Discrete Mathematics 1 Lectures, Part 1

Tomasz Brengos

1 Counting (Combinatorics)

Counting forms the basis of combinatorics. In these lectures we explore several counting rules, examples, and proofs.

1.1 Rule of Sum (Addition Principle)

If a set S is partitioned into disjoint subsets,

$$S = S_1 \cup S_2 \cup \cdots \cup S_k,$$

then the total number of elements in S is the sum of the number of elements in each subset:

$$|S| = |S_1| + |S_2| + \cdots + |S_k|.$$

Example: Suppose we wish to count the number of ways to choose a subset of a set X of size u, but we only consider subsets of a fixed size k. If we let S be the family of all such subsets, then using the rule of sum by dividing the choices according to a distinguished element (say, whether a chosen element is included or not) we can count the subsets by summing over the possibilities. (This idea is used later in proofs for binomial coefficients and the power set.)

Theorem:

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

Proof: Consider $S = \binom{X}{k}$, the set of all subsets of X of size k. Take any element $a \in X$. Define: S_1 as the subsets in S that contain a and S_2 as the subsets in S that do not contain a.

Since every subset of S either contains a or does not, we see that S_1 and S_2 are disjoint and their union forms S, i.e.,

$$S_1 \cup S_2 = S.$$

By the rule of sum, we get:

$$|S| = |S_1| + |S_2|.$$

Now, each subset in S_1 must contain a, so we choose the remaining $k-1$ elements from $X \setminus \{a\}$, which has $n-1$ elements. Thus, $|S_1| = \binom{n-1}{k-1}$. Each subset in S_2 does not contain a, so we choose all k elements from $X \setminus \{a\}$. Thus, $|S_2| = \binom{n-1}{k}$.

Therefore,

$$\binom{n}{k} = |S| = |S_1| + |S_2| = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Example: Let $S = \{\triangle, \square, \circ\}$ and $k = 2$, choosing $a = \circ$. Fixing $\circ$ as one of the elements in the subset of size k, we get:

$$S_1 = \{\{\circ, \triangle\}, \{\circ, \square\}\}.$$

Taking all subsets of size k without $\circ$:

$$S_2 = \{\{\triangle, \square\}\}.$$

We have $|S_1| = 2$ and $|S_2| = 1$, so $|S_1| + |S_2| = 3$.
On the other hand,

$$\binom{3}{2} = \frac{3!}{2!(3-2)!} = 3.$$

Thus, $|S| = |S_1| + |S_2| = 3$, verifying the identity.

1.2 Rule of Product (Multiplication Principle)

When an object is constructed by a sequence of choices, where:

- The first choice can be made in a ways,
- The second in b ways,
- ...

the total number of objects is the product:

$$a \times b \times \cdots .$$

Example: A word of length n over the binary alphabet $\{0, 1\}$ is formed by choosing one of 2 possibilities for each position. Hence, there are

$$2^n$$

possible words.

1.3 Rule of Bijection

If there exists a bijection (a one-to-one and onto mapping) between two sets S and T, then they have the same number of elements:

$$|S| = |T|.$$

Example: Consider the power set of a set X, denoted by $\mathcal{P}(X)$. There is a natural bijection between $\mathcal{P}(X)$ and the set of binary sequences of length $|X|$: for each subset $A \subseteq X$, assign the sequence $(a_1, a_2, \ldots, a_n)$ where

$$a_i = \begin{cases} 1, & \text{if } x_i \in A, \\ 0, & \text{if } x_i \notin A. \end{cases}$$

This shows that

$$|\mathcal{P}(X)| = 2^{|X|}.$$

1.4 Counting in Two Ways

Rule of Counting in Two Ways When two formulae enumerate the same quantity, they must be equal.

Example:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Proof: Consider a lattice grid of size $(n+1) \times (n+1)$, defined as:

$$X = \{(i, j) \mid i, j \in \{1, 2, \ldots, n+1\}\}.$$

Clearly, $|X| = (n+1)^2$.

Now, partition X into three subsets: - X_1, the points strictly below the secondary diagonal. - X_2, the points strictly above the secondary diagonal. - X_3, the points on the secondary diagonal itself.

Since these three sets form a partition, we have:

$$|X| = |X_1| + |X_2| + |X_3|.$$

Observing their sizes:

$$|X_1| = |X_2| = 1 + 2 + \cdots + n, \quad |X_3| = n + 1.$$

Thus,

$$(n+1)^2 = 2(1 + 2 + \cdots + n) + (n+1).$$

Rearranging, we get:

$$1 + 2 + \cdots + n = \frac{(n+1)^2 - (n+1)}{2} = \frac{n(n+1)}{2}.$$

Hence, we have proven the formula:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

1.5 Binomial Coefficients and Permutations

Let X be a set with $|X| = n$.

Subsets: The number of ways to choose a k-subset of X is given by the binomial coefficient

$$\binom{n}{k}.$$

Permutations: A k-permutation of a set X of size n is a k-word over the alphabet X whose entries are distinct.

Theorem: There are exactly

$$n(n-1)(n-2)\ldots(n-k+1)$$

k-permutations of an n-set.

Question: How are k-permutations of an n-set related to k-subsets of an n-set?

Answer: The difference between a k-permutation and a k-subset is that a permutation is ordered, while a subset is not. To express a k-permutation in terms of a k-subset, we need to account for all possible arrangements of the elements, which is $k!$. Thus,

$$k\text{-permutation} = \binom{n}{k} \cdot k!$$

Expressing $\binom{n}{k}$ as

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

we obtain:

$$k\text{-permutation} = \frac{n!}{(n-k)!}.$$

Proof by Counting in Two Ways: Count the number of k-permutations of an n-set in two ways:

(1) Directly, by applying the rule of product:

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

(2) First choose a k-subset (in $\binom{n}{k}$ ways) and then arrange it (in $k!$ ways), giving

$$\binom{n}{k} \cdot k!.$$

Equate these two counts to obtain the relation.

