

MATH 239 — Combinatorics

Kevin James

Spring 2014

Contents

| | | |
|----------|--|-----------|
| 1 | Combinatorics | 2 |
| 1.1 | Course Notation | 2 |
| 1.2 | Functions | 3 |
| 2 | Combinatorial Proofs (Bijective Proofs) | 3 |
| 3 | Permutations | 3 |
| 3.1 | Formal Power Series | 6 |
| 4 | Restricted Compositions | 9 |
| 5 | Binary Strings | 11 |
| 5.1 | Recursive Decompositions | 12 |
| 5.2 | Recurrences with Repeated Roots | 12 |
| 6 | Graph Theory | 12 |
| 6.1 | Connectivity | 14 |

1 Combinatorics

Combinatorics is discrete math dealing with ‘counting questions’ and graph theory. For example:

“How many binary strings of length n are there?”: 2^n

“How many binary strings of length n are there which do not contain the (continuous) substring ‘0101’?”

“How many ways can you make change for a dollar? (in Canada!)”

“How many k -element subsets are there in an n -element set?”: n choose $k = \frac{n!}{k!(n-k)!}$

“How many ways are there to order the numbers from 1 to n with no constraints?”: $n!$

“Given 123 letters addressed to the 123 students in this class and 123 associated envelopes, how many ways are there to put one letter in each envelope such that nobody gets the right letter?”: $\approx \frac{123!}{e}$

“How many n -polynomials (tetris blocks) are there?”: $2 \rightarrow 1, 3 \rightarrow 2, 4 \rightarrow 5|7$

“How many prime numbers p are there such that $p + 2$ is also prime?”: infinite?

“How many rooted binary trees are there with n vertices?”

“Can the vertices of a graph be colored by n colors in such a way that every adjacent vertex is given a different color?”

“Can a graph be drawn such that no two edges are crossing?”

“Which graphs can be drawn in 3d-space to correspond to a fair symmetrical die?”

1.1 Course Notation

- $[n] = \{1, 2, 3, \dots, n\}$
- $\mathbb{N} = \{1, 2, 3, \dots\}$
- $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- $|A \cup B| = |A| + |B| - |A \cap B|$
- $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$
- $|A \times B| = |A||B|$
- $\mathbb{R} \times \mathbb{R}$ is the cartesian plane
- $\mathbb{Z} \times \mathbb{Z}$ is the cartesian lattice
- $(a, b) \neq (b, a)$
- $\binom{n}{k}$ is the number of k -element subsets of n .

1.2 Functions

A **function** $f : A \rightarrow B$ is a subset of $A \times B$ such that each element of A occurs as the first element of exactly one pair in the subset.

Given the set $\{(dog, 4), (duck, 2), (cat, 3), (cow, 4)\}$, the mapping from first to second values in each tuple is a function.

A **bijective** (\mapsto) function is a ‘one-to-one’ (no two elements of A map to the same element of B) and ‘onto’ (each element of B is mapped to by some element of A) function.

A function f is bijective if and only if it has an **inverse**: a function $g : B \rightarrow A$ such that $f(g(x)) = x$ and $g(f(y)) = y$. If A and B are finite and a bijection $f : A \mapsto B$ exists, then $|A| = |B|$.

2 Combinatorial Proofs (Bijective Proofs)

Lemma 2.1. *There are 2^n subsets of $[n]$.*

Proof. Let X_n be the set of all subsets of $[n]$. Let Y_n be the set of binary strings of length $[n]$. We know that $|Y_n| = 2^n$. For each set $S \in X_n$, let $f(S) = a_1, a_2, \dots, a_n$, where

$$a_i = \begin{cases} 1, & i \in S \\ 0, & \text{otherwise.} \end{cases}$$

For each string $a_1, a_2, \dots, a_n \in Y_n$, let $g(a_1, a_2, \dots, a_n) = \{i \in [n] : a_i = 1\}$. Then, g is an inverse function of f , so f is a bijective function and thus $|X_n| = |Y_n| = 2^n$ \square

Lemma 2.2. $\binom{n}{k} = \binom{n}{n-k}$ for all $0 \leq k \leq n$.

Proof. Let $x = \{k\text{-element subsets of } [n]\}$. Let $y = \{n - k\text{-element subsets of } [n]\}$. We know that $|y| = \binom{n}{n-k}$. For each set $S \in X$, let $f(S) = [n] \setminus S$ and let $g(S) = [n] \setminus S$. Then f is a bijective function and thus $|x| = |y|$ and so $\binom{n}{k} = \binom{n}{n-k}$. \square

3 Permutations

A **permutation** of a set S is $A \mapsto A$. this can be thought of as an “ordering” of the elements of A .

