MATH 239: Introduction to Combinatorics

Chris Thomson

Winter 2013, University of Waterloo

Notes written from Bertrand Guenin's lectures.

Contents

1 Introduction, Permutations, and Combinations

1.1 Course Structure

The grading scheme is ~~50%~~ 55% final, 30% midterm, ~~10% quizzes~~ 5% participation marks (clicker questions), and 10% assignments. There are ~~ten quizzes and~~ ten assignments. ~~The quizzes will not be announced in advance, and each quiz consists of a single clicker question.~~ Assignments are typically due on Friday mornings at 10 am. in the dropboxes outside of MC 4066. The midterm exam is scheduled for March 7, 2013, from 4:30 pm - 6:20 pm. There is no textbook for the course, but there are course notes available at Media.doc in MC, and they're *highly* recommended.

MATH 239 is split into two parts: counting (weeks 1-5) and graph theory (weeks 6-12).

See the course syllabus for more information – it's available on Waterloo LEARN.

1.2 Sample Counting Problems

Problem 1.1. How many ways are there to cut a string of length 5 into parts of sizes 1 and 2?

Here are a few example cuts:

1	2	3	4	5	5 cuts: size 1, size 1, size 1, size 1, size 1.
1	1	2	2	3	3 cuts: size 2, size 2, size 1.
1	2	2	3	3	3 cuts: size 1, size 2, size 2.

This is a finite problem. You could count all of the possibilities manually in this case. However, this problem could be made more complicated to a point where manually counting all possibilities would become quite cumbersome, as is the case in the next problem.

Problem 1.2 (Cuts)**.** How many ways are there to cut a string of size 372,694 into parts of sizes 3, 17, 24, and 96?

Definition. A positive integer n has a **composition** $(m_1, m_2, \ldots, m_k)$, where $m_1, \ldots, m_k$ are positive integers and where $n = m_1 + m_2 + \ldots + m_k$. $m_1, \ldots, m_k$ are the **parts** of the composition.

Problem 1 could be rephrased as looking for the number of compositions of 5 where all parts are 1 or 2.

Problem 1.3. How many compositions of n exist such that all parts are odd?

Problem 1.4 (Binary Strings)**.** Let $S = a_1, a_2, \ldots, a_n$ where $a_i \in \{0, 1\}$. How many strings S exist?

For each a_i, there is the choice between 0 or 1, and that choice is independent for each character of the string (for each a_i). So, there are 2^n binary strings of length n.

Problem 1.5. How many binary strings of size n exist that do not include the substring 1100?

3

For example: 10101<u>1100</u>101 $\notin S$.

Problem 1.6. How many binary strings of size n exist such that there is no odd-length sequences of zeroes?

For example: 100100<u>100</u>011 $\notin S$.

Problem 1.7 (Recurrences)**.** How many times does a recursive function get called for a particular input n?

1.3   Sample Graph Theory Problems

Problem 1.8. For any arbitrary map of regions, color the regions such that no two touching boundaries do not have the same color, with the least number of colors possible.

The **four-color theorem** (proven later in the course) states that you can always do this with four colors. It's also always possible to color these regions with five colors. It's *sometimes* possible to color the regions with three or fewer colors, depending on the layout of the regions and their boundaries.

1.4   Permutations and Combinations

1.4.1   Set Notation

The usual set and sequence notation is used in this course. $(1, 2, 3)$ is a sequence (where order matters), and $\{1, 2, 3\}$ is a set (where order does not matter).

We will also be using one piece of notation you may not be familiar with: $[n] := \{1, 2, \ldots, n\}$.

1.4.2   Permutations

Definition. A **permutation** of $[n]$ is a rearrangement of the elements of $[n]$. The number of permutations of a set of n objects is $n \times (n-1) \times \ldots \times 1 = n!$.

For example: the number of permutations of 6 objects is $6 \times 5 \times 4 \times 3 \times 2 \times 1 = 6!$ permutations.

Why is this the case? Simple: there are n choices for the first position, $(n-1)$ choices for the second position, $(n-2)$ choices for the third position, and so on, until there's 1 choice for the nth position.

Definition. A k**-subset** is a subset of size k.

Problem 1.9. How many k-subsets of $[n]$ exist?

Let's consider a more specific case: how many 4-subsets of 6 are there? $\frac{6 \times 5 \times 4 \times 3}{4!}$.

For simplicity's sake, we will introduce notation for this, which we will refer to as a **combination**, denoted as $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ where $n, k \in \mathbb{Z} \geq 0$.

Proposition. *There are $\binom{n}{k}$ k-subsets of $[n]$.*

1.4.3 Application: Binomial Theorem

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

Why is this true?

$$(1+x)^3 = \overbrace{(1+x)}^{1}\overbrace{(1+x)}^{2}\overbrace{(1+x)}^{3} = 1 + 3x + 3x^2 + x^3 = \binom{3}{0} + \binom{3}{1}x + \binom{3}{2}x^2 + \binom{3}{3}x^3$$

Proof.

$$(1+x)^n = \overbrace{(1+x)}^{1}\overbrace{(1+x)}^{2}\cdots\overbrace{(1+x)}^{n}$$

In order to get x^k, we need to choose x in k of $\{1, \ldots, n\}$. There are $\binom{n}{k}$ ways of doing this. □

2 Simple Tools for Counting

2.1 Partitioning

Sets S_1, S_2 partition the set S if $S = S_1 \cup S_2$ and $S_1 \cap S_2 = \emptyset$.

Example 2.1.

$$S = [5] = \begin{cases} S_1 = \{1, 2\} \\ S_2 = \{3, 4, 5\} \end{cases}$$
$$|S| = |S_1| + |S_2|$$

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

Proof. We will discuss two proof methods.

1. **Algebraic proof**. Set $x = 1$ in the Binomial Theorem.

2. **Combinatorial proof**. We will count the left-hand side and the right-hand side in different ways to reach the same result.

   Let S be the set of subsets of $[n]$. $|S| = 2^n$, since for every element of $[n]$ we have two possibilities: include or don't include the element in S.

   Aside: suppose $n = 2$. Then $S = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

   Partition S into $S_0, S_1, \ldots, S_n$, where S_k is the set of k-subsets of $[n]$.

$$\underbrace{|S|}_{2^n} = \underbrace{|S_0|}_{\binom{n}{0}} + \underbrace{|S_1|}_{\binom{n}{1}} + \cdots + \underbrace{|S_n|}_{\binom{n}{n}}$$

5

$\square$

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

Proof. Let S be the set of k-subsets of $[n]$. Then $|S| = \binom{n}{k}$. Partitioning S, let S_1 be the subsets of S containing n, and let S_2 be the subsets of S not containing n.

It's easy to see that $|S_1| = \binom{n-1}{k-1}$ (n is already included in our choices) and $|S_2| = \binom{n-1}{k}$. We now have $|S| = |S_1| + |S_2| = \binom{n-1}{k-1} + \binom{n-1}{k}$. $\square$

2.2 Pascal's Triangle

Pascal's Triangle is a triangle where each value is determined by the sum of its two direct parents. The uppermost value is 1.

$$
\begin{array}{c}
n = 0: \qquad\qquad\qquad 1 \\
n = 1: \qquad\qquad\quad 1 \qquad 1 \\
n = 2: \qquad\quad 1 \qquad 2 \qquad 1 \\
n = 3: \quad 1 \qquad 3 \qquad 3 \qquad 1 \\
n = 4: \quad 1 \qquad 4 \qquad 6 \qquad 4 \qquad 1
\end{array}
$$

Proposition. $\dbinom{q+r}{q} = \sum_{i=0}^{r} \dbinom{q+i-1}{q-1}$

For example: let $q = 3, r = 2$. Then we have: $\dbinom{5}{3} = \dbinom{2}{2} + \dbinom{3}{2} + \dbinom{4}{2}$.

Proof. Let S be the set of q-subsets of $[q+r]$, so $|S| = \binom{q+r}{q}$. Partition S such that S_i is the set of q-subsets where the largest element is $q + i$ (where $i = 0, \ldots, r$).

We have: $|S| = |S_0| + |S_1| + \cdots + |S_r|$. Note that $|S_i| = \binom{q+i-1}{q-1}$. That gives us:

$$
\underbrace{|S|}_{\binom{q+r}{q}} = \sum_{i=0}^{r} \underbrace{|S_i|}_{\binom{q+i-1}{q-1}}
$$

$\square$

2.3 Injections, Bijections, and Onto

Let's consider a function $f : S \to T$.

Definition. The function f is an **injection** if for all $x_1, x_2 \in S, x_1 \neq x_2$ such that $f(x_1) \neq f(x_2)$. That is, no element in the codomain T is the image of more than one element in S.

Definition. The function f is **onto** (or a **surjection**) if for all $y \in T$, there exists $x \in S$ such that $f(x) = y$. That is, all elements in the codomain T are the image of an element in S. Multiple elements in S can map to the same element in T.

Definition. The function f is a **bijection** if it is both injective and onto. That is, there is a one-to-one mapping between elements in S and T, and vice versa.

Proposition. *If S and T are finite, $|S| = |T|$ if f is bijective.*

Definition. g is the inverse of f if:

1. For all $x \in S, g(f(x)) = x$.

2. For all $y \in T, f(g(y)) = y$.

In order to show that a function has a bijection, find the inverse function.

2.4 Application: Binomial Coefficients

Proposition. $\dbinom{n}{k} = \dbinom{n}{n-k}$

Proof. I will prove this proposition in a combinatorial proof using the bijection technique. We want to show that the cardinalities are the same.

Let S_1 be the set of k-subsets of $[n]$, so $|S_1| = \binom{n}{k}$, as shown earlier. Let S_2 be the set of $(n-k)$-subsets of $[n]$, so $|S_2| = \binom{n}{n-k}$. We need to show that $|S_1| = |S_2|$, so we need to show that there is a bijection between S_1 and S_2, $f : S_1 \to S_2$.

<u>Aside</u>: suppose $n = 5$ and $k = 2$. Then, the bijection could be $\{1,3\} \to \{2,4,5\}$ (the complement function).

The bijective function is $f(A) = [n] \backslash A$ (the complement function). Check: f is its own inverse (let $g = f$). $\qquad \square$

3 Power Series and Generating Functions

3.1 Power Series

Definition. Let $(a_0, a_1, \ldots)$ be a sequence of rational numbers. Then:

$$A(x) = \sum_{i \geq 0} a_i x^i$$

This is called a **power series**.

Example 3.1. $a_i = 2^i \implies A(x) = 1 + 2x + 4x^2 + 8x^3 + \cdots$

If the sequence is finite, it is just a polynomial.

3.1.1 A General Counting Problem

Let S be the set of objects σ. Each object σ has a weight $w(\sigma)$. We want to know how many objects of S have some weight k.

Example 3.2. Let $\sigma \subseteq [n], w(\sigma) = |\sigma|$. The question becomes: how many k-subsets of $[n]$?

Example 3.3. Let σ be the set of coins (1¢, 5¢, 10¢, 25¢, \$1, \$2), and let $w(\sigma)$ be the total value of the coins in σ.

The question becomes: how many sets of coins have total value k? In other words, how many ways are there to give change on k amount?

3.2 Generating Functions

Definition. Given S as the set of objects σ and a weight function $w(\sigma)$:

$$\phi_S(x) = \sum_{\sigma \in S} x^{w(\sigma)}$$

This is called the **generating function for S, w**.

Example 3.4. Let $S = \{\sigma | \sigma \subseteq \{1, 2, 3\}\}, w(\sigma) = |\sigma|$.

σ	$w(\sigma)$	$x^{w(\sigma)}$
$\emptyset$	0	1
$\{1\}$	1	x
$\{2\}$	1	x
$\{3\}$	1	x
$\{1, 2\}$	2	x^2
$\{1, 3\}$	2	x^2
$\{2, 3\}$	2	x^2
$\{1, 2, 3\}$	3	x^3

$\phi_S(x) = 1 + 3x + 3x^2 + x^3 = (1 + x)^3$ is the generating function. Notice the coefficients are the number of objects whose weight is equal to the exponent.

Remember: the generating function for S with weights w is $\phi_S(x) = \sum_{k \geq 0} a_k x^k$, where a_k is the number of objects of size k in S.

Example 3.5. Let S be the set of subsets of [n], and $w(\sigma) = |\sigma|$.

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

Note that $\binom{n}{k}$ is included because that's the number of k-subsets of $[n]$. $\phi_S(x) = (1 + x)^n$ by the binomial theorem.

Proposition. *Let $\phi_S(x)$ be the generating function for finite-size S with weight w. Then:*

1. $\phi_S(1) = |S|$

2. $\phi'_S(1) =$ *sum of the weight of all the objects in S.*

8

Together, we get:

$$\frac{\phi'_S(1)}{\phi_S(1)} = \textit{average weight of objects in } S$$

Considering the previous example again, we know that $|S| = 2^n$ and the average weight is clearly $\frac{n}{2}$. We can verify that with this proposition.

$$\phi_S(x) = (1+x)^n \implies \phi_S(1) = (1+1)^n = 2^n$$
$$\phi'_S(x) = n(1+x)^{n-1} \implies \phi'_S(1) = n2^{n-1}$$
$$\text{average weight } = \frac{\phi'_S(1)}{\phi_S(1)} = \frac{n2^{n-1}}{2^n} = \frac{n}{2}$$

We'll now prove the proposition more generally.

