Do you feel lucky?

CS1212 Introduction to Theoretical Computer Science
Lecture 9-11

Kuan Yang

水源社区

一种图鉴抽卡类游戏的概率问题

水源广场　谈笑风生

R我所愿　10 月 16 日

刚才摸鱼摸到把池塘里的鱼都摸光了，给自己找了条大鱼摸：

最近在玩一种抽卡补充图鉴类的游戏，图鉴上一共16张卡，每次等概率抽到1张，我现在13次抽到了9种，问我是欧还是非？也就是算16张卡抽13次出的种数期望。

3　回复

水源社区

一种图鉴抽卡类游戏的概率问题

水源广场 谈笑风生

R我所愿 10 月 16 日

刚才摸鱼摸到把池塘里的鱼都摸光了，给自己找了条大鱼摸：

最近在玩一种抽卡补充图鉴类的游戏，图鉴上一共16张卡，每次等概率抽到1张，我现在13次抽到了9种，问我是欧还是非？也就是算16张卡抽13次出的种数期望。

3 回复

Do you feel lucky?

水源社区

一种图鉴抽卡类游戏的概率问题

水源广场 谈笑风生

R我所愿 10 月 16 日

刚才摸鱼摸到把池塘里的鱼都摸光了，给自己找了条大鱼摸：

最近在玩一种抽卡补充图鉴类的游戏，图鉴上一共16张卡，每次等概率抽到1张，我现在13次抽到了9种，问我是欧还是非？也就是算16张卡抽13次出的种数期望。

3 回复

Do you feel lucky?

An introduction to probability and randomized algorithms

Polynomial identity

Polynomial identity

- Given 2 univariate polynomials $f(x), g(x) : \mathbb{R} \rightarrow \mathbb{R}$

Polynomial identity

- Given 2 univariate polynomials $f(x), g(x) : \mathbb{R} \to \mathbb{R}$
- Assume $f(x) = \sum_{n=0}^{d} a_n \cdot x^n$ and $g(x) = b_0 \cdot \prod_{n=1}^{d} (x - b_n)$

Polynomial identity

- Given 2 univariate polynomials $f(x), g(x) : \mathbb{R} \to \mathbb{R}$
- Assume $f(x) = \sum_{n=0}^{d} a_n \cdot x^n$ and $g(x) = b_0 \cdot \prod_{n=1}^{d} (x - b_n)$
- Determine whether $f(x) \equiv g(x)$

Polynomial identity

- Given 2 univariate polynomials $f(x), g(x) : \mathbb{R} \to \mathbb{R}$
- Assume $f(x) = \sum_{n=0}^{d} a_n \cdot x^n$ and $g(x) = b_0 \cdot \prod_{n=1}^{d} (x - b_n)$
- Determine whether $f(x) \equiv g(x)$
- Expand $g(x)$ then compare all coefficients

Polynomial identity

- Given 2 univariate polynomials $f(x), g(x) : \mathbb{R} \to \mathbb{R}$
- Assume $f(x) = \sum_{n=0}^{d} a_n \cdot x^n$ and $g(x) = b_0 \cdot \prod_{n=1}^{d} (x - b_n)$
- Determine whether $f(x) \equiv g(x)$

- Expand $g(x)$ then compare all coefficients
- $O(d^2)$ multiplication or $O(d \log d)$ with Fourier transform

Polynomial identity

Polynomial identity

- More clever?

Polynomial identity

- More clever?
- Select $c_0, c_1, \ldots, c_d$ then check if $f(c_i) = g(c_i)$

Polynomial identity

- More clever?
- Select $c_0, c_1, \ldots, c_d$ then check if $f(c_i) = g(c_i)$
- Fundamental theorem of algebra: $f(x) - g(x)$ has $\leq d$ roots

Polynomial identity

- More clever?
- Select $c_0, c_1, \ldots, c_d$ then check if $f(c_i) = g(c_i)$
- Fundamental theorem of algebra: $f(x) - g(x)$ has $\leq d$ roots
- Still need $O(d^2)$ times multiplication

Polynomial identity

- More clever?
- Select $c_0, c_1, \ldots, c_d$ then check if $f(c_i) = g(c_i)$
- Fundamental theorem of algebra: $f(x) - g(x)$ has $\leq d$ roots
- Still need $O(d^2)$ times multiplication
- However if we allow errors with low probabilities... say 0.01

Polynomial identity

- More clever?
- Select $c_0, c_1, \ldots, c_d$ then check if $f(c_i) = g(c_i)$
- Fundamental theorem of algebra: $f(x) - g(x)$ has $\leq d$ roots
- Still need $O(d^2)$ times multiplication
- However if we allow errors with low probabilities... say 0.01
- Choose S of size $100d$ then select $c \in S$ uniformly at random

Polynomial identity

Polynomial identity

- Suppose $f(x) \not\equiv g(x)$, no matter what $f(x), g(x)$ are

Polynomial identity

- Suppose $f(x) \not\equiv g(x)$, no matter what $f(x), g(x)$ are
- At most d numbers $c_1, c_2, \ldots, c_d$ in S satisfy $f(c_i) = g(c_i)$

Polynomial identity

- Suppose $f(x) \not\equiv g(x)$, no matter what $f(x), g(x)$ are
- At most d numbers $c_1, c_2, \ldots, c_d$ in S satisfy $f(c_i) = g(c_i)$
- Select $c \in S$ uniformly, then $\Pr[f(c) = g(c)] \leq d/|S| = 1/100$

Polynomial identity

- Suppose $f(x) \not\equiv g(x)$, no matter what $f(x), g(x)$ are
- At most d numbers $c_1, c_2, \ldots, c_d$ in S satisfy $f(c_i) = g(c_i)$
- Select $c \in S$ uniformly, then $\Pr[f(c) = g(c)] \leq d/|S| = 1/100$
- How about lower mistake probability?

Polynomial identity

- Suppose $f(x) \not\equiv g(x)$, no matter what $f(x), g(x)$ are
- At most d numbers $c_1, c_2, \ldots, c_d$ in S satisfy $f(c_i) = g(c_i)$
- Select $c \in S$ uniformly, then $\Pr[f(c) = g(c)] \leq d/|S| = 1/100$
- How about lower mistake probability?
- Select $c_1, c_2 \in S$ independently, then $\Pr[\forall\, i, f(c_i) = g(c_i)] \leq 1/100^2$

Polynomial identity

- Suppose $f(x) \not\equiv g(x)$, no matter what $f(x), g(x)$ are
- At most d numbers $c_1, c_2, \ldots, c_d$ in S satisfy $f(c_i) = g(c_i)$
- Select $c \in S$ uniformly, then $\Pr[f(c) = g(c)] \leq d/|S| = 1/100$
- How about lower mistake probability?
- Select $c_1, c_2 \in S$ independently, then $\Pr[\forall i, f(c_i) = g(c_i)] \leq 1/100^2$
- $O(d \log(1/\varepsilon))$ times multiplication if allow mistake probability ε

What is probability?

What is probability?

- Why do we use a large set S ?

What is probability?

- Why do we use a large set S ?
- What are we talking about when we say "probability" ?

What is probability?

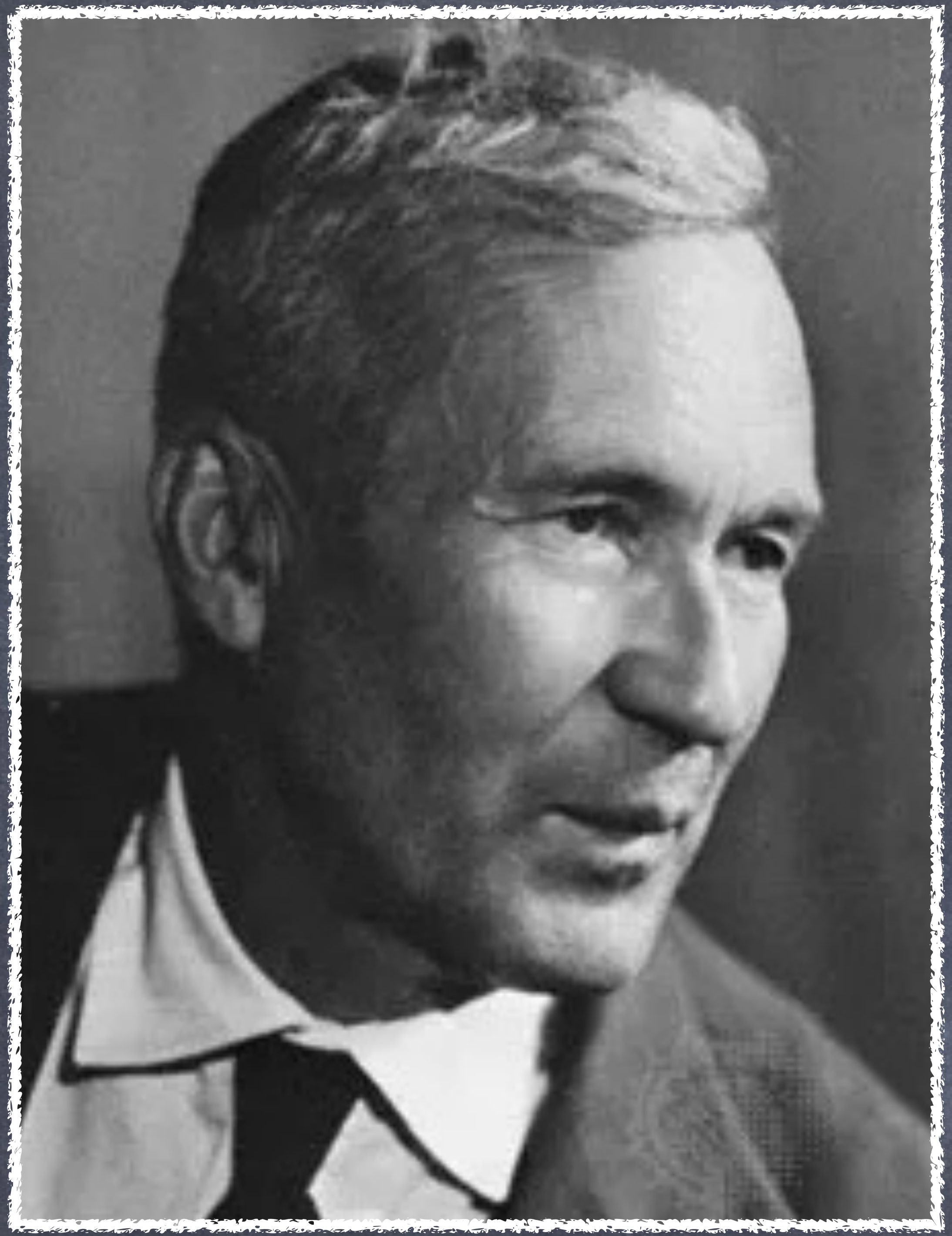
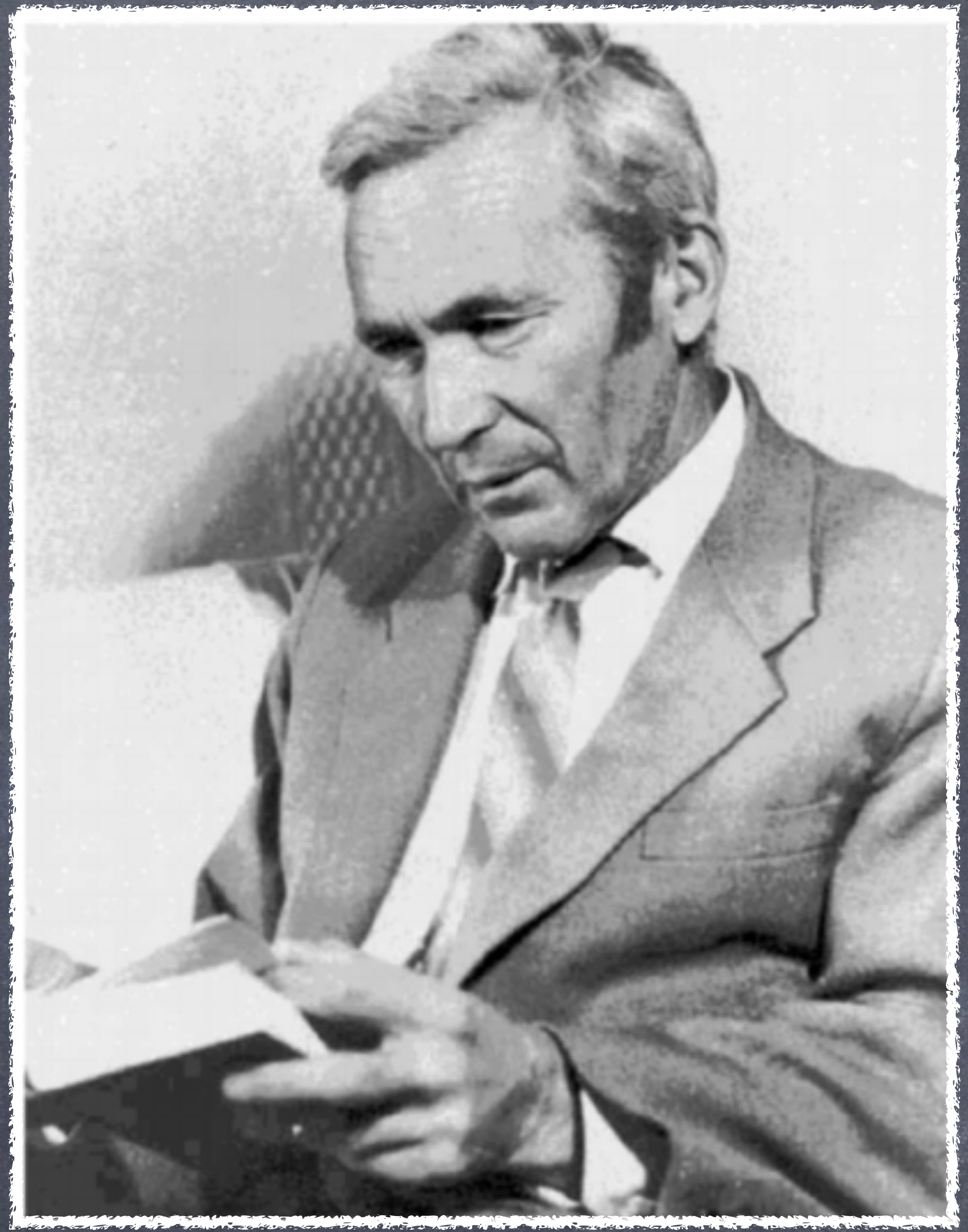
- Why do we use a large set S ?
- What are we talking about when we say "probability" ?
- Throw a dice, $\Pr[6 \text{ appearing}] = 1/2$ due to 2 outcomes ?

