Recap :

$P = (\Omega, p)$: prob. dist^n.

Sampling x from P : picking an element from Ω, prob. of x being picked is $p(x)$.

Random Var. $X : \Omega \to \mathbb{R}$

Expected value of r.v. X

$$E[X] = \sum_{\omega \in \Omega} X(\omega) \cdot p(\omega)$$

$$= \sum_{z \in \text{Range}(X)} z \cdot \underbrace{\Pr[X^{-1}(z)]}_{\text{also written as } \Pr[X = z]}$$

Linearity of Expectation :

$$E[X_1 + X_2 + \cdots + X_k] = E[X_1] + \cdots + E[X_k]$$

- follows from def^n of expectation
- holds for <u>ANY</u> random variables $X_1, \cdots, X_k$. The random variables can be arbitrarily dependent on each other.

Plan for Lecture 18 :

using these basic probability definitions / results for

Part a : proving existence (via prob. method)

Part b : analyzing simple algorithms / processes - a surprising puzzle.

PROBABILISTIC METHOD :

For showing existence of objects with special property

To show existence of object with certain property P, sample the object from some distribution, and show that prob. of the sample having property P is greater than 0.

Example 1 : The Satisfiability Problem (SAT)

Given a formula ϕ on n variables $x_1 \cdots x_n$, does there exist an assignment to these variables s.t. $\phi(x_1 \cdots x_n) = 1$?

Hard computational problem, unlikely to have a poly(n) time algorithm.

A simplification : 3-Conjunctive Normal Form Satisfiability Problem (3-CNF-SAT / 3-SAT)

$$\phi(x_1 \cdots x_n) = (x_1 \vee x_4 \vee x_{10}) \wedge (\neg x_3 \vee x_4 \vee \neg x_{10}) \wedge (\neg x_4 \vee \neg x_1 \vee x_{10}) \wedge (x_3 \vee \neg x_{10} \vee x_1)$$

ϕ is an AND of m clauses, each clause is an OR of 3 x_is / their negations.

each clause must have three different literals.

However, a clause can have both x_i and $\neg x_i$.

Hard computational problem, unlikely to have a poly(n) time algorithm.

QN : Show that for any 3-CNF formula ϕ with n variables and m clauses, there exists an assignment to $x_1 \cdots x_n$ that satisfies at least $7m/8$ clauses.

Proof: Using probabilistic method.

Pick uniformly random value $b_i \leftarrow \{0,1\}$ for each $i \in [n]$, set $x_i = b_i$.

To prove:

$$p = \Pr\left[\begin{array}{c}\text{at least } 7m/8 \text{ clauses of } \phi \\ \text{are satisfied by the assignment}\end{array}\right] > 0$$

Observation: Let X be a random var. denoting the number of clauses satisfied. If we prove that $E[X] \geq 7m/8$, then we can conclude that $p > 0$.

$$E[X] = \sum_{i=1}^{m} i \cdot \Pr\left[\begin{array}{c}i \text{ clauses are} \\ \text{satisfied}\end{array}\right]$$

If $\Pr\left[\begin{array}{c}i \text{ clauses are} \\ \text{satisfied}\end{array}\right]$ is 0

for all $i \geq 7m/8$, then $E[X]$ has to be less than $7m/8$.

To prove :

$$E[X] \geq 7m/8.$$

Computing $E[X]$ directly can be difficult.

Observation : Let random var. $X_i = 1$ if i^{th} clause is satisfied, and 0 otherwise.

Then, $X = X_1 + \cdots + X_m$, and therefore

$$E[X] = E[X_1] + \cdots + E[X_m].$$

Observation : For any $i \in \{1, 2, \ldots, m\}$,

$$E[X_i] \geq 7/8$$

Proof : $E[X_i] = Pr[X_i^{-1}(1)]$

Suppose i^{th} clause is $y_{i_1} \vee y_{i_2} \vee y_{i_3}$

where $i_1, i_2, i_3 \in \{1, 2, \ldots, n\}$ and y_{i_j} is either x_{i_j} or $\neg x_{i_j}$.

If the clause contains a variable and its negation, then the clause will always evaluate to 1.

If they are all distinct, then

$$\Pr\left[\, i^{th} \text{ clause evaluates to } 0 \,\right] = 1/8.$$

$$\therefore \quad E[X_i] = \Pr\left[\, X_i(1) \,\right] \geq 7/8$$

■

Therefore, we have shown $E[X] \geq \frac{7m}{8}$.

