10\8\08

X is a random variable and its value are $0, 1, 2, \ldots$

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

First Moment Method

$$E(X) = E(X \mid X=0)\, P(X=0) + E(X \mid X \geq 1)\, P(X \geq 1)$$

$$= \underbrace{E(X \mid X \geq 1)}_{\geq 1}\, P(X \geq 1)$$

$$\geq P(X \geq 1)$$

# Union Distinct Families

$\mathcal{A} \subseteq \{0,1\}^{[n]}$

is a collection of subsets of $[n]$

$\mathcal{A}$ is union free if $A_1 \cup A_2 \neq A_3 \cup A_4$ for distinct $A_1, A_2, A_3, A_4 \in \mathcal{A}$.

$\mathcal{A} = \{1\}, \{2\}, \{3\}, \ldots \{n\}$

is union-free

Choose a collection of $p$ random sets.

$X_1, X_2, \ldots, X_p$

$Z = \#$ of $i, j, k, l$ s.t. $X_i \cup X_j = X_k \cup X_l$

For a suitable choice of $p$, $E(Z) < 1$

$\Longrightarrow P(Z \geq 1) < 1$   First moment method

$\Longrightarrow \exists\ p$ sets with required property

$$E(Z) = p(p-1)(p-2)(p-3)\, P_r(X_i \cup X_j = X_k \cup X_l)$$
$$= p(p-1)(p-2)(p-3)\left(5/8\right)^n$$

$$E(Z) = p(p-1)(p-2)(p-3)\Pr(X_i \cup X_j = X_k \cup X_l)$$

$$= p(p-1)(p-2)(p-3)\left(5/8\right)^n$$

$X_i \cup X_j \neq X_k \cup X_l$

iff $\exists\, x \in [n]$ s.t.:

$x \in X_i \cup X_j \setminus X_k \cup X_l$

or $x \in X_k \cup X_l \setminus X_i \cup X_j$

$$\Pr\left( \begin{matrix} x \in X_i \cup X_j \setminus X_k \cup X_l \\ \text{or} \\ x \in X_k \cup X_l \setminus X_i \cup X_j \end{matrix} \right) = 3/8$$

$$\Pr\left(\begin{array}{c} x \in X_i \cup X_j \setminus X_k \cup X_l \\ \text{or } x \in X_k \cup X_l \setminus X_i \cup X_j \end{array}\right) = \frac{3}{8}$$

2 events are disjoint

$$\Pr(x \in X_i \cup X_j \setminus X_k \cup X_l) = \frac{3}{16}$$

| | $X_i$ | $X_j$ | $X_k$ | $X_l$ | $P$ |
|---|---|---|---|---|---|
| $x \notin$ any | 0 | 0 | 0 | 0 | $1/16$ |
| $x \in X_i$, $x \notin X_j \cup X_k \cup X_l$ | 1 | 0 | 0 | 0 | |
| | 0 | 1 | 0 | 0 | |
| | 1 | 1 | 0 | 0 | |
| | ⋮ | ⋮ | | | |
| | 1 | 1 | 1 | 1 | |

$$E(Z) = p(p-1)(p-2)(p-3)\left(\frac{5}{8}\right)^n$$

$$p \leq \left(\frac{8}{5}\right)^{n/4}$$

$$E(Z) < p^4\left(\frac{5}{8}\right)^n \leq 1 \quad \Rightarrow \exists \text{ family.}$$

$Z_1$ = # of repetitions $X_i = X_j$

$$E(Z_1) = \binom{p}{2}\left(\frac{1}{2}\right)^n$$

$$P(Z + Z_1 \neq 0) \leq E(Z) + E(Z_1)$$

$$\leq p^4\left(\frac{5}{8}\right)^n + p^2\left(\frac{1}{2}\right)^n$$

Homework:

Show $\exists$ large family $\mathcal{A}$ : $A_i, A_j, A_k \subseteq \mathcal{A}$

$\Rightarrow \quad A_i \cap A_j \cancel{\subseteq} A_k$.

Person $i$ knows the keys in $A_i$, person $j \neq i$ only knows the set $A_j$

N people

1 2 3 N

$k$ secret keys

Each person is given a subset $A_i$, $i = 1, 2, \ldots N$ of the keys.

Suppose $i$ wants to talk to $j$

$i$ sends the keys in $A_i \cap A_j$

because $A_k \not\supseteq A_i \cap A_j$

$k$ cannot pretend to be $i$

Point is, only need $O(\log N)$ keys each.

# Finding Minimum of $n$ values

input $x_1, x_2, \ldots, x_n$ <u>distinct</u>

min $= \infty$

for $i = 1$ to $n$ do

begin

if $x_i <$ min then min $= x_i$

end

output min

$Z$ = # times happens

on a random order.

$$Z = Z_1 + Z_2 + \cdots + Z_n$$

$$Z_i = \mathbb{1}_{\text{statement is executed on } i\text{th value.}}$$

$$E(Z) = \sum_{i=1}^{n} E(Z_i) = \sum_{i=1}^{n} \frac{1}{i} \approx \log_e n$$

$$E(Z_i) = Pr(Z_i = 1)$$

$$= Pr(X_i \text{ is the smallest of } X_1, X_2, \ldots, X_i)$$

$$= 1/i$$