

Lecture 18 - Counting

6.042 - April 24, 2003

One of the most common mathematical problems in computer science is counting the number of elements in a set. This is often the core difficulty in determining a program's running time and memory consumption. Counting also comes up in the analysis of communications networks and is at the root of almost every complicated probability problem. We'll see several of the most useful counting techniques in this course, but this is only the tip of the iceberg. There is an entire subfield of mathematics, *enumerative combinatorics*, devoted to this task.

1 Three Simple Rules

Let's begin with three simple counting rules.

Rule 1 (Sum Rule) *Let A and B be finite, disjoint sets. Then:*

$$|A \cup B| = |A| + |B|$$

Rule 2 (Product Rule) *Let A and B be finite sets. Then:*

$$|A \times B| = |A| \cdot |B|$$

In contrast to the sum rule, the sets A and B in the product rule need not be disjoint. As an example of the product rule, let's count the number of different n -bit strings. Formally, we want to find the cardinality of the set:

$$\{0, 1\}^n = \underbrace{\{0, 1\} \times \{0, 1\} \times \dots \times \{0, 1\}}_{n \text{ terms}}$$

By the product rule, we have:

$$\begin{aligned} |\{0, 1\}^n| &= |\{0, 1\}|^n \\ &= 2^n \end{aligned}$$

Rule 3 (Bijection Rule) *Let A and B be finite sets. If there exists a bijective function $f : A \rightarrow B$, then:*

$$|A| = |B|$$

The bijection rule is like induction and the pigeonhole principle, in the sense that it is an “obvious” statement that leads to very nonobvious conclusions when cleverly applied. But let’s start with a not-so-clever application of the bijection rule. Let S be the set $\{x_1, x_2, \dots, x_n\}$. How many different subsets does S have?

We can solve this problem by constructing a bijection $f : A \rightarrow B$, where A is the set of all n -bit strings and B is the set of all subsets of S . In particular, let a be an n -bit string, and let $f(a)$ be the subset of S that contains element x_i if and only if the i -th bit of a is a 1. For example, we would map the 10-bit string 0100111011 to a subset of $\{x_1, x_2, \dots, x_{10}\}$ as follows:

$$\begin{array}{rcl} a & = & \{ 0, 1, 0, 0, 1, 1, 1, 0, 1, 1 \} \\ S & = & \{ x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10} \} \\ f(a) & = & \{ x_2, x_5, x_6, x_7, x_9, x_{10} \} \end{array}$$

In this case, it is pretty clear that this mapping is a bijection. Sometimes this is not so obvious and a proof is required. The existence of such a bijection implies that $|B| = |A| = 2^n$.

In general, the set of all subsets of a set S is denoted 2^S and is called the *power set* of S . The reason for this notation is apparent from the preceding analysis: the power set of S has $2^{|S|}$ elements.

2 Permutations

Definition 1 *An r -permutation of a set T is a sequence of r distinct elements of T .*

For example, the 2-permutations of the set $\{A, B, C, D\}$ are the sequences:

$$\begin{array}{cccccc} (A, B) & (A, C) & (A, D) & (B, A) & (B, C) & (B, D) \\ (C, A) & (C, B) & (C, D) & (D, A) & (D, B) & (D, C) \end{array}$$

How many r -permutations of an n -element set are there? Intuitively, there are n ways to choose the first element of an r -permutation, $n - 1$ ways to choose the second element, $n - 2$ ways to choose the third, etc. Finally, there are $n - r + 1$ ways to choose the r -th element. A routine induction confirms this intuition.

Rule 4 (number of r -permutations) *The number of r -permutations of an n -element set is denoted $P(n, r)$ and equal to:*

$$\begin{aligned} P(n, r) &= n \cdot (n - 1) \cdot (n - 2) \cdots (n - r + 1) \\ &= \frac{n!}{(n - r)!} \end{aligned}$$

In the example above, we listed all the 2-permutations of the 4-element set $\{A, B, C, D\}$. Sure enough, we found $4!/2! = 12$.