Theorem 3.1. *There are $n!$ permutations of an n -element set.*

For example, a permutation of $[5]$ could be $\sigma = (3, 1, 4, 2, 5)$.

Lemma 3.2. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ for $0 \leq k \leq n$

Proof. Let L be the set of all ordered k -tuples (selections) of distinct elements of $[n]$. We will compute $|L|$ in two different ways: since there are n choices for the first element, $n - 1$ for the next, et cetera, we have

$$\begin{aligned} |L| &= n(n-1) \dots (n-k+1) \\ &= \frac{n(n-1) \dots (n-k+1)(n-k) \dots 2 \times 1}{(n-k)(n-k-1) \dots 2 \times 1} \\ &= \frac{n!}{(n-k)!} \end{aligned}$$

Alternatively, we could choose an element of L by first specifying the set of elements to be selected, then choosing their order. So $L = \binom{n}{k} k!$, where $\binom{n}{k}$ is the number of ways of choosing the set of K things to be selected and $k!$ is the number of ways of putting the k elements in order.

So $\binom{n}{k} k! = |L| = \frac{n!}{(n-k)!} \implies \binom{n}{k} = \frac{n!}{k!(n-k)!}$ □

Incidentally, given this proof we can easily find $\binom{n}{k} \equiv \binom{n}{n-k}$.

Theorem 3.3 (Binomial Theorem). $(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k$

Proof. Consider $(1+y_1)(1+y_2)(1+y_3) = 1 + y_1 + y_2 + y_3 + y_1y_2 + y_1y_3 + y_2y_3 + y_1y_2y_3$. We can associate these terms with $\{\}, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}$. The statement $\binom{3}{2} = 3$ is equivalent to the fact that there exist 3 2-element subsets in this list. If we now set $y_1 = y_2 = y_3 = x$, we get $(1+x)^3 = 1 + 3x + 3x^2 + x^3$ or $\binom{3}{0} + \binom{3}{1}x + \binom{3}{2}x^2 + \binom{3}{3}x^3$. □

Lemma 3.4. $\binom{n+k}{n} = \sum_{i=0}^n \binom{n+i-1}{n-i}$

Proof. The first term is the number of n -element subsets of $[n+k]$ which must have a largest element l equal to $n \leq l \leq n+k$. Now, the right-hand side could be expanded to $\binom{n-1}{n-1} + \binom{n}{n-1} + \binom{n+1}{n-1} + \dots + \binom{n+k-1}{n-1}$ which are respectively equivalent to the number of n -element subsets of $[n+k]$ with largest element $n, n+1, n+2, \dots, n+k$. □

How many binary strings of length n are there? How many subsets of $[n]$ are there of size k ? How many permutatinos are there of a set of size n ?

We can unify these three problems (and more) by ‘abstracting out’ the idea of size or length. Let S be a set. Suppose that each $\sigma \in S$ is assigned a non-negative integer ‘weight’ $w(\sigma)$.

So if $S = \{\text{subsets of } [n]\}$ then maybe $w(\sigma) = (\text{size of } \sigma)$ for each $\sigma \in S$. Or, we could set $w(\sigma) = \text{the sum of the elements of } \sigma$. If S is the set of all binary strings, then maybe $w(\sigma) = \text{the number of 1's in } \sigma$ or, alternatively, the length of σ .

Example 3.1. Given a set S (of numbers, strings, sets, or whatever) and a weight function $w(\sigma)$ assigning a non-negative integer weight to each σ , how many elements of S have weight k ?

Proof. Given S and w , define $\Phi_S(x)$ by $\Phi_S(x) = \sum_{\sigma \in S} x^{w(\sigma)}$. This is the **generating series** for S and σ .

For example: Assume $S = \{1, 3, 5\} \times \{2, 4, 6\}$. Let $w(a, b) = a + b$ for $a, b \in S$. The $S = \{(1, 2), (1, 4), (1, 6), (3, 2), (3, 4), (3, 6), (5, 2), (5, 4), (5, 6)\}$ and the weights are $[3, 5, 7, 5, 7, 9, 7, 9, 11]$.

Then we have $\Phi_S(x) = x^3 + 2x^5 + 3x^7 + 2x^9 + x^{11} = (x^1 + x^3 + x^5)(x^2 + x^4 + x^6)$. More generally, we have $\Phi_S(x) = \sum_{k \geq 0} (\text{number of elements of } S \text{ with weight } k)x^k$. \square

Example 3.2. Let S be the set of odd numbers beginning with 1 and $w(\sigma) = \sigma, \forall \sigma \in S$.

