# The Lovász Local Lemma

Aalto University
School of Science

Antonio Cruciani

antonio.cruciani@aalto.fi

# Intro

In the probabilistic method we want to show an outcome happens with **positive probability**.

# Intro

In the probabilistic method we want to show an outcome happens with **positive probability**.

**Question**

Is there a common situation where an outcome might happen with low but positive probability?

# Intro

In the probabilistic method we want to show an outcome happens with **positive probability**.

**Question**
Is there a common situation where an outcome might happen with low but positive probability?

Yes: e.g. the intersection of many **independent** events!

$E_1, \dots E_n$ are independent events with $\Pr(E_i) = p > 0$.

Then

$$\Pr\left(\bigcap_{i=1}^{n} E_i\right) = p^n > 0$$

Does this still hold if the events are **mostly independent**?

# Mutual Independence

How do we formalize **mostly independent**?

# Mutual Independence

How do we formalize **mostly independent**?

**Definition 1.** *An event $A$ is mutually independent of the events $B_1, \ldots, B_n$ if for any subset*

$$I \subseteq \{1, \ldots, n\}$$

*it holds that*

$$\Pr\left(A \mid \cap_{i \in I} B_i\right) = \Pr(A)$$

# The Dependency Graph

**Definition 2.** *A dependency graph for a set of events $E_1, \ldots, E_n$ is a graph $G = (V, E)$ where*

- $V = \{1, \ldots, n\}$
- *For all $i$, $E_i$ is mutually independent of the events $\{E_j : (i, j) \notin E\}$*

# The Lovász Local Lemma

The **Lovász Local Lemma** shows that if a set of bad events that are

# The Lovász Local Lemma

The **Lovász Local Lemma** shows that if a set of bad events that are

- "mostly" mutually independent, and

# The Lovász Local Lemma

The **Lovász Local Lemma** shows that if a set of bad events that are

- "mostly" mutually independent, and
- happen with low probability,

# The Lovász Local Lemma

The **Lovász Local Lemma** shows that if a set of bad events that are

- "mostly" mutually independent, and
- happen with low probability,

then with positive probability none of them happen.

# The Lovász Local Lemma

**Theorem 1** (Lovász Local Lemma)**.** *Let $d \in \mathbb{N}$ and $p \in \mathbb{R}$ with $4dp \leq 1$. Let $E_1, E_2, \ldots, E_n$ be events. If*

- $\Pr(E_i) \leq p$ *for all $i$, and*
- *The degree of their dependency graph is bounded by $d$*

*then*

$$\Pr\left(\bigcap_{1 \leq i \leq n} \overline{E}_i\right) > 0$$

# Using the LLL

# Edge-disjoint paths

Assume $n$ 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.

# Edge-disjoint paths

Assume $n$ 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 all $i \neq j$, let

$$E_{\{i,j\}} = \{\text{The path chosen by pairs } i \text{ and } j \text{ share an edge}\}$$

# Edge-disjoint paths

Assume $n$ 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 all $i \neq j$, let

$$E_{\{i,j\}} = \{\text{The path chosen by pairs } i \text{ and } j \text{ share an edge}\}$$

**Observation:** $E_{\{i,j\}}$ is independent of all events $E_{\{i',j'\}}$ where $\{i,j\} \cap \{i',j'\} = \emptyset$.

# Edge-disjoint paths

Assume $n$ 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 all $i \neq j$, let

$$E_{\{i,j\}} = \{\text{The path chosen by pairs } i \text{ and } j \text{ share an edge}\}$$

**Observation:** $E_{\{i,j\}}$ is independent of all events $E_{\{i',j'\}}$ where $\{i,j\} \cap \{i',j'\} = \emptyset$.

This means that each event has less than $2n$ neighbors in the dependency graph.

How many events do we have?

# Edge-disjoint paths

Assume $n$ pairs of users need to communicate in a graph.

Each pair $i \in \{1, \dots n\}$ can choose from a collection $F_i$ of paths.

For all $i \neq j$, let

$$E_{\{i,j\}} = \{\text{The path chosen by pairs } i \text{ and } j \text{ share an edge}\}$$

**Observation:** $E_{\{i,j\}}$ is independent of all events $E_{\{i',j'\}}$ where $\{i,j\} \cap \{i',j'\} = \emptyset$.

This means that each event has less than $2n$ neighbors in the dependency graph.

