Counting

Rajiv Raman

October 30, 2023

Abstract

These notes provide a quick background on basic Counting.

1 Introduction

Theorem 1

Let X and Y be two sets, where $|X| = n$ and $|Y| = m$. The number of functions $f : X \to Y$ is m^n.

Proof. We prove by induction on $|X|$. If $X = \emptyset$, then there is just one function, namely the empty function, which is $m^0 = 1$. Suppose for $|X| = n$ and any $m = |Y|$, the number of functions is m^n. Consider a set X of size $n+1$. Let $x_1, \ldots, x_{n+1}$ be the elements in X. For any function $f : X \to Y$, there are m functions $f' : X \setminus \{x_{n+1}\} \to Y$ for each available choice for the element x_{n+1}. By the inductive hypothesis, the number of function $f' : X \setminus \{x_{n+1}\} \to Y$ is m^n. Therefore, the number of functions $f : X \to Y$ is

$$m^n m = m^{n+1}$$

□

Exercise 1

How many distinct 7 letter words are there in the English alphabet?

Solution: Since there is a bijection between the number of functions from a set of size 7 to a set of size 26, the number of words is 26^7.

Exercise 2

There are 26 types of postcards at a store. You want to select 7 postcards to send to your friends. In how many different ways can you choose the postcards to send to your friends?

Solution: There is a bijection between the number of functions from a set of size 7 to a set of size 26 to the different ways in which you can select 26 types of postcards to your seven friends.

In both cases, we viewed the set X as the letters of the 7 letter word in the first case, and the 7 friends in the second case; the set Y is the 26 letters of the English alphabet. Each position of the word gets a single letter, and similarly each friend receives a single postcard. Since there are no other restrictions, it is easy to see that the numbers in both cases are equivalent to the number of functions between appropriately chosen sets.

The idea of obtaining a *bijection* is a central idea in counting. To count the number of elements in a set, obtain a bijection to a set whose cardinality is known.

Theorem 2

Any set X of size n has 2^n subsets.

Proof. Let $f : X \to \{0, 1\}$. By Theorem 1, the number of such functions is 2^n. Such a function is called a *characteristic function*. There is a bijection between the power set of X and functions $f : X \to \{0, 1\}$. For a function f, let $S = \{x : f(x) = 1\}$. In other words, let $\mathcal{F}$ denote the set of all functions from X to $\{0, 1\}$. Note that each element in $\mathcal{F}$ is a function. Let $\mathcal{P}(X)$ denote the power set of X.

Let $g : \mathcal{F} \to \mathcal{P}(X)$ be the following function:

$$g(f) = \{x \in X : f(x) = 1\}$$

That is, g maps a particular function f to the subset of X that it maps to 1. To see that this is a bijection, note that g is an injection, and g^{-1} is well defined; for $S \in \mathcal{P}(X)$, $g^{-1}(S) = \{f : X \to \{0, 1\} : f(x) = 1 \Leftrightarrow x \in S\}$. □

Theorem 3

Any non-empty set X has exactly 2^{n-1} sets of odd size and 2^{n-1} sets of even size.

Proof. Let $n = |X|$. Let $a \in X$, and consider the set $X' = X \setminus \{a\}$. Then, the number of functions from $X' \to \{0, 1\}$ is 2^{n-1} by Theorem 2. Let $A' \subseteq X'$. We associate a subset $A \subseteq X$ as follows: If A' is an odd-sized subset, then set $A = A'$. Otherwise, set $A = A \cup \{a\}$. Hence, we have established a bijection between the number of odd-sized subsets of X and all subsets of $X \setminus \{a\}$. Therefore, the number of odd-sized subsets of X is 2^{n-1}. □

We provide an alternate proof.

Alternate proof: Let $\mathcal{O}_X, \mathcal{E}_X$ denote the odd-sized subsets and even-sized subsets, respectively of X. That is, $\mathcal{O}_X = \{S \in \mathcal{P}(X) : |S| \text{ is odd}\}$, and $\mathcal{E}_X = \{S \in \mathcal{P}(X) : |S| \text{ is even}\}$. Note that $\mathcal{O}_X$ and $\mathcal{E}_X$ form a *partition* of $\mathcal{P}(X)$, i.e.,

$$\mathcal{O}_X \cap \mathcal{E}_X = \emptyset$$
$$\mathcal{O}_X \cup \mathcal{E}_X = \mathcal{P}(X)$$

Thus, if we show that $|\mathcal{O}_X| = |\mathcal{E}_X|$, then it must be that $|\mathcal{O}_X| = |\mathcal{P}(X)|/2 = 2^{n-1}$. Let $X = \{x_1, \ldots, x_n\}$. Consider the function $f : \mathcal{O}_X \to \mathcal{E}_X$ defined as follows:

$$f(S) = \begin{cases} S \cup \{x_n\}, & x_n \notin S \\ S \setminus \{x_n\}, & x_n \in S \end{cases}$$

In other words, fix an element of X, say x_n. If a set $S \in \mathcal{O}_n$ contained x_n, it is mapped to the set $S \setminus \{x_n\}$, which has even cardinality and hence in $\mathcal{E}_n$. On the other hand, if $x_n \notin S$, we map S to the set $S \cup \{x_n\}$, which again is even; and hence in $\mathcal{E}_n$. It is easy to check that f is a bijection, which implies $|\mathcal{O}_n| = |\mathcal{E}_n|$ and we are done. □

Now we compute the number of injective functions from a finite set X to a set Y. Note that if there is an injective function, then necessarily $|X| \leq |Y|$.

Theorem 4

The number of injective functions from a set X of size n to a set Y of size m is

$$m^{\underline{n}} = m(m-1)\ldots(m-n+1)$$

If $m = n$, the number of functions is $m! = m(m-1)\ldots 1$.

Proof. We prove by induction on X. If $X = \emptyset$, then the empty function is injective. Suppose for $|X| = n-1$, the number of injective functions is as claimed. Consider a set $X = \{x_1, \ldots, x_n\}$ of size n. Let $X' = X \setminus \{x_n\}$. By the inductive hypothesis, the number of injective functions from X' to Y is $m^{\underline{n-1}} = m(m-1)\ldots(m-n+1)$. For each of the $m-1$ choices for x_n, we have by induction, $(m-1)^{\underline{n-1}}$ injective functions from X' to $Y \setminus \{f(x_n)\}$. Hence, the number of injective functions from X to Y is

$$\begin{aligned} m \cdot (m-1)^{\underline{n-1}} &= m(m-1)\ldots(m-n+1) \\ &= m^{\underline{n}} \end{aligned}$$

□

Exercise 3

How many 7 letter words with distinct letters can be formed with letters from the English alphabet?

Solution:
This is precisely the number of injective functions from a set of size 7 to a set of size 26, and is therefore given by $26^{\underline{7}} = 26(26-1)(26-2)\ldots(26-6)$.

Exercise 4

Determine the number of ordered pairs (A, B), where $A \subseteq B \subseteq X$, where $|X| = n$.

Exercise 5

Show that a natural number $n \geq 1$, has an odd number of divisors (including 1 and itself) if and only if $\sqrt{n}$ is an integer.

Exercise 6

Determine the number of surjective functions from a set X of size n to a set Y of size m.

2 Permutations

if $|X| = |Y|$, and $f : X \to Y$ is an injective function, it follows that f is a bijection. A bijective function $f : X \to X$ is called a *permutation*. By Theorem 4, the number of permutations of an n element set is $n!$.

We represent permutations in a two-row form as follows:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

The first row consists of the elements of the set X and the second row lists $f(x)$ where f is the permutation. Sometimes, we use a shortened notation:

$$(2\ 1\ 4\ 3)$$

Another way of representing permutations is via their cycles. For example, if f is the permutation (4 5 3 2 9 0 1 7 6 8), which is represented in Figure 1. Using cycles, the permutation can also be represented as $((0, 4, 9, 8, 6, 1, 5)(2, 3)(7))$.

Exercise 7

How many permutations have a single cycle? (n-1)!

For a permutation, let p^2 denote the composition of p with itself, i.e., $p^2 = p \circ p$. Note that p^2 is a permutation as the composition of bijections is a bijection. Similarly, we define

$$p^k = \underbrace{p \circ p \ldots p}_{k \text{ times}}$$

Let *id* denote the *identity permutation*, i.e., the permutation that maps each element to itself. For a permutation p on n elements, let the *order* of a permutation be the smallest k such that $p^k = id$.

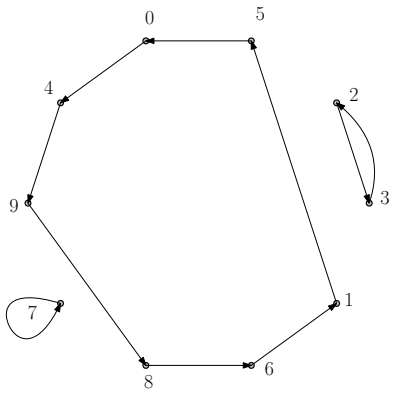


Figure 1: A cycle representation of the permutation (4 5 3 2 9 0 1 7 6 8)

Exercise 8

1. Prove that for any permutation on n elements, its order is finite.
2. If $p = C_1C_2 \dots C_\ell$ be a permutation written as a product of cycles $C_1C_2 \dots C_\ell$. What is the relation between $|C_i|$ and the order of a permutation?

2.1 Cyclic Permutations

In many settings, we are interested in counting the number of different ways we can place the elements of a set in a circular fashion. In this setting, any cyclic shift correspond to the same permutation.

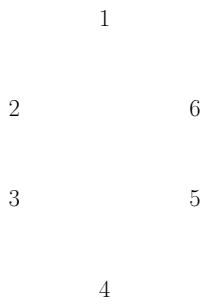


Figure 2: A cyclic permutation of $\{1, 2 \dots, 6\}$

For example, the set of permutations $123456, 234561, 345612, 456123, 561234, 612345$ all yield the same the of cyclic permutation in Figure 2. Thus, 6 permutations map to a single cyclic permutation. The number of cyclic permutations is therefore given as follows:

Theorem 5

The number of circular r-permutations of a set of n elements is given by

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

In particular, the number of cyclic permutations of an n element set is $(n-1)!$

Exercise 9

In how many ways can ten students, two of whom do not wish to sit next to each other be seated around a round table?

Exercise 10

How many different necklaces can we make with 12 distinct beads? *Note: we could consider two cyclic sequences of beads to be identical if one can be obtained from the other by reflection, but we don't consider such operations. We only allow cyclic shifts.*

3 r-Permutations

An r-permutation of a set of n elements is a permutation of r elements of a set. The number of r permutations of a set of n elements is equal to the number of injective functions from an r element set to an n element set. Thus, the number of r-permutations of an n-element set, denoted $P(n,r)$ is given by

$$P(n,r) = n(n-1)\dots(n-r+1) = \frac{n!}{(n-r)!}$$

Exercise 11

In how many ways can we order the 26 letters of the English alphabet so that no two vowels, i.e., the letters $\{a,e,i,o,u\}$ appear consecutively?

Solution: The number of permutations of the 21 consonants is 21!. Since no two vowels are consecutive, they occupy the *gaps* between the consonants. There are 22 gaps between the consonants including the gap before the first consonant, or after the last consonant. The number of such permutations is given by

$$P(22,5) = \frac{22!}{(22-5)!} = \frac{22!}{17!}$$

Any permutation of the consonants and any choice of the permutation for the vowels yields a permutation such that no two vowels are consecutive. Therefore, the total number

of permutations is

$$21! \cdot \frac{22!}{17!}$$

Exercise 12

How many 7 digit numbers can be formed by using distinct digits such that the digits 5 or 6 do not appear consecutively?