Given

$$\begin{aligned}\Phi_S(x) &= \sum_{\sigma \in S} x^{w(\sigma)} \\ &= x^{w(1)} + x^{w(3)} + x^{w(5)} + \dots \\ &= x^1 + x^3 + x^5 + \dots \\ &= x(1 + x^2 + x^4 + \dots) \\ &= x\left(\frac{1}{1 - x^2}\right) \\ &= \frac{x}{1 - x^2}\end{aligned}$$

Theorem 3.5. For a finite S and any weight function on S , $\Phi_S(1) = |S|$.

Proof. $\Phi_S(1) = \sum_{\sigma \in S} 1^{w(\sigma)} = \sum_{\sigma \in S} 1 = |S|$. \square

Theorem 3.6. $\frac{d\Phi_S(1)}{dS} = \text{the total weight of the elements of } S$.

Theorem 3.7. $\frac{d\Phi_S(1)}{d\Phi_S(1)} = \text{the average weight of an element of } S$.

Example 3.3. Let S be the set of binary strings of a length less than or equal to n and $w(\sigma)$ be the length of σ .

$$\begin{aligned}\Phi_S(x) &= \sum_{\sigma \in S} x^{w(\sigma)} \\ &= \sigma_{k \geq 0} (\text{number of elements of } S \text{ with weight } k)x^k \\ &= \sum_{k \geq 0} (\text{number of binary strings of length } \leq n \text{ of weight } k)x^k \\ &= \sum_{k=0}^n 2^k x^k \\ &= \sum_{k=0}^n (2x)^k \\ &= 1 + 2x + (2x)^2 + \dots + (2x)^n \\ &= \frac{1 - (2x)^{n+1}}{1 - 2x}\end{aligned}$$

and thus we have $\Phi_S(1) = \frac{1 - (2x)^{n+1}}{1 - 2x} = 2^{n+1} - 1$.

And so

$$\begin{aligned}\frac{d\Phi_S(x)}{dS} &= \sum_{k=0}^n k2^k x^{k-1} \\ \frac{d\Phi_S(1)}{dS} &= \sum_{k=0}^n k2^k \\ &= (n-1)2^{n+1} + 2\end{aligned}$$

The average length is thus

$$\frac{d\Phi_S(1)}{d\Phi_S(1)} = \frac{(n-1)2^{n+1} + 2}{2^{n+1} - 1} = n - 1 + \frac{n+1}{2^{n+1} - 1} \approx n - 1$$

3.1 Formal Power Series

A **formal power series** is an expansion (i.e. generating function) of the form $\sum_{k \geq 0} a_k x^k$.

“A **generating function** is a clothesline on which we hang a sequence of coefficients for display.”
-H. Wilf

We often treat formal power series as actual power series when using them. If $A(x) = \sum_{k \geq 0} a_k x^k$, $B(x) =$

$\sum_{k \geq 0} b_k x^k$, then we define $(A + B)(x) = \sum_{k \geq 0} (a_k + b_k) x^k$. We can also multiply: with the same $A(x)$

and $B(x)$, we have $AB(x) = \sum_{k \geq 0} \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k$.

We can also perform **coefficient extraction**; $[x^k]A(x)$ is defined to be the coefficient of x^k in $A(x)$.

We can easily solve linear equations whose variables are formal power series (FPS).

Example 3.4. Find a FPS $A(x)$ such that $(1 + x + x^2 + \dots)A(x) = 1 - x$.

Let $A(x) = a_0 + a_1 x + a_2 x^2 + \dots$. We want to solve

$$\begin{aligned}(1 + x + x^2 + \dots)(a_0 + a_1 x + a_2 x^2 + \dots) &= 1 - x + (0x^2 + 0x^3 + 0x^4 + \dots) \\ a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + \dots &= 1 + (-1)x + 0x^2 + 0x^3 + \dots\end{aligned}$$

Equating coefficients gives

$$\begin{aligned}a_0 &= 1 \\ a_0 + a_1 &= -1 \\ a_0 + a_1 + a_2 &= 0 \\ a_0 + a_1 + a_2 + a_3 &= 0 \\ &\dots\end{aligned}$$

or more usefully

$$\begin{aligned}a_0 &= 1 \\a_1 &= -2 \\a_2 &= 1 \\a_3 &= 0 \\a_4 &= 0 \\&\dots\end{aligned}$$

So the solution is $A(x) = 1 - 2x + x^2$.

More simply, we have

$$\begin{aligned}\frac{1}{1-x}A(x) &= 1-x \\A(x) &= 1-2x+x^2\end{aligned}$$

Given a power series $P(x)$, if $Q(x)$ is another power series such that $PQ(x) = 1$ then $Q(x)$ is an inverse of $P(x)$. We write $Q(x) = P^{-1}(x) = \frac{1}{P(x)}$.

Lemma 3.8. $P(x) = \sum_{k \geq 0} P_k x^k$ has an inverse if and only if $p_0 \neq 0$.