2.1 Special Dollar Bills

The serial number on a dollar bill has 8 digits. What is the probability that all the digits are distinct? As a first step, we can use the product rule to determine how many serial numbers are possible overall:

$$\begin{aligned} |\{0, 1, 2, 3, \dots, 9\}^8| &= |\{0, 1, 2, 3, \dots, 9\}|^8 \\ &= 10^8 \end{aligned}$$

If we assume that all serial numbers are equally likely, then each serial number must appear with probability $1/10^8$. Now the serial numbers with all digits distinct are precisely the 8-permutations of the 10-element set $\{0, 1, 2, 3, \dots, 9\}$. Thus, there are $P(10, 8)$ such serial numbers. Therefore, the probability of the event that a random serial number has all digits distinct is:

$$\begin{aligned} \Pr \{\text{all digits distinct}\} &= \frac{P(10, 8)}{10^8} \\ &= \frac{10!}{10^8 \cdot 2!} \\ &\approx 0.0181 \end{aligned}$$

So only about 1 dollar bill in 55 has a serial number with no digit appearing more than once.

3 The Division Rule

Counting often requires a bit of fudging. That is, it may be convenient to initially overcount the number of elements in a set and afterward introduce a corrective “fudge factor” to get the

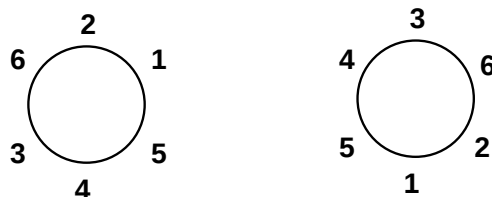
real answer. For example, we could determine the number of people in a room by counting ears. Of course, this means that everyone is initially counted twice. But then dividing by a fudge factor of 2 gives the correct number of people in the room. The term “fudge factor” suggests imprecision, but the *division rule* makes this an exact procedure.

Rule 5 (Division Rule) *Let A and B be finite sets, and suppose that $f : A \rightarrow B$ maps exactly k distinct elements of A to each element of B . Then $|A| = k \cdot |B|$.*

A function of the sort described in this rule is called a *k-to-1 function*, because k distinct elements of the domain are mapped to each element of the range.

3.1 Knights at the Round Table

In how many ways can King Arthur seat n knights at his round table? Two seatings are considered equivalent if one can be obtained from the other by rotation. For example, the following two arrangements are equivalent:



Let A be the set of all ways to line up the n knights against a wall, and let B be the set of all possible seating arrangements at the round table. We can map each lineup in set A to a circular seating arrangement in set B by seating the first knight in the lineup anywhere, putting the second knight to his left, the third knight to the left of the second, and so forth all the way around the table. This is an n -to-1 function. To see why, consider the reverse procedure; given a circular seating arrangement, we can “cut” the circle at n different points to produce n different lineups. Therefore, by the division rule, the number of circular seating arrangements is:

$$\begin{aligned} |B| &= \frac{|A|}{n} \\ &= \frac{n!}{n} \\ &= (n-1)! \end{aligned}$$

The first step uses the division rule. The second uses the fact that there are $P(n, n) = n!$ ways to line up the knights.

4 Combinations

Definition 2 An r -combination of a set T is a subset of T with exactly r elements.

For example, the 2-combinations of the set $\{A, B, C, D\}$ are the subsets:

$$\begin{array}{ccc} \{A, B\} & \{A, C\} & \{A, D\} \\ \{B, C\} & \{B, D\} & \{C, D\} \end{array}$$

Notice that permutations are *sequences*, but combinations are *sets*. Thus, (A, B) and (B, A) are two *different* permutations, but $\{A, B\}$ and $\{B, A\}$ are just two ways of describing the *same* combination.

Naturally, the next step to count r -combinations.

Rule 6 (number of r -combinations) The number of r -combinations of an n -element set is denoted $C(n, r)$ and equal to:

$$\begin{aligned} C(n, r) &= \frac{P(n, r)}{r!} \\ &= \frac{n!}{r! (n - r)!} \end{aligned}$$

The proof of this fact uses the division rule. There is a natural mapping from r -permutations to r -combinations: map the r -permutation $(x_1, \dots, x_r)$ to the r -combination $\{x_1, \dots, x_r\}$. This mapping is $r!$ -to-1, because every r -permutation with the same elements in a different order is also mapped to the same r -combination. Therefore, there are $r!$ times more r -permutations than r -combinations, as claimed.