Proof. We will prove the two parts of the proposition separately. The average weight clearly follows from those two results.

1.

$$\phi_S(x) = \sum_{\sigma \in S} x^{w(\sigma)}$$

Choose $x = 1$. Then $\phi_S(1) = \sum_{\sigma \in S} 1 = |S|$.

2.

$$\phi'_S(x) = \sum_{\sigma \in S} w(\sigma)x^{w(\sigma)-1}$$

Choose $x = 1$. Then $\phi'_S(1) = \sum_{\sigma \in S} w(\sigma) \cdot 1 = \text{total weight of all objects in } S$.

$\square$

In order to work further with generating functions, we'll first need to learn how to manipulate power series generally.

3.3   Working With (Formal) Power Series

For the following definitions, we will assume the following power series are defined:

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$
$$B(x) = b_0 + b_1 x + b_2 x^2 + \cdots$$

Definition. We define **addition of power series** as follows.

$$A(x) + B(x) := \sum_{n \geq 0} (a_n + b_n)x^n$$

Note that this definition is consistent with the definition of addition for polynomials.

Definition. We define **multiplication of power series** as follows.

$$A(x)B(x) := \sum_{n \geq 0} \sum_{k=0}^{n} a_k b_{n-k} x^n$$

Example 3.6.

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

Definition. $B(x)$ is the **inverse** of $A(x)$ if $A(x)B(x) = 1$ (alternatively, $B(x)A(x) = 1$).

We will use the notation $B(x) = \frac{1}{A(x)}$ to indicate that $B(x)$ is the inverse of $A(x)$, and vice versa.

Example 3.7. The inverse of $(1 + x + x^2 + \cdots)$ is $(1 - x)$, as shown in the previous example.

Question: does every power series have an inverse? No. For example, $(x + x^2)$ does not have an inverse. But suppose for a moment that it does.

Proof. If $(x + x^2)$ has an inverse, there would exist constants b_i such that

$$(x + x^2)(b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots) = 1$$

Clearly, this is impossible. In order to equal 1, b_0 must multiply by some constant term, however there is no other constant term. Therefore, our assumption was incorrect, meaning $(x + x^2)$ does not have an inverse. $\square$

Remark: if a power series does not have a constant term then it has no inverse, and vice versa.

Theorem. *If the constant term of $A(x)$ is non-zero, then $A(x)$ has an inverse, and we can find it.*

Notation: given a power series $A(x)$, we say $[x^k]A(x)$ represents the coefficient of x^k.

Example 3.8. Find the inverse of $1 - x + x^2 - x^3 + x^4 - \cdots$.

$$\underbrace{(1 - x + x^2 - x^3 + x^4 - \cdots)(b_0 + b_1 x + b_2 x^2 + \cdots)}_{(\star)} = 1$$

$$[x^0](\star) = 1 \implies 1 \cdot b_0 = 1 \implies b_0 = 1$$
$$[x^1](\star) = 0 \implies 1 \cdot b_1 - 1 \cdot b_0 = 0 \implies b_1 = b_0 = 1$$
$$[x^2](\star) = 0 \implies 1 \cdot b_2 - 1 \cdot b_1 + 1 \cdot b_0 = 0 \implies b_2 = b_1 - b_0 = 0$$

Similarly, $b_3 = b_4 = \cdots = 0$. Thus, the inverse is $(1 + x)$.

It's clear that the inverse for a power series is **unique**. We made no choices when determining the inverse, therefore it must be unique.

3.3.1 Finding Inverses

Given:

$$A(x) = \sum_{n \geq 0} a_n x^n \text{ where } (a_0 \neq 0)$$

We want to find:

$$B(x) = \sum_{n \geq 0} b_n x^n$$

We'll start by finding b_0:

$$[x^0]A(x)B(x) = a_0 b_0 = 1 \implies b_0 = \frac{1}{a_0}$$

Notice that if we didn't have the restriction on a_0, we would've run into trouble here. Now, suppose you found $b_0, b_1, \ldots, b_{n-1}$ for $n \geq 1$. Find b_n.

$$b_n = \frac{1}{a_0} \cdot (-a_1 b_{n-1} - a_2 b_{n-2} - \ldots - a_n b_0)$$

Proposition. *Let $A(x)$ and $P(x)$ be formal power series. Suppose the constant for $A(x)$ is not 0. Then there exists a unique $B(x)$ such that $A(x)B(x) = P(x)$.*

Some useful formulæ:

$$\frac{1}{1-x} = 1 + x + x^2 + x_3 + \cdots \text{ since } 1 = (1 + x + x^2 + \cdots)(1-x)$$

$$\frac{1 - x^{k+1}}{1 - x} = 1 + x + x^2 + \cdots + x^k \text{ since } 1 - x^{k+1} = (1 + x + x^2 + \cdots + x^k)(1-x)$$

3.3.2 Compositions

Definition. Let $A(x)$ and $B(x)$ be formal power series defined by:

$$A(x) = \sum_{n \geq 0} a_n x^n \qquad B(x) = \sum_{n \geq 0} b_n x^n$$

We define the **composition** as:

$$A(B(x)) := \sum_{n \geq 0} a_n [B(x)]^n$$

Example 3.9. Let $A(x) = 1 + x + x^2 + x^3 + \cdots$ and $B(x) = 2x$. Then the composition is $A(B(x)) = 1 + 2x + 4x^2 + 8x^3 + \cdots$.

Question: is the composition of two formal power series a formal power series itself? No.

Example 3.10. Suppose we pick $A(x) = 1 + x + x^2 + x^3 + \cdots$ and $B(x) = 1 + x$.

We have $A(B(x)) = 1 + (1 + x) + (1 + x)^2 + (1 + x)^3 + \cdots$. This cannot be a formal power series because a formal power series requires that all coefficients (a_k) need to be rational numbers, and in this case a_0 is infinite.

11

Example 3.11. Suppose we pick $A(x) = 1 + x + x^2 + x^3 + \cdots$ and $B(x) = x + x^2$.

We have $A(B(x)) = 1 + (x + x^2)^1 + (x + x^2)^2 + \cdots$. In order to show that this is a formal power series, we need to show that the coefficient of x^k (which is a_k) is finite for all k.

Theorem. *Let $A(x)$ and $B(x)$ be formal power series, and $[x^0]B(x) = 0$ ($B(x)$'s constant is zero). Then $A(B(x))$ is a formal power series.*

Aside:

$$a(b(x)) = 1 + \underbrace{(x + x^2)^1}_{x(1+x)} + \underbrace{(x + x^2)^2}_{x(1+x)} + \underbrace{(x + x^2)^3}_{x(1+x)} + \cdots$$

Proof. We need to show that for any fixed k, $[x^k]A(B(x))$ is finite.

Let $R(x)$ be such that $B(x) = xR(x)$. Then we have:

$$[x^k]A(B(x)) = [x^k] \sum_{n \geq 0} a_n [B(x)]^n$$

$$= [x^k] \sum_{n \geq 0} a_n x^n R(x)$$

$$= [x^k] \sum_{n \geq 0}^{k} a_n x^n (R(x))^n$$

We made the last sum finite because we're interested in the coefficient of x^k only. Note that this last line shows we can determine the coefficient in a finite number of steps, since k is finite. $\qquad\square$

Example 3.12. Let $y \mapsto x^2$ (I will call x^2, y).

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

$$= 1 + x^2 + x^4 + x^6 + \cdots$$

We used composition with $A(x) = 1 + y + y^2 + \cdots$ and $B(x) = x^2$ (constant is zero). We were only allowed to do this because $[x^0]B(x) = 0$.

3.3.3   Cartesian Product

Definition. Let A and B be sets. The **cartesian product** is defined as:

$$A \times B := \{(a, b) \,|\, a \in A, b \in B\}$$

Note that (a, b) is an ordered pair.

Example 3.13. Let $A = \{1, 2, 3\}$ and $B = \{x, y\}$. Then $A \times B = \{(1, x), (2, x), (3, x), (1, y), (2, y), (3, y)\}$.

The cardinality of $A \times B$ is the product of the cardinalities of A and B: $|A \times B| = |A||B|$.

3.4 The Sum and Product Lemmas

Let's consider a bin of two red marbles – one large marble (denoted R), and one small marble (denoted r). We define A to be the set of all selections of ≥ 1 marbles. We know:

$$A = \{\{r\}, \{R\}, \{r, R\}\}$$
$$w(\sigma) = |\sigma|$$
$$\phi_A(x) = x + x + x^2 = 2x + x^2$$

Let's now consider a bin of green marbles – two large marbles (denoted G). We define B to be the set of all selections of ≥ 1 marbles. We know:

$$B = \{\{G\}, \{G, G\}\}$$
$$w(\sigma) = |\sigma|$$
$$\phi_B(x) = x + x^2$$

3.4.1 Sum Lemma

Let $S = A \cup B = \{\{r\}, \{R\}, \{r, R\}, \{G\}, \{G, G\}\}$, and note that $A \cap B = \emptyset$. What is the generating function for S?

$$\phi_S(x) = \underbrace{(x + x + x^2)}_{\phi_A(x)} + \underbrace{(x + x^2)}_{\phi_B(x)}$$

This works in general.

Theorem (Sum Lemma). *We have a set S of objects with weight w. Let A and B be partitions of S. Then:*

$$\phi_S(x) = \phi_A(x) + \phi_B(x)$$

Proof.

$$\phi_S(x) = \sum_{\sigma \in S} x^{w(\sigma)} = \underbrace{\sum_{\sigma \in A} x^{w(\sigma)}}_{\phi_A(x)} + \underbrace{\sum_{\sigma \in B} x^{w(\sigma)}}_{\phi_B(x)}$$

$\square$

3.4.2 Product Lemma

Let $S = A \times B = \{(\{r\}, \{G\}), (\{R\}, \{G\}), (\{r, R\}, \{G\}), (\{r\}, \{G, G\}), (\{R\}, \{G, G\}), (\{r, R\}, \{G, \overline{G}\})\}$. S is the various ways of selecting marbles from both bins. Let $w(\sigma)$ be the number of marbles selected in total.

Note: you can think of a generating series as the sum of all objects' $x^{w(\sigma)}$, or you can think of it as the sum of all $a_k x^k$.

$$\phi_S(x) = x^2 + x^2 + x^3 + x^3 + x^3 + x^4$$
$$= 2x^2 + 3x^3 + x^4$$
$$= (x + x + x^2)(x + x^2)$$
$$= \phi_A(x) \cdot \phi_B(x)$$

13

This works in general.

Each term in $\phi_A(x)$ corresponds to an object in A, and each term in $\phi_B(x)$ corresponds to an object in B. When you find the product, it automatically does the counting for you, due to exponentiation laws.

Theorem (Product Lemma). *Let A be a set where objects have weight α, and let B be a set where objects have weight β. Let $S = A \times B$ be a set of all objects $(a, b) \in S$, where $w[(a, b)] = \alpha(a) + \beta(b)$. Then:*

$$\phi_S(x) = \phi_A(x) \cdot \phi_B(x)$$

Proof.

$$\phi_S(x) = \sum (a, b) \in S x^{w[(a,b)]}$$
$$= \sum_{(a,b) \in S} x^{\alpha(a) + \beta(b)}$$
$$= \underbrace{\left[\sum_{a \in A} x^{\alpha(a)} \right]}_{\phi_A(x)} \cdot \underbrace{\left[\sum_{b \in B} x^{\beta(b)} \right]}_{\phi_B(x)}$$

$\square$

Example 3.14. Given integers $n \geq 0$ and $k \geq 0$, how many k-tuples $(m_1, m_2, \ldots, m_k)$ (where $m_i \geq 0, m_i \in \mathbb{Z}$) exist where $m_1 + m_2 + \ldots + m_k = n$?

Suppose $n = 3$ and $k = 2$. You'll have $(0, 3), (1, 2), (2, 1)$, and $(3, 0)$ – four possibilities (notice order matters).

We have $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}, w(a) = a$. Then:

$$\phi_{\mathbb{N}_0}(x) = \sum_{n \geq 0} a_n x^n = 1 + x + x^2 + x^3 + \ldots = \frac{1}{1 - x}$$

Now, let $S = \overbrace{\mathbb{N}_0 \times \mathbb{N}_0 \times \ldots \times \mathbb{N}_0}^{\mathbb{N}_0 \text{ appears } k \text{ times}}$. The objects in S are sequences of form $(m_1, m_2, \ldots, m_k)$, where $m_i \geq 0, m_i \in \mathbb{Z}$. We define $w[(m_1, m_2, \ldots, m_k)] = m_1 + m_2 + \ldots + m_k$.

$$\phi_S(x) = [\phi_{\mathbb{N}_0}(x)]^k = \frac{1}{(1 - x)^k} \text{ by the product lemma}$$

Therefore, the number of k-tuples $(m_1, m_2, \ldots, m_k)$ (where $m_i \geq 0, m_i \in \mathbb{Z}$) where $m_1 + m_2 + \ldots + m_k = n$ is given by $[x^n] \frac{1}{(1-x)^k}$. But we cannot figure out the coefficient. Let's leave generating functions for now, and find a combinatorial proof for this.