We can often write formal power series more concisely in terms of their inverses. This can be useful for simplifying a series, for example:

$$\begin{aligned}(1+x+x^2+\dots)B(x) &= 1-x \\ \frac{1}{1-x}B(x) &= 1-x \\ B(x) &= (1-x)^2 \\ &= 1-2x+x^2\end{aligned}$$

A common way to compute inverses is to use the formula for the sum of a geometric series

$$\sum_{k \geq 0} x^k = \frac{1}{1-x}$$

We can ‘substitute’ any formal power series $P(x)$ in place of x in this formula if $P(x)$ has a constant term with a value of zero (e.g. has no constant terms).

Example 3.5. How many ways are there to eat n pieces of fruit if you must eat

- at most five apples
- at least three bananas
- an even number of cherries

The solution is

$$f(x) = [x^n](1+x+x^2+x^3+x^4+x^5)(x^3+x^4+x^5+\dots)(1+x^2+x^4+\dots)$$

$$\begin{aligned}
&= [x^n] \left(\frac{1-x^6}{1-x} \right) \left(\frac{x^3}{1-x} \right) \left(\frac{1}{1-x^2} \right) \\
&= [x^n] \left(\frac{x^3(1-x^6)}{(1-x)^2(1-x^2)} \right)
\end{aligned}$$

Given a set S and a weight function w assigning a non-negative integer value to each $\sigma \in S$, we defined

$$\Phi_S(x) = \sum_{\sigma \in S} x^{w(\sigma)} = \sum_{k \geq 0} \left(\begin{array}{c} \# \text{ elements in } S \\ \text{with weight } k \end{array} \right) x^k$$

Lemma 3.9 (sum lemma). *Given a set S with a weight function w , if A and B are disjoint sets such that $A \cup B = S$, then $\Phi_S(x) = \Phi_A(x) + \Phi_B(x)$.*

Lemma 3.10 (product lemma). *Let A and B be sets with weight functions α and β . If $S = A \times B$ and a weight function w on S is defined by $w(a, b) = \alpha(a) + \beta(b) \cdot \forall a, b \in S$, then*

$$\Phi_S(x) = \Phi_A(x) \Phi_B(x)$$

Theorem 3.11 (power theory). *The power theory is given by*

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

Equivalently, $[x^n](1-x)^{-k} = \binom{n+k-1}{k-1}$.

Proof. We have

$$\begin{aligned}
[x^n](1-x)^{-k} &= [x^n] \left(\frac{1}{1-x} \right)^k \\
&= [x^n] (1+x+x^2+x^3+\dots)(1+x+x^2+x^3+\dots) \dots (1+x+x^2+x^3+\dots)
\end{aligned}$$

which is equivalent to the number of solutions to $a_1 + a_2 + a_3 + \dots + a_n = n$ where $a_1, a_2, a_3, \dots, a_k \geq 0$. We need to prove this.

Claim: the number of solutions to $a_1 + a_2 + a_3 + \dots + a_n = n$ where $a_1, a_2, a_3, \dots, a_k \geq 0$ is equal to $\binom{n+k-1}{k-1}$.

Let $T = \{\text{solutions to the equation}\}$ and $S = \{\text{binary strings of length } n+k-1 \text{ having } k-1 \text{ ones}\}$. Thus $|S| = \binom{n+k-1}{k-1}$. We associate each solution $(a_1, a_2, \dots, a_n) \in T$ with the string

$$000\dots 01000\dots 1\dots 1000\dots 0 \in S$$

where each lenth of 0's is equal in leangth to a_1, a_2, \dots, a_k .

This mapping is clearlt invertible, so it is a bijection. Therefore $|S| = |T|$ as required. \square

A **composition** of an integer n into k parts is a k -tuple (a_1, a_2, \dots, a_k) such that $a_1 + a_2 + \dots + a_k = n$ and $a_1, a_2, \dots, a_k \in \mathbb{N} \geq 1$. Special case: there is a single composition of zero.

Theorem 3.12. *For $n, k \geq 1$, there are $\binom{n-1}{k-1}$ compositions of n into k parts.*

Proof. For each composition (a_1, a_2, \dots, a_k) of n , $(a_1 - 1, a_2 - 1, \dots, a_k - 1)$ is a “composition” of $n - k$, except with parts allowed to be zero. There are $\binom{(n-k)+k-1}{k-1} = \binom{n-1}{k-1}$ of these by the claim. \square

Theorem 3.13. *For $n \geq 1$, there are 2^{n-1} compositions of n .*

Proof. Summing the previous answer over all k , we get

$$\sum_{k=1}^n \binom{n-1}{k-1} = \binom{n-1}{0} + \binom{n-1}{1} + \dots + \binom{n-1}{n-1} = 2^{n-1}$$

\square

4 Restricted Compositions

Many problems ask us to count the number of compositions of n subject to restrictions on both the size and number of the parts. We can solve these ‘all’ with generating series and the sum/product lemmas.