How many events do we have? $\binom{n}{2} = \frac{n(n-1)}{2}$

# Edge-disjoint paths

Assume

- each $F_i$ consists of $m$ paths
- for any $i$ and $j$, a path in $F_i$ intersect with at most $k$ paths in $F_j$

Then,

$$\Pr\left(E_{\{i,j\}}\right) \leq \frac{k}{m}$$

# Edge-disjoint paths

Assume

- each $F_i$ consists of $m$ paths
- for any $i$ and $j$, a path in $F_i$ intersect with at most $k$ paths in $F_j$

Then,

$$\Pr\left(E_{\{i,j\}}\right) \leq \frac{k}{m}$$

**Remember**: the degree of the dependency graph is $d < 2n$, so

$$4dp < \frac{8nk}{m} \leq 1$$

If $\frac{8nk}{m} \leq 1$, then there is a choice of paths such that the $n$ paths are disjoint.

# $k$-Satisfiability

**Input:** A collection of clauses $C_1, C_2, \ldots, C_m$ over $n$ boolean variables $(x_1, \ldots, x_n)$ in $k$-CNF, i.e., each $C_i$ is a **OR** of $k$ variables and $\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$

**Goal:** Find a truth assignment to $x_1, \ldots, x_n$, that satisfies $\phi$.

# $k$-Satisfiability

**Theorem 2.** *Let $\phi = C_1 \wedge \cdots \wedge C_m$, where each $C_i$ has exactly $k$ literals. If no variable appears in more than $T = 2^k/(4k)$ clauses then $\phi$ is satisfiable.*

# $k$-Satisfiability

**Theorem 2.** *Let $\phi = C_1 \wedge \cdots \wedge C_m$, where each $C_i$ has exactly $k$ literals. If no variable appears in more than $T = 2^k/(4k)$ clauses then $\phi$ is satisfiable.*

*Proof.* Assign random truth values to the variables. Let

$$E_i = \{i\text{-th clause is false}\}$$

# $k$-Satisfiability

**Theorem 2.** *Let $\phi = C_1 \wedge \cdots \wedge C_m$, where each $C_i$ has exactly $k$ literals. If no variable appears in more than $T = 2^k/(4k)$ clauses then $\phi$ is satisfiable.*

*Proof.* Assign random truth values to the variables. Let

$$E_i = \{i\text{-th clause is false}\}$$

Then

$$\Pr(E_i) = \left(\frac{1}{2}\right)^k$$

# $k$-Satisfiability

**Theorem 2.** *Let $\phi = C_1 \wedge \cdots \wedge C_m$, where each $C_i$ has exactly $k$ literals. If no variable appears in more than $T = 2^k/(4k)$ clauses then $\phi$ is satisfiable.*

*Proof.* Assign random truth values to the variables. Let

$$E_i = \{i\text{-th clause is false}\}$$

Then

$$\Pr(E_i) = \left(\frac{1}{2}\right)^k$$

**Note:** $C_i$ is independent of $C_j$ if they don't share a variable.

# $k$-Satisfiability

**Theorem 2.** *Let $\phi = C_1 \wedge \cdots \wedge C_m$, where each $C_i$ has exactly $k$ literals. If no variable appears in more than $T = 2^k/(4k)$ clauses then $\phi$ is satisfiable.*

*Proof.* Assign random truth values to the variables. Let

$$E_i = \{i\text{-th clause is false}\}$$

Then

$$\Pr(E_i) = \left(\frac{1}{2}\right)^k$$

**Note:** $C_i$ is independent of $C_j$ if they don't share a variable.

**But:** Each of the $k$ variables of a clause $C_i$ can appear in $T$ other clauses! So

$$d \leq k \cdot T \leq 2^k/4.$$

# $k$-Satisfiability

**Theorem 2.** *Let $\phi = C_1 \wedge \cdots \wedge C_m$, where each $C_i$ has exactly $k$ literals. If no variable appears in more than $T = 2^k/(4k)$ clauses then $\phi$ is satisfiable.*

