Solving System of Polynomial Equations

Carlos Osco Huaricapcha

Summer 2017, Mathematics Science Research Institute

Notes written from Maurice Rojas' lectures.

[1] I'd love to hear your feedback. Feel free to email me at coscohua@mail.sfsu.edu.

Contents

1 Introduction, Algebraic Geometry

← June 26, 2017

1.1 What is it?

Ideally, Agebraic Geometry occurs over rings other than $\mathbb{C}$. Let's see some examples of polynomial solving.

Example 1.1. Let $N = pq$ where N is a positive integer and $p, q > 1$. (Factoring.) Usually, we are given N, so we can find p and q.
The security of the R.S.A. Crypto-system is based on this *hardness*.

Example 1.2. Equilibria in Chemical Analysis systems (reaction networks).

$$\begin{aligned} \text{linear ordinary differential equation} \rightarrow \qquad && \dot{x} = 3x + 7 \\ \text{non-linear ordinary differential equation} \rightarrow \qquad && \dot{x} = \text{polynomial}(x)(\text{deg} \geq 2) \end{aligned}$$

Differential equations govern chemical reaction rates. So, when the reaction settles down the concentrations reactions an *equilibrium*, and the concentrations wind up being *real* solutions to a system of polynomial equations. It is fair to say that *real solving* in fact makes up to more than 30% of electrical engineering.

Example 1.3. $\mathbb{F}_1$: Finite field with q elements in coding theory and cryptography. You often do arithmetic over $\mathbb{F}_q$, and polynomial system solving occurs very often. (q=prime power).

Example 1.4. $\mathbb{Q}_p$(p-acid reactions): This field is related to the solution of Weil-conjectures around the mid-20th century. Multiple fields medals were ensued.

Fun fact: 40% of the field medals are awarded to Algebraic Geometry.
Let's start with easy equations (1 equation, 1 variable, 2 terms, $\mathbb{C}$).

Example 1.5. Given $c_1, c_2 \in \mathbb{C}; a_1, a_2 \in \mathbb{Z}$. How do we solve

$$c_1 x_1^{a_1} + c_2 x_1^{a_2} = 0$$

? Notice that it is easy to reduce to the case

$$x^d = c \quad \text{where} \quad d \in \mathbb{Z}; c \in \mathbb{C}.$$

In fact if you throw-out $x_1 = 0$, then we may assume $c \neq 0$.

1.2 Euler's Formula

It is easy to take d$^{\text{th}}$ roots.

$$\exp^{\sqrt{-1}\tau} = \cos\tau + \sqrt{-1}\sin\tau.$$

Exercise 1. What is a simple formula for the roots of $x_1^d = c$ using Euler's formula?

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?

For example: $10101\underline{1100}101 \notin S$.

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

For example: $1001001\underline{000}11 \notin S$.

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, colour the regions such that no two touching boundaries do not have the same colour, with the least number of colours possible.

The **four-colour theorem** states that you can always do this with four colours. It's also always possible to colour these regions with five colours. It's *sometimes* possible to colour the regions with three or fewer colours, 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

← January 9, 2013

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

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

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 $[n]$.

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

□

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

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

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.

$$\begin{array}{lccccccccc}
n = 0: & & & & & 1 & & & & \\
n = 1: & & & & 1 & & 1 & & & \\
n = 2: & & & 1 & & 2 & & 1 & & \\
n = 3: & & 1 & & 3 & & 3 & & 1 & \\
n = 4: & 1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

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

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

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:

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

□

2.3 Injections, Bijections, and Onto

← January 11, 2013

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

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, $f : S_1 \to S_2$.

Aside: 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 $g = f$). □

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 a 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 k amount of change?

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 that the coefficients of each term are the number of objects who have that the weight indicated by the exponent of the x in that term.

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.

← January 14, 2013

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.*

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.

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

We'll now prove this 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 $\phi'_S(1) = \sum_{\sigma \in S} w(\sigma) \cdot 1 =$ total weight of all objects in S.

□

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:

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + \cdots \\ B(x) &= b_0 + b_1 x + b_2 x^2 + \cdots \end{aligned}$$

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.

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

Example 3.6.

$$\begin{aligned} &(1 + x + x^2 + x^3 + \cdots)(1 - x) \\ &= 1 \cdot 1 + (1 \cdot -1 + 1 \cdot 1)x + (1 \cdot 1 + 1 \cdot -1)x^2 + \cdots \\ &= 1 \end{aligned}$$

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.

Proof. Suppose $(x+x^2)$ has an inverse. 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. □

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 $1 - x + x^2 - x^3 + x^4 - \cdots$.

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

$$\begin{aligned}
[x^0](\star) = 1 &\implies 1 \cdot b_0 = 1 \implies b_0 = 1 \\
[x^1](\star) = 0 &\implies 1 \cdot b_1 - 1 \cdot b_0 = 0 \implies b_1 = b_0 = 1 \\
[x^2](\star) = 0 &\implies 1 \cdot b_2 - 1 \cdot b_1 + 1 \cdot b_0 = 0 \implies b_2 = b_1 - b_0 = 0
\end{aligned}$$

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

← January 16, 2013

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.

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:

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

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:

$$\begin{aligned}[x^k]A(B(x)) &= [x^k]\sum_{n\geq 0} a_n[B(x)]^n \\ &= [x^k]\sum_{n\geq 0} a_n x^n R(x) \\ &= [x^k]\sum_{n\geq 0}^{k} a_n x^n (R(x))^n\end{aligned}$$

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. □

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

$$\begin{aligned}\frac{1}{1-x^2} = \frac{1}{1-y} &= 1 + y + y^2 + y^3 + \cdots \\ &= 1 + x^2 + x^4 + x^6 + \cdots\end{aligned}$$

This is a 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:

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

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:

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

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:

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

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.

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

□

3.4.2 Product Lemma

← January 18, 2013

Let $S = A \times B = \{(\{r\}, \{G\}), (\{R\}, \{G\}), (\{r, R\}, \{G\}), (\{r\}, \{G, G\}), (\{R\}, \{G, G\}), (\{r, R\}, \{G, G\})\}$. 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 $a_k x^k$.

$$\begin{aligned}\phi_S(x) &= x^2 + x^2 + x^3 + x^3 + x^3 + x^4 \\ &= 2x^2 + 3x^3 + x^4 \\ &= (x + x + x^2)(x + x^2) \\ &= \phi_A(x) \cdot \phi_B(x)\end{aligned}$$

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.

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

□

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 $\mathbb{N}_0 = \{0,1,2,3,\ldots\}, w(a) = a$ (for $a \in \mathbb{N}_0$). 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 $[x^n]\frac{1}{(1-x)^k}$. We cannot figure out this 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.

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

(1, 2, 2): • | • • | • •
(2, 3, 0): • • | • • • |

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 $\mathbb{N} = \{1, 2, 3, \ldots\}, w(a) = a$ (for $a \in \mathbb{N}$), 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).

Let $S = \overbrace{\mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N}}^{k \text{ occurrences of } \mathbb{N} \text{ here}}$. 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 $[x^n]x^k\frac{1}{(1-x)^k}$. ← January 21, 2013

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

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:

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

We want:

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

Which is a composition of:

$$\begin{aligned}
A(y) &= y + y^2 + y^3 + \ldots = y(1 + y + y^2 + \ldots) = \frac{y}{1-y} \\
B(x) &= \frac{x}{1-x}
\end{aligned}$$

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 $[x^n]\frac{x}{1-2x}$.

$$\begin{aligned}
[x^n]\frac{x}{1-2x} &= [x^{n-1}]\frac{1}{1-2x} \qquad (1)\\
&= [x^{n-1}](1+y+y^2+\ldots) \qquad (2)\\
&= [x^{n-1}](1+(2x)+(2x)^2+\ldots) \qquad (3)\\
&= 2^{n-1} \qquad (4)
\end{aligned}$$

(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:

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

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

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).

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

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

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

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

← January 23, 2013

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:

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

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.

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

$$\begin{align}
\phi_{\mathbb{N}_{\text{odd}}}(x) &= x + x^3 + x^5 + x^7 + \ldots \tag{1}\\
&= x(1 + x^2 + x^4 + x^6 + \ldots) \tag{2}\\
&= x(1 + y + y^2 + y^3 + \ldots) \text{ where } y = x^2 \tag{3}\\
&= \frac{x}{1-y} \tag{4}\\
&= \frac{x}{1-x^2} \tag{5}
\end{align}$$

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

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

$$\begin{align}
\phi_S(x) &= 1 + \sum_{k \geq 1} \phi_{\mathbb{N}_{\text{odd}}}^k(x) \tag{1}\\
&= 1 + \sum_{k \geq 1} \left(\frac{x}{1-x^2}\right)^k \tag{2}\\
&= \sum_{k \geq 0} \left(\frac{x}{1-x}\right)^k \tag{3}\\
&= 1 + z + z^2 + z^3 + \ldots \text{ where } z = \frac{x}{1-x^2} \tag{4}\\
&= \frac{1}{1-z} \tag{5}\\
&= \frac{1}{1-\frac{x}{1-x^2}} \tag{6}\\
&= \frac{1-x^2}{1-x-x^2} \tag{7}
\end{align}$$

(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 canceling them out.)

$$\begin{aligned}
\frac{1-x^2}{1-x-x^2} &= \sum_{n \geq 0} a_n x^n\\
1 - x^2 &= (1-x-x^2)(a_0 + a_1 x + a_2 x^2 + \ldots)\\
&= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots - a_0 x - a_1 x^2 - a_2 x^3 - a_3 x^4 - \ldots - a_0 x^2 - a_1 x^3 - a_2 x^4 - a_3 x^5 - \ldots\\
&= a_0 + (a_1 - a_0)x + (a_2 - a_1 - a_0)x^2 + (a_3 - a_2 - a_1)x^3 + \ldots
\end{aligned}$$

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

$$\begin{aligned} & a_0 = 1 \\ a_1 - a_0 = 0 \implies & a_1 = 1 \\ a_2 - a_1 - a_0 = -1 \implies & a_2 = -1 + a_1 + a_0 = 1 \\ a_3 - a_2 - a_1 = 0 \implies & a_3 = a_1 + a_2 = 2 \\ & a_4 = a_3 + a_2 = 3 \\ & a_5 = a_4 + a_3 = 5 \\ & \vdots \end{aligned}$$

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 $\frac{a+b}{a} = \frac{a}{b}$. 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: ← January 25, 2013

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

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_1a_2. For example, if $a_1 = 110$ and $a_2 = 011$, the concatenation $a_1a_2 = 110011$.

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: $a = 011000\underline{111}01001 \notin S$, $b = 0\underline{111}10 \notin S$, 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:

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

← January 28, 2013

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:

$$\begin{aligned} \phi_A(x) \cdot \phi_B(x) &= (x + x^2) \cdot (x + x^2) \\ &= x^2 + 2x^3 + x^4 \end{aligned}$$

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 $|A \times B| \neq |AB|$.

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 between AB and $A \times B$.

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 $\text{length}(a) + \text{length}(b) = n$. 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 of 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:

$$|S_n| = |T_n| = [x^n]\phi_{A\times B}(x) = [x^n]\phi_A(x) \cdot \phi_B(x)$$

□

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 generating functions in general.

Definition. An expression is **unambiguous** if there exists a unique way of writing every 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 $\phi_{A^k}(x)$?

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

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

← January 30, 2013

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 an unambiguous expression.

We have:

$$\begin{aligned}
\phi_{\{0,10,110\}}(x) &= x + x^2 + x^3 \\
\phi_{\{0,10,110\}^\star}(x) &= \frac{1}{1-x-x^2-x^3} \text{ by proposition} \\
\phi_{\{\epsilon,1,11\}}(x) &= 1 + x + x^2
\end{aligned}$$

$$\begin{aligned}
\phi_S(x) &= \phi_{\{0,10,110\}^\star}(x) \cdot \phi_{\{\epsilon,1,11\}}(x) \text{ by the product lemma for strings} \\
&= \frac{1+x+x^2}{1-x-x^2-x^3}
\end{aligned}$$

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

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

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

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

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

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

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

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

4.2.1 Recursive String Definitions

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

← February 1, 2013

Example 4.9. Let S be the set of all binary strings. We can define S recursively as $S = \{\epsilon\} \cup \{0, 1\}S$. 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, applying the sum & product lemmas, we get:

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

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

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

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.

<u>Idea</u>:

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.

<u>Showing $\{\epsilon\} \cup S\{0, 1\} \subseteq S \cup F$</u>: 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. ← February 4, 2013

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 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, $01\underline{0001}011 \notin S$, 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

← February 6, 2013

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:

$$\begin{aligned}\frac{1-5x}{1-5x+6x^2} &= \frac{1-5x}{(1-2x)(1-3x)} = \frac{A}{1-2x} + \frac{B}{1-3x} \\ \implies 1-5x &= A(1-3x) + B(1-2x) \\ 1-5x &= (A+B) + x(-3A-2B)\end{aligned}$$

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:

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

We can generalize this result.

Generalize: we want $[x^n]\frac{f(x)}{g(x)}$ where $\deg(f) < \deg(g)$, where $g(x) = (1-a_1x)(1-a_2x)\ldots(1-a_kx)$ 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:

$$\begin{aligned}(\star) &= \frac{1+4x^2}{1-6x+12x^2-8x^3} \\ &= \frac{1+4x^2}{1+3(-2x)+3(-2x)^2+1(-2x)^3} \\ &= \frac{1+4x^2}{(1-2x)^3} \text{ (binomial coefficients)}\end{aligned}$$

So, we're interested in finding:

$$\begin{aligned}[x^n](\star) &= [x^n]\frac{1+4x^2}{(1-2x)^3} \\ &= [x^n]\left[\frac{A}{1-2x} + \frac{B}{(1-2x)^2} + \frac{C}{(1-2x)^3}\right]\end{aligned}$$

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

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

← February 11, 2013

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

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

6 Solving Recurrence Relations

Example 6.1. We're given:

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

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

$$(1 - 3x + 2x^2)(a_0 + a_1x + a_2x^2 + \ldots) = c_0 + c_1x$$

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:

$$\begin{aligned}(1 - 3x + 2x^2)(a_0 + a_1x + a_2x^2 + \ldots) &= c_0 + c_1x \text{ from earlier}\\ \sum_{n\geq 0} a_nx^n &= \frac{c_0 + c_1}{1 - 3x + 2x^2}\\ &= \frac{A}{1-2x} + \frac{B}{1-x} \text{ by partial fraction expansion}\end{aligned}$$

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.

$$\begin{aligned}a_0 = 1 &\implies A \cdot 2^0 + B \cdot 1^0 = 1\\ a_1 = 4 &\implies A \cdot 2^1 + B \cdot 1^1 = 4\\ \\ &\implies A = 3, B = -2\end{aligned}$$

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.

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

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

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

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 $a_n + c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_m a_{n-m} = 0$ 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 $a_0, a_1, \ldots, a_{m-1}$.