We used $C(n, r)$ above to denote the number of r -combinations of an n -element set. However, there is a special notation for this quantity that is more commonly used:

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

The expression $\binom{n}{r}$ is read “ n choose r ”, which is a terse reference to quantity it represents, “the number of ways to choose r distinct elements from a set of n elements”. Numbers of the form $\binom{n}{r}$ are often called “binomial coefficients”, because of their appearance in the famous Binomial Theorem.

There are an enormous number of identities involving binomial coefficients. Perhaps the simplest is:

$$\binom{n}{r} = \binom{n}{n-r}$$

This identity is easy to prove algebraically; replace each binomial coefficient by the equivalent expression involving factorials and note that they are identical. However, there is another proof that uses no algebra at all! Let's count the number of ways to choose r distinct elements from a set of size n in two different ways. On one hand, our counting rule says that this can be done in $\binom{n}{r}$ ways. On the other hand, we could choose the r elements by an alternative procedure: choose $n - r$ elements, throw those out, and take the r elements that remain. Our counting rule says that we can throw out $n - r$ elements in $\binom{n}{n-r}$ different ways. Therefore, $\binom{n}{r}$ and $\binom{n}{n-r}$ both count the number of ways to choose r distinct elements from a set of size n , and so the two expressions must be equal!

An argument of this type is called a *combinatorial proof*. The general idea is that counting the elements of the same set in two different ways must give expressions that are equal. As another example, let's prove the following identity combinatorially:

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

We'll count the number of subsets of a set of size n in two different ways. On one hand, we earlier used a bijection with binary strings to show that an n -element set has 2^n subsets. On the other hand, each subset of an n -element set contains between 0 and n elements, and there are $\binom{n}{k}$ ways to choose a subset of size k . Therefore, there are $\sum_{k=0}^n \binom{n}{k}$ different subsets of an n element set in all. We've shown that the two sides of the equation above are both equal to the number of subsets of an n -element set and therefore they must be equal to each other.

Combinatorial proofs are perfectly valid and are often much more convincing than the reams of algebra that might otherwise be needed to prove an identity.

5 Poker

We now have a critical mass of counting rules. By combining them in various ways, we can solve a wide range of counting problems. And we can also handle a lot of probability problems that boil down to counting. As an exercise, let's compute the probabilities of some poker hands.

A poker hand consists of 5 cards chosen from a 52-card deck. Thus, there are $\binom{52}{5}$ different poker hands in all. Let's assume that hands are dealt from a well-shuffled deck so that every hand is equally likely.

Recall that each card has a *suit* ($\clubsuit$, $\diamondsuit$, $\spadesuit$, or $\heartsuit$) and a *rank* (ace, 2, 3, ..., 10, jack, queen, or king). Two cards of the same rank are called a *pair*, and three cards of the same rank are called a *3-of-a-kind*. A hand containing both a pair and a three-of-a-kind is called a *full house*. For example, here is one possible full house:

$$7\heartsuit 7\clubsuit 10\clubsuit 10\diamondsuit 10\spadesuit$$

A hand containing two pairs of different ranks and a fifth card of yet another rank is said to have *two pairs*. For example, here is a hand with two pairs:

$$7\heartsuit 7\clubsuit 10\clubsuit 10\diamondsuit 2\spadesuit$$

Note that, as defined here, a hand with two pairs can not be a full house.

5.1 What is the probability of a full house?

We can generate every full house in a unique way by the following procedure:

1. Choose the rank of the pair. This can be done in 13 ways.
2. Choose the suits of the pair. This can be done in $\binom{4}{2}$ ways, since we must select 2 of the 4 suits.
3. Choose the rank of the 3-of-a-kind. This can be done in only 12 ways, since one rank is already taken by the pair.
4. Choose the suits of the 3-of-a-kind. This can be done in $\binom{4}{3}$ ways, since we must select 3 of the 4 suits.

