Oct27

Tuesday, October 27, 2020 9:58 PM

A brief foray into probability theory

In implementing RSA there were a few thing we "left to chance"

↑albeit in a controlled way.

① probably Prime (p):

* chose a random $a < p$
* tests to see if a is a MR witness for p being composite.
* Repeats x20.

→ If any a is a witness. p is composite 100%.

→ If no a is a witness, then p is "very likely" prime.

↑ what does this mean?

If p composite:

✱
* a has > 75% chance of being an MR witness
* a has < 25% change of not being

one.

* We have a $(.25)^{20}$ chance of picking 20 nonwitnesses

$\underbrace{0.00000000009\%}_{*}$

⚠ Tempting to say that this implies $1-(.25)^{20}$ chance p is prime if get 20 nonwitnesses.

* Probabilities depend on p being composite.

Example
If no primes in our range & probPrime(p) returns true, still 0% chance that p is prime!!

upshot
Relationship btwn prob that composite # returns true on probablyPrime & chance that a # that returns true is prime depends on overall prob that a random # in our range is prime.

→ Conditional probability & Bayes' thm allow us to formalize this relationship.

→ We will do this to finish prob 7 on TH9.

② findPrime (lower, upper).

→ guessed random #s btwn lower & upper.

→ Checked if they were prime (used probablyPrime(n))

Ex

For me, my algorithm found a 500 digit in ≈ 700 guesses on average.

↑ why?

Remarkably, this worked!!

How long should I expect it to take?

These first 2 examples measure practicality of implementing algorithms.

③ Measuring resistance to attacks

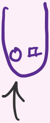
- Resistance to brute force attacks.
- Collision Algorithms
  - ↑ attacks using clever guessing
- Probabilistic attacks.

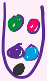
Review of Counting

(§5.1 in [HPS])

Example

2 jars





Pick an object from each jar.

Q. How many possible outcomes?

(square or circle) (1 out of 5 colors)

↑ ↑

$2 \cdot 5 = 10.$

Counting Principle

2 indep experiments

Exp 1 has n outcomes $\{x_1, \dots, x_n\}$

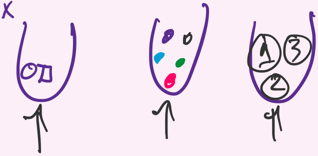
Exp 2 has m outcomes $\{y_1, \dots, y_m\}$

Total # outcomes is $n \cdot m$

Proof Correspond to pairs (x_i, y_j)

This extends to arbitrarily many exps

Ex



$2 \cdot 5 \cdot 3 = 30$ total possible outcomes.

Prop k experiments w/ outcomes $E_1, \dots, E_k$, each experiment has n_i outcomes S_i. Total # possible outcomes is $n_1 n_2 \cdots n_k$.

Pf/ Counting tuples in $S_1 \times S_2 \times \dots \times S_k$ (induction on k).

Permutations

Example: How many ways can we reorder the #'s 1 through 10.

8, 2, 1, 7, 5, 3, 4, 6, 9, 10

10 choices

can't choose 8
9 choices

- - - - -

only 10 remains
1 choice.

$10 \cdot 9 \cdot 8 \cdot \dots \cdot 1 = 10! = 3628800$

counting principle.

Defn Let S be a set containing n objects. A permutation of S is an ordered list of the elts of S.

* If $n \in \mathbb{N}$, a permutation of n is a permutation of set $\{1, 2, \dots, n\}$

Prop If S is a set of n elts, there are $n!$ permutations of S.

Pf/ Same as example above ∅

Remark

$$\begin{tikzcd}
\text{Permutations } \{a_1, \dots, a_n\} \arrow[r, leftrightarrow] & \left\{ \text{Bijections } \{1, 2, \dots, n\} \to \{1, 2, \dots, n\} \right\}
\end{tikzcd}$$

$$a_{\phi(1)}, a_{\phi(2)}, \dots, a_{\phi(n)} \longleftarrow\!\shortmid \ \phi$$

$$a_{i_1}, a_{i_2}, \dots, a_{i_n} \longmapsto \phi(k) = i_k.$$

This set is naturally a group under composition.
Called Symetric group S_n.

Example

Substitution cipher.

$$\{A, B, \cdots, Z\} \xrightarrow{\pi} \{A, B, \cdots, Z\}$$

$$A \longmapsto \pi(A)$$

$$B \longmapsto \pi(B) \neq \pi(A)$$

$$\vdots \qquad \vdots$$

is same as a permutation of alphabet.

There are 26! of these.

Important Example

Permutations w/ indistinguishable objects.

$$S = \{A, A, A, B, B\}$$

How many ways can they be arranged?

$\leq 5!$

But AABBA could arise twice as a naive permutation of a 5 elt set.

$$S = \{A_1, A_2, A_3, B_1, B_2\}$$

$$\left\{ \begin{array}{l} A_1 A_3 B_2 B_1 A_2 \\ A_3 A_2 B_1 B_2 A_1 \end{array} \right\} \text{Same}$$

5! total permutations. But I overcount stuff like

Question

How many ways can I acheive same result?

① Permute A_1, A_2, A_3 ← 3!

② Permut B_1, B_2 ← 2!

$\Longrightarrow$ $3! \cdot 2!$ ways I can get same result.

↑ can get AABBA 12 ways

So total #

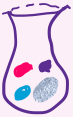
$$\boxed{10} = \frac{5!}{3! \cdot 2!}$$

← naive permutations

← each permutation appears this many times.

Combinations

Example



Pick 3 balls

What are total # of outcomes?

