MATH 239 Fall 2022:
Lecture Notes

Lecture notes taken, unless otherwise specified, by myself during section 002 of the Fall 2022 offering of MATH 239, taught by Luke Postle.

Part/chapter titles vaguely follow the official course notes.

Part I

Enumeration

Chapter 1

Introduction

Lecture 1 (09/07; Section 004)

By convention, define the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$. If we want the non-negative integers, we can write $\mathbb{N}_{\geq 1}$.

Recall from set theory, for sets A and B, the union $A \cup B = \{c : c \in A \vee c \in B\}$ and intersection $A \cap B = \{c : c \in A \wedge c \in B\}$. We call a union $A \cup B$ disjoint if $A \cap B = \varnothing$. When considering the sizes of finite sets, the disjoint union corresponds to addition: $|A \cup B| = |A| + |B|$.

Recall also the Cartesian product $A \times B = \{(a, b) : a \in A, b \in B\}$. Again for finite sets, $|A \times B| = |A| \cdot |B|$.

Definition (*bijection*)

A function $f : A \to B$ such that f is injective (i.e., $f(a) = f(a') \implies a = a'$) and surjective (i.e., $\forall b, \exists a, f(a) = b$). When f exists, we write $A \rightleftharpoons B$.

Theorem (*Bijective Proofs*)

If $A \rightleftharpoons B$, then $|A| = |B|$.

Proof. Let $f : A \to B$ be a bijection. For each element of B, it is the image of at least one element of A under f (by surjectivity) and at most one element (by injectivity). Therefore, A contains the same number of elements as B. $\square$

Lecture 2 (09/09)

By convention, let $[n] := \{1, \dots, n\}$.

Theorem

Let A be the set of subsets of $[n]$. Let B be the set of binary strings of length n. There exists a bijection from A to B.

Proof. Let $f : A \to B$ be defined as $f(S) = a_1 \dots a_n$ where $a_i = 1$ if $i \in S$ and 0 otherwise. Then, $f^{-1}(a_1 \dots a_n) = \{i \in [n] : a_i = 1\}$. Since $f^{-1} \circ f = \mathrm{id}$ and $f \circ f^{-1} = \mathrm{id}$, we have a bijection. $\square$

Theorem

Let A be the set of subsets of $[n]$ of size exactly k. Let B be the set of binary strings of length n with exactly k ones. There exists a bijection from A to B.

Proof. Restrict the domain of f from above. □

Definition (*permutation*)

A list of $[n]$ for some positive integer n. That is, a bijection from $[n]$ to $[n]$. Notate the set of permutations of $[n]$ by P_n.

Theorem (*1.3*)

The number of subsets of $[n]$ is 2^n.

Proof. $\mathcal{P}([n]) \rightleftharpoons \{0,1\}^n$ by the above theorem. But we know $|\{0,1\}^n| = |\{0,1\}|^n = 2^n$. Then, $|\mathcal{P}([n])| = 2^n$. □

Theorem (*1.5*)

The number of subsets of $[n]$ of size k is $\binom{n}{k}$.

Proof. Let $S_{n,k}$ be the subsets of $[n]$ of size k.

For each $A \in S_{n,k}$ define $P_A := \{\sigma_1 \dots \sigma_n \in P_n : \{\sigma_1, \dots, \sigma_n\} = A\}$. Then, P_n is the disjoint union of the sets P_A. Also, $P_A \rightleftharpoons P_k \times P_{n-k}$ because the first k entries are a list of A and the last $n-k$ entries are a list of $[n] \setminus A$.

Therefore, $|P_A| = k! \cdot (n-k)!$ and $|S_{n,k}| = \frac{|P_n|}{k! \cdot (n-k)!} = \binom{n}{k}$ as the sets are of equal size. □

In general, to prove that A has some size, we can either

(1) Prove A is a disjoint union of smaller sets of known size
(2) Prove A is a Cartesian product of smaller sets of known size
(3) Give a bijection $A \rightleftharpoons B$ to a set of known size
(4) Show a family of sets A_i satisfies a recurrence relation and use induction

Definition (*composition*)

A finite sequence $n = (m_1, \dots, m_k)$ of positive integers called parts. The size of the composition $|n| = \sum m_i$.

Theorem

For all $n \geq 1$, there are 2^{n-1} compositions of size n

Proof. Proceed by induction on n.

When $n = 1$, there is exactly one composition (1). Assume $n \geq 2$.

Let A_n be compositions of size n. Also let $B_{1,n} := \{(a_1, \dots) \in A_n : a_1 = 1\}$ and $B_{2,n} := \{(a_1, \dots) \in A_n : a_1 \geq 2\}$. Notice that since a_1 is a positive integer so either $a_1 = 1$ or $a_1 \geq 2$, so A_n is the disjoint union of $B_{1,n}$ and $B_{2,n}$.

Let $f : B_{1,n} \to A_{n-1}$ be given by $f((b_1, \dots, b_k)) = (b_2, \dots, b_k)$ and we can find the inverse $f^{-1}((a_1, \dots, a_k)) = (1, a_1, \dots, a_k)$.