Therefore, the number of different full houses is $13 \cdot \binom{4}{2} \cdot 12 \cdot \binom{4}{3}$. Since all $\binom{52}{5}$ possible hands are equally likely, the probability of being dealt a full house is:

$$\begin{aligned} \Pr \{\text{full house}\} &= \frac{13 \cdot \binom{4}{2} \cdot 12 \cdot \binom{4}{3}}{\binom{52}{5}} \\ &\approx 0.00144 \end{aligned}$$

This means that only about 1 hand in 700 is a full house.

5.2 What is the probability of two pairs?

To answer this question, we must count the number of hands that have two pairs. Our first attempt gives the *wrong answer*, but it is helpful to understand why this attempt fails. Suppose that we generate hands with two pairs by the following procedure:

1. Choose the rank of the first pair in one of 13 ways.
2. Choose the suits of the first pair in one of $\binom{4}{2}$ ways.
3. Choose the rank of the second pair in one of 12 ways.
4. Choose the suits of the second pair in one of $\binom{4}{2}$ ways.
5. Choose the final card from among the 44 cards with a rank different from the ranks of the two pairs.

The problem is that we are *double counting*. Every hand with two pairs can be generated in *two different ways* by this procedure. For example, consider the hand:

$$7\heartsuit 7\spadesuit 9\heartsuit 9\diamondsuit 2\clubsuit$$

We could generate this hand either by choosing rank 7 in the first step and rank 9 in the third step or vice versa! We can find the actual number of hands with two pairs via the division rule, which pretty much just provides a lofty justification for dividing by 2.

$$\# \text{ hands with two pairs} = \frac{13 \cdot \binom{4}{2} \cdot 12 \cdot \binom{4}{2} \cdot 44}{2}$$

There is nothing wrong with this approach. We initially overcounted, but then corrected the count with an appropriate fudge factor. But be careful: it is easy to accidentally overcount and not realize that a corrective factor is needed!

Alternatively, we can generate each poker hand with two pairs in a unique way by the following procedure.

1. Choose the ranks of the pairs in one of $\binom{13}{2}$ ways.
2. Choose the suits for the pair of higher rank in one of $\binom{4}{2}$ ways.
3. Choose the suits for the pair of lower rank in one of $\binom{4}{2}$ ways.
4. Choose the remaining card in 44 different ways.

This approach removes the whole issue of double counting, and we get the same answer as before. Either way, the probability of two pairs is:

$$\begin{aligned}\Pr \{\text{two pairs}\} &= \frac{\binom{13}{2} \cdot \binom{4}{2}^2 \cdot 44}{\binom{52}{5}} \\ &\approx 0.0475 \dots\end{aligned}$$

This means that about 1 hand in 21 has two pairs.

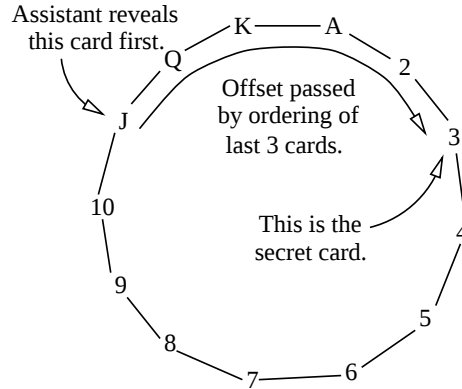
6 A Magic Trick

There is a magician and an assistant. The assistant goes into the audience with a deck of cards while the magician looks away. Five audience members are asked to select one card each from the deck. The assistant then gathers up the five cards and announces four of them to the magician. The magician thinks for a time and then correctly names the secret, fifth card!

6.1 How the Trick Works

The assistant has somehow communicated the secret card to the magician just by naming the other four cards. In particular, the assistant has two ways to communicate. First, he can announce the four cards in any order. The number of orderings of four cards is $4! = 24$, so this alone is insufficient to identify which of the remaining 48 cards is the secret one. Second, the assistant can choose which four of the five cards to reveal. The amount of information that can be conveyed this way is harder to pin down. The assistant has $\binom{5}{4} = 5$ ways to choose the four cards revealed, but the magician can not determine which of these five possibilities the assistant selected, since he does not know the secret card! Nevertheless, these two forms of communication allow the assistant to covertly reveal the secret card to the magician.