When you use the product lemma, you need to ensure:

1. Ensure it's used on something found by taking the cartesian product.

2. The weight is equal to the sum of the weights.

14

Example 3.15. Let $n = 5$ and $k = 3$. We have:

$$(1, 2, 2): \bullet \mid \bullet \bullet \mid \bullet \bullet$$
$$(2, 3, 0): \bullet \bullet \mid \bullet \bullet \bullet \mid$$

We have n dots and $k - 1$ intervals, which gives us:

$$\binom{n + (k-1)}{k-1} = \binom{7}{2} \text{ (in this case)}$$

We always want two bars because $k = 3$. In general, we always want $k - 1$ bars. We want n dots. The combination above is formed by the need to place $k - 1$ bars among all of the positions.

By combining the previous two examples, we have proven the following theorem.

Theorem (Theorem 1.6.5)**.**

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

Definition. Some integer n has **composition** $(m_1, m_2, \ldots, m_k)$ if $m_1 + m_2 + \ldots + m_k = n$, where $m_i \geq 1, m_i \in \mathbb{Z}$. Note that the only difference from earlier is that $m_i \geq 1$ instead of $m_i \geq 0$.

Example 3.16. We have $\mathbb{N} = \{1, 2, 3, \ldots\}, w(a) = a$, which gives us:

$$\phi_{\mathbb{N}}(x) = x + x^2 + x^3 + \ldots = x(1 + x + x^2 + \ldots) = \frac{x}{1-x}$$

Note that $\phi_{\mathbb{N}}(x)$ is missing the object of size zero (the constant term).

$$\overbrace{\phantom{\mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N}}}^{k \text{ occurrences of } \mathbb{N} \text{ here}}$$
Let $S = \mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N}$. We also define the weight as $w[(m_1, m_2, \ldots, m_k)] = m_1 + m_2 + \ldots + m_k$. Then:

$$\phi_S(x) = [\phi_{\mathbb{N}}(x)]^k = \frac{x^k}{(1-x)^k}$$

We're interested in finding $[x^k]x^k\frac{1}{(1-x)^k}$.

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

Example 3.17. We now want to know the number of compositions of n (where $n \geq 1$) where we have an arbitrary number of parts. We have: $S = \mathbb{N} \cup \mathbb{N}^2 \cup \mathbb{N}^3 \cup \mathbb{N}^4 \cup \mathbb{N}^5 \cup \ldots$. The weight function is the same as before – the sum of the parts. That gives us:

$$\phi_S(x) = \sum_{k \geq 1} \phi_{\mathbb{N}^k}(x) = \sum_{k \geq 1} \left(\frac{x}{1-x}\right)^k$$

15

We want:

$$[x^n] \sum_{k \geq 1} \left(\frac{x}{1-x} \right)^k$$

Which is a composition of:

$$A(y) = y + y^2 + y^3 + \ldots = y(1 + y + y^2 + \ldots) = \frac{y}{1-y}$$

$$B(x) = \frac{x}{1-x}$$

The composition is $A(B(x))$, but we need to be careful before using compositions. We can easily check that the constant of $B(x)$ is not zero, as required:

$$B(x) = \frac{x}{1-x} = x(1 + x + x^2 + \ldots) \implies [x^0]B(x) = 0$$

The composition is well-defined. So, we have:

$$\sum_{k \geq 1} \left(\frac{x}{1-x} \right)^k = \frac{\frac{x}{1-x}}{1 - \frac{x}{1-x}} = \frac{x}{1-2x}$$

We still need to figure out the coefficient $[x^n]\frac{x}{1-2x}$.

$$[x^n]\frac{x}{1-2x} = [x^{n-1}]\frac{1}{1-2x} \tag{1}$$
$$= [x^{n-1}](1 + y + y^2 + \ldots) \tag{2}$$
$$= [x^{n-1}](1 + (2x) + (2x)^2 + \ldots) \tag{3}$$
$$= 2^{n-1} \tag{4}$$

(1) is a common, useful trick. We eliminate any instances of x that are simply multiplied by something, by reducing the power of the coefficient we're looking for. (4) is true since every term is in the form $(2x)^k$.

We might be able to avoid generating functions in some cases by using a combinatorial proof. Now, we'll look at an arbitrary, convoluted example where a combinatorial proof would not suffice. This aims to show that generating functions are solid and can apply in many more situations than combinatorial proofs.

Example 3.18. We want to find the number of compositions of n with $2k$ parts, where the first k parts are ≤ 5 and the last k parts are ≥ 3.

A specific instance of this problem is when $n = 22$ and $k = 3$, we have:

$$(\underbrace{\ldots}_{\leq 5}, \underbrace{\ldots}_{\geq 3})$$

$$(\underbrace{1, 3, 5}_{\leq 5}, \underbrace{3, 6, 4}_{\geq 3})$$

16

It's useful to think about what you're counting. In this case, you're counting the k-tuples, so this is the cartesian product of six sets (the first three being the set of positive integers ≤ 5 and the last three being the set of integers ≥ 3).

$$\mathbb{N}_{\leq 5} = \{1, 2, 3, 4, 5\}$$
$$\mathbb{N}_{\geq 3} = \{3, 4, 5, \ldots\}$$

$$S = (\mathbb{N}_{\leq 5})^k \times (\mathbb{N}_{\geq 3})^k$$

The weight is the sum of the six individual numbers, since $\mathbb{N}_{\leq 5}$ and $\mathbb{N}_{\geq 3}$'s weights are both defined by $w(a) = a$, which gives us:

$$\phi_{\mathbb{N}_{\leq 5}}(x) = x + x^2 + x^3 + x^4 + x^5$$
$$\phi_{\mathbb{N}_{\geq 3}}(x) = x^3 + x^4 + x^5 + \ldots$$

We can expand the generating functions $\phi_{\mathbb{N}_{\leq 5}}(x)$ and $\phi_{\mathbb{N}_{\geq 3}}(x)$.

$$\begin{aligned}\phi_{\mathbb{N}_{\leq 5}}(x) &= x + x^2 + x^3 + x^4 + x^5 \\ &= x(1 + x + x^2 + x^3 + x^4) \\ &= x\left(\frac{1 - x^5}{1 - x}\right)\end{aligned}$$

$$\begin{aligned}\phi_{\mathbb{N}_{\geq 3}}(x) &= x^3 + x^4 + x^5 + \ldots \\ &= x^3(1 + x + x^2 + \ldots) \\ &= \frac{x^3}{1 - x}\end{aligned}$$

Now, we have $S = (\mathbb{N}_{\leq 5})^k \times (\mathbb{N}_{\geq 3})^k$ with weight function $w[(a_1, \ldots, a_{2k})] = a_1 + a_2 + \ldots + a_{2k}$. By the product lemma, we get:

$$\begin{aligned}\phi_S(x) &= x^k \left(\frac{1 - x^5}{1 - x}\right)^k \left(\frac{x^3}{1 - x}\right)^k \\ &= x^{4k}(1 - x^5)^k(1 - x)^{-2k}\end{aligned}$$

We're still interested in finding $[x^n]\phi_S(x)$. This becomes tedious, but the general idea is:

$$[x^n] \quad \underbrace{x^{4k}}_{\text{collapse into } [x^n] \text{ to become } [x^{n-4k}]} \cdot \underbrace{(1 - x^5)^k}_{\text{expand with binomial theorem}} \cdot \underbrace{(1 - x)^{-2k}}_{\text{use formula } [x^n]\frac{1}{(1-x)^k}}$$

After much tedious work, you'll discover that the final result is:

$$[x^n]\phi_S(x) = \sum_{i=0}^{\lfloor \frac{n-4k}{5} \rfloor} (-1)^i \binom{k}{i} \binom{n - 5i - 2k - 1}{2k - 1}$$

This couldn't have been found with a combinatorial proof. That's why generating functions are powerful – they work even in convoluted situations like this one.

17

Example 3.19. We're interested in the number of compositions of n where all parts are odd. There can be an arbitrary number of parts.

For example, with $n = 5$, the five solutions are:

$$\{(1, 1, 1, 1, 1), (5), (3, 1, 1), (1, 3, 1), (1, 1, 3)\}$$

We'll define $n = 0$ to have a unique composition (), the empty tuple.

We have $\mathbb{N}_{\mathrm{odd}} = \{1, 3, 5, 7, \ldots\}$, with its weight function defined to be $w(a) = a$ for any $a \in \mathbb{N}_{\mathrm{odd}}$. That gives us its generating function:

$$\phi_{\mathbb{N}_{\mathrm{odd}}}(x) = x + x^3 + x^5 + x^7 + \ldots \tag{1}$$

$$= x(1 + x^2 + x^4 + x^6 + \ldots) \tag{2}$$

$$= x(1 + y + y^2 + y^3 + \ldots) \text{ where } y = x^2 \tag{3}$$

$$= \frac{x}{1 - y} \tag{4}$$

$$= \frac{x}{1 - x^2} \tag{5}$$

(3) is an acceptable composition because x^2 has a constant term of zero.

Now, we have that $S = () \cup_{k \geq 1} \mathbb{N}_{\mathrm{odd}}^k$. By the sum and product lemmas, the generating function for S is:

$$\phi_S(x) = 1 + \sum_{k \geq 1} \phi_{\mathbb{N}_{\mathrm{odd}}}^k(x) \tag{1}$$

$$= 1 + \sum_{k \geq 1} \left(\frac{x}{1 - x^2} \right)^k \tag{2}$$

$$= \sum_{k \geq 0} \left(\frac{x}{1 - x} \right)^k \tag{3}$$

$$= 1 + z + z^2 + z^3 + \ldots \text{ where } z = \frac{x}{1 - x^2} \tag{4}$$

$$= \frac{1}{1 - z} \tag{5}$$

$$= \frac{1}{1 - \frac{x}{1 - x^2}} \tag{6}$$

$$= \frac{1 - x^2}{1 - x - x^2} \tag{7}$$

(4) is a valid composition because $\frac{x}{1 - x^2}$ has a constant term of zero.

What is $[x^n]\frac{1 - x^2}{1 - x - x^2}$? (Don't think of assigning values to x. Just focus on cancelling them out.)

$$\frac{1-x^2}{1-x-x^2} = \sum_{n\geq 0} a_n x^n$$

$$1 - x^2 = (1 - x - x^2)(a_0 + a_1 x + a_2 x^2 + \ldots)$$

$$= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots - a_0 x - a_1 x^2 - a_2 x^3 - a_3 x^4 - \ldots - a_0 x^2 - a_1 x^3 - a_2 x^4 - a_3 x^5 - \ldots$$

$$= a_0 + (a_1 - a_0)x + (a_2 - a_1 - a_0)x^2 + (a_3 - a_2 - a_1)x^3 + \ldots$$

We know $a_0 = 1$ and $(a_1 - a_0) = 0$, and so on. We can express a recurrence relation for this.

$$a_0 = 1$$
$$a_1 - a_0 = 0 \implies a_1 = 1$$
$$a_2 - a_1 - a_0 = -1 \implies a_2 = -1 + a_1 + a_0 = 1$$
$$a_3 - a_2 - a_1 = 0 \implies a_3 = a_1 + a_2 = 2$$
$$a_4 = a_3 + a_2 = 3$$
$$a_5 = a_4 + a_3 = 5$$
$$\vdots$$

For all $n \geq 3$, we have that $a_n = a_{n-1} + a_{n-2}$. This defines the **fibonacci numbers**.

Definition. The **golden ratio** is a pair of integers a and b such that $\frac{a+b}{a} = ab$. It's a ratio that comes up in nature a lot, and is aesthetically pleasing.

You can approximate the golden ratio with the Fibonacci numbers. $\frac{a_n}{a_{n-1}}$ approaches the golden ratio as $n \to \infty$.

Example 3.20. Let S_n be the set of compositions into odd numbers of n. $|S_n| = |S_{n-1}| + |S_{n-2}|$ for $n \geq 2$. S_n is partitioned by S_{n-1} and S_{n-2}. Is there a bijection between S_n and $S_{n-1} \cup S_{n-2}$?

Let's look at the case where $n = 5$. We have:

$$\overbrace{\{(1,1,1,1,1),(3,1,1),(1,3,1),(1,1,3),(5)\}}^{S_n}$$
$$\{(1,1,1,1),(3,1),(1,3),\underbrace{(1,1,1),(3)}_{S_{n-2}}\}$$

where S_{n-1} underbraces $\{(1,1,1,1),(3,1),(1,3)\}$.

Notice that each element in S_{n-1} and S_{n-2} can be obtained from S_n by either removing the last element entirely, or by subtracting 2 from the last element. That's the bijection we're looking for, which we will now define more formally as $f : S_n \to S_{n-1} \cup S_{n-2}$:

$$f(a_1, \ldots, a_k) = \begin{cases} (a_1, \ldots, a_{k-1}) & a_k = 1 \\ (a_1, \ldots, a_{k-2}) & a_k \geq 3 \end{cases}$$

Note that $f(a_1, \ldots, a_k)$ is undefined for $1 < k < 3$, but that's okay because we're only interested in odd natural numbers.

We have to somehow show that f actually is a bijection. We can do that by constructing its inverse. In our case, the inverse is simply providing an inverse procedure.

Therefore, $|S_n| = |S_{n-1}| + |S_{n-2}|$, which is a general property of bijections.