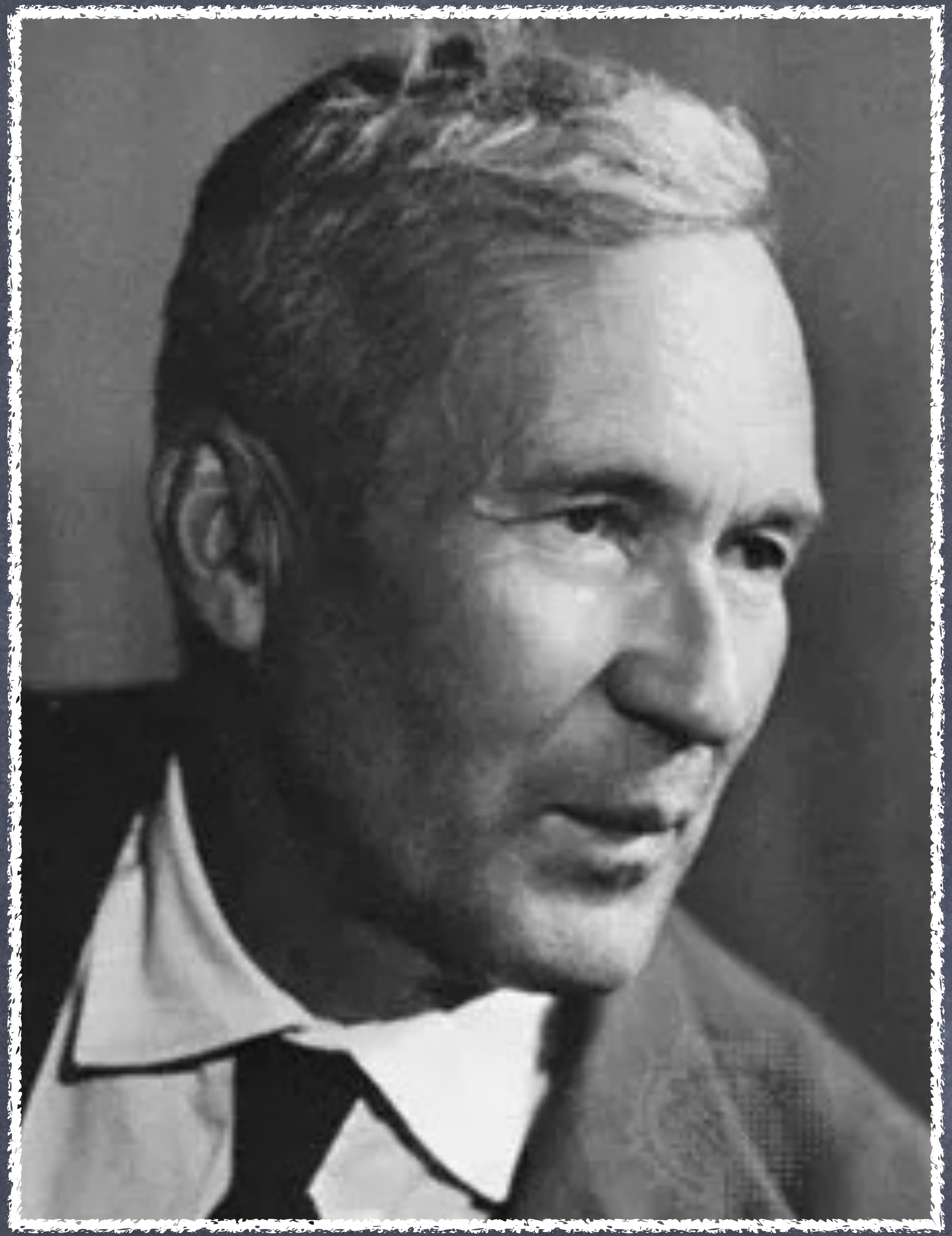
What is probability?

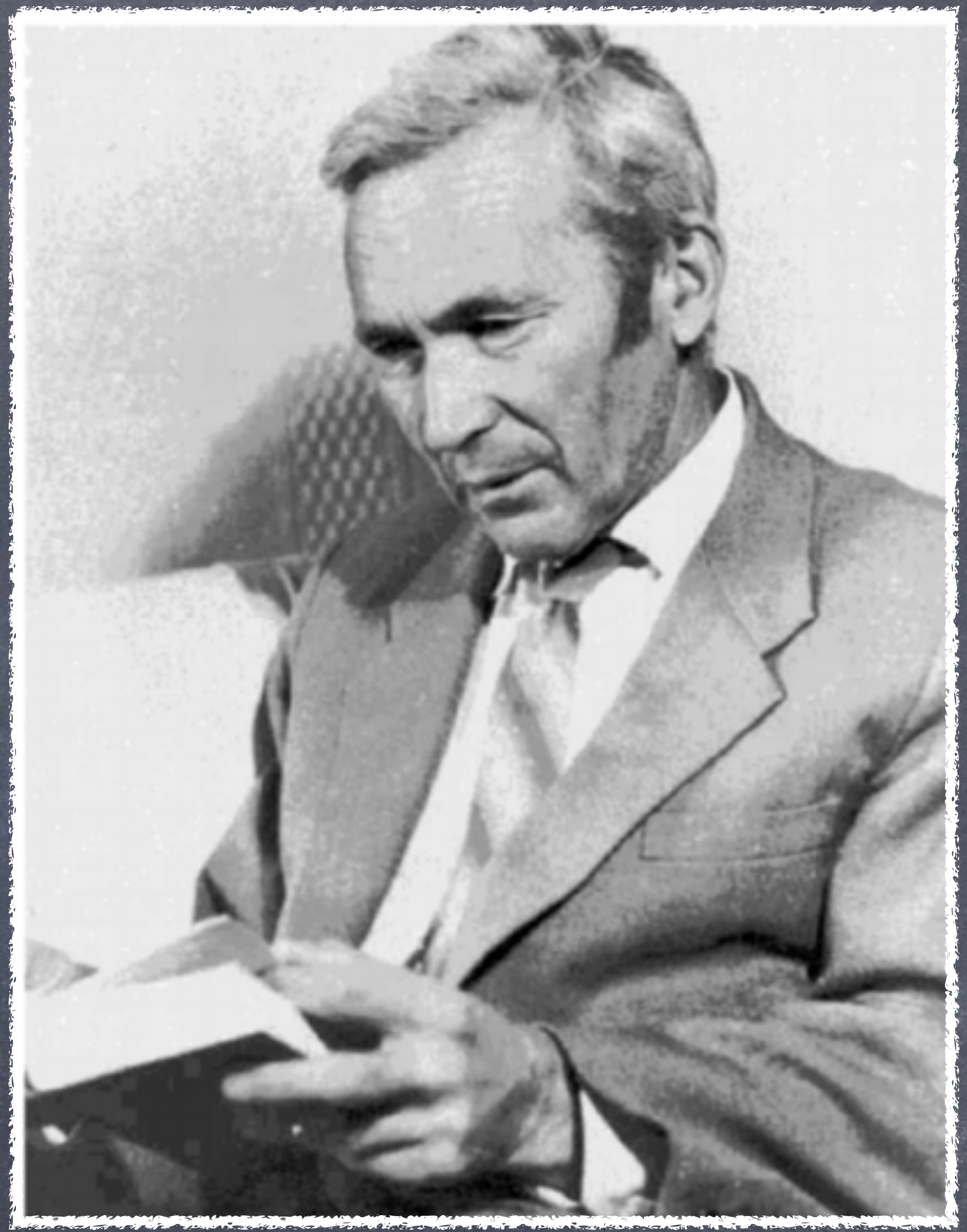
- Why do we use a large set S ?
- What are we talking about when we say "probability" ?
- Throw a dice, $\Pr[6$ appearing$] = 1/2$ due to 2 outcomes ?
- Pick an integer uniformly at random...... ?

What is probability?

- Why do we use a large set S ?
- What are we talking about when we say "probability" ?
- Throw a dice, $\Pr[6 \text{ appearing}] = 1/2$ due to 2 outcomes ?
- Pick an integer uniformly at random...... ?
- There are two boxes having x and $\lfloor x/2 \rfloor$ coins respectively. Open a box and find 100 coins. $\mathbb{E}[\text{coins in another}] = 125$?





Andrey Nikolaevich Kolmogorov

(1903.4.25 – 1987.10.20)

What is probability?

What is probability?