Solution: Consider the set of all such numbers that can be formed: They can be classified into three types - those that don't contain either 5 or 6, those that contain exactly one of 5 or 6; and finally, those that contain both 5 and 6 but not consecutively. It will turn out to be easier to count these types separately.

The first type is easiest, there are 8 digits and since there is no restriction the number of 7 digit numbers that can be formed is $P(8,7) = 8!/(8-7)! = 8!$.

For the second type, we can again split into two types - those that contain only 5 and those that contain only 6. Their cardinalities are the same, and the number of each is $P(9,7) = 9!/2!$. Therefore, the total number of digits containing exactly one of 5 or 6 is $2 \cdot 9!/2!$.

Finally, for the third type, the argument is similar to the one in the problem above. There are $P(8,5) = 8!/3!$ permutations of 5 digits from the digits $\{0,\ldots,9\}\setminus\{5,6\}$. Since 5 and 6 do not appear consecutively, they occupy the 6 gaps between these digits. The number of ways in which we can place 5 and 6 so that they don't appear consecutively is therefore $P(6,2) = 6!/4!$. Hence, the total number of the third type is $8!/3!6!/4!$.

The total number of digits is therefore, the number of digits of each of the three types which is

$$8! + 2\frac{9!}{2!} + \frac{8!6!}{3!4!} = 8! + 9! + \frac{8!6!}{3!4!}$$

Exercise 13

How many orderings of a deck of 52 cards can we form if all cards of the same suit are together?

Exercise 14

How many distinct positive divisors do the following numbers have?

1. $3^4 \times 5^2 \times 7^6 \times 11$
2. 620

3. 10^10

Exercise 15

Determine the largest power of 10 that is a factor of the following numbers:

1. 50!
2. 1000!

4 r-Combinations

The number of unordered subsets of size r a set X of size n is called an r-combination. The number of r-combinations is given by the following argument. The number of r-permutations is $P(n,r)$. For any subset or r elements of X, they yield $r!$ distinct permutations. Therefore, the number of r combinations is $P(n,r)/r!$. The number of r-combinations, denoted $C(n,r)$, or more popularly as $\binom{n}{r}$ is given by:

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

By symmetry, we can readily observe that the number of r-combinations of a set of size n is identical to the number of $n-r$-combinations. One way to see this is that there is a bijection between sets of size r and sets of size $n-r$ - for a set S of size r, we map it to the unique set $X \setminus S$ of size $n-r$. Alternately, this follows immediately from the symmetry of the function $C(n,r)$.

Proposition 1.

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

Proposition 2.

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

Proof. The number of subsets of a set of size n is 2^n as we proved earlier. We can partition the subsets by their size, and for size, their number is given by the number of r-combinations, i.e., $\binom{n}{i}$. □

We now prove a very useful identity that we'll see many times.

Theorem 6 (Pascal's identity)

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

Proof. The LHS counts the number of subsets of size r of a set X of size n. Fix a particular element $x \in X$. The subsets of size r can be partitioned into two types: those that contain x and those that don't. The number of subsets is therefore the sum of the cardinalities of the two types of subsets The number of the first type is $\binom{n-1}{r}$ as we are not allowed to choose the element x. The number of the second type is $\binom{n-1}{r-1}$, as we choose x into a subset, and then choose the remaining $r-1$ elements from the remaining $n-1$ elements. □

Of course, we can also prove the identity by painful algebraic manipulation. The proof given above is an example of a *combinatorial proof*, and to prove binomial identities, when we ask to show a binomial identity via a combinatorial argument, we mean an argument like the one above.

Next, we will see some more examples of combinatorial proofs of binomial identities.

Exercise 16

$\sum_{j=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$

Solution: The right hand side counts the number of ways in which we can choose n elements from a collection of $2n$ elements. From Proposition 1, we have $\binom{n}{r} = \binom{n}{n-r}$. So let us write

$$\binom{n}{r}^2 = \binom{n}{r}\binom{n}{n-r}$$

We can view the right hand side as the number of ways in which to choose n balls from two boxes B_1 and B_2. Box B_1 contains n red balls and box B_2 contains n blue balls. Then, the RHS in the expression above counts the number of ways in which we can pick r red and $n-r$ blue balls. With this interpretation, we can give a combinatorial interpretation of the LHS of the identity. The sum over the terms $\binom{n}{r}\binom{n}{n-r}$ is the total number of ways in which we can choose n elements from $2n$ elements, n of which are red and the remaining are blue. We can do this by choosing r of them that are red and the remaining ones that are blue, where r ranges from 0 to n.

5 Multisets

A *multiset* is a generalization of a set, where we allow *multiplicites* of the elements. For example $\{2 \cdot a, 3 \cdot b, 1 \cdot c\}$ is a multiset containing two as, 3 bs and one c. Likewise $\{\infty \cdot a, \infty \cdot b\}$ is a multiset containing infinitely many as and infinitely many bs. When we say infinitely many, we always mean countably infinite. The elements a, b, c are called the *types*.

Theorem 7

Let S be a multiset with k types of objects, each of infinite multiplicity. The number of r-permutations of S is k^r.

Proof. Each of the r positions in the permutation can be occupied by any one of the k types of elements. □

Theorem 8

Let S be a multiset with objects of k different types with multiplicities $n_1, \ldots, n_k$. Let the set S be $n = n_1 + \ldots + n_k$. The number of permutations of S is given by

$$\binom{n}{n_1; n_2; \ldots; n_k} = \frac{n!}{n_1! n_2! \ldots n_k!}$$

Proof. The first element can choose n_1 of the n positions in $\binom{n}{n_1}$ ways. The second can choose n_2 among the remaining positions in $\binom{n-n_1}{n_2}$ ways. The third can choose n_3 in the remaining positions in $\binom{n-n_1-n_2}{n_3}$ ways, and so on. This gives:

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-n_2-\ldots-n_{k-1}}{n_k}$$

Expanding and simplifying, we get the desired expression. □

We can view the previous expression as the number of ways in which we can place n labelled balls into k labelled boxes.

Theorem 9

The number of ways in which we can place n labelled balls into k labelled bins such that Bin i receives n_i balls is $\binom{n}{n_1;\ldots;n_k}$.

Typically, counting problems where the number of bins is unlabelled are harder. However, for the following problem we have a simple expression.

Theorem 10

The number of ways in which n balls can be placed into k unlabelled bins so that each bin receives $m = n/k$ balls is given by

$$\frac{n!}{k!(m!)^k}$$

Proof. If we temporarily label the boxes, we have $k!$ different assignments of balls that correspond to the same assignment if the boxes are unlabelled. Putting $n_1 = n_2 = \ldots = n_k$, and dividing the expression in the previous theorem by $k!$ we obtain the desired expression. □

Exercise 17

In how many ways can we place 8 rooks on a chessboard so that the rooks don't pairwise attack each other.

Solution: Each row and each column can have at most one rook. So we can label any assignment as $(A, i_1), \ldots, (H, i_8)$, where $i_1, \ldots, i_8$ correspond to the columns where the rooks are placed and $A, \ldots, H$ correspond to the rows. Since no column can contain more than one rook, it follows that $i_1, \ldots, i_8$ form a permutation. Therefore, there are 8! different ways of placing rooks so that they don't attack each other.

Exercise 18

In the previous question, what if all the rooks are colored distinctly?

In this case, for each of the 8! distinct placements of non-attacking rooks, there are 8! distinct permutations of the rooks at these positions as the rooks are distinct. Therefore, the total number of placements is $(8!)^2$.

Exercise 19

In the previous question, what if there are 3 red, 2 blue and 3 green rooks?

In this case, for each of the 8! distinct placements of non-attacking rooks, there are $\frac{8!}{3!2!3!}$ distinct permutations of the 3 red, 2 blue and 3 green rooks. Therefore, the total number of placements is $\frac{(8!)^2}{3!2!3!}$.

6 Combination of Multisets

Given a multiset S with k types $a_1, \ldots, a_k$ with multiplicities $n_1, \ldots, n_k$, respectively, an r-combination of S is a sub-multiset S' of S with multiplicities $n'_1, \ldots, n'_k$ of the types $a_1, \ldots, a_k$ such that $n'_1 + n'_2 + \ldots + n'_k = r$.

Theorem 11

Let S be a multiset with k types, each with multiplicity ∞. The number of r-combinations of S is

$$\binom{k+r-1}{r}$$

Proof. Consider a sub-multiset S' of size r obtained from S. We can arrange the elements in S' in sequence according to their type - the elements of type a_1 followed by the elements of type a_2,..., and finally the elements of type a_k. Each sub-multiset S' then corresponds uniquely to such a sequence. We map such sequences bijectively to a sequence with 2 types of elements, namely $*$ and $|$. If the sub-sequence S' has n'_1 $a'_1 s$, n'_2 a_2's and so on, then we associate S' to a sequence with n'_1 $*$s followed by a $|$, followed by a sequence of n'_2 $*$'s, and so on. For example, if S had four types $a_1, \ldots, a_4$ and $S' = a_1 a_1 a_1 a_3 a_3 a_4$ then, we obtain the sequence $* * * | | * * | *$. But, we know how to count such sequences - it is the number of permutations of r $*$'s and $k-1$ $|$'s, which is given by $\frac{(k+r-1)!}{r!(k-1)!} = \binom{r+k-1}{r}$. □

Example 1

A sweet shop sells 8 different types of sweets. In how many ways can you make a box of a dozen sweets?

Solution: By a direct application of the theorem above, we obtain that the number distinct boxes we can make is

$$\binom{12+8-1}{12} = \binom{19}{12}$$

Example 2

How many non-decreasing sequences of length r can we form with numbers from $\{1, \ldots, k\}$?

Solution: We can construct any non-decreasing sequence of length r as follows: We choose r_1 1's, r_2 2's, and so on and r_k k's such that $r_1 + \ldots + r_k = r$. For any such choice of numbers, there is exactly one permutation that is non-decreasing. Therefore the number of non-decreasing sequences are, from the theorem above,

$$\binom{r+k-1}{r}$$

Example 3

Let $S = \{10 \cdot a, 10 \cdot b, 10 \cdot c, 10 \cdot d\}$. How many 10-combinations can we form so that each of a, b, c and d appear at least once?

Solution: We can select one each of a, b, c and d. This leaves us with a choice of 6 elements from a multiset $S' = \{9 \cdot a, 9 \cdot b, 9 \cdot c, 9 \cdot d\}$, which is $\binom{6+4-1}{6}$.

Example 4

How many integer solutions do we have of $x_1 + x_2 + x_3 + x_4 = 20$ such that $x_1 \geq 3, x_2 \geq 1, x_3 \geq 0, x_4 \geq 5$?

Solution: We apply a change of variables $y_1 = x_1 - 3, y_2 = x_2 - 1, y_3 = x_3, y_4 = x_4 - 5$. With this transformation, the problem becomes the problem of counting the number of integer solutions to $y_1 + y_2 + y_3 + y_4 = 11$ s.t. $y_i \geq 0$, $i = 1, \ldots, 4$. This number is $\binom{11+4-1}{11} = \binom{13}{11}$.

6.1 Balls and Bins

7 Binomial Coefficients

We have already seen that the terms $\binom{n}{k}$ are called Binomial coefficients. The reason for this term is because of the binomial theorem which we see next.

