The Basics of Counting

Chapter 6

Chapter Summary

- The Basics of Counting
- The Pigeonhole Principle
- Permutations and Combinations
- Binomial Coefficients and Identities
- Generalized Permutations and Combinations

Basic Counting: The Product Rule

Basic Counting: The Product Rule

Recall: For a set A, $|A|$ is the cardinality of A (# of elements of A).

For a pair of sets A and B, $A \times B$ denotes their cartesian product:

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Product Rule

If A and B are finite sets, then: $|A \times B| = |A| \cdot |B|$.

Proof: Obvious, but prove it yourself by induction on |A|. □

general Product Rule

If $A_1, A_2, \ldots, A_m$ are finite sets, then

$$|A_1 \times A_2 \times \ldots \times A_m| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_m|$$

Proof: By induction on m, using the (basic) product rule. □

Product Rule: examples

- **Example 1:** How many bit strings of length seven are there?
- **Solution:** Since each bit is either 0 or 1, applying the product rule, the answer is $2^7 = 128$.
- **Example 2:** How many different car license plates can be made if each plate contains a sequence of three uppercase English letters followed by three digits?
- **Solution:** 26 . 26 . 26 . 10 . 10 . 10 = 17,576,000.

Counting Subsets

Number of Subsets of a Finite Set

A finite set, S, has $2^{|S|}$ distinct subsets.

Proof: Suppose $S = \{s_1, s_2, \ldots, s_m\}$.
There is a one-to-one correspondence (bijection), between subsets of S and bit s∈ings of length $m = |S|$.
The bit string of length $|S|$ we associate with a subset $A \subseteq S$ has a 1 in position i if $s_i \in A$, and 0 in position i if $s_i \notin A$, for all $i \in \{1, \ldots, m\}$.

$$\{s_2, s_4, s_5, \ldots, s_m\} \quad \cong \quad \underbrace{\begin{array}{|c|c|c|c|c|c|c|} \hline 0 & 1 & 0 & 1 & 1 & \ldots & 1 \\ \hline \end{array}}_{m}$$

By the product rule, there are $2^{|S|}$ such bit strings. $\square$

Counting Functions

Number of Functions

For all finite sets A and B, the number of distinct functions, $f : A \to B$, mapping A to B is:

$$|B|^{|A|}$$

Proof: Suppose $A = \{a_1, \ldots, a_m\}$.
There is a one-to-one correspondence between functions $f : A \to B$ and strings (sequences) of length $m = |A|$ over an alphabet of size $n = |B|$:

$$(f : A \to B) \quad \cong \quad \boxed{f(a_1) \mid f(a_2) \mid f(a_3) \mid \ldots \mid f(a_m)}$$

By the product rule, there are n^m such strings of length m. $\square$

Sum Rule

Sum Rule

If A and B are finite sets that are disjoint (meaning $A \cap B = \emptyset$), then

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

Proof. Obvious. (If you must, prove it yourself by induction on $|A|$.) $\square$

general Sum Rule

If $A_1, \ldots, A_m$ are finite sets that are pairwise disjoint, meaning $A_i \cap A_j = \emptyset$, for all $i, j \in \{1, \ldots, m\}$, then

$$|A_1 \cup A_2 \cup \ldots \cup A_m| = |A_1| + |A_2| + \ldots + |A_m|$$

Sum Rule: Examples

Example 1: Suppose variable names in a programming language can be either a single uppercase letter or an uppercase letter followed by a digit. Find the number of possible variable names.

Solution: Use the sum and product rules: $26 + 26 \cdot 10 = 286$. $\square$

Example 2: Each user on a computer system has a password which must be six to eight characters long.
Each character is an uppercase letter or digit.
Each password must contain at least one digit.
How many possible passwords are there?

Solution: Let P be the total number of passwords, and let P_6, P_7, P_8 be the number of passwords of lengths 6, 7, and 8, respectively.

- By the sum rule $P = P_6 + P_7 + P_8$.
- $P_6 = 36^6 - 26^6$; $P_7 = 36^7 - 26^7$; $P_8 = 36^8 - 26^8$.
- So, $P = P_6 + P_7 + P_8 = \sum_{i=6}^{8}(36^i - 26^i)$. $\square$

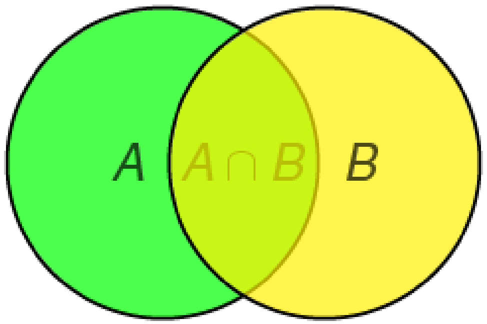
Subtraction Rule (Inclusion-Exclusion for two sets)

Subtraction Rule

For any finite sets A and B (not necessarily disjoint),

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

Proof: Venn Diagram:



$|A| + |B|$ overcounts (twice) exactly those elements in $A \cap B$. □

Subtraction Rule: Example

Example: How many bit strings of length 8 either start with a 1 bit or end with the two bits 00?