4   Binary Strings

Definition. A **binary string** is a string composed of 0s and 1s. For example, 011001110011 is a binary string.

Definition. We define the operation of **concatenation of two binary strings** a_1, a_2 as $a_1 a_2$. For example, if $a_1 = 110$ and $a_2 = 011$, the concatenation $a_1 a_2 = 110011$.

Definition. The **concatenation AB of two sets** (A and B) of binary strings is defined as all possible strings formed as concatenations of one string from set A followed by one string from set B. For example, if $A = \{011, 11\}$ and $B = \{10, 0\}$, then $AB = \{01110, 0110, 1110, 110\}$.

Definition. Suppose A is a set of strings. Then $A^k = \underbrace{AAAAA \ldots A}_{k \text{ times}}$.

Definition. We define $A^\star = \{\epsilon\} \cup A \cup A^2 \cup A^3 \cup \ldots$, where ϵ represents the empty string.

Example 4.1. What is $\{0, 1\}^\star$? It's the set of *all* binary strings.

Example 4.2. What's $\{0, 1\}^5$? $\{0, 1\}^5 = \{0, 1\}\{0, 1\}\{0, 1\}\{0, 1\}\{0, 1\}$. $\{0, 1\}^5$ is the set of all binary strings of length 5.

Example 4.3. Describe the set S of all binary strings with no three consecutive 1s. For example: $a = 0110001\underline{111}01001 \notin S$, $b = 0\underline{111}10 \notin S$, but $c = 0110010011011 \in S$. We aim to express S using expression-$\star$ concatenation.

Let's take a second look at c.

$$c = \underbrace{0, 110, 0, 10, 0, 110,}_{(1)} \underbrace{11}_{(2)} \in S$$

1. A sequence of at most two ones followed by zero, repeated: $\{0, 10, 110\}^\star$

2. A sequence of zero, one, or two ones: $\{\epsilon, 1, 11\}$.

Therefore, $S = \{0, 10, 110\}^\star \{\epsilon, 1, 11\}$. Note that ϵ is an element of $\{\text{anything}\}^\star$.

Definition. A **block** in a binary string is equal to the maximum sequence of 0s or 1s.

Example 4.4. List all the blocks in the string 1100011110110101.

$$\underbrace{11}\,\underbrace{000}\,\underbrace{1111}\,\underbrace{0}\,\underbrace{11}\,\underbrace{0}\,\underbrace{1}\,\underbrace{0}\,\underbrace{1}$$

Example 4.5. Describe the set S of strings with no blocks of length 2. For example, $a = 10\underline{11}000101 \notin S$, but $b = 1110111000101000 \in S$.

Let's take another look at b.

$$b = \underbrace{111}_{(1)}, \underbrace{0111, 0001, 01}_{(2)}, \underbrace{000}_{(3)} \in S$$

1. A sequence of ones, of any length other than length 2: $\{\epsilon, 1, 111, 1111, 11111, \ldots\}$.

2. A sequence of zeroes (of any non-zero length other than length 2), followed by a sequence of ones (of any non-zero length other than length 2), repeated: $[\{0, 000, 0000, \ldots\}\{1, 111, 1111, \ldots\}]^\star$.

3. A sequence of zeroes, of any length other than length 2: $\{\epsilon, 0, 000, 0000, 00000, \ldots\}$.

It's important to note that $\{1, 111, 1111, \ldots, 0, 000, 0000, \ldots\}^\star$ does not work because you could pick two zeroes or two ones consecutively, which is not allowed. You have to be very careful that you don't generate strings that you don't want to generate.

4.1 Generating Functions for Strings

We'd like to have something like the product lemma but for strings.

Let S be the set of binary strings. Then the generating function for S is defined as:

$$\phi_S(x) = \sum_{n \geq 0} a_n x^n \text{ where } a_n \text{ is the number of strings of length } n \in S$$

Example 4.6. Let $A = \{0, 01\}$ and $B = \{0, 10\}$. Their generating functions are $\phi_A(x) = \phi_B(x) = x + x^2$. What is the generating function for AB?

It's easy to see that $AB = \{00, 010, 0110\}$, which gives us $\phi_{AB}(x) = x^2 + x^3 + x^4$. Also note that:

$$\phi_A(x) \cdot \phi_B(x) = (x + x^2) \cdot (x + x^2)$$
$$= x^2 + 2x^3 + x^4$$

Therefore, in this case, $\phi_{AB}(x) \neq \phi_A(x) \cdot \phi_B(x)$. Why is this? $A \times B = \{(0, 0), (01, 0), (0, 10), (01, 10)\}$. Note that the string for $(01, 0)$ and $(0, 10)$ is the same (010), but it's only going to be included in AB once. That's where the trouble is.

Definition. A, B is **ambiguous** if all three of these properties hold:

- $(a_1, b_1), (a_2, b_2) \in A \times B$
- $(a_1, b_1) \neq (a_2, b_2)$
- $a_1 b_1 = a_2 b_2$

In the previous example, $(0, 10)(01, 0) \in A \times B$ and $(0, 10) \neq (10, 0)$, but $010 = 010$.

Note that the definition of ambiguity is equivalent to saying that $|A \times B| \neq |AB|$.

21

Theorem (Product Lemma for Strings). *Let A, B be sets of binary strings. If A, B are unambiguous, then $\phi_{AB}(x) = \phi_A(x) \cdot \phi_B(x)$.*

Proof. In order to prove this theorem, we need to show that under the given assumptions, $|AB| = |A \times B|$, which we can show by showing there is a bijection.

Let S_n be the set of strings of length n of AB, and let T_n be the set of pairs $(a, b) \in A \times B$ such that $length(a) + length(b) = n$. Our claim is that $f[(a, b)] = ab, f : T_n \to S_n$ is a bijection.

In order to prove that $T_n \to S_n$ is a bijection, two things must be proven. We have to show that it is both onto and injective.

1. Onto. Every set in S_n is in the form ab where $a \in A$ and $b \in B$ such that $ab = f[(a, b)]$.

2. Injective. Let $(a_1, b_1), (a_2, b_2) \in T_n$. Suppose:
$$\underbrace{f[(a_1, b_1)]}_{a_1 b_1} = \underbrace{f[(a_2, b_2)]}_{a_2 b_2}$$

Then since A, B is unambiguous, $(a_1, b_1) = (a_2, b_2)$.

Using the claim we just proved, $|S_n| = |T_n|$. By the product lemma (on generating functions in general), we have:
$$|S_n| = |T_n| = [x^n]\phi_{A \times B}(x) = [x^n]\phi_A(x) \cdot \phi_B(x)$$

$\square$

Theorem (Sum Lemma for Strings). *Let S be a set of binary strings. Let A, B be partitions of S. Then $\phi_S(x) = \phi_A(x) + \phi_B(x)$.*

The proof of the sum lemma for strings is the same as the proof of the sum lemma for sets in general.

Definition. An expression is **unambiguous** if there exists a unique way of writing the string according to the expression.

For example: $\{0, 10, 110\}^\star\{\epsilon, 1, 11\}$ is the set of strings with no more than two consecutive ones. Let's examine the arbitrary string 0001101011001. If we split the string after every zero, we get $0, 0, 0, 110, 10, 110, 0, 1$, which is a unique way of breaking down the string.

Proposition. *Suppose $A^\star$ is unambiguous and $\epsilon \notin A$. Then $\phi_{A^\star}(x) = \frac{1}{1 - \phi_A(x)}$.*

Proof. We have $A^\star = \{\epsilon\} \cup A \cup A^2 \cup A^3 \cup A^4 \cup \ldots$. What is $\phi_{A^k}(x)$?

$$\begin{aligned}
\phi_{A^k}(x) &= [\phi_A(x)]^k \text{ by the product lemma for strings} \\
&= 1 + \phi_A(x) + \phi_{A^2}(x) + \phi_{A^3}(x) + \ldots \text{ by the sum lemma} \\
&= 1 + \phi_A(x) + [\phi_A(x)]^2 + [\phi_A(x)]^3 + \ldots \\
&= 1 + y + y^2 + y^3 \text{ by letting } y = \phi_A(x) \\
&= \frac{1}{1 - y} \\
&= \frac{1}{1 - \phi_A(x)}
\end{aligned}$$

22

Note that the composition used in this proof is valid because $\epsilon \notin A$, so the constant of $\phi_A(x)$ is zero as required. That is, $[x^0]\phi_A(x) = 0$ makes the composition acceptable. □

4.2 Counting Strings

Example 4.7. Let S be the set of binary strings with no three consecutive ones (111). We can express S as $S = \{0, 10, 110\}^\star \{\epsilon, 1, 11\}$. You can verify that this is unambiguous.

We have:

$$\phi_{\{0,10,110\}}(x) = x + x^2 + x^3$$

$$\phi_{\{0,10,110\}^\star}(x) = \frac{1}{1 - x - x^2 - x^3} \text{ by proposition}$$

$$\phi_{\{\epsilon,1,11\}}(x) = 1 + x + x^2$$

$$\phi_S(x) = \phi_{\{0,10,110\}^\star}(x) \cdot \phi_{\{\epsilon,1,11\}}(x) \text{ by the product lemma for strings}$$

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

Example 4.8. Let S be the set of binary strings where no block has length 2. Recall from before:

$$S = ABC$$
$$A = \{\epsilon, 1, 111, 1111, \ldots\}$$
$$B = (\{0, 000, 0000, \ldots\}\{1, 111, 1111, \ldots\})^\star$$

For the sake of convenience, we'll define f as follows.

$$f = x + x^3 + x^4 + x^5 + \ldots$$
$$= x + x^2 + x^4 + x^5 + \ldots - x^2 \text{ by adding and removing } x^2$$
$$= x(1 + x + x^2 + \ldots) - x^2$$
$$= \frac{x}{1 - x} - x^2$$

Now, we can easily state the generating functions for A, B, and C:

$$\phi_A(x) = 1 + f$$
$$\phi_B(x) = \frac{1}{1 - f^2}$$
$$\phi_C(x) = 1 + f$$

We can now use the product lemma on ABC to find $\phi_S(x)$.

$$\phi_S(x) = \phi_A(x) \cdot \phi_B(x) \cdot \phi_C(x)$$
$$= \frac{(1+f)^2}{1-f^2}$$
$$= \frac{(1+f)(1+f)}{(1+f)(1-f)}$$
$$= \frac{1+f}{1-f}$$
$$\vdots$$
$$= \frac{1-x^2+x^3}{1-2x+x^2-x^3}$$

4.2.1   Recursive String Definitions

There's another way of constructing binary strings: recursive definitions.

Example 4.9. Let S be the set of all binary strings. We can define S recursively as $S = \{\epsilon\} \cup \{0,1\}$. Whenever you write an expression like this, you should take great care to ensure that both sides are actually equal.

One might attempt to describe S as $\{\epsilon, 0, 1\}S$, however that is ambiguous. $S = \{\epsilon\} \cup \{0,1\}S$ is unambiguous. Since there are two terms of length 1, and applying the sum & product lemmas, we get:

$$\phi_S(x) = \phi_{\{\epsilon\}}(x) + \phi_{\{0,1\}}(x) \cdot \phi_S(x) \text{ by the sum lemma}$$
$$= 1 + 2x \cdot \phi_S(x)$$
$$= \frac{1}{2-x}$$
$$= 1 + 2x + 4x^2 + 8x^3 + \dots \text{ by composition}$$

Note that $[x^n]\phi_S(x) = 2^n$ because the number of strings with length n is 2^n.

Example 4.10. Let S be the set of all binary strings with no three consecutive ones (111).

Consider the arbitrary string $110000100110100011 \in S$. There are no three consecutive ones in that string. We can prefix this string with 0, 10, or 110 while maintaining the constraint that the string cannot have three consecutive ones. With this recursive definition, we're building the string from right to left.

We can express S as $S = \{\epsilon, 1, 11\} \cup S\{0, 01, 011\}$.

In order to check this, we must verify that the two sides of the union are disjoint. That's easy to confirm: the elements on the left have no zeroes in them, and all elements on the

24

right have a zero. Therefore, the sum lemma applies.

$$\phi_S(x) = \phi_{\{\epsilon,1,11\}}(x) + \phi_{\{0,10,110\}}(x) \cdot \phi_S(x)$$
$$= 1 + x + x^2 + (x + x^2 + x^3) \cdot \phi_S(x)$$
$$= \frac{1 + x + x^2}{1 - x - x^2 - x^3}$$

Example 4.11 (A harder problem)**.** Let S be the set of all strings not containing 11010. That is, 11010 is the forbidden string. Let F be the set of all strings ending in 11010, where the entire string except the last character is an element in S. That is, F is the set of strings where 11010 is at the end of the string but nowhere else in the string.

Idea:

1. Write two equations relating S and F. This is the trickiest part.

2. Write two equations relating $\phi_S(x)$ and $\phi_F(x)$.

3. Solve and get an expression for $\phi_S(x)$.

The first equation relating S and F is $\{\epsilon\} \cup S\{0,1\} = S \cup F$. We need to verify this by showing both directions of the equality.

Showing $\{\epsilon\} \cup S\{0,1\} \subseteq S \cup F$: let $a \in \{\epsilon\} \cup S\{0,1\}$. We need to show that $a \in S$ or $a \in F$.