1.6 Binomial Theorem

For any x, y in a field and nonnegative integer n, the binomial theorem states:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Explanation: This theorem is a direct consequence of counting the number of ways to choose k copies of x (and the remaining $n-k$ copies of y) when expanding the product.

1.7 Multisets

Definition: A multiset of a set X of size n is a function

$$m : X \to \mathbb{N}$$

that assigns a non-negative integer to each element of X, representing its multiplicity in the multiset.

Example: Let $X = \{a, b, c\}$, and consider the multiset $\{a, a, b\}$. Then, the function m is given by:

$$m(a) = 2, \quad m(b) = 1, \quad m(c) = 0.$$

Question: What is the number of k-multisets of a set of size n?

Theorem: The number of all k-multisets of an n-set is

$$\binom{n+k-1}{k}.$$

Proof: Let X be the set of all k-multisets of an n-set. Let Y be the set of all distributions of k identical objects into n buckets.

Claim 1: There is a bijection from X to Y. Thus, by the rule of bijection, we have

$$|X| = |Y|.$$

Claim 2: Let Z be the set of all binary sequences of length $n+k-1$ with exactly $n-1$ ones (or equivalently, k zeros). There is a bijection from Y to Z. Hence,

$$|Y| = |Z| \Rightarrow |X| = |Z|.$$

Since the number of such binary sequences is given by

$$\binom{n+k-1}{k},$$

we conclude that

$$|X| = \binom{n+k-1}{k}.$$

1.8 Lattice Paths

Consider an $m \times n$ grid with lattice points at the intersections.

Problem: How many paths are there from $(0,0)$ to (m,n) if one may only move right or up?

Solution: Every path consists of exactly m right moves and n up moves. Thus, a path can be represented as a sequence of $m+n$ moves, where we choose n positions (out of $m+n$) for the up moves. Hence, the number of paths is:

$$\binom{m+n}{n}.$$

Bijection Explanation: There is a bijection between the set of such lattice paths and the set of binary sequences of length $m+n$ with exactly n ones (representing the up moves).

2 Partitions and Stirling Numbers

2.1 Set Partitions

Definition: A set $\{A_1, A_2, \ldots, A_k\}$ of subsets of N forms a *partition of* the set N if:

$$A_i \neq \emptyset, \quad A_i \cap A_j = \emptyset \text{ for } i \neq j, \quad \text{and} \quad N = A_1 \cup A_2 \cup \cdots \cup A_k.$$

If a partition P of the set N is of size k then we say that P partitions N into k blocks.

Example: For $N = \{1,2,3,4\}$, one partition into 2 blocks could be

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

All possible partitions of a set N are denoted by $\Pi(N)$.

2.2 Stirling Numbers of the Second Kind

Question: How many k-partitions of an n-set are there?

Answer: Let $S(n,k)$ (or $\{n\ k\}$) denote the answer to our question, called the *Stirling number of the second kind*. We define the base cases as follows:

$$S(0,0) := 1, \quad S(0,k) := 0 \quad \text{for } k > 0.$$

Theorem: The total number of set partitions of N is given by

$$|\Pi(N)| = \sum_{k=0}^{|N|} S(|N|, k).$$

Remark: The quantity

$$B(|N|) := |\Pi(N)| = \sum_{k=0}^{|N|} S(|N|, k)$$

is called the *Bell number*.

Example: Let $N = [5] = \{1, 2, 3, 4, 5\}$. List all possible 2-partitions of N.

Firstly, consider cases where the first subset contains only one element:

$$1|2\,3\,4\,5, \quad 2|1\,3\,4\,5, \quad 3|1\,2\,4\,5, \quad 4|1\,2\,3\,5, \quad 5|1\,2\,3\,4.$$

Now, consider cases where the first subset contains two elements:

$$1\,2|3\,4\,5, \quad 1\,3|2\,4\,5, \quad 1\,4|2\,3\,5, \quad 1\,5|2\,3\,4,$$

$$2\,3|1\,4\,5, \quad 2\,4|1\,3\,5, \quad 2\,5|1\,3\,4, \quad 3\,4|1\,2\,5, \quad 3\,5|1\,2\,4, \quad 4\,5|1\,2\,3.$$

Since we are only interested in the contents of the two subsets (not their arrangement or order), we do not list cases where the first subset has three or four elements, as these would be overcounting. For example, the partitions $1\,2|3\,4\,5$ and $3\,4\,5|1\,2$ are considered the same.

Thus, all possible partitions have been listed, and their total number is 15. Therefore,

$$S(5, 2) = 15.$$

Note: Stirling numbers consider objects that we distribute as distinct, the boxes (subsets) as identical, and the size of subsets as known. Due to this, in the example, we did not consider the cases $1\,2|3\,4\,5$ and $3\,4\,5|1\,2$ as distinct.

Additionally, Bell's number counts all possible partitions, meaning the number of subsets k is not fixed but varies from 0 to $|N|$. This concept may seem similar to multisets; however, Bell's number treats objects being distributed as distinct and the boxes(subsets) as identical, while multisets treat objects as identical and boxes as distinct.

Recurrence Relation: These numbers satisfy the recurrence:

$$S(n, k) = S(n-1, k-1) + k\, S(n-1, k).$$

Proof: Let $N = [n]$ and P be the set of all k-partitions of N. We observe that $|P| = S(n, k)$, where $S(n, k)$ denotes the Stirling number of the second kind.