Theorem 12 (Binomial Theorem)

For any $n \in \mathbb{N}$ and $x, y \in \mathbb{R}$,

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

Proof. We prove by induction on n. For $n = 1$, the left hand side is $(x + y)$. The RHS is

$$\binom{1}{0} x y^0 + \binom{1}{1} x^0 y = x + y$$

Suppose the equation holds for n. Then,

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= (x+y)\left(\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\right) && [\because \text{ I.H}] \\
&= x\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k + y\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} \\
&= \binom{n}{0}x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} \\
&= \binom{n}{0}x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} + \binom{n}{n}y^{n+1} \\
&= \binom{n}{0}x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=1}^{n}\binom{n}{k-1}x^{n-k+1}y^k + \binom{n}{n}y^{n+1} \\
&= \binom{n+1}{0}x^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k} + \binom{n}{k-1}\right]x^{n-k+1}y^k + \binom{n+1}{n+1}y^{n+1} \\
&= \binom{n+1}{0}x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^{n-k+1}y^k + \binom{n+1}{n+1}y^{n+1} && [\because \text{ Pascal's identity}] \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k
\end{aligned}$$

□

Next, we give a shorter combinatorial proof of the same result.

Alternate proof:

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

To obtain the term $x^{n-k}y^k$ we choose y's from k of the terms and the x's from the remaining $(n-k)$. This can be done in $\binom{n}{k}$ ways, Since we have terms $x^{n-k}y^k$ for each $k = 0, \ldots, n$, the result follows. □

The binomial theorem is often stated in the following easier form

Corollary 1. $(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$

Next we see some applications of the binomial theorem:

Example 5

$\sum_{k=0}^{n} \binom{n}{k} = 2^n$ Thus, the number of subsets of a set of size n is 2^n. Put $x = 1$ in the corollary of the binomial theorem. Then the LHS is $(1+x)^n = (1+1)^n = 2^n$. The RHS is $\sum_{k=0}^{n} \binom{n}{k}$

Example 6

The number of even sized subsets of a set of size n is equal to the number of odd-sized subsets.

Solution: Put $x = -1$ in the corollary of the binomial theorem. Then, the LHS is $(1-1)^n = 0^n = 0$. The RHS is $\sum_{k=0}^{n} \binom{n}{k}(-1)^k$, thus

$$0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots + (-1)^n \binom{n}{n}$$

Thus, we obtain

$$\binom{n}{0} + \binom{n}{2} + \ldots + \binom{n}{2\lfloor n/2 \rfloor} = \binom{n}{1} + \binom{n}{3} + \ldots + \binom{n}{2\lfloor n/2 \rfloor + 1}$$

Thus, the number of odd-sized subsets of a set of size n is equal to the number of even sized subsets of a set of size n. Since the total number of sets is 2^n, each collection has size 2^{n-1}.

8 Pascal's triangle

Arranging the binomial coefficients in rows we obtain the following triangle called Pascal's triangle. The figure below shows the first 9 rows. Replacing the binomial coefficients by their values, we obtain the next figure. A lot of binomial identities can be inferred from the triangle.

$$\begin{array}{ccccccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & & & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & & & & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} & & & & \\
 & \binom{7}{0} & & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & \binom{7}{7} & \\
\binom{8}{0} & & \binom{8}{1} & & \binom{8}{2} & & \binom{8}{3} & & \binom{8}{4} & & \binom{8}{5} & & \binom{8}{6} & & \binom{8}{7} & & \binom{8}{8}
\end{array}$$

$$
\begin{array}{ccccccccccccccc}
 & & & & & & 1 & & & & & & & & \\
 & & & & & 1 & & 1 & & & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & \\
 & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & \\
8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1
\end{array}
$$

Let the rows be numbered from 0 onwards. It is easy to check that the sum of entries in row i add up to 2^i. Applying Pascal's identity, it follows that obtain the entry $\binom{n}{i}$, we add up the two entries that are diagonally above, that is $\binom{n-1}{i-1}$ and $\binom{n-1}{i}$.

$$
\begin{array}{ccccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & & & \\
 & & & & & \swarrow & & \searrow & & & & & & & \\
 & & & & \binom{1}{0} & & & & \binom{1}{1} & & & & & & \\
 & & & \swarrow & & \searrow & & \swarrow & & \searrow & & & & & \\
 & & \binom{2}{0} & & & & \binom{2}{1} & & & & \binom{2}{2} & & & & \\
 & \swarrow & & \searrow & & \swarrow & & \searrow & & \swarrow & & \searrow & & & \\
\binom{3}{0} & & & & \binom{3}{1} & & & & \binom{3}{2} & & & & \binom{3}{3} & & \\
 & \swarrow & & \searrow & & \swarrow & & \searrow & & \swarrow & & \searrow & & & \\
 & & \binom{4}{0} & & & & \binom{4}{1} & & & & \binom{4}{2} & & & & \binom{4}{3} & & & & \binom{4}{4}
\end{array}
$$

Next, let us observe that $1^2 = 1$, $1^2 + 1^2 = 2$, $1^2 + 2^2 + 1^2 = 6$, $1^2 + 3^2 + 3^2 + 1^2 = 20$, $1^2 + 4^2 + 6^2 + 6^2 + 4^2 + 1^2 = 70$, and so on. That is,

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

We have already proved this identity.

Next, we prove the *hockeystick identity* - summing up the entries starting from $\binom{n}{0}$ and going down diagonally to the right. Observe that $\binom{0}{0} + \binom{1}{1} = 1+1 = 2 = \binom{2}{1}$, $\binom{0}{0} + \binom{1}{1} + \binom{2}{2} = 1+1+1 = 3 = \binom{3}{1}$, and so on. Likewise,

Figure 3: The figure above shows the hockeystick identity, i.e., $\sum_{j=0}^{r} \binom{n+j}{j} = \binom{n+r+1}{r}$.

Of course, while Pascal's triangle allows us to observe potential identities, we still need to prove them to be certain that what we're seeing is not an artifact of the subset of the triangle we are observing. Thus, let us prove the above hockeystick identity.

Theorem 13

For any $n \in \mathbb{N}$ and $r \in \mathbb{N}$, $r \leq n$ we have

$$\sum_{j=0}^{r} \binom{n+j}{j} = \binom{n+r+1}{r}$$

Proof. We prove by induction on r. For $r = 0$, we have $\binom{n}{0} = \binom{n+1}{0} = 1$.

Suppose the identity holds for $r-1$. Then,

$$\begin{aligned}
\sum_{j=0}^{r} \binom{n+j}{j} &= \sum_{j=0}^{r-1} \binom{n+j}{j} + \binom{n+r}{r} \\
&= \binom{n+r}{r-1} + \binom{n+r}{r} \\
&= \binom{n+r+1}{r} && [\because \text{ Pascal's identity}]
\end{aligned}$$

□

We give an alternate *combinatorial proof.*

Alternate proof. A subset of size $r+1$ from a set of size $n+r+1$ can be obtained by choosing the largest element and then the rest. There are $\binom{n+r}{r}$ subsets such that the $(n+r+1)^{th}$ element is the largest. There are $\binom{n+r-1}{r-1}$ elements where both the $(n+r+1)^{th}$ and $(n+r)^{th}$ elements are chosen. There are $\binom{n+r-2}{r-2}$ subsets where the $(n+r+1)^{th}, (n+r)^{th}$, and $(n+r-1)^{th}$ elements are chosen, and so on. Hence, the RHS counts the number of subsets of size $r+1$ that can be formed from a set of size $n+r+1$ where the largest element is chosen. The LHS counts the number of subsets where the largest $n+r-j$ elements are chosen. □

9 Multinomial theorem

The terms $\binom{n!}{n_1!\ldots n_k!} = \binom{n}{n_1;\ldots;n_k}$, where $n_1 + \ldots + n_k = n$ are called the *multinomial co-efficients.* They are so called because they are the coefficients in the multinomial expansion.

Theorem 14

$$(x_1 + \ldots + x_k)^n = \sum_{n_1+n_2+\ldots+n_k=n, n_i \geq 0} \binom{n}{n_1; n_2; \ldots; n_k} x_1^{n_1} x_2^{n_2} \ldots x_r^{n_r}$$

Proof. The proof follows by induction and is left as an exercise. □

Note that there are $\binom{n+k-1}{k-1}$ terms in the expansion.

Example 7

What is the co-efficient of $x_1^2 x_3 x_4^3 x_5$ in $(x_1 + \ldots + x_5)^7$?

Solution: Directly by the multinomial theorem, we obtain that the coefficient is $\binom{7}{2;3;3;1}$.

Example 8

What is the co-efficient of $x_1^3 x_2 x_3^2$ in $(2x_1 - 3x_2 + 5x_3)^6$?

Solution: Directly by the multinomial theorem we obtain $\binom{6}{3;1;2}(2)^3(-3)(5)^2$.

10 Newton's binomial Theorem

We can extend the definition of the binomial co-efficients when the upper term is not an integer. This is defined as follows.

Definition 1 (Generalized Binomial Co-efficients)

For $\alpha \in \mathbb{R}$ and $k \in \mathbb{N}$,

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\ldots(\alpha-k+1)}{k!}$$

For example, for $\alpha = 4/3$ and $k = 3$ we have

$$\begin{aligned}\binom{4/3}{3} &= \frac{(4/3)(4/3-1)(4/3-2)}{3!} \\ &= \frac{(4/3(1/3)(-1)}{6} \\ &= \frac{-4}{54}\end{aligned}$$

and for $\alpha = -1, k = 3$ we have

$$\begin{aligned}\binom{-1}{3} &= \frac{-1(-2)(-3)}{3!} \\ &= -1\end{aligned}$$

Now we are ready to describe Newton's extension of the binomial theorem.

Theorem 15 (Newton's binomial theorem)

For $\alpha \in \mathbb{R}$, and $x, y \in \mathbb{R}$ s.t. $|x| < |y|$ we have

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

Let us see what happens for specific values of α. For $\alpha = -n$, $n \in \mathbb{N}$ and $|z| < 1 weobtain$

$$(1+z)^{-n} = \frac{1}{(1+z)^n} = \sum_{k=0}^{\infty} \binom{-n}{k} z^k \tag{1}$$

Now,

$$\begin{aligned}\binom{-n}{k} &= \frac{(-n)(-n-1)\dots(-n-k+1)}{k!} \\ &= \frac{(-1)^k n(n+1)\dots(n+k-1)}{k!} \\ &= (-1)^k \binom{n+k-1}{k}\end{aligned}$$

Thus, Eqn (1) becomes

$$(1+z)^{-n} = \frac{1}{(1+z)^n} = \sum_{k=0}^{\infty} (-1)^k \binom{n+k-1}{k} z^k$$

Let us specialize further and set $n = 1$. Then, we obtain

$$(1+z)^{-1} = \frac{1}{(1+z)} = \sum_{k=0}^{\infty} (-1)^k z^k [\because \binom{1+k-1}{k} = 1]$$

Similarly, we obtain

$$(1-z)^{-1} = \frac{1}{(1-z)} = \sum_{k=0}^{\infty} z^k \qquad [\because (-1)^k (-z)^k = z^k]$$

which is the familiar sum of the geometric series.

11 Recursion

For many counting problems it is easier to express the count as a *recurrence*, i.e., a function defined on the natural numbers whose definition involves the function for smaller values including

conditions. For example, a function of the form $f(n) = f(n-1) + 1$ is an example of a recurrence, whose values can be determined if we are given the boundary, or initial values.

We have already encountered recursive definitions, for example in the definition of well-formed formulae. Here, we see how recurrences occur naturally in several counting problems. We will first look at how to express the solution of a counting problem as a recurrence, and then develop tools to solve recurrences.

As a first example, let us consider the famous problem of the *tower of hanoi*.

