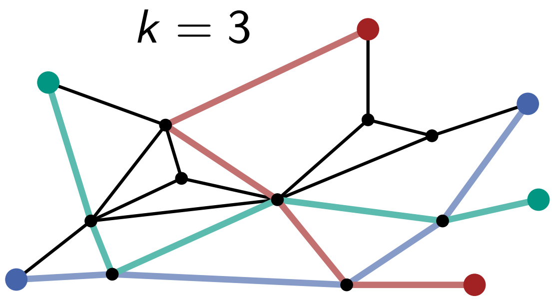
- $p = \max_{i \in [n]} \Pr[E_i]$
- $E_i$ independent of $\{E_1, \dots, E_n\} \setminus \bigcup_{j \in \{i\} \cup D_i} E_j$ with $|D_i| \leq d$
- $4dp \leq 1$

Then, $Pr[\bigcap_{i \in [n]} \neg E_i] > 0$.

# Application: Independent Paths

Karlsruhe Institute of Technology

- Given a network and $k$ vertex pairs that want to communicate
- Each $i \in [k]$ has a set $S_i$ of candidate communication paths
- Does there exist a choice of paths (one $P_i$ from each $S_i$) that are pairwise edge-disjoint? (NP-complete to decide)




**Theorem**: Let $m = \min_{i\in[k]}\{|S_i|\}$. Then, there exists a valid choice if any path in $S_i$ shares edges with at most $\ell \leq m/(8k)$ paths in $S_j$ for $i \neq j$.

**Proof**

*Random Process*: Ind., unif. at random choose $P_i$ from $S_i$

*Positive Probability*

- Let $E_{ij}$ be the event that $P_i$ and $P_j$ share an edge

$$\Pr[\textstyle\bigcap_{i<j} \neg E_{ij}] > 0 \checkmark \qquad D_{ij} = \{E_{st} \mid \{s,t\} \cap \{i,j\} \neq \emptyset\}$$

$$\Pr[E_{ij}] \leq \frac{\ell}{m} =: p \qquad |D_{ij}| = (k-1) + (k-1) - 1 < 2k =: d$$

$$4dp = 4 \cdot 2k \cdot \frac{\ell}{m} = \ell \cdot \frac{8k}{m} \leq 1$$

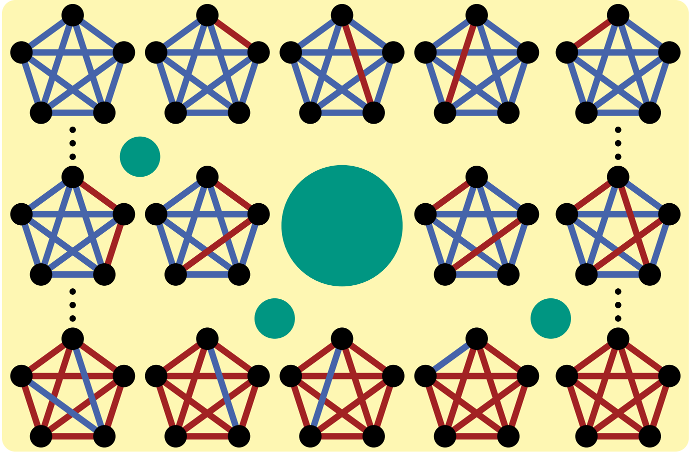
**Probabilistic Method**: Show that something exists by proving that it has a *positive* probability of occuring from a random process.

**LLL**: Events $E_1, \ldots, E_n$

- $p = \max_{i\in[n]} \Pr[E_i]$
- $E_i$ independent of $\{E_1, \ldots, E_n\} \setminus \bigcup_{j\in\{i\}\cup D_i} E_j$ with $|D_i| \leq d$
- $4dp \leq 1$

Then, $Pr[\bigcap_{i\in[n]} \neg E_i] > 0$.

# Conclusion



## Probabilistic Method

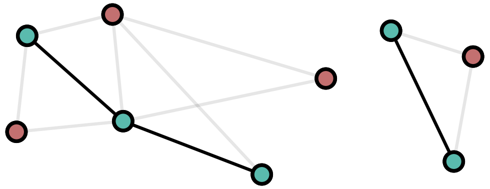
- Show that something exists *deterministically*, by showing that it occurs with positive probability from a random process
- Reasoning: At least one object in the sample space has the desired property

## Expectation Argument

- Useful tool when applying probabilistic method
- $\Pr[X \geq \mathbb{E}[X]] > 0$ and $\Pr[X \leq \mathbb{E}[X]] > 0$.

## Sample via Modification

- Example Vertex Cover: remove vertices/edges at random



## Lovász Local Lemma

- Show that something exists by showing that all events that prevent its existence do not occur, with positive probability
- Lemma works as long as there are not too many dependencies