As a result, there exists an assignment such that at least $7m/8$ clauses are satisfied.

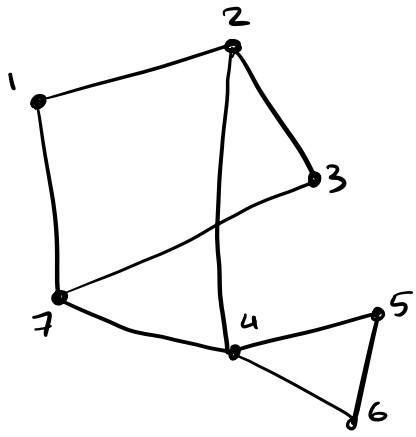
■

Example 2: Graphs with large bipartite subgraph.

Graph $G = (V, E)$

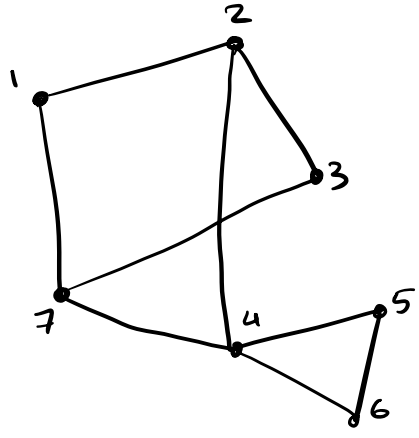
V: set of vertices

E: set of edges (undirected)

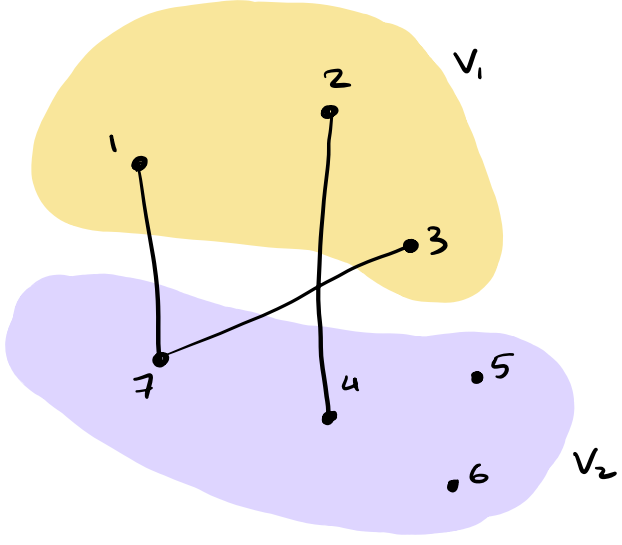


Subgraph $H = (V, F)$ where $F \subseteq E$.

H is bipartite if $V = V_1 \cup V_2$, $V_1 \cap V_2 = \emptyset$, and all edges in F have one endpoint in V_1 and another in V_2.



G



H

Qn: Let $|V| = n$, $|E| = m$.
How large can $|F|$ be?

Claim: For any graph $G = (V, E)$, $\exists$ subgraph $H = (V, F)$ s.t. H is bipartite and $|F| \geq m/2$

We want to use the probabilistic method. We have two properties that are somewhat conflicting:
P_1: graph is bipartite P_2: graph has many edges.

Attempt 1: sample a unif. rand. bipartite subgraph of G. How to show
$\Pr[$ sampled subgraph has $\geq m/2$ edges $] > 0$?

Attempt 2: sample a unif. rand. subgraph with at least $m/2$ edges. How to show
$\Pr[$ sampled subgraph is bipartite $] > 0$?

Proof: Using coloring.

For each $v \in V$, color v red w.p. $1/2$, color it blue w.p. $1/2$.
V_1: red colored vertices V_2: blue colored vert.

X = no. of edges with one endpt in V_1, another in V_2.

Claim: $E[X] \geq m/2$

Proof: For each edge $e \in E$, let

$$X_e = \begin{cases} 1 & \text{if exactly one endpt of } e \text{ is in } V_1 \\ 0 & \text{otherwise.} \end{cases}$$

$$E[X] = \sum_{e \in E} E[X_e]$$

For any $e \in E$, $Pr[X_e^{-1}(1)] = 1/2$

$\therefore$ $E[X] = m/2$. ∎

Since $E[X] = m/2$, there exists a red/blue coloring s.t. number of edges with different colored endpoints is at least $m/2$.

