An introduction to discrete probabilities

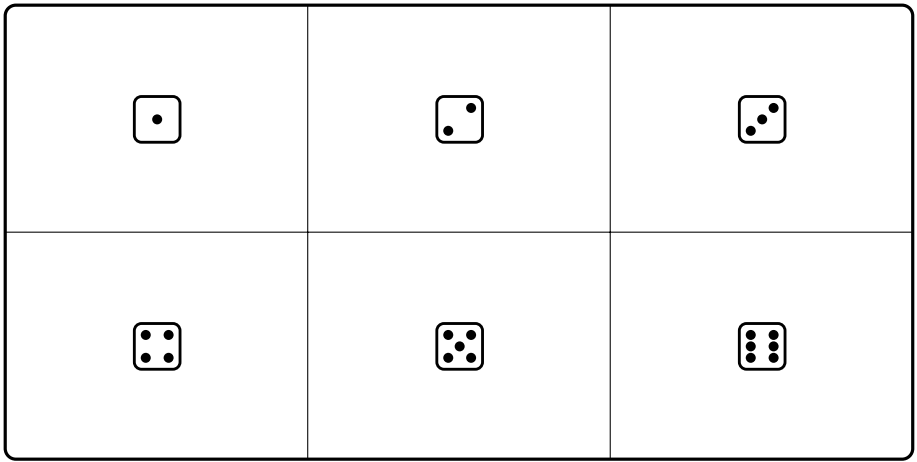
Bruno Grenet

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

Introduction to cryptology
Université Grenoble Alpes – IM²AG
M1 INFO, MOSIG & AM

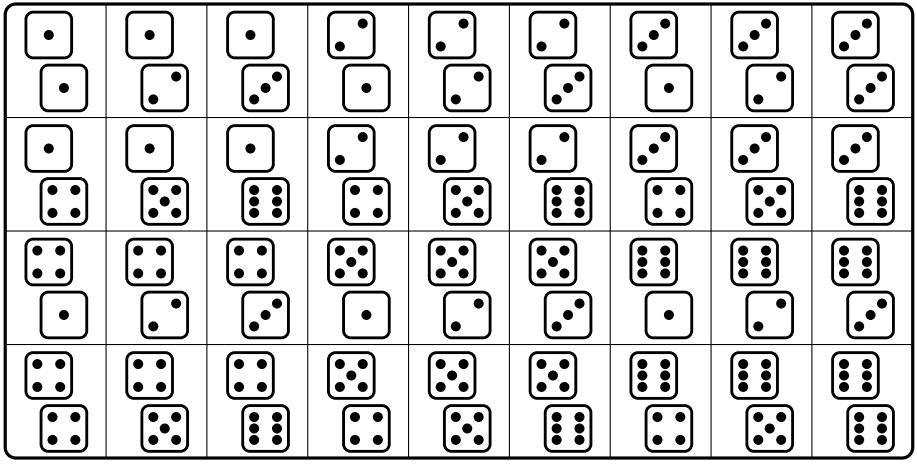
Contents

Outcomes



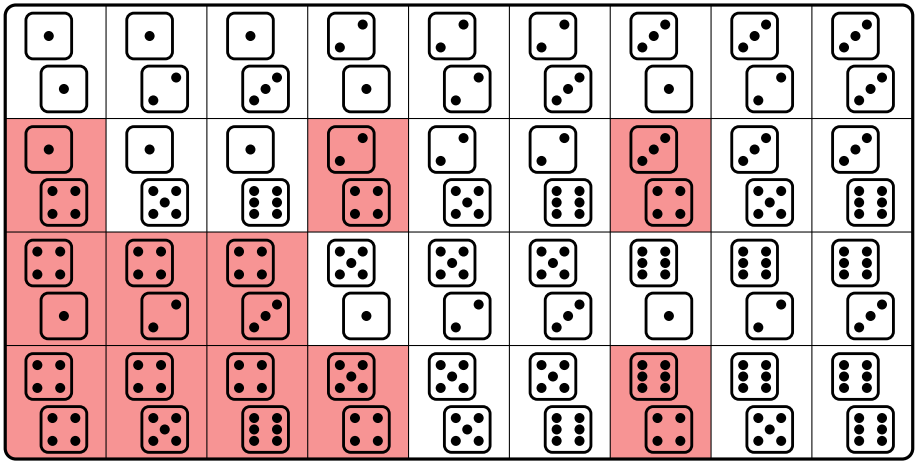
- Six outcomes: ⚀, ⚁, ⚂, ⚃, ⚄, ⚅
- $\Pr[⚀] = \Pr[⚁] = \Pr[⚂] = \Pr[⚃] = \Pr[⚄] = \Pr[⚅] = \frac{1}{6}$