Example 9

In a tower of hanoi problem we are given three spindles labeled A, B and C. There are n disks $D_1, \ldots, D_n$ on spindle A such that the radii of the disks are in increasing order from top-down, i.e., $radius(D_i) < radius(D_j)$ for $i < j$. The goal is to move all disks from spindle A to spindle C such that (i) in each move, we can move only move one disk, and (ii) at no point can a smaller disk be placed below a larger disk. The problem asks for the number of moves required to move the n disks.

Solution: The first move naturally involves moving the smallest disk D_1 to one of the spindles A or B. Now, we move the second disk D_2 to the other empty spindle. Now, we have only one available move - namely, move D_1 on top of D_2. Next we move D_3 to the empty spindle. But going on this way we will only get entangled in a web of such arguments.

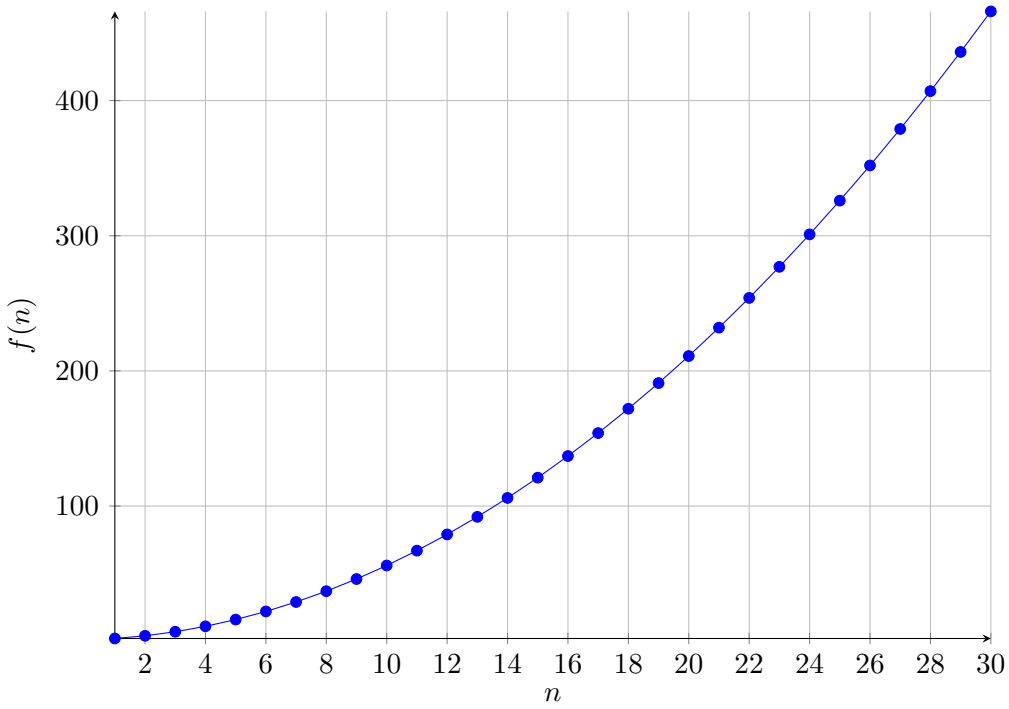
Here is a way to think about this problem *recursively*: Since D_n can't be moved before moving all of $D_1, \ldots, D_{n-1}$ and they must be placed on either spindle B or C in increasing order of radii, this is equivalent to solving the tower-of-hanoi problem with the $n-1$ disks $D_1, \ldots, D_{n-1}$. Thus, if we could move the disks $D_1, \ldots, D_{n-1}$ to spindle B then we could move D_n to spindle C in one move, and now we are again left with a tower-of-hanoi problem with $n-1$ disks, i.e., move $D_1, \ldots, D_{n-1}$ from spindle B to spindle C. Let $T(n)$ denote the number of moves required to solve a tower-of-hanoi problem with n disks. Then, we obtain the following recurrence for $T(n)$:

$$T(n) \leq 2T(n-1) + 1$$

If we are given 0 disks, then we require 0 moves, and if we have one disk, we can move this single disk from spindle A to spindle C in one move. Thus, $T(0) = 0$ is the initial condition.

Let us now attempt to solve this recurrence, by building a table and guessing the value of $T(n)$. The value $T(n)$ for small values of n are shown in Figure **??**

From the table, it is easy to check that $T(n) \leq 2^n - 1$. Of course, this doesn't constitute a proof. Typically, the best way to solve some recurrences is via a *guess-and-check* method. That is, from the few examples we see that $T(n) \leq 2^n - 1$ must be a closed form of a recurrence. We prove this by induction. For $n = 0$, $2^n - 1 = 0$. Suppose the $T(n-1) \leq 2^{n-1} - 1$, then $T(n) \leq 2T(n-1) + 1 = 2 \cdot 2^{n-1} - 1 = 2^n - 1$, and we are done.



Example 10

Now we look at an example you are already familiar with. Given a set of n lines in the plane in general position, we want to count the number of distinct regions the lines divide the plane into. The reasoning is similar to how we obtained a count via induction. But, let us obtain a recurrence for the count. Let $R(n)$ denote the number of regions into which n lines in general position partition the plane. Since the lines are in general position, no two lines are parallel and no three lines intersect at a point. Thus, if we knew $R(n-1)$, then the line ℓ_n intersects each of the $n-1$ lines and this creates an additional n regions. This gives the recurrence:

$$R(n) = R(n-1) + n$$

The initial condition is $R(0) = 1$. We could again build a table of initial values to guess the general form of the recurrence. The table is given in Figure fig:lines

In this case, it is not immediately clear what a closed form of this recurrence is. Plotting the values gives us a clue that the function is quadratic, and playing around with the constants of a quadratic, we can obtain a closed form $R(n) = n(n+1)/2 + 1$ and check it by induction.

We only show the inductive step.

$$\begin{aligned} R(n) &= R(n-1) + n \\ &= n(n-1)/2 + 1 + n \\ &= (n^2 - n + 2n)/2 + 1 \\ &= \frac{n(n+1)}{2} + 1 \end{aligned}$$

If you think the guessing is a bit magical, then here's another way to solve the recurrence - *unfolding the recurrence*.

$$\begin{aligned} R(n) &= R(n-1) + n \\ &= R(n-2) + (n-1) + n \\ &= R(n-3) + (n-2) + (n-1) + n \\ &\vdots \\ &= R(0) + 1 + 2 + \ldots + n \\ &= 1 + \frac{n(n+1)}{2} \end{aligned}$$

Example 11

Now, instead of lines in the plane suppose we have *zigs* as shown in Figure **??**. Determine $Z(n)$, the maximum number of regions that can be obtained by using n zigs in the plane. It is easy to check that $Z(1) = 2, Z(2) = 7$, and so on.

A single zig is like two lines where the three regions beyond the intersection point of the zig are merged. Therefore, we obtain only two regions instead of 4. To obtain the maximum number of regions, it is clear that we have to arrange the zigs so that the intersection points are outside the intersection with the other zigs. This gives the following recurrence relation:

$$\begin{aligned} Z(2n) &= R(2n) - 2n \\ &= \frac{2n(2n+1)}{2} + 1 - 2n \\ &= \frac{4n^2 - 2n}{2} + 1 \\ &= 2n^2 - n + 1 \end{aligned}$$

Thus, $Z(n) \approx \frac{n^2}{2}$.

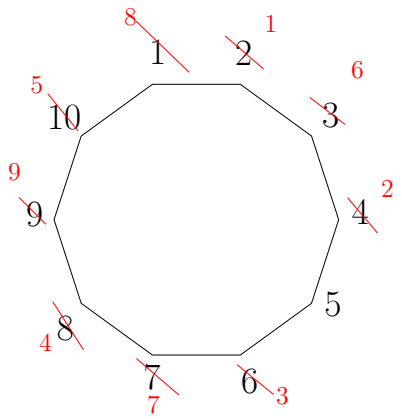


Figure 4: The figure above shows a run of the Josephus problem when $n = 10$ and every second person is killed. The number in red above the number in black shows the sequence of people killed. The last person surviving is the 5^{th}.

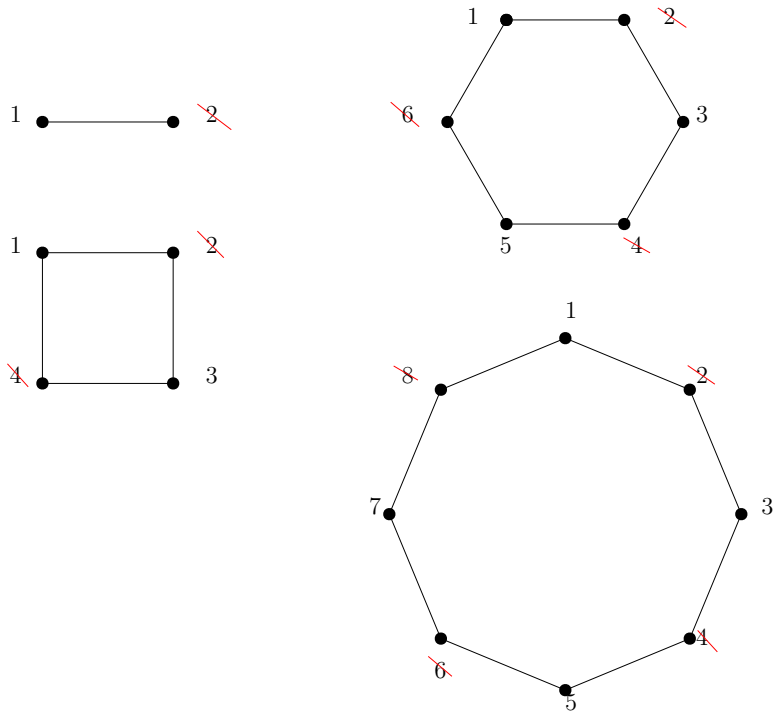


Figure 5: The figure above shows one round of the Josephus problem for some even n.

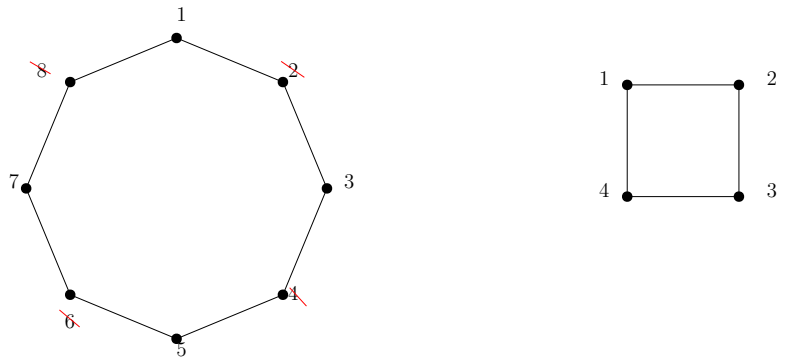


Figure 6: The figure above shows one round of the Josephus problem for $n = 6$, and the resulting smaller instance.