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:

$$\begin{aligned} p(x) &= x^2 - x - 1 = 0 \\ \implies x &= \frac{1 \pm \sqrt{5}}{2} \end{aligned}$$

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:

$$\begin{aligned} n = 0 &\implies A_1 + A_2 = 0 \\ n = 1 &\implies A_1\left(\frac{1+\sqrt{5}}{2}\right) + A_2\left(\frac{1-\sqrt{5}}{2}\right) = 1 \end{aligned}$$

$$\begin{aligned} &\implies A_1 = \frac{1}{\sqrt{5}} \\ &\implies A_2 = -\frac{1}{\sqrt{5}} \end{aligned}$$

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:

$$\begin{aligned} p(x) &= x^3 + 3x^2 - 4 \\ &= (x+2)^2(x-1) \end{aligned}$$

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:

$$\begin{aligned} \sum_{n \geq 0} a_n x^n &= \frac{f(x)}{1 + 3x - 4x^3} \\ &= \frac{f(x)}{(1+2x)^2(1-x)} \end{aligned}$$

We know that $a_n = (A + Bn) \cdot (-2)^n + C \cdot 1^n$. Solving, we get that $A = -2, B = 1$, and $C = 2$. ← February 13, 2013

We do the same transformation as we did before.

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

Theorem. *If we have:*

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

The characteristic polynomial would be:

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

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

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.

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

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:

$$\begin{aligned} \alpha n + \alpha(n-1) - 2\alpha(n-2) &= 9 \\ \alpha &= 3 \end{aligned}$$

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

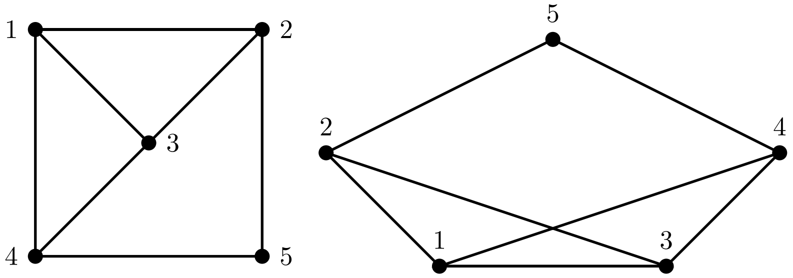
This concludes the counting portion of the course.

7 Introduction to Graph Theory

← February 15, 2013

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.

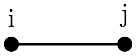
Example 7.1. Let's say we have the graph $G = (V, E)$, where $V = \{1, 2, 3, 4, 5\}$ and $E = \{12, 13, 14, 23, 34, 25, 45\}$. Note that for edges, we're using the shorthand of xy to mean $\{x, y\}$ (for example: edge $12 = \{1, 2\}$).



These are two different illustrations that both represent G.

Definition. The **complement** of the graph G, denoted $\overline{G}$, is the graph with $V(\overline{G}) = V(G)$ and edges $uv \in E(\overline{G})$ if and only if $uv \notin E(G)$.

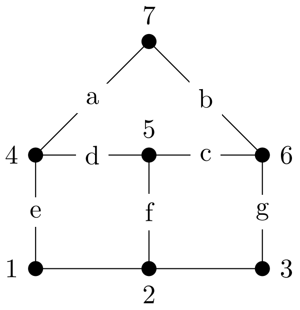
Definition. Given the following graph:



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 $\{u \in V | vu \in E\}$.

Example 7.2. Given the following graph:



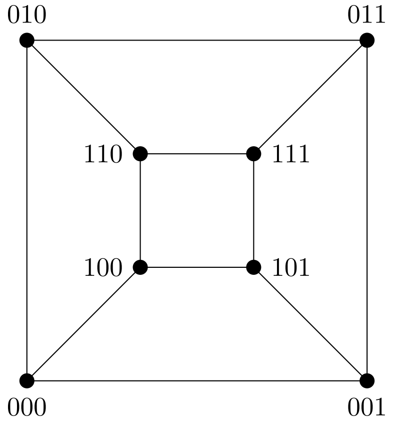
The endpoints of f are 2 and 5. 1 and 2 are adjacent. c, d, and f are the edges incident to 5. The neighbours of 2 are 1, 3, and 5.

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.

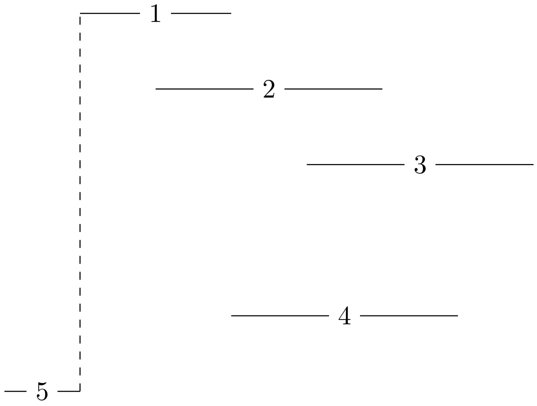
Example 7.4. If we were to represent a network of people, V would be a set of individuals and E would be the various relationships between those people (sets of friends).

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

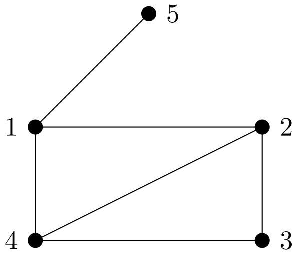
$uv \in E$ if u and v differ in exactly k positions. This is the definition of an n-cube. We have $n = 3$ (since at most 3 differ) and $k = 1$. We get the following graph:



Example 7.6. If we have the following interval graph:



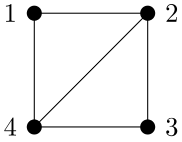
The overlaps are the edges. We can represent the same graph as:



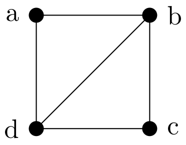
7.1 Isomorphism

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 $uv \notin E_1 \to \phi(u)\phi(v) \notin E_2$.

In other words, two graphs are isomorphic if adjacency is preserved.

Examining the two graphs above, we have:

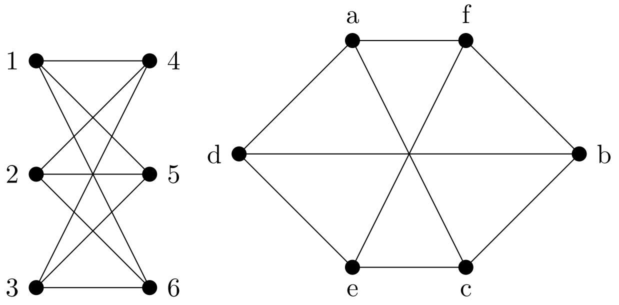
$$\begin{aligned}\phi(1) &= a\\ \phi(2) &= b\\ \phi(3) &= c\\ \phi(4) &= d\end{aligned}$$

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?

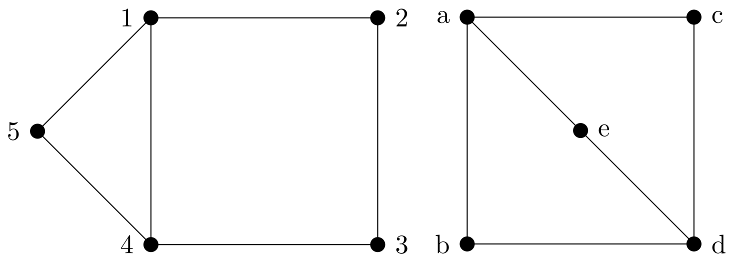


Yes! There exists a bijection ϕ:

$$\begin{aligned}1 &\to a\\ 2 &\to b\\ 3 &\to e\\ 4 &\to f\\ 5 &\to d\\ 6 &\to c\end{aligned}$$

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?

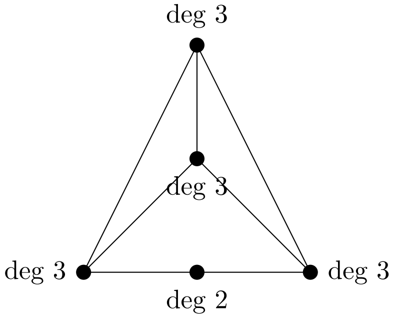


No. 1, 4, and 5 are pairwise adjacent but there are no corresponding vertices on the second graph.

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

Corollary (Handshake Lemma)**.** *There is an even number of vertices of odd degree.*

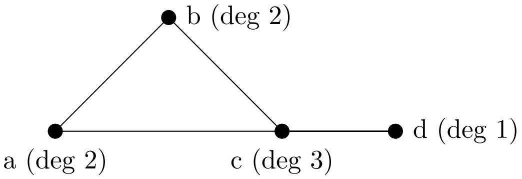
Example 7.10. Given the following table:

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.

← February 25, 2013

Example 7.11. Given the following graph:



Let's examine the degrees of a, b, c, and d:

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

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 $\deg(b)$. □

Definition. A graph in which every vertex has degree k (for some fixed k) is called a ***k*-regular** graph.

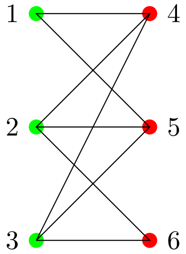
Definition. A **complete graph** is a graph in which all pairs of distinct vertices are adjacent to each other. That is, each vertex is joined to every other vertex. The complete graph with p vertices is denoted K_p (where $p \geq 1$).

7.3 Bipartite Graphs

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

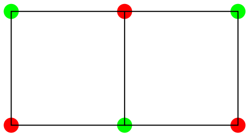
Definition. The **complete bipartite graph** $\boldsymbol{K_{m,n}}$ is a bipartite graph with partitions A and B such that all vertices in A are adjacent to the all the vertices in B, where $|A| = m$ and $|B| = n$.

Example 7.12. Is the following graph bipartite?



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).

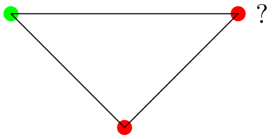
Example 7.13. Is the following graph bipartite?



Yes, this graph is bipartite.

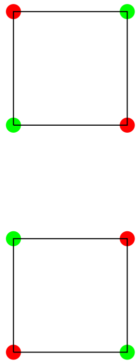
Not every graph is bipartite, however.

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.

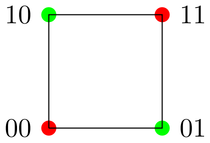
Example 7.15. Is the following graph bipartite, and is the partitioning unique?



Yes, this graph is bipartite, however its partitioning is not unique. We can flip the colours (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.

Definition. 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 n-cube:



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. □

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

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

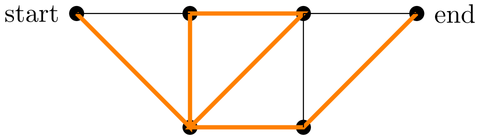
Each edge has one endpoint in V_1 and one endpoint in V_2, which is why this intuitively makes sense. Let's state this more formally.

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

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.

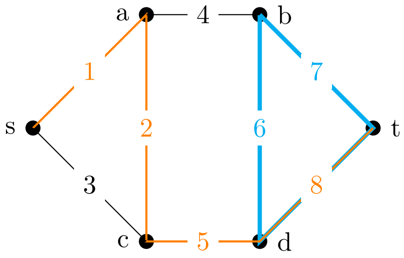


Definition. A **walk** W on graph $G = (V, E)$ from v_0 to v_n is a sequence $v_0e_1v_1e_2v_2e_3v_3 \dots v_{n-1}e_nv_n$ for $i = 1, \dots, n$ where edge e_i has endpoints v_{i-1} and v_i.

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

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

Example 7.16. We have the following graph:

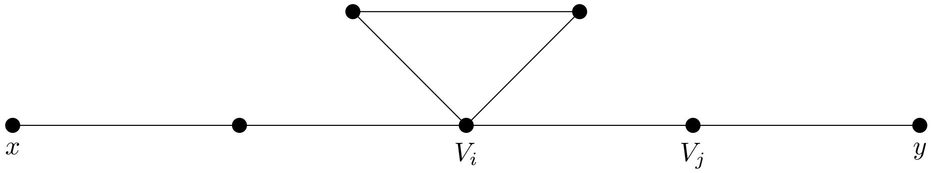


In this graph, we've visualized a path P (in orange) and a cycle C (in blue). We can express P as $P = s1a2c5d8t$ and we can express C similarly as $C = b7t8d6b$.

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. ← February 27, 2013

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:

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

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

$$\begin{aligned} W &= V_0 \dots e_i \underbrace{V_i e_{i+1} \dots e_j}_{\text{cut off}} V_j e_{j+1} \dots V_n \\ \implies W' &= V_0 \dots e_i V_j e_{j+1} \dots V_n \end{aligned}$$

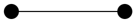
W' is still a walk from x to y. But W' has fewer edges than W, which is a contradiction. □

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.*

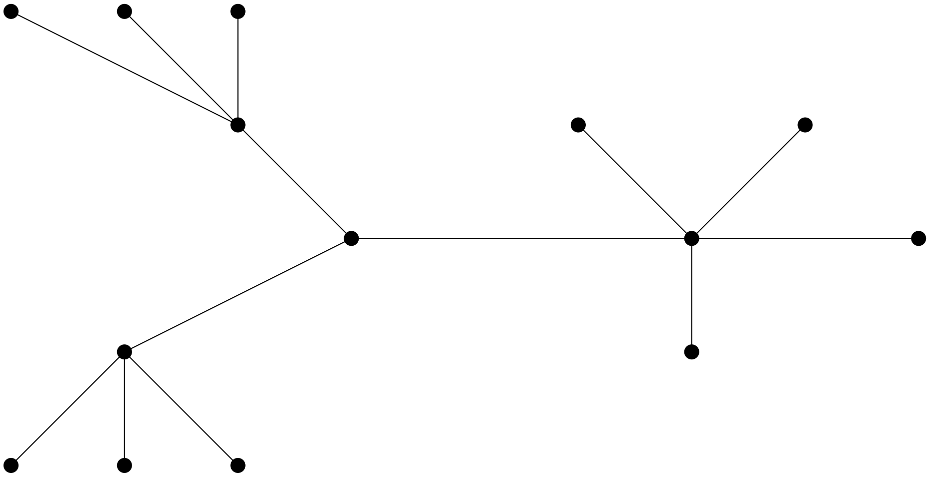
This corollary is not as trivial to show as you might initially think. You can't just join the two paths, because the two paths may share some vertices.

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. □

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:



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, pick a path P with as many edges as possible. We have:

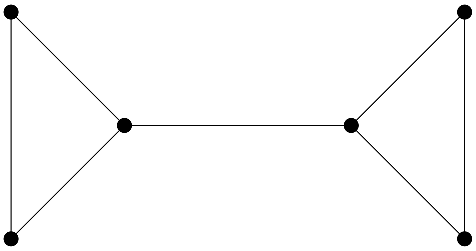
$$P = V_0 e_1 V_1 e_2 \dots e_n V_n$$

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 $i \in \{0, \dots, n-2\}$. Then we have the cycle C:

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

□

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



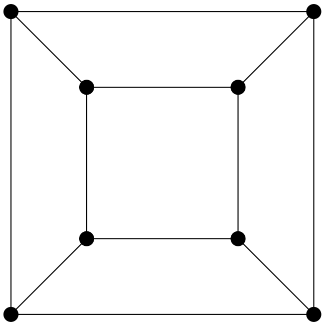
Definition. The **girth** of a graph G, denoted $g(G)$, is the length of the shortest cycle in G. If G has no cycles, then $g(G)$ is infinite.