Events



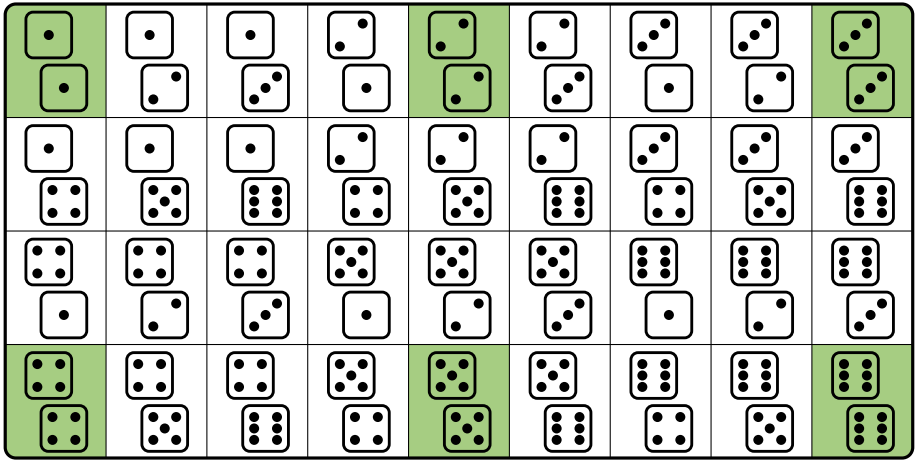
- 36 outcomes, each of probability 1/36

Events



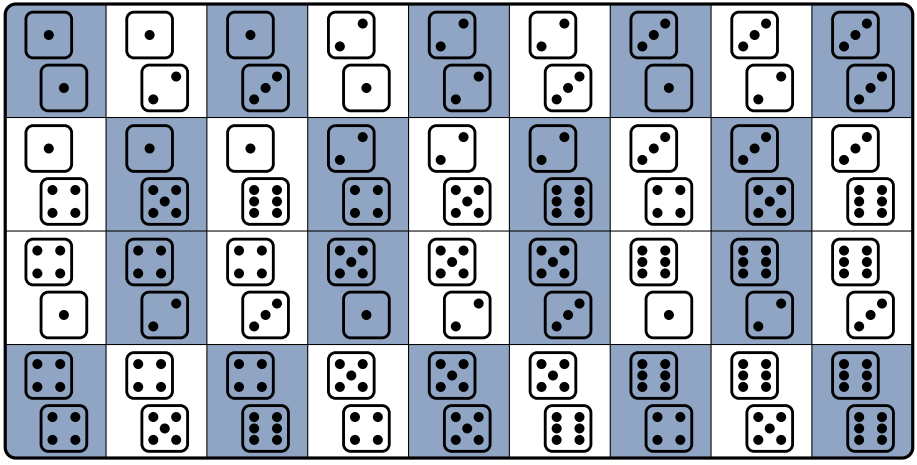
- 36 outcomes, each of probability 1/36
- Event: « at least one ⚄ » of probability 11/36

Events



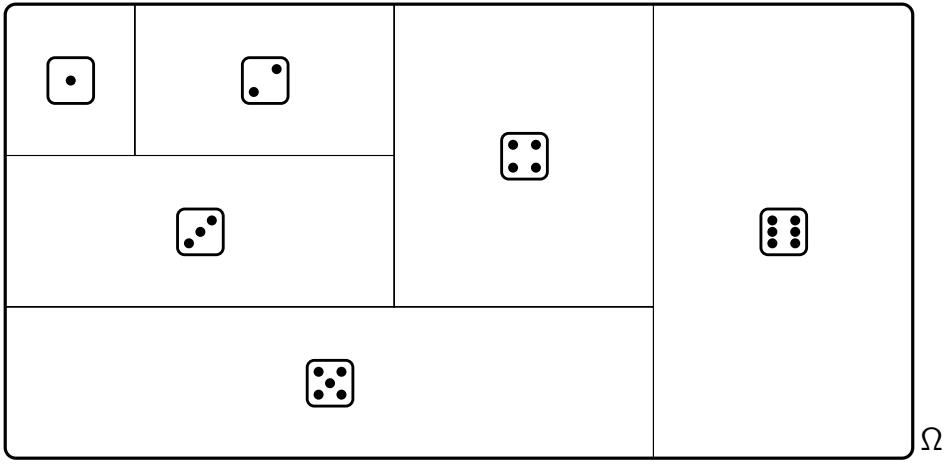
- 36 outcomes, each of probability $1/36$
- Event: « two identical dice » of probability $6/36 = 1/6$