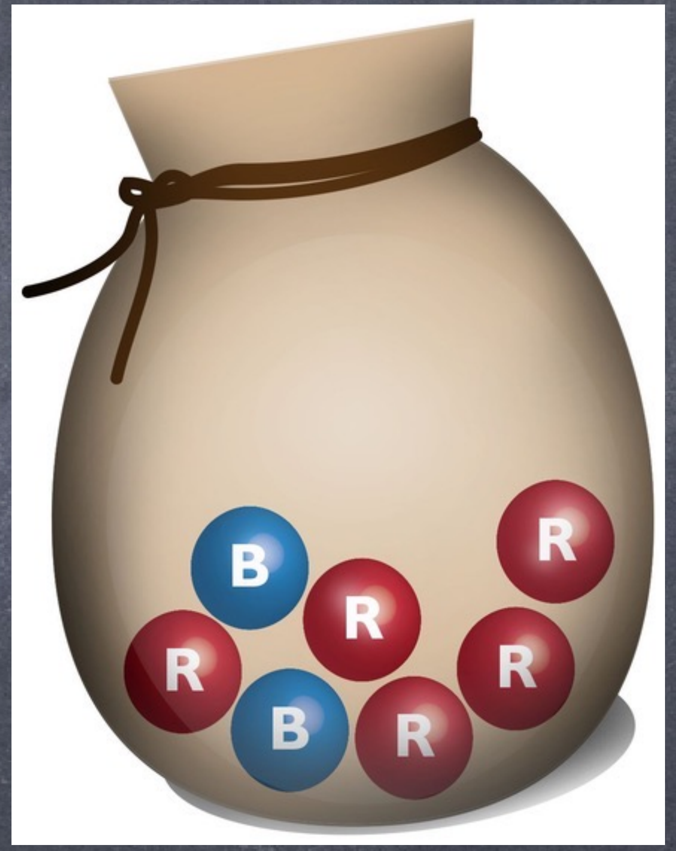
- We only consider discrete / finite models

What is probability?

- We only consider discrete / finite models
- Probability is counting...

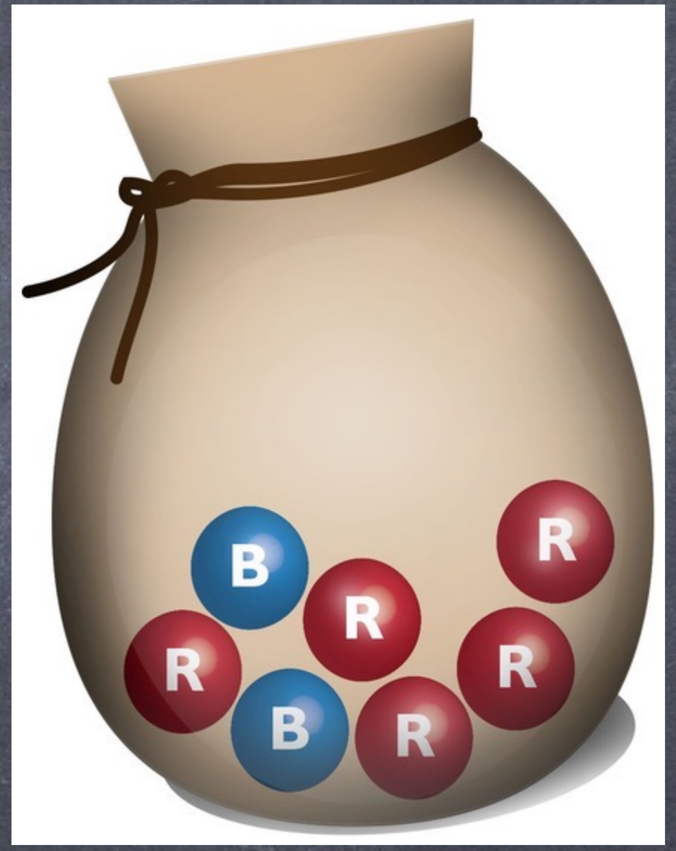
What is probability?

- We only consider discrete / finite models
- Probability is counting...



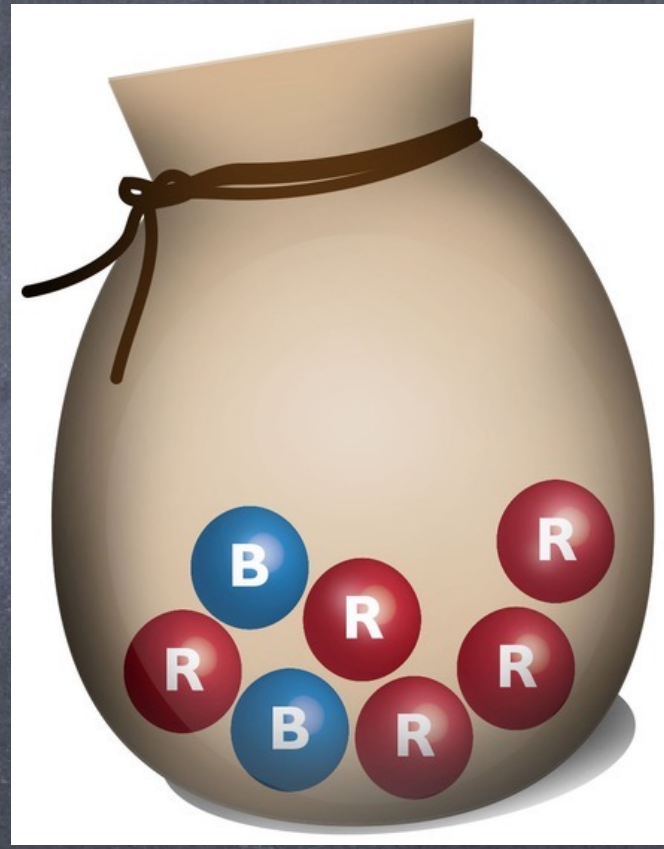
What is probability?

- We only consider discrete / finite models
- Probability is counting...
- Each event is a set of outcomes



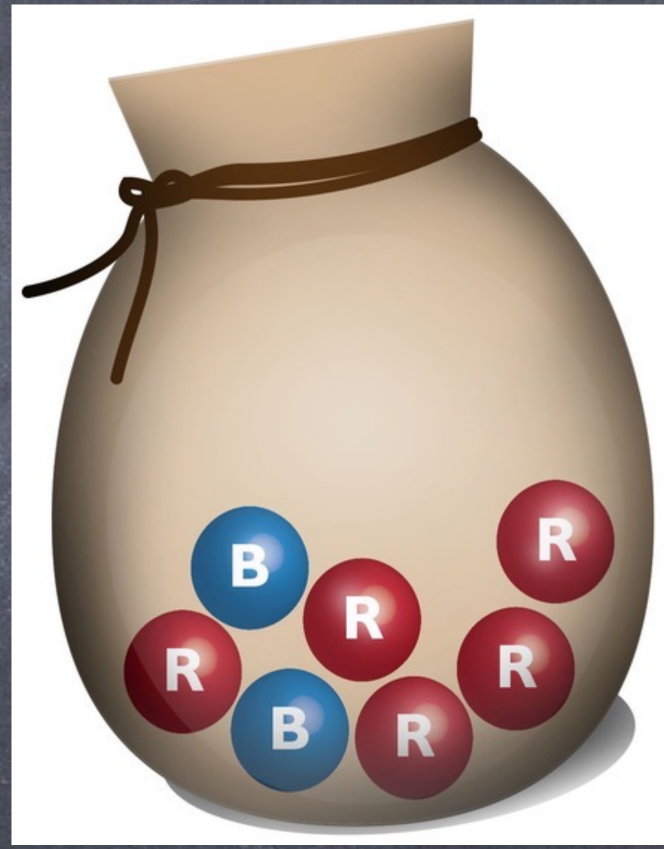
What is probability?

- We only consider discrete / finite models
- Probability is counting...
- Each event is a set of outcomes
- uniform: equal probabilities



What is probability?

- We only consider discrete / finite models
- Probability is counting...
- Each event is a set of outcomes
- uniform: equal probabilities
- Conditional probability: $\Pr[A \mid B] = \Pr[A \cap B] / \Pr[B]$



Independent events

Independent events

- Independence: $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$

Independent events

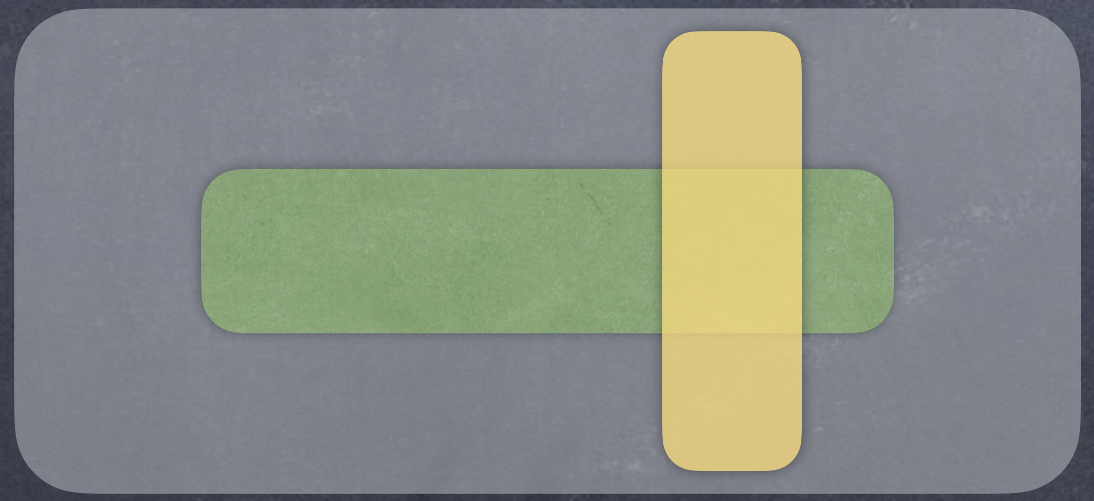
- Independence: $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$
- Using conditional probability: $\Pr[A \mid B] = \Pr[A]$

Independent events

- Independence: $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$
- Using conditional probability: $\Pr[A \mid B] = \Pr[A]$
- Warning: distinguish independent and disjoint events

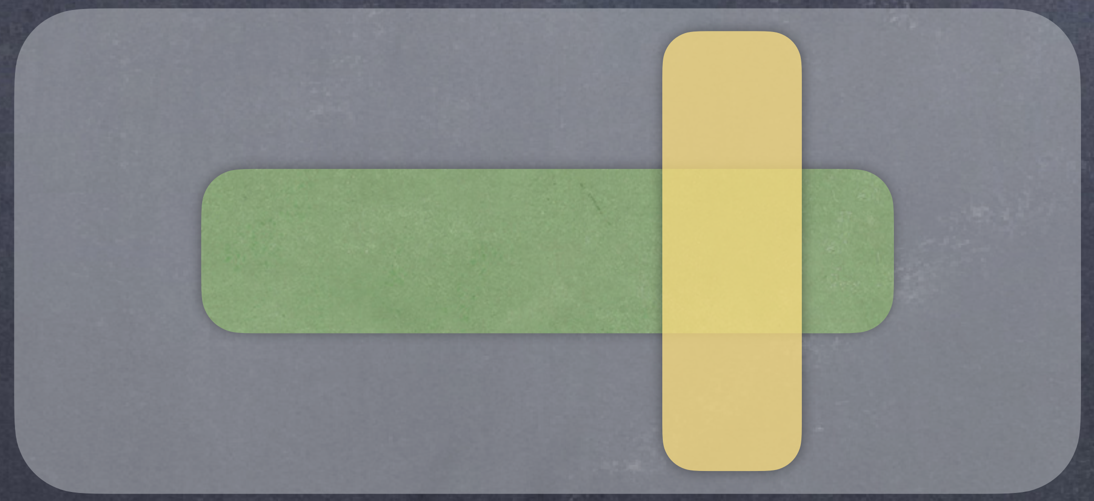
Independent events

- Independence: $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$
- Using conditional probability: $\Pr[A \mid B] = \Pr[A]$
- Warning: distinguish independent and disjoint events



Independent events

- Independence: $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$
- Using conditional probability: $\Pr[A \mid B] = \Pr[A]$
- Warning: distinguish independent and disjoint events



- Disjoint events are highly dependent!