*Proof.* Assign random truth values to the variables. Let

$$E_i = \{i\text{-th clause is false}\}$$

Then

$$\Pr(E_i) = \left(\frac{1}{2}\right)^k$$

**Note:** $C_i$ is independent of $C_j$ if they don't share a variable.

**But:** Each of the $k$ variables of a clause $C_i$ can appear in $T$ other clauses! So

$$d \leq k \cdot T \leq 2^k/4.$$

**Therefore:** $4pd \leq 1$ and we can conclude that a satisfying assignment exists. □

# Hypergraph Coloring

**Definition 3** (Hypergraph)**.** *A hypergraph is a pair $H = (V, \mathcal{E})$, where $V$ is the set of vertices and $\mathcal{E}$ is the set of* **hyperedges***, where each hyperedge is a subset of $V$.*

Unlike in an ordinary graph, a hyperedge can connect any number of vertices, not just two.

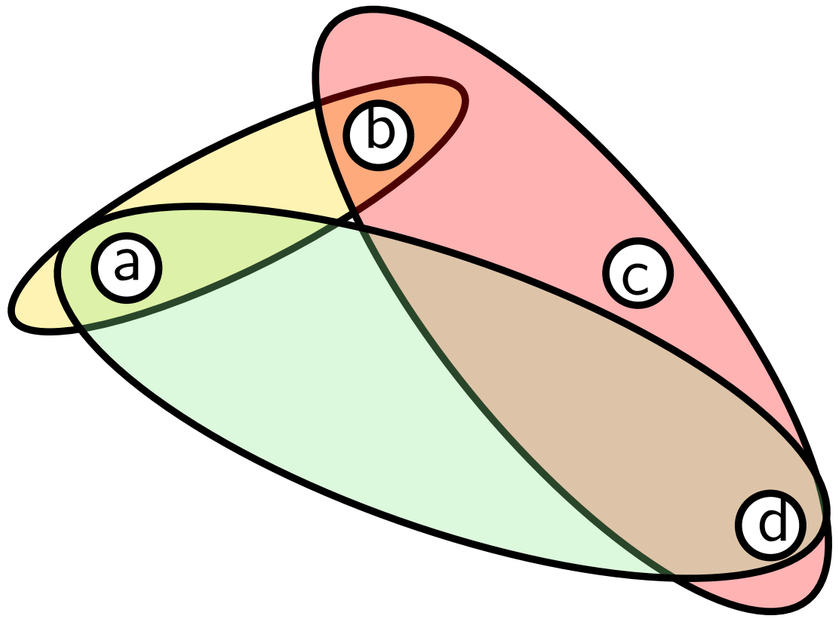
# Hypergraph Coloring

**Definition 3** (Hypergraph)**.** *A hypergraph is a pair $H = (V, \mathcal{E})$, where $V$ is the set of vertices and $\mathcal{E}$ is the set of* **hyperedges***, where each hyperedge is a subset of $V$.*

Unlike in an ordinary graph, a hyperedge can connect any number of vertices, not just two.

**Example:**

$$V = \{a, b, c, d\}, \qquad \text{and} \qquad \mathcal{E} = \{\{a, b\}, \{b, c, d\}, \{a, d\}\}$$



