Algorithms

May 7, 2025

PROBABILISTIC ANALYSIS AND RANDOMIZED ALGORITHMS

Motivation

- Worst case does not usually happen
  - Average case analysis
  - Amortized analysis

- Randomization helps avoid worst-case and attacks by evil users
  - Choosing the pivot in quick-sort at random
- Randomization necessary in cryptography
- Can we get randomness?
  - How to extract randomness (extractors)
  - Longer "random behaving" strings from small seed (pseudorandom generators)

Probabilistic Analysis: The Hiring Problem

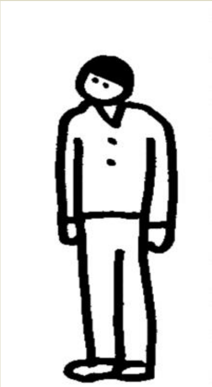
NY Knicks are going to hire one new basketball player

- the taller the better

They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Example:



current best

candidate

Probabilistic Analysis: The Hiring Problem

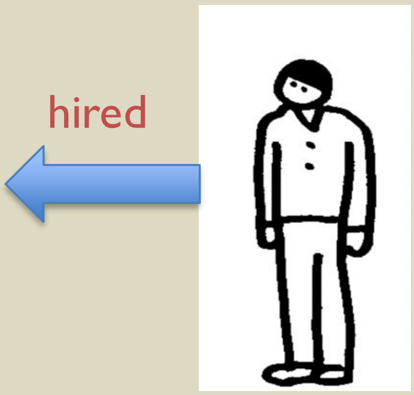
NY Knicks are going to hire one new basketball player

- the taller the better

They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Example:



Probabilistic Analysis: The Hiring Problem

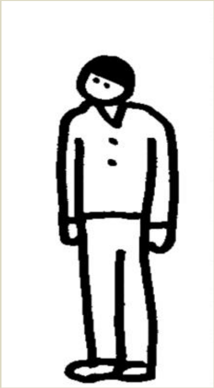
NY Knicks are going to hire one new basketball player

- the taller the better

They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Example:



current best candidate

Probabilistic Analysis: The Hiring Problem

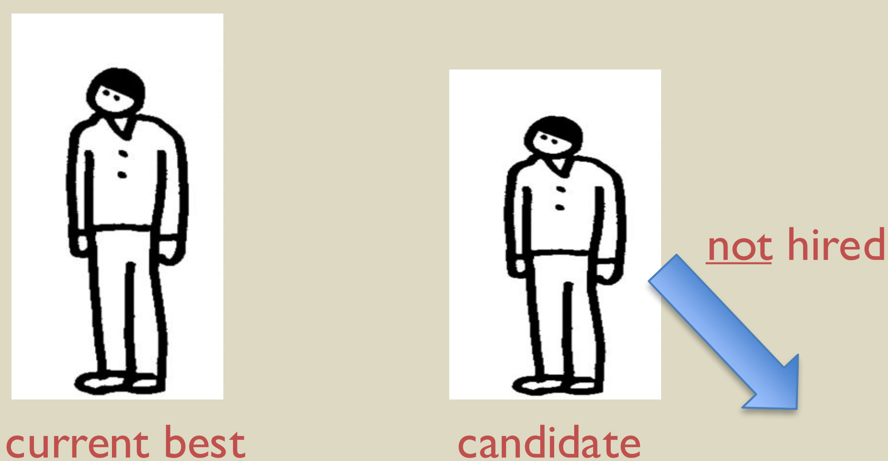
NY Knicks are going to hire one new basketball player

- the taller the better

They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Example:



Probabilistic Analysis: The Hiring Problem

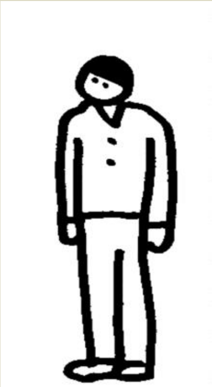
NY Knicks are going to hire one new basketball player

- the taller the better

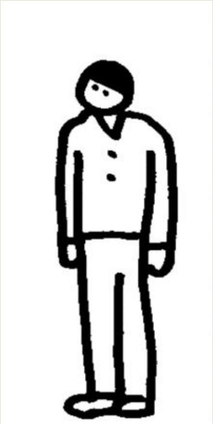
They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Example:



current best



candidate

Probabilistic Analysis: The Hiring Problem

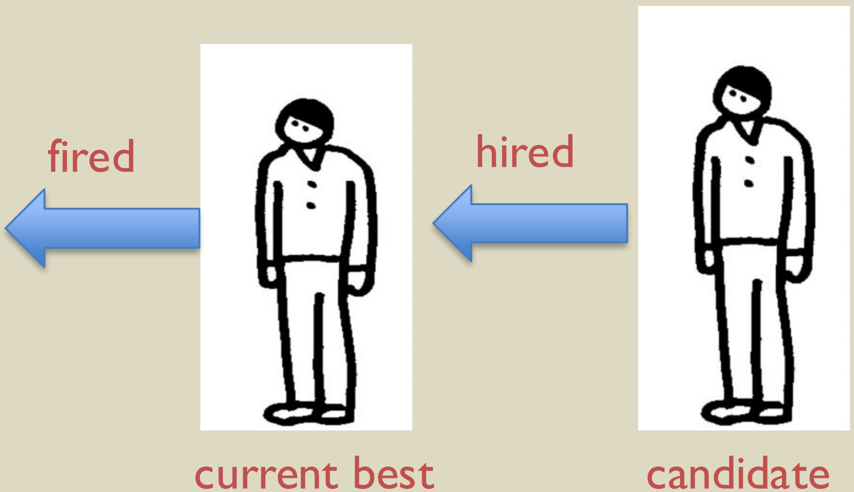
NY Knicks are going to hire one new basketball player