Multivariate polynomials

Multivariate polynomials

- No generalization of fundamental theorem of algebra

Multivariate polynomials

- No generalization of fundamental theorem of algebra
- $Q \in \mathbb{C}[x_1, x_2, \ldots, x_n]$: a polynomial of n variables and degree $\leq d$

Multivariate polynomials

- No generalization of fundamental theorem of algebra
- $Q \in \mathbb{C}[x_1, x_2, \ldots, x_n]$: a polynomial of n variables and degree $\leq d$
- Schwartz-Zippel lemma: for any $U \subseteq \mathbb{C}$,

Multivariate polynomials

- No generalization of fundamental theorem of algebra
- $Q \in \mathbb{C}[x_1, x_2, \ldots, x_n]$: a polynomial of n variables and degree $\leq d$
- Schwartz-Zippel lemma: for any $U \subseteq \mathbb{C}$,

$$\Pr_{r_1, r_2, \ldots, r_n \in U}\left[Q(r_1, r_2, \ldots, r_n) = 0\right] \leq \frac{d}{|U|}$$

Multivariate polynomials

- No generalization of fundamental theorem of algebra
- $Q \in \mathbb{C}[x_1, x_2, \ldots, x_n]$: a polynomial of n variables and degree $\leq d$
- Schwartz-Zippel lemma: for any $U \subseteq \mathbb{C}$,

$$\Pr_{r_1, r_2, \ldots, r_n \in U}\left[Q(r_1, r_2, \ldots, r_n) = 0\right] \leq \frac{d}{|U|}$$

- Counting version: for any $U \subseteq \mathbb{C}$,

Multivariate polynomials

- No generalization of fundamental theorem of algebra
- $Q \in \mathbb{C}[x_1, x_2, \ldots, x_n]$: a polynomial of n variables and degree $\leq d$
- Schwartz-Zippel lemma: for any $U \subseteq \mathbb{C}$,

$$\Pr_{r_1, r_2, \ldots, r_n \in U}\left[Q(r_1, r_2, \ldots, r_n) = 0\right] \leq \frac{d}{|U|}$$

- Counting version: for any $U \subseteq \mathbb{C}$,

$$Q(x_1, x_2, \ldots, x_n) \text{ has } \leq d|U|^{n-1} \text{ roots if } x_1, x_2, \ldots, x_n \in U$$

Min-cut problem

Min-cut problem

- $G = (V, E)$, a cut is a subset of E that partitions V

Min-cut problem

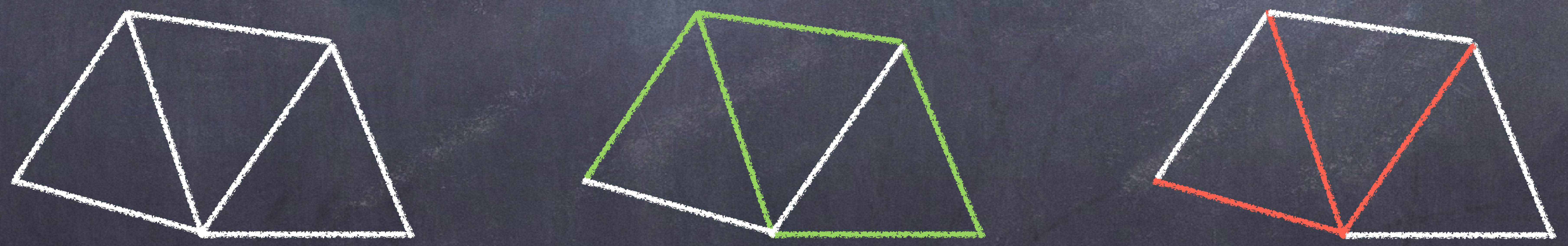
- $G = (V, E)$, a cut is a subset of E that partitions V
- $V = S \cup T$, where $S \neq \emptyset$, $T \neq \emptyset$, but $S \cap T = \emptyset$

Min-cut problem

- $G = (V, E)$, a cut is a subset of E that partitions V
- $V = S \cup T$, where $S \neq \emptyset$, $T \neq \emptyset$, but $S \cap T = \emptyset$
- Subset of edges connecting S and T is a cut

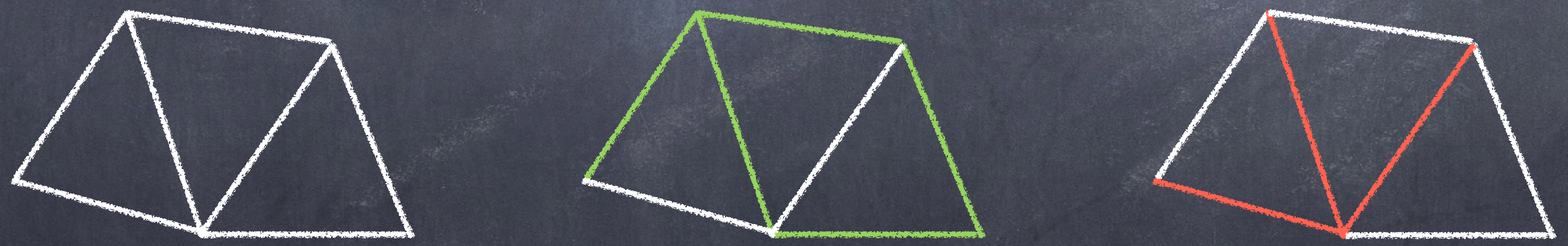
Min-cut problem

- $G = (V, E)$, a cut is a subset of E that partitions V
- $V = S \cup T$, where $S \neq \emptyset$, $T \neq \emptyset$, but $S \cap T = \emptyset$
- Subset of edges connecting S and T is a cut



Min-cut problem

- $G = (V, E)$, a cut is a subset of E that partitions V
- $V = S \cup T$, where $S \neq \emptyset$, $T \neq \emptyset$, but $S \cap T = \emptyset$
- Subset of edges connecting S and T is a cut



- Min-cut: a cut of the minimum size

Finding min-cut

Finding min-cut

- We would like to randomly find a cut

Finding min-cut

- We would like to randomly find a cut
- A naïve attempt: uniformly partition V

Finding min-cut

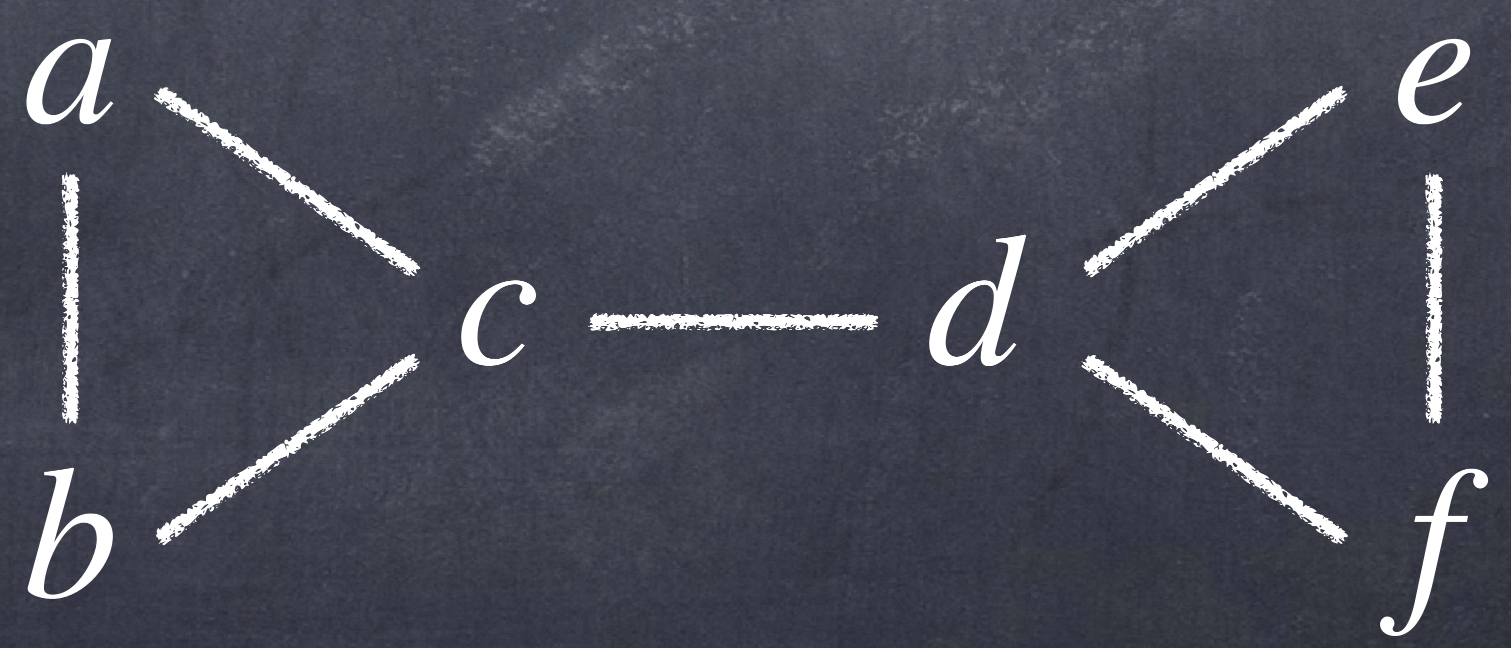
- We would like to randomly find a cut
- A naïve attempt: uniformly partition V
- Assign each vertex $v \in V$ a $0/1$ bit, $0 : v \in S$ and $1 : v \in T$

Finding min-cut

- We would like to randomly find a cut
- A naïve attempt: uniformly partition V
- Assign each vertex $v \in V$ a $0/1$ bit, $0 : v \in S$ and $1 : v \in T$
- What is the probability of finding a minimum cut?

Finding min-cut

- We would like to randomly find a cut
- A naïve attempt: uniformly partition V
- Assign each vertex $v \in V$ a $0/1$ bit, $0 : v \in S$ and $1 : v \in T$
- What is the probability of finding a minimum cut?