Events



- 36 outcomes, each of probability $1/36$
- Event: « the sum is even » of probability $18/36 = 1/2$

Non-uniform distribution



$\Pr[\square] = \frac{1}{21}, \Pr[\square] = \frac{2}{21}, \Pr[\square] = \frac{3}{21}, \Pr[\square] = \frac{4}{21}, \Pr[\square] = \frac{5}{21}, \Pr[\square] = \frac{6}{21}$

Vocabulary, notations and pictures

Discrete probability space

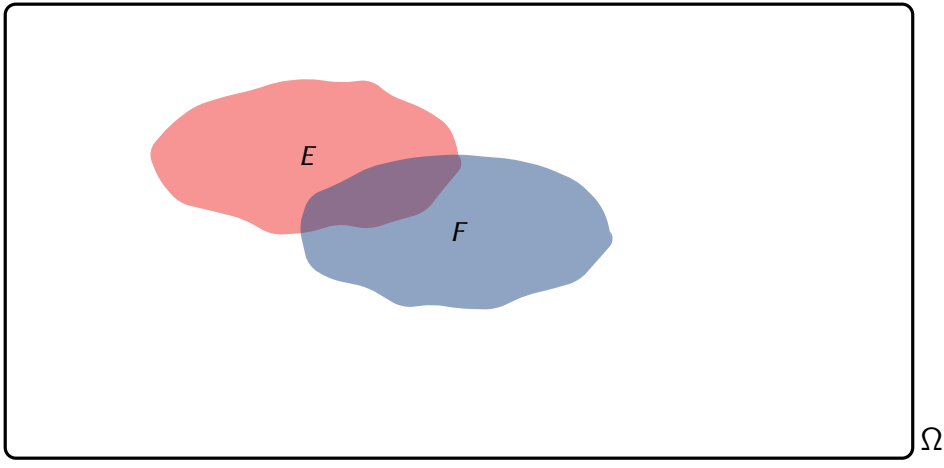
- Finite ou countable set Ω of possible *outcomes*
- Each outcome $\omega \in \Omega$ has a probability $\Pr[\omega]$ such that $\sum_{\omega \in \Omega} \Pr[\omega] = 1$
- An event E is a subset of Ω of probability $\Pr[E] = \sum_{\omega \in E} \Pr[\omega]$
  - $E \wedge F$ denotes the event $E \cap F = \{\omega : \omega \in E \wedge \omega \in F\}$ "E is true **and** F is true"
  - $E \vee F$ denotes the event $E \cup F = \{\omega : \omega \in E \vee \omega \in F\}$ "E is true **or** F is true"
  - $\neg E$ denotes the event $\Omega \setminus E = \{\omega : \omega \notin E\}$ "E is **not** true"

Understanding pictures: $\Pr[E]$ is the size of E!

- Ω is a rectangle of *size* 1 *measure* 1
  - the rectangle is split into disjoint zones, one of size $\Pr[\omega]$ for each $\omega \in \Omega$
- An *event* E is a part of the rectange, of size $\Pr[E]$

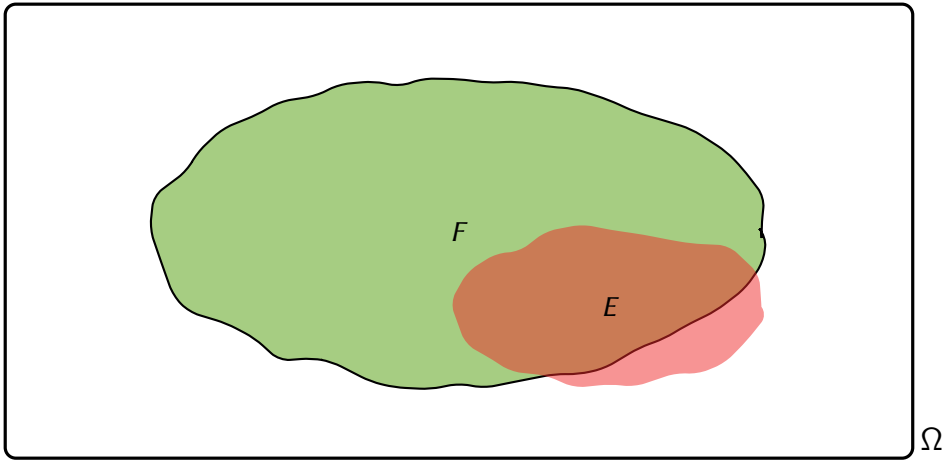
In the following, we forget about *outcomes*: they are special cases of *events*