- the taller the better

They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Example:



Probabilistic Analysis: The Hiring Problem

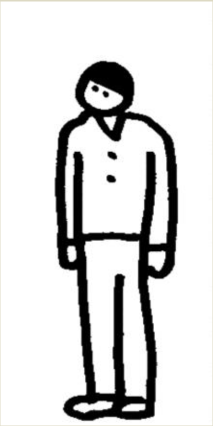
NY Knicks are going to hire one new basketball player

- the taller the better

They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Example:



current best candidate

Probabilistic Analysis: The Hiring Problem

NY Knicks are going to hire one new basketball player

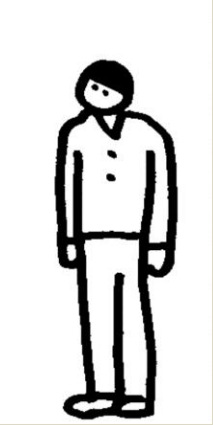
- the taller the better

They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Question: **how many players did we (temporarily) hire?**

Example:



current best

candidate

Probabilistic Analysis: The Hiring Problem

NY Knicks are going to hire one new basketball player

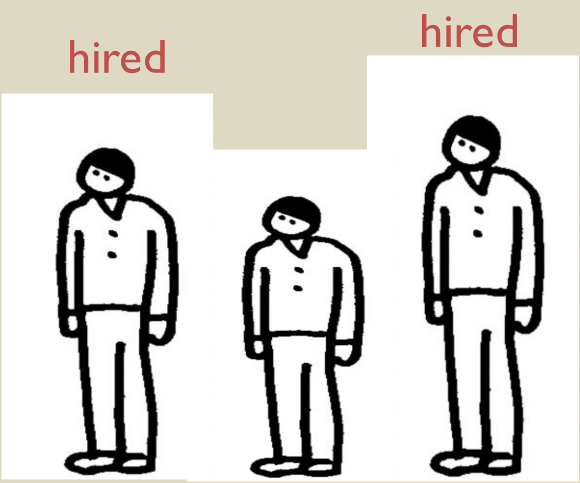
- the taller the better

They have **n** candidates that they call for interview

Strategy: each candidate is hired that is taller than the current best/tallest

Question: **how many players did we (temporarily) hire?**

Example:



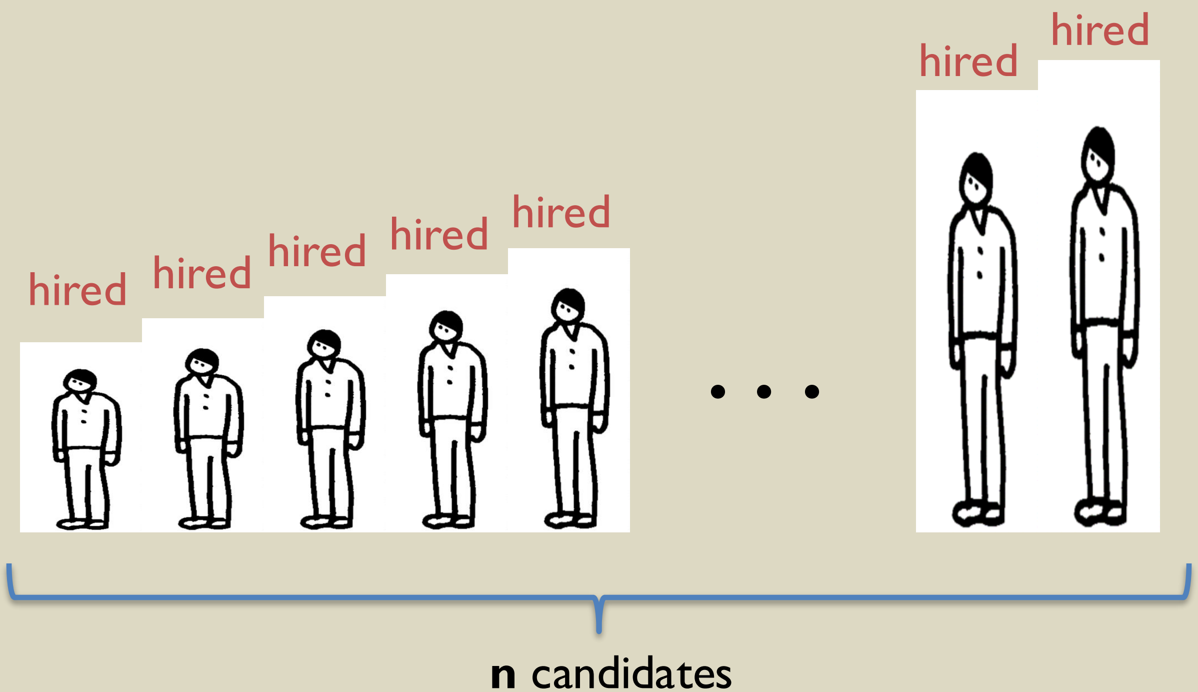
= 2

Worst-case analysis

In the **worst case**: how many players/candidates do we temporarily hire?