Solution:

- Number of bit strings of length 8 that start with 1: $2^7 = 128$.
- Number of bit strings of length 8 that end with 00: $2^6 = 64$.
- Number of bit strings of length 8 that start with 1 and end with 00: $2^5 = 32$.

Applying the subtraction rule, the number is $128 + 64 - 32 = 160$. $\square$

The Pigeonhole Principle

Pigeonhole Principle

For any positive integer k, if $k+1$ objects (pigeons) are placed in k boxes (pigeonholes), then at least one box contains two or more objects.

Proof: Suppose no box has more than 1 object. Sum up the number of objects in the k boxes. There can't be more than k. Contradiction. □

Pigeonhole Principle (rephrased more formally)

If a function $f : A \rightarrow B$ maps a finite set A with $|A| = k+1$ to a finite set B, with $|B| = k$, then f is not one-to-one.

(**Recall:** a function $f : A \rightarrow B$ is called **one-to-one** if $\forall a_1, a_2 \in A$, if $a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$.)

Pigeonhole Principle: Examples

- **Example 1:** At least two students registered for this course will receive exactly the same final exam mark. Why?
- **Reason:** There are at least 102 students registered for DS ,so, at least 102 objects. Final exam marks are integers in the range 0-100 (so, exactly 101 boxes).

Generalized Pigeonhole Principle

Generalized Pigeonhole Principle (GPP)

If $N \geq 0$ objects are placed in $k \geq 1$ boxes, then at least one box contains at least $\lceil \frac{N}{k} \rceil$ objects.

Proof: Suppose no box has more than $\lceil \frac{N}{k} \rceil - 1$ objects. Sum up the number of objects in the k boxes. It is at most

$$k \cdot (\left\lceil \frac{N}{k} \right\rceil - 1) < k \cdot ((\frac{N}{k} + 1) - 1) = N$$

Thus, there must be fewer than N. Contradiction.
(We are using the fact that $\lceil \frac{N}{k} \rceil < \frac{N}{k} + 1$.) □

Exercise: Rephrase GPP as a statement about functions $f : A \rightarrow B$ that map a finite set A with $|A| = N$ to a finite set B, with $|B| = k$.

Generalized Pigeonhole Principle: Examples

Example 1: Consider the following statement:

"At least d students in this course were born in the same month." (1)

Suppose the actual number of students registered for DMMR is 145. What is the maximum number d for which it is certain that statement (1) is true?

Solution: Since we are assuming there are 145 registered students in DMMR.
$\lceil \frac{145}{12} \rceil = 13$, so by GPP we know statement (1) is true for $d = 13$.
Statement (1) need not be true for $d = 14$, because if 145 students are distributed *as evenly as possible* into 12 months, the maximum number of students in any month is 13, with other months having only 12. □

(In **probability theory** you will learn that nevertheless it is highly probable, assuming birthdays are randomly distributed, that at least 14 of you (and more) were indeed born in the same month.)

GPP: more Examples

Example 2: How many cards must be selected from a standard deck of 52 cards to guarantee that at least thee cards of the same suit are chosen?

Solution: There are 4 suits. (In a standard deck of 52 cards, every card has exactly one suit. There are no jokers.) So, we need to choose N cards, such that $\lceil \frac{N}{4} \rceil \geq 3$. The smallest integer N such that $\lceil \frac{N}{4} \rceil \geq 3$ is $2 \cdot 4 + 1 = 9$. $\square$

Permutations

Permutation

A **permutation** of a set S is an ordered arrangement of the elements of S.

In other words, it is a sequence containing every element of S exactly once.

Example: Consider the set $S = \{1, 2, 3\}$.

The sequence $(3, 1, 2)$ is one permutation of S.

There are 6 different permutations of S. They are:

$$(1,2,3)\ ,\ (1,3,2)\ ,\ (2,1,3)\ ,\ (2,3,1)\ ,\ (3,1,2)\ ,\ (3,2,1)$$

Permutations (an alternative view)

A permutation of a set S can alternatively be viewed as a bijection (a one-to-one and onto function), $\pi : S \to S$, from S to itself.