Union bound



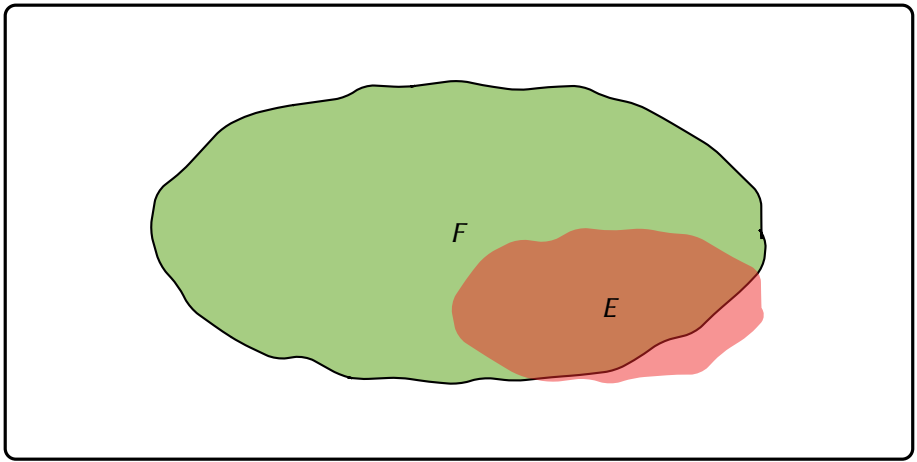
- $\Pr[E \vee F] = \Pr[E] + \Pr[F] - \Pr[E \wedge F] \leq \Pr[E] + \Pr[F]$
  - "The size of $E \vee F$ is $\leq$ the sum of the sizes of E and F"

Conditional probability: changing the universe



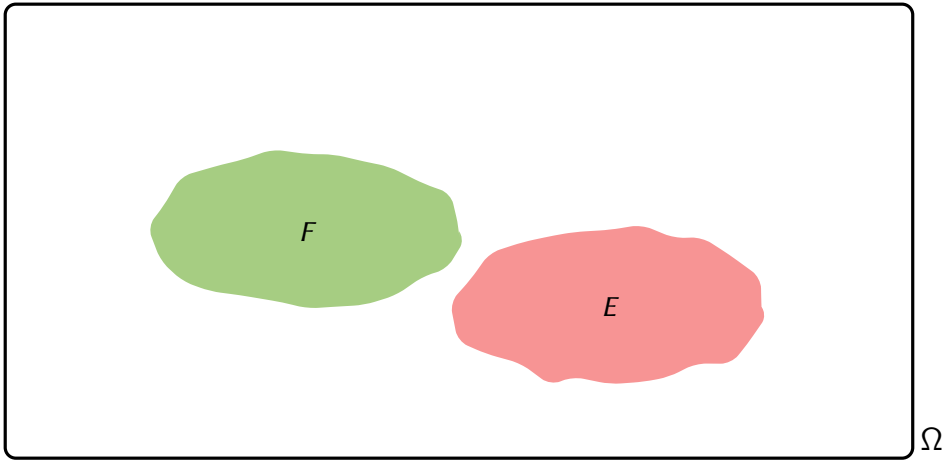
- $\Pr[E|F] = \Pr[E \wedge F] / \Pr[F]$: "probability of E knowing F"
  - probability of E *assuming the the universe is now* F: normalization $\Pr[F] \to 1$
  - $\Pr[E] = \Pr[E|\Omega]$ every probability is conditional