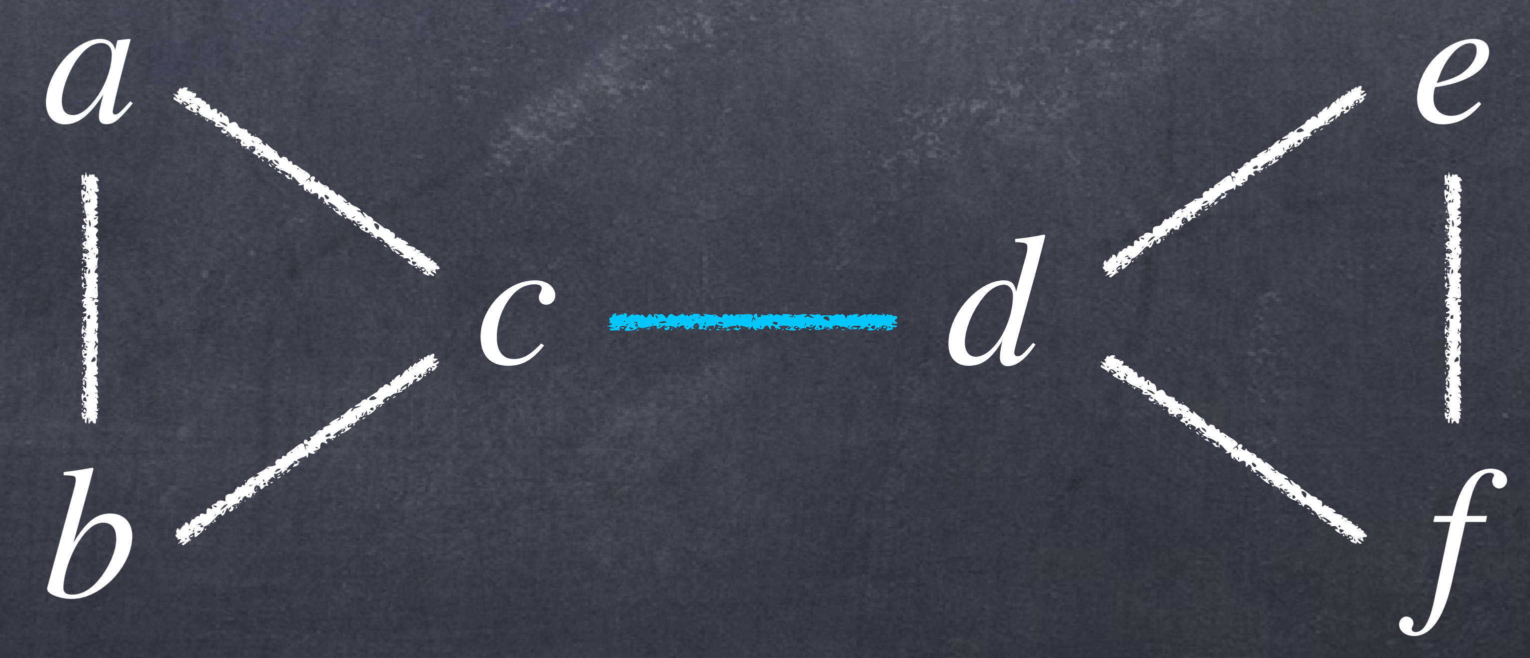


Finding min-cut

- We would like to randomly find a cut
- A naïve attempt: uniformly partition V
- Assign each vertex $v \in V$ a $0/1$ bit, $0 : v \in S$ and $1 : v \in T$
- What is the probability of finding a minimum cut?
- For a particular cut

Finding min-cut

- We would like to randomly find a cut
- A naïve attempt: uniformly partition V
- Assign each vertex $v \in V$ a 0/1 bit, $0 : v \in S$ and $1 : v \in T$
- What is the probability of finding a minimum cut?
- For a particular cut



Finding min-cut

- We would like to randomly find a cut
- A naïve attempt: uniformly partition V
- Assign each vertex $v \in V$ a $0/1$ bit, $0 : v \in S$ and $1 : v \in T$
- What is the probability of finding a minimum cut?
- For a particular cut
- $\Pr[\text{finding it}] = 2^{1-n}$

Finding min-cut

- We would like to randomly find a cut
- A naïve attempt: uniformly partition V
- Assign each vertex $v \in V$ a $0/1$ bit, $0 : v \in S$ and $1 : v \in T$
- What is the probability of finding a minimum cut?
- For a particular cut
- $\Pr[\text{finding it}] = 2^{1-n}$

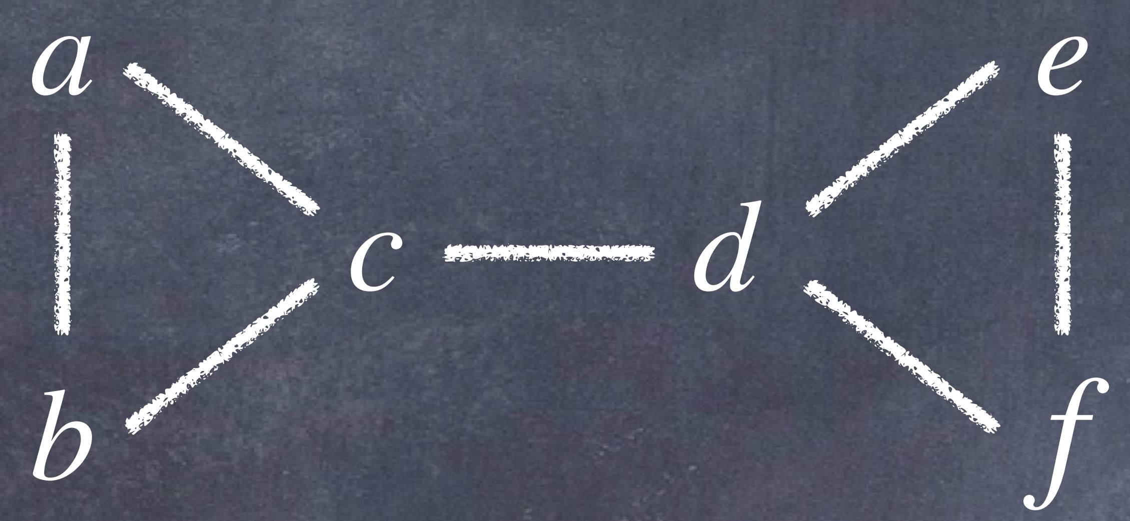
Karger's algorithm

Karger's algorithm

- At each step, contract an edge uniformly at random

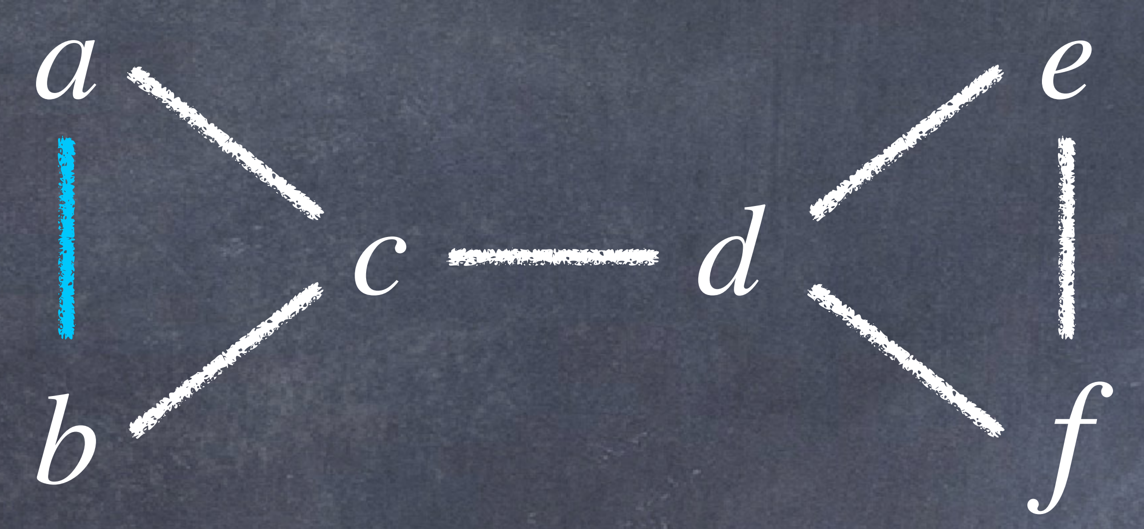
Karger's algorithm

- At each step, contract an edge uniformly at random



Karger's algorithm

- At each step, contract an edge uniformly at random

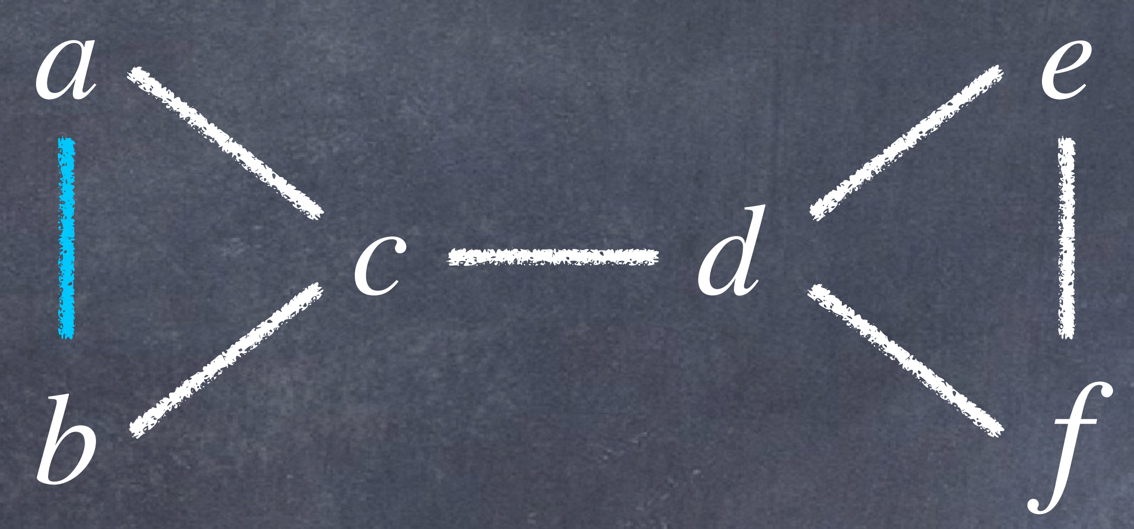


Karger's algorithm

- At each step, contract an edge uniformly at random

Karger's algorithm

- At each step, contract an edge uniformly at random



- Until there are two vertices, output the cut between them

Karger's algorithm

- At each step, contract an edge uniformly at random

- Until there are two vertices, output the cut between them

$$abc \text{ ———— } def$$

Karger's algorithm

Karger's algorithm

- Let S be the event of outputting a (particular) min-cut

Karger's algorithm

- Let S be the event of outputting a (particular) min-cut
- S_i be the event of not contracting an edge in the min-cut

Karger's algorithm

- Let S be the event of outputting a (particular) min-cut
- S_i be the event of not contracting an edge in the min-cut
- $S = S_1 \cap S_2 \cap \cdots \cap S_{n-2}$

Karger's algorithm

- Let S be the event of outputting a (particular) min-cut
- S_i be the event of not contracting an edge in the min-cut
- $S = S_1 \cap S_2 \cap \cdots \cap S_{n-2}$
- $\Pr[S] = \Pr[S_1] \cdot \Pr[S_2 \mid S_1] \cdot \cdots \cdot \Pr[S_{n-2} \mid S_1 \cap \cdots \cap S_{n-3}]$

Karger's algorithm

- Let S be the event of outputting a (particular) min-cut
- S_i be the event of not contracting an edge in the min-cut
- $S = S_1 \cap S_2 \cap \cdots \cap S_{n-2}$
- $\Pr[S] = \Pr[S_1] \cdot \Pr[S_2 \mid S_1] \cdot \cdots \cdot \Pr[S_{n-2} \mid S_1 \cap \cdots \cap S_{n-3}]$
- Suppose the min-cut has k edges...