Let $g : B_{2,n} \to A_{n-1}$ be given by $g((b_1, \dots, b_k)) = (b_1 - 1, b_2 \dots, b_k)$ whose inverse we can likewise find $g^{-1}((a_1, \dots, a_k)) = (a_1 + 1, a_2, \dots, a_k)$ assuming A_{n-1} is nonempty, i.e., $n \geq 2$.

As these are bijections, $\left|B_{1,n}\right| = |n-1| = \left|B_{2,n}\right|$. By induction $|A_{n-1}| = 2^{n-2}$ and hence $|A_n| = \left|B_{1,n}\right| + \left|B_{2,n}\right| = 2|A_{n-1}| = 2^{n-1}$ as desired. □

Lecture 3 (09/12)

Theorem (*Binomial Theorem*)

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

Proof. Must choose either 1 or x from each monomial, so we have $(1+x)^n = \sum_{S\subseteq[n]} x^{|S|} = \sum_{k=0}^{n} \binom{n}{k} x^k$ by grouping choices by the number of x chosen and applying Theorem 1.5. □

Corollary. If $x = 1$, then $2^n = \sum_{k=0}^{n} \binom{n}{k}$, i.e., Theorem 1.3.

Proof. From Theorem 1.2, $|\mathcal{P}([n])| = 2^n$. But $|\mathcal{P}([n])| = \left|\bigcup S_{n,k}\right| = \sum \left|S_{n,k}\right| = \sum \binom{n}{k}$ by Theorem 1.5. □

Corollary. If $x = -1$, then $0 = \sum_{k=0}^{n} \binom{n}{k} (-1)^k$.

Proof. See Tutorial 1-2. □

Definition (*multiset of t types*)

Sequence $a_1, \dots, a_t$ where each a_i is a non-negative integer. The a_i are the *parts* and the sum $\sum a_i$ is the *size*.

Like compositions but permitting zero and restricting $i = 1, \dots, t$. For example, consider the multiset $(3, 2, 0, 1)$ as being like a "set" $\{a_1, a_1, a_1, a_2, a_2, a_4\}$.

Theorem (*1.9*)

The number of multisets of t types and size n is $\binom{n+t-1}{t-1}$.

Proof. Consider the creation of a multiset like dividing up the line of elements (e.g. $(3, 2, 0, 1)$ as $* * * \mid ** \mid \mid *$).

Encode this as a binary string where 0 means take an element and 1 means switch to the next set (in this case, 000100110). This is a string of length $n+t-1$ with exactly $t-1$ ones. That is, a subset of $[n+t-1]$ with size $t-1$, of which there are $\binom{n+t-1}{t-1}$.

To be formal, write out and prove that the set of multisets A bijects with $B = S_{n+t-1,t-1}$.

Under $f : A \to B : (a_1, \dots, a_t) \mapsto \{a_1 + 1, \dots, a_{t-1} + 1\}$ with inverse $f^{-1} : B \to A : \{b_1, \dots, b_{n-1}\} \mapsto (b_1 - 1, b_2 - b_1 - 1, b_3 - b_2 - 1, \dots, n - b_{t-1} - 1)$, $A \rightleftharpoons B$ and we have $|A| = \binom{n+t-1}{t-1}$, as desired. □

Theorem (*Negative Binomial Series*)

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

Proof. Notice that $\frac{1}{(1-x)^t} = \underbrace{(1+x+x^2+\cdots)\cdots(1+x+x^2+\cdots)}_{t\text{ times}}$. The coefficient of x^k is the number of multisets $(\alpha_1, \dots, \alpha_t)$ of k size so apply Theorem 1.9. □

Lecture 4 (09/14)

Example 4.1 (Pascal's Identity)**.** $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

Proof (informal). We are counting $S \subseteq [n]$. There are two kinds of subsets: $n \in S$ and $n \notin S$. If $n \in S$, then $S \setminus \{n\} \subseteq [n-1]$ with size $n-1$, i.e., there are $\binom{n-1}{k-1}$ of these. If $n \notin S$, then $S \subseteq [n-1]$, i.e., there are $\binom{n-1}{k}$ of these. ☐

Proof. Let $S_{n,k} := \{S \subseteq [n] : |S| = k\}$ be the set of subsets of $[n]$ with size exactly k. By Theorem 1.5, $\left|S_{n,k}\right| = \binom{n}{k}$.

Let $A_1 = \{S \in S_{n,k} : n \in S\}$ and $A_2 = \{S \in S_{n,k} : n \notin S\}$. Then, $S_{n,k}$ is the disjoint union of A_1 and A_2 since either $n \in S$ or $n \notin S$. Thus, $\left|S_{n,k}\right| = |A_1| + |A_2|$.

Claim $A_1 \rightleftharpoons S_{n-1,k-1}$ under $f : A_1 \to S_{n-1,k-1} : S \mapsto S \setminus \{n\