Why? Suppose not. Then, this means that $Pr[X = \alpha] = 0$ for all $\alpha \geq m/2$.

We know $E[X] = \sum_{z=1}^{m} z \cdot Pr[X^{-1}(z)]$

$$= \sum_{z=1}^{m/2-1} z \cdot Pr[X^{-1}(z)]$$

$$\leq (m/2 - 1) \sum_{z=1}^{m/2-1} Pr[X^{-1}(z)] = (m/2 - 1)$$

Let V_1, V_2 be the partitioning of V s.t. at least $m/2$ edges go across V_1

$H = (V, F)$ where $F = \{(u,v) : u \in V_1, v \in V_2\}$

$|F| \geq m/2$. Hence H is the required bipartite subgraph.

■

H.W. 1: Show that there exist ECCs with msg space $\{0,1\}^n$, code space $\{0,1\}^{4n}$ that are $n/4$ - noise tolerant.

H.W. 2: Prove that for any set $A \subseteq \mathbb{N}$ s.t. $|A| = n$, $\exists\ S \subseteq A$, $|S| \geq n/3$ s.t. $\forall\ i, j, k \in S$, $i + j \neq k$.

ANALYZING ALGORITHMS / PROCESSES

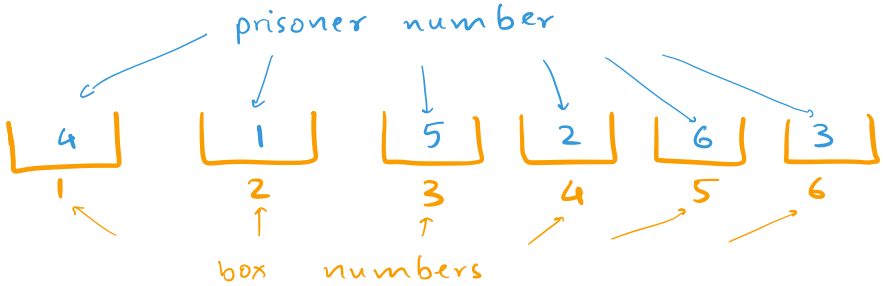
1. 2n prisoners problem

There are $2n$ prisoners in a jail, numbered 1 to $2n$.
Jailer has $2n$ boxes, numbered $1, 2, \ldots, 2n$. Jailer picks a unif. rand. perm. π, and for each $i \in \{1, 2, \ldots, 2n\}$, puts name of $\pi(i)^{th}$ prisoner in box i.

Example: Suppose $n = 3$,

$\pi(1) = 4$ $\pi(2) = 1$ $\pi(3) = 5$ $\pi(4) = 2$

$\pi(5) = 6$ $\pi(6) = 3$



Prisoners can decide some strategy. After the strategy is finalized, the prisoners are not allowed to communicate.
They must go in, one by one, and are allowed to open at most n boxes.

All $2n$ prisoners are released if EVERYONE finds their name in one of the n boxes that they opened.

Can the prisoners come up with a strategy to maximize the probability that all $2n$ prisoners are released?

Naive Strategy: every prisoner opens n uniformly random boxes.

$$\Pr[\text{all prisoners are released}] = \frac{1}{2^{2n}}.$$

Surprisingly, there exists a strategy to ensure that all prisoners are released with prob. at least 0.3 !!

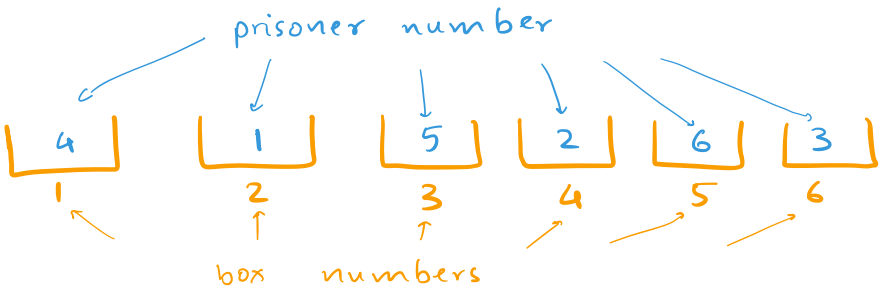
Moreover, the strategy is deterministic (and therefore the probability is only governed by the choice of perm. π).