Independence



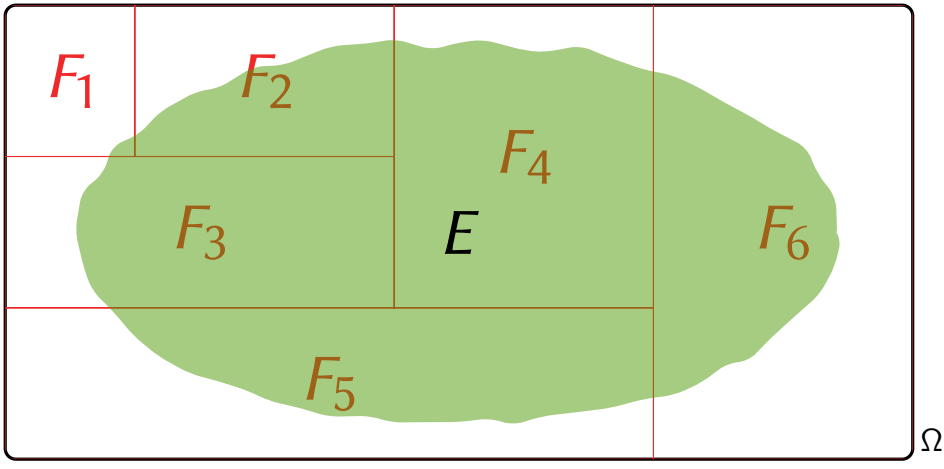
- E is *independent from* F if $\Pr[E] = \Pr[E|F]$ *E is as likely within F than within Ω*
- E is independent from $F \Leftrightarrow F$ independent from $E \Leftrightarrow \Pr[E \wedge F] = \Pr[E]\Pr[F]$

Beware: independent $\neq$ disjoint



- E and F are *disjoint* if $\Pr[E \wedge F] = 0$

Law of total probabilities: proof by exhaustion / case analysis



- $\Pr[E] = \sum_{i=1}^{n} \Pr[E \wedge F_i] = \sum_{i=1}^{n} \Pr[E|F_i] \Pr[F_i]$ if $\Omega = F_1 \sqcup F_2 \sqcup \cdots \sqcup F_n$
  - "to compute the size E, we split it according to the F_i's"

Birthday bounds

In a room of ≥ 23 people, two of them share the same birthday with probability $\geq \frac{1}{2}$

Theorem

Let $y_1, \ldots, y_q, z_1, \ldots, z_q$ be uniformly and independently drawn from a size-N set. Then

classical bound:	$1 - e^{-\frac{q(q-1)}{2N}}$	$\leq$	$\Pr[\exists i \neq j, y_i = y_j]$	$\leq$	$\frac{q(q-1)}{2N}$
variant:	$1 - e^{-\frac{q^2}{N}}$	$\leq$	$\Pr[\exists i, j, y_i = z_j]$	$\leq$	$\frac{q^2}{N}$

Special case

Since $1 - e^{-x} \geq \frac{1}{2}x$ for $0 \leq x \leq 1$,

If $q \leq \sqrt{2N}$,	$\frac{q(q-1)}{4N}$	$\leq$	$\Pr[\exists i \neq j, y_i = y_j]$	$\leq$	$\frac{q(q-1)}{2N}$
If $q \leq \sqrt{N}$,	$\frac{q^2}{2N}$	$\leq$	$\Pr[\exists i, j, y_i = z_j]$	$\leq$	$\frac{q^2}{N}$

Contents

The secret

A random variable is neither a variable nor random!

Definition

A (real) random variable $X : \Omega \to \mathbb{R}$ is a function from the universe to the reals

Events defined by random variables $X, Y : \Omega \to \mathbb{R}$

- "$X = 12$" is the event $\{\omega : X(\omega) = 12\}$
- "$X \leq 0$" is the event $\{\omega : X(\omega) \leq 0\}$
- "$X \neq Y$" is the event $\{\omega : X(\omega) \neq Y(\omega)\}$

Independence

- X and Y are independent if "$X = u$" and "$Y = v$" are independent for all $u, v \in \mathbb{R}$

All events we consider are defined using random variables

Expectation

The *expectation* of a random variable is its average value

Definition

The expectation of a random variable $X : \Omega \to \mathbb{R}$ is

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

- if Ω is finite/countable, the sum $\sum_{v \in \mathbb{R}}$ has only a finite/countable number of terms
- the expectation is defined *only if* the sum is well defined ($\neq \pm\infty$ for instance)

Visually

- $X(\omega)$ provides a *height* for the zone of ω within the rectangle Ω
- $\mathbb{E}[X]$ is the total volume of the 3d shape created

Properties of expectation

Linearity of expectation

For **all** random variables $X, Y : \Omega \to \mathbb{R}$ with a defined expectation,

$$\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y]$$

(addition of volumes)