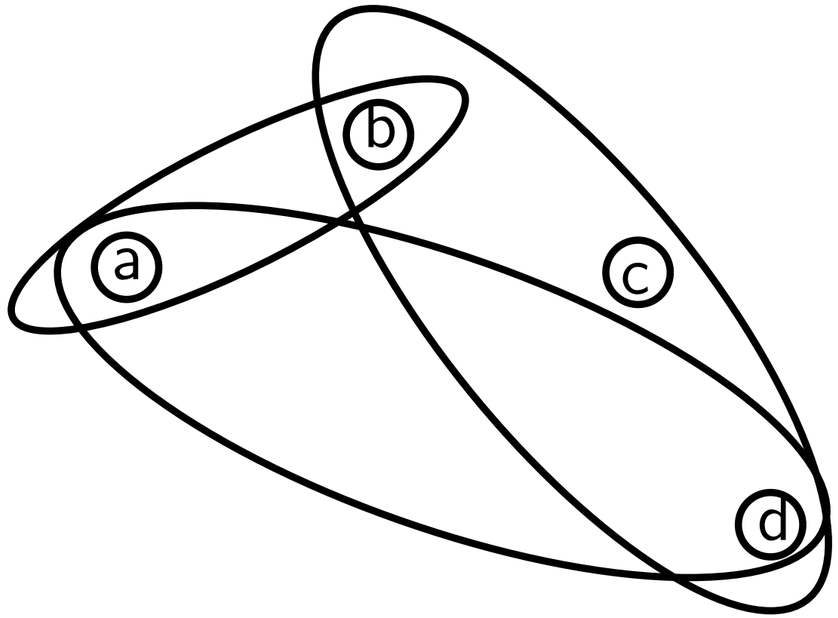
# Hypergraph Coloring

A hypergraph $H$ has **Property B** (i.e., $2$-colorable) if there exists a $2$-coloring of $V(H)$ s.t. no hyperedge is monochromatic.

# Hypergraph Coloring

A hypergraph $H$ has **Property B** (i.e., $2$-colorable) if there exists a $2$-coloring of $V(H)$ s.t. no hyperedge is monochromatic.

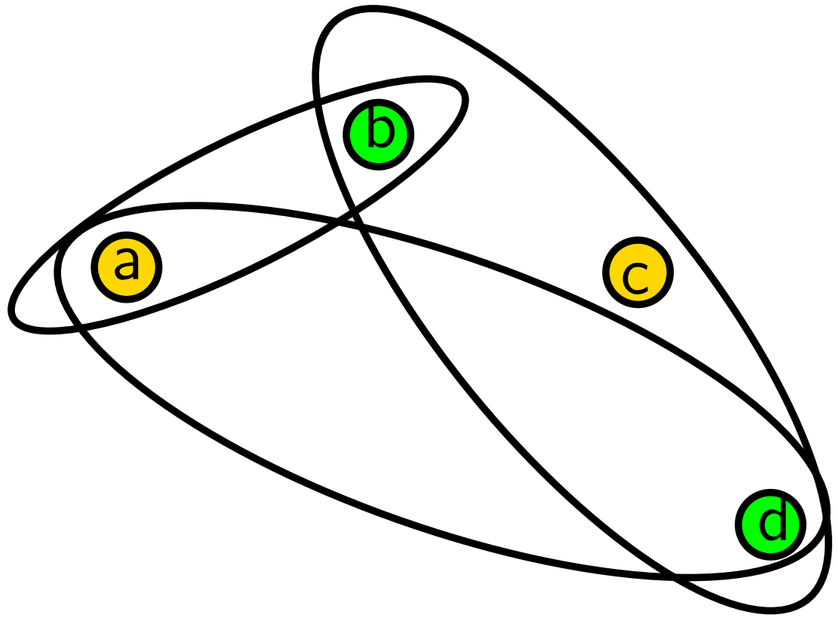
Is this hypergraph $2$-colorable?



# Hypergraph Coloring

A hypergraph $H$ has **Property B** (i.e., $2$-colorable) if there exists a $2$-coloring of $V(H)$ s.t. no hyperedge is monochromatic.

Is this hypergraph $2$-colorable?



**Theorem 3** (Lovász Local Lemma)**.** *Let $d \in \mathbb{N}$ and $p \in \mathbb{R}$ with*

$$ep(d+1) \leq 1.$$

*Let $E_1, E_2, \ldots, E_n$ be events. If*

- $\Pr(E_i) \leq p$ *for all $i$, and*
- *The degree of their dependency graph is bounded by $d$*

*then*

$$\Pr\left(\bigcap_{1 \leq i \leq n} \overline{E}_i\right) > 0$$

# Hypergraph Coloring

**Theorem 4.** *Let $H = (V, \mathcal{E})$ be a hypergraph. If $\forall e \in \mathcal{E}$, $e$ has size at least $k$ and intersect at most $d$ other edges, and*

$$e(d+1) \leq 2^{k-1}$$

*the $H$ has property $B$ (i.e., 2-colorable).*

# Hypergraph Coloring

**Theorem 4.** *Let $H = (V, \mathcal{E})$ be a hypergraph. If $\forall e \in \mathcal{E}$, $e$ has size at least $k$ and intersect at most $d$ other edges, and*

$$e(d+1) \leq 2^{k-1}$$

*the $H$ has property $B$ (i.e., 2-colorable).*

*Proof.* Consider a random 2-coloring of $V(H)$.