Karger's algorithm

- Let S be the event of outputting a (particular) min-cut
- S_i be the event of not contracting an edge in the min-cut
- $S = S_1 \cap S_2 \cap \cdots \cap S_{n-2}$
- $\Pr[S] = \Pr[S_1] \cdot \Pr[S_2 \mid S_1] \cdot \cdots \cdot \Pr[S_{n-2} \mid S_1 \cap \cdots \cap S_{n-3}]$
- Suppose the min-cut has k edges...
- Key observation: at anytime, the minimum degree $\geq k$

Karger's algorithm

Karger's algorithm

- At i-th step, graph has $\geq (n - i + 1)k/2$ edges

Karger's algorithm

- At i-th step, graph has $\geq (n-i+1)k/2$ edges
- $\Pr[\text{contracting a min-cut edge}] \leq \dfrac{k}{k(n-i+1)/2} = \dfrac{2}{n-i+1}$

Karger's algorithm

- At i-th step, graph has $\geq (n-i+1)k/2$ edges
- $\Pr[\text{contracting a min-cut edge}] \leq \dfrac{k}{k(n-i+1)/2} = \dfrac{2}{n-i+1}$

$$\Pr[\text{find the min-cut}] \geq \prod_{i=1}^{n-2} \frac{n-i-1}{n-i+1} = \frac{2}{n(n-1)}$$

Karger's algorithm

- At i-th step, graph has $\geq (n-i+1)k/2$ edges
- Pr[contracting a min-cut edge] $\leq \dfrac{k}{k(n-i+1)/2} = \dfrac{2}{n-i+1}$

$$\Pr[\text{find the min-cut}] \geq \prod_{i=1}^{n-2} \frac{n-i-1}{n-i+1} = \frac{2}{n(n-1)}$$

- Run Karger's algorithm $c \cdot n^2$ times, and output the optimal

Karger's algorithm

- At i-th step, graph has $\geq (n-i+1)k/2$ edges
- $\Pr[\text{contracting a min-cut edge}] \leq \dfrac{k}{k(n-i+1)/2} = \dfrac{2}{n-i+1}$

$$\Pr[\text{find the min-cut}] \geq \prod_{i=1}^{n-2} \frac{n-i-1}{n-i+1} = \frac{2}{n(n-1)}$$

- Run Karger's algorithm $c \cdot n^2$ times, and output the optimal

$$\Pr[\text{not output a min-cut}] \leq \left(1 - \frac{2}{n(n-1)}\right)^{cn^2} \leq e^{-c/2}$$

Expectation

Expectation

- **Random variable**: $X : \Omega \to \mathbb{R}$ is a function of all outcomes

Expectation

- Random variable: $X : \Omega \to \mathbb{R}$ is a function of all outcomes
- Expectation:

Expectation

- Random variable: $X : \Omega \to \mathbb{R}$ is a function of all outcomes
- Expectation:

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

Expectation

- Random variable: $X : \Omega \to \mathbb{R}$ is a function of all outcomes
- Expectation:

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

- Another definition: (double counting)

Expectation

- Random variable: $X : \Omega \to \mathbb{R}$ is a function of all outcomes
- Expectation:

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

- Another definition: (double counting)

$$\mathbb{E}[X] = \sum_{x \in \mathbb{R}} x \cdot \Pr_{\omega}[X(\omega) = x]$$

Expectation

- Random variable: $X : \Omega \to \mathbb{R}$ is a function of all outcomes
- Expectation:

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

- Another definition: (double counting)

$$\mathbb{E}[X] = \sum_{x \in \mathbb{R}} x \cdot \Pr_{\omega}[X(\omega) = x]$$

- Warning: forget everything about conditional expectations

Linearity of expectation

Linearity of expectation

- Ω: set of outcomes

Linearity of expectation

- Ω: set of outcomes
- $X_1, X_2, \ldots, X_n$: random variables

Linearity of expectation

- Ω: set of outcomes
- $X_1, X_2, \ldots, X_n$: random variables
- Linearity of expectation:

Linearity of expectation

- Ω: set of outcomes
- $X_1, X_2, \ldots, X_n$: random variables
- Linearity of expectation:

$$\mathbb{E}[X_1 + X_2 + \cdots + X_n] = \mathbb{E}[X_1] + \mathbb{E}[X_2] + \cdots + \mathbb{E}[X_n]$$

Linearity of expectation

- Ω: set of outcomes
- $X_1, X_2, \ldots, X_n$: random variables
- Linearity of expectation:

$$\mathbb{E}[X_1 + X_2 + \cdots + X_n] = \mathbb{E}[X_1] + \mathbb{E}[X_2] + \cdots + \mathbb{E}[X_n]$$

- Proof: $\mathbb{E}[X_1 + X_2] = \sum_{\omega \in \Omega} \Pr[\omega] \cdot \big(X_1(\omega) + X_2(\omega)\big) = \mathbb{E}[X_1] + \mathbb{E}[X_2]$

Linearity of expectation

- Ω: set of outcomes
- $X_1, X_2, \ldots, X_n$: random variables
- Linearity of expectation:

$$\mathbb{E}[X_1 + X_2 + \cdots + X_n] = \mathbb{E}[X_1] + \mathbb{E}[X_2] + \cdots + \mathbb{E}[X_n]$$

- Proof: $\mathbb{E}[X_1 + X_2] = \sum_{\omega \in \Omega} \Pr[\omega] \cdot \big(X_1(\omega) + X_2(\omega)\big) = \mathbb{E}[X_1] + \mathbb{E}[X_2]$
- Do not assume any independence here

Linearity of expectation

Linearity of expectation

- Throw a dice twice and denoted by two independent r.v.s X_1, X_2

Linearity of expectation

- Throw a dice twice and denoted by two independent r.v.s X_1, X_2
- $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \frac{1}{6} \cdot (1 + 2 + 3 + 4 + 5 + 6) = \frac{7}{2}$

Linearity of expectation

- Throw a dice twice and denoted by two independent r.v.s X_1, X_2
- $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \frac{1}{6} \cdot (1 + 2 + 3 + 4 + 5 + 6) = \frac{7}{2}$
- $\mathbb{E}[X_1 + X_2] = \frac{1}{36} \cdot (2 + 3 + 3 + 4 + 4 + 4 + \cdots + 11 + 11 + 12) = 7$

Linearity of expectation

- Throw a dice twice and denoted by two independent r.v.s X_1, X_2
- $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \frac{1}{6} \cdot (1+2+3+4+5+6) = \frac{7}{2}$
- $\mathbb{E}[X_1 + X_2] = \frac{1}{36} \cdot (2+3+3+4+4+4+\cdots+11+11+12) = 7$
- Throw a dice once and denoted by two identical r.v.s $X_1 = X_2$

Linearity of expectation

- Throw a dice twice and denoted by two independent r.v.s X_1, X_2
- $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \frac{1}{6} \cdot (1 + 2 + 3 + 4 + 5 + 6) = \frac{7}{2}$
- $\mathbb{E}[X_1 + X_2] = \frac{1}{36} \cdot (2 + 3 + 3 + 4 + 4 + 4 + \cdots + 11 + 11 + 12) = 7$
- Throw a dice once and denoted by two identical r.v.s $X_1 = X_2$
- $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \frac{1}{6} \cdot (1 + 2 + 3 + 4 + 5 + 6) = \frac{7}{2}$

Linearity of expectation

- Throw a dice twice and denoted by two independent r.v.s X_1, X_2
- $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \frac{1}{6} \cdot (1+2+3+4+5+6) = \frac{7}{2}$
- $\mathbb{E}[X_1 + X_2] = \frac{1}{36} \cdot (2+3+3+4+4+4+\cdots+11+11+12) = 7$
- Throw a dice once and denoted by two identical r.v.s $X_1 = X_2$
- $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \frac{1}{6} \cdot (1+2+3+4+5+6) = \frac{7}{2}$
- $\mathbb{E}[X_1 + X_2] = \frac{1}{6} \cdot (2+4+6+8+10+12) = 7$

Random permutation

Random permutation

- Consider a permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ of n elements

Random permutation

- Consider a permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ of n elements
- We say i is a fixed point if $\pi_i = i$

Random permutation

- Consider a permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ of n elements
- We say i is a fixed point if $\pi_i = i$
- Question: if π is chosen randomly, how many fixed points ?

Random permutation

- Consider a permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ of n elements
- We say i is a fixed point if $\pi_i = i$
- Question: if π is chosen randomly, how many fixed points ?
- $X_i = 1$ if $\pi_i = i$, and $X_i = 0$ otherwise

Random permutation

- Consider a permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ of n elements
- We say i is a fixed point if $\pi_i = i$
- Question: if π is chosen randomly, how many fixed points ?
- $X_i = 1$ if $\pi_i = i$, and $X_i = 0$ otherwise
- $\mathbb{E}[X_i] = \Pr[X_i = 1] = \Pr[\pi_i = i] = (n-1)!/n! = 1/n$

Random permutation

- Consider a permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$ of n elements
- We say i is a fixed point if $\pi_i = i$
- Question: if π is chosen randomly, how many fixed points ?
- $X_i = 1$ if $\pi_i = i$, and $X_i = 0$ otherwise
- $\mathbb{E}[X_i] = \Pr[X_i = 1] = \Pr[\pi_i = i] = (n-1)!/n! = 1/n$

$$\mathbb{E}[X] = \sum_{i=1}^{n} \mathbb{E}[X_i] = 1$$

Coupon collector

Coupon collector

Coupon collector

Coupon collector

Coupon collector

- n types of coupons

Coupon collector

- n types of coupons
- Each time draw a coupon from n types uniformly at random

Coupon collector

- n types of coupons
- Each time draw a coupon from n types uniformly at random
- Question: how many coupons drawn until collecting all types?

Coupon collector

Coupon collector

- Let X be the number of coupons drawn

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3	4

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3	4	5	6	7	8

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3	4	5	6	7	8	…	…

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3	4	5	6	7	8	…	…	X-3	X-2	X-1

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3	4	5	6	7	8	…	…	X-3	X-2	X-1	X

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3	4	5	6	7	8	…	…	X-3	X-2	X-1	X

- X_i : # of coupons until meet a new type, if having i types already

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3	4	5	6	7	8	…	…	X-3	X-2	X-1	X

- X_i : # of coupons until meet a new type, if having i types already

$$X = \sum_{i=0}^{n-1} X_i \implies \mathbb{E}[X] = \sum_{i=0}^{n-1} \mathbb{E}[X_i]$$

Coupon collector

- Let X be the number of coupons drawn
- Compute X by enumerating all possibilities?

1	2	3	4	5	6	7	8	…	…	X-3	X-2	X-1	X

- X_i : # of coupons until meet a new type, if having i types already

$$X = \sum_{i=0}^{n-1} X_i \implies \mathbb{E}[X] = \sum_{i=0}^{n-1} \mathbb{E}[X_i]$$

- But how to compute $\mathbb{E}[X_i]$?

Coupon collector

Coupon collector

- Pr[collect a new type | have i types already] = $(n - i)/n$

Coupon collector

- $\Pr[\text{collect a new type} \mid \text{have } i \text{ types already}] = (n - i)/n$
- Bernoulli trial: independent trials with success probability p

Coupon collector

- $\Pr[\text{collect a new type} \mid \text{have } i \text{ types already}] = (n - i)/n$
- **Bernoulli trial**: independent trials with success probability p
- Question: how many trials until success?

Coupon collector

- $\Pr[\text{collect a new type} \mid \text{have } i \text{ types already}] = (n-i)/n$
- Bernoulli trial: independent trials with success probability p
- Question: how many trials until success?
- $\mathbb{E} = \sum_{k=1}^{\infty} k \cdot p \cdot (1-p)^{k-1} = \sum_{k=0}^{\infty} (1-p)^k = 1/p$

Coupon collector

- Pr[collect a new type | have i types already] $= (n - i)/n$
- Bernoulli trial: independent trials with success probability p
- Question: how many trials until success?
- $\mathbb{E} = \sum_{k=1}^{\infty} k \cdot p \cdot (1-p)^{k-1} = \sum_{k=0}^{\infty} (1-p)^k = 1/p$
- $\mathbb{E}[X_i] = n/(n-i)$

Coupon collector

- $\Pr[\text{collect a new type} \mid \text{have } i \text{ types already}] = (n-i)/n$
- Bernoulli trial: independent trials with success probability p
- Question: how many trials until success?
- $\mathbb{E} = \sum_{k=1}^{\infty} k \cdot p \cdot (1-p)^{k-1} = \sum_{k=0}^{\infty} (1-p)^k = 1/p$
- $\mathbb{E}[X_i] = n/(n-i)$

$$\mathbb{E}[X] = \sum_{i=0}^{n-1} \mathbb{E}[X_i] = n \sum_{i=1}^{n} 1/i \approx n \cdot (\ln n + \gamma)$$

Do you feel lucky?