Product of independent variables

For **independent** random variables $X, Y : \Omega \to \mathbb{R}$ with a defined expectation,

$$\mathbb{E}[X \times Y] = \mathbb{E}[X] \times \mathbb{E}[Y]$$

Expectation of integral variables

If $X : \Omega \to \mathbb{Z}_{\geq 0}$, $\mathbb{E}[X] = \sum_{i \geq 0} \Pr[X \geq i]$

Law of total expectation

Conditional expectation

- $\mathbb{E}[X \mid F] = \sum_{v \in \mathbb{R}} v \cdot \Pr[X = v | F]$ — expectation of X knowing F
  - expectation assuming the universe is now F — (volume restricted to F, normalized)

Law of total expectations

- $\mathbb{E}[X] = \sum_{i=1}^{n} \mathbb{E}[X \mid F_i] \Pr[F_i]$ — if $\Omega = F_1 \sqcup F_2 \sqcup \cdots \sqcup F_n$
  - volume computed as the sum of the volumes within universes F_i

Inequalities

Markov inequality

- If $X : \Omega \to \mathbb{R}_{\geq 0}$, $\Pr[X \geq \lambda \cdot \mathbb{E}[X]] \leq 1/\lambda$

Chernoff inequality

- Let $X_1, \ldots, X_n : \Omega \to \{0, 1\}$ be *independent* random variables
- Let $X = X_1 + \cdots + X_n$ and $\mu = \mathbb{E}[X]$
- Then for $0 \leq \delta \leq 1$,

$$\Pr\big[|X - \mu| \geq \delta\mu\big] \leq 2e^{-\delta^2\mu/3}$$

Contents

Bernoulli distribution

Toss a biased coin with probability p to get HEAD

Definition

- Outcomes: HEAD and TAIL
- Probabilities: $\Pr[\text{HEAD}] = p$, $\Pr[\text{TAIL}] = 1 - p$
- Random variable: $X(\text{HEAD}) = 1$, $X(\text{TAIL}) = 0$

Results

- $\Pr[X = 1] = p$
- $\mathbb{E}[X] = p \times 1 + (1 - p) \times 0 = p$

Uniform distribution

Throw an unbiased dice with n sides

Definition

- Outcomes: the n faces ⚀, ⚁, …
- Probabilities: $\Pr[⚀] = \Pr[⚁] = \cdots = 1/n$
- Random variable: $X(⚀) = 1$, $X(⚁) = 2$, …

Results

- $\Pr[X = i] = 1/n$ for all i
- $\mathbb{E}[X] = \sum_{i=1}^{n} i \cdot \frac{1}{n} = \frac{1}{2}(n+1)$

Binomial distribution

Toss n times, independently, a biased coin with probability p to get HEAD

Definition

- Outcomes: a list of n HEAD/TAIL
- Random variable: $X = X_1 + \cdots + X_n$ where is X_i is a Bernoulli random variable $\Pr[X_i = 1] = p$, $\Pr[X_i = 0] = 1 - p$

Results

- $\Pr[X = k] = \binom{n}{k} p^k (1-p)^{n-k}$
- $\mathbb{E}[X] = \sum_i \mathbb{E}[X_i] = np$

Geometric distribution

Toss a biased coin with probability p to get HEAD, until the first HEAD occurs

Definition

- Outcomes: a list of TAIL followed by a HEAD
- Random variable: $X : \Omega \to \mathbb{Z}_{>0}$ defined as the length of the list

Results

- $\Pr[X = k] = (1-p)^{k-1} \cdot p$
- $\mathbb{E}[X] = 1/p$

Random bit strings

Uniform random bit

- Bernoulli variable of parameter $p = \frac{1}{2}$

Uniform random bit string of length n

- Binomial variable of parameters $p = \frac{1}{2}$ and n
  - For a fixed string s, $\Pr[S = s] = 1/2^n$
  - $\mathbb{E}[\text{number of 1's}] = \frac{1}{2} \cdot n$

Random functions

Uniform random function $f : X \to Y$

- Uniform distribution on the set of the $\#Y^{\#X}$ functions
- Equivalent:
  - for each x, $f(x)$ is uniform in Y independently
  - uniform random string of length $\#X$ over the *alphabet* Y
  - case $Y = \{0, 1\}$: uniform random bit string of length $\#X$

Uniform random permutation $\pi : X \to X$

- Uniform distribution on the set of the $(\#X)!$ permutations
  - Ex.: permutations of the set of length-n bit strings: set of size $(2^n)!$