Consider an element $x \in [n]$. Define the following subsets of P: X_1 consists of partitions in P where x forms a singleton block, i.e., one of the subsets A_i in the partition $\{A_1, A_2, \ldots, A_k\}$ is $\{x\}$. $X_2 = P \setminus X_1$, meaning X_2 consists of partitions where x is not a singleton block but instead belongs to one of the k subsets.

Now, we compute their cardinalities: Since X_1 consists of partitions where x is a singleton, the remaining $n-1$ elements must be partitioned into $k-1$ subsets. Thus,

$$|X_1| = S(n-1, k-1).$$

In X_2, the element x is assigned to one of the k subsets after partitioning the remaining $n-1$ elements into k subsets. Thus,

$$|X_2| = k \cdot S(n-1, k).$$

By the rule of sum,

$$S(n,k) = |X_1| + |X_2| = S(n-1,k-1) + k \cdot S(n-1,k).$$

This completes the proof.

2.3 Counting Maps

Setup: Consider two finite sets N and R of sizes n and r respectively. We want to answer three main questions about the functions from N to R:

Q1: How many functions from N to R are there?

Answer: Each of the n elements of N can be mapped to any of the r elements of R. Hence, there are r^n possible functions in total.

Q2: How many injective (one-to-one) functions from N to R?

Answer: To build an injective function, choose a distinct image in R for each element of N. Thus, the number of injective functions is

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

Q3: How many surjective (onto) functions from N to R?

Answer: A function $f : N \to R$ is surjective if every element of R has a nonempty preimage. Equivalently, the sets

$$f^{-1}(y_1), \quad f^{-1}(y_2), \quad \ldots, \quad f^{-1}(y_r)$$

form a partition of N into r nonempty blocks. Since there are $S(n,r)$ ways to partition N into r nonempty subsets (where $S(n,r)$ is the Stirling number of the second kind), and each partition can be labeled in $r!$ ways (assigning each of the r blocks to a different $y_i \in R$), the total number of surjections is

$$\mathrm{Sur}(n,r) = r! \cdot S(n,r)$$

Corollary: Let N and R be finite sets with $|N| = n$ and $|R| = r$. Then the total number of functions from N to R can be expressed as

$$|\mathrm{Map}(N,R)| \;=\; r^n \;=\; \sum_{k=0}^{r} \binom{r}{k} \, k! \, S(n,k).$$

2.4 Number Partitions

Definition. A *number partition* of $n \in \mathbb{N}$ is an expression

$$n = \lambda_1 + \lambda_2 + \cdots + \lambda_k,$$

where

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1.$$

Example. List all possible different number partitions of $n = 5$ into two summands:

$$5 = 4 + 1 \quad \text{and} \quad 5 = 3 + 2.$$

Question. How many k-partitions of n are there?

Answer. Define

$$P(n,k) = \Big\{ (\lambda_1, \ldots, \lambda_k) \,\Big|\, n = \lambda_1 + \lambda_2 + \cdots + \lambda_k,\ \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1 \Big\},$$

and let

$$p(n,k) = |P(n,k)|.$$

Moreover, set

$$P(n) = \bigcup_{k=1}^{n} P(n,k) \quad \text{and} \quad p(n) = |P(n)|.$$

An immediate observation is that

$$p(n) = \sum_{k=0}^{n} p(n,k).$$

Example. List all possible different number partitions of $n = 5$:

$$P(5) = \Big\{ \{5\},\ \{4,1\},\ \{3,2\},\ \{3,1,1\},\ \{2,2,1\},\ \{2,1,1,1\},\ \{1,1,1,1,1\} \Big\},$$

with, for instance,

$$P(5,1) = \{\{5\}\}, \quad P(5,2) = \{\{4,1\},\{3,2\}\}, \quad P(5,3) = \{\{3,1,1\},\{2,2,1\}\},$$

$$P(5,4) = \{\{2,1,1,1\}\}, \quad P(5,5) = \{\{1,1,1,1,1\}\}.$$

To derive recursive formulas for $p(n)$ and $p(n,k)$, we introduce the notation

$$p(n, \leq k) \stackrel{\text{def}}{=} |P(n, \leq k)|, \quad \text{where} \quad P(n, \leq k) = \bigcup_{i=1}^{k} P(n,i).$$

- **Observation 1:** $P(n, \leq n) = P(n)$ and hence $p(n, \leq n) = p(n)$.
- **Observation 2:**

$$p(n, \leq k) = \sum_{i=1}^{k} p(n,i) = p(n,1) + p(n,2) + \cdots + p(n,k).$$

Theorem. There is a bijection

$$\Phi \colon P(n,k) \longrightarrow P(n-k, \leq k),$$

defined as follows.

Represent a partition

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \in P(n,k)$$

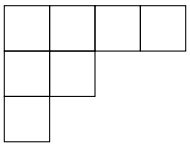
by its Ferrers diagram drawn in the standard way (with the largest row on top). In this diagram, the top row has λ_1 cells, the second row has λ_2 cells, and so on.

Explanation of the Mapping. Our goal is to relate partitions of n into exactly k parts to partitions of $n-k$ with at most k parts. Notice that if we subtract 1 from each part λ_i, then

$$n = \lambda_1 + \lambda_2 + \cdots + \lambda_k \quad \Longrightarrow \quad n - k = (\lambda_1 - 1) + (\lambda_2 - 1) + \cdots + (\lambda_k - 1).$$

Graphically, subtracting 1 from a part corresponds to removing one cell from its corresponding row. Since the Ferrers diagram is left-justified, every row begins with a cell in the leftmost column. Thus, removing the entire leftmost column is equivalent to subtracting 1 from each λ_i. In this way, the original diagram representing a partition of n with k parts is transformed into a diagram representing a partition of $n-k$ that has at most k parts (some rows may vanish if $\lambda_i = 1$).