Let

$$A_f = \{f \text{ is monochromatic}\}, \qquad \forall f \in \mathcal{E}(H)$$

# Hypergraph Coloring

**Theorem 4.** *Let $H = (V, \mathcal{E})$ be a hypergraph. If $\forall e \in \mathcal{E}$, $e$ has size at least $k$ and intersect at most $d$ other edges, and*

$$e(d+1) \leq 2^{k-1}$$

*the $H$ has property $B$ (i.e., 2-colorable).*

*Proof.* Consider a random 2-coloring of $V(H)$.

Let

$$A_f = \{f \text{ is monochromatic}\}, \qquad \forall f \in \mathcal{E}(H)$$

Then

$$\Pr(A_f) = 2 \cdot \left(\frac{1}{2}\right)^{|f|} = \frac{2}{2^{|f|}} \leq \frac{2}{2^k} \leq 2^{1-k} = p$$

# Hypergraph Coloring

**Theorem 4.** *Let $H = (V, \mathcal{E})$ be a hypergraph. If $\forall e \in \mathcal{E}$, $e$ has size at least $k$ and intersect at most $d$ other edges, and*

$$e(d+1) \leq 2^{k-1}$$

*the $H$ has property $B$ (i.e., 2-colorable).*

*Proof.* Consider a random 2-coloring of $V(H)$.

Let

$$A_f = \{f \text{ is monochromatic}\}, \qquad \forall f \in \mathcal{E}(H)$$

Then

$$\Pr(A_f) = 2 \cdot \left(\frac{1}{2}\right)^{|f|} = \frac{2}{2^{|f|}} \leq \frac{2}{2^k} \leq 2^{1-k} = p$$

Let's discuss the dependencies,

$$D_f = \{f' \in \mathcal{E}(H) \,:\, f' \cap f \neq \emptyset\}$$

# Hypergraph Coloring

**Theorem 4.** *Let $H = (V, \mathcal{E})$ be a hypergraph. If $\forall e \in \mathcal{E}$, $e$ has size at least $k$ and intersect at most $d$ other edges, and*

$$e(d+1) \leq 2^{k-1}$$

*the $H$ has property $B$ (i.e., 2-colorable).*

*Proof.* Consider a random 2-coloring of $V(H)$.

Let

$$A_f = \{f \text{ is monochromatic}\}, \qquad \forall f \in \mathcal{E}(H)$$

Then

$$\Pr(A_f) = 2 \cdot \left(\frac{1}{2}\right)^{|f|} = \frac{2}{2^{|f|}} \leq \frac{2}{2^k} \leq 2^{1-k} = p$$

Let's discuss the dependencies,

$$D_f = \{f' \in \mathcal{E}(H) \,:\, f' \cap f \neq \emptyset\}$$

By assumption $|D_f| \leq d$.

# Hypergraph Coloring

**Theorem 4.** *Let $H = (V, \mathcal{E})$ be a hypergraph. If $\forall e \in \mathcal{E}$, $e$ has size at least $k$ and intersect at most $d$ other edges, and*

$$e(d+1) \leq 2^{k-1}$$

*the $H$ has property $B$ (i.e., 2-colorable).*

*Proof.* Consider a random 2-coloring of $V(H)$.

Let

$$A_f = \{f \text{ is monochromatic}\}, \qquad \forall f \in \mathcal{E}(H)$$

Then

$$\Pr(A_f) = 2 \cdot \left(\frac{1}{2}\right)^{|f|} = \frac{2}{2^{|f|}} \leq \frac{2}{2^k} \leq 2^{1-k} = p$$

Let's discuss the dependencies,

$$D_f = \{f' \in \mathcal{E}(H) \,:\, f' \cap f \neq \emptyset\}$$

By assumption $|D_f| \leq d$. Since $ep(d+1) \leq 1$ then $H$ has property $B$. □