If $a = \epsilon$, then $a \in S$ since $\epsilon \in S$. If $a = a'0$ or $a = a'1$ where $a' \in S$, then either:

- a does not have the forbidden string in it, so $a \in S$.

- a' has the forbidden string at the end, since $a' \in S$, so $a \in F$.

Showing $\{\epsilon\} \cup S\{0,1\} \supseteq S \cup F$: let $a \in S \cup F$. We need to show that $a \in \{\epsilon\} \cup S\{0,1\}$.

Suppose $a \in S$, or $a = \epsilon$. Then clearly, $a \in S\{0,1\}$. Suppose $a \in F$, then $a \in S\{0,1\}$.

The second equation relating S and F is $S\{11010\} = F$. As before, we need to verify this by showing both directions of the equality.

Showing $S\{11010\} \supseteq F$: let $a \in F$. Then we know that the string a with its last character truncated off is an element of S (it no longer can contain the forbidden string). Therefore, the prefix to 11010 is also an element of S, as required.

Showing $S\{11010\} \subseteq F$: let $a \in S\{11010\}$. We need to show that the string ends in 11010, and that the forbidden string does not occur elsewhere. But what if the forbidden string is partially in the $\in S$ part and partially in the 11010 part? Shifting the forbidden string to the left by one character several times shows that it is not possible to construct the forbidden string partially from the prefix and partially from the suffix (11010), for all shifts.

Now, let's find the generating functions of both sides of these two equations.

The intersection of $\{\epsilon\}$ and $S\{0,1\}$ is empty, so the sum lemma applies. We'll also apply the

25

product lemma to $S\{0,1\}$. The generating function for $\{\epsilon\} \cup S\{0,1\}$ is therefore $1 + \phi_S(x)2x$. On the other side of equation 1, we get $\phi_F(x) + \phi_S(x)$ by the sum lemma, since it's a partition (F only contains elements ending in the forbidden string, and S does not contain the forbidden string at all). So, for the first equation we have $1 + \phi_S(x)2x = \phi_F(x) + \phi_S(x)$.

By the product lemma, we get the generating function for $S\{11010\}$ to be $\phi_S(x)x^5$. The other side of equation 2 has a generating function of $\phi_F(x)$. So, for equation 2 we have $\phi_S(x)x^5 = \phi_F(x)$.

Next, we'll substitute $\phi_F(x)$ from equation 2 into the generating function for equation 1:

$$1 + \phi_S(x)2x = \phi_S(x)x^5 + \phi_S(x)$$

$$\vdots$$

$$\phi_S(x) = \frac{1}{1 - 2x + x^5}$$

Example 4.12. Let S be the set of strings not containing 1010, and let F be the set of strings that end in 1010, but if the last character of $f \in F$ is removed, $f \in S$. We'll apply a similar method as in the previous example.

The first equation is $\{\epsilon\} \cup S\{0,1\} = S \cup F$, as before. There is nothing about this specific forbidden string in this equation, so it applies generally.

The second equation we'd logically like to try is $S\{1010\} \overset{?}{=} F$. Let's see if that works. Let $A \in S\{1010\}$. If we're unlucky, then the prefix of 1010 will be 10, which means the forbidden string will occur with 10 in the prefix and 10 in the suffix (forming 1010). So, $S\{1010\} \neq F$.

We could instead use $S\{1010\} = F \cup F\{10\}$. Note that in the case where the forbidden string occurs partially in the prefix and partially in the suffix, we could say that is an instance of a forbidden string followed by an additional 10, which is what this equation is expressing. We would also need to check the opposite direction, $\in F \cup F\{10\} \implies \in S\{1010\}$, but we'll omit that here.

Finding the generating functions, we get $1 + \phi_S(x)2x = \phi_S(x) + \phi_F(x)$ (for equation 1) and $\phi_S(x)x^4 = \phi_F(x) + \phi_F(x)x^2$ (for equation 2), which gives us:

$$\phi_F(x) = \frac{x^4}{1 + x^2} \cdot \phi_S(x)$$

Substituting $\phi_F(x)$ into the generating function for equation 1 gives us:

$$\phi_S(x) = \left(1 - 2x + \frac{x^4}{1 + x^2}\right)^{-1}$$

Example 4.13. Let S be the set of strings where there is no odd block of 0s that is immediately followed by an odd block of 1s. For example, $010\underline{0001}011 \notin S$, but $111011000 \in S$.

First, let A be the set of a block of zeroes followed by a block of ones. That is, strings

in A are composed of at least one 0 followed by at least one 1. We can express A by $A = \{0\}\{0\}^\star\{1\}\{1\}^\star$.

Next, let B be the set of an odd block of zeroes followed by an odd block of ones. We can express B as $B = \{0\}\{00\}^\star\{1\}\{11\}^\star$.

Next, let C be the set of a block of zeroes followed by a block of ones where both blocks cannot be odd simultaneously (one can be odd, but not both of them). C can be expressed as $C = A \setminus B$.

We then have that $S = \{1\}^\star(A \setminus B)^\star\{0\}^\star$.

5 Coefficients from Rational Functions

We're interested in finding $[x^n]\frac{f(x)}{g(x)}$ where $f(x)$ and $g(x)$ are polynomials.

Suppose $\deg(f) \geq \deg(g)$, which implies $f(x) = q(x) \cdot g(x) + r(x)$, where $q(x)$ is a polynomial and $r(x)$ is a polynomial of a lower degree than f. Dividing both sides by $g(x)$ gives:

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

$$[x^n]\frac{f(x)}{g(x)} = [x^n]q(x) + [x^n]\frac{r(x)}{g(x)}$$

Example 5.1.

$$\frac{6x^4 - 5x^3 - 5x^2}{1 - 5x + 6x^2} = (x^2 - 1) + \frac{1 - 5x}{1 - 5x + 6x^2} \text{ by long division of polynomials}$$

Now, we may assume that $\deg(f) < \deg(g)$. We will have to apply a partial fraction expansion. For example:

$$\frac{1 - 5x}{1 - 5x + 6x^2} = \frac{1 - 5x}{(1 - 2x)(1 - 3x)} = \frac{A}{1 - 2x} + \frac{B}{1 - 3x}$$

$$\implies 1 - 5x = A(1 - 3x) + B(1 - 2x)$$

$$1 - 5x = (A + B) + x(-3A - 2B)$$

We need $A + B = 1$ and $-3A - 2B = -5$. After solving this system of two equations in two unknowns, you'll get $A = 3$ and $B = -2$. So, we now have:

$$\frac{1 - 5x}{1 - 5x + 6x^2} = 3[x^n] \underbrace{\frac{1}{1 - 2x}}_{1 + (2x)^1 + (2x)^2 + \ldots} -2[x^n] \underbrace{\frac{1}{1 - 3x}}_{1 + (3x)^1 + (3x)^2 + \ldots}$$

$$= 3 \cdot 2^n - 2 \cdot 3^n$$

We can generalize this result.

Generalize: we want $[x^n]\frac{f(x)}{g(x)}$ where $\deg(f) < \deg(g)$, where $g(x) = (1 - a_1 x)(1 -$

27

$a_2x)\ldots(1 - a_kx)$ where $a_1, \ldots, a_k$ are distinct. We can only apply this partial fractions method if all the roots are distinct (there are subtle differences if the roots aren't distinct). We know that:

$$\frac{f(x)}{g(x)} = \frac{c_1}{1 - a_1x} + \frac{c_2}{1 - a_2x} + \ldots + \frac{c_k}{1 - a_kx}$$

However, note that $\frac{1}{1-a_1x} = 1 + (a_1x) + (a_1x)^2 + \ldots$. So, we have:

$$[x^n]\frac{f(x)}{g(x)} = c_1a_1^n + c_2a_2^n + \ldots + c_ka_k^n$$

The previous example used this generalized form but with $k = 2$, $c_1 = A = 3$, and $c_2 = B = -2$, which made $a_1 = 2$ and $a_2 = 3$ (from the denominators).

Example 5.2. Suppose we want to find the n-th coefficient of:

$$(\star) = \frac{1 + 4x^2}{1 - 6x + 12x^2 - 8x^3}$$

$$= \frac{1 + 4x^2}{1 + 3(-2x) + 3(-2x)^2 + 1(-2x)^3}$$

$$= \frac{1 + 4x^2}{(1 - 2x)^3} \text{ (binomial coefficients)}$$

So, we're interested in finding:

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

$$= [x^n]\left[\frac{A}{1 - 2x} + \frac{B}{(1 - 2x)^2} + \frac{C}{(1 - 2x)^3}\right]$$

After solving for A, B, and C, you'll discover that $A = 1, B = -2$, and $C = 2$. Therefore, we're now looking for:

$$[x^n](\star) = [x^n]\underbrace{\frac{1}{1 - 2x}}_{(1)} - \underbrace{2[x^n]\frac{1}{(1 - 2x)^2}}_{(2)} + \underbrace{2[x^n]\frac{1}{(1 - 2x)^3}}_{(3)}$$

1. 2^n, as before.

2. Recall:

$$\frac{1}{(1 - y)^p} = \sum_{n \geq 0} \binom{n + p - 1}{p - 1} y^n$$

Let $y = 2x$. Then we get:

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

28

3. Consider $y = 2x$ again. We get:

$$2^n \binom{n + 3 - 1}{3 - 1} = \binom{n + 2}{2} 2^n$$

Putting (1), (2), and (3) together gives us:

$$[x^n](\star) = 2^n - 2(n+1)2^n + 2\binom{n+2}{2}2^n = 2^n \underbrace{[1 - 2(n+1) + \binom{n+2}{2}]}_{\text{degree } 2}$$

We can generalize this result.

Generalize: we're interested in $[x^n]\frac{f(x)}{g(x)}$ where $\deg(f) < \deg(g)$, and where $g(x) = (1-ax)^k$. We know that:

$$[x^n]\frac{1}{(1 - ax)^p} = a^n \binom{n + p - 1}{p - 1}$$

Which gives us:

$$[x^n]\frac{f(x)}{g(x)} = \sum_{p=1}^{k} C_p \binom{n + p - 1}{p - 1} a^n$$

(where C_p is the coefficient determined from the partial fraction expansion)

Remark:

$$[x^n]\frac{f(x)}{g(x)} = a^n \times (\text{polynomial of } n \text{ of degree } k - 1)$$

$$[x^n]\frac{f(x)}{(x - 3)^2(x + 2)} = [x^n]\frac{A}{(x - 3)} + [x^n]\frac{B}{(x - 3)^2} + [x^n]\frac{C}{x + 2}$$
$$= (\text{polynomial of } n \text{ of degree } \leq 1) \cdot 3^n + (\text{constant}) \cdot (-2)^n$$

(for $f(x)$ of degree 2)

6　Solving Recurrence Relations

Example 6.1. We're given:

$$(\star) = a_n - 3a_{n-1} + 2a_{n-2} = 0 \text{ for } n \geq 2$$
$$a_0 = 1$$
$$a_1 = 4$$

Let's take the coefficients of a_n, a_{n-1}, and a_{n-2} to guess:

$$(1 - 3x + 2x^2)(a_0 + a_1 x + a_2 x^2 + \ldots) = c_0 + c_1 x$$

29

We want a polynomial of degree at most 1 on the right-hand side.

We know that $[x^n]LHS = [x^n]RHS$, so for $n \geq 2, [x^n]RHS = 0$. Multiplying out, we get $(\star)$. We can say that for $n \geq 2$, $(1 - 3x + 2x^2)(a_0 + a_1x + \ldots) = c_0 + c_1x$ encodes $(\star)$.

Let's continue:

$$(1 - 3x + 2x^2)(a_0 + a_1x + a_2x^2 + \ldots) = c_0 + c_1x \text{ from earlier}$$

$$\sum_{n \geq 0} a_nx^n = \frac{c_0 + c_1}{1 - 3x + 2x^2}$$

$$= \frac{A}{1 - 2x} + \frac{B}{1 - x} \text{ by partial fraction expansion}$$

This holds when the roots are distinct, otherwise the partial fraction expansion would work out differently.

So, we have that $a_n = A \cdot 2^n + B \cdot 1^n$. We can solve for A and B using the given values for a_0 and a_1.

$$a_0 = 1 \implies A \cdot 2^0 + B \cdot 1^0 = 1$$
$$a_1 = 4 \implies A \cdot 2^1 + B \cdot 1^1 = 4$$

$$\implies A = 3, B = -2$$

Substituting the values for A and B back into our equation from earlier, we get $a_n = 3 \cdot 2^n - 2$.

Let's now look at a more efficient (lazy) approach to this.

$$q(x) = 1 - 3x + 2x^2$$
$$= (1 - \underline{2}x)(1 - \underline{1}x)$$

Now, we will define $p(x)$ such that it is a polynomial with roots 2 and 1.

$$p(x) = x^2 q\left(\frac{1}{x}\right)$$
$$= x^2\left(1 - 2\frac{1}{x}\right)\left(1 - \frac{1}{x}\right)$$
$$= (x - 2)(x - 1)$$

Now, we're just interested in the roots of $p(x)$ instead of coefficients within the factored form of $q(x)$, which is much cleaner.

Definition. A **homogeneous recurrence relation** is $a_n + c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ma_{n-m} = 0$ with initial conditions $a_0, a_1, \ldots, a_{m-1}$ (m initial terms).