Example. Consider the partition $(\lambda_1, \lambda_2, \lambda_3) = (4, 2, 1)$ of $n = 7$ into 3 parts. Its Ferrers diagram is:



Ferrers Diagram for $(4, 2, 1)$

Removing the leftmost column yields:

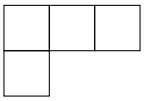


Diagram after removing leftmost column

The new diagram represents the partition $(3, 1)$, which is a partition of $7 - 3 = 4$ (since there were $k = 3$ rows, and we removed one cell per row). Note that $(3, 1)$ is an element of $P(4, \leq 3)$.

Justification of Bijectivity. The mapping

$$\Phi\colon (\lambda_1, \lambda_2, \ldots, \lambda_k) \mapsto (\lambda_1 - 1, \lambda_2 - 1, \ldots, \lambda_k - 1)$$

is invertible. Given any partition μ in $P(n-k, \leq k)$ (which has at most k parts), we can reconstruct a unique partition in $P(n, k)$ by adding 1 to each part and, if necessary, appending enough parts equal to 1 so that the total number of parts becomes exactly k. In other words, the inverse mapping Φ^{-1} is defined by:

$$\Phi^{-1}\colon \mu = (\mu_1, \mu_2, \ldots, \mu_r) \mapsto (\mu_1 + 1, \mu_2 + 1, \ldots, \mu_r + 1, \underbrace{1, 1, \ldots, 1}_{k-r \text{ times}}),$$

with $r \leq k$. It is straightforward to check that Φ and Φ^{-1} are mutual inverses. Thus, the mapping Φ is a bijection, and we have the relation:

$$p(n, k) = |P(n, k)| = |P(n-k, \leq k)| = p(n-k, \leq k).$$

This bijective correspondence is the key step in obtaining a recursive formula for $p(n, k)$.

Corollary 1. *For all integers $n \geq k \geq 1$, we have*

$$p(n, k) = p(n-k, \leq k) = p(n-k, 1) + p(n-k, 2) + \cdots + p(n-k, k-1) + p(n-k, k).$$

That is, the total number of k-partitions of n can be split into partitions of $n-k$ with at most k parts:

$$p(n, k) = p(n-k, \leq k-1) + p(n-k, k).$$

Moreover, since

$$p(n-k, \leq k-1) = p((n-k) + (k-1), k-1) = p(n-1, k-1),$$

we obtain the recurrence relation

$$p(n, k) = p(n-1, k-1) + p(n-k, k).$$

3 Inclusion-Exclusion Principle

Very often, we need to calculate the number of elements in the union of certain sets. Assuming that we know the sizes of these sets, and their mutual intersections, the principle of inclusion and exclusion allows us to do exactly that.

Suppose you have two sets A and B. The size of the union is certainly at most $|A| + |B|$. However, in doing so we count each element of $A \cap B$ twice. To correct for this, we subtract $|A \cap B|$ to obtain

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

In general, the formula gets more complicated because we must take into account intersections of multiple sets. The following statement is what we call the *principle of inclusion and exclusion*:

Lemma 1. *For any collection of finite sets $A_1, A_2, \ldots, A_n$, we have*

$$\left|\bigcup_{i=1}^{n} A_i\right| \;=\; \sum_{\substack{I \subseteq [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|.$$

Equivalently,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| \;=\; \textstyle\sum_{i=1}^{n} |A_i| \;-\; \sum_{1 \le i < j \le n} |A_i \cap A_j| \;+\; \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \;-\; \cdots \;+\; (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Proof Outline (informal): *Each element that belongs to exactly t of the sets A_i is counted $\binom{t}{1}$ times in the first summation, then subtracted $\binom{t}{2}$ times in the second summation, added $\binom{t}{3}$ times in the third, and so on. In other words, its total contribution is*

$$\binom{t}{1} - \binom{t}{2} + \binom{t}{3} - \cdots + (-1)^{t-1}\binom{t}{t},$$

which equals 1. This alternating sum ensures that each element is ultimately counted exactly once, thereby correcting for any overcounting.

4 Permutations and Derangements

4.1 Permutations

A *permutation* of n elements is an arrangement (ordering) of those elements. For example, there are 6 permutations of the set $\{a, b, c\}$:

$$(a, b, c), \quad (a, c, b), \quad (b, a, c), \quad (b, c, a), \quad (c, a, b), \quad (c, b, a).$$

Since there are 3 choices for the first element, 2 for the second (once the first is chosen), and 1 for the last, by the multiplicative principle there are $3 \cdot 2 \cdot 1 = 3! = 6$ permutations in total.

Factorials and counting. In general, the number of permutations of n (distinct) elements is given by

$$n! \;=\; n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1.$$

Partial permutations (k-permutations). Sometimes we only permute k of the n elements, where $1 \le k \le n$. The number of ways to do this is denoted $P(n, k)$ and can be found by thinking:

$$P(n, k) \;=\; n \times (n-1) \times \cdots \times (n-k+1).$$

There are k factors in that product. Using factorial notation, we can write

$$P(n, k) \;=\; \frac{n!}{(n-k)!}.$$

Relationship to combinations. An alternate derivation uses combinations: first *choose* which k elements from the n will appear (that can be done in $\binom{n}{k}$ ways), then *arrange* those k in order (which can be done in $k!$ ways). Hence,

$$P(n,k) \;=\; \binom{n}{k}\, k!.$$

Since $\binom{n}{k} = \dfrac{n!}{(n-k)!\,k!}$, multiplying by $k!$ yields exactly $\dfrac{n!}{(n-k)!}$, consistent with the direct counting approach.