# The General Lovász Local Lemma

**Theorem 5** (General Lovász Local Lemma)**.** *Let $E_1, E_2, \ldots, E_n$ be events in an arbitrary probability space $\Omega$ and let $G = (V, E)$ be the dependency graph of these events. Assume there exists $x_1, \ldots, x_n \in [0, 1]$ such that, for al $1 \leq i \leq n$,*

$$\Pr(E_i) \leq x_i \prod_{(i,j) \in E} (1 - x_j).$$

*Then*

$$\Pr\left(\bigcap_{1 \leq i \leq n} \overline{E}_i\right) > \prod_{i=1}^{n} (1 - x_i)$$

# The Lovász Local Lemma

*Proof.* Consider the following claim:

**Claim 1.** *For all $S \subseteq \{1, \ldots, n\}$ and $k \notin S$,*

$$\Pr\left(E_k \mid \bigcap_{i \in S} \overline{E}_i\right) \leq 2p.$$

If the claim holds, then the Local Lemma would follow because

$$\Pr\left(\bigcap_{1 \leq i \leq n} \overline{E}_i\right) = \prod_{1 \leq i \leq n} \Pr\left(\overline{E}_i \mid \bigcap_{1 \leq j \leq i} \overline{E}_j\right)$$

# The Lovász Local Lemma

*Proof.* Consider the following claim:

**Claim 1.** *For all $S \subseteq \{1, \ldots, n\}$ and $k \notin S$,*

$$\Pr\left(E_k \mid \bigcap_{i \in S} \overline{E}_i\right) \leq 2p.$$

If the claim holds, then the Local Lemma would follow because

$$\Pr\left(\bigcap_{1 \leq i \leq n} \overline{E}_i\right) = \prod_{1 \leq i \leq n} \Pr\left(\overline{E}_i \mid \bigcap_{1 \leq j \leq i} \overline{E}_j\right)$$

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

# The Lovász Local Lemma

*Proof.* Consider the following claim:

**Claim 1.** *For all $S \subseteq \{1, \ldots, n\}$ and $k \notin S$,*

$$\Pr\left(E_k \mid \bigcap_{i \in S} \overline{E}_i\right) \leq 2p.$$

If the claim holds, then the Local Lemma would follow because

$$\Pr\left(\bigcap_{1 \leq i \leq n} \overline{E}_i\right) = \prod_{1 \leq i \leq n} \Pr\left(\overline{E}_i \mid \bigcap_{1 \leq j \leq i} \overline{E}_j\right)$$

$$= \prod_{1 \leq i \leq n} \left[1 - \Pr\left(E_i \mid \bigcap_{1 \leq j \leq i} \overline{E}_j\right)\right] \geq \prod_{1 \leq i \leq n} (1 - 2p) > 0.$$

□

# The Mistic Lemma

**Lemma 1.** *For all $S \subseteq \{1, \ldots, n\}$ and $k \notin S$,*

$$\Pr\left(E_k \mid \bigcap_{i \in S} \overline{E}_i\right) \leq 2p.$$

# Proof of The Mistic Lemma

*Proof.* By induction on $s = |S|$.

# Proof of The Mistic Lemma

*Proof.* By induction on $s = |S|$.

**Base case $s = 0$ :** follows from the assumption.

$$\Pr(E_i) \leq p.$$

Otherwise, we can split $S$ into

$$S_1 = \{i \mid k \text{ and } i \text{ are connected in the dependency graph}\} \quad \text{and} \quad S_2 = S \setminus S_1$$

If $S_1 = \emptyset$, then $E_k$ is mutually independent of all the events in $S$.

# Proof of The Mistic Lemma

*Proof.* By induction on $s = |S|$.

**Base case $s = 0$ :** follows from the assumption.

$$\Pr(E_i) \leq p.$$

Otherwise, we can split $S$ into

$$S_1 = \{i \mid k \text{ and } i \text{ are connected in the dependency graph}\} \quad \text{and} \quad S_2 = S \setminus S_1$$

If $S_1 = \emptyset$, then $E_k$ is mutually independent of all the events in $S$.

Assume that $|S_2| < |S|$ and let $F_{S_1} = \cap_{i \in S_1} \overline{E}_i$ and define $F_{S_2}$ and $F_S$ analogously.