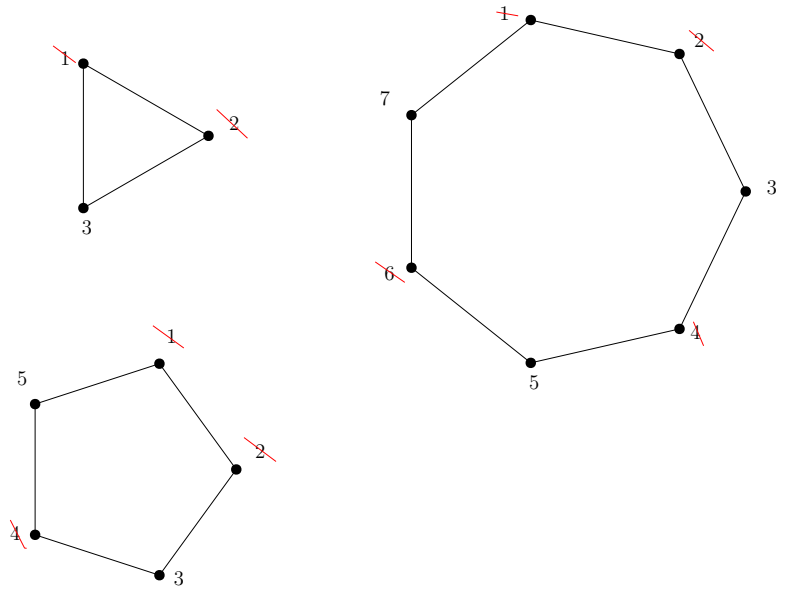


Figure 7: The figure above shows one round of the Josephus problem for some odd n.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1

Table 3: The table shows the survivor for the Josephus problem for small values of n

Example 13

We now describe the famous *Josephus problem*. A group of 41 Jewish soldiers were trapped in a cave during the Roman-Jewish wars. They preferred suicide to capture and so formed a circle and started counting out every third person until only one person was

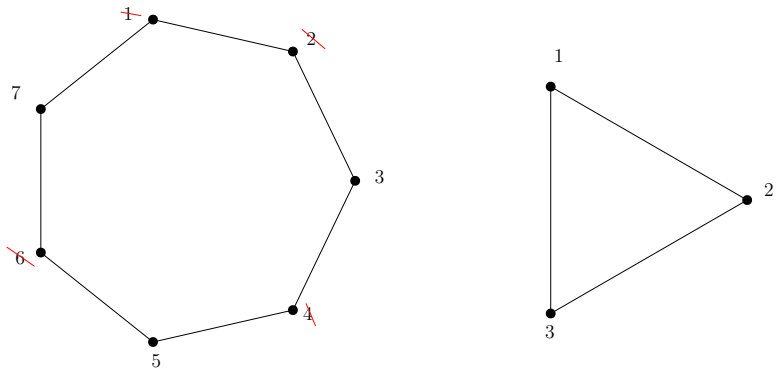


Figure 8: The figure above shows one round of the Josephus problem for $n = 7$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1

Table 4: The table shows the survivor for the Josephus problem for small values of n

left. The problem is that Josephus didn't want to die. So he had to choose a position so that he would be the last to be killed.

The general problem is this: Given n people, so that every k^{th} person is killed, determine the last surviving person. For us, we use $k = 2$.

Given n people so that every *second* person is killed, determine the position of the last surviving person. For example, if $n = 10$, Figure 4 shows the sequence of people killed in the problem and the last surviving member. Let $J(n)$ be the last survivor if there are n people and every second person is killed.

In this problem it is not immediately clear what the recurrence is. Let us analyze the problem for even numbers: $n = 2, 4, 6, 8$. Figure 5 shows the state of the Josephus problem after one round. From the figure above, we see that after one round, all players at even positions are killed. But, more importantly, at the end of this round, the gun is back to player 1, and it looks like a *smaller version* of the Josephus problem with $n = n/2$, where the i^{th} player in the smaller instance has label $2i - 1$ in the larger instance. Figure 6 shows this for $n = 8$.

Next, let us look at the same example for an odd number of players. Figure 7 shows the run of one round of the problem if the number of players is odd. In this case, the first player is killed and we obtain a *smaller instance* where a player labeled i in the smaller instance has label $2i+1$ in the larger instance. Now we are ready to write the recurrence.

$$J(n) = \begin{cases} 2J(n/2) - 1, & n \text{ is even,} \\ 2J((n-1)/2) + 1, & n \text{ is odd} \end{cases}$$

Now that we have obtained a recurrence, we can attempt to solve it. However, it is unclear yet how we can solve this recurrence. Let us compute the value $J(n)$ for small

values of n and hope that a pattern emerges. Table 3 shows the survivor for small values of n. The pattern may not be immediately clear, but the pattern should be clear from Table 4. Let $n = 2^m$. We can now guess that

$$J(2^m + \ell) = 2\ell + 1,\ m \geq 0, 0 \leq \ell < 2^m$$

We can indeed prove this bound by induction on m. If $m = 0$, then $\ell = 0$, and $J(2^0 + 0) = 2\ell + 1 = 1$ as required. For the inductive step, we break the proof into two parts depending on whether ℓ is odd or ℓ is even. If ℓ is even, then

$$\begin{aligned} J(2^m + \ell) &= 2J(2^{m-1} + \ell/2) - 1 \\ &= 2(2\ell/2 + 1) - 1 && [\because \text{ I.H}] \\ &= 2\ell + 1 \end{aligned}$$

If ℓ is even, then

$$\begin{aligned} J(2^m + \ell) &= 2J(2^{m-1} + (\ell - 1)/2) + 1 \\ &= 2\left(2(\ell - 1)/2 + 1\right) + 1 && [\because \text{ I.H}] \\ &= 2\ell + 1 \end{aligned}$$

Exercise 20

In this modification of the tower of Hanoi problem, we want to move all disks from spindle A to spindle C as before. However, we are not allowed to move any disk directly from disk A to disk C. We can only move disks to and from the middle peg B. Determine the number of moves required to move disks from spindle A to spindle C.

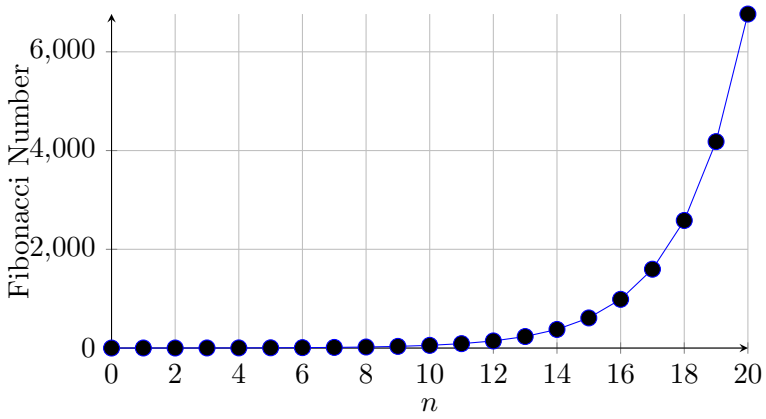
M(n) = 2M(n-1) + 2 2^(n+1) - 2.

12 Linear Homogenous Recurrences

In this section, we develop techniques to solve *linear homogenous recurrences*. A recurrence is a linear homogenous recurrence if it can be expressed as a linear function of smaller terms, but with no constant term. A classic example we start with is the Fibonacci sequence.

$$F(n) = \begin{cases} F(n-1) + f(n-2), & n \geq 2 \\ 1, & n = 1 \\ 0, & n = 0 \end{cases}$$

In order to obtain a closed form solution, we proceed follows. Let us *guess* that the solution to the recurrence is of the form $F(n) = cq^n$ for some $c, q > 0$. We can guess this by plotting the value of $F(n)$ for small values of n and see that the function grows exponentially fast as the graph



below shows.

Thus, plugging into the recurrence we obtain

Thus, canceling out the constant c and powers of q on either side, we obtain the quadratic equation.

$$q^2 - q - 1 = 0$$

whose roots are $q_1 = \frac{1+\sqrt{5}}{2}$ and $q_2 = \frac{1-\sqrt{5}}{2}$. Thus, $F(n) = cq_1^n$ and $F(n) = cq_2^n$ are both solutions to the Fibonacci recurrence. Since the fibonacci recurrence is linear and homogenous (there are no constant terms), it follows that if

$$\begin{aligned} &F(n) = c_1' q_1^n \\ &F(n) = c_2' q_2^n, \text{ then}, F(n) &= c_1 q_1^n + c_2 q_2^n \end{aligned}$$

where $c_i = c_i'/2$ for $i = 1, 2$. Since we have $F(0) = 0$ and $F(1) = 1 we have the following system of two equations in two$

$$\begin{aligned} c_1 + c_2 &= 0 \\ c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) &= 1 \end{aligned}$$

Solving this system we obtain $c_1 = 1/\sqrt{5}$ and $c_2 = -1/\sqrt{5}$. Thus,

$$F(n) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n, \; n \geq 0$$

Remarkably, although this closed-form expression involves irrationals, they magically cancel out to yield integer values for integer values n. This is the general form of the fibonacci sequence for any initial values. Thus, if we had the same recurrence with initial values

$$F(0) = a, F(1) = b$$

for some constants a, b then we obtain the system of equations

$$\begin{aligned} c_1 + c_2 &= a \\ c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) &= b \end{aligned}$$

Or in matrix form

$$\begin{bmatrix} 1 & 1 \\ \left(\frac{1+\sqrt{5}}{2}\right) & \left(\frac{1-\sqrt{5}}{2}\right) \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

Since the matrix is non-singular, we can invert it and obtain the values of c_1 and c_2 for any initial values $F(0)$ and $F(1)$.

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} \left(\frac{1-\sqrt{5}}{2}\right) & -1 \\ \left(-\frac{1+\sqrt{5}}{2}\right) & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a\left(\frac{1-\sqrt{5}}{2}\right) - b \\ -a\left(\frac{1+\sqrt{5}}{2}\right) + b \end{bmatrix}$$

For example, the initial conditions are $F(0) = 2$ and $F(1) = -1$, then we obtain

$$F(n) = \frac{\sqrt{5}-2}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{\sqrt{5}+2}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n, n \geq 0$$

Let us now look at a combinatorial problem where the Fibonacci numbers occur naturally. Given a $2 \times n$ board, determine the number of ways in which we can tile it with a 1×2 domino. Figure 9 shows a sample tiling.

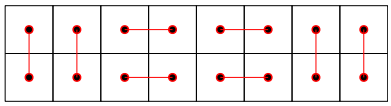


Figure 9: The figure above shows a particular tiling with a 2×1 domino. The line segment shows the orientation of the domino.

Let $H(n)$ denote the number of distinct tilings of a $2 \times n$ grid. Let us define $H(0) = 1$. As can be easily checked, $H(1) = 1, H(2) = 2$. To obtain a recurrence, we proceed as follows. There are two choices - the domino at the top-left can be placed either horizontally or vertically. If the domino covering the top-left grid cell is placed vertically, then we are left with the problem of covering a $2 \times (n-1)$ grid. If it is placed horizontally, then so must the domino covering the bottom-left grid cell. This leaves a $2 \times (n-2)$ grid. Thus, we obtain the necessary recurrence.

$$H(n) \begin{array}{ll} H(n-1) + H(n-2), & n \geq 2 \\ 1, n = 0, 1 \end{array}$$

Thus, we obtain the desired solution from the general solution to the fibonacci recurrence above.

Exercise 21

Determine the number of ways in which we can tile a $1 \times n$ grid with tiles of size 2×1 and tiles of size 1×1.

The techniques above yield a general way to solve homogenous linear recurrences. The guess is of the form q^n for some q, and we follow the recipe above to compute the roots of the *characteristic polynomial* obtained, and then use the initial conditions to determine the constants and to obtain a general solution.

13 Asymptotic notation

In this section, we take a digression to introduce asymptotic notation, and we will use it to obtain asymptotic solutions to *divide-and-conquer recurrences*. We will then use the asymptotic notation again to get a better grip on commonly occurring combinatorial functions such as the binomial coefficients.