4.2 Derangements

A *derangement* of n elements is a permutation where no element remains in its original position. More precisely, if we think of a permutation as a bijection θ on the set $\{1, 2, \ldots, n\}$, then θ is a derangement if and only if

$$\theta(k) \;\neq\; k \quad \text{for all } k \in \{1, 2, \ldots, n\}.$$

Equivalently, a derangement has no fixed points.

For example, for $n = 3$, the permutations of $\{1, 2, 3\}$ are:

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

Among these, the derangements are $(2, 3, 1)$ and $(3, 1, 2)$; the other permutations fix at least one of the elements.

Counting Derangements via Inclusion-Exclusion

Let $D(n)$ denote the number of derangements of n elements. We will use the principle of inclusion-exclusion. Suppose we label the elements as $1, 2, \ldots, n$, and define A_i to be the set of permutations that fix the element i (i.e. $\theta(i) = i$). Then any derangement is a permutation that lies in none of the sets A_i (for $1 \le i \le n$). We have

$$\big|A_i\big| \;=\; (n-1)!,$$

since if we fix one position i, then we permute the remaining $n-1$ elements freely. In general,

$$\big|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}\big| \;=\; (n-k)!.$$

By inclusion-exclusion, the size of the union $A_1 \cup A_2 \cup \cdots \cup A_n$ is

$$\sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)!.$$

Hence the number of permutations that do not lie in this union—i.e. the number of derangements—is

$$D(n) \;=\; n! \;-\; \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \cdots + (-1)^n \binom{n}{n}(n-n)!.$$

$$D(n) \;=\; \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \;=\; n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Thus, a concise closed-form for the number of derangements is

$$D(n) \;=\; n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Note on the series for e^{-1}:
In Calculus, one learns that the exponential function has a power series expansion

$$e^x \;=\; \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

Setting $x = -1$ gives

$$e^{-1} \;=\; \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}.$$

Hence,

$$\sum_{k=0}^{n} \frac{(-1)^k}{k!} \;\xrightarrow[n\to\infty]{}\; e^{-1}.$$

If you have not taken (or do not recall) a full course in Calculus, think of this as a special case of a well-known infinite series expansion for the exponential function.

Since the finite sum $\sum_{k=0}^{n} \frac{(-1)^k}{k!}$ converges to e^{-1} as $n \to \infty$, we conclude that

$$\lim_{n\to\infty} \frac{D(n)}{n!} \;=\; \lim_{n\to\infty} \sum_{k=0}^{n} \frac{(-1)^k}{k!} \;=\; e^{-1}.$$

Numerically, this means that for large n, about $1/e \approx 36.8\%$ of all permutations of $\{1, \ldots, n\}$ are derangements (i.e. have no fixed points).

A Recurrence Relation

We can also show that $D(n)$ satisfies the recurrence

$$D(n) \;=\; (n-1)\big(D(n-1) + D(n-2)\big), \quad \text{with } D(1) = 0,\ D(2) = 1.$$

One way to see this: consider where 1 goes in a derangement of $\{1, 2, \ldots, n\}$. It can go to any of $n-1$ positions. If 1 goes to position j, then either (i) the element j goes to position 1 (a swap), which reduces the problem to deranging the remaining $n-2$ elements, or (ii) the element j does *not* go to position 1, effectively reducing the problem to deranging $n-1$ elements. This yields the above recurrence.

5 Functions Between Sets

Let N and R be sets with $|N| = n$ and $|R| = r$.

(i) **Total Functions:** The number of functions from N to R is

$$r^n.$$

Explanation: For every element in N, there are $|R| = r$ possible values in R. Thus, for the first element, there are r choices, for the second element, there are r choices, and so on. Applying the rule of product, the total number of functions is r^n.

(ii) **Injective Functions:** When $r \geq n$, an injective function (one-to-one) from N to R can be chosen by assigning distinct images to the n elements.

If a function is injective, then for each value in the range there is only one corresponding argument. This means that function values cannot repeat, ensuring that $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$.

Since there are $|R| = r$ choices for the first argument, $r-1$ choices for the second, $r-2$ for the third, and so on, applying the rule of product, the number of injective functions from N to R is:

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

(iii) **Surjective Functions:** A function is surjective (onto) if every element in R has a pre-image in N, meaning every element in R is an image of some element in N. Consider a surjection $f : N \to R = \{y_1, y_2, \ldots, y_r\}$. We observe that the preimages $f^{-1}(y_1), f^{-1}(y_2), \ldots, f^{-1}(y_r)$ form a partition of N into r non-empty subsets, as each element y_i in R corresponds to one or more elements from N. The number of ways to partition N into r parts is given by the Stirling number $S(n, r)$, and since we can permute the r elements in R in $r!$ ways, the total number of surjective functions from N to R is:

$$r!\, S(n, r),$$

where $S(n, r)$ is the Stirling number of the second kind, counting the ways to partition N into r non-empty subsets.

Example: For $N = \{1, 2, 3\}$ and $R = \{y_1, y_2\}$:
Here $|N| = 3$ and $|R| = 2$.