Strategy for i^{th} prisoner:

Let $p_0 = i$.

For $j = 1$ to n, do:

1. open box numbered p_{j-1}. Let z denote the number in box p_{j-1}.
2. If $z = i$, then exit. Else set $p_j = z$.



Example:

- Prisoner 1 opens boxes numbered 1, 4 and 2
- Prisoner 2 opens boxes numbered 2, 1 and 4.
- Prisoner 3 opens boxes numbered 3, 5 and 6
- Prisoner 4 opens boxes numbered 4, 2 and 1.
- Prisoner 5 opens boxes numbered 5, 6 and 3.
- Prisoner 6 opens boxes numbered 6, 3, and 5.

All of them find their numbers in at most n box openings.

This puzzle is essentially a problem on random permutations.

Def^n [Cycle Decomposition of a permutation]

Given permutation π, we can partition $\{1, 2, \ldots, n\}$ into disjoint subsets $P_1 \ldots P_t$ s.t. for every $i \in [t]$, for every $x \in P_i$,

$$\{x, \pi(x), \pi(\pi(x)), \ldots\} = P_i .$$

Examples :

$\pi(1) = 4$, $\pi(2) = 6$ $\pi(3) = 2$ $\pi(4) = 1$

$\pi(5) = 5$ $\pi(6) = 7$ $\pi(7) = 3$.

$P_1 = \{4, 1\}$, $P_2 = \{6, 7, 3, 2\}$, $P_3 = \{5\}$.

The partitioning is unique, and can be achieved as follows : start with 1, compute $\pi(1)$, $\pi(\pi(1))$, ... until the elements start repeating. These form the first partition. Remove these from $\{1, 2, \ldots, n\}$.

Then take one of the remaining numbers, say z, compute $\pi(z)$, $\pi(\pi(z))$, ..., and these form the second partition.

The success probability of the prisoners relies on the following two claims.

Claim 1: Suppose the jailer picks permutation π. π has a unique cycle decomposition. If all partitions in this decomposition have size $\leq n$, then all prisoners find their number within n steps (and therefore all are released).

Claim 2: For a unif. rand. permutation π,

$$\Pr\left[\begin{array}{l}\text{the cycle decomp. of } \pi \text{ has} \\ \text{a partition of size } > n\end{array}\right] = \frac{1}{n+1} + \cdots + \frac{1}{2n}$$

$$\sim \ln 2$$

we will see the proofs of these two claims in the next lecture.

Summary :

1. Using probabilistic method for showing existence: want to show that there exists objects having property P. We show this by sampling the object from some dist^n, and show that $\Pr[\text{sampled object has property } P] > 0$.

(a) For any 3CNF formula ϕ, there exists an assignment that satisfies at least $7m/8$ clauses.

Pick a random assignment. Show that $E[\text{clauses satisfied}] \geq 7m/8$

(b) Any graph $G=(V,E)$ has a bipartite subgraph $H=(V,F)$ s.t. $|F| \geq |E|/2$.

Pick a random partition of the vertices.

$E[\text{number of edges going across partition}] = \frac{m}{2}$

Hence, there exists a partitioning with at least $m/2$ edges going across the partition.

Both (a) and (b) crucially use linearity of expectation.

2. Properties of random permutations.

- cycle decomposition of a random perm.
- To prove (next class): with constant prob, all cycles have size at most n.

QUESTIONS:

H.W. 1: Show that there exist ECCs with msg space $\{0,1\}^n$, code space $\{0,1\}^{4n}$ that are $n/4$ - noise tolerant.

H.W. 2: Prove that for any set $A \subseteq \mathbb{N}$ s.t. $|A| = n$, $\exists\ S \subseteq A$, $|S| \geq n/3$ s.t. $\forall\ i, j, k \in S$, $i + j \neq k$.

H.W. 3: Pick a unif. rand. permutation σ
X = number of elements i s.t. $\sigma(i) = i$
What is $E[X]$?

H.W. 4: Pick a unif. rand. permutation σ.
Consider the cycle decomp. of σ.
X = size of partition containing 1.
What is $E[X]$?