Specifically, if the finite set is $S = \{s_1, \ldots, s_m\}$, then by fixing the ordering $s_1, \ldots, s_m$, we can uniquely associate to each bijection $\pi : S \to S$ a sequence ordering $\{s_1, \ldots, s_m\}$ as follows:

$$(\pi : S \to S) \quad \cong \quad \begin{array}{|c|c|c|c|c|}\hline \pi(s_1) & \pi(s_2) & \pi(s_3) & \ldots & \pi(s_m) \\ \hline\end{array}$$

Note that π is a bijection if and only if the sequence on the right containing every element of S exactly once.

r-Permutation

r-Permutation

An r**-permutation** of a set S, is an ordered arrangement (sequence) of r distinct elements of S.

(For this to be well-defined, r needs to be an integer with $0 \leq r \leq |S|$.)

Examples:

There is only one 0-permutation of any set: the empty sequence ().

For the set $S = \{1, 2, 3\}$, the sequence $(3, 1)$ is a 2-permutation.

$(3, 2, 1)$ is both a permutation and 3-permutation of S (since $|S| = 3$).

There are 6 different different 2-permutations of S. They are:

$$(1, 2)\ ,\ (1, 3)\ ,\ (2, 1)\ ,\ (2, 3)\ ,\ (3, 1)\ ,\ (3, 2)$$

Question: How many r-permutations of an n-element set are there?

r-Permutations (an alternative view)

An r-permutation of a set S, with $1 \leq r \leq |S|$, can alternatively be viewed as a one-to-one function, $f : \{1, \ldots, r\} \to S$.

Specifically, we can uniquely associate to each one-to-one function $f : \{1, \ldots, r\} \to S$, an r-permutation of S as follows:

$$(f : \{1, \ldots, r\} \to S) \quad \cong \quad \boxed{f(1) \mid f(2) \mid f(3) \mid \ldots \mid f(r)}$$

Note that f is one-to-one if and only if the sequence on the right is an r-permutation of S.

So, for a set S with $|S| = n$, the number of r-permutions of S, $1 \leq r \leq n$, is equal to the number of one-to-one functions:

$$f : \{1, \ldots, r\} \to \{1, \ldots, n\}$$

Formula for # of permutations, and # of r -permutations

Let $\mathbf{P}(n, r)$ denote the number of r-permutations of an n-element set.

$P(n, 0) = 1$, because the only 0-permutation is the empty sequence.

Theorem

For all integers $n \geq 1$, and all integers r such that $1 \leq r \leq n$:

$$P(n, r) = n \cdot (n-1) \cdot (n-2) \ldots (n-r+1) \; = \; \frac{n!}{(n-r)!}$$

Proof. There are n different choices for the first element of the sequence. For each of those choices, there are $n-1$ remaining choices for the second element. For every combination of the first two choices, there are $n-2$ choices for the third element, and so forth. □

Corollary: the number of permutations of an n element set is:

$$n! \; = \; n \cdot (n-1) \cdot (n-2) \ldots \cdot 2 \cdot 1 = P(n, n)$$

Example: a simple counting problem

Example: How many permutations of the letters ABCDEFGH contain the string ABC as a (consecutive) substring?

Solution: We solve this by noting that this number is the same as the number of permutations of the following six objects: ABC, D, E, F, G, and H. So the answer is:

$$6! = 720:$$

Combinations

r-Combinations

An r**-combination** of a set S is an unordered collection of r elements of S. In other words, it is simply a subset of S of size r.

Example: Consider the set $S = \{1, 2, 3, 4, 5\}$.

The set $\{2, 5\}$ is a 2-combination of S.

There are 10 different 2-combinations of S. They are:

$\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{1, 5\}$,
$\{2, 3\}$, $\{2, 4\}$, $\{2, 5\}$,
$\{3, 4\}$, $\{3, 5\}$,
$\{4, 5\}$

Question: How many r-combinations of an n-element set are there?

Formula for the number of r-combinations

Let $\mathbf{C}(n, r)$ denote the number of r-combinations of an n-element set. Another notation for $C(n, r)$ is: $\binom{n}{r}$

These are called **binomial coefficients**, and are read as "n choose r".

