Combinatorics

The Mathematics of Counting

Lecture notes of Alexander Wood
CSCI 360 Cryptography and Cryptanalysis
awood@jjay.cuny.edu

John Jay College of Criminal Justice

How hard is it to count?

Let's say you and a friend decide to flip a coin twice. How many possible heads-tails combinations are there?

What if you flip it three times?

How hard is it to count?

What if instead of coins, you are rolling two dice? Three dice? Twenty dice?

How hard is it to count?

What if instead of coins, you are rolling two dice? Three dice? Twenty dice?

A die has 6 sides. Thus there are six possible outcomes for the first die, and six for the second, resulting in a total of $6 \times 6 = 36$ outcomes.

Three dice: $6 \times 6 \times 6 = 6^3$ outcomes.

Twenty dice: 6^{20} outcomes.

HOLD UP! Exponent Review!

- **Zero-Exponent Rule:** $a^0 = 1$ for any number a.
- **Power Rule:** $(a^m)^n = a^{mn}$
- **Negative Exponent Rule:** $a^{-m} = \frac{1}{a^m}$ and $\frac{1}{a^{-m}} = a^m$.
- **Product Rule:** $a^m a^n = a^{m+n}$
- **Quotient Rule:** $\frac{a^m}{a^n} = a^{m-n}$

Exponents Examples

- $1000^0 = 1$
- $(4^2)^7 = 4^{14}$
- $7^{-1} = \frac{1}{7}$
- $\frac{1}{a^{-3}} = a^3$
- $6^2 6^8 = 6^{10}$

Exponents Examples

$$2^8 4^6 = 2^8 (2^2)^6 = 2^8 2^{12} = 2^{20}$$

$$\left(\frac{x^2}{y^5}\right)^{-2} = \frac{(x^2)^{-2}}{(y^5)^{-2}} = \frac{x^{-4}}{y^{-10}} = \frac{y^{10}}{x^4}$$

For more exponents examples, visit this helpful webpage:
`http://www.mesacc.edu/~scotz47781/mat120/notes/exponents/review/review.html`

Counting, without counting!

We would like to determine how many possible combinations there are given various conditions and properties.

With flipping a couple coins it is easy, but what about flipping 100 coins?

With some mathematics and a bit of clever thinking, we can count all sorts of things.

HOLD UP! Logical Operators, aka, and vs. or

Logical operators return Boolean (TRUE or FALSE) values.

- **and**: `condition1 AND condition2` evaluates to True if and only if both `condition1` and `condition2` are true.
- **or**: `condition1 OR condition2` evaluates to True if and only if at least one of `condition1` and `condition2` is true.
- **not**: `NOT condition` reverses the truth value of the condition.

The Sum Principle

If there are m ways to do A and n ways to do B, then the number of ways to do A **or** B is $m + n$.

The Sum Principle

For example, say you are making dinner. There are four ways you could prepare a chicken dish, and three ways you could prepare a steak dish.

How many ways could you make a chicken dish *or* a steak dish? Seven.

The Product Principle

Say there are m ways to do A and n ways to do B. The number of ways to do A **and** B is $m \times n$.

Note that here, the ways of doing A and the ways of doing B are *independent*, meaning they do not depend on one another. (For dependent choices, see slide 7)

Example: Subcommittees

Say there are 5 members of your student council. How many possible ways could a subcommittee be formed?

Solution 1: Subcommittees

- There are $N1$ ways of forming 1-member subcommittees
- There are $N2$ ways of forming 2-member subcommittees
- There are $N3$ ways of forming 3-member subcommittees
- There are $N4$ ways of forming 4-member subcommittees
- There are $N5$ way(s) of forming a 5-member subcommittees
- By the sum principle, there are

$$N = N1 + N2 + N3 + N4 + N5$$

ways of forming the subcommittee.

Solution 2: Use the Product Principle

Each student council member is either in the committee, or not in the committee. Thus it is much simpler to apply the product principle.

$$2 \times 2 \times 2 \times 2 \times 2 = 2^5 = 32$$

possible committee combinations.

A bad calculation

The math here is incorrect. How many things would they actually need to try?

Combinatorics and Security: PINs

Each digit in your PIN can be one of 10 values (0, 1, 2, . . . , 9). Your PIN is four numbers long. How many possible PIN numbers are there?

Combinatorics and Security: PINs

Each digit in your PIN can be one of 10 values (0, 1, 2, . . . , 9). Your PIN is four numbers long. How many possible PIN numbers are there?

There are 10 choices for each value, so there are

$$10 \times 10 \times 10 \times 10 = 10^4 = 10,000$$

possible PIN choices.

Combinatorics and Security: PINs

Say you are trying to break into someone's bank account. You can try one PIN every 5 seconds. How long would it take to check every combination?

Combinatorics and Security: PINs

Say you are trying to break into someone's bank account. You can try one PIN every 5 seconds. How long would it take to check every combination?

Solution:

$$10,000 \text{ combinations} \times 5 \text{ seconds} = 50,000 \text{ seconds}$$

or 13 hours, 53 minutes, and 20 seconds.

Combinatorics and Security: PINs

Say that you are only able to try entering the PIN 10 times before the system locks you out. What is your probability of success?

Combinatorics and Security: PINs

Say that you are only able to try entering the PIN 10 times before the system locks you out. What is your probability of success?

You can try 10 out of 10,000 possible combinations, so your probability of success is

$$\frac{10}{10,000} = \frac{1}{1,000} = 0.001 = 0.1\%$$

How hard is it to count?