Strategy:

1. Find the general form for a_n.

2. Use the initial conditions $a_0, a_1, \ldots, a_{m-1}$.

30

We have the characteristic polynomial:

$$p(x) = x^m + c_1 x^{m-1} + \ldots + c_m x^0$$

Theorem. *If $p(x)$ has m distinct roots $\beta_1, \ldots, \beta_m$ then the general form for a_n is:*

$$A_1 \beta_1^n + A_2 \beta_2^n + \ldots + A_m \beta_m^n$$

Example 6.2. We have the Fibonacci sequence $a_n - a_{n-1} - a_{n-2} = 0$ for $n \geq 2$. The initial conditions are $a_0 = 0$ and $a_1 = 1$.

We have:

$$p(x) = x^2 - x - 1 = 0$$

$$\implies x = \frac{1 \pm \sqrt{5}}{2}$$

The general form is:

$$(\star) = A_1 \left(\frac{1 + \sqrt{5}}{2} \right)^n + A_2 \left(\frac{1 - \sqrt{5}}{2} \right)^n$$

Using the initial conditions $a_0 = 0$ and $a_1 = 1$, we get:

$$n = 0 \implies A_1 + A_2 = 0$$

$$n = 1 \implies A_1 \left(\frac{1 + \sqrt{5}}{2} \right) + A_2 \left(\frac{1 - \sqrt{5}}{2} \right) = 1$$

$$\implies A_1 = \frac{1}{\sqrt{5}}$$

$$\implies A_2 = -\frac{1}{\sqrt{5}}$$

Substituting these values for A_1 and A_2 into $(\star)$ we get:

$$\frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n$$

$$\implies a_{20} = 4181$$

Example 6.3. We have the recurrence relation $a_n + 3a_{n-1} - 4a_{n-3} = 0$ for $n \geq 3$. The initial conditions are $a_0 = 0, a_1 = 4$, and $a_2 = 2$.

We have:

$$p(x) = x^2 + 3x^2 - 4$$
$$= (x + 2)^2 (x - 1)$$

31

Note that we cannot use the previous theorem here. Instead, let's pick:

$$(1 + 3x - 4x^3)(a_0 + a_1 x + a_2 x^2 + \ldots) = f(x)$$

(for $n \geq 3$ where $f(x)$ is of degree 2)

We know that $[x^n]LHS = [x^n]RHS = 0$, and we know that the LHS is $a_n + 3a_{n-1} - 4a_{n-3}$. So, we get:

$$\sum_{n \geq 0} a_n x^n = \frac{f(x)}{1 + 3x - 4x^3}$$

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

We know that $a_n = (A + Bn) \cdot (-2)^n + C \cdot 1^n$. Solving, we get that $A = -2, B = 1$, and $C = 2$.

We do the same transformation as we did before.

$$q(x) = (1 + 2x)^2(1 - x)$$
$$p(x) = x^3 q\left(\frac{1}{x}\right)$$
$$= x^3 \left(1 + 2\frac{1}{x}\right)^2 \left(1 - \frac{1}{x}\right)$$
$$= (x + 2)^2(x - 1)$$

Theorem. *If we have:*

$$a_n + c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_m a_{n-m} = 0 \ \text{where } c_m \neq 0$$

The characteristic polynomial would be:

$$p(x) = x^m + c_1 x^{m-1} + c_2 x^{m-2} + \ldots + c_m x^{m-m}$$
$$= x^m + c_1 x^{m-1} + c_2 x^{m-2} + \ldots + c_m$$

Suppose $p(x)$ has root β_i with multiplicity m_i, for $i = 1, \ldots, k$. That is, $\sum_{i=1}^{k} m_i = m$.

The general form for a_n is:

$$\sum_{i=1}^{k} Q(m_i) \beta_i^n$$

where Q is a polynomial of degree $m_i - 1$.

This result generalizes the result from last time, except now the roots don't need to be distinct.

Example 6.4. We have the recurrence relation $a_n + 3a_{n-1} + 3a_{n-2} + a_{n-3} = 0$ for $n \geq 3$, with initial conditions that we don't care about. Find the general form.

32

First, we'll write the characteristic polynomial, which will be of degree 3 since we have a_{n-3} included as one of the terms:

$$p(x) = x^3 + 3x^2 + 3x + 1 = (1 + x)^3 \text{ by binomial theorem}$$

There is one root of $p(x)$, -1, with multiplicity 3. The general form of a_n is:

$$a_n = (A + Bn + Cn^2)(-1)^n$$

6.1 Non-homogeneous Recurrences

Example 6.5. Suppose we have the recurrence relation $(\star_1) = a_n + 3a_{n-1} + 4a_{n-3} = 6 \times 2^n$ for $n \geq 3$. The initial conditions are $a_0 = 5, a_1 = 3$, and $a_3 = 25$.

Let's ignore the initial conditions for now. Let's take a guess and pick $a_n = \alpha 2^n$, where α is some constant that we'll decide on later.

$$\alpha 2^n + 3\alpha 2^{n-1} - 4\alpha 2^{n-3} = 6 \times 2^n$$
$$2^n(\alpha + \frac{3}{2}\alpha - \frac{4}{8}\alpha) = 6 \times 2^n$$
$$2\alpha = 6$$
$$\alpha = 3$$

We still haven't satisfied the initial conditions though. We want to find b_n such that $(\star_2) = b_n + 3b_{n-1} - 4b_{n-3} = 0$ (which is the same relation as before, but $= 0$). Then:

$$(a_n + b_n) + 3(a_{n-1} + b_{n-1}) - 4(a_{n-3} + b_{n-3}) = 6 \times 2^n$$

a_n is a solution to $(\star_1)$, ignoring the initial conditions. If b_n is a solution to $(\star_2)$, then $a_n + b_n$ is a solution to $(\star_1)$.

We previously showed the general form for $(\star_2)$ to be:

$$b_n = (A + B_n)(-2)^n + C$$

Therefore, the general form for $(\star_1)$ is:

$$a_n + b_n = (A + B_n) - 2^n + C + 3 \times 2^n$$

Using the initial conditions, we can solve to get $A = 1, B = 1$, and $C = 1$.

Example 6.6. Suppose we have the recurrence relation $a_n + a_{n-1} - 2a_{n-2} = 9$, with initial conditions $a_0 = 2$ and $a_1 = 2$.

We'll guess that $a_n = \alpha$ (a constant). We'd then have that $\alpha + \alpha - 2\alpha \overset{?}{=} 9$, but $0 \neq 9$, so this won't work for any value of α. It was a bad guess.

That guess didn't work, so we'll try a higher degree. Our second guess is $a_n = \alpha n$ for some constant α, which would give us:

$$\alpha n + alpha(n - 1) - 2\alpha(n - 2) = 9$$
$$\alpha = 3$$

So, $a_n = 3n$ will satisfy $a_n + a_{n-1} - 2a_{n-2} = 9$ for any n.

This concludes the counting portion of the course.

7 Introduction to Graph Theory

Definition. A **graph** G is defined as $G = (V, E)$, where V is a finite set of vertices and E is a set of edges, in the form of a set of unordered pairs of V.

Example 7.1. Let's say we have the graph $G = (V, E)$, where $V = \{1, 2, 3, 4, 5\}$ and $E = \{12, 13, 14, 23, 34, 25, 45\}$. Note that for edges, we're using the shorthand of xy to mean $\{x, y\}$ (for example: edge $12 = \{1, 2\}$).
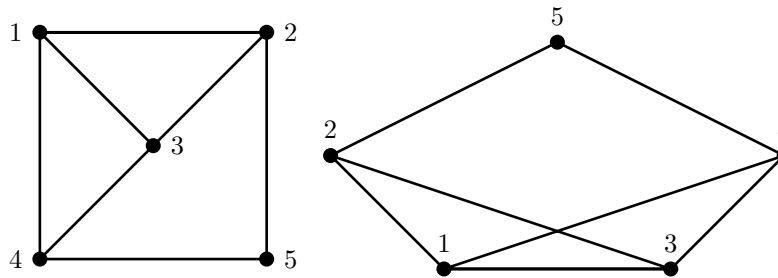
These are two different illustrations that both represent G.

Definition. Given the following graph:
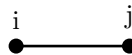
If $ij \in E$, we say i and j are **endpoints** of ij. We also say that i, j are **adjacent**, and that edge ij is **incident** to i and j.

The neighbours of $v \in V$ are defined as $\{v \in V | vu \in E\}$.

Example 7.2. Given the following graph:
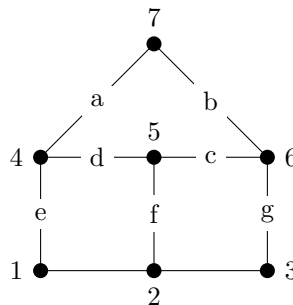
The endpoints of f are 2 and 5. 1 and 2 are adjacent. c, d, and f are the edges incident to 5. The neighbours of 2 are 1, 3, and 5.

Example 7.3. If we were to represent a street map as a graph, V would be the set of intersections and E would be the set of streets.

Example 7.4. If we were to represent a network of people, V would be a set of individuals and E would be the various relationships between those people (sets of friends).

Example 7.5. Let V be the set of binary strings of length n.

$uv \in E$ if u and v differ in exactly k positions. We have $n = 3$ (since at most 3 differ) and $k = 1$. We get the following graph:
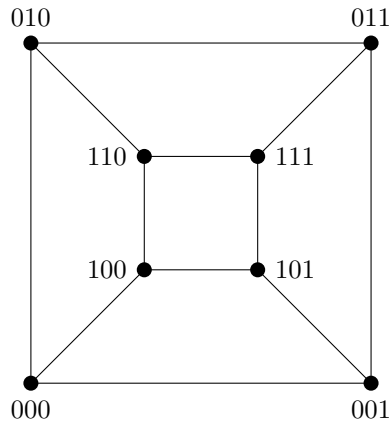
Example 7.6. If we have the following interval graph:
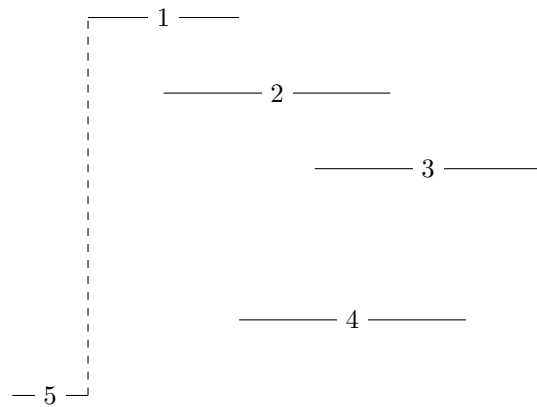
The overlaps are the edges. We can represent the same graph as:
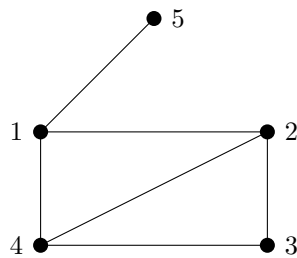
7.1   Isomorphism

Are the following two graphs the same?

G_1, with vertices $V = \{1, 2, 3, 4\}$:
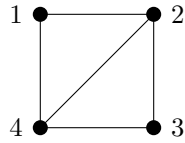
G_2, with vertices $V = \{a, b, c, d\}$:
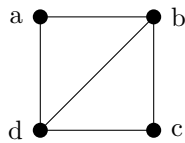
Definition. $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are **isomorphic** if there exists a bijection $\phi : V_1 \to V_2$ such that $uv \in E_1 \to \phi(u)\phi(v) \in E_2$ and $uv \notin E_1 \to \phi(u)\phi(v) \notin E_2$.

Examining the two graphs above, we have:

$$\phi(1) = a$$
$$\phi(2) = b$$
$$\phi(3) = c$$
$$\phi(4) = d$$

Pairing 1 and 3, we get $13 \in E_1 \to \phi(1)\phi(3) = ac \notin E_2$.

Pairing 4 and 3, we get $43 \in E_1 \to \phi(4)\phi(3) = dc \in E_2$.

We must continue to consider these pairings for all edges.

Example 7.7. Are the following graphs isomorphic?
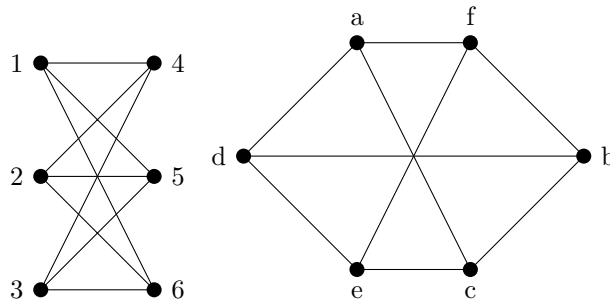
Yes! There exists a bijection ϕ:

$$1 \to a$$
$$2 \to b$$
$$3 \to e$$
$$4 \to f$$
$$5 \to d$$
$$6 \to c$$

There is no general algorithm for finding a bijection. In this case, you could see that 1, 2, and 3 have no edges and a, b, and e also have no edges.