Worst-case analysis

In the **worst case**: how many players/candidates do we temporarily hire?



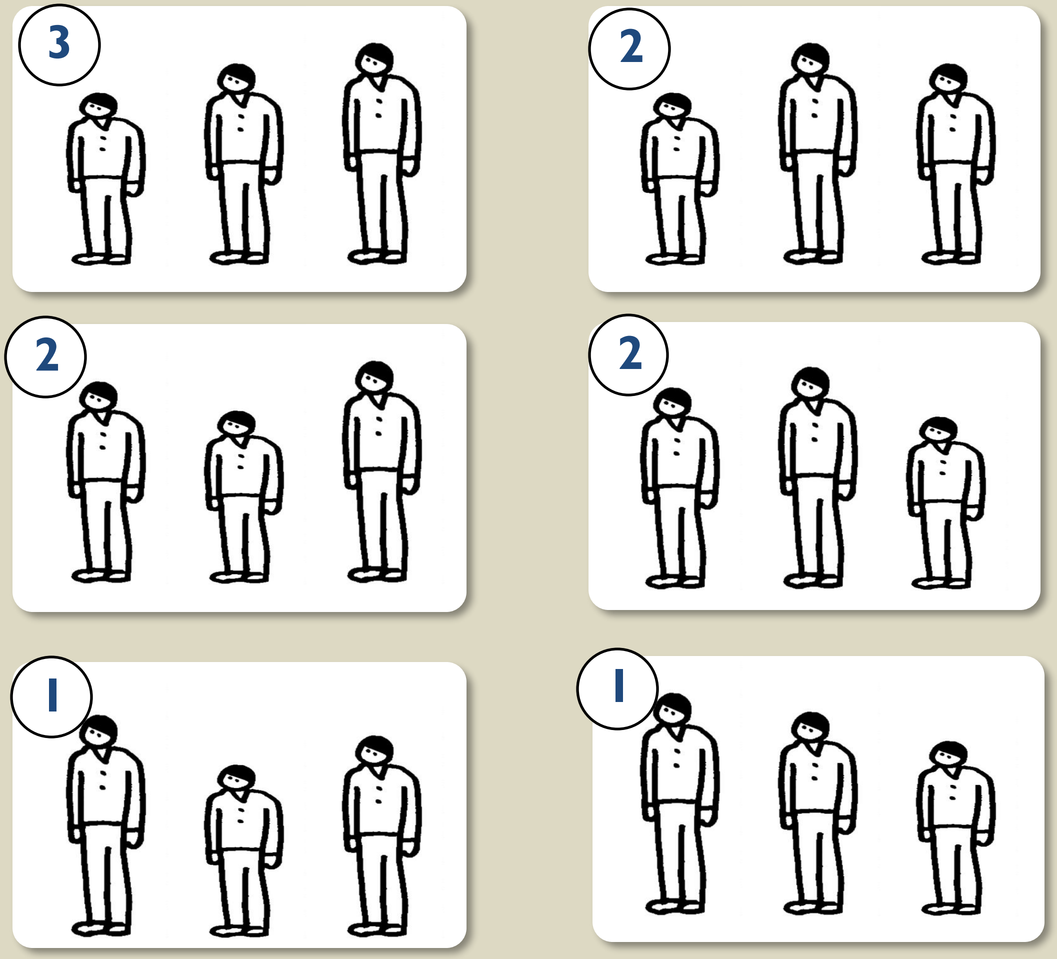
Answer: in the worst case we hire all **n** candidates

Worst-case unlikely to happen

- We only hire all candidates if they arrive in a specific order
- They are likely to arrive in a random order
- More interesting question (probabilistic analysis):

What is the expected number of hires we make over all the permutations of the candidates?

Example



Expected number of hires=

$$\frac{3+2+2+2+1+1}{6}$$

which equals 1+5/6

Calculating the expectation in general 1st trial

- **n!** permutations each equally likely
- Expectation = sum of hires in each permutation divided by **n!**

$$\frac{A_1 + A_2 + \cdots + A_{n!}}{n!}$$

Calculating the expectation in general 1st trial

- **n!** permutations each equally likely
- Expectation = sum of hires in each permutation divided by **n!**

$$\frac{A_1 + A_2 + \cdots + A_{n!}}{n!}$$

- For **n=5** we have **120** terms

Calculating the expectation in general 1st trial

- **n!** permutations each equally likely
- Expectation = sum of hires in each permutation divided by **n!**

$$\frac{A_1 + A_2 + \cdots + A_{n!}}{n!}$$

- For **n=5** we have **120** terms
- For **n=10** we have **3 628 800** terms

Calculating the expectation in general 1st trial

- **n!** permutations each equally likely
- Expectation = sum of hires in each permutation divided by **n!**

$$\frac{A_1 + A_2 + \cdots + A_{n!}}{n!}$$

- For **n=5** we have **120** terms
- For **n=10** we have **3 628 800** terms

NEED A MORE CLEVER METHOD

Indicator Random Variables

- Simple yet powerful technique for computing the expected value
- In particular, in situations in which there may be dependence