7.4.1 Hamiltonian Cycles

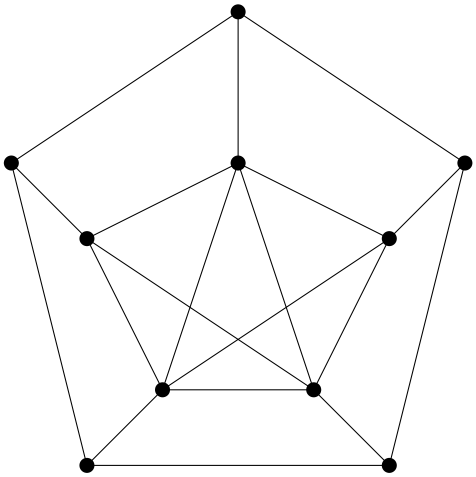
Definition. A cycle is **Hamiltonian** if every vertex is in the cycle.

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:



Example 7.19. Here's another example of a graph with a Hamiltonian cycle.



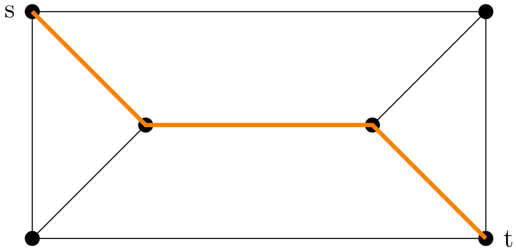
Do we always have a Hamiltonian cycle? No, not necessarily.

Theorem (Dirac's Theorem)**.** *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

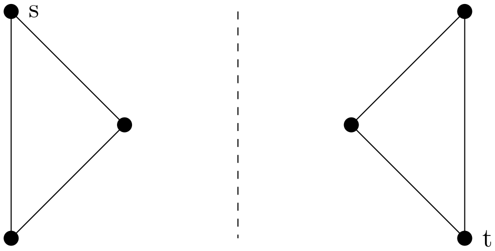
← March 1, 2013

Example 7.20. Given the following graph:



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

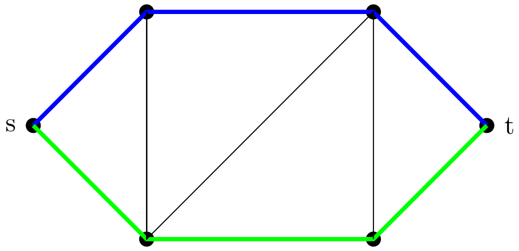
Example 7.21. Given the following graph:



Is there a path from s to t? No. The two sets of vertices have no edges between them.

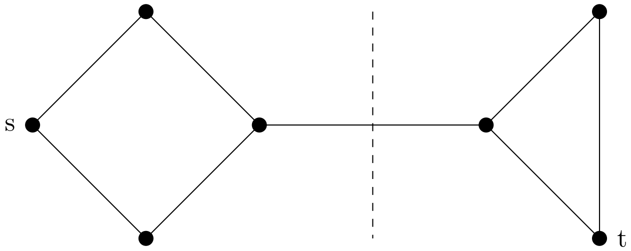
Definition. A pair of paths is **edge disjoint** if the paths do not share an edge.

Example 7.22. Given the following graph:



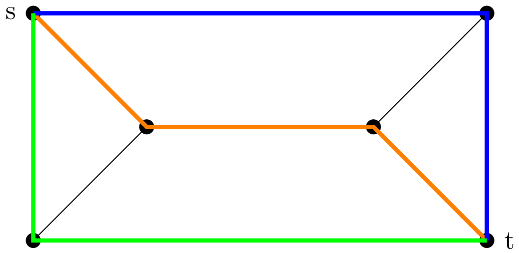
Are there two edge disjoint paths from s to t? Yes. There is no edge that is both blue and green, so the two paths are disjoint.

Example 7.23. Given the following graph:



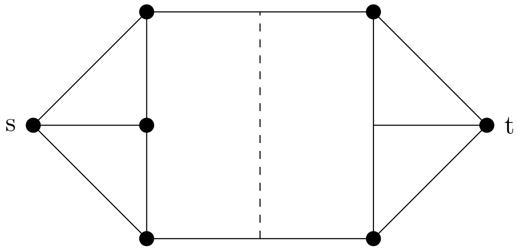
Are there two edge disjoint paths from s to t? No. For the same reason as the two examples above, the center edge must be used in all paths because it is the only edge that connects two otherwise disjoint sets of vertices.

Example 7.24. Given the following graph:



Are there three 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.

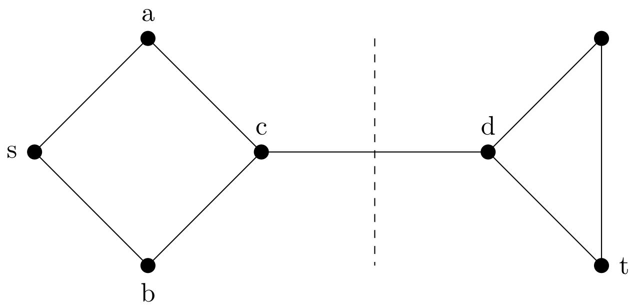
Definition. Let $G = (V, E)$, and let $S \subseteq V, S \neq \emptyset, S \neq V$ (we pick a proper subset of vertices). The **cut induced** by S is:

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

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.

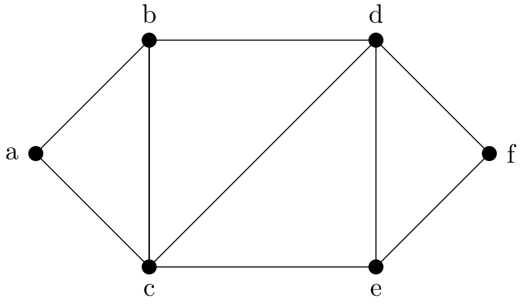
Informally, $\delta(S)$ is the set of edges between V and $V \backslash S$.

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. 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 7.25, 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 $\delta(S)$, $|\delta(S)| \geq k$.*

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

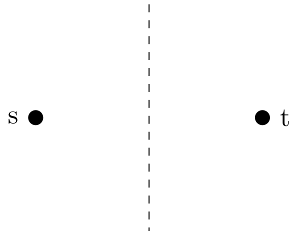
Proof. Let $\delta(S)$ be an st-cut ($s \in S, t \notin S$). Let $i \in \{1, \dots, k\}$. Follow P_i from s to t. Let v_i be the last vertex in S of P_i, and let w_i be the first vertex *not* in S of P_i. Then $e_i = v_i w_i$ is an edge of P_i and $e_i \in \delta(S)$. This implies $\{e_1, e_2, \dots,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

Since $P_1, P_2, \dots, P_k$ are edge disjoint, $e_1, e_2, \dots, e_k$ 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. □

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 $P_1, \dots, P_k$ 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:



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.

□

← March 4, 2013

Corollary. *There exists a path from s to t (1) if and only if for all $S \subseteq V, s \in S, \delta(S) \neq \emptyset$ (2).*

Proof. Let us prove that (2) implies (1).

Let $U = \{s\} \cup \{v | \exists$ a path from s to $v\}$. If $t \in U$, we're done.

Let's assume $t \notin U$. By (2), there exists $ab \in \delta(v)$, say $a \in U, b \notin U$. That is, we have at least one edge leaving U.

Informally, we know we have a path from s to a. We can take that path and add the edge ab to get us a path from s to b. However, then b should be in U as well, because there exists a path from s to b.

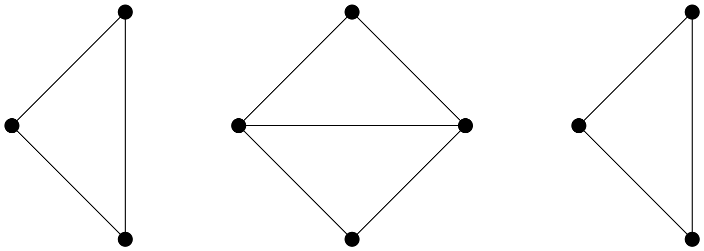
Formally, since $a \in U$, there exists a path P_a from s to a. Construct a path P_b by adding edge ab at the end of P_a. This implies that $b \in U$, which is a contradiction. □

7.5.2 Connectedness, Subgraphs, and Components

Definition. A graph is **connected** if there exists a path between any pair of vertices. If a graph is not connected, it is **disconnected**.

Example 7.28. This graph is disconnected:

Example 7.29. This graph (considered as a whole) is disconnected:

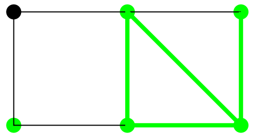


This corollary follows immediately from our characterization of *st*-cuts:

Corollary. *G is connected (1) if and only if for all $X \subseteq V, X \neq \emptyset, X \neq V, \delta(X) \neq \emptyset$ (2).*

Definition. $H = (V_H, E_H)$ is a **subgraph** of $G = (V_G, E_G)$ if $V_H \subseteq V_G$ and $E_H \subseteq E_G$.

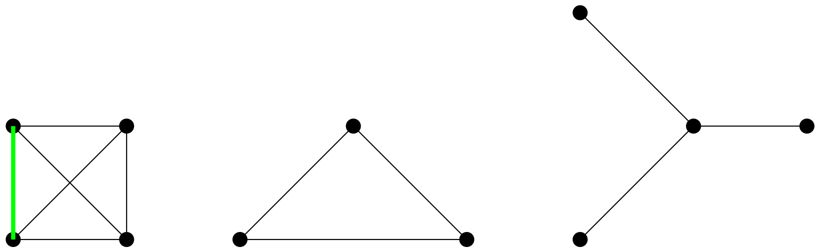
Example 7.30. The highlighted portion of this graph is a subgraph:



Note that in order to keep an edge in a subgraph, we must keep both of its vertices. When we discard a vertex, we must discard all edges that have that vertex as an endpoint.

Definition. A **component** of a graph is a maximal connected subgraph H of G. That is, H is connected and no subgraph of G that properly contains H is connected.

Example 7.31. Given the following graph G (considered as a whole):



Each of these three obviously-disjoint subgraphs are components. The highlighted portion is not itself a component (as expected), because it is not a maximal subgraph.

Corollary. *G is connected if and only if G has a single component.*

7.5.3 Equivalence Relations

Definition. $\sim$ is an **equivalence relation** for S (an infinite set) if all of the following hold:

1. For all $a \in S$, $a \sim a$ (reflexivity).
2. For all $a, b \in S$, $a \sim b \implies b \sim a$ (symmetry).
3. For all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$ (transitivity).

Example 7.32. Let S be the set of all integers. Pick some integer $m \geq 1$. A sample equivalence relation would be $a \sim b$ if $a - b$ is a multiple of m.

You can always partition your set S into **equivalence classes**.

Example 7.33. Let $G = (V, E)$ be a graph. Given $a, b \in V$, $a \sim b$ if $a = b$ or there exists a path from a to b. We propose that $\sim$ is an equivalence relation, and we want to prove it.

Proof. We have to prove all three parts of the definition of equivalence relations.

(1) is true by definition.

(2) is true because if there exists a path from a to b, then there exists a path from b to a.

(3) is true because if there exists a path from a to b and there exists a path from b to c, then there exists a path from a to c (by theorem).

Therefore, we have shown that $\sim$ is indeed an equivalence relation. □

Question: what do the equivalence classes correspond to? Any two vertices with one component should have a path *and* one vertex from a component and one vertex from another component should *not* have a path between them. The equivalence classes correspond to the vertices of each of the components of G.

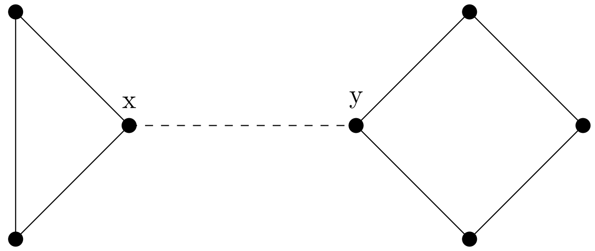
Exercise: look at set S (the set of all possible graphs). We propose that $G \sim H$ if G is isomorphic to H. Prove that $\sim$ is an equivalence relation.

Remark: it's useful to think of paths and cycles as sets of edges. Reflexivity makes a lot more sense under this interpretation, for instance. Cycles become a set of edges of a connected subgraph where every vertex has degree two. Paths are edges of a connected subgraph where two vertices have degree one and every other vertex degree two.

7.5.4 Bridges

Definition. Let $G = (V, E)$ be a graph, and $e \in E$. Then, $G \backslash e$ is the graph obtained from G by deleting edge e. We say e is a **bridge** of G if $G \backslash e$ has more components than G.

Example 7.34. Given the following graph:



The edge xy is a bridge, because if it was removed the number of components will increase from one to two. If this edge was removed, x and y would be in different components. This can be proven by transitivity.

← March 6, 2013

Proposition. *If $e = xy$ is a bridge of G, then x and y are in distinct components of $G \backslash e$.*

Proof. There exists ab such that a and b are in the same component of G, but a and b are in distinct components of $G \backslash e$. This implies that there exists a path P in G between a and b that uses e.

Suppose for a contradiction that x and y are in the same component of $G \backslash e$. We know:

- a and x are in the same component of $G \backslash e$ (because of P).
- b and y are in the same component of $G \backslash e$ (because of P).

By transitivity, a and b must be in the same component, which is a contradiction. □

Proposition. *Let $G = (V, E)$ be a connected graph, and let e be a bridge of G. Then $G \backslash e$ has exactly two components.*

Proof. Let X be the vertices in the component of $G \backslash e$ that contains x. Let $Y = V \backslash X$. We need to show that any two vertices in Y are connected by a path in $G \backslash e$.

Let $a, b \in Y$. Since G is connected, there exists a path P_a between a and x in G, and there exists a path P_b between b and x in G. Moreover, P_a and P_b both use the edge e. This implies:

- a and y are in the same component of $G \backslash e$.
- b and y are in the same component of $G \backslash e$.

By transitivity, a and b are in the same component of $G \backslash e$. □

Note that we didn't just prove that there exists a path from a and b to y because we wanted to ensure that the path did not use the edge e.

Proposition. *Let $G = (V, E)$ be a graph, and $e \in E$. e is* not *a bridge (1) if and only if e is in a cycle (2).*

In fact, this is the only reason you wouldn't have a bridge.

Proof. Assume $e = xy$. We'll start by proving that (1) implies (2).

The fact that $e = xy$ is not a bridge implies that there exists a path P between x and y in $G\backslash e$. Then, $P \cup \{e\}$ is a cycle.

Now, we'll prove (2) implies (1).

If e is in a cycle C, then $C\backslash e$ is a path between x and y. This implies that e is not a bridge, otherwise x and y are in distinct components of $G\backslash e$, as proven earlier. □

Proposition. *Let $G = (V, E)$ be a graph. Let $a, b \in V$ (where $a \neq b$). Suppose there exists paths P_1, P_2 between a and b where P_1 and P_2 are distinct. Then G has a cycle.*

We want to show that there is a cycle that uses the edge e. So, we need to show that there exists a path from x to y that does not use the edge e.