Example 7.8. Are the following graphs isomorphic?
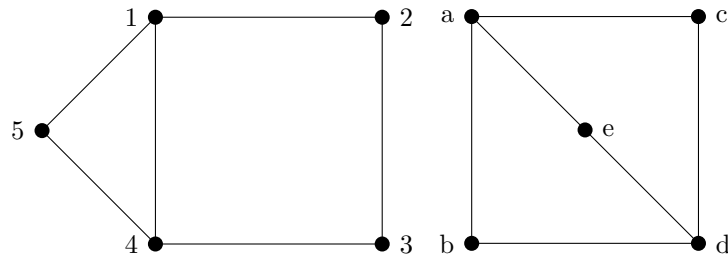
No. 1, 4, and 5 are pairwise adjacent but there are no corresponding vertices on the second graph.

7.2   Degrees of Vertices

Definition. The **degree** of a vertex is the number of edges incident to that vertex.

Example 7.9. We have the following graph, with each vertex indicating its degree:
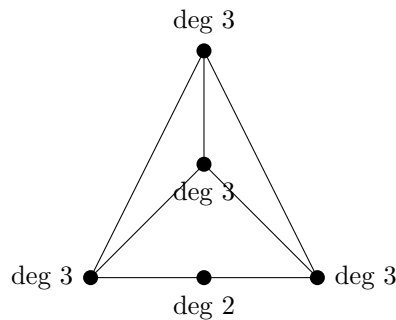
Note that $|E| = 7$, and the sum of all degrees is $3 + 3 + 3 + 3 + 2 = 14$.

Theorem. *For any graph $G = (V, E)$, $(\star) = \displaystyle\sum_{v \in V} \deg(v) = 2|E|$.*

Also, note that there is an even number of vertices of an odd degree.

37

Example 7.10. Given the following table:

Individuals	# of friends among $\{a, \ldots, i\}$
a	6
b	3
c	4
d	1
e	5
f	3
g	7
h	2
i	4

There are 5 odd numbers of friends. One of them must be lying.

Example 7.11. Given the following graph:
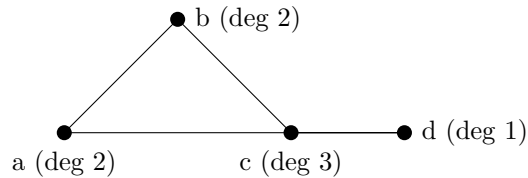
Let's examine the degrees of a, b, c, and d:

$$\deg(a) + \deg(b) + \deg(c) + \deg(d)$$
$$= |\{ab, ac\}| + |\{ab, bc\}| + |\{ac, bc, cd\}| + |\{cd\}|$$

Note that each edge appears exactly twice in the above equation – once for each endpoint. This is the general idea behind the proof for the previous theorem.

Proof. For each edge $ab \in E$, ab contributes 1 to $(\star)$ for $\deg(a)$ and ab contributes 1 to $(\star)$ for $\deg(b)$. □

7.3 Bipartite Graphs

Definition. A graph $G = (V, E)$ is **bipartite** if there exists a partittion of V into V_1 and V_2 such that every edge has one endpoint in V_1 and one endpoint in V_2.

Example 7.12. Is the following graph bipartite?

38
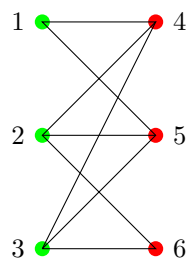
Yes, this graph is bipartite because V_1 could be the vertices on the left-hand side (1, 2, and 3), and V_2 could be the vertices on the right-hand side (4, 5, and 6).

Example 7.13. Is the following graph bipartite?
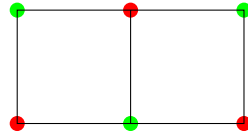
Yes, this graph is bipartite.

Not every graph is bipartite, however.

Example 7.14. Is the following graph bipartite?
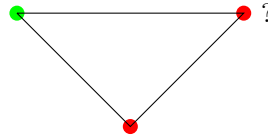
No, this graph is not bipartite as shown. This is the simplest graph that is not bipartite, in fact.

Example 7.15. Is the following graph bipartite, and is the partitioning unique?
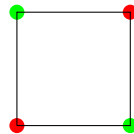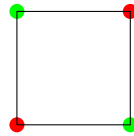
Yes, this graph is bipartite, however its partitioning is not unique. We can flip the colors (of both the squares of the graph) and still show the graph to be bipartite. So, in general, the partitioning of V into V_1 and V_2 is not unique.

The n-cube is the graph $G = (V, E)$ where V is the set of binary strings of length n and uv is an edge if u and v differ in exactly one position. For $n = 2$, we have the following graph:
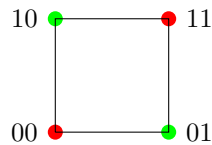
Is the n-cube bipartite for any n? Yes!

Proof. Let V_1 be the set of strings with an even number of ones, and let V_2 be the set of strings with an odd number of ones. Let $uv \in E$.

Note that we can split u and v each into two pieces, split on the single element (character) that differs between u and v. Corresponding pieces of u and v are the same.

The parity of the number of ones in u is different from the number of ones in v, since aside from that single character difference, the parity of ones is the same between u and v. Therefore, u and v are not both in V_1 or both in V_2. So, the n-cube is bipartite. $\qquad\square$

Proposition. *Let $G = (V, E)$ be a bipartite graph with partition $V = V_1 \cup V_2$. Then:*

$$\underbrace{\sum_{v \in V_1} \deg(v)}_{(1)} = \underbrace{\sum_{v \in V_2} \deg(v)}_{(2)} = |E|$$

Each edge has one endpoint in V_1 and one endpoint in V_2, which is why this intuitively makes sense. More formally:

Proof. Consider any edge $ab \in E$. Then ab contributes 1 to (1) and ab contributes 1 to (2). $\qquad\square$

Theorem (Corollary)**.** *If $|V_1| = |V_2|$, then the average degree of vertices in V_1 is equal to the average degree of vertices in V_2.*

7.4 Walks, Cycles, and Paths

A walk is like a comet flying off track – they're continuous lines.
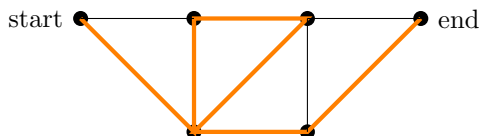
Definition. A **walk** W on graph $G = (V, E)$ from v_0 to v_n is a sequence $v_0 e_1 v_1 e_2 v_2 e_3 v_3 \ldots v_{n-1} e_n v_n$ for $i = 1, \ldots, n$ where edge e_i has endpoints v_{i-1} and v_i.

Definition. A **path** is a walk W in which $v_0, v_1, \ldots, v_n$ are all distinct.

Definition. A **cycle** occurs if $v_0, v_1, \ldots, v_{n-1}$ are distinct but $v_0 = v_n$ (the start and ending vertices are the same).

Example 7.16. We have the following graph:
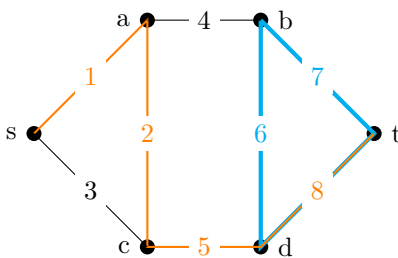
In this graph, we've visualized a path P (in orange) and a cycle C (in blue). We can express P as $P = s1a2c5d8t$ and we can express C similarly as $C = b7t8d6b$.

Proposition. *Let $G = (V, E)$ be a graph, and $x, y \in V$ where $x \neq y$. If there exists a walk from x to y, then there also exists a path from x to y.*

To find the path from a walk, when you reach a vertex that is equal to another, you ignore that cycle.

Example 7.17. Let's say you have the following graph:
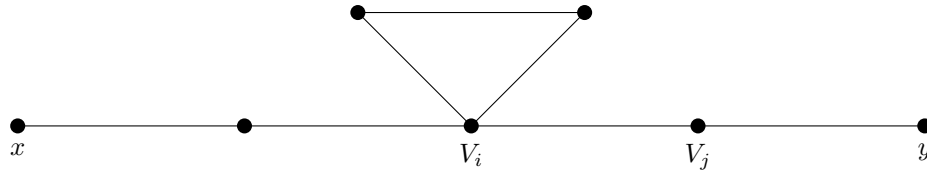
Heading from x to y, while going through the nodes in the triangle in the middle, is a walk. However, if we were to skip visiting the V_i-th node entirely, we would have a path.

Proof. Among all walks from x to y, pick a walk W with as few edges as possible. We would pick:

$$W = V_0 e_1 V_1 e_2 V_2 \ldots e_n V_n \text{ where } V_0 = x_1 \text{ and } V_n = y$$

We need to show that $V_0, V_1, \ldots, V_n$ are all distinct. Suppose for a contradiction that there exists $V_i = V_j$ for some $i < j$. That would mean:

$$W = V_0 \ldots e_i \underbrace{V_i e_{i+1} \ldots e_j}_{\text{cut off}} V_j e_{j+1} \ldots V_n$$

$$\implies W' = V_0 \ldots e_i V_j e_{j+1} \ldots V_n$$

W' is still a walk from x to y. But W' has fewer edges than W, which is a contradiction. $\square$

Theorem (Corollary). *If there exists a path from x to y and there exists a path from y to z, then there exists a path from x to z.*

This corollary is not as trivial to show as you might initially think. You can't just join the two paths, because the two paths may share some vertices.

Proof. The path from x to y followed by the path from y to z is a walk from x to z (*not* a path). By the previous result, there exists a path from x to z. $\square$

Does every graph have a cycle?

This graph does clearly not have a cycle, but it's not a terribly interesting graph. This more complicated graph also does not have a cycle:

41
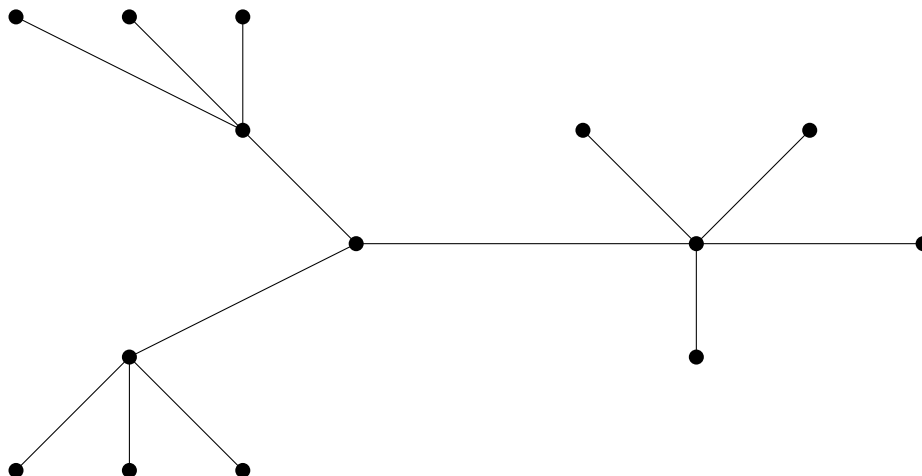
But what if every vertex has degree at least 2? In that case, it is not possible to create a graph that does *not* have a cycle. In order for each vertex to have degree of at least 2, it must loop back somewhere.

Proposition. *Let $G = (V, E)$. If for all $v \in V$, $\deg(v) \geq 2$, then G has a cycle.*

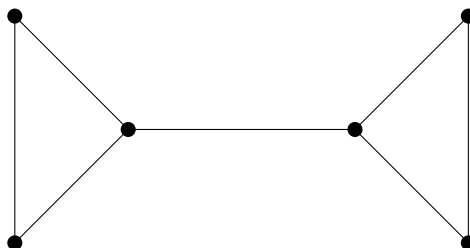*Proof.* Among all paths, pcik a path P with as many edges as possible. We have:

$$P = V_0 e_1 V_1 e_2 \ldots e_n V_n$$

Since $\deg(V_n) \geq 2$, there exists $V_n w \neq e_n$. Since P is the longest path, $w = V_i$ for some $i \in \{0, \ldots, n-2\}$. Then we have the cycle C:

$$C = V_i e_i V_{i+1} \ldots e_n V_n e_{n+1} V_i$$

$\square$

Note that it doesn't necessarily have to loop back to the "first" vertex because you may have a graph like this:

7.4.1 Hamiltonian Cycles

Definition. A cycle is **Hamiltonian** if every vertex is in the cycle.

You can think of a Hamiltonian cycle in terms of a graph of cities, where you have a person who wants to visit all the cities once and then return to their initial city.

Example 7.18. Here's an example of a Hamiltonian cycle:
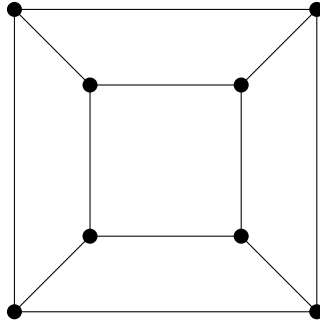
Do we always have a Hamiltonian cycle? No.