Here is an overview of how the trick works. The secret card has the same suit as the first card announced. Furthermore, the assistant can ensure that the rank of the secret card is between one and six steps clockwise from the rank of the first card in the diagram below. This offset is communicated by the order of the last three cards.



Here are the details. The audience selects five cards and there are only four suits in the deck. Therefore, by the pigeonhole principle, the assistant can always pick out two cards with the same suit. One of these will become the secret card, and the other will be the first card that he announces.

Here is how he decides which is which. Note that for any two card ranks, one is at most six clockwise steps away from the other in the diagram above. For example, if the card ranks are 2 and Q , then 2 is three clockwise steps away from Q . The assistant ensures that the rank of the secret card is offset between one and six clockwise steps from the first card he announces.

The offset is communicated by the order in which the assistant announces the last three cards. The magician and assistant agree in advance on an order for all 52 cards in the deck. For example, they might use:

$$A \clubsuit, 2 \clubsuit, \dots, K \clubsuit, A \diamondsuit, \dots, K \diamondsuit, A \heartsuit, \dots, K \heartsuit, A \spadesuit, \dots, K \spadesuit$$

With this order, one of the last three cards announced is the smallest (S), one is largest (L), and the other is medium (M). The offset is encoded by the order of these three cards:

$$\begin{aligned} SML &= 1 & SLM &= 2 & MSL &= 3 \\ MLS &= 4 & LSM &= 5 & LMS &= 6 \end{aligned}$$

For example, suppose that the audience selects $3\heartsuit, 8\diamondsuit, A\spadesuit, J\heartsuit, 6\diamondsuit$. The assistant picks out two cards with the same suit, say $3\heartsuit$ and $J\heartsuit$. The $3\heartsuit$ is five clockwise steps from $J\heartsuit$. So the assistant makes $3\heartsuit$ the secret card, announces $J\heartsuit$ first, and then encodes the number 5 by the order in which he announces the last three cards: $A\spadesuit, 6\diamondsuit, 8\diamondsuit = LSM = 5$.

6.2 Same Trick with Four Cards?

Could the same magic trick work with just four cards? That is, if the audience picks four cards, and the assistant reveals three, then can the magician determine the fourth card? The

answer turns out to be “no”. The proof relies on counting and the pigeonhole principle.

Theorem 1 *The magic trick is not possible with four cards.*

Proof. The audience can select any 4-combination of the 52 cards; let A be the set of all such 4-combinations. The assistant can announce any 3-permutation of cards to the magician; let B be the set of all such 3-permutations. The rules for the number of r -combinations and r -permutations give the following sizes for A and B :

$$\begin{aligned} |A| &= C(52, 4) \\ &= \frac{52!}{48! 4!} \\ &= 270,725 \\ |B| &= P(52, 3) \\ &= \frac{52!}{49!} \\ &= 132,600 \end{aligned}$$

The assistant sees a 4-combination of cards selected by the audience and must announce a 3-permutation to the magician. Let $f : A \rightarrow B$ be the function that the assistant uses in mapping one to the other. Since $|A| > |B|$, the pigeonhole principle implies that f maps at least two 4-combinations to the same 3-permutation. That is, there are two different sets of four cards that the audience can pick for which the assistant says exactly the same thing to the magician.

For these two sets of four cards, three cards must be the same (since the assistant announces the same three cards in both cases) and one card must be different (since the two sets are different). For example, these might be the two sets of four cards for which the assistant says exactly the same thing to the magician:

$$\begin{array}{l} 3\heartsuit \ 8\diamondsuit \ A\spadesuit \ J\heartsuit \\ 3\heartsuit \ 8\diamondsuit \ A\spadesuit \ K\diamondsuit \end{array}$$

In this case, the assistant announces $3\heartsuit \ 8\diamondsuit \ A\spadesuit$ in some order. The magician is now stuck; he can not determine whether the remaining card is $J\heartsuit$ or $K\diamondsuit$. $\square$