Proof. Since P_1 is distinct from P_2, there exists an edge $e = xy$ in P_2 that is not in P_1. After possibly interchanging a and b, we know:

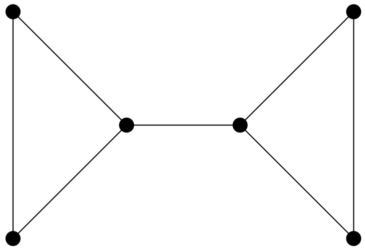
- a and x are in the same component of $G\backslash e$ (because of P_2).
- y and b are in the same component of $G\backslash e$ (because of P_2).
- a and b are in the same component of $G\backslash e$ (because of P_1).

Using those facts, by transitivity we know there exists a path P between x and y in $G\backslash e$. Then $P \cup \{e\}$ is a cycle. □

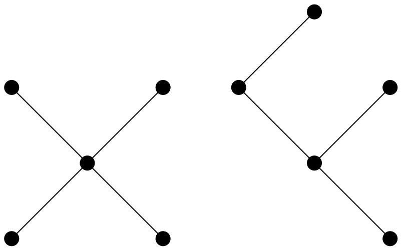
8 Trees

Definition. A graph G is a **tree** if G is connected and G has no cycle.

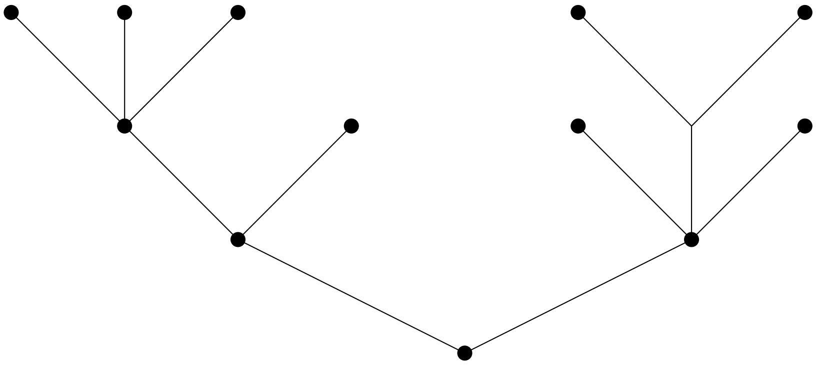
Example 8.1. This graph is not a tree because it contains cycles:



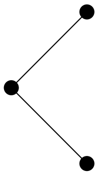
Example 8.2. This graph (considered as a whole) is not a tree because it is disconnected:



Example 8.3. This graph is a tree because it is connected and has no cycles:



Example 8.4. This graph is also a tree:



Example 8.5. This is the simplest graph that is a tree:

Keep this graph (just one vertex with no edges) in mind when doing inductive proofs involving trees.

← March 8, 2013

Proposition. *If G is a tree, then:*

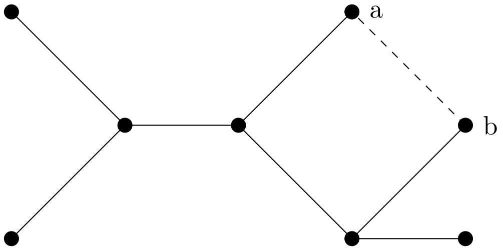
1. *Any two distinct vertices are joined by a unique path.*
2. *Every edge is a bridge.*

Proof. We will prove each part of this proposition in turn.

1. Since the tree is connected, there exists at least one path. If there exists two distinct paths between a pair of vertices, then there exists a cycle, which is a contradiction.
2. If an edge is not a bridge, then that edge is in a cycle, which is a contradiction. □

Proposition. *Let $H = (V, E)$ be a tree. Let $a, b \in V$ be two distinct vertices with no edge between them. Let G be the graph obtained from H by adding the edge ab. Then G has exactly one cycle.*

Example 8.6. Let's add the edge ab to the following tree:



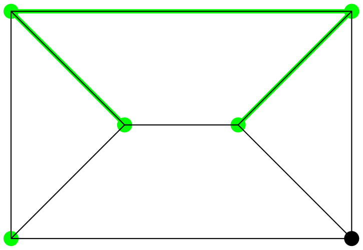
According to the previous proposition, this graph should contain only one cycle.

Proof. C is a cycle of G if and only if $C\backslash\{e\}$ is a path of H between a and b. We know that there exists a unique such path. □

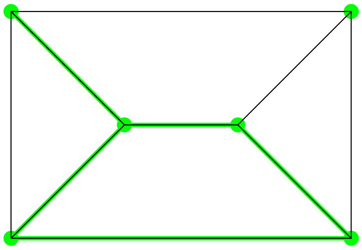
You could add an edge to create a cycle, then remove *any* edge from within the cycle to get a different tree. This technique could be used by shipping companies to find the most optimal cost-efficient route to ship a package.

Definition. Let $G' = (V', E')$ be a subgraph of $G = (V, E)$. G' is a **spanning subgraph** if $V' = V$.

Example 8.7. This is not a spanning subgraph because one vertex in V is not included in V':

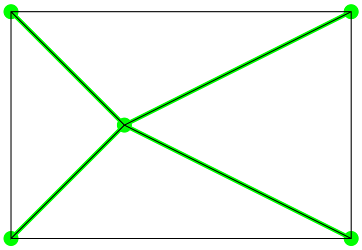


Example 8.8. This is a spanning subgraph because $V' = V$:

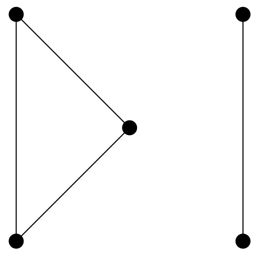


Proposition. *Let $G = (V, E)$ be a graph. G is connected (1) if and only if G contains a spanning tree (2).*

Example 8.9. This is a graph that is connected. Its spanning tree is highlighted:



Example 8.10. We have to specify that G contains a *spanning* tree because otherwise we would say the following graph (considered as a whole) is connected (which it is not):



Proof. We'll first prove that (2) implies (1). For all $a, b \in V$ ($a \neq b$), there exists a path between a and b in the spanning tree. But this is also a path of G.

Now, we'll prove that (1) implies (2). Among all spanning subgraphs of G that are connected, pick one with as few edges as possible. Call that subgraph T.

We claim that T is a tree. We need to verify that.

- T is clearly connected.
- T does not contain a cycle, otherwise any edge on that cycle could be removed while still keeping the graph connected (edges in cycles are not bridges).

□

Let n be the number of vertices in a graph G. If $n = 1$, we must have zero edges. If $n = 2$, we must have one edge. If $n = 3$, we must have two edges. If $n = 4$, we must have three edges. If $n = 5$, we must have four edges. Let's generalize this.

Proposition. *In a tree, the number of edges is equal to the number of vertices minus one.*

In order to prove this with induction, we want to start with the larger graph to see how we built it up. We can't do induction the normal way initially with graphs in general because of how graphs can be constructed (there are multiple graphs we can form where $n = 5$ from a graph where $n = 4$).

Proof. Let $G = (V, E)$ be a tree. By induction on $|V|$:

Base case: $|V| = 1, |E| = 0$.

Assume $|V| \geq 2$. We claim that there exists a vertex v of degree 1 (otherwise there exists a cycle). So, v is adjacent to a unique vertex w.

Let $G' = (V', E')$ be the graph obtained from G by deleting the edge wv and the vertex v. Note that G' is a tree because the degree of v is one in G.

By induction, $|E'| = |V'| - 1$. We know that $|E| = |E'| + 1$ and $|V| = |V'| + 1$, which gives us $|E| = |V| - 1$, as required. □

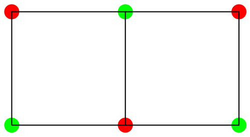
If you're ever asked to determine a result involving the number of edges in a tree, you'll likely use this proposition.

8.1 More on Bipartite Graphs

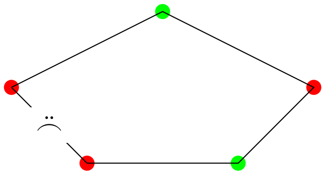
Proposition. *If a graph has a cycle with an odd number of edges, then it is not bipartite.*

← March 11, 2013

This graph is bipartite:



But this one is not:



Proof. Let $C = V_1, V_2, \ldots, V_{2n}$, where $V_1 = V_{2n}$.

Suppose there exists partition X, Y. We may assume $V_1 \in X, V_2 \in Y, V_3 \in X, \ldots$. This implies that $V_{2n} \in Y$ since all vertices with even indices are members of Y.

Notice that $V_1 \in X$ and $V_{2n} \in Y$, but $V_1 = V_{2n}$. This is a contradiction. □

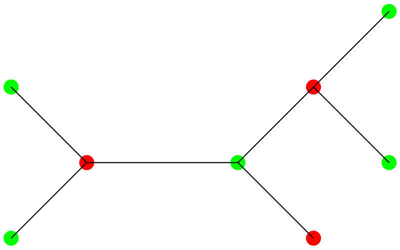
We want to show that this is the *only* reason why a graph would not be bipartite.

Proposition. *A graph is bipartite if and only if all its components are bipartite.*

The proof of this proposition is left as an exercise.

Proposition. *Trees are bipartite.*

For example, this tree is bipartite:



There are a couple of different proof techniques we could use to prove this proposition.

1. We could call one vertex V_1 and then define even/odd vertices based on whether their distance from V_1 is even or odd (since there exists a unique path from V_1 to any other vertex in a tree).
2. More simplistically, we could build up the partition recursively. As we add an additional edge, each endpoint of the edge should be in the opposite partition.

We'll use approach (2) to prove this proposition.

Proof. Let $T = (V, E)$. We're going to perform induction on $|V|$.

Base case: $|V| = 1$, i.e. $V = \{v\}$, set $X = \{v\}, Y = \emptyset$.

Otherwise, $|V| \geq 2$. Since T is a tree, there exists vertex u of degree 1. Then, u is adjacent to a unique vertex w.

Let T' be obtained by removing uv and u. Note that T' is still a tree. We can verify that fact by seeing that we're certainly not adding any cycles (not possible when removing an edge) and since u has degree 1, the tree remains connected.

By induction, there exists a partition X', Y' of the vertices of T' such that every edge of T' has one end in X' and one end in Y'.

If $w \in X'$ then $X = X'$ and $Y = Y' \cup \{u\}$. Otherwise (if $w \in Y'$), $X = X' \cup \{u\}$ and $Y = Y'$. □

Theorem. *$G = (V, E)$ is bipartite (1) if and only if G has no odd cycles (2).*

Proof. We proved NOT (2) implies NOT (1), which is equivalent to proving (1) implies (2). Now, we'll prove the other direction: (2) implies (1).

Due to the proposition from earlier, we may assume G is connected, without loss of generality. This implies that G contains a spanning tree $T = (V, E')$.

We showed that T is bipartite. Let X, Y be the corresponding partition of V.

Claim: for all $ab \in E$, $a \in X$ and $b \in Y$, or vice versa ($a \in Y, b \in X$). We may assume $ab \in E \backslash E'$.

Let P be the unique path in T between a and b. Suppose $a, b \in X$ (or $a, b \in Y$). Then P has an even number of edges.

This implies that the cycle $P \cup \{ab\}$ is an odd cycle, which is a contradiction. □

8.2 Graph Colouring

Problem 8.1. Assign colours to vertices such that every edge has endpoints of different colours. The goal is to use as few colours as possible.

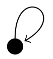
What graphs can be coloured with two colours? Easy: bipartite graphs.

What graphs can be coloured with three colours? No clue. There's no efficient or reliable way of colouring an arbitrary graph with any constant (even very large) number of colours.

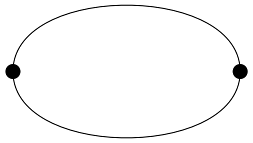
9 Planar Graphs

We will allow:

- Loops:

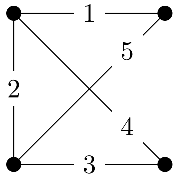


- Parallel edges:

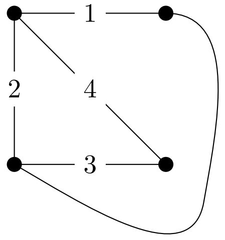


Definition. A **planar embedding** is a drawing of a graph where no two edges cross.

Example 9.1. This is not a planar embedding of a graph G because two edges cross:

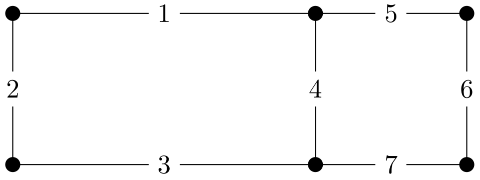


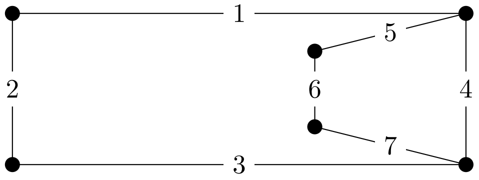
This is a planar embedding for the same graph:



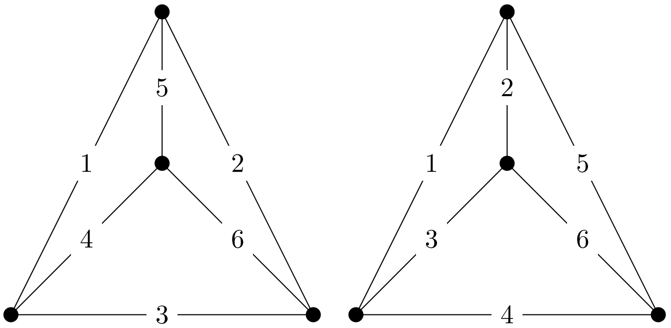
Observation: the same graph can have many different planar embeddings. We'll formally define "different" a bit later.

Example 9.2. Here are two planar embeddings of the same graph G_1:



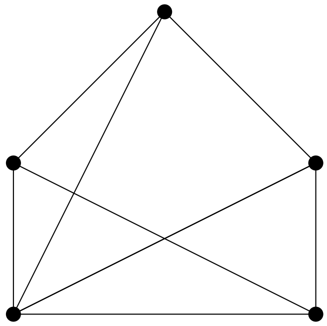


Example 9.3. Here are two planar embeddings of the same graph G_2 that look similar, except the edges are labeled differently:



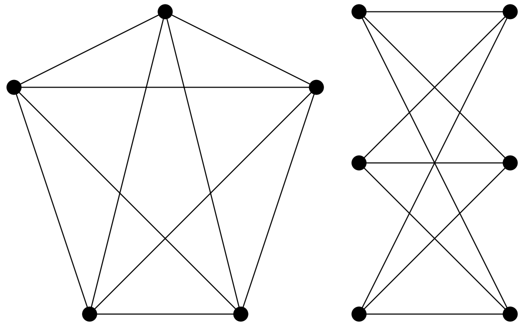
Definition. A graph is **planar** if there exists a planar embedding.

Example 9.4. This graph is planar:



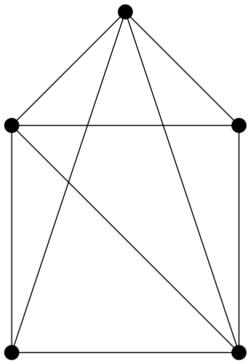
It is possible to find a planar embedding for this graph.