Example 4.1. *How many compositions of n are there into 2, 3, or 4 parts, where the first part is at most 4 and the rest of the parts are odd?*

We have

$$\begin{aligned} [x^n] & \left((x^1 + x^2 + x^3 + x^4)(x^1 + x^3 + \dots) \right. \\ & + (x^1 + x^2 + x^3 + x^4)(x^1 + x^3 + \dots)(x^1 + x^3 + \dots) \\ & \left. + (x^1 + x^2 + x^3 + x^4)(x^1 + x^3 + \dots)(x^1 + x^3 + \dots)(x^1 + x^3 + \dots) \right) \end{aligned}$$

or more simply

$$[x^n] \left((x^1 + x^2 + x^3 + x^4) \left(\frac{x}{1-x} + \left(\frac{x}{1-x} \right)^2 + \left(\frac{x}{1-x} \right)^3 \right) \right)$$

Example 4.2. *How many compositions of n are there into k parts where each part is 1 or 2?*

The answer is

$$\begin{aligned} [x^n](x^1 + x^2)^k &= [x^n]x^k(1+x)^k \\ &= [x^{n-k}](1+x)^k \\ &= \binom{k}{n-k} \end{aligned}$$

Example 4.3. *How many compositions of n are there into parts of size 1 or 2?*

By the previous example, the answer is

$$\sum_{k=0}^{\infty} \binom{k}{n-k}$$

Alternatively, since the answer for k parts is $[x^n]x^k(1+x)^k$, we know that the answer for any number of parts is

$$\begin{aligned} & [x^n](1 + x(1+x) + x^2(1+x)^2 + x^3(1+x)^3 + \dots) \\ &= [x^n](1 + x(1+x) + (x(1+x))^2) \\ &= [x^n]\frac{1}{1 - x(1+x)} \\ &= [x^n]\frac{1}{1 - x - x^2} \end{aligned}$$

which is the n th Fibonacci number.

Example 4.4. How many compositions of n are there into parts of an odd size?

$$\begin{aligned} & [x^n]\left(1 + () + ()() + ()()() + \dots\right) \\ &= [x^n]\left(1 + (x^1 + x^3 + \dots) + (x^1 + x^3 + \dots)^2 + (x^1 + x^3 + \dots)^3 + \dots\right) \\ &= [x^n]\left(1 + \frac{x}{1-x^2} + \frac{x}{1-x^2}^2 + \frac{x}{1-x^2}^3 + \dots\right) \\ &= [x^n]\left(\frac{1}{1 - \frac{x}{1-x^2}}\right) \\ &= [x^n]\left(\frac{1-x^2}{1-x-x^2}\right) \end{aligned}$$

If $A(x) = \frac{1-x^2}{1-x-x^2}$, we get

$$(1 - x - x^2)A(x) = 1 - x^2$$

which we can use to find $a = (1, 1, 1, 2, 3, 5, 8, 13, 21, \dots)$.

Example 4.5. Why is the number of compositions of n parts of size 1 or 2 equal to the number of compositions of $n+1$ into parts of odd sizes? And why are both of these equal to the n th Fibonacci number?

We proved these facts algebraically; now we will do so combinatorially.

Proof. Let $S_n = \{\text{compositions of } n \text{ into parts of size 1 or 2}\}$. We will show that $|S_0| = |S_1| = 1$ and $|S_n| = |S_{n-1}| + |S_{n-2}|$ for $n \geq 2$.

The base case is obvious: there exists only one composition of one and one composition of zero by definition.

Let $S'_n = \{\text{compositions in } S_n \text{ with last part 1}\}$ and $S''_n = \{\text{compositions in } S_n \text{ with last part 2}\}$. Then we have a bijection from S_n^{prime} to S_{n-1} and from $S - n''$ to S_{n-2} by removing the last element in each composition.

For $(a_1, a_2, \dots, a_k) \in S_n$, let $f(a_1, a_2, \dots, a_k) = (a_1, a_2, \dots, a_{k-1})$. If $(a_1, \dots, a_k) \in S'_n$, then $a_k = 1$ so $f(a_1, a_2, \dots, a_k) \in S_{n-1}$. Moreover, ‘adding back’ a 1 to $f(a_1, \dots, a_k)$ gives (a_1, \dots, a_k) so $f : S'_n \rightarrow S_{n-1}$ is invertible and is thus a bijection, so $|S'_n| = |S_{n-1}|$.

Similarly, if $(a_1, \dots, a_k) \in S_n''$, then $a_k = 2$ so $f(a_1, \dots, a_k) \in S_{n-2}$. Again, $f : S_n'' \rightarrow S_{n-2}$ is invertible, so $|S_n''| = |S_{n-2}|$.