Many times we deal with functions that are rather complicated and unwieldy to work with. Further, in many cases we are interested only in the *asymptotic behavior* of functions, i.e., the value of the function as $n \to \infty$, and in such cases, we will be interested in lower or upper-bounding the function by a simpler function as $n \to \infty$. For functions $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$, we introduce a *partial order* on functions, where $f \preceq g$ if there exists an $n_0, c > 0$ s.t. $\forall\ n \geq n_0$, $f(n) \leq cg(n)$. This inequality can be seen as a *soft inequality* between the functions f and g, i.e., it holds only for sufficiently large n. We now introduce the *big-Oh* notation that is very commonly used to compare functions.

Definition 2 (Big-Oh)

For functions $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$, $f(n) = O(g(n))$ if $\exists\ c, n_0 > 0$ s.t. $f(n) \leq cg(n)$, $\forall\ n \geq n_0$. We usually say that "g is big-Oh of f".

For example, we only require that $c > 0$. Therefore, while it is clear that for $f = n, g = 3n$, $f(n) = O(g(n))$, it is also true that $g(n) = O(f(n))$ for $c = 1/3$ and $n_0 \geq 0$. As another example, if $f(n) = 10n^2 + 5n + 3$, then it follows from the definition that $f(n) = O(n^2)$ for constants $c = 11$ and $n_0 \geq 6$. More generally, if $f(n) = \sum_{k=0}^{d} a_k n^k$, then $f(n) = O(n^d)$.

While the definition says that $f(n)$ is at most $g(n)$ for large enough values of n, it doesn't say how much larger $g(n)$ is. Thus, $n = O(n^2)$. The big-Oh notation is used to simplify functions as stated earlier. For example, if $f(n) = (10n^2 + 40n - 2)(12n^3 + n^2 + 21n + 1), then f(n) = O(n^5)$.

Lemma 1. *Let $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$. Then, $f_1(n) + f_2(n) = O(g_1(n) + g_2(n))$.*

Proof. Since $f_1(n) = O(g_1(n))$, by definition, $\exists c_1, n_1 > 0$ s.t. $f_1(n) \leq c_1 g_1(n)$, $\forall; n \geq n_1$. Similarly, $\exists c_2, n_2 > 0$ s.t. $f_2(n) \leq c_2 g_2(n)$, $\forall; n \geq n_2$. Thus, it follows that

$$\begin{aligned} f_1(n) + f_2(n) &\leq c_1 g_1(n) + c_2 g_2(n),\ \forall n_0 \geq \max\{n_1, n_2\} \\ &\leq c(g_1(n) + g_2(n)), \quad \text{for } c = \max\{c_1, c_2\} \end{aligned}$$

Hence, $f_1(n) + f_2(n) = O(g_1(n) + g_2(n))$. □

Exercise 22

The following bounds follow directly from the definition:

1. $n^\alpha = O(n^\beta)$ for $1 \leq \alpha \leq \beta$. A polynomial of larger degree is *larger than* a polynomial of smaller degree.
2. $n^c = O(\alpha^n)$ for $c > 0, \alpha \geq 1$, i.e., exponential functions grow faster than any polynomial.
3. $(\ln n)^c = O(n^\alpha)$ for $\alpha > 0$. That is a polynomial function grows faster than any poly-log (polynomial of a logarithmic) function.

Consider the following example: $f(n) = 1^3 + 2^3 + \ldots + n^3$. We obtained a closed form expression for this sum, but it turned out to be quite tedious. However, it is easier to get asymptotic estimates. First note that $f(n) = \sum_{j=1}^{n} j^3 \leq nn^3 = n^4$. Thus, $f(n) = O(n^4)$. On the other hand, we obtain the following lower bound:

$$\begin{aligned} f(n) &= 1^3 + 2^3 + \ldots + n^3 \geq (1^3 + \ldots + (\lceil n/2 \rceil)^3) + ((\lceil n/2 \rceil + 1)^3 + \ldots + n^3) \\ &\geq \left\lceil \frac{n}{2} \right\rceil 1^3 + \left\lceil \frac{n}{2} \right\rceil (\lceil n/2 \rceil)^3 \\ &\geq \frac{n}{2} + \frac{n}{2} \left(\frac{n}{2}\right)^3 \\ &\geq \left(\frac{n}{2}\right)^4 \end{aligned}$$

Thus, the upper bound is in the right ball-park.
Similar to the Big-Oh notation, we define similar asymptotic notation for lower bounds.

Definition 3 (Big-Omega)

For functions $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$, $f(n) = \Omega(g(n))$ if $\exists\ c, n_0 > 0$ s.t. $f(n) \geq cg(n)$ for all $n \geq n_0$.

We also introduce notation to say that two functions are *asymptotically the same*, i.e., they have the same rate of growth.

Definition 4 (Big-Theta)

For functions $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$, $f(n) = \Theta(g(n))$ if $\exists\ c_1, c_2, n_0 > 0$ s.t. $c_1 g(n) \leq f(n) \geq c_2 g(n)$ for all $n \geq n_0$.

We also introduce notation to say that one function grows *strictly faster* or *strictly slower* than another function. Thus,

Definition 5 (little-o)

For functions $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$, $f(n) = o(g(n))$ if $\forall\ c, \exists n_0 > 0$ s.t. $f(n) \leq cg(n)$ for all $n \geq n_0$. Note that use the universal quantifier with the constant c.

Definition 6 (little-omega)

For functions $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$, $f(n) = omega(g(n))$ if $\forall\ c, \exists n_0 > 0$ s.t. $f(n) \geq cg(n)$ for all $n \geq n_0$. Note that use the universal quantifier with the constant c.

We can also define these terms using limits, as decribed in the table below.

$f(n) = O(g(n))$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} \leq c$
$f(n) = \Omega(g(n))$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} \geq c$
$f(n) = \Theta(g(n))$	$c_1 \leq \lim_{n\to\infty} \frac{f(n)}{g(n)} \leq c_2$
$f(n) = o(g(n))$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$
$f(n) = \omega(g(n))$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty$

Exercise 23

Show that the relation $\preceq$ defined above is a transitive relation.

Exercise 26

Check if we have $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$, then $f_1(n) + f_2(n) = O(g_1(n) + g_2(n))$ and $f_1(n)f_2(n) = O(g_1(n)g_2(n))$.

Now, we give a proof of the infinitude of the primes via asymptotics.

Theorem 16

There are infinitely many primes.

Proof. Like Euclid's proof, let us suppose for the sake of contradiction that the number of primes is finite. Let $p_1, \ldots, p_k$ be the set of primes. Any number can be expressed uniquely as a product of primes. Thus, any integer $s \in \mathbb{N}$ can be expressed uniqely as

$$s = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

for some $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Hence, the function $\phi(s) = (\alpha_1, \ldots, \alpha_k)$ is a bijection.

Now, consider an integer $n \in \mathbb{N}$ large enough. It follows that for any $s \in \{1, \ldots, n\}$, and any $i \in \{1, \ldots, k\}$

$$\begin{aligned} p_i^{\alpha_i} &\leq s \qquad \leq n \\ \alpha_i &\leq \log_{p_i} s \leq \log_{p_i} n \end{aligned}$$

Where the second inequality follows by taking $\log_{p_i}$.

Since $\log_{p_i} n \leq \log_2 n$, it follows that

$$\begin{aligned} \alpha_i &\leq \log_2 n + 1 && [\because \ \alpha_i \text{ is an integer}] \\ &\leq 2 \log_2 n \end{aligned}$$

Therefore, the number of vectors $(\alpha_1, \ldots, \alpha_k)$ corresponding to the numbers $s \in \{1, \ldots, n\}$ is at most $(2 \log_2^k n)^k$, in other words it is *poly-logarithimic*. However, since the function ϕ is a bijection, we have have that the number of distinct vectors is at least n. Thus,

$$(2 \log_2 n)^k \geq n$$

But, $\lim_{n \to \infty} \frac{n}{2 \log_2^k n} = 0$, or in other words, for any $k \in \mathbb{N}$, *exists* $n_0 \in \mathbb{N}$ s.t. $(2 \log_2 n)^k < n$, a contradiction. Therefore, our assumption that the number of primes is finite must be wrong. This proves that there are infinitely many primes. □

Here is another example.

Theorem 17

$\sum_{p:prime} \frac{1}{p}$ diverges.

Proof. We prove by contradiction. Suppose the sum converges. Let

$$\sum_{p:\text{prime}} \frac{1}{p} = c$$

Then, there is some prime q s.t.

$$\sum_{p:\text{prime}, p \leq q} \frac{1}{p} > c - \frac{1}{2}$$

Therefore,

$$\sum_{p:\text{prime}, p > q} \frac{1}{p} < \frac{1}{2} \tag{2}$$

Let us call the primes smaller than q the *small primes* and the others, the *large primes*. Since any number $s \in \mathbb{N}$ has a unique representation as a product of primes, let $s \in \mathbb{N}$ be called *extraordinary* if it can be expressed as a product of only small primes. Otherwise, we call s *ordinary*. By arguments in the previous proof, corresponding to each extraordinary number, we can associate a vector $(\alpha_1, \ldots, \alpha_p)$ s.t. $s = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are the primes that are at most q.

Again, consider the set of numbers in $\{1, , n\}$. The number of factorizations extraordinary numbers in this set, by the considerations similar to the previous proof is at most $(2 \log_2 n)^k$. For a given prime p, the number of elements in $\{1, \ldots, n\}$ divisible by it is $\lfloor n/p \rfloor \leq n/p$. Thus, the total number of ordinary numbers in the set is at most $\sum n/p$, where p ranges over the large primes. By Eqn (2), this sum is at most $n/2$. Thus, of the n values, at most $n/2$ are ordinary. Hence, at least $n/2$ are extraordinary. This implies,

$$(2 \log_2 n)^k \geq \frac{n}{2}$$

which is a contradiction. Therefore, the sum diverges. □

14 Divide and Conquer recurrences

In this section, we develop techniques to deal with *divide-and-conquer* recurrences, i.e., recurrences of the form $T(n) = aT(n/b) + f(n)$. Divide and conquer recurrences show up naturally as running times of algorithms. In such cases, we are more interested in obtaining solutions as opposed to exact solutions. Throughout this section, we ignore floors and ceilings (we argue that this doesn't make a difference if we are looking for asymptotic solutions, a proof of this is tedious and is therefore not included).

Consider the following recurrence: $T(n) = 2T(n/2) + n, T(1) = 1$. A natural way to solve this recurrence is via *unrolling the recursion*. Thus,

$$\begin{aligned} T(n) &= 2T(n/2) + n \\ &= 2\left(2T(n/4) + n/2\right) + n \\ &= 4T(n/4) + n + n \\ &= 8T(n/8) + 3n \\ &\vdots \\ &= 2^k T(n/2^k) + kn \end{aligned}$$

The recursion bottoms out when $k = \log n$ at which point, we have $T(1) = 1$. Thus,

$$\begin{aligned} T(n) &= 2^{\log n} + n \log n \\ &= n + n \log n \\ &= n(\log n + 1) \end{aligned}$$

A fail-safe way to solve recurrences is the *guess-and-check* method. Let us guess a solution, and try to prove by induction that it works. Let us guess that $T(n) = cn$ for some constant $c > 0$

and try to prove the upper bound. We assume that $T(n') = cn'$ for $n' < n$. Now, we try to prove the inductive step.

$$\begin{aligned} T(n) &= 2T(n/2) + n \\ &\leq 2cn/2 + n && [\because \text{ I.H}] \\ &= n(c+1) \end{aligned}$$

But, $n(c+1) \leq cn$ is not true for any $c > 0$ and therefore, our guess is wrong. Let us therefore guess that $T(n) = cn^2$. The inductive step proceeds as follows:

$$\begin{aligned} T(n) &= 2T(n/2) + n \\ &\leq 2cn^2/4 + n \\ &= cn^2/2 + n \\ &\leq cn^2 \end{aligned}$$

where the last inequality holds for large enough n for any fixed c. Therefore, $T(n) = O(n^2)$. However, since the last inequality holds for any constant, it is possible that our guess is not tight. Let us make another guess. Let $T(n) = cn \log n$. Then, the inductive step is as follows:

$$\begin{aligned} T(n) &= 2T(n/2) + n \\ &\leq 2c\,(n/2 \log n/2) + n \\ &= c(n \log n - n) + n \\ &= cn \log n - n(c-1) \\ &\leq cn \log n \end{aligned}$$

Therefore, $T(n) \leq cn \log n$ for $c \leq 1$.