Example 9.5. These two graphs are not planar:

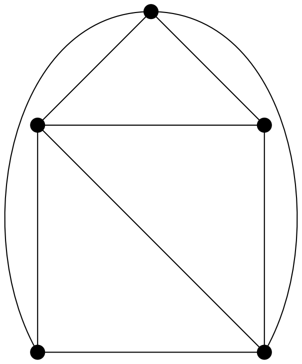


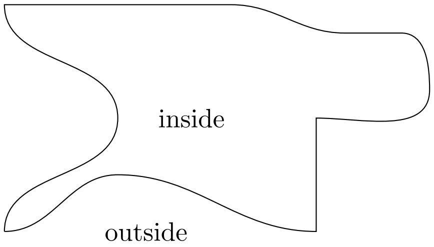
← March 13, 2013

This is a planar graph G:

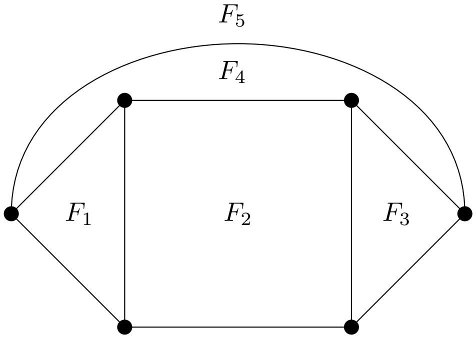


G is a planar graph because a planar embedding exists for G. In particular, the following is one planar embedding of G (no two edges cross):

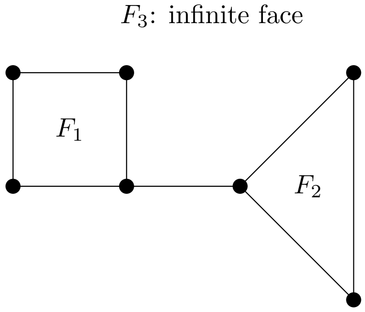




Theorem (Jordan Curve Theorem)**.** *A closed, continuous, non-self-crossing curve on the plane partitions the plane into two connected components.*



Definition. The Jordan Curve Theorem implies that a planar embedding partitions the plane into connected components, called **faces**.

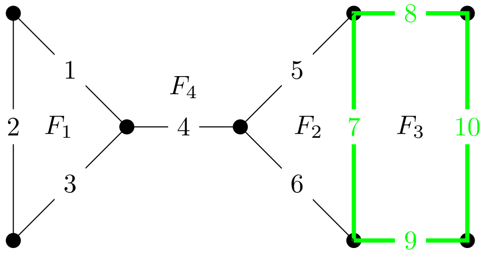


Theorem. *G has an embedding on the plane if and only if G has an embedding on the sphere.*

The truthfulness of this theorem is easy to see. To show an embedding on a plane implies an embedding on the sphere, place your plane flat on the ground, then it's a plane on a sphere (Earth). For the opposite direction, just imagine a sphere so huge that the entire graph appears on a portion of the sphere that appears like a flat plane.

Definition. For any face F, the **boundary walk** of F is the closed walk obtained by following the edges bounding the face.

Suppose we have this graph G:



In G, we have the following boundary walks:

$F_1 : 1, 3, 2$

$F_2 : 5, 7, 6$

$F_3 : 8, 10, 9, 7$ (in green above)

$F_4 : 1, 4, 5, 8, 10, 9, 6, 4, 3, 2$

Note that in the boundary walk for F_4, the edge 4 appears twice. This is acceptable under the usual definition of walks.

Definition. For a face F, $\deg(F)$ is equal to the number of edges in the boundary walk of F.

For example, we have $\deg(F_1) = 3, \deg(F_2) = 3, \deg(F_3) = 4$, and $\deg(F_4) = 10$. Note that in $\deg(F_4)$, we must count the edge "4" twice.

Notice:

$$\begin{aligned}\sum_{i=1}^{4} \deg(F_i) &= \deg(F_1) + \deg(F_2) + \deg(F_3) + \deg(F_4) \\ &= 20 \\ &= 2 \times \text{ number of edges}\end{aligned}$$

This is similar to a theorem proven when we talked about degrees under the earlier definition for degrees. That's why we defined the degree of a face in the way we did.

Theorem. *Consider a planar embedding of $G = (V, E)$. Then $(\star) = \sum_{F \in faces} \deg(F) = 2|E|$.*

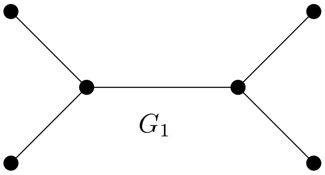
Why is this true? Each edge contributes to two faces, except edge "4" which is only in the boundary walk of F_4. However, edge "4" occurs twice in that boundary walk so it's still counted twice. We'll state this proof more formally now.

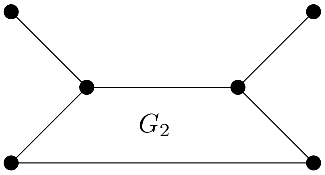
Proof. We want to show that every edge e is counted twice in $(\star)$. There are two cases.

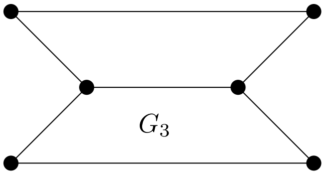
Case 1: suppose e is not a bridge. Then e appears in exactly two different faces.

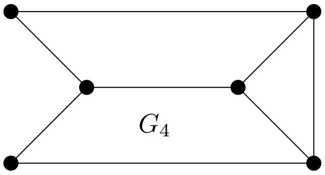
Case 2: suppose e is a bridge. Then e appears in one face but twice in the boundary walk for that face. □

Let p be the number of vertices, q be the number of edges, and f be the number of faces. Here are G_1, G_2, G_3, and G_4:









In G_1, we have $p = 6, q = 5$, and $f = 1$. In G_2, we have $p = 6, q = 6$, and $f = 2$. In G_3, we have $p = 6, q = 7$, and $f = 3$. In G_4, we have $p = 6, q = 8$, and $f = 4$.

G_1 is a spanning tree, so we have $p = q + 1$. This implies that $p - q + f = 2$.

Theorem (Euler's Formula)**.** *For any connected planar embedding of a graph $G = (V, E)$, we have $p - q + f = 2$, where p is the number of vertices, q is the number of edges, and f is the number of faces.*

Proof. We'll prove this theorem by performing induction on q.

Base case: G is a tree. This implies that $q = p - 1$, as proven previously. Since G is a tree, $f = 1$. So, we have $p - q + f = 2$.

Otherwise, let $e \in E$ be an edge in a cycle (we can assume this because we aren't in our base case). Let $G' = G \backslash e$.

Note G' has a planar embedding obtained by erasing edge e. G' is connected because e is not a bridge of G.

By induction, $p' - q' + f' = 2$, where p' is the number of vertices of G', q' is the number of edges of G', and f' is the number of faces in the embedding of G'.

We know that $p' = p$ and $q' = (q - 1)$, but we need to show that $f' = (f - 1)$. $f' = (f - 1)$ follows from the Jordan Curve Theorem, because by adding another edge we're adding an additional boundary which creates a new face. □

← March 15, 2013

Definition. A graph is **simple** if it has no parallel edges and it has no loops. A graph that is not simple is called a **multigraph**.

Proposition. *Let G be a simple planar graph. Then:*

1. $q \leq 3p - 6$.
2. $q \leq 2p - 4$ *when G has no triangle (no cycle of length 3).*

Proof. We'll prove each part of this proposition in turn.

1. The fact that G is planar implies that there exists a planar embedding with f faces. Since the graph is simple, every face F must have $\deg(F) \geq 3$. So, we know:

$$\begin{aligned} 2q &= \sum_{F \in \text{faces}} \underbrace{\deg(F)}_{\geq 3} \\ \implies 2q &\geq 3f \\ &\geq 3(2 - p + q) \\ &\geq 6 - 3p + 3q \\ \implies 6 - 3p + q &\leq 0 \end{aligned}$$

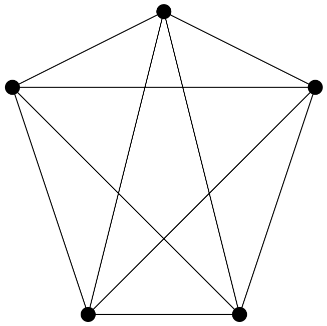
Euler's formula can be used as a general trick when we want to compare two of these quantities.

2. Now, let's also exclude triangles (cycles of length 3). We have:

$$\begin{aligned} 2q &= \sum_{F \in \text{faces}} \underbrace{\deg(F)}_{\geq 4} \\ \implies 2q &\geq 4f \\ &\geq 4(2 - p + q) \\ &\geq 8 - 4p + 4q \\ \implies q &\leq 2p - 4 \end{aligned}$$

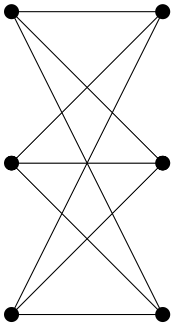
□

Let K_n denote the complete graph with n vertices. Is K_5 planar?



Well, how many edges can a planar graph with 5 vertices have? Note that # of edges $\leq 3 \times 5 - 6 = 9$. But K_5 has $\binom{5}{2} = 10$ edges. So, no, K_5 is not planar.

Let $K_{m,n}$ denote the complete bipartite graph with m vertices and n vertices in each part of the partition. Is $K_{3,3}$ planar?



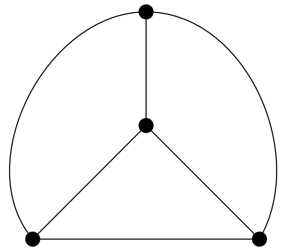
We have $9 \leq 3 \times 6 - 6$, which does not yield a contradiction. However, $K_{3,3}$ is bipartite, so we know there's no cycle of length 3. Applying (2), we get $9 \leq 2 \times 6 - 4 \not\leq 8$, which is a contradiction. Therefore, $K_{3,3}$ is not planar.

9.1 Platonic Graphs

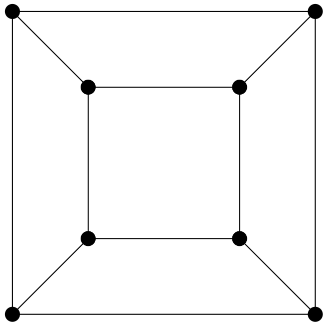
Definition. A graph is **platonic** if it has a planar embedding such that every face has degree $l \geq 3$ and every vertex has degree $k \geq 3$.

Theorem. *There exist only five platonic graphs.*

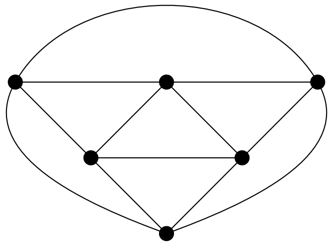
The platonic graph where $k = 3, l = 3$ is:



The platonic graph where $k = 3, l = 4$ is:



The platonic graph where $k = 4, l = 3$ is:



There are also two more graphs ($k = 3, l = 5$ and $k = 5, l = 3$), which we won't show here for simplicity.

9.2 Review of Planar Graphs

← March 18, 2013

- $\deg(f)$ is the length of the boundary walk about the face f.
- Handshake Lemma:
$$\sum_{v \in V} \deg(v) = 2q$$
- Dual Handshake Lemma:
$$\sum_{f \in \text{faces}} \deg(f) = 2q$$
- Euler's Formula:
$$p - q + s = 1 + c$$
(where p is the number of vertices, q is the number of edges, s is the number of faces (earlier, we denoted this as f), and c is the number of components.)

9.3 Planar Solids

There are solids that correspond to the five platonic graphs. What do they have in common? Every vertex has the same degree *and* every face has the same degree.

We'll now finally define platonic graphs formally.

Definition. A **platonic graph** is a graph such that there are integers $k, l \geq 3$ such that every vertex has degree k and every face has degree l.

Does the data of (k, l) determine the graph? Yes! When drawing these graphs, they are unique because there are no ambiguous decisions to be made.

Which values of (k, l) are possible? If we try drawing the graphs for $(4, 4)$ and $(5, 4)$, we'll see that as we're constructing them, they'd each need to be infinite in size to satisfy the k and l constraints. Since these graphs cannot be finite, we say $(4, 4)$ and $(5, 4)$ are two particular instances of (k, l) for which the constraints are not satisfied.

Idea: use the facts about planar graphs to constrain (k, l).

- By the handshake lemma, $\sum \deg(v) = kp = 2q$.
- By the dual handshake lemma, $\sum \deg(f) = ls = 2q$. This implies that $p = \frac{2q}{k} = s = \frac{2q}{l}$. This is known as the duality of graphs.
- By Euler's formula, $p - q + s = 2$.

This gives us:

$$\begin{aligned}
\frac{2q}{k} - q + \frac{2q}{l} &= 2 > 0 \\
\frac{2}{k} - 1 + \frac{2}{l} &= \frac{2}{q} > 0 \\
\frac{2}{k} + \frac{2}{l} &> 1 \\
2l + 2k &> kl \\
kl - 2k - 2l &< 0 \\
kl - 2k - 2l + 4 - 4 &< 0 \\
(k-2)(l-2) &< 4
\end{aligned}$$

So, we know that $k \geq 3$ and $l \geq 3$. This gives us:

$$\begin{aligned}
&(k-2)(l-2) < 4 \\
\implies &k-2, l-2 \geq 1 \text{ and } k-2, l-2 < 4 \\
\implies &k, l \leq 5
\end{aligned}$$

All of this gives us:

- If $k = 3$, then l can be 3, 4, or 5.
- If $k = 4$, then l can only be 3.

- If $k = 5$, then l can only be 3.

Theorem. *If G is a platonic graph, then (k, l) must be one of (3, 3), (3, 4), (3, 5), (4, 3), or (5, 3).*

Does each of these possibilities of (k, l) occur for a platonic graph? That is, we know these are all *possibilities*, but are they all *actually* possible? For any choice of (k, l), how many platonic graphs are there?

Claim: each of the five possibilities for (k, l) can be achieved by a platonic graph.

Proof. Just use the five platonic solids that we know.

- (3, 3): tetrahedron.
- (3, 4): cube.
- (3, 5): dodecahedron.
- (4, 3): octahedron.
- (5, 3): icosahedron. □

Claim: the only platonic graphs are the five coming from platonic solids.