Do you feel lucky?

- Expectation is a notion of "average value"

Do you feel lucky?

- Expectation is a notion of "average value"
- Is it possible that do not collect all after too many times?

Do you feel lucky?

- Expectation is a notion of "average value"
- Is it possible that do not collect all after too many times?
- Suppose we have drawn $n \ln n + cn$ coupons

Do you feel lucky?

- Expectation is a notion of "average value"
- Is it possible that do not collect all after too many times?
- Suppose we have drawn $n \ln n + cn$ coupons
- $\Pr[\text{do not collect type } i] = (1 - 1/n)^{n \ln n + cn} < e^{-(\ln n + c)} = e^{-c}/n$

Do you feel lucky?

- Expectation is a notion of "average value"
- Is it possible that do not collect all after too many times?
- Suppose we have drawn $n \ln n + cn$ coupons
- $\Pr[\text{do not collect type } i] = (1 - 1/n)^{n \ln n + cn} < e^{-(\ln n + c)} = e^{-c}/n$
- Union bound: $\Pr[A \cup B] \leq \Pr[A] + \Pr[B]$

Do you feel lucky?

- Expectation is a notion of "average value"
- Is it possible that do not collect all after too many times?
- Suppose we have drawn $n \ln n + cn$ coupons
- $\Pr[\text{do not collect type } i] = (1 - 1/n)^{n \ln n + cn} < e^{-(\ln n + c)} = e^{-c}/n$
- Union bound: $\Pr[A \cup B] \leq \Pr[A] + \Pr[B]$

$$\Pr[\text{do not collect all types}] \leq n \cdot e^{-c}/n = e^{-c}$$

Quick-sort

Quick-sort

- Recall Quick-select algorithm...

Quick-sort

- Recall Quick-select algorithm...
- Find a pivot, then divide and conquer

Quick-sort

- Recall Quick-select algorithm...
- Find a pivot, then divide and conquer
- Modify the algorithm into a sorting algorithm:

Quick-sort

- Recall Quick-select algorithm...
- Find a pivot, then divide and conquer
- Modify the algorithm into a sorting algorithm:
- Sort L and R respectively, then return L+M+R

Quick-sort

- Recall Quick-select algorithm…
- Find a pivot, then divide and conquer
- Modify the algorithm into a sorting algorithm:
- Sort L and R respectively, then return L+M+R

Quick-sort

- Recall Quick-select algorithm...
- Find a pivot, then divide and conquer
- Modify the algorithm into a sorting algorithm:
- Sort L and R respectively, then return L+M+R

6	3	1	5	4	2	7

Quick-sort

- Recall Quick-select algorithm...
- Find a pivot, then divide and conquer
- Modify the algorithm into a sorting algorithm:
- Sort L and R respectively, then return L+M+R

6	3	1	5	4	2	7

3	1	4	2	5	6	7

Quick-sort

Quick-sort

- Let $T(n)$ be the running time of sorting an n-array

Quick-sort

- Let $T(n)$ be the running time of sorting an n-array
- If we choose pivots unluckily… $T(n) = (n - 1) + T(n - 1)$

Quick-sort

- Let $T(n)$ be the running time of sorting an n-array
- If we choose pivots unluckily... $T(n) = (n-1) + T(n-1)$
- $T(n) = O(n^2)$... Too bad !

Quick-sort

- Let $T(n)$ be the running time of sorting an n-array
- If we choose pivots unluckily... $T(n) = (n-1) + T(n-1)$
- $T(n) = O(n^2)$... Too bad !
- Now we choose pivots randomly...

Quick-sort

- Let $T(n)$ be the running time of sorting an n-array
- If we choose pivots unluckily… $T(n) = (n-1) + T(n-1)$
- $T(n) = O(n^2)$… Too bad !
- Now we choose pivots randomly…
- Consider the expected running time $\mathbb{E}[T(n)]$…

Quick-sort

- Let $T(n)$ be the running time of sorting an n-array
- If we choose pivots unluckily... $T(n) = (n-1) + T(n-1)$
- $T(n) = O(n^2)$... Too bad !
- Now we choose pivots randomly...
- Consider the expected running time $\mathbb{E}[T(n)]$...

$$\mathbb{E}[T(n)] = (n-1) + \frac{1}{n}\sum_{k=1}^{n-1} \mathbb{E}[T(k)] + \mathbb{E}[T(n-k-1)]$$

Quick-sort

Quick-sort

- We guess that $\mathbb{E}[T(n)] \approx c \cdot n \ln n$ for some constant c

Quick-sort

- We guess that $\mathbb{E}[T(n)] \approx c \cdot n \ln n$ for some constant c
- Prove by induction

Quick-sort

- We guess that $\mathbb{E}[T(n)] \approx c \cdot n \ln n$ for some constant c
- Prove by induction
- More clever?

Quick-sort

- We guess that $\mathbb{E}[T(n)] \approx c \cdot n \ln n$ for some constant c
- Prove by induction
- More clever?
- $T(n)$ is the number of comparisons!

Quick-sort

- We guess that $\mathbb{E}[T(n)] \approx c \cdot n \ln n$ for some constant c
- Prove by induction
- More clever?
- $T(n)$ is the number of comparisons!
- Let X_{ij} be the number of comparisons between a_i and a_j

Quick-sort

- We guess that $\mathbb{E}[T(n)] \approx c \cdot n \ln n$ for some constant c
- Prove by induction
- More clever?
- $T(n)$ is the number of comparisons!
- Let X_{ij} be the number of comparisons between a_i and a_j
- $\mathbb{E}[T(n)] = \mathbb{E}\left[\sum_{1 \le i < j \le n} X_{ij}\right] = \sum_{1 \le i < j \le n} \mathbb{E}[X_{ij}]$

Quick-sort

Quick-sort

- We only compare pivot with other variables

Quick-sort

- We only compare pivot with other variables
- Assume $a_i < a_j$, $X_{ij} = 1$ means a_i or a_j is pivot, and...

Quick-sort

- We only compare pivot with other variables
- Assume $a_i < a_j$, $X_{ij} = 1$ means a_i or a_j is pivot, and...
- any a_k such that $a_i < a_k < a_j$ are not chosen before taking a_i or a_j

Quick-sort

- We only compare pivot with other variables
- Assume $a_i < a_j$, $X_{ij} = 1$ means a_i or a_j is pivot, and...
- any a_k such that $a_i < a_k < a_j$ are not chosen before taking a_i or a_j
- So $\Pr[X_{ij} = 1] = ?$

Quick-sort

- We only compare pivot with other variables
- Assume $a_i < a_j$, $X_{ij} = 1$ means a_i or a_j is pivot, and...
- any a_k such that $a_i < a_k < a_j$ are not chosen before taking a_i or a_j
- So $\Pr[X_{ij} = 1] = ?$
- More clever?

Quick-sort

- We only compare pivot with other variables
- Assume $a_i < a_j$, $X_{ij} = 1$ means a_i or a_j is pivot, and...
- any a_k such that $a_i < a_k < a_j$ are not chosen before taking a_i or a_j
- So $\Pr[X_{ij} = 1] = ?$
- More clever?
- $X_{ij} = \#$ of comparisons between *i-th smallest* and *j-th smallest*

Quick-sort

Quick-sort

- Pick a random permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$

Quick-sort

- Pick a random permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$
- For any subsequence $[a_l, \ldots, a_r]$, choose pivot a_k with smallest π_k

Quick-sort

- Pick a random permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$
- For any subsequence $[a_l, \ldots, a_r]$, choose pivot a_k with smallest π_k

$$\Pr[X_{ij} = 1] = 2/(j - i + 1)$$

Quick-sort

- Pick a random permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$
- For any subsequence $[a_l, \ldots, a_r]$, choose pivot a_k with smallest π_k

$$\Pr[X_{ij} = 1] = 2/(j - i + 1)$$

- $\mathbb{E}[T(n)] = \sum_{1 \le i < j \le n} \mathbb{E}[X_{ij}] = \sum_{1 \le i < j \le n} \Pr[X_{ij} = 1] = \sum_{i<j} 2/(j - i + 1)$

Quick-sort

- Pick a random permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$
- For any subsequence $[a_l, \ldots, a_r]$, choose pivot a_k with smallest π_k

$$\Pr[X_{ij} = 1] = 2/(j - i + 1)$$

- $\mathbb{E}[T(n)] = \sum_{1 \le i < j \le n} \mathbb{E}[X_{ij}] = \sum_{1 \le i < j \le n} \Pr[X_{ij} = 1] = \sum_{i<j} 2/(j - i + 1)$
- Let $H_n = \sum_{i=1}^{n} 1/i \approx \ln n + \gamma$

Quick-sort

- Pick a random permutation $\pi = (\pi_1, \pi_2, \ldots, \pi_n)$
- For any subsequence $[a_l, \ldots, a_r]$, choose pivot a_k with smallest π_k

$$\Pr[X_{ij} = 1] = 2/(j - i + 1)$$

- $\mathbb{E}[T(n)] = \sum_{1 \le i < j \le n} \mathbb{E}[X_{ij}] = \sum_{1 \le i < j \le n} \Pr[X_{ij} = 1] = \sum_{i<j} 2/(j - i + 1)$
- Let $H_n = \sum_{i=1}^{n} 1/i \approx \ln n + \gamma$

$$\mathbb{E}[T(n)] = 2\sum_{i=1}^{n-1} (H_{n-i+1} - 1) \le 2(n-1)(H_n - 1) \le 2n \ln n$$

Markov's inequality

Markov's inequality

- Markov's inequality: Suppose $X \geq 0$ is a nonnegative r.v.

Markov's inequality

- Markov's inequality: Suppose $X \geq 0$ is a nonnegative r.v.

  Then for any $C > 0$, $\Pr[X \geq C] \leq \frac{\mathbb{E}[X]}{C}$.

Markov's inequality

- Markov's inequality: Suppose $X \geq 0$ is a nonnegative r.v.

  Then for any $C > 0$, $\Pr[X \geq C] \leq \frac{\mathbb{E}[X]}{C}$.

- Proof: $\mathbb{E}[X] = \sum_{\omega} \omega \cdot \Pr[X = \omega] \geq 0 \cdot \Pr[X < C] + C \cdot \Pr[X \geq C]$

Markov's inequality

- Markov's inequality: Suppose $X \geq 0$ is a nonnegative r.v.

  Then for any $C > 0$, $\Pr[X \geq C] \leq \frac{\mathbb{E}[X]}{C}$.

- Proof: $\mathbb{E}[X] = \sum_{\omega} \omega \cdot \Pr[X = \omega] \geq 0 \cdot \Pr[X < C] + C \cdot \Pr[X \geq C]$

- Application: Randomized Quick-Sort

Markov's inequality

- Markov's inequality: Suppose $X \geq 0$ is a nonnegative r.v.

  Then for any $C > 0$, $\Pr[X \geq C] \leq \frac{\mathbb{E}[X]}{C}$.