# Proof of The Mistic Lemma

*Proof.* By induction on $s = |S|$.

**Base case $s = 0$ :** follows from the assumption.

$$\Pr(E_i) \leq p.$$

Otherwise, we can split $S$ into

$$S_1 = \{i \mid k \text{ and } i \text{ are connected in the dependency graph}\} \quad \text{and} \quad S_2 = S \setminus S_1$$

If $S_1 = \emptyset$, then $E_k$ is mutually independent of all the events in $S$.

Assume that $|S_2| < |S|$ and let $F_{S_1} = \cap_{i \in S_1} \overline{E}_i$ and define $F_{S_2}$ and $F_S$ analogously.

Observation: $|S_1| \leq d$

# Proof of The Mistic Lemma

*Proof.* Split $S$ into

$$S_1 = \{i \mid k \text{ and } i \text{ are connected in the dependency graph}\} \quad \text{and} \quad S_2 = S \setminus S_1$$

If $S_1 = \emptyset$, then $E_k$ is mutually independent of all the events in $S$.

Assume that $|S_2| < |S|$ and let $F_{S_1} = \cap_{i \in S_1} \overline{E}_i$ and define $F_{S_2}$ and $F_S$ analogously.

Observation: $|S_1| \leq d$. Now

$$\Pr\left(E_k \mid F_S\right) = \frac{\Pr\left(E_k \cap F_S\right)}{\Pr\left(F_S\right)}$$

# Proof of The Mistic Lemma

*Proof.* Split $S$ into

$$S_1 = \{i \mid k \text{ and } i \text{ are connected in the dependency graph}\} \quad \text{and} \quad S_2 = S \setminus S_1$$

If $S_1 = \emptyset$, then $E_k$ is mutually independent of all the events in $S$.

Assume that $|S_2| < |S|$ and let $F_{S_1} = \cap_{i \in S_1} \overline{E}_i$ and define $F_{S_2}$ and $F_S$ analogously.

Observation: $|S_1| \leq d$. Now

$$\Pr(E_k \mid F_S) = \frac{\Pr(E_k \cap F_S)}{\Pr(F_S)} = \frac{\Pr(E_k \cap F_{S_1} \mid F_{S_2}) \Pr(F_{S_2})}{\Pr(F_{S_1} \mid F_{S_2}) \Pr(F_{S_2})}$$

# Proof of The Mistic Lemma

*Proof.* Split $S$ into

$$S_1 = \{i \mid k \text{ and } i \text{ are connected in the dependency graph}\} \quad \text{and} \quad S_2 = S \setminus S_1$$

If $S_1 = \emptyset$, then $E_k$ is mutually independent of all the events in $S$.

Assume that $|S_2| < |S|$ and let $F_{S_1} = \cap_{i \in S_1} \overline{E}_i$ and define $F_{S_2}$ and $F_S$ analogously.

Observation: $|S_1| \leq d$. Now

$$\Pr(E_k \mid F_S) = \frac{\Pr(E_k \cap F_S)}{\Pr(F_S)} = \frac{\Pr(E_k \cap F_{S_1} \mid F_{S_2}) \Pr(F_{S_2})}{\Pr(F_{S_1} \mid F_{S_2}) \Pr(F_{S_2})}$$

We know that

$$\Pr(E_k \cap F_{S_1} \mid F_{S_2}) \leq \Pr(E_k \mid F_{S_2}) \leq p$$

because $E_k$ is independent of $S_2$

# Proof of The Mistic Lemma

*Proof.* Assume that $|S_2| < |S|$ and let $F_{S_1} = \cap_{i \in S_1} \overline{E}_i$ and define $F_{S_2}$ and $F_S$ analogously.