For the lower bound, again we check that $T(n) = dn \log n$ for $d \geq 0$. Then, for the inductive step

$$\begin{aligned} T(n) &= 2T(n/2) + n \\ &\geq dn \log n - n(d-1) \\ &\geq dn \log n \end{aligned}$$

for $d \geq 1$. Thus, $T(n) = n \log n$.

As another example, let us consider the recursion $T(n) = T(n/2) + n,\ T(1) = 1$. Again, by unrolling the recursion, we obtain

$$\begin{aligned} T(n) &= T(n/2) + n \\ &= T(n/4) + n/2 + n \\ &= T(n/8) + n/4 + n/2 + n \\ &\vdots \\ &= T(n/2^k) + n\,(1 + 1/2 + 1/4 + 1/8 + \ldots) \end{aligned}$$

The recursion bottoms out when $k = \log n$, and hence we obtain $T(n) = \sum_{j=0}^{\log n} n/2^j \leq 2n\left(1 - 2^{-\log n - 1}\right) \leq 2n$ Using the *guess-n-check method*, we guess that $T(n) \leq cn$ for some constant $c > 0$. The induction step becomes

$$\begin{aligned} T(n) &\leq cn/2 + n \\ &= n(1 + c/2) \\ &\leq cn \qquad\qquad [\text{ for } c \geq 2] \end{aligned}$$

Here is a more complicated divide-and-conquer recurrence: Let $T(n) = \sqrt{n}T(\sqrt{n}) + n$. Let us guess that $T(n) \leq cn \log n$, for some constant $c > 0$. Then, the inductive step becomes

$$\begin{aligned} T(n) &= \sqrt{n}T(\sqrt{n}) + n \\ &\leq \sqrt{n}\left(c\sqrt{n}\log\sqrt{n}\right) + n \\ &= c/2n \log n + n \\ &\leq cn \log n \end{aligned}$$

This implies $T(n) = O(n \log n)$ Let us try to prove a lower bound. Suppose $T(n) \geq dn \log n$ for some constant $d > 0$, then the inductive step becomes

$$T(n) \geq \frac{d}{2} n \log n + n$$

But from this it isn't true that $T(n) \geq dn \log n + n$. Therefore, our guess must be too big. Let us guess $T(n) = cn$ for some constant $c > 0$. Then,

$$\begin{aligned} T(n) &\leq \sqrt{n}\left(c\sqrt{n}\right) + n \\ &\leq (c+1)n \end{aligned}$$

But then it isn't true that $T(n) \leq cn$. Therefore, our guess must be too small. What lies between cn and $cn \log n$? Let us guess $T(n) = n \log\log n$. Then,

$$\begin{aligned} T(n) &\leq \sqrt{n}\left(c\sqrt{n}\log\log\sqrt{n}\right) + n \\ &= cn\left(\log\log\sqrt{n}\right) + n \\ &= cn \log\left(\frac{1}{2}\log n\right) + n \\ &= cn\log\log n - cn + n \\ &= cn\log\log n + n(1-c) \\ &\leq cn \log\log n, \qquad\qquad [\text{ for } c \leq 1] \end{aligned}$$

Thus, $T(n) = O(n \log\log n)$. What about the lower bound? Let us guess that $T(n) \geq d \log\log n$ for some $d > 0$. Then,

$$T(n) \geq d \log + n(1-d), \qquad [\text{ for } d \geq 1]$$

Therefore, we obtain that $T(n) = \Theta(n \log \log n)$.

14.1 Recursion Trees

The way to think about a divide-and-conquer recurrence of the form $T(n) = aT(n/b) + f(n)$ is that to compute the value of $T(n)$, we require the values of a copies of $T(n/b)$ and require $f(n)$ time to obtain these a copies. Thus, the recursion can be expressed as a *recursion tree* as shown in Figure **??**.

The root of the recursion tree is the value $f(n)$. Each node in the tree has a children, where the nodes at depth i store the value $f(n/b^i)$, and the tree has depth $\lceil \log_b n \rceil$, as at this level we have $T(1)$, which we assume is a constant (if not mentioned explicitly).

$T(n)$ is the total number of nodes in the recursion tree, which is

$$T(n) = \sum_{j=0}^{L} a^j f(n/b^j)$$

where $L = \lceil \log_b n \rceil$. Now, let us look at the bounds we obtain for the recurrences above.

$$\begin{aligned} T(n) &= 2T(n/2) + n \\ &= \sum_{j=0}^{\lceil \log_2 n \rceil} 2^j \left(\frac{n}{2^j}\right) \\ &= \sum_{j=0}^{\lceil \log_2 n \rceil} n \\ &= \Theta(n \log n) \end{aligned}$$

$$\begin{aligned} T(n) &= T(n/2) + n \\ &= \sum_{j=0}^{\lceil \log_2 n \rceil} 1^j \left(\frac{n}{2^j}\right) \\ &= \Theta(n) \end{aligned}$$

$$\begin{aligned} T(n) &= \sqrt{n}T(\sqrt{n}) + n \\ &= \sum_{j=0}^{L} \left(\sqrt{n}\right)^j \left(\frac{n}{\sqrt{n}^j}\right) \\ &= \sum_{j=0}^{L} n^{j/2} n^{1-j/2} \\ &= n \sum_{j=0}^{L} 1 \end{aligned}$$

In this case, what is L? We want $n^{1/2^L} = 1$, or $L = \log\log n$. Therefore, we obtain

$$T(n) = \sqrt{n}T(\sqrt{n}) + n = \Theta(n \log\log n).$$

Let us now look at some more examples.

$$\begin{aligned} T(n) &= T(3n/4) + n \\ &= \sum_{j=0}^{L} 1^j \left(\frac{n}{(4/3)^j}\right) \\ &= n \sum_{j=0}^{L} \left(\frac{3}{4}\right)^j \end{aligned}$$

Here, $L = \log_{4/3} n$. Thus,

$$\begin{aligned} T(n) &= n \sum_{j=0}^{\log_{4/3} n} \left(\frac{3}{4}\right)^j \\ &\leq n \sum_{j=0}^{\infty} \left(\frac{3}{4}\right)^j \\ &\leq 4n \\ &= \Theta(n) \end{aligned}$$

Here is another example.

$$\begin{aligned} T(n) &= 3T(n/2) + n \\ &= \sum_{j=0}^{L} 3^j \frac{n}{2^j} \\ &= n \sum_{j=0}^{L} \left(\frac{3}{2}\right)^j \end{aligned}$$

Here, $L = \log_2 n$. However, in the geometric sum above, the multiplier is larger than one. Thus, unlike before, we cannot upper bound the sum by the sum of the infinite series. We obtain the value of the recurrence.

$$\begin{aligned}
T(n) &= n \sum_{j=0}^{\log n} \left(\frac{3}{2}\right)^j \\
&\leq 2n \left(\left(\frac{3}{2}\right)^{\log_2 n} - 1 \right) \\
&\leq 2n \left(\frac{3}{2}\right)^{\log_2 n} \\
&\leq 2n^{\log_2 3} && [\because\ 3^{\log_2 n} = n^{\log_2 3}] = \Theta(n^{\log_2 3})
\end{aligned}$$

Now for something a little more complicated.

$$\begin{aligned}
T(n) &= 2T(n/2) + n/\log n \\
&= \sum_{j=0}^{L} 2^j \frac{n/2^j}{\log(n/2^j)} \\
&= n \sum_{j=0}^{\log_2 n} \frac{1}{\log n - j} \\
&= nH_{\log n} \\
&= \Theta(n \log\log n)
\end{aligned}$$

where $H_k = \sum_{j=1}^{k} \frac{1}{i}$ and we have seen that $H_k \leq \log n + 1$.

$$\begin{aligned}
T(n) &= 4T(n/2) + n\log n \\
&= \sum_{j=0}^{\log n} 4^j \frac{n}{2^j} \log(n/2^j) \\
&= \sum_{j=0}^{\log n} 2^j n(\log n - j) \\
&= n \sum_{j=0}^{\log n} 2^j (\log n - j) \\
&= n \sum_{j=0}^{\log n} 2^{\log n - j} j \\
&= n^2 \sum_{j=0}^{\log n} \frac{j}{2^j} \\
&= \Theta(n^2)
\end{aligned}$$

Now, let us look at a recurrence that is not quite in the divide-and-conquer form, but that we can still solve via recursion trees.

$$T(n) = T(n/4) + T(3n/4) + n$$

In this case, we obtain lower and upper bounds via the recursion tree. Each leaf of the recursion tree is at depth between $\log_4 n$ and $\log_{4/3} n$. To obtain a lower bound, we can sum up to a depth $\log_{4/3} n$ and to obtain an upper bound, we can complete the tree and sum up to the depth of a deepest leaf, i.e., $\log_4 n$. Thus, we obtain

$$\begin{aligned}
T(n) &\geq \sum_{j=0}^{\log_4 n} 4^j \frac{n}{(4)^j} \\
&= \Omega(n \log_4 n)
\end{aligned}$$

Similarly, we obtain an upper bound by extending the tree to the deepest leaf, and thus $T(n) = (n \log_{4/3} n)$, and thus

$$T(n) = \Theta(n \log n)$$

15 Estimates

In this section, we derive estimates for many basic functions we encounter in combinatorics and discrete math. We start with the harmonic functions, which we have seen already.

15.1 Harmonic function

For any integer $n \in \mathbb{N}$, the *harmonic function* H_n is defined as follows.

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

We obtain an upper bound on H_n in the following manner:

$$\begin{aligned}
H_n &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16} + \ldots \\
&= 1 + \left(\frac{1}{2} + \frac{1}{3}\right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7}\right) + \left(\frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15}\right) + \left(\frac{1}{16} + \ldots \right. \\
&\leq 1 + 2\frac{1}{2} + 4\frac{1}{4} + \ldots + 2^{\log n}\frac{1}{2^{\log n}} \\
&\leq 1 + \log_2 n
\end{aligned}$$

For the lower bound, we proceed in a similar manner.

$$\begin{aligned}
H_n &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16} + \ldots \\
H_n &= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \left(\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16}\right) + \ldots \\
&\geq 1 + \frac{1}{2} + 2\frac{1}{2^2} + 2^2\frac{1}{2^3} + \ldots + 2^j\frac{1}{2^{j+1}} + \ldots + 2^{\log n - 1}\frac{1}{2^{\log n}} \\
&= 1 + \frac{\log n}{2}
\end{aligned}$$

Thus,

$$1 + \frac{\log n}{2} \leq H_n \leq 1 + \log_2 n$$

15.2 Factorial function

We now give lower and upper bounds for the *factorial function*. For $n \in \mathbb{N}$, $n! = n(n-1)\ldots 1$. We start with a simple lower bound and then continue with a slightly more sophisticated bound by Gauss, and finally derive Sterling's approximation to the factorial function. We assume that n is even. The analysis when n is odd is similar and is left as an exercise. By replacing the fist $n/2$ terms by n, and the next $n/2$ by $n/2$, we obtain

$$\begin{aligned}
n! &= n(n-1)(n/2)(n/2-1)\ldots 1 \\
&\leq n^{n/2}\left(\frac{n}{2}\right)^{\frac{n}{2}} \\
&= \frac{n^n}{2^n}
\end{aligned}$$

A lower bound can be obtained similarly by replacing the largest $n/2$ terms by $n/2$ and the smallest $n/2$ terms by 1.

$$\begin{aligned} n! &= n(n-1)(n/2)(n/2-1)\dots 1 \\ &\geq (n/2)^{n/2}(1)^{n/2} \\ &= \frac{n^{n/2}}{2^{n/2}} \end{aligned}$$

Thus,

$$\left(\frac{n}{2}\right)^{n/2} \leq n! \leq \left(\frac{n}{2}\right)^{n}$$

Here is an application of this result - given n cards and n people, each person selects a card at random and returns it to the deck in an arbitrary positoin. What is the probability that no two people pick the same card? A little thought will tell you that this is equivalent to the following question - if we pick a random function $f : [n] \to [n]$, what is the probability that f is a permutation?