Proof. Just try to draw six platonic graphs. As you keep drawing, the graph will be uniquely determined. □

How many faces, edges, and vertices does each have?

$$\begin{aligned} q\left(\frac{2}{k} + \frac{2}{l} + 1\right) &= 2 \\ p &= \frac{2q}{k} \\ s &= \frac{2q}{l} \end{aligned}$$

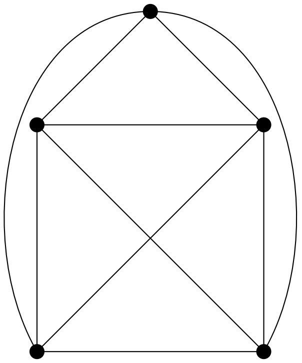
$$\begin{aligned} \implies q &= \frac{2}{\frac{2}{k} + \frac{2}{l} - 1} \\ &= \frac{2kl}{2l + 2k - kl} \end{aligned}$$

$$\begin{aligned} \implies s &= \frac{2q}{l} \\ &= \frac{4k}{2l + 2k - kl} \end{aligned}$$

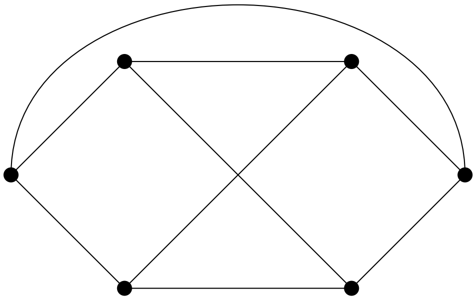
We can verify this. If $(k, l) = (3, 5)$, then $s = \frac{12}{10+6-15} = 12$, as expected.

9.4 Non-Planar Graphs

← March 20, 2013



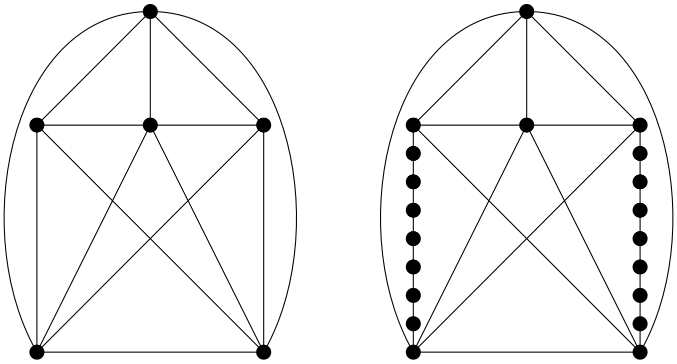
K_5



$K_{3,3}$

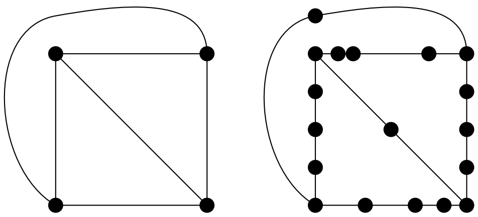
K_5 and $K_{3,3}$ are non-planar because they have edges that unavoidably must cross. Are there any other planar graphs? Yes! You can just add more edges to K_5 or $K_{3,3}$. We could also add some vertices in the middle or edges, if we'd like.

The two following graphs are also non-planar, and are built by adding more edges and vertices to K_5.

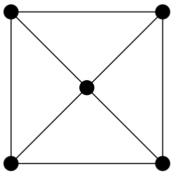


Definition. A graph H is a **subdivision** of a graph G if H is obtained from G by replacing each edge by a path.

Example 9.6. Here's a graph G and a subdivision of G.

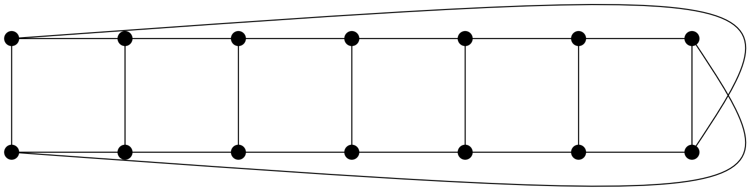


In addition, the following is *not* a subdivision of G because a vertex was introduced where there was previously a crossing:



Theorem. *If G has a subgraph that is a subdivision of K_5 or $K_{3,3}$, then G is not planar.*

Example 9.7. Consider the following graph, G.



Katz claims he has a bridge in New York and some cheap land in Florida to sell you, and he claims he has a planar embedding for G. Why must he be lying?

Essentially, we know he's lying about having a planar embedding for G, since then he could erase subdivisions and get a planar embedding for $K_{3,3}$. Let's state that more formally.

Proof. Suppose G is planar. Then, take a planar embedding of G. Since H is a subgraph of G, we get a planar embedding of H. Undo that subdivision. Then we get a planar embedding of $K_{3,3}$ or K_5, and that's "unpossible." □

9.5 Kuratowski's Theorem

Theorem (Kuratowski's Theorem)**.** *A graph G is non-planar if and only if it contains a subdivision of $K_{3,3}$ or K_5.*

Definition. The **crossing number** of a graph G is the minimum number of crossings in drawings of G.

That is, there may be some ways to draw non-planar graphs that are smarter than other ways. Smarter ways involve drawing the graph in such a way that the crossing number is minimized.

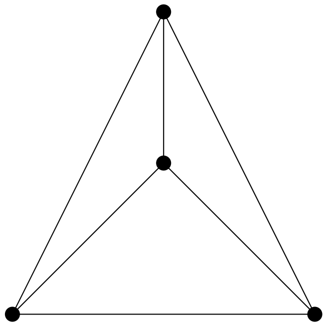
Observation: a graph is planar if and only if it has crossing number zero.

It's generally hard to compute crossing numbers. It's an open question to d the crossing number of $K_{m,n}$, since we'd have to check all possible drawings.

9.6 Graph Colouring

Definition. Let n be a positive integer. A **graph colouring** is an assignment of one of $\{1, 2, \ldots, n\}$ to each vertex such that no edge connects vertices with the same label. (In other words, no two adjacent vertices are assigned the same colour.)

Example 9.8. This is K_4:



Since every vertex of K_4 has an edge to every other vertex, every edge needs its own colour.

Note: K_n needs n colours. You must colour every vertex differently.

Note: $K_{m,n}$ needs two colours, because it's a bipartite graph.

Theorem (Four Colour Theorem)**.** *Every planar graph is 4-colourable.*

The four colour theorem is known to be true, but it's not known to be true in a nice way. The proof is basically a bunch of counterexamples. The proof also involved a computer to generate various cases. ← March 22, 2013

We only consider simple graphs when discussing graph colouring. We can't colour loops, for instance.

We can expand on the four colour theorem and also introduce two very similar theorems.

Theorem (Five Colour Theorem)**.** *Every simple planar graph can be 5-coloured.*

Theorem (Six Colour Theorem)**.** *Every simple planar graph can be 6-coloured.*

We know that simple planar graphs cannot have too many edges. This implies that there exists a vertex of low degree. We'll use this information to derive a lemma.

Theorem. *Let $G = (V, E)$ be a simple graph. There exists a vertex $v \in V$ of degree $< k$. ($k = 6$)*

Proof. Assume that for all $v \in V$, $\deg(v) \geq k$. We have:

$$2q = \sum_{v \in V} \underbrace{\deg(v)}_{\geq k} \geq pk$$

We also know that $q \leq 3p - 6$, since G is a simple planar graph. That means $2q \leq 6p - 12$. Combining these expressions, we get that $pk \leq 2q$, so $pk \leq 6p - 12$. We get a contradiction for $k \geq 6$. □

So, we can update our lemma's statement with $k = 6$.

Let's now prove the six colour theorem.

Proof. Let $G = (V, E)$ be a simple planar graph. By induction on $k = |V|$:

Base case: $|V| = 1$. You can colour this vertex any colour.

Assume for $k \geq 2$ that we can 6-colour every simple planar graph with $\leq k - 1$ vertices.

By the lemma we just introduced, there exists some $v \in V$ such that $\deg(v) \leq 5$.

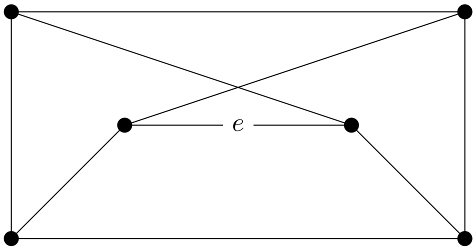
Let $H = G\backslash v$ be the graph obtained by deleting v from G. Note that H is a simple planar graph. By induction, there exists a 6-colouring of H.

Since $\deg(v) \leq 5$, one colour, say c, does not appear among the vertices adjacent to v. Pick colour c for v. □

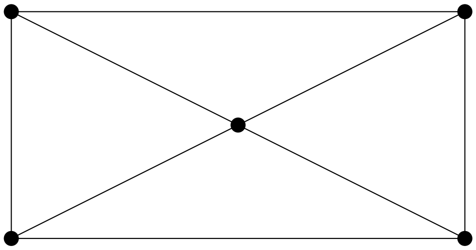
Before we can prove the five colour theorem, we need one more ingredient: contraction.

Definition. Let $G = (V, E)$ be a graph, and $e = uv \in E$. Then G/e is the graph obtained by identifying u and v in G and deleting e. We call this **contracting** the edge.

Example 9.9. Consider the following graph.

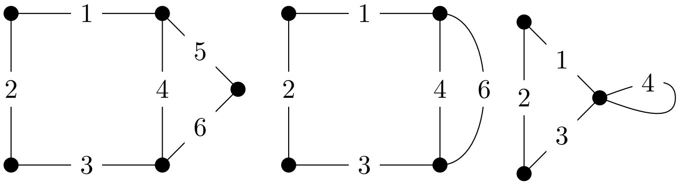


If we were to contract edge e, we would get the following graph:



When you apply contraction, you could introduce loops into the graph. Be careful.

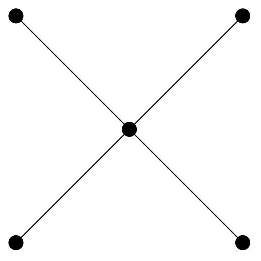
Example 9.10. We'll take a graph and then contract edge 5, then contract edge 6. Notice that this introduces a loop into the graph.



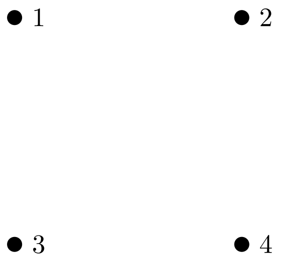
Proposition. *If G is planar, then G/e is planar.*

Our goal is to 5-colour a planar graph. We can do this by taking a graph with five vertices, removing a vertex, applying colours, then adding back the vertex that we removed.

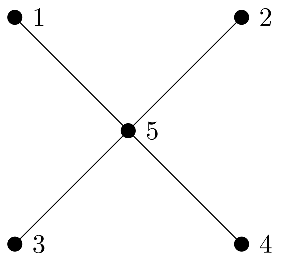
Example 9.11. We're going to 5-colour the following graph.



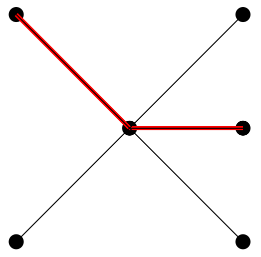
First, we'll remove the vertex in the middle and colour the remaining vertices:



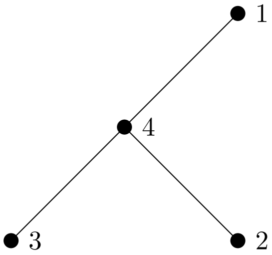
Then, we'll put the middle vertex back and give it the remaining colour:



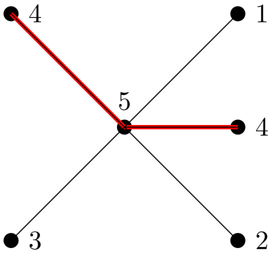
Example 9.12. Let's now look at a slightly more complex graph – a graph with six vertices.



We're going to contract the edges indicated in red, and then assign colours to the remaining vertices.



Finally, let's uncontract and assign a colour to the re-introduced vertices.



Note that in this example, it could've been possible for a loop to be created, if the two endpoints of the red path had an edge.

We know there must exist a pair of vertices that do not have an edge between them. Otherwise, we'd have K_5, but we were told the graph is planar.

Let's now prove the five colour theorem.

Proof. Let $G = (V, E)$ be a simple planar graph. By induction on $k = |V|$:

Base case: $|V| = k = 1$. You can colour this vertex any colour.

Assume for $k \geq 2$ that every simple planar graph with $\leq k - 1$ vertices is 5-colourable.

Case 1 (there exists a vertex of degree ≤ 4):

Let $H = G \backslash v$ be the graph obtained by deleting v from G. Note that H is a simple planar graph. By induction, there exists a 5-colouring of H.

Since $\deg(v) \leq 5$, one colour, say c, does not appear among the vertices adjacent to v. Pick colour c for v.

Otherwise, for all $v \in V$, $\deg(v) \geq 5$. By lemma, we have Case 2.

Case 2 (there exists $v \in V$ with $\deg(v) = 5$):

We claim that there exists $a, b \in V$, adjacent to v, such that a, b are not adjacent (otherwise, G contains K_5, so G would not be planar).

Let $H = (G/av)/vb$. Because of our claim, H has no loop. By induction, there exists a 5-colouring of H.

Extend the colouring of H to G such that vertices a, b of G are assigned the same colour as the vertex $a = b = v$ in H.

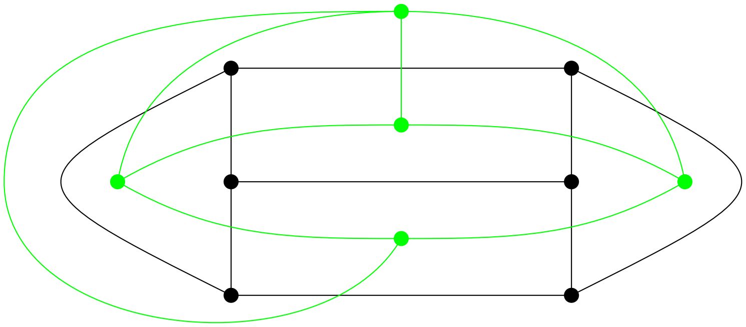
Thus, we have coloured all vertices of G except v, and the same colour appears twice among the neighbours of v. We can pick colour c, unused among the neighbours of v, to colour v. □

9.7 Dual Graphs

← March 25, 2013

Whenever you find a planar graph, you actually find two. You get two planar graphs for the price of one!

Example 9.13. Here's a planar graph, and its dual.



Here, we started with five faces, and created one new vertex per face (including the infinite face). The faces in the original planar graph correspond to vertices in the dual (indicated as the green graph, above). For each edge in the boundary walk of each face, draw an edge between the two faces. We call this second graph the dual graph.

If we had a bridge in our original graph, we could create an edge with both endpoints being the same, but the edge would have to cross the bridge visually. That is, we make an edge that is a loop.

Definition. Let $G = (V, E)$ be a graph with a planar embedding and faces $F_1, F_2, \ldots, F_f$. The **dual graph** $G^\star$ is the graph where:

- Vertices of $G^\star$ are $F_1, F_2, \ldots, F_f$.
- If e is in the boundary of F_i, F_j in G, then e is joining F_i, F_j in $G^\star$.
- If e appears twice in the boundary walk F_j in G, then e is a loop of $G^\star$ with endpoints F_j.

We're only going to define dual graphs for connected graphs, just so we don't have to worry about messy edge cases.

Remark: $G^\star$ is planar, but $G^\star$ need not be simple even if G is simple. Consider the case when G is a triangle. Then $G^\star$ is one edge connecting the face with the infinite face, as well as two additional parallel edges, which prevents $G^\star$ from being simple. Or, if G is just two vertices joined by an edge, $G^\star$ is just a single loop, which is not allowed in simple graphs.

Recall that if G has a planar embedding, then:

$$\sum_{f \in \text{faces}} \deg(f) = 2q$$

where q is the number of edges of G. We will now provide an alternate proof of this using dual graphs.