Indicator Random Variables

- Simple yet powerful technique for computing the expected value
- In particular, in situations in which there may be dependence

DEFINITION: Given a sample space and an event **A**, we define the **indicator random variable**

$$I\{A\} = \begin{cases} 1 & \text{if } A \text{ occurs,} \\ 0 & \text{if } A \text{ does not occur} \end{cases}$$

Indicator Random Variables

DEFINITION: Given a sample space and an event **A**, we define the **indicator random variable**

$$I\{A\} = \begin{cases} 1 & \text{if } A \text{ occurs,} \\ 0 & \text{if } A \text{ does not occur} \end{cases}$$

Indicator Random Variables

DEFINITION: Given a sample space and an event **A**, we define the **indicator random variable**

$$I\{A\} = \begin{cases} 1 & \text{if } A \text{ occurs,} \\ 0 & \text{if } A \text{ does not occur} \end{cases}$$

LEMMA: For an event **A**, let $\mathbf{X_A = I\{A\}}$. Then $\mathbf{E[X_A] = Pr[A]}$

Indicator Random Variables

DEFINITION: Given a sample space and an event **A**, we define the **indicator random variable**

$$I\{A\} = \begin{cases} 1 & \text{if } A \text{ occurs,} \\ 0 & \text{if } A \text{ does not occur} \end{cases}$$

LEMMA: For an event **A**, let $\mathbf{X_A = I\{A\}}$. Then $\mathbf{E[X_A] = Pr[A]}$

PROOF: $\mathbf{E[X_A] = 1 * Pr\{A\} + 0 * Pr\{\overline{A}\} = Pr\{A\}}$

Simple Example: Coin Flip

Determine the expected number of heads when we flip a coin one time

Simple Example: Coin Flip

Determine the expected number of heads when we flip a coin one time

- Sample space is **{H,T}**
- **Pr{H} = Pr{T} = ½**

Simple Example: Coin Flip

Determine the expected number of heads when we flip a coin one time

- Sample space is **{H,T}**
- **Pr{H} = Pr{T} = ½**

- Define indicator variable $\mathbf{X_H = I\{H\}}$

Simple Example: Coin Flip

Determine the expected number of heads when we flip a coin one time

- Sample space is **{H,T}**
- **Pr{H} = Pr{T} = ½**

- Define indicator variable $\mathbf{X_H = I\{H\}}$
    - $\mathbf{X_H}$ counts the number of heads in one flip

Simple Example: Coin Flip

Determine the expected number of heads when we flip a coin one time

- Sample space is **{H,T}**
- **Pr{H} = Pr{T} = ½**

- Define indicator variable $\mathbf{X_H = I\{H\}}$
  - $\mathbf{X_H}$ counts the number of heads in one flip

- Since **Pr{H} = 1/2**, previous lemma says that $\mathbf{E[X_H] = 1/2}$

Slightly More Complex: **n** Coin Flips

Determine the expected number of heads when we flip n coins

- Let **X** be a random variable for the number of heads in **n** flips

Slightly More Complex: **n** Coin Flips

Determine the expected number of heads when we flip n coins

- Let **X** be a random variable for the number of heads in **n** flips

- Could calculate

$$E[X] = \sum_{k=0}^{n} k \cdot \Pr\{X = k\}$$

- … but cumbersome

- Instead use indicator variables

Slightly More Complex: **n** Coin Flips

Determine the expected number of heads when we flip n coins

- Let **X** be a random variable for the number of heads in **n** flips

- For **i = 1, …, n**, define $\mathbf{X_i}$ **= I{the i'th flip results in event H}**

Slightly More Complex: **n** Coin Flips

Determine the expected number of heads when we flip n coins

- Let **X** be a random variable for the number of heads in **n** flips

- For **i = 1, …, n**, define $\mathbf{X_i}$ **= I{the i'th flip results in event H}**
  - Then $\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n]}$

Slightly More Complex: **n** Coin Flips

Determine the expected number of heads when we flip n coins

- Let **X** be a random variable for the number of heads in **n** flips

- For **i = 1, …, n**, define $\mathbf{X_i}$ **= I{the i'th flip results in event H}**
  - Then $\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n]}$

- By linearity of expectation i.e., that **E[aX + bY] = aE[X] + bE[Y]**

  holds even if ***X*** *and* ***Y*** *are dependent*

Slightly More Complex: **n** Coin Flips

Determine the expected number of heads when we flip n coins

- Let **X** be a random variable for the number of heads in **n** flips

- For **i = 1, …, n**, define $\mathbf{X_i}$ **= I{the i'th flip results in event H}**
  - Then $\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n]}$

- By linearity of expectation i.e., that $\mathbf{E[aX + bY] = aE[X] + bE[Y]}$

  *holds even if **X** and **Y** are dependent*

$$\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n] = E[X_1] + E[X_2] + \ldots + E[X_n]}$$

Slightly More Complex: **n** Coin Flips

Determine the expected number of heads when we flip n coins

- Let **X** be a random variable for the number of heads in **n** flips

- For **i = 1, …, n**, define $\mathbf{X_i}$ **= I{the i'th flip results in event H}**
  - Then $\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n]}$

- By linearity of expectation i.e., that $\mathbf{E[aX + bY] = aE[X] + bE[Y]}$

  holds even if ***X*** *and* ***Y*** *are dependent*

$$\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n] = E[X_1] + E[X_2] + \ldots + E[X_n]}$$