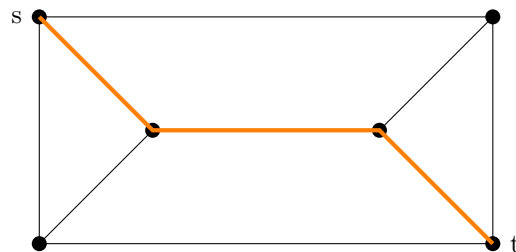**Example 7.19.** Here's an example of a graph without a Hamiltonian cycle.
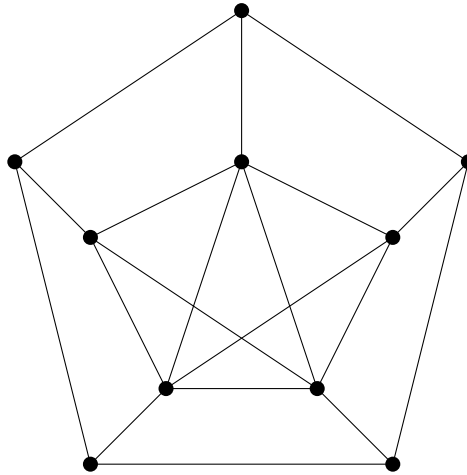
Proposition. *Let $G = (V, E)$. If for all $v \in V$, $\deg(v) \geq \frac{|V|}{2}$, then there exists a Hamiltonian cycle.*
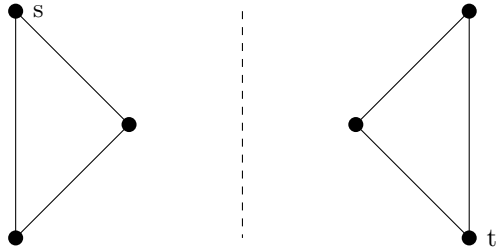
7.5   Disjoint Paths

Example 7.20. Given the following graph:
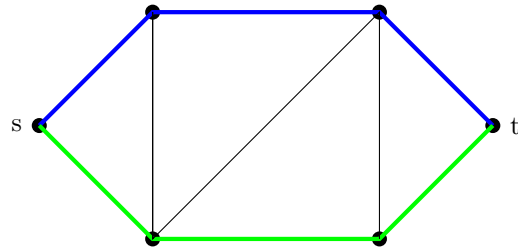

Is there a path from s to t? Yes, there are several.

Example 7.21. Given the following graph:

Is there a path from s to t? No. The two sets of vertices have no edges between them.
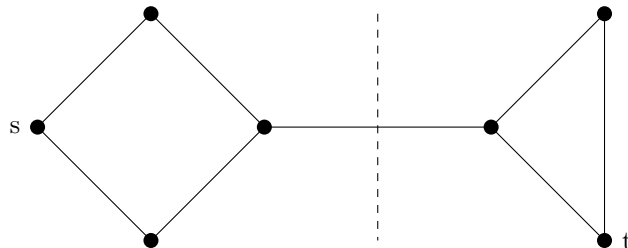
Definition. A pair of paths is **edge disjoint** if the paths do not share an edge.
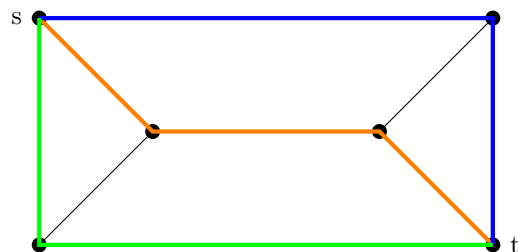
Example 7.22. Given the following graph:

Are there two edge disjoint paths from s to t? Yes. There is no edge that is both blue and green, so the two paths are disjoint.

**Example 7.23.** Given the following graph:

Are there two edge disjoint paths from s to t? No. For the same reason as the two examples above, the center edge must be used in all paths because it is the only edge that connects two otherwise disjoint sets of vertices.

Example 7.24. Given the following graph:

Are there <u>three</u> edge disjoint paths from s to t? Yes, as shown.

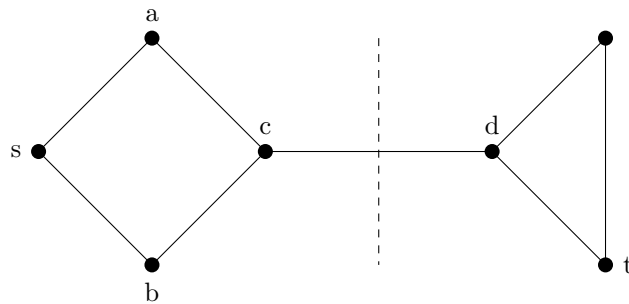**Example 7.25.** Given the following graph:
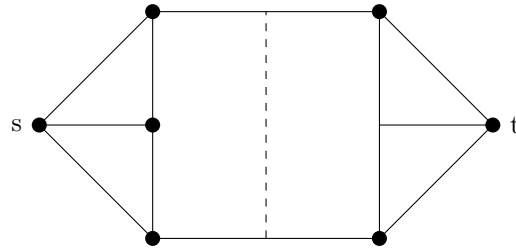
This is an example of a graph with two disjoint paths but not three. There are just two edges connecting two otherwise disjoint sets of vertices.

Let $G = (V, E)$, and let $S \subseteq V, S \neq \emptyset, S \neq V$ (we pick a proper subset of vertices). We define:

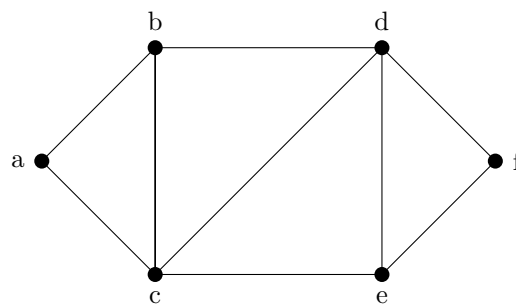$$\delta(S) := \{uv \in E | u \in S, v \notin S\}$$

Informally, $\delta(S)$ is the set of edges between V and $V \backslash S$.

Example 7.26. Given the following graph:

If $S = \{s, a, b, c\}$, we get $\delta(S) = \{cd\}$.

Example 7.27. Given the following graph:

If $S = \{b, e\}$, we get $\delta(S) = \{ab, bc, bd, ec, ed, ef\}$.

Definition. $\delta(S)$ (which is a set of edges) is the **cut induced** by S.

We say it's a cut because if we removed (cut) those edges, we would get two sets of edges with no edges connecting the two sets, so the graph would fall apart.

Definition. Let $s, t \in V (s \neq t)$. If $s \in S$ and $t \notin S$, then $\delta(S)$ is an **st-cut**.

In Example 7.24, we have a st-cut of size 2, which is why we cannot find three disjoint paths from s to t.

7.5.1 Menger's Theorem

Theorem. *Let $G = (V, E)$ be a graph, and $s, t \in V (s \neq t)$. If there exists edge disjoint paths $P_1, P_2, \ldots, P_k$ from s to t, then for all st-cuts of $\delta(S)$, $|\delta(S)| \geq k$.*

Equivalently, if you have an st-cut of size less than k, you cannot find k disjoint paths from s to t.

Proof. Let $\delta(S)$ be an st-cut ($s \in S, t \notin S$). Let $i \in \{1, \ldots, k\}$. Follow P_i from s to t. Let v_i be the last vertex in S of P_i, and let w_i be the first vertex *not* in S of P_i. Then $e_i = v_i w_i$ is an edge of P_i and $e_i \in \delta(S)$. This implies $\{e_1, e_2, \ldots, e_k\} \subseteq \delta(S)$.

Since $P_1, P_2, \ldots, P_k$ are edge disjoint, $e_1, e_2, \ldots, e_k$ are all different. This implies that $\delta(S)| \geq k$. Since $\delta(S)$ was an arbitrary cut, we have shown that all st-cuts have at least k edges. $\qquad\square$

The converse is also true, which is known as Menger's Theorem.

Theorem (Menger's Theorem). *Let $G = (V, E)$ be a graph, and $s, t \in V (s \neq t)$. If for all st-cuts $\delta(S)$, $|\delta(S)| \geq k$, then there exist edge disjoint paths $P_1, \ldots, P_k$ from s to t.*

Proof. The proof of Menger's Theorem is by performing induction on $|E| + |V|$. The base case is where you have two vertices and no edge between them, as seen here:

$$s \; \bullet \qquad\qquad \bullet \; t$$
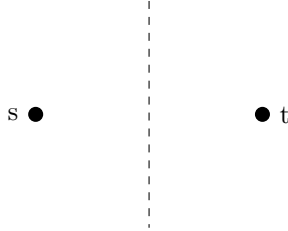
There are then two cases:

1. There exists e_1 and no st-cut that contains e_1 has exactly k edges.

2. Say, $k = 3$, for instance. Divide the graph in two, and shrink the vertices from half the graph into a single consolidated vertex. Then apply the same logic for the other half of the graph. By induction, we can find three paths on both of the smaller graphs. We want to combine these two smaller paths, which we can do by connecting the corresponding paths of the two sub-graphs.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Clicker Questions

- How many bijections are there from $\{1,\dots,n\}$ to $\{1,\dots,n\}$? $n!$, since you can't map two elements in the first set to the same one element in the second set.

- Let S be a set of objects with weight function w. Suppose that $S = A \cup B$. Does $\phi_S(x) = \phi_A(x) + \phi_B(x)$? No, not always. The sum lemma only applies when A and B are partitions of S.

- Let $S = \{(a,b)|a,b \geq 1 \in \mathbb{Z}\}, w[(a,b)] = a - b$. What is the generating function for S? There is no generating function for S, since it is not a power series. There are an infinite number of pairings – that is, there are an infinite number of objects with the same weight.

- Does $x^2 - x^4 + x^6 - x^8 + x^10 - \dots$ have an inverse? No. There is no constant term that isn't equal to zero, therefore it does not have an inverse.

- Is a composition of $A(x) = 1 + x + x^2 + x^3 + \dots$ and $B(x) = \frac{1}{1-x}$ a power series? No. $B(x)$ must have a constant term that is not zero in order for a composition to be acceptable.

- What is the power series $x^2 + x^3 + x^4 + x^5 + \dots$ equal to? It is equal to $\frac{x^2}{1-x}$, since:

$$x^2 + x^3 + x^4 + x^5 + \dots = x^2(1 + x + x^2 + \dots) = x^2\left(\frac{1}{1-x}\right) = \frac{x^2}{1-x}$$

- Is $A(B(x))$ a power series for $A(x) = 1 + x + x^2 + \dots$ and $B(x) = \frac{1}{1-x}$? No! We can only get a power series if $[x^0]B(x) = 0$, but $B(x) = \frac{1}{1-x} = 1 + x + x^2 + \dots$.

- What is the coefficient of x^3 for $\frac{1}{(1-x)^7}$? The coefficient is $\binom{9}{2}$. This could be found using the formula:

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

- The number of ways of spending exactly \$237 to buy oranges (\$1 each) and/or mangos (\$2 each) is...? It's $[x^{237}](1 + x + x^2 + x^3 + \dots)(1 + x^2 + x^4 + x^6 + \dots)$.

  You can represent this as a pair, (a,b), where a is the number of oranges and b is the number of mangos. Define a weight function $w[(a,b)] = a + 2b$. We also have $S = \{(a,b)\}, A = \{0, 1, \dots\}, B = \{0, 1, \dots\}$. Also, define weight functions for A and B: $w(a) = a, w(b) = 2b$. The generating series are $\phi_A(x) = 1 + x + x^2 + \dots$ and $\phi_B(x) = 1 + x^2 + x^4 + \dots$. Finally, use the product lemma on $\phi_A(x) \cdot \phi_B(x)$.

- The set of binary strings without consecutive zeroes can be described as...? The set can be described as $(\{\epsilon, 0\}\{1\})^\star\{\epsilon, 0\}$.

  We have to make sure this expression does not generate anything that is not in the set. Then we think about how to generate any arbitrary string contained in the set we're trying to express. There is a unique way to generate each string with the expression.

- The general solution of the recurrence relation $a_n - 4a_{n-2} = 0$ is given by $a_n = c_1 2^n + c_2(-2)^n$.

  a_{n-2} indicates that the degree of the characteristic polynomial is 2. So, we get that $p(x) = x^2 - 4 = (x+2)(x-2)$, which has roots -2 and 2.

- Suppose $a_n = (c_1 n + c_2)3^n$. Then it is the general solution to the recurrence $a_n - 6a_{n-1} + 9a_{n-2} = 0$.

  Note that 3 corresponds to the root, which appears with multiplicity 2. The characteristic polynomial is $p(x) = (x-3)^2 = x^2 - 6x + 9$.

- How many vertices are there in a 4-regular graph with 40 edges? 20.

  Recall that $\sum_{v \in V} \deg(v) = 2|E|$ (by theorem), so we get:
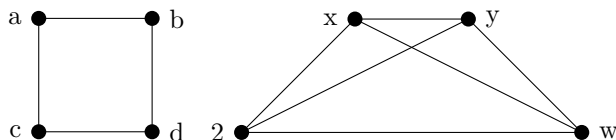
  $$\sum_{v \in V} \deg(v) = 2|E|$$
  $$4|V| = 2|40|$$
  $$4|V| = 80$$
  $$|V| = 20$$

- Are the following two graphs isomorphic?

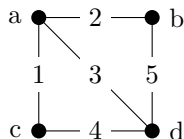 Yes! Here's a bijection between their vertices:

  $$a \to x$$
  $$d \to y$$
  $$c \to z$$
  $$b \to w$$

- Consider this graph. Is $W = a1c4d3a2b$ a walk, cycle, and/or path?

  W is a walk but not a cycle nor a path.

48