Thus $|S_n| = |S_n'| + |S_n''| = |S_{n-1}| + |S_{n-2}|$, as required. \square

Proof. Let $T_n = \{\text{compositions of } n \text{ into parts of odd sizes}\}$. Clearly $|T_1| = |T_2| = 1$; we will show that $|T_n| = |T_{n-1}| + |T_{n-2}|$ for $n \geq 3$.

Let $T_n' = \{\text{compositions in } T_n \text{ with last part } 1\}$ and $T_n'' = \{\text{compositions in } T_n \text{ with last part } > 1\}$.

The rest of this proof is the same as the above. \square

5 Binary Strings

A binary string (e.g. 011010) has length 6. We write $\ell(a)$ for the length of a binary string a . For nearly all counting problems we will do, $\ell(a)$ will be our weight function on the set of binary strings.

‘Multiplication’ of binary strings is concatenation, e.g. for $a = 101$ and $b = 0011$, $a^2b = aab = 1011010011$.

If A and B are sets of binary strings, then $AB := \{ab : a \in A, b \in B\}$. Note that we do not necessarily have $|AB| = |A||B|$, since this function is not required to produce unique outputs ab .

We write A^2 for AA , A^3 for AAA , etc, and $A^* = \{\varepsilon\} \cup A \cup A^2 \cup \dots = \bigcup_{i \geq 0} A^i$.

A **substring** of a string s is a string b such that $s = abc$ for some a and c . A **block** of s is a maximal substring of solely ones or zeros.

This decomposition of s is unambiguous—that is, every string in S can be uniquely expressed as a concatenation of ones and zeros.

This is not always the case: when we have $|AB| \neq |A| \times |B|$, some decompositions are ambiguous.

Example 5.1. Find $\Phi_S(x)$ where S is the set of binary strings without 000 as a substring.

We find the regular expression representing this set as $\{\varepsilon, 0, 00\}\{1, 10, 100\}^*$. Then we have

$$\begin{aligned} \Phi_S(x) &= \Phi_{\{\varepsilon, 0, 00\}}(x) \Phi_{\{1, 10, 100\}^*}(x) \\ &= \Phi_{\{\varepsilon, 0, 00\}}(x) \frac{1}{1 - \Phi_{\{1, 10, 100\}}(x)} \\ &= (x^0 + x^1 + x^2) \frac{1}{1 - (x^1 + x^2 + x^3)} \\ &= \frac{1 + x + x^2}{1 - x - x^2 - x^3} \end{aligned}$$

In general, $0^*(11^*00^*)^*1^*$ and $1^*(00^*11^*)^*0^*$ are unambiguous decompositions of the set of all binary strings that expose the ‘block’ structure. We can often ‘refine’ these to answer questions.

Example 5.2. Let S be the set of all binary strings where an even-sized block of zeros is never followed by an odd-sized block of ones.

We can find $S = 1 * (0(00) * 11 * \cup 00(00) * 11(11) *) * 0*$. Then we have

$$\begin{aligned}\Phi_S(x) &= \Phi_{1*}(x) \frac{1}{1 - \Phi_{\{0(00)*11*\cup 00(00)*11(11)*\}}(x)} \Phi_{0*}(x) \\ &= \frac{1}{1-x} \frac{1}{1 - (x \frac{1}{1-x^2} x \frac{1}{1-x} + x^2 \frac{1}{1-x^2} x^2 \frac{1}{1-x^2})} \frac{1}{1-x}\end{aligned}$$

5.1 Recursive Decompositions

Often, we can decompose a set of strings in terms of itself.

Example 5.3. Let S be the set of all binary strings.

Each string in S is either the empty string or a string in S followed by a zero or a one. Thus $S = \{\varepsilon\} \cup S\{0, 1\}$.

So, by our decomposition rules

$$\begin{aligned}\Phi_S(x) &= \Phi_{\{\varepsilon\}}(x) + \Phi_S(x) \Phi_{\{0,1\}}(x) \\ &= 1 + \Phi_S(x)(2x) \\ &= \frac{1}{1-2x}\end{aligned}$$

5.2 Recurrences with Repeated Roots

Theorem 5.1. If $(a_n : n \geq 0)$ is a sequence defined by a recursion with characteristic polynomial $f(x) = (x - \theta_1)^{m_1}(x - \theta_2)^{m_2} \dots (x - \theta_k)^{m_k}$, then $a_n = p_1(n)\theta_1^n + p_2(n)\theta_2^n + \dots + p_k(n)\theta_k^n$, for some polynomials $p_1(n), \dots, p_k(n)$ where each p_i has degree $< m_i$.