By Lemma equals Pr{H} = 1/2

Slightly More Complex: **n** Coin Flips

Determine the expected number of heads when we flip n coins

- Let $\mathbf{X}$ be a random variable for the number of heads in $\mathbf{n}$ flips

- For $\mathbf{i = 1, \ldots, n}$, define $\mathbf{X_i = I\{\text{the i'th flip results in event H}\}}$
  - Then $\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n]}$

- By linearity of expectation i.e., that $\mathbf{E[aX + bY] = aE[X] + bE[Y]}$

  *holds even if **X** and **Y** are dependent*

$$E[X] = E[X_1 + X_2 + \ldots + X_n] = \underbrace{E[X_1]}_{\text{By Lemma equals } Pr\{H\} = 1/2} + E[X_2] + \ldots + E[X_n]$$

By Lemma equals Pr{H} = 1/2

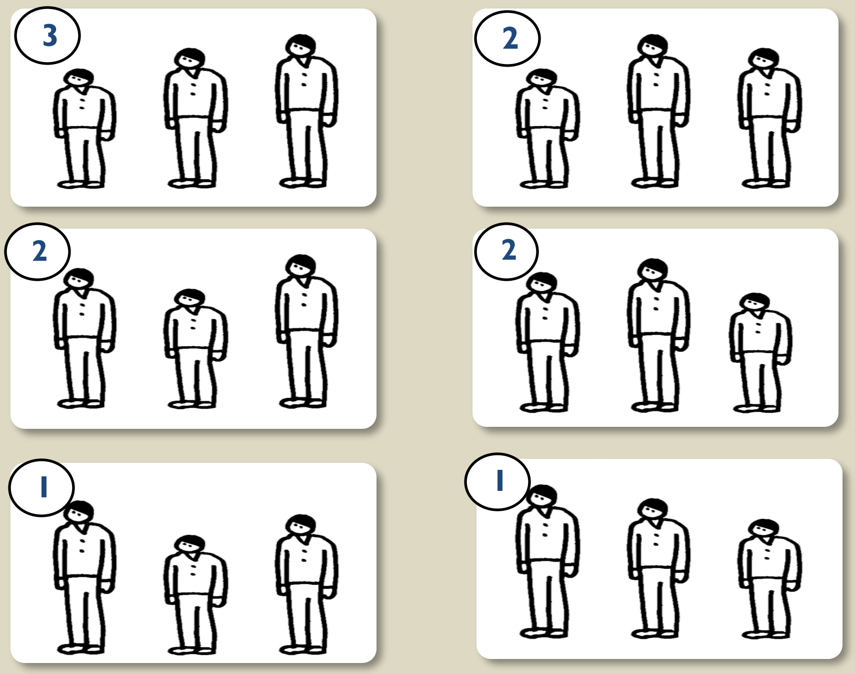
$$= n/2$$

Probabilistic Analysis of Hiring Problem

- Candidates arrive in random order
- Let **X** be a random variable that equals the number of time we hire a player

Probabilistic Analysis of Hiring Problem

- Candidates arrive in random order
- Let **X** be a random variable that equals the number of times we hire a player



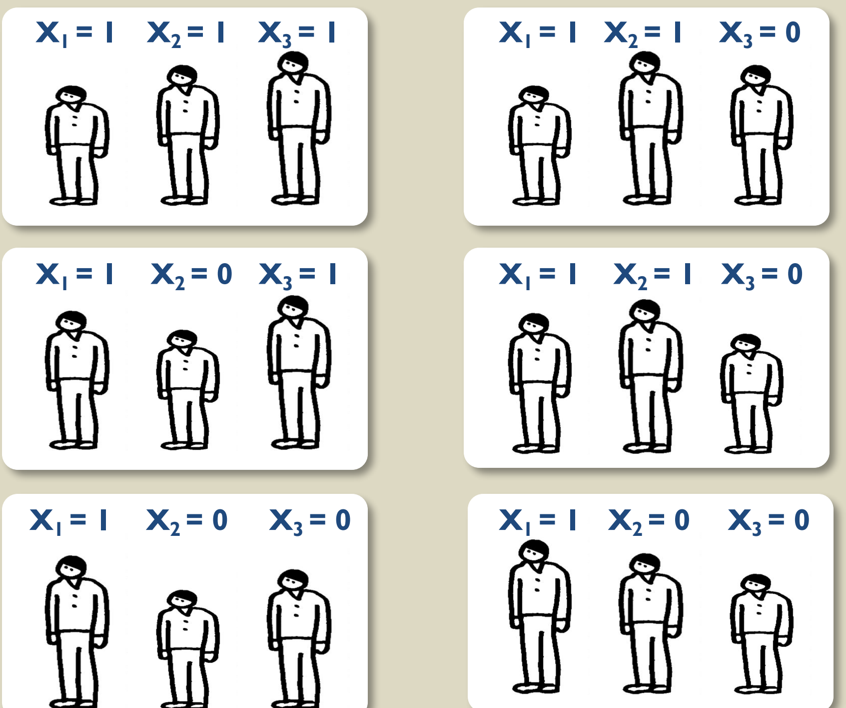
$$\mathbf{E[X]} = \frac{3+2+2+2+1+1}{6}$$

which equals 1+5/6

Probabilistic Analysis of Hiring Problem

- Candidates arrive in random order
- Let **X** be a random variable that equals the number of time we hire a player
- Define indicator variables $\mathbf{X_1, X_2, \ldots, X_n}$ where

$$\mathbf{X_i = I\{\text{candidate } i \text{ is hired}\}}$$



$$\mathbf{E[X] = E[X_1+X_2+X_3]}$$

$$\mathbf{= E[X_1] + E[X_2] + E[X_3]}$$

$$\mathbf{= 1 + 1/2 + 1/3 = 1 + 5/6}$$

Probabilistic Analysis of Hiring Problem

- Candidates arrive in random order
- Let **X** be a random variable that equals the number of time we hire a player
- Define indicator variables $\mathbf{X_1, X_2, \ldots, X_n}$ where