- Total functions: $2^3 = 8$.
- Injective functions: Not possible since $|R| < |N|$.
- Surjective functions: Consider all possible surjective functions:
  $f_1 : \{1, 2\} \mapsto y_1, 3 \mapsto y_2$ - Another possible permutation for this partition: $f_2 : \{1, 2\} \mapsto y_2, 3 \mapsto y_1$
  $f_3 : \{2, 3\} \mapsto y_1, 1 \mapsto y_2$ - Another possible permutation for this partition: $f_4 : 1 \mapsto y_1, \{2, 3\} \mapsto y_2$
  $f_5 : \{1, 3\} \mapsto y_1, 2 \mapsto y_2$ - Another possible permutation for this partition: $f_6 : 2 \mapsto y_1, \{1, 3\} \mapsto y_2$
  So, we have 6 surjective functions. Using the formula for surjective functions, we first find the Stirling number $S(3, 2) = 3$, which corresponds to the number of partitions without considering permutations. Then, accounting for the permutations of the $r = 2$ elements in R, we compute:

$$2! \cdot S(3, 2) = 2! \cdot 3 = 6,$$

which matches the number of surjective functions we listed.

6 Generating functions

Generating Series

Instead of viewing a sequence as a function that returns its nth term, a *generating series* packages all of its terms into a single power series whose coefficients are exactly the sequence entries. Concretely, the sequence

$$2,\ 3,\ 5,\ 8,\ 12,\ \ldots$$

is encoded by the generating series

$$2 + 3x + 5x^2 + 8x^3 + 12x^4 + \cdots .$$

In general, given any sequence $\{c_n\}_{n \geq 0}$, its generating series is the formal power series

$$G(x) \;=\; \sum_{n=0}^{\infty} c_n x^n \;=\; c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots .$$

We say that $G(x)$ "generates" the sequence $\{c_n\}$ because each coefficient of x^n in $G(x)$ is precisely c_n. Generating series turn sequence-based problems into algebraic manipulations of power series, a technique we will exploit heavily in what follows.

Recall of the Basic Series

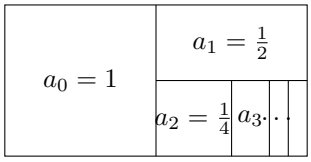


Figure 1: A geometric interpretation of the binary series, showing how $\sum_{n=0}^{\infty} \frac{1}{2^n} = 2$.

A Geometric View of the Binary Series For $|x| < 1$, we have the infinite geometric series

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \sum_{n=0}^{\infty} x^n.$$

We now present a quick proof of this result by performing long division of 1 by $1 - x$.

$$\begin{array}{r|l} & 1 + x + x^2 + x^3 + \cdots \\ 1 - x & 1 \\ \hline & \underline{1 - x} \\ & x \\ & \underline{x - x^2} \\ & x^2 \\ & \underline{x^2 - x^3} \\ & x^3 \\ & \vdots \end{array}$$

The process works as follows: The long-division proceeds by repeatedly dividing the current remainder by the leading term of the divisor, producing one new power of x at each step:

1. Divide 1 by $1 - x$. The multiplier needed to eliminate the constant term is 1, so

   $$1 - 1 \cdot (1 - x) = x.$$

   Thus the first summand is 1, leaving a remainder of x.

2. Divide the remainder x by $1 - x$. The multiplier is x, so

   $$x - x \cdot (1 - x) = x^2.$$

   Hence the second summand is x, leaving a remainder of x^2.

3. Divide x^2 by $1 - x$. The multiplier is x^2, giving

   $$x^2 - x^2 \cdot (1 - x) = x^3.$$

   Therefore the third summand is x^2, with remainder x^3.

4. Continuing in this fashion produces the infinite series

   $$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots .$$

Continuing indefinitely produces

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \sum_{n=0}^{\infty} x^n,$$

as claimed.
We will use this fact in further examples throughout the notes.

Building Generating Functions

The simplest (or "basic") generating function is

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots,$$

which generates the constant sequence $1, 1, 1, \ldots$.

Replacing x with $-x$:

$$\frac{1}{1-(-x)} = \frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots,$$

generating $1, -1, 1, -1, \ldots$.

Replacing x with $3x$:

$$\frac{1}{1-3x} = 1 + 3x + 9x^2 + 27x^3 + \cdots,$$

generating $1, 3, 9, 27, \ldots$.

Scaling a sequence by 3:

$$\frac{3}{1-3x} = 3 + 9x + 27x^2 + 81x^3 + \cdots,$$

generating $3, 9, 27, 81, \ldots$.

Termwise addition of sequences:
Adding the generating functions for $1, 1, 1, \ldots$ and $1, 3, 9, \ldots$ gives

$$\frac{1}{1-x} + \frac{1}{1-3x} = 2 + 4x + 10x^2 + 28x^3 + \cdots,$$

which generates $2, 4, 10, 28, \ldots$.

Replacing x with x^2:

$$\frac{1}{1-x^2} = 1 + x^2 + x^4 + x^6 + \cdots,$$

generating $1, 0, 1, 0, 1, 0, \ldots$.

Shifting a sequence:
Multiplying by x shifts all coefficients right by one:

$$\frac{x}{1-3x} = 0 + x + 3x^2 + 9x^3 + \cdots,$$

generating $0, 1, 3, 9, \ldots$, and

$$\frac{x}{1-x^2} = 0 + x + 0x^2 + x^3 + \cdots,$$

generating $0, 1, 0, 1, \ldots$.

Combining shifted sequences:
Adding the two "even-odd" generating functions recovers

$$\frac{1}{1-x^2} + \frac{x}{1-x^2} = \frac{1+x}{1-x^2} = \frac{1}{1-x},$$

which generates $1, 1, 1, 1, \ldots$.

Differentiation:
Differentiating the basic Generating Function

$$\frac{d}{dx}\Big(\frac{1}{1-x}\Big) = \frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + 4x^3 + \cdots,$$

yields the generating function for $1, 2, 3, 4, \ldots$.

Recurrence Relations & Generating Functions

We conclude with an example of one of the many reasons studying generating functions is helpful: solving recurrence relations via algebraic manipulation of power series.