6 Graph Theory

A **graph** is a pair (V, E) where V is a finite set of ‘vertices’ and E is a finite set of unordered pairs of distinct elements of V (two-element subset of V) called ‘edges’.

If two vertices are connected by an edge, they are considered adjacent. Otherwise, they are non-adjacent. The edge between two vertices is incident to each of those vertices and the vertices adjacent to another vertex are its neighbours.

We say that two graphs are isomorphic (“equivalent”) if they can be drawn identically. More rigorously, we can prove that if there exists some function f such that f is a bijection between the vertices of each of two graphs and performing this bijection also causes the set of edges to become equivalent, then those graphs are isomorphic. This bijection must maintain adjacency, etc.

Foramllly, we have: G_1 and G_2 are isomorphic if there exists a bijection $\varphi : V_1 \rightarrow V_2$ such that x and y are adjacent in G_1 if and only if $\varphi(x)$ and $\varphi(y)$ are adjacent in G_2 .

Note that there is a difference between being isomorphic and being “the same graph”. If two graph drawings have the same vertex labels and edge connections, not only are they isomorphic (all graphs are isomorphic to themselves), they are also equivalent (i.e. they are the same graph).

Theorem 6.1 (The Handshake Theorem). $\sum_{v \in V} \deg(v) = 2|E|$

Corollary: every graph has an even number of vertices of odd degree.

A graph is **regular** if all vertices have the same degree. It is d -regular if every vertex has degree d . A graph whose vertex set V has a partition (A, B) such that every edge is incident with a vertex in A and a vertex in B is said to be a **bipartite** graph. (A, B) is a **bipartition** of G .

We define a **cycle** as a graph G with vertex set $\{v_1, v_2, \dots, v_n\}$ and edge set $\{v_1v_2, v_2v_3, \dots, v_nv_1\}$.

Lemma 6.2. *A cycle C is bipartite if and only if the number of vertices is even.*

Proof. If n is even, $(\{v_1, v_3, \dots, v_{n-1}\}, \{v_2, v_4, \dots, v_n\})$ is a bipartition. Thus C is bipartite.

If n is odd, we let (A, B) be a bipartition where $v_1 \in A$. Since v_2 is adjacent to v_1 , v_2 must be in B . Similarly, v_3 is in A . By an inductive argument, $v_i \in A$ if and only if i is odd. So $v_n \in A$, but since v_1 we have v_1v_n is an edge between two vertices in A . Thus, we have a contradiction and n cannot be odd. \square

A graph in which all vertices are connected to each other is a **complete** graph (also called a **clique**). A complete graph K_n has vertex set $\{v_1, v_2, \dots, v_n\}$ and edge set $\{v_iv_j : 1 \leq i < j \leq n\}$. K_n has n vertices and $\binom{n}{2}$ edges. Only K_2 is a bipartite, all other complete graphs are not.

Lemma 6.3. *Every graph on two or more vertices has two vertices of the same degree.*

A **complete bipartite** graph is a graph K_{mn} with vertex set $\{u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n\}$ and edge set $E = \{u_iv_j : 1 \leq i \leq m, 1 \leq j \leq n\}$. This graph is regular if and only if $m = n$.

An **n-cube** is a graph with a vertex set of the binary string of length n such that two vertices are adjacent if and only if they differ in exactly one position. By definition, we know that an n -cube is bipartite. Each vertex of an n -cube has degree n . By the handshake theorem $|E| = n2^{n-1}$.

The n -cube can be recursively constructed from the $(n-1)$ -cube by taking two copies and joining the pairs of corresponding vertices.

A **subgraph** of $G = (V, E)$ is a graph $G' = (V', E')$ where $V' \subseteq V$ and $E' \subseteq E$.

A **walk** in a graph is a sequence which alternates between vertices and edges in such a way that each edge is incident to the vertices preceding and following it. A walk must begin and end with vertices and is defined to have a length equal to the number of edges. If the first and last vertex in the walk are the same, the walk is considered **closed**. Note that a walk can pass through a vertex any number of times, whether or not it is closed.

A **path** is a walk with no repeated vertices. A closed walk with no repeated vertices (except the first and last) is a **cycle**.