Proof. Consider the graph $G^\star$. We have:

$$\begin{aligned} 2q &= \sum_{v \in V(G^\star)} \deg(v) \text{by the handshake lemma} \\ &= \sum_{f \in \text{faces}(G)} \deg(f) \end{aligned}$$

□

Note that $G^{\star\star} = G$, as long as the graph G is connected.

How do colourings work with dual graphs? Let's look at the four colour theorem, stated in a different way.

Theorem (Four Colour Theorem – Face Version)**.** *Let G be a graph with a planar embedding. Assume G is connected and has no bridge. Then we can colour the faces of G with four colours such that any two faces sharing an edge are assigned distinct colours.*

Proof. Let $G^\star$ be the dual of G. Since G has no bridge, $G^\star$ has no loop. By the vertex version of the four colour theorem, there exists a 4-colouring of the vertices of $G^\star$, which gives a 4-colouring of the faces of G. □

That's all we're going to discuss about planar graphs.

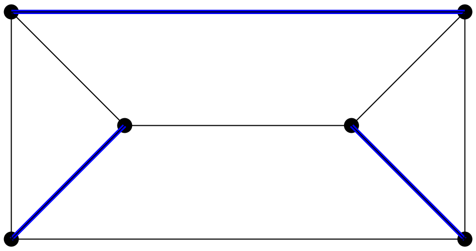
10 Matching

We will assume graphs are simple for the rest of the course.

Definition. Let $G = (V, E)$ be a graph. The **matching** M of G is a subset of the edges such that no two edges of M share an endpoint.

It's trivial to see that $\emptyset$ is a matching, as is any single edge in the graph.

Example 10.1. The highlighted edges in the following graph form a matching because no two edges share a vertex.



Our goal for the remainder of the course: we want to find an algorithm to produce a matching with as many edges as possible. That's a tough goal, so we will restrict ourselves to finding a maximum matching in bipartite graphs only.

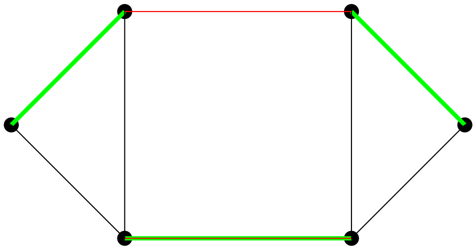
Ideally, the algorithm will be fast and easily verifiable. We need to be able to quickly produce a result, and we need to be able to easily convince someone that it is indeed a *maximum* matching.

Definition. A **maximum matching** is a matching with as many edges as possible in G.

Definition. A matching is said to be **maximal** if adding any additional edge will result in a set that is no longer a matching.

← March 27, 2013

Example 10.2. Find a maximum matching (a matching with as many edges as possible) for the following graph.



(The bottom-center edge is both green and red.)

The red edges represent a matching that is not maximum. The green edges represent a maximum matching, as required.

10.1 Application: co-op

Let A be a set of applicants, and let J be a set of jobs. For all $a \in A$ and $j \in J$, we know if applicant a is qualified for job j.

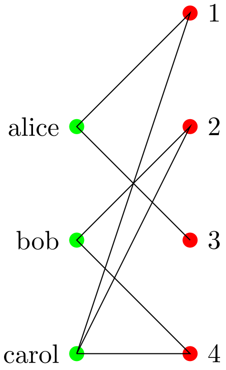
Suppose $A = \{\text{alice}, \text{bob}, \text{carol}\}$ and $J = \{1, 2, 3, 4\}$. We also have that:

- Alice is qualified for jobs 1 and 3.
- Bob is qualified for jobs 2 and 4.
- Carol is qualified for jobs 1, 2, and 4.

We want to assign applicants to jobs such that:

- No applicant is assigned two or more jobs.
- No job is assigned two or more applicants.

We want to represent this as a graph problem. Note that it's a bipartite graph, as illustrated here:



The edges represent all cases where a particular applicant is considered to be qualified for a job. The vertices are partitioned into applicants and jobs.

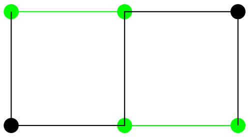
We want to assign as many applicants to jobs as possible. That's equivalent to saying we want to find a maximum matching.

10.2 Saturation

In order for us to move on, we need a few definitions.

Definition. Let G be a graph with matching M. Vertex v is **saturated** if v is the endpoint of an edge of M. Otherwise, v is said to be **unsaturated**.

Example 10.3. Consider the following matching M, illustrated as green edges:

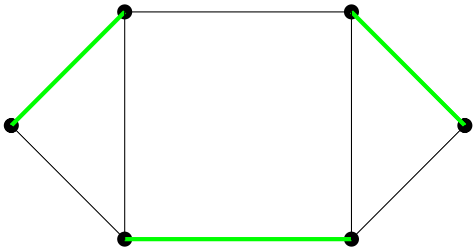


The green vertices are saturated.

Note that choosing a different matching may give you a different set of saturated vertices.

Definition. A matching is **perfect** is every vertex is saturated.

Example 10.4. The following matching is perfect:



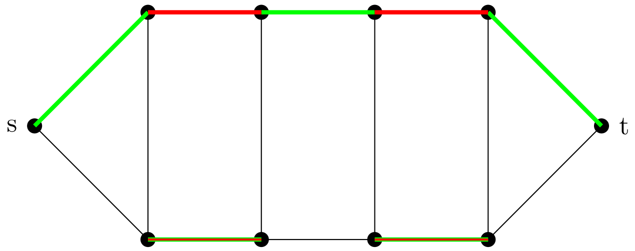
Suppose you're given $K_{n,m}$ (a complete bipartite graph). How many perfect matchings are there? Well, we have two cases:

1. $n \neq m$. Zero perfect matchings exist. One vertex will not have any corresponding vertex in the other partition.

2. $n = m$. $n!$ perfect matchings exist. For the first vertex, we have n choices, $n-1$ choices for the second vertex, and so on.

Writing down every matching to determine a maximum matching is probably not a great idea. Factorials become large very quickly.

We want to know how to make a matching bigger. Consider this graph:



In this graph, the red edges are a smaller, non-perfect matching, and the green edges represent a perfect matching.

To get a larger matching, we need to remove something and add something – we can't just add an edge. In the red path, the first and last edges are not in the matching, and they're alternating. We can just shift our matching over to add that additional edge (which is what the green matching represents). This will result in matching that is larger by one edge.

Definition. Let G be a graph with matching M, and let $P = e_1, e_2, \ldots, e_k$ be a path between vertices s and t. P is **alternating** if for all $i = 1, \ldots, k-1$, exactly one of e_i, e_{i+1} is in M.

Definition. P is **augmenting** if it is alternating and s and t are unsaturated.

Remark: let G be a graph, and let M be a matching of G. Let P be an augmenting path. Let $M' = M \Delta P$ (where $M \Delta P = (M \cup P) \backslash (M \cap P)$). Then M' is a matching and $|M'| = |M| + 1$.

10.2.1 Algorithm for Maximum Matching

← April 1, 2013

A high-level algorithm for finding a maximum matching is as follows.

```
M = $\emptyset$;
while (loop) do
    if $M$ is maximum then STOP;
    else
        find an augmenting path $P$;
        $M := M \Delta P$;
    end
end
```

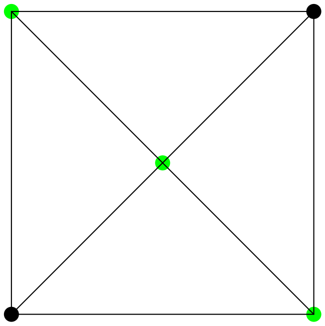
This algorithm is a nice idea, but it is not nearly precise enough – you couldn't program it currently. How do we know if M is maximum? We can't simply enumerate all matchings, that'd get out of hand quickly. Also, how do we find an augmenting path P?

We will determine how to know if M is maximum, and how to find an augmenting path P, on bipartite graphs.

10.3 Vertex Covers

Informally, a vertex cover is a set of vertices where every edge in a graph has at least one endpoint that is a vertex in that set.

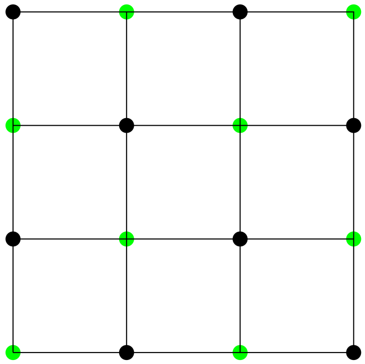
Example 10.5. The vertices in green are a vertex cover of the graph:



Definition. $C \supseteq V$ is a **vertex cover** if every edge has at least one endpoint in C.

Note that the easiest vertex cover is the cover where $C = V$. However, we're interested in picking a cover with as few vertices as possible. This is similar to how the empty set is a matching, but we aren't interested in that – we're interested in matchings with as many edges as possible.

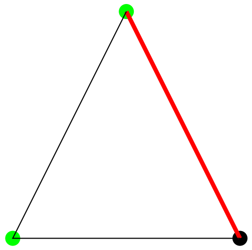
Example 10.6. A minimum vertex cover is indicated in green:



The **minimum vertex cover problem** is where you aim to find a vertex cover with as few vertices as possible.

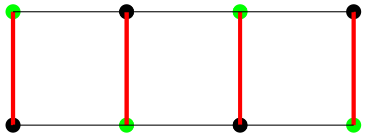
Let's examine the size of a graph's maximum matching with the size of its minimum vertex cover.

Example 10.7. Consider the following graph.



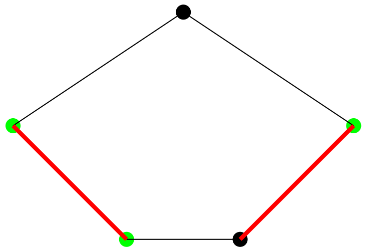
In this graph, $|M| = 1$ and $|C| = 2$.

Example 10.8. Consider the following graph.



In this graph, $|M| = 4$ and $|C| = 4$.

Example 10.9. Consider the following graph.



In this graph, $|M| = 2$ and $|C| = 3$.

We'll use these results to introduce a lemma.

Theorem. *Let M be a matching, and let C be a cover. Then $|M| \leq |C|$.*

To prove this lemma, just look at the edges in the matching. At least one vertex is needed for every edge in the matching, and those vertices are all distinct. Let's formalize this proof.

Proof. Let $M = \{e_1, \ldots, e_k\}$ be a matching. Since C is a cover, for every edge e_i, C contains one endpoint, say w_i, of e_i.

Moreover, since M is a matching, $w_1, \ldots, w_k$ are all distinct.

As $C \supseteq \{w_1, \ldots, w_k\}$, $|C| \geq k$. □

Now, how can we convince someone that a particular matching is a maximum matching? We can note that there exists a cover of a certain size, which implies that no matching of a greater size exists, according to the lemma we just introduced.

Theorem. *Let M be a matching, and let C be a cover. Suppose $|M| = |C|$. Then:*

1. *M is a maximum matching.*

2. *C is a minimum cover.*

Proof. For (1): let M' be any matching. We know that $|M'| \leq |C|$, by the previous theorem, and we know that $|C| = |M|$ (by definition in this lemma). Therefore, $|M'| \leq |M|$.

For (2): let C' be any cover. We know that $|C'| \geq |M|$, by the previous theorem, and we know that $|M| = |C|$ (by definition in this theorem). Therefore, $|C'| \geq |C|$. □

Note that the second theorem we just introduced implies that $\max\{|M| : M \text{ is a matching}\} \leq \min\{|C| : C \text{ is a cover}\}$. However, is this $\leq$, or is it always $=$? It turns out, if the graph contains an odd cycle, then $|M| \neq |C|$.

Theorem (König's Theorem)**.** *In a bipartite graph,* $\max\{|M| : M \textit{ is a matching}\} \leq \min\{|C| : C \textit{ is a cover}\}$ *holds with equality.*

That is, König's Theorem states that the size of the maximum matching of a bipartite graph is equal to the size of the smallest cover of that graph.

Before we can discuss the proof of König's Theorem, we'll need to introduce some additional terminology.

10.4 XY-Structures

Let $G = (V, E)$ be a bipartite graph with partition A, B of V. Let M be a matching of G.

Definition. A vertex v is **special** if:

1. $v \in A$ and v is not saturated, or

2. There exists an alternating path $P(v)$ where one endpoint is v and the other is of type (1).

← April 3, 2013

Definition. Let X denote the special vertices in partition A, and let Y denote the special vertices in partition B.

Let's now prove König's Theorem.

Proof. Let M be a maximum matching, and let $C = (A \backslash X) \cup Y$.

We aim to show:

1. C is a cover.
2. $|C| = |M|$.

Let's start with (1). Suppose C is not a cover. Then there exists an edge uv with $u \in X$ and $v \in B \backslash Y$.

Case 1: u is unsaturated. The edge uv implies that v must be special, which implies that $v \in Y$, which is a contradiction.

Case 2: u is the endpoint of $P(u)$. Then $P(u)$ together with uv is an alternating path. This implies that v is special, which means $v \in Y$, which is a contradiction.

We've proven (1). Let's now prove (2).

For (2), we want to show that $|C| = |M|$. Intuitively, we want to show that $|M| = |Y| + |A \backslash X|$, since $|Y| + |A \backslash X| = |C|$. In order to prove this, we really need to prove these three things:

(i) Edges of M are between X and Y and between $A \backslash X$ and $B \backslash Y$.

(ii) Vertices in $A \backslash X$ are saturated.

(iii) Vertices in Y are saturated.

Let's start with (i). Suppose (i) does not hold. Then there exists an edge $uv \in M$ where $u \in Y$ and $v \in A \backslash X$. Since v is special, there exists an alternating path $P(u)$. The alternating path obtained by adding uv to $P(u)$ implies that v is special, which implies that $v \in X$, which is a contradiction.

The proof for (ii) is very simple. (ii) holds because unsaturated vertices of A are in X.

Finally, let's prove (iii). Suppose there exists $u \in Y$ where u is not saturated. Then $P(u)$ is an alternating path. This is a contradiction since M is a *maximum* matching. □

We'll use a similar approach to that of this proof for the algorithm we need.

10.4.1 Algorithm For Finding a Maximum Matching and Minimal Vertex Cover

Input: a bipartite graph $G = (V, E)$ with partition A, B.

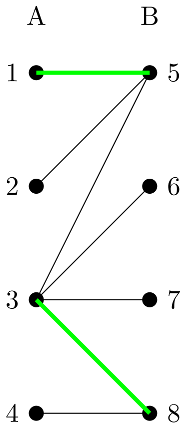
Output: a matching M and a cover C where $|M| = |C|$.

```
$M = \emptyset$ (or any other matching);
while (loop) do
    Construct $X, Y$;
    if there exists $u \in Y$ where $u$ is unsaturated then
        $M := M \Delta P(u)$;
    else
        $C = (A \backslash X) \cup Y$ is a cover;
        $|C| = |M|$, STOP;
    end
end
```

In this algorithm, $S_1 \Delta S_2$ (for any sets S_1 and S_2) is defined as the symmetric difference of S_1 and S_2 (the same way as earlier). That is, $S_1 \Delta S_2 := (S_1 \cup S_2) \backslash (S_1 \cap S_2)$.