  $\mathbf{X_i = I\{candidate\ i\ is\ hired\}}$
- Note that $\mathbf{X = X_1 + X_2 + \ldots + X_n}$ and $\mathbf{E[X_i] = Pr}\{$candidate $\mathbf{i}$ is hired$\}$

Probabilistic Analysis of Hiring Problem

- Candidates arrive in random order
- Let **X** be a random variable that equals the number of time we hire a player
- Define indicator variables $\mathbf{X_1, X_2, \ldots, X_n}$ where

  $\mathbf{X_i}$ **= I{candidate i is hired}**

- Note that $\mathbf{X = X_1 + X_2 + \ldots + X_n}$ and $\mathbf{E[X_i] = Pr}$**{**candidate **i** is hired**}**

- By linearity of expectation,

  $$\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n] = E[X_1] + E[X_2] + \ldots + E[X_n]}$$

Probabilistic Analysis of Hiring Problem

- Candidates arrive in random order
- Let **X** be a random variable that equals the number of time we hire a player
- Define indicator variables $\mathbf{X_1, X_2, \ldots, X_n}$ where

  $\mathbf{X_i = I\{candidate\ i\ is\ hired\}}$

- Note that $\mathbf{X = X_1 + X_2 + \ldots + X_n}$ and $\mathbf{E[X_i] = Pr}$**{**candidate **i** is hired**}**

- By linearity of expectation,

  $$\mathbf{E[X] = E[X_1 + X_2 + \ldots + X_n] = E[X_1] + E[X_2] + \ldots + E[X_n]}$$

which equals

Pr{candidate **1** is hired**}** + **Pr{**candidate **2** is hired**}** + … + **Pr{**candidate **n** is hired**}**

