The Probabilistic Method

Techniques

- Union bound
- Argument from expectation
- Alterations
- The second moment method
- **The (Lovasz) Local Lemma**

And much more

- Alon and Spencer, "The Probabilistic Method"
- Bolobas, "Random Graphs"

Lovasz Local Lemma: Main Idea

- Recall the union bound technique:
  - want to prove $\text{Prob}[A] > 0$
  - $\bar{A} \Rightarrow$ (or $\Leftrightarrow$) some bad events $B_1 \cup \cdots \cup B_n$
  - done if $\text{Prob}[B_1 \cup \cdots \cup B_n] < 1$

Lovasz Local Lemma: Main Idea

- Recall the union bound technique:
  - want to prove Prob$[A] > 0$
  - $\bar{A} \Rightarrow$ (or $\Leftrightarrow$) some bad events $B_1 \cup \cdots \cup B_n$
  - done if Prob$[B_1 \cup \cdots \cup B_n] < 1$
- Could also have tried to show

$$\text{Prob}[\bar{B}_1 \cap \cdots \cap \bar{B}_n] > 0$$

Lovasz Local Lemma: Main Idea

- Recall the union bound technique:
  - want to prove Prob$[A] > 0$
  - $\bar{A} \Rightarrow$ (or $\Leftrightarrow$) some bad events $B_1 \cup \cdots \cup B_n$
  - done if Prob$[B_1 \cup \cdots \cup B_n] < 1$
- Could also have tried to show

$$\text{Prob}[\bar{B}_1 \cap \cdots \cap \bar{B}_n] > 0$$

- Would be much simpler if the B_i were mutually independent, because

$$\text{Prob}[\bar{B}_1 \cap \cdots \cap \bar{B}_n] = \prod_{i=1}^{n} \text{Prob}[\bar{B}_i] > 0$$

Lovasz Local Lemma: Main Idea

- Recall the union bound technique:
  - want to prove $\text{Prob}[A] > 0$
  - $\bar{A} \Rightarrow$ (or $\Leftrightarrow$) some bad events $B_1 \cup \cdots \cup B_n$
  - done if $\text{Prob}[B_1 \cup \cdots \cup B_n] < 1$
- Could also have tried to show

$$\text{Prob}[\bar{B}_1 \cap \cdots \cap \bar{B}_n] > 0$$

- Would be much simpler if the B_i were mutually independent, because

$$\text{Prob}[\bar{B}_1 \cap \cdots \cap \bar{B}_n] = \prod_{i=1}^{n} \text{Prob}[\bar{B}_i] > 0$$

Main Idea

Lovasz Local Lemma is a sort of generalization of this idea when the "bad" events are not mutually independent

PTCF: Mutual Independence

Definition (Recall)

A set $B_1, \dots, B_n$ of events are said to be mutually independent (or simply independent) if and only if, for any subset $S \subseteq [n]$,

$$\text{Prob}\left[\bigcap_{i \in S} B_i\right] = \prod_{i \in S} \text{Prob}[B_i]$$

PTCF: Mutual Independence

Definition (Recall)

A set $B_1, \dots, B_n$ of events are said to be mutually independent (or simply independent) if and only if, for any subset $S \subseteq [n]$,

$$\text{Prob}\left[\bigcap_{i \in S} B_i\right] = \prod_{i \in S} \text{Prob}[B_i]$$

Definition (New)

An event B is mutually independent of events $B_1, \cdots, B_k$ if, for any subset $S \subseteq [k]$,

$$\text{Prob}\left[B \mid \bigcap_{i \in S} B_i\right] = \text{Prob}[B]$$

PTCF: Mutual Independence

Definition (Recall)

A set $B_1, \dots, B_n$ of events are said to be mutually independent (or simply independent) if and only if, for any subset $S \subseteq [n]$,

$$\text{Prob}\left[\bigcap_{i \in S} B_i\right] = \prod_{i \in S} \text{Prob}[B_i]$$

Definition (New)

An event B is mutually independent of events $B_1, \cdots, B_k$ if, for any subset $S \subseteq [k]$,

$$\text{Prob}\left[B \mid \bigcap_{i \in S} B_i\right] = \text{Prob}[B]$$

Question: can you find B, B_1, B_2, B_3 such that B is mutually independent of B_1 and B_2 but not from all three?

PTCF: Dependency Graph

Definition

Given a set of events $B_1, \cdots, B_n$, a directed graph $D = ([n], E)$ is called a dependency digraph for the events if every event B_i is independent of all events B_j for which $(i, j) \notin E$.

PTCF: Dependency Graph

Definition

Given a set of events $B_1, \cdots, B_n$, a directed graph $D = ([n], E)$ is called a dependency digraph for the events if every event B_i is independent of all events B_j for which $(i, j) \notin E$.

- What's a dependency digraph of a set of mutually independence events?

PTCF: Dependency Graph

Definition

Given a set of events $B_1, \cdots, B_n$, a directed graph $D = ([n], E)$ is called a dependency digraph for the events if every event B_i is independent of all events B_j for which $(i, j) \notin E$.

- What's a dependency digraph of a set of mutually independence events?
- Dependency digraph is **not unique**!

Lemma (General Case)

Let $B_1, \cdots, B_n$ be events in some probability space. Suppose $D = ([n], E)$ is a dependency digraph of these events, and suppose there are real numbers $x_1, \cdots, x_n$ such that

- $0 \leq x_i < 1$
- $\text{Prob}[B_i] \leq x_i \prod_{(i,j)\in E} (1 - x_j)$ *for all* $i \in [n]$

Then,

$$\text{Prob}\left[\bigcap_{i=1}^{n} \bar{B}_i\right] \geq \prod_{i=1}^{n}(1 - x_i)$$

The Local Lemma

Lemma (Symmetric Case)

Let $B_1, \cdots, B_n$ *be events in some probability space. Suppose* $D = ([n], E)$ *is a dependency digraph of these events with maximum out-degree at most* Δ. *If, for all* i,

$$\text{Prob}[B_i] \leq p \leq \frac{1}{e(\Delta + 1)}$$

then

$$\text{Prob}\left[\bigcap_{i=1}^{n} \bar{B}_i\right] > 0.$$

The conclusion also holds if

$$\text{Prob}[B_i] \leq p \leq \frac{1}{4\Delta}$$

Example 1: Hypergraph Coloring

- $G = (V, E)$ a hypergraph, each edge has $\geq k$ vertices
- Each edge f intersects at most Δ other edges

Example 1: Hypergraph Coloring

- $G = (V, E)$ a hypergraph, each edge has $\geq k$ vertices
- Each edge f intersects at most Δ other edges
- Color each vertex randomly with red or blue
- B_f: event that f is monochromatic

$$\text{Prob}[B_f] = \frac{2}{2^{|f|}} \leq \frac{1}{2^{k-1}}$$

- There's a dependency digraph for the B_f with max out-degree $\leq \Delta$

Theorem

G is 2-colorable if

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

Example 2: k-SAT

Theorem

In a k-CNF formula φ, if no variable appears in more than $2^{k-2}/k$ clauses, then φ is satisfiable.

Example 3: Edge-Disjoint Paths

- $\mathcal{N}$ a directed graph with n inputs and n outputs
- From input a_i to output b_i there is a set P_i of m paths
- In switching networks, we often want to find (or want to know if there exists) a set of edge-disjoint $(a_i \to b_i)$-paths

Theorem

Suppose $8nk \leq m$ and each path in P_i shares an edge with at most k paths in any P_j, $j \neq i$. Then, there exists a set of edge-disjoint $(a_i \to b_i)$-paths.