Lemma 6.4. *If there is a walk between two vertices u and v in a graph G , then there is a path between u and v in G .*

Proof. Let $u = v_0, v_1, v_2, \dots, v_k = v$ be a **shortest** walk between u and v (use as few edges as possible). If this walk is not a path, then $v_i = v_j$ for some $0 \leq i < j \leq k$. But then $v_0, v_1, \dots, v_i, v_{j+1}, \dots, v_k$ is a shorter walk—which is a contradiction. \square

Lemma 6.5. *If u, v, w are vertices of G and there is a path from u to v and a path from v to w , then there is a path from u to w .*

Proof. Putting the two paths together, we get a walk (not necessarily a path) from u to w . By lemma 6.4, there is a path from u to w . \square

Lemma 6.6. *If every vertex in G has degree $d \geq 2$, then G has a cycle.*

Proof. Let $v_0, v_1, v_2, \dots, v_k$ be a longest path in G . Since the path is longest, each number of v_k is in the path and since $\deg(v_k) \geq 2$, v_k has a neighbour $v_i \neq v_{k-1}$. Now $v_i, v_{i+1}, \dots, v_k, v_i$ is a cycle. \square

Theorem 6.7 (Dirac). *If G is a graph with $n \geq 3$ vertices where every vertex has degree $d \geq \frac{n}{2}$, then G has a cycle containing every vertex (a **Hamiltonian Cycle**).*

Proof. Let $P = (v_0, v_1, \dots, v_k)$ be a longest path of G . We claim that there is a cycle C with vertex set $\{v_0, v_1, \dots, v_k\}$ and that every vertex is in C . We know that each of v_0, v_k has $\geq \frac{n}{2}$ neighbours; by maximality of P , each such neighbour is in P .

Now let I be the set of vertices in P adjacent to v_0 and J be the vertices in P that are one to the right of a neighbour of v_k . \square

6.1 Connectivity

A graph G is **connected** if, for every pair of vertices u, v in G , there is a path (or walk) from u to v . Complete graphs, complete bipartite graphs with non-empty sides, graphs with a hamiltonian cycle, and n -cube graphs are all connected.

Lemma 6.8. *If G is a graph and x is a vertex in G such that, for every vertex y in G , there is a path from x to y , then G is connected.*

Proof. Suppose such a vertex x exists. Let u and v be vertices of G . By hypothesis there is a path from u to x and a path from x to v , so there is a path from u to v by lemma 6.5. \square

A **component** of a graph G is a maximal connected subgraph of G . That is, a connected subgraph of G that is not contained as a subgraph in any larger connected subgraph of G .

Often, to understand a graph in some way it will suffice to understand the graph's components. For example: G is bipartite if and only if each of its components are bipartite.

If (A, B) is a partition of the vertex set of a graph G , then the **cut** of G induced by (A, B) is the set of edges of G with one end in A and one end in B .

Lemma 6.9. *A graph G is disconnected if and only if there exists a partition (A, B) of its vertex set such that $A, B \neq \emptyset$ and (A, B) induces an empty cut.*

Theorem 6.10 (Chuatal '72). *If G is a graph on n vertices with degrees $d_1 \leq d_2 \leq \dots \leq d_n$, then if $(d_i > i \text{ or } d_{n-1} \geq n - i)$ for all $i < \frac{1}{2}n$, then G is Hamiltonian.*

A graph is **k-connected** if there are k ‘internally disjoint’ paths between any pair of its vertices. Equivalently, for any $k - 1$ vertices, removing them leaves a connected graph.

It was postulated that “If G is a 3-connected graph that can be drawn in the plane without edges crossing, then G is Hamiltonian.” This, though, we proven wrong by the Tutte Graph; instead, we postulate that every 4-connected graph that can be drawn in the plane without crossings is Hamiltonian.

Theorem 6.11. *Every connected graph in which every vertex has even degree is Eulerian.*

Proof. If the edge set is empty, the theorem is obviously true. Suppose the theorem holds for all graphs on $< m$ edges. Let G be a connected graph with m edges and all even degrees. By the propositions, G contains a cycle. Let F be the edge set of a largest-possible closed walk of G that doesn’t repeat edges. If $F = E$, we’re done. Otherwise, $(V, E - F)$ is a graph with even degrees and fewer edges than G , so by the IH each of its components has a Euler tour. Combining such a Euler tour with F gives a longer closed walk with no repeated edges, a contradiction. \square

An edge e of a graph G is a **bridge** of G if $G - e$ has more components than G .

Lemma 6.12. *If $E = xy$ is a bridge of G , then x and y are in different components of $G - e$.*

Lemma 6.13. *If e is a bridge of G , then $G - e$ has exactly one more component than G .*

Proof. In the case where G is connected: $G - e$ has ≥ 2 components. Suppose for a contradiction that $G - e$ has ≥ 3 components; let C_0, C_1, C_2 be distinct components of $G - e$. At least one of these components contains neither end of e , and is therefore a component of G . Since it does not contain e , it is not all of G ; thus G is disconnected. \square

A graph is **k-edge-connected** if deleting any $k - 1$ edges leaves a connected graph.

Theorem 6.14 (Menger’s Theorem (Edge version)). *If G is a k -edge-connected graph, then there are k edge-disjoint paths between every pair of vertices in G .*

Theorem 6.15. *Let G be a connected graph with no bridge. For any pair of vertices x, y in G , there are two edge-disjoint paths of G between x and y .*