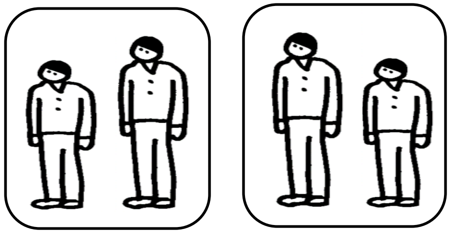
Probability of Hiring i'th Candidate

Pr{candidate **1** is hired**} = 1**

Probability of Hiring i'th Candidate

Pr{candidate **1** is hired} **= 1**

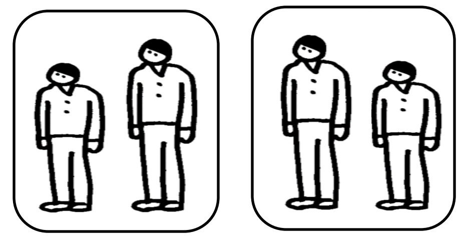
Pr{candidate **2** is hired} **= 1/2**



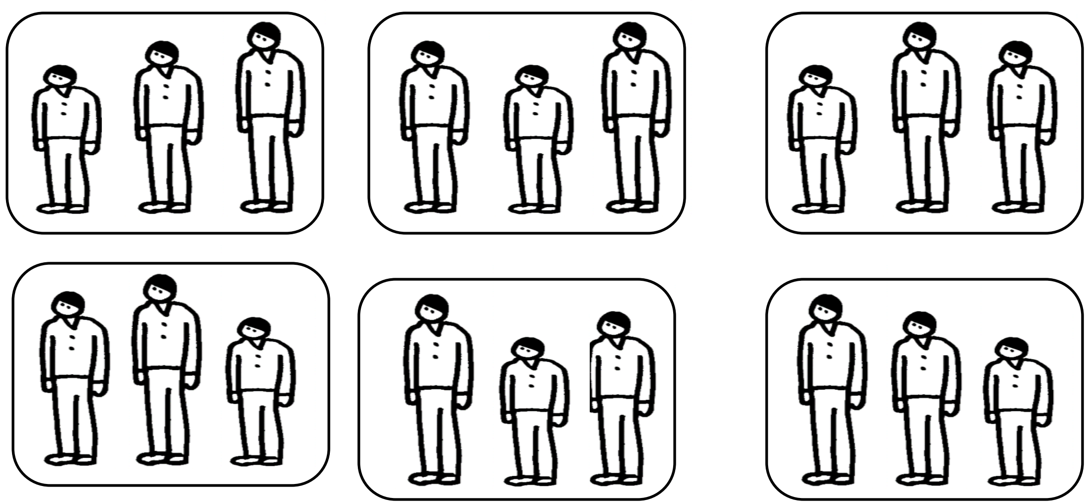
Probability of Hiring i'th Candidate

Pr{candidate **1** is hired**} = 1**

Pr{candidate **2** is hired**} = 1/2**



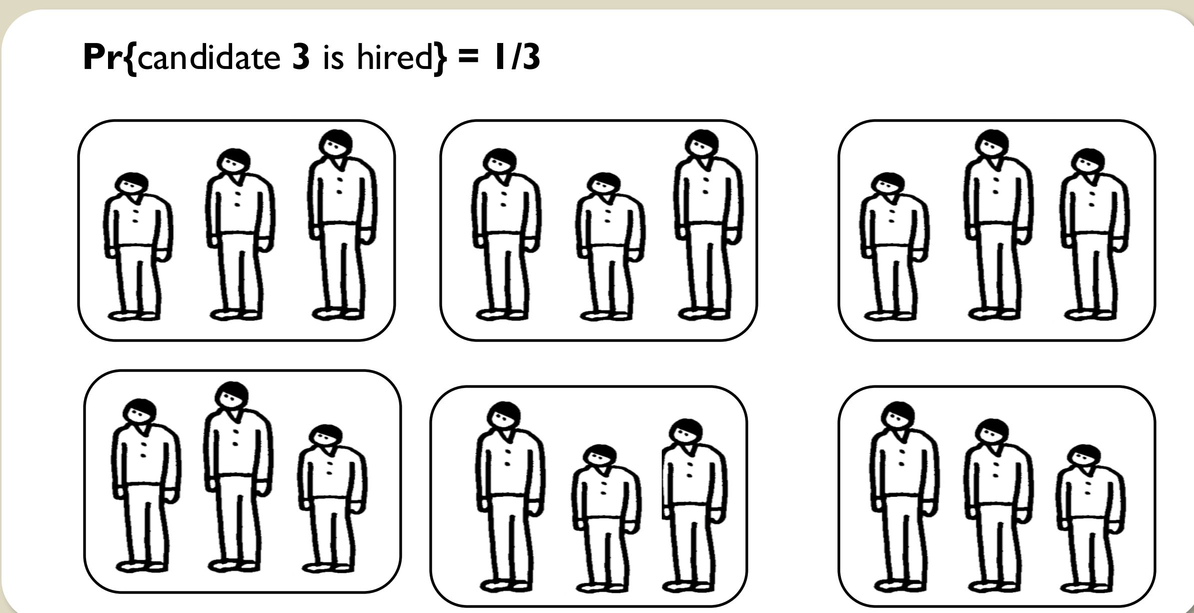
Pr{candidate **3** is hired**} = 1/3**



Probability of Hiring i'th Candidate

- i'th candidate hired iff he is tallest among the first i candidates
- Since they arrive in random order, any one of these first i candidates are equally likely to be the tallest =>

Pr{candidate **i** is hired**} = 1/i**



Expected Number of Hires

Recall that **E[number of hires] = E[X] =**

Pr{candidate **1** is hired**} + Pr{**candidate **2** is hired**} + … + Pr{**candidate **n** is hired**}**

Expected Number of Hires

Recall that **E[number of hires] = E[X] =**

Pr{candidate **1** is hired**} + Pr{**candidate **2** is hired**} + … + Pr{**candidate **n** is hired**}**

which equals

1/1 + 1/2 + 1/3 + 1/4 + 1/5 + … + 1/n

Expected Number of Hires

Recall that **E[number of hires] = E[X] =**

Pr{candidate **1** is hired**} + Pr{**candidate **2** is hired**} + … + Pr{**candidate **n** is hired**}**

which equals

1/1 + 1/2 + 1/3 + 1/4 + 1/5 + … + 1/n = $\mathbf{H_n}$

n:th harmonic number

Expected Number of Hires

Recall that **E[number of hires] = E[X] =**

Pr{candidate **1** is hired**} + Pr{**candidate **2** is hired**} + … + Pr{**candidate **n** is hired**}**

which equals

1/1 + 1/2 + 1/3 + 1/4 + 1/5 + … + 1/n = H_n **= ln n + O(1)**

n:th harmonic number

Expected Number of Hires

Recall that **E[number of hires] = E[X] =**

Pr{candidate **1** is hired**} + Pr{**candidate **2** is hired**} + … + Pr{**candidate **n** is hired**}**

which equals

1/1 + 1/2 + 1/3 + 1/4 + 1/5 + … + 1/n = H_n **= ln n + O(1)**

n:th harmonic number

Examples:

- Expected number of hires for **n=6** is **2.45**
- Expected number of hires for **n=100** is **5.1874**
- Expected number of hires for **n=10000** is **9.7876**

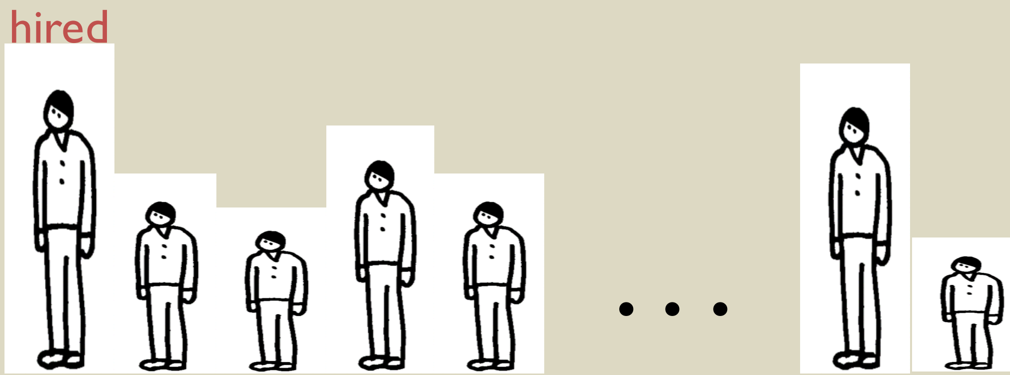
Questions

- What is the probability that we hire only one candidate?