You'd like to visit all 5 boroughs of NYC. How many different ways can you do this?

How hard is it to count?

You'd like to visit all 5 boroughs of NYC. How many different ways can you do this?

There are 5 ways to pick the first borough, 4 ways to pick the second, 3 ways to pick the third, 2 ways to pick the fourth, and 1 way to pick the last. Thus there are

$$5! = 5 \times 4 \times 3 \times 2 \times 1$$

HOLD UP! What's a factorial?!

Factorials are just products. For a positive integer n define

$$n! = n(n-1)(n-2)\cdots(2)(1)$$

Examples:

- $4! = 4(3)(2)(1) = 24$
- $6! = 6(5)(4)(3)(2)(1) = 720$

Permutations Example

Sarah, Juan, and Belle take a cab to the movies and sit in the back seat. How many possible ways are there that they can sit in the back of the cab?

Permutations Example

Sarah, Juan, and Belle take a cab to the movies and sit in the back seat. How many possible ways are there that they can sit in the back of the cab?

There are three choices for who sits on the left, two choices for who sits in the middle, and one remaining choice for who sits on the right. Thus there are

$$3! = 3 \times 2 \times 1 = 6$$

ways for them to arrange themselves in the back seat.

Permutations

A **permutation**, or an **ordering**, is the number of ways of arranging items in some order. The number of permutations of n objects is given by $n!$.

Even more permutations

We have five letters, (A, B, C, D, E), and we wish to find all possible permutations of three of these letters. For example, ABC, CBA, ABD, CDE, EBC, etc.

Even more permutations

We have five letters, (A, B, C, D, E), and we wish to find all possible permutations of three of these letters. For example, ABC, CBA, ABD, CDE, EBC, etc.

There are five choices for the first letter, four choices for the second letter, and three choices for the second letter.

$$5 \times 4 \times 3 = 60 \text{ choices}$$

Permutations

The number of permutations of n objects taken k at a time is given by

$$\frac{n!}{(n-k)!} = n(n-1)\cdots(n-k+1)$$

Permutations & Security

You decide to disguise a message by replacing each of 26 English letters with a letter from a Chinese character dictionary you own, picking from the 30 most frequently-used characters. How many possible ways could you set up your cipher?

Permutations & Security

You decide to disguise a message by replacing each of 26 English letters with a letter from a Chinese character dictionary you own, picking from the 30 most frequently-used characters. How many possible ways could you set up your cipher?

This is a permutation problem! We want to know how many possible ways we can associate each letter in the English language with one of 30 Chinese characters. In other words, how many permutations of these 30 characters are there, taken 26 at a time?

$$\frac{30!}{(30-26)!} = \frac{30!}{4!} = 1105220249217462744317952000000$$

Combinations Example

How many ways are there to choose 4 letters out of 7 letters?

Combinations Example

How many ways are there to choose 4 letters out of 7 letters?

There are $\frac{7!}{(7-4)!} = 840$ permutations of 4 letters taken from 7 letters. However, now we need to discard all permutations, since ABCD, DCBA, BADC, etc, are all the same case now.

Combinations Example

How many ways are there to choose 4 letters out of 7 letters?

There are $\frac{7!}{(7-4)!} = 840$ permutations of 4 letters taken from 7 letters. However, now we need to discard all permutations, since ABCD, DCBA, BADC, etc, are all the same case now.

Note that each four-letter choice has 4! permutations. Thus the total number of ways to choose four letters out of seven letters is

$$\frac{7!}{4!(7-4)!} = 35$$

Combinations

The number of possible ways of picking k (unordered) outcomes from n possibilities is called the number of **combinations**, or the **binomial coefficient**. It is denoted by $\binom{n}{k}$, pronounced "n choose k," and given by

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

Exercise 1

A door lock has a key pad with the numbers 1 through 9. The key to the door consists of a sequence of six digits. How many possible keys are there?

Solution 1

There are 9^6 possible keys.

Exercise 2

A gym lock dial has 50 numbers, and you unlock it by turning the dial 3 times to 3 numbers. If a thief can check 6 combinations per minute, how long will it take the thief to check all possible combinations?

Solution 2

There are 50^3 possible lock combinations. At a rate of 6 per minute, it will take the theif

$$\frac{50^3}{6} = 20833.\bar{3} \text{ minutes}$$

or 14 days, 11 hours, 13 minutes, and 20 seconds.

Exercise 3

A nuclear missile launcher requires 6 physical keys to be activated. These 6 keys are stored in a box with 30 other decoy keys. If someone was to grab 6 keys from this cabinet, what is the likelihood that they could launch the missile?

Solution 3

The order in which we pick the keys does not matter, as long as we pick all 6 of the correct keys. Thus we first wish to deduce how many possible ways there are to choose 6 keys out of 36 keys (decoy keys plus real keys). This is given by

$$\binom{36}{6} = 1,947,792 \text{ possibilities}$$

Solution 3 cont.

Only one of these possible ways of grabbing the keys is correct, so the probability of randomly grabbing the correct key combo is given by

$$\frac{1}{1947792} \approx 5.13 \times 10^{-7} = 0.0000513\%$$

Quiz Next Week!

Some sample problems will be posted on the course Piazza page. You can use the Piazza platform to discuss any problems you get stuck on with your classmates and myself.

References and Further Reading

- http://www.cs.cornell.edu/courses/cs280/2004fa/280wk6_x4.pdf