$4 \cdot 3 \cdot 2 = 24$ ← True if you care about order.

first ball

second

What if I care about which 3 balls?

● ● ● same ● ● ● ← any permutation of 3 balls gives same outcome.

$$\frac{4 \cdot 3 \cdot 2}{3!} = 4$$

← looks right. b/c # of outcomes of remaining ball.

Instead 20 balls in urn.

$$\nearrow \frac{20\cdot 19\cdot 18}{3!}\cdot\frac{17!}{17!} = \frac{20!}{3!\cdot 17!} \leftarrow \text{convenient}$$

Def^n

S be a set of n elements. A combination of r objects in S is a subset of r distinct elts of S (unordered).

Prop/Def^n

The number of all such combinations is

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

$\nwarrow$ n choose r.

Rmk $0! = 1$ by convention

$$\binom{n}{0} = \frac{n!}{0!\,n!} = 1 \leftarrow \text{only 1 way to choose 0 things.}$$

$$\binom{n}{n} = \frac{n!}{n!\cdot 0!} = 1 \leftarrow \text{only one way to choose everything.}$$

Pf/ # ways to choose r elts

$x_1, x_2, \dots, x_r$

ordered $\rightarrow$

$$\frac{n\cdot(n-1)\cdot(n-2)\cdots(n-r+1)}{r!}\cdot\frac{(n-r)!}{(n-r)!} = \frac{n!}{r!(n-r)!}$$

Application: Binomial Theorem.

$$(x+y)^n = \sum_{j=1}^{n} \underset{\uparrow}{\binom{n}{j}} \underset{\wedge}{\underline{x^j y^{n-j}}}$$

Pf/ $(x+y)^3 = (x+y)(x+y)(x+y) = x^3 + 3x^2y + 3xy^2 + y^3$

what is coeff of x^2y?

(foiling). x^2y appears by choosing x in 2 terms & y in 3rd

Choose 2 terms for x appear in

$\underline{1,2, \quad 1,3, \quad 2,3}$ ← choose 2 elts from a set of 3

$$\binom{3}{2} = \frac{3!}{2! \cdot 1!} = 3$$

In general

$$(x+y)^n = (x+y)(x+y)\cdots(x+y)$$

Coeff of $x^j y^{n-j}$ is I need to count # of times $x^j y^{n-j}$ appers when distributing.

Each apperence amounts to choosing j binomials for x, (the remaining will be y).

$\binom{n}{j}$ ways to do this

Probability Theory (Basics)

Probability Space: 2 peices

① Finite set Ω consisting of all possible outcomes of an experiment.

② A method for assigning probabilities to any given outcome:

$$\begin{array}{ccc} \Pr : \Omega & \longrightarrow & \mathbb{R} \\ \rotatebox{90}{$\in$} & & \\ \omega & \longmapsto & \Pr(\omega) \\ & & \rotatebox{90}{$=$} \\ & & \text{"probability that } \omega \text{ occurs"} \end{array}$$

Examples

① A single coin toss.

$\Omega = \{\text{Heads}, \text{Tails}\}$

$$\Pr : \Omega \longrightarrow \mathbb{R}.$$

$\Pr(H) = 1/2$

$\Pr(T) = 1/2$

② Roll of 2 dice. (red die & blue die)

$\Omega = \{(n, m) \mid n, m = \{1, \dots, 6\}\}.$

Each roll is equally likely. (unsatisfying for the lazy).

$\Pr(m, n) = 1/36.$

③ An urn w/ 100 balls.

21 are red. 79 are blue.

Choose 10 balls @ random.
What is probability of ↑exactly 3 red.

→ Select 3 red balls

$\binom{21}{3}$ ← # ways

→ Select 7 blue balls

$\binom{79}{7}$ ←

Total # ways I can get 3 red & 7 blue
is $\binom{21}{3}\binom{79}{7} = 20271005$ ← # good outcomes

Total # ways of picking 10 balls ← # outcomes

$\binom{100}{10} = 91015876$

Prob of picking exactly 3 reds is

$$\to \frac{\binom{21}{3}\binom{79}{7}}{\binom{100}{10}} = .223 \leftarrow$$

---

④ Roll 2 dice. How likely to get at least 1 6?

$\{(1,6),(2,6),(3,6),\dots,(6,6),(6,5),\dots,(6,1)\}$
↑ 11

36 total rolls. so $\frac{11}{36}$.

↳ Instead

$$\frac{1}{6} + \frac{1}{6} - \frac{1}{36} = \frac{11}{36}$$

(inclusion exclusion)

↑ first die is a 6

← second die a 6

← double counted (6,6)

Subdivided our event (at least 1 6) into 2 known events (first (or second) a 6) & made sure we didn't overcount.

Goal: Compute compound probs from known ones in systematic ways.

Defn A prob space is
A sample space (or set of outcomes) which is a nonempty finite* set together w/ a function $Pr: \Omega \to \cancel{\mathbb{R}}\ [0,1]$ assigning a prob to each outcome in $\omega \in \Omega$. Satisfying.

① $0 \leq Pr(\omega) \leq 1$ $\quad Pr(\omega)=0$ ← never, $Pr(\omega)=1$ ← always.

② $\sum_{\omega \in \Omega} Pr(\omega) = 1$ ← some outcome must occur.

Defn An event is any subset $E \subseteq \Omega$.

The probability of an event occurring is the sum of the probabilities of each outcome in that event.

$$Pr(E) := \sum_{\omega \in E} Pr(\omega).$$

↑ e.g. at least on 6