- What is the probability that we hire **n** candidates?

Questions

- What is the probability that we hire only one candidate? **1/n** (tallest first)



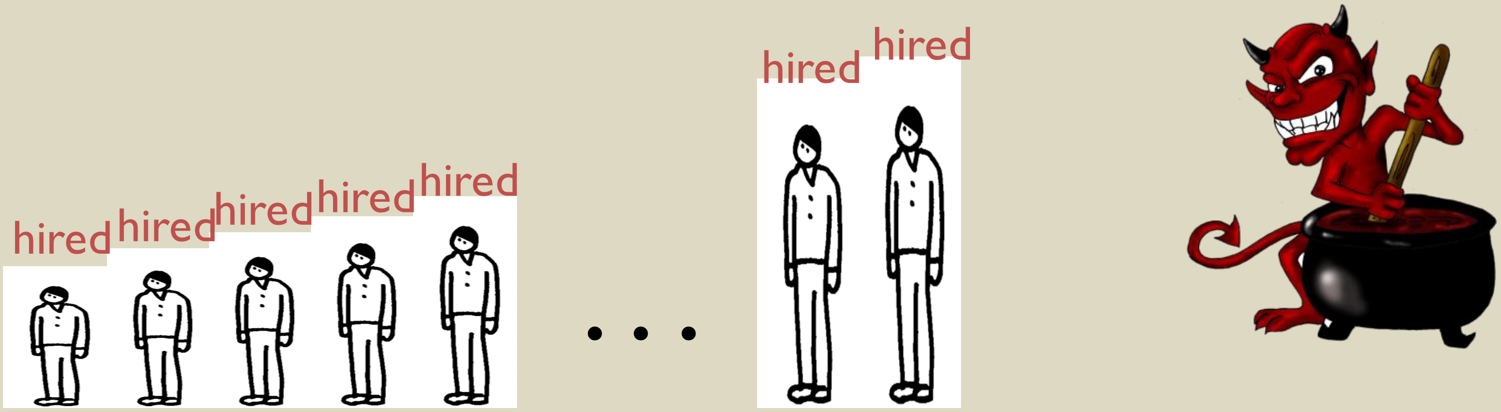
- What is the probability that we hire **n** candidates? **1/n!** (worst case order)

Randomized Algorithm

- Instead of assuming that the candidates arrive in random order
- **We/the algorithm** pick a random order and call the candidates in this order

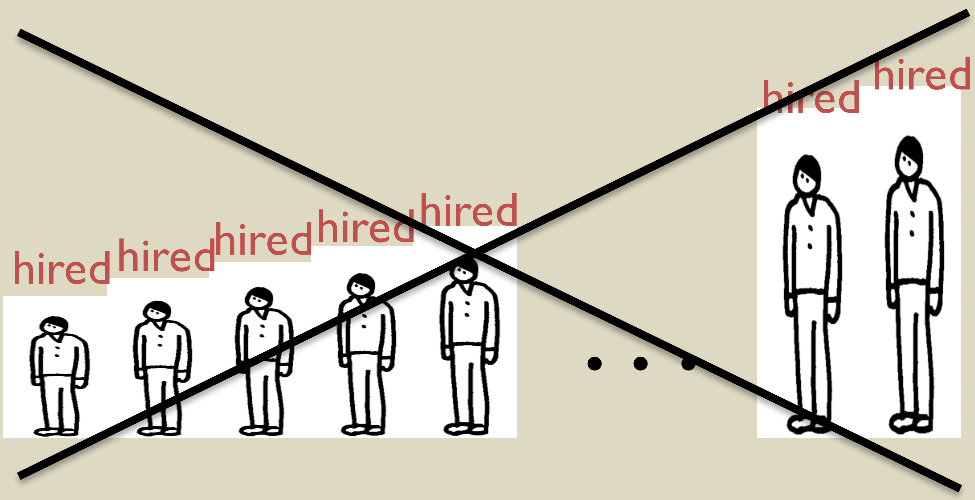
Randomized Algorithm

- Instead of assuming that the candidates arrive in random order
- **We/the algorithm** pick a random order and call the candidates in this order



Randomized Algorithm

- Instead of assuming that the candidates arrive in random order
- **We/the algorithm** pick a random order and call the candidates in this order
- **In this way we can foul malicious users**



Question

- Given a function **RANDOM** that returns **1** with probability **p** and **0** with probability **1-p**

- How to use **RANDOM** for generating an unbiased bit?

Question

- Given a function **RANDOM** that returns **1** with probability **p** and **0** with probability **1-p**

- How to use **RANDOM** for generating an unbiased bit?

- Pick a pair (a,b) of random numbers: a = **RANDOM** and b = **RANDOM**
  - If $a \neq b$ return a
  - Otherwise pick a new pair