Observation: $|S_1| \leq d$. Now

$$\Pr\left(E_k \mid F_S\right) = \frac{\Pr\left(E_k \cap F_S\right)}{\Pr\left(F_S\right)} = \frac{\Pr\left(E_k \cap F_{S_1} \mid F_{S_2}\right) \Pr\left(F_{S_2}\right)}{\Pr\left(F_{S_1} \mid F_{S_2}\right) \Pr\left(F_{S_2}\right)}$$

We know that

$$\Pr\left(E_k \cap F_{S_1} \mid F_{S_2}\right) \leq \Pr\left(E_k \mid F_{S_2}\right) \leq p$$

because $E_k$ is independent of $S_2$, and

$$\Pr\left(F_{S_1} \mid F_{S_2}\right) = \Pr\left(\cap_{i \in S_1} \overline{E}_i \mid F_{S_2}\right)$$

# Proof of The Mistic Lemma

*Proof.* Assume that $|S_2| < |S|$ and let $F_{S_1} = \cap_{i \in S_1} \overline{E}_i$ and define $F_{S_2}$ and $F_S$ analogously.

Observation: $|S_1| \leq d$. Now

$$\Pr\left(E_k \mid F_S\right) = \frac{\Pr\left(E_k \cap F_S\right)}{\Pr\left(F_S\right)} = \frac{\Pr\left(E_k \cap F_{S_1} \mid F_{S_2}\right) \Pr\left(F_{S_2}\right)}{\Pr\left(F_{S_1} \mid F_{S_2}\right) \Pr\left(F_{S_2}\right)}$$

We know that

$$\Pr\left(E_k \cap F_{S_1} \mid F_{S_2}\right) \leq \Pr\left(E_k \mid F_{S_2}\right) \leq p$$

because $E_k$ is independent of $S_2$, and

$$\Pr\left(F_{S_1} \mid F_{S_2}\right) = \Pr\left(\cap_{i \in S_1} \overline{E}_i \mid F_{S_2}\right) \geq 1 - \sum_{i \in S_1} \Pr\left(E_i \mid F_{S_2}\right)$$

# Proof of The Mistic Lemma – Almost there...

*Proof.* Assume that $|S_2| < |S|$ and let $F_{S_1} = \cap_{i \in S_1} \overline{E}_i$ and define $F_{S_2}$ and $F_S$ analogously.

Observation: $|S_1| \leq d$. Now

$$\Pr\left(E_k \mid F_S\right) = \frac{\Pr\left(E_k \cap F_S\right)}{\Pr\left(F_S\right)} = \frac{\Pr\left(E_k \cap F_{S_1} \mid F_{S_2}\right)\Pr\left(F_{S_2}\right)}{\Pr\left(F_{S_1} \mid F_{S_2}\right)\Pr\left(F_{S_2}\right)}$$

We know that

$$\Pr\left(E_k \cap F_{S_1} \mid F_{S_2}\right) \leq \Pr\left(E_k \mid F_{S_2}\right) \leq p$$

because $E_k$ is independent of $S_2$, and

$$\Pr\left(F_{S_1} \mid F_{S_2}\right) = \Pr\left(\cap_{i \in S_1} \overline{E}_i \mid F_{S_2}\right) \geq 1 - \sum_{i \in S_1} \Pr\left(E_i \mid F_{S_2}\right) \geq 1 - \sum_{i \in S_1} 2p \geq 2pd \geq \frac{1}{2}$$

Inductive HP on the second inequality (since $|S_2| < |S| = s$ and $i \notin S_2, \forall i \in S_1$) and $|S_1| < d$ for the third one.

# Proof of The Mistic Lemma

*Proof.* Putting all together:

$$\Pr\left(E_k \cap F_{S_1} \mid F_{S_2}\right) \leq \Pr\left(E_k \mid F_{S_2}\right) \leq p$$

And

$$\Pr\left(F_{S_1} \mid F_{S_2}\right) = \Pr\left(\cap_{i \in S_1} \overline{E}_i \mid F_{S_2}\right) \geq 1 - \sum_{i \in S_1} \Pr\left(E_i \mid F_{S_2}\right) \geq 1 - \sum_{i \in S_1} 2p \geq 2pd \geq \frac{1}{2}.$$

We have

$$\Pr\left(E_k \mid F_S\right) = \frac{\Pr\left(E_k \cap F_S\right)}{\Pr\left(F_S\right)} = \frac{\Pr\left(E_k \cap F_{S_1} \mid F_{S_2}\right) \Pr\left(F_{S_2}\right)}{\Pr\left(F_{S_1} \mid F_{S_2}\right) \Pr\left(F_{S_2}\right)} \leq \frac{p}{1/2} = 2p$$

□