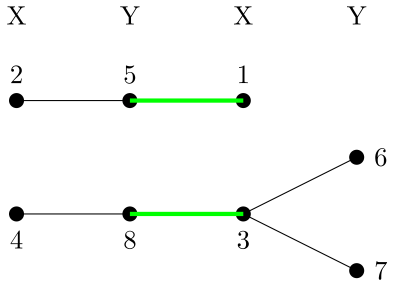
← April 5, 2013

Example 10.10. Let's say you've already run the algorithm for a few iterations, and you have this bipartite graph:



X is defined as all unsaturated vertices in A and all vertices accessible to such vertices via an alternating path. The definition of Y is similar, but on partition B.

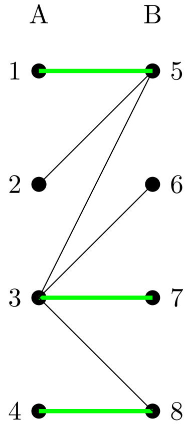
So, we have:



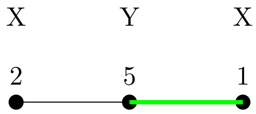
We now have that $7 \in Y$ is unsaturated. $P(7) = 48, 83, 37$. We now have M':

$$M' = \{15, 38\} \Delta \{48, 38, 37\} = \{15, 48, 37\}$$

We now have to repeat the process with our new matching M'.



At this point we have:

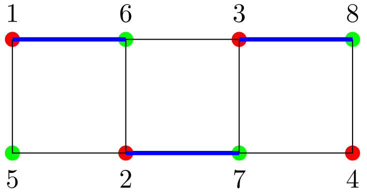


We have that $X = \{1, 2\}$ and $Y = \{5\}$. Y contains only saturated vertices, so we stop. The cover we found is:

$$C = (A \backslash X) \cup Y = \{1, 2, 3, 4\} \backslash \{1, 2\} \cup \{5\} = \{3, 4, 5\}$$

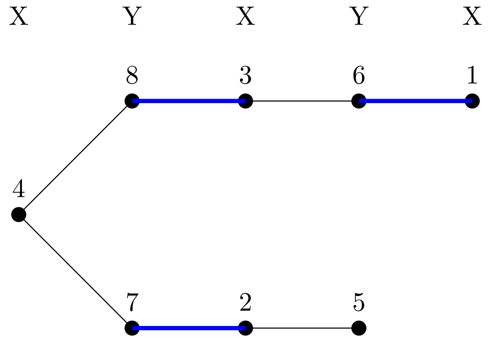
Take the time to verify that the cover is valid.

Example 10.11. Once again, suppose you have run the algorithm for a few iterations and you currently have this:



This is a bipartite graph with partitions $A = \{1, 2, 3, 4\}$ (red) and $B = \{5, 6, 7, 8\}$ (green).

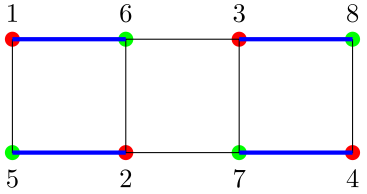
We have $4 \in A$ as an unsaturated vertex, so we get:



We now have $5 \in Y$ which is an unsaturated vertex. $P(5) = 47, 72, 25$. We now have M':

$$M' = M \Delta P(5) = \{16, 38, 27\} \backslash \{47, 72, 25\} = \{16, 38, 47, 25\}$$

We have to repeat the procedure on M'.

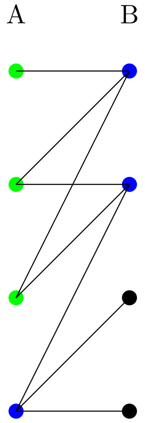


We now have that $X = Y = \emptyset$. There is no vertex in A that is unsaturated, so we should be done. The cover we found is:

$$C = (A \backslash X) \cup Y = A = \{1, 2, 3, 4\}$$

10.5 Hall's Theorem

Consider the following graph:



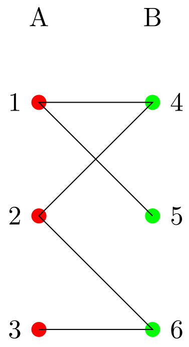
Does this graph have a perfect matching? No, since there exists a cover of size 3 (indicated in blue).

Let's look at another reason we wouldn't have a perfect matching. Look at the vertices indicated in green. One of these vertices will not be covered by a matching.

We need at least the same number of vertices in $N(S)$ (the neighbours of S), otherwise a perfect matching is not possible.

Definition. Let $G = (V, E)$ be a bipartite graph with partitions A and B. Let $S \subseteq A$. Then $N(S) = \{v \in V | \exists uv \in E, u \in S\}$. That is, $N(S)$ denotes the **neighbours** of S.

Example 10.12. Consider the following graph.



In this graph, if $S = \{1\}, N(S) = \{4, 5\}$. Similarly, if $S = \{2, 3\}, N(S) = \{4, 6\}$.

Proposition. *Suppose the bipartite graph $G = (V, E)$ has a perfect matching. Then:*

1. $|A| = |B|$.
2. $\forall S \subseteq A$, $|N(S) \geq |S|$.

((1) and (2) are necessary conditions.)

Proof. Let M be a perfect matching.

1. This is like a function, because each vertex in A should map to exactly one vertex in B. More formally, M defines a bijection between A & B. Therefore, $|A| = |B|$.
2. Let $S = \{v_1, \ldots, v_k\}$. Since M is a perfect matching, there exist edges of M $v_i w_i$ for $i = i, \ldots, k$. This implies that $w_1, \ldots, w_k \in N(S)$, since $w_i, \ldots, w_k$ are distinct. Therefore, $|N(S)| \geq k = |S|$. □

Theorem (Hall's Theorem)**.** *A bipartite graph $G = (V, E)$ with partitions A and B has a perfect matching if and only if $|A| = |B|$ and for all $S \subseteq A, |N(S)| \geq |S|$.*

← April 8, 2013

Proof. We proved the forwards direction of this statement in the previous proposition.

For the reverse direction, assume $|A| = |B|$ and suppose there does not exist a perfect matching. We need to show that there exists $S \subseteq A$ such that $|N(S)| < S$ (that is, we're aiming to prove the contrapositive).

Since there does not exist a perfect matching, we know that the size of the maximum matching is less than $|A|$. By König's theorem, we know there exists a cover C where $|C| < |M|$.

Claim: $N(A\backslash C) \subseteq B \cap C$, since C is a cover. We have:

$$\begin{aligned} |N(A\backslash C)| &\leq |B \cap C| \\ &\leq \underbrace{|B \cap C| + |A \cap C|}_{|C|} - |A \cap C| \\ |C| - |A \cap C| &< |A| - |A \cap C| \\ &< |A\backslash C| \text{ since } |C| < |A| \text{ by König's Theorem} \end{aligned}$$

Therefore, $|N(A\backslash C)| < |A\backslash C|$, as necessary. □

We'll now look at one application of this.

Corollary. *Let $G = (V, E)$ be a bipartite graph with partitions A, B. Suppose G is k-regular ($k \geq 1$). Then G has a perfect matching.*

Proof. We'll check the hypothesis of Hall's Theorem.

1. Check that $|A| = |B|$. We have:

$$k|A| = \sum_{v \in A} \deg(v) = |E| = \sum_{v \in B} \deg(v) = k|B|$$

   This implies that $|A| = |B|$ by dividing by k (since $k \neq 0$).

2. Check that for every $S \subseteq A, |N(S) \geq |S|$. We have:

$$k|S| = \sum_{v \in S} \deg(v) \leq \sum_{v \in N(S)} \deg(v) = k|N(S)|$$

   This implies that $|S| \leq |N(S)|$.

Therefore, by Hall's Theorem, G is a perfect matching. □

Clicker Questions

← January 21, 2013

- How many bijections are there from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$? $n!$, 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 $x^2 - x^4 + x^6 - x^8 + x^10 - \ldots$ 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 $A(x) = 1 + x + x^2 + x^3 + \ldots$ 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.

← January 30, 2013

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

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

- Is $A(B(x))$ a power series for $A(x) = 1 + x + x^2 + \ldots$ and $B(x) = \frac{1}{1-x}$? No! We can only get a power series if $[x^0]B(x) = 0$, but $B(x) = \frac{1}{1-x} = 1 + x + x^2 + \ldots$.
- 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 $[x^{237}](1 + x + x^2 + x^3 + \ldots)(1 + x^2 + x^4 + x^6 + \ldots)$.

  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 $S = \{(a, b)\}, A = \{0, 1, \ldots\}, B = \{0, 1, \ldots\}$. Also, define weight functions for A and B: $w(a) = a, w(b) = 2b$. The generating series are $\phi_A(x) = 1 + x + x^2 + \ldots$ and $\phi_B(x) = 1 + x^2 + x^4 + \ldots$. 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.

← February 27, 2013

- 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 $a_n - 6a_{n-1} + 9a_{n-2} = 0$.

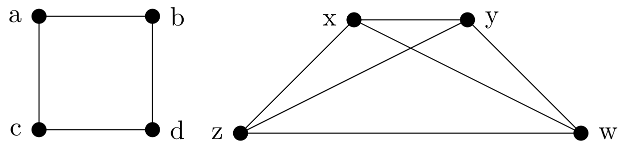
  Note that 3 corresponds to the root, which appears with multiplicity 2. The characteristic polynomial is $p(x) = (x-3)^2 = x^2 - 6x + 9$.

- 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:

$$\begin{aligned}\sum_{v \in V} \deg(v) &= 2|E| \\ 4|V| &= 2|40| \\ 4|V| &= 80 \\ |V| &= 20\end{aligned}$$

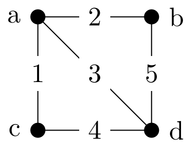
- Are the following two graphs isomorphic?



  Yes! Here's a bijection between their vertices:

$$\begin{aligned}a &\to x \\ d &\to y \\ c &\to z \\ b &\to w\end{aligned}$$

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



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

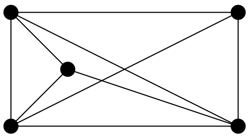
← March 15, 2013

- Let T be a tree with 123 vertices. How many bridges does it have? 122, since no edge is in a cycle in a tree, and the number of edges is equal to the number of vertices minus one (in a tree).

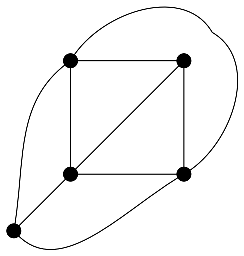
- Let G be a graph with p vertices and q edges. Suppose G has 17 components and no cycles. Then $q = p + 17$. Each of the 17 components is a tree, and every tree has one more vertex than edges.

- Let G be a bipartite graph with partitions X, Y. Suppose G is $k \geq 1$ regular. Is $|X| = |Y|$ true? Yes, always, since $|X|k$ is equal to the number of edges, which equals $|Y|k$.

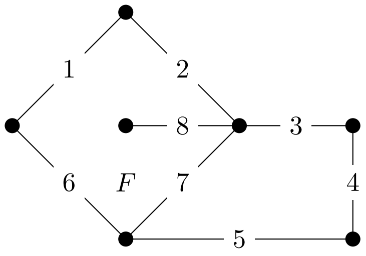
- Is the following graph G planar?

  Yes, G is planar. Here's a planar embedding for G:

- Consider the following graph:

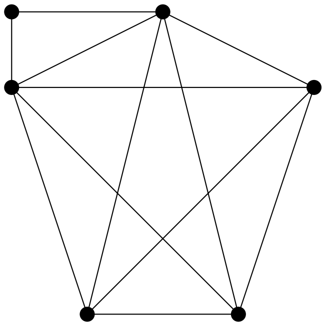
  

  What is the boundary walk for F? 7, 8, 8, 2, 1, 6. (Note that 8 is included twice.)

- Can 2, 2, 3, 3, 4, 4, 5, 6 be the degree sequence for the faces of a planar embedding? No. There must be an even number of odd faces.

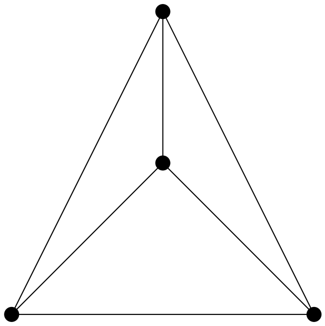
← March 27, 2013

- Is the following graph planar?

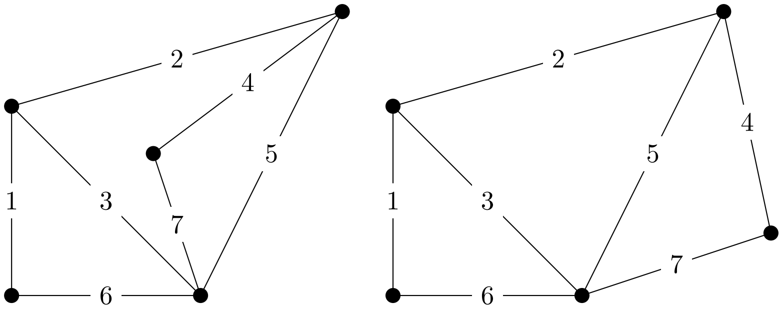


No. There is a subdivision of K_5 in this graph, which makes it non-planar.

- What is the minimum number of colours needed to colour this graph (not shown here)? Four, because this was contained within the graph:



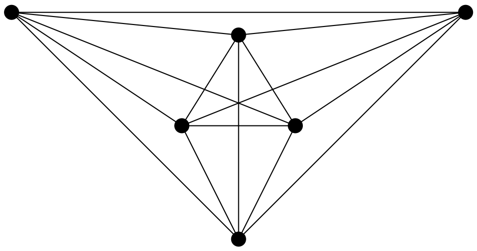
- Do the following embeddings have the same duals?



No. There are no boundary walks of length five in the first graph, but there are in the second. The planar duals are not the same. Note that the dual is of the *drawing*, not of the graph itself.

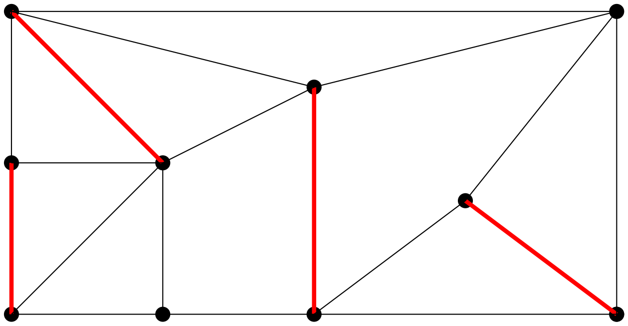
- How many faces does a connected planar graph with 30 vertices and 100 edges have? By Euler's formula, $p - q + f2$, we get that $f = 2 - p + q = 2 - 30 + 100 = 72$.

- What is the minimum number of edges you need to remove from this graph to make it planar?



3. Note that the number of edges is $\binom{6}{2} = 15$. A planar graph with six vertices can only have $3 \cdot 6 - 6 = 12$ edges.

- Do the red edges in the following form a matching?



Yes.