- Proof: $\mathbb{E}[X] = \sum_{\omega} \omega \cdot \Pr[X = \omega] \geq 0 \cdot \Pr[X < C] + C \cdot \Pr[X \geq C]$

- Application: Randomized Quick-Sort

- Recall that $\mathbb{E}[T(n)] \leq 2n \ln n$

Markov's inequality

- Markov's inequality: Suppose $X \geq 0$ is a nonnegative r.v.

  Then for any $C > 0$, $\Pr[X \geq C] \leq \frac{\mathbb{E}[X]}{C}$.

- Proof: $\mathbb{E}[X] = \sum_{\omega} \omega \cdot \Pr[X = \omega] \geq 0 \cdot \Pr[X < C] + C \cdot \Pr[X \geq C]$

- Application: Randomized Quick-Sort

- Recall that $\mathbb{E}[T(n)] \leq 2n \ln n$

$$\Pr[T(n) \geq 2cn \ln n] \leq 1/c$$

Beyond Markov's inequality

Beyond Markov's inequality

- Suppose $X \geq 0$, Markov's inequality asserts $\Pr[X \geq C]$

Beyond Markov's inequality

- Suppose $X \geq 0$, Markov's inequality asserts $\Pr[X \geq C]$
- How about $\Pr[X \leq C]$?

Beyond Markov's inequality

- Suppose $X \geq 0$, Markov's inequality asserts $\Pr[X \geq C]$
- How about $\Pr[X \leq C]$?
- "600 million Chinese people have monthly income ≤ 1000"

Beyond Markov's inequality

- Suppose $X \geq 0$, Markov's inequality asserts $\Pr[X \geq C]$
- How about $\Pr[X \leq C]$?
- "600 million Chinese people have monthly income ≤ 1000"
- Chebyshev's inequality: $\Pr\left[|X - \mathbb{E}[X]| \geq t\right] \leq \mathrm{Var}[X]/t^2$

Beyond Markov's inequality

- Suppose $X \geq 0$, Markov's inequality asserts $\Pr[X \geq C]$
- How about $\Pr[X \leq C]$?
- "600 million Chinese people have monthly income ≤ 1000"
- Chebyshev's inequality: $\Pr\left[|X - \mathbb{E}[X]| \geq t\right] \leq \mathrm{Var}[X]/t^2$
- Application in analysis: Weierstrass approximation theorem

Beyond Markov's inequality

- Suppose $X \geq 0$, Markov's inequality asserts $\Pr[X \geq C]$
- How about $\Pr[X \leq C]$?
- "600 million Chinese people have monthly income ≤ 1000"
- Chebyshev's inequality: $\Pr\left[|X - \mathbb{E}[X]| \geq t\right] \leq \mathrm{Var}[X]/t^2$
- Application in analysis: Weierstrass approximation theorem
- More general: concentration of measures...

Linearity may fail...

Linearity may fail...

- Linearity may fail if the number of r.v.s is infinite

Linearity may fail...

- Linearity may fail if the number of r.v.s is infinite
- Linearity may fail if the number of r.v.s is random

Linearity may fail…

- Linearity may fail if the number of r.v.s is infinite
- Linearity may fail if the number of r.v.s is random
- Let N be a random number

Linearity may fail...

- Linearity may fail if the number of r.v.s is infinite
- Linearity may fail if the number of r.v.s is random
- Let N be a random number
- $X_1, \ldots, X_N$ are independently identically distributed (i.i.d.)

Linearity may fail...

- Linearity may fail if the number of r.v.s is infinite
- Linearity may fail if the number of r.v.s is random
- Let N be a random number
- $X_1, \ldots, X_N$ are independently identically distributed (i.i.d.)
- We may expect $\mathbb{E}[X_1 + X_2 + \cdots + X_N] = \mathbb{E}[N] \cdot \mathbb{E}[X_i]$

Linearity may fail...

- Linearity may fail if the number of r.v.s is infinite
- Linearity may fail if the number of r.v.s is random
- Let N be a random number
- $X_1, \ldots, X_N$ are independently identically distributed (i.i.d.)
- We may expect $\mathbb{E}[X_1 + X_2 + \cdots + X_N] = \mathbb{E}[N] \cdot \mathbb{E}[X_i]$
- Is it true?

Random number of r.v.s

Random number of r.v.s

- Throw a dice, and let N be the result

Random number of r.v.s

- Throw a dice, and let N be the result
- Then let $X_1 = X_2 = \cdots = X_N = N$ be N r.v.s

Random number of r.v.s

- Throw a dice, and let N be the result
- Then let $X_1 = X_2 = \cdots = X_N = N$ be N r.v.s
- Clearly, $\mathbb{E}[N] = \mathbb{E}[X_i] = \frac{7}{2}$

Random number of r.v.s

- Throw a dice, and let N be the result
- Then let $X_1 = X_2 = \cdots = X_N = N$ be N r.v.s
- Clearly, $\mathbb{E}[N] = \mathbb{E}[X_i] = \frac{7}{2}$
- However, $\mathbb{E}[X_1 + \cdots + X_N] = \mathbb{E}[N^2] = \frac{91}{6} \neq \mathbb{E}[N]^2$

Random number of r.v.s

- Throw a dice, and let N be the result
- Then let $X_1 = X_2 = \cdots = X_N = N$ be N r.v.s
- Clearly, $\mathbb{E}[N] = \mathbb{E}[X_i] = \frac{7}{2}$
- However, $\mathbb{E}[X_1 + \cdots + X_N] = \mathbb{E}[N^2] = \frac{91}{6} \neq \mathbb{E}[N]^2$
- We may guess that this is because $X_1, \ldots, X_N$ are not independent

Random number of r.v.s

- Throw a dice, and let N be the result
- Then let $X_1 = X_2 = \cdots = X_N = N$ be N r.v.s
- Clearly, $\mathbb{E}[N] = \mathbb{E}[X_i] = \frac{7}{2}$
- However, $\mathbb{E}[X_1 + \cdots + X_N] = \mathbb{E}[N^2] = \frac{91}{6} \neq \mathbb{E}[N]^2$
- We may guess that this is because $X_1, \ldots, X_N$ are not independent
- How about randomly many independent r.v.s?

St. Petersburg paradox

St. Petersburg paradox

- A gambler plays a game of guessing a fair (uniform) coin

St. Petersburg paradox

- A gambler plays a game of guessing a fair (uniform) coin
- At the first round, the gambler bets $\$1$

St. Petersburg paradox

- A gambler plays a game of guessing a fair (uniform) coin
- At the first round, the gambler bets $\$1$
- If the gambler wins, they stops the game

St. Petersburg paradox

- A gambler plays a game of guessing a fair (uniform) coin
- At the first round, the gambler bets $1
- If the gambler wins, they stops the game
- If the gambler loses, they doubles the bet and guesses again

St. Petersburg paradox

- A gambler plays a game of guessing a fair (uniform) coin
- At the first round, the gambler bets $\$1$
- If the gambler wins, they stops the game
- If the gambler loses, they doubles the bet and guesses again
- Clearly, at each round $\mathbb{E}[X_i] = 0$

St. Petersburg paradox

- A gambler plays a game of guessing a fair (uniform) coin
- At the first round, the gambler bets $\$1$
- If the gambler wins, they stops the game
- If the gambler loses, they doubles the bet and guesses again
- Clearly, at each round $\mathbb{E}[X_i] = 0$
- However, the gambler always stops with winning $\$1$ ($\sum X_i = 1$)

Enjoy the world of randomness !

Thank you

Wald's equation

Wald's equation

- Wald's equation (simple version):

Wald's equation

- Wald's equation (simple version):
- Suppose N is a r.v. bounded by n, and independent of all X_i

Wald's equation

- **Wald's equation** (simple version):
- Suppose N is a r.v. bounded by n, and independent of all X_i
- Consider the random variable $X_k \cdot \mathbf{1}_{[X \geq k]}$

Wald's equation

- Wald's equation (simple version):
- Suppose N is a r.v. bounded by n, and independent of all X_i
- Consider the random variable $X_k \cdot \mathbf{1}_{[X \geq k]}$
- Since X_k and $\mathbf{1}_{[X \geq k]}$ are independent, $\mathbb{E}\left[X_k \cdot \mathbf{1}_{[X \geq k]}\right] = \mathbb{E}[X_k] \cdot \mathbb{E}\left[\mathbf{1}_{[X \geq k]}\right]$

Wald's equation

- Wald's equation (simple version):
- Suppose N is a r.v. bounded by n, and independent of all X_i
- Consider the random variable $X_k \cdot \mathbf{1}_{[X \geq k]}$
- Since X_k and $\mathbf{1}_{[X \geq k]}$ are independent, $\mathbb{E}\left[X_k \cdot \mathbf{1}_{[X \geq k]}\right] = \mathbb{E}[X_k] \cdot \mathbb{E}\left[\mathbf{1}_{[X \geq k]}\right]$
- Then $\mathbb{E}[X_1 + \cdots + X_N] = \sum_{k=1}^{n} \mathbb{E}[X_k] \cdot \mathbb{E}\left[\mathbf{1}_{[X \geq k]}\right]$

Wald's equation

- **Wald's equation** (simple version):
- Suppose N is a r.v. bounded by n, and independent of all X_i
- Consider the random variable $X_k \cdot \mathbf{1}_{[X \geq k]}$
- Since X_k and $\mathbf{1}_{[X \geq k]}$ are independent, $\mathbb{E}\left[X_k \cdot \mathbf{1}_{[X \geq k]}\right] = \mathbb{E}[X_k] \cdot \mathbb{E}\left[\mathbf{1}_{[X \geq k]}\right]$
- Then $\mathbb{E}[X_1 + \cdots + X_N] = \sum_{k=1}^{n} \mathbb{E}[X_k] \cdot \mathbb{E}\left[\mathbf{1}_{[X \geq k]}\right]$
- In particular, if $\mathbb{E}[X_k] = \mu$, $\mathbb{E}[X_1 + \cdots + X_N] = \mu \cdot \mathbb{E}[N]$

Random number of r.v.s

Random number of r.v.s

- Throw a dice, and let N be the result

Random number of r.v.s

- Throw a dice, and let N be the result
- Throw again and let $X_1 = X_2 = \cdots = X_N$ be the result

Random number of r.v.s

- Throw a dice, and let N be the result
- Throw again and let $X_1 = X_2 = \cdots = X_N$ be the result
- Clearly, $\mathbb{E}[N] = \mathbb{E}[X_i] = \frac{7}{2}$

Random number of r.v.s

- Throw a dice, and let N be the result
- Throw again and let $X_1 = X_2 = \cdots = X_N$ be the result
- Clearly, $\mathbb{E}[N] = \mathbb{E}[X_i] = \frac{7}{2}$
- Let $\mu = \mathbb{E}[X_i] = \frac{7}{2}$. Then $\mu \cdot \mathbb{E}[N] = \frac{49}{4}$

Random number of r.v.s

- Throw a dice, and let N be the result
- Throw again and let $X_1 = X_2 = \cdots = X_N$ be the result
- Clearly, $\mathbb{E}[N] = \mathbb{E}[X_i] = \frac{7}{2}$
- Let $\mu = \mathbb{E}[X_i] = \frac{7}{2}$. Then $\mu \cdot \mathbb{E}[N] = \frac{49}{4}$
- $\mathbb{E}[X_1 + \cdots + X_N] = \frac{1}{36} \cdot (21 + 21 \cdot 2 + \cdots + 21 \cdot 6) = \frac{21^2}{36} = \frac{49}{4}$

Random recurrence

KUW inequality

Quick-Select revisit

Coupon collector revisit

Yao's lemma

Monte Carlo vs. Las Vegas

Complexity class

Enjoy the world of randomness !

Thank you