There are n^n functions from $[n] \to [n]$ and $n!$ permutations of n elements. Therefore,

$$\begin{aligned} \mathbb{P}[f \text{ is a permutation}] &\leq \frac{n!}{n^n} \\ &\leq \frac{1}{2^n} \end{aligned}$$

Thus, for reasonable values of n this is probability is quite small. Let us now try to extend this bound slightly via a technique of Gauss.

Theorem 18

$\mathrm{n}^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n$

In order to prove this bound, we require the famous $AM - GM$ inequality, i.e., the arithmetic mean-geometric mean inequality. For a set of positive numbers $a_1, \dots, a_n$, the arithmetic mean is given by $(a_1 + \dots + a_n)/n$, and the geometric mean is given by $(a_1 \dots a_n)^{1/n}$. The AM-GM inequality says that $AM \geq GM$. Thus,

$$\frac{\sum_{j=1}^{n} a_i}{n} \geq \left(a_1 \dots a_n\right)^{1/n}$$

For $n = 2$, the bound says

$$\frac{a_1 + a_2}{2} \geq \sqrt{a_1 a_2}$$

and in this case, the bound is easy to prove. Since $(\sqrt{a_1} - \sqrt{a_2})^2$ is a square, it follows that $(\sqrt{a_1} - \sqrt{a_2})^{\geq} 0$. Thus, $a_1 a_2 - 2\sqrt{a_1 a_2} \geq 0$, and thus, rearranging the terms, we obtain $(a_1 + a_2)/2 \geq (a_1 a_2)^{1/2}$. The general AM-GM inequality is left as an exercise.

Exercise 27

Prove the AM-GM inequality.

The idea of the proof is to consider the pair of numbers $i(n-i+1)$ and use the AM-GM inequality. Thus, from the AM-GM inequality, it directly follows that

$$(i(n-i+1))^{/2} \leq \frac{i+n-i+1}{2}, \text{ thus,}$$
$$(i(n-i+1))^{/2} \leq \frac{n+1}{2} \tag{3}$$

Now we are ready to prove the upper bound.

$$\begin{aligned}(n!)^2 &= (n(n-1)\dots(2)1)\,(1\cdot 2\cdot\dots(n-1)n)\\ &= (n\cdot 1)((n-1)2)((n-2)3)\dots((n-i+1)i)\dots(1\cdot n)\\ &\leq \left(\frac{n+1}{2}\right)^{2n}\end{aligned}$$

Thus,

$$n! \leq \left(\frac{n+1}{2}\right)^{n}$$

For the lower bound, we need a lower bound on $i(n-i+1)$. It is easy to check for any $2 \leq i \leq n$, $i(n-i+1) \geq n$. For $i \leq n/2$, $i(n-i+1) \geq 2(n/2+1) \geq n$, and for $i \geq n/2$, we have $i(n-i+1) \geq (n/2)2 \geq n$. Now, we are ready to prove the lower bound.

$$\begin{aligned}(n!)^2 &= (n(n-1)\dots(2)1)\,(1\cdot 2\cdot\dots(n-1)n)\\ &= (n\cdot 1)((n-1)2)((n-2)3)\dots((n-i+1)i)\dots(1\cdot n)\\ &\geq n^2\left(n^{n-2}\right)\\ &= n^n\end{aligned}$$

Thus, $n! \geq n^{n/2}$.
We now use the following bound that is well-worth remembering.

Theorem 19

$1 + x \leq e^x \; \forall x \in \mathbb{R}$

Theorem 20

$e\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n$

Proof. We prove by induction on n. For $n = 1$, it is easy to check that the inequality holds. Thus, suppose the inequality holds for values smaller than n. Then, for the induction step,

$$\begin{aligned}
n! &= n(n-1)! \\
&\leq ne(n-1)\left(\frac{n-1}{e}\right)^{n-1} && [\because \text{ I.H}] \\
&= \left(ne\left(\frac{n}{e}\right)^{n}\right)(n-1)\left(\frac{e}{n}\right)^{n}\left(\frac{n-1}{e}\right)^{n-1} \\
&= \left(ne\left(\frac{n}{e}\right)^{n}\right)e\left(1-\frac{1}{n}\right)^{n} \\
&\leq ne\left(\frac{n}{e}\right)^{n} && [\because 1+x \leq e^{x}]
\end{aligned}$$

For the lower bound, we proceed similarly.

$$\begin{aligned}
n! &= n(n-1)! \\
&\geq ne\left(\frac{n-1}{e}\right)^{n-1} && [\because \text{ I.H}] \\
&= ne\left(\frac{n}{e}\right)^{n}\left(\frac{e}{n}\right)^{n}\left(\frac{n-1}{e}\right)^{n-1} \\
&= \left(e\left(\frac{n}{e}\right)^{n}\right)e\left(\frac{n-1}{n}\right)^{n-1} \\
&= \left(e\left(\frac{n}{e}\right)^{n}\right)e\left(\frac{n-1}{1+(n-1)}\right)^{n-1} \\
&= \left(e\left(\frac{n}{e}\right)^{n}\right)e\left(\frac{1}{1+\frac{1}{(n-1)}}\right)^{n-1} && [\because 1+x \leq e^{x}] \\
&\geq \left(e\left(\frac{n}{e}\right)^{n}\right)e\left(\frac{1}{e^{1/(n-1)}}\right)^{n-1} \\
&\geq e\left(\frac{n}{e}\right)^{n}
\end{aligned}$$

□

Finally, we prove Stirling's formula.

Theorem 21 (Stirling's approximation)

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^{n}$$

Here we use $\sim$ to denote the fact that $\lim_{n\to\infty} \frac{f(n)}{n!} \to 1$, where $f(n)$ is the approximation to the factorial in Stirling's formula.

Proof. To be added... □

15.3 Binomial Coefficients

In this section, we give bounds on the Binomial coefficients $\binom{n}{k}$. Again, we start with a reasonably simple bound and then refine it.

The first bound is especially useful for small values of k.

Theorem 22

For $n, k \in \mathbb{N}$,

$$\left(\frac{n}{k}\right)^k \binom{n}{k} \leq n^k$$

Proof. For the upper bound:

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)\dots(n-k+1)}{k!} \\ &\leq \frac{n^k}{k!} \\ &\leq n^k\end{aligned}$$

For the lower bound:

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)\dots(n-k+1)}{k!} \\ &= \frac{n}{k}\frac{n-1}{k-1}\cdots\frac{n-k+1}{1} \\ &\geq \left(\frac{n}{k}\right)^k && \left[\because \frac{n-i}{k-i} \geq \frac{n}{k}\right]\end{aligned}$$

□

Now, we prove a better upper bound.

Theorem 23

For $n \leq k \in \mathbb{N}$,

$$\binom{n}{k} \leq \left(\frac{ne}{k}\right)^k$$

Proof. We prove a stronger bound, namely that

$$\sum_{j=0}^{k} \binom{n}{j} \leq \left(\frac{ne}{k}\right)^k$$

From the binomial theorem.

$$\begin{aligned}(1+x)^n &= \binom{n}{0}x^0 + \binom{n}{1}x^1 + \ldots + \binom{n}{n}x^n \\ &\geq \binom{n}{0}x^0 + \ldots + \binom{n}{k}x^k\end{aligned}$$

Hence, dividing by x^k we obtain

$$\begin{aligned}\frac{(1+x)^n}{x^k} &\geq \binom{n}{0}x^{-k} + \binom{n}{1}x^{-k+1} + \ldots + \binom{n}{k}x^0 \\ &\geq \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k} && [\because x^{-j} \geq 1, j = 0, \ldots, k]\end{aligned}$$

Since the inequality holds for any $0 < x < 1$, to get a good bound, we try to find the value of x that maximizes the LHS. We can do this by differentiating the LHS wrt x and setting it to 0. It can be checked that the value of x that maximizes the LHS is k/n. Thus,

$$\begin{aligned}\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k} &\leq \frac{(1+\frac{k}{n})^n}{\frac{k}{n}^k} \\ &\leq e^k \left(\frac{n}{k}\right)^k \\ &= \left(\frac{ne}{k}\right)^k\end{aligned}$$

□

15.4 The middle binomial coefficient

We now give bounds for the middle binomial coefficient $\binom{n}{\lfloor n/2 \rfloor}$.

Theorem 24

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$$

Proof. Consider the number

$$P = \frac{1 \cdot 3 \cdot 5 \cdot \ldots (2m-1)}{2 \cdot 4 \cdot 6 \ldots 2m}$$

Since,

$$\begin{aligned} P &= \frac{1 \cdot 3 \cdot 5 \cdot \ldots (2m-1)}{2 \cdot 4 \cdot 6 \ldots 2m} \frac{2 \cdot 4 \cdot \ldots 2m}{2 \cdot 4 \cdot \ldots 2m} \\ &= \frac{1 \cdot 2 \cdot 3 \ldots 2m}{2 \cdot 4 \cdot 6 \cdot \ldots 2m} \frac{1}{2 \cdot 4 \ldots 2m} \\ &= \frac{(2m)!}{2^{2m} m! m!} \\ &= \frac{1}{2^{2m}} \binom{2m}{m} \end{aligned}$$

Thus, we want to prove that $\frac{1}{2\sqrt{m}} \leq P \leq \frac{1}{\sqrt{2m}}$. For the upper bound, consider the product

$$\begin{aligned} &\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{4^2}\right) \ldots \left(1 - \frac{1}{(2m)^2}\right) \\ &= \left(\frac{1 \cdot 3}{2^2}\right)\left(\frac{3 \cdot 5}{4^2}\right) \cdots \left(\frac{(2m-1)(2m+1)}{(2m)^2}\right) \\ &= (2m+1)P^2 < 1 \end{aligned}$$

Hence, $P \leq 1/\sqrt{2m}$. The lower bound is similar. We consider the product

$$\begin{aligned} &\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right) \ldots \left(1 - \frac{1}{(2m-1)^2}\right) \\ &= \left(\frac{2 \cdot 4}{3^2}\right)\left(\frac{4 \cdot 6}{5^2}\right) \cdots \left(\frac{(2m-2)(2m)}{(2m-1)^2}\right) \\ &= \frac{1}{2 \cdot (2m) \cdot P^2} \end{aligned}$$

Hence, $P \geq \frac{1}{2\sqrt{m}}$. □