Theorem

For all integers $n \geq 1$, and all integers r such that $0 \leq r \leq n$:

$$C(n, r) \doteq \binom{n}{r} = \frac{n!}{r! \cdot (n-r)!} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-r+1)}{r!}$$

Proof. We can see that $P(n, r) = C(n, r) \cdot P(r, r)$. (To get an r-permutation: first choose r elements, then order them.) Thus

$$C(n, r) = \frac{P(n, r)}{P(r, r)} = \frac{n!/(n-r)!}{r!/(r-r)!} = \frac{n!}{r! \cdot (n-r)!} \qquad \square$$

Combinations: examples

Example:

1. How many different 5-card poker hands can be dealt from a deck of 52 cards?
2. How many different 47-card poker hands can be dealt from a deck of 52 cards?

Solutions:

1. $$\binom{52}{5} = \frac{52!}{5! \cdot 47!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 2,598,960$$
2. $$\binom{52}{47} = \frac{52!}{47! \cdot 5!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 2,598,960$$

Question: Why are these numbers the same?

Combinations: an identity

Theorem

For all integers $n \geq 1$, and all integers r, $1 \leq r \leq n$:

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

Proof:

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

We can also give a **combinatorial proof**: Suppose $|S| = n$. A function, f, that maps each r-element subset A of S to the $(n-r)$-element subset $(S - A)$ is a bijection.
Any two finite sets having a bijection between them must have exactly the same number of elements. $\square$

Binomial Coefficients

Consider the polynomial in two variables, x and y, given by:

$$(x+y)^n = \underbrace{(x+y)\cdot(x+y)\ldots(x+y)}_{n}$$

By multiplying out the n terms, we can expand this polynomial and write it in a standard sum-of-monomials form:

$$(x+y)^n = \sum_{j=0}^{n} c_j x^{n-j} y^j$$

Question: What are the coefficients c_j? (These are called binomial coefficients.)

Examples:

$$(x+y)^2 = x^2 + 2xy + y^2$$

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

The Binomial Theorem

Binomial Theorem

For all $n \geq 0$:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \ldots + \binom{n}{n} y^n$$

Proof: What is the coefficient of $x^{n-j} y^j$?
To obtain a term $x^{n-j} y^j$ in the expansion of the product

$$(x+y)^n = \underbrace{(x+y)(x+y)\ldots(x+y)}_{n}$$

we have to choose exactly $n-j$ copies of x and (thus) j copies of y.
How many ways are there to do this? Answer: $\binom{n}{j} = \binom{n}{n-j}$. □

Corollary: $\sum_{j=0}^{n} \binom{n}{j} = 2^n$.

Proof: By the binomial theorem, $2^n = (1+1)^n = \sum_{j=0}^{n} \binom{n}{j}$. □

Pascal's Identity

Theorem (Pascal's Identity)

For all integers $n \geq 0$, and all integers r, $0 \leq r \leq n+1$:

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

Proof: Suppose $S = \{s_0, s_1, \ldots, s_n\}$. We wish to choose s subset $A \subseteq S$ such that $|A| = r$. We can do this in two ways. We can either:
(I) choose a subset A such that $s_0 \in A$, or
(II) choose a subset A such that $s_0 \notin A$.

There are $\binom{n}{r-1}$ sets of the first kind,
and there are $\binom{n}{r}$ sets of the second kind.
So, $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$. □

Pascal's Triangle

$$\binom{0}{0}$$
$$\binom{1}{0}\ \binom{1}{1}$$
$$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$$
$$\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3}$$
$$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$$
$$\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5}$$
$$\binom{6}{0}\ \binom{6}{1}\ \binom{6}{2}\ \binom{6}{3}\ \binom{6}{4}\ \binom{6}{5}\ \binom{6}{6}$$
$$\binom{7}{0}\ \binom{7}{1}\ \binom{7}{2}\ \binom{7}{3}\ \binom{7}{4}\ \binom{7}{5}\ \binom{7}{6}\ \binom{7}{7}$$
$$\binom{8}{0}\ \binom{8}{1}\ \binom{8}{2}\ \binom{8}{3}\ \binom{8}{4}\ \binom{8}{5}\ \binom{8}{6}\ \binom{8}{7}\ \binom{8}{8}$$
$$\cdots$$

By Pascal's identity:

$$\binom{6}{4} + \binom{6}{5} = \binom{7}{5}$$

$$1$$
$$1 \quad 1$$
$$1 \quad 2 \quad 1$$
$$1 \quad 3 \quad 3 \quad 1$$
$$1 \quad 4 \quad 6 \quad 4 \quad 1$$
$$1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1$$
$$1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1$$
$$1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1$$
$$1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1$$
$$\cdots$$