Example: Tower of Hanoi The minimum number of moves required to transfer n disks satisfies

$$a_0 = 0, \quad a_1 = 1, \quad a_n = 2\,a_{n-1} + 1 \quad (n \geq 1),$$

giving the sequence

$$0,\ 1,\ 3,\ 7,\ 15,\ 31, \ldots$$

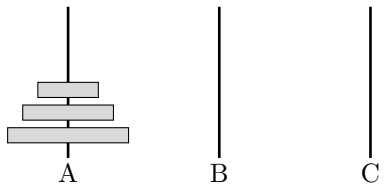


Figure 2: Initial configuration for Tower of Hanoi (3 disks).

Define the generating function

$$f(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Using the recurrence for $n \geq 1$:

$$\sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty} \big(2a_{n-1} + 1\big)x^n = 2x \sum_{n=0}^{\infty} a_n x^n + \sum_{n=1}^{\infty} x^n,$$

so

$$f(x) - a_0 = 2x\, f(x) + \frac{x}{1-x},$$

and since $a_0 = 0$,

$$f(x) = \frac{x}{(1-x)(1-2x)}.$$

Performing partial fractions:

$$\frac{x}{(1-x)(1-2x)} = \frac{-1}{1-x} + \frac{1}{1-2x},$$

hence

$$f(x) = -\frac{1}{1-x} + \frac{1}{1-2x}.$$

Extracting coefficients yields the closed-form solution

$$a_n = 2^n - 1,$$

confirming the well-known formula for the Tower of Hanoi moves.

6.1 Introduction to the Fibonacci Sequence

The Fibonacci sequence famously arises from a puzzle involving rabbit populations. Imagine starting with a single pair of rabbits that takes one month to mature. After maturing, each pair produces a new pair of rabbits every month. Mathematically, if F_n represents the number of rabbit pairs in month n, the sequence satisfies the initial conditions

$$F_0 = 0, \quad F_1 = 1,$$

and the recurrence

$$F_{n+2} = F_{n+1} + F_n \quad \text{for } n \geq 0.$$

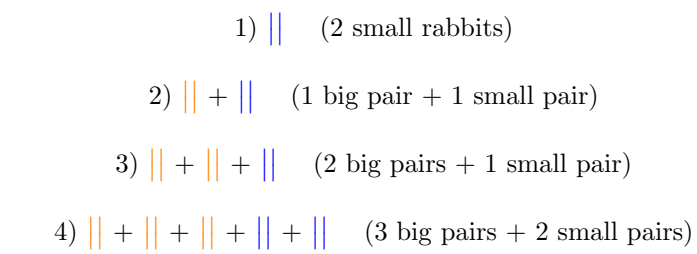


Figure 3: Illustration of rabbit pairs over successive months. Blue bars represent small rabbits; orange bars represent big (mature) rabbits.

Q: is there a non-recursive (closed-form) formula for F_n ?

Idea: consider and calculate it

6.2 Deriving the Closed-Form for the Fibonacci Sequence

Step 1: Define the generating function. Let $\{F_n\}_{n=0}^{\infty}$ be the Fibonacci sequence with

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n \quad (n \geq 0).$$

Define the generating function

$$f(x) \;=\; \sum_{n=0}^{\infty} F_n\, x^n.$$

We aim to find a closed-form expression for $f(x)$, and then extract a formula for F_n.

Step 2: Use the Fibonacci recurrence in $f(x)$. Starting from

$$f(x) \;=\; F_0 + F_1 x + \sum_{n=2}^{\infty} F_n\, x^n,$$

and noting $F_0 = 0$, $F_1 = 1$, we have

$$f(x) \;=\; x + \sum_{n=2}^{\infty} \big(F_{n-1} + F_{n-2}\big)\, x^n$$

because $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Separate the sums:

$$f(x) = x + \sum_{n=2}^{\infty} F_{n-1}\, x^n + \sum_{n=2}^{\infty} F_{n-2}\, x^n.$$

Shift indices to factor out $f(x)$:

$$\sum_{n=2}^{\infty} F_{n-1}\, x^n = x \sum_{n=2}^{\infty} F_{n-1}\, x^{n-1} = x \sum_{m=1}^{\infty} F_m\, x^m = x\big(f(x) - F_0\big) = x\, f(x),$$

since $F_0 = 0$. Similarly,

$$\sum_{n=2}^{\infty} F_{n-2}\, x^n = x^2 \sum_{n=2}^{\infty} F_{n-2}\, x^{n-2} = x^2 \sum_{k=0}^{\infty} F_k\, x^k = x^2\, f(x).$$

Hence,

$$f(x) = x + x\, f(x) + x^2\, f(x) \;\;\Longrightarrow\;\; f(x)\big(1 - x - x^2\big) = x.$$

Thus,

$$f(x) = \frac{x}{1 - x - x^2}.$$

Step 3: Partial-Fraction Decomposition (as in the images). First, rewrite

$$\frac{1}{1 - x - x^2} \;=\; \frac{1}{-\big(x^2 + x - 1\big)} \;=\; -\,\frac{1}{x^2 + x - 1}.$$

Next, factor $x^2 + x - 1$. Observe that the roots of

$$x^2 + x - 1 \;=\; 0$$

are

$$x \;=\; -\,\frac{1 + \sqrt{5}}{2} \quad \text{and} \quad x \;=\; -\,\frac{1 - \sqrt{5}}{2}.$$

Hence,

$$x^2 + x - 1 \;=\; \Big(x + \tfrac{1+\sqrt{5}}{2}\Big) \cdot \Big(x + \tfrac{1-\sqrt{5}}{2}\Big).$$

Therefore,

$$-\,\frac{1}{x^2 + x - 1} \;=\; -\,\frac{1}{\Big(x + \frac{1+\sqrt{5}}{2}\Big)\Big(x + \frac{1-\sqrt{5}}{2}\Big)}.$$

We look for constants A and B such that

$$-\,\frac{1}{\Big(x + \frac{1+\sqrt{5}}{2}\Big)\Big(x + \frac{1-\sqrt{5}}{2}\Big)} \;=\; \frac{A}{x + \frac{1+\sqrt{5}}{2}} \;+\; \frac{B}{x + \frac{1-\sqrt{5}}{2}}.$$

Step 4: Solve for A and B. Comparing coefficients of x and the constant term in

$$-1 \;=\; A\Big(x+\beta\Big) \;+\; B\Big(x+\alpha\Big),$$

we obtain the system

$$\begin{cases} A + B = 0, \\ A\,\beta + B\,\alpha = -1. \end{cases}$$

It follows that

$$B = -A, \quad A\,(\beta-\alpha) = -1 \;\;\Longrightarrow\;\; A = \frac{1}{\alpha-\beta} \quad \text{and} \quad B = -\,\frac{1}{\alpha-\beta}.$$

Hence,

$$-\,\frac{1}{(x+\alpha)(x+\beta)} \;=\; \frac{1}{\alpha-\beta}\,\frac{1}{x+\alpha} \;-\; \frac{1}{\alpha-\beta}\,\frac{1}{x+\beta}.$$

Step 5: Combine with the earlier factor -1 and rewrite. Recalling that

$$\frac{1}{1-x-x^2} \;=\; -\,\frac{1}{x^2+x-1} \;=\; -\,\frac{1}{(x+\alpha)\,(x+\beta)},$$

we combine the above result to conclude

$$\frac{1}{1-x-x^2} \;=\; \frac{1}{\alpha-\beta}\left(\frac{1}{x+\alpha} \;-\; \frac{1}{x+\beta}\right).$$

Step 6: Expand each term in a power series. Notice that

$$\frac{1}{x+\alpha} \;=\; \frac{1}{\alpha}\,\frac{1}{1+\frac{x}{\alpha}} \;=\; \frac{1}{\alpha}\sum_{n=0}^{\infty}\big(-\tfrac{x}{\alpha}\big)^n \;=\; \sum_{n=0}^{\infty}\frac{(-1)^n}{\alpha^{\,n+1}}\,x^n,$$

valid for $\left|\frac{x}{\alpha}\right| < 1$. Similarly,

$$\frac{1}{x+\beta} \;=\; \sum_{n=0}^{\infty}\frac{(-1)^n}{\beta^{\,n+1}}\,x^n.$$

Hence,

$$\frac{1}{1-x-x^2} \;=\; \frac{1}{\alpha-\beta}\left[\sum_{n=0}^{\infty}\frac{(-1)^n}{\alpha^{\,n+1}}\,x^n \;-\; \sum_{n=0}^{\infty}\frac{(-1)^n}{\beta^{\,n+1}}\,x^n\right] = \sum_{n=0}^{\infty}\left[\frac{1}{\alpha-\beta}\Big(\frac{(-1)^n}{\alpha^{\,n+1}} \;-\; \frac{(-1)^n}{\beta^{\,n+1}}\Big)\right]x^n.$$

Step 7: Identify Fibonacci numbers. Recall that $\alpha-\beta=\sqrt{5}$, and

$$F_n \;=\; \frac{\alpha^n-\beta^n}{\alpha-\beta} \;=\; \frac{\alpha^n-\beta^n}{\sqrt{5}}.$$

One checks (or uses known identities) to see that the coefficient of x^n in the above power series is exactly F_n. Consequently,

$$\sum_{n=0}^{\infty}F_n\,x^n \;=\; \frac{1}{1-x-x^2},$$

which is the generating function for the Fibonacci sequence.

Conclusion. We have shown that the generating function for the Fibonacci sequence is $\frac{x}{1-x-x^2}$. Through partial fractions and comparing coefficients, we deduced that

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

This gives a non-recursive (closed-form) expression for F_n, completing the derivation.

Additional Examples and Proofs from the Notes

Example on Counting Words

Let S be the set of all words of length n over the alphabet $\{0, 1\}$. By the rule of product, each letter has 2 choices, and hence

$$|S| = 2^n.$$

Furthermore, if one wants to count the number of words with a given number of zeros and ones, one uses the binomial coefficient.

Example on Bijections for Power Sets

Consider a set $X = \{x_1, x_2, \ldots, x_n\}$. Each subset of X can be represented by an n-tuple of 0's and 1's. The mapping that sends each subset to its corresponding binary vector is a bijection. This proves that

$$|\mathcal{P}(X)| = 2^n.$$

Proof of the Recurrence for Stirling Numbers

Given an n-set, consider the addition of a new element x. When partitioning the set into k blocks, either:

- x forms a block by itself (which gives $S(n-1, k-1)$ partitions), or
- x is added to one of the k blocks of a partition of the remaining $n-1$ elements (which gives $k\,S(n-1, k)$ partitions).

Thus, we obtain

$$S(n, k) = S(n-1, k-1) + k\,S(n-1, k).$$

Proof of Derangements using Inclusion-Exclusion

For the set $N = \{1, 2, \ldots, n\}$, define

$$A_i = \{\sigma \in S_n \mid \sigma(i) = i\}.$$

Then, by the inclusion-exclusion principle,

$$D(n) = n! - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|.$$

Since $|A_i| = (n-1)!$, $|A_i \cap A_j| = (n-2)!$, and in general

$$|A_{i_1} \cap \cdots \cap A_{i_k}| = (n-k)!,$$

we have:

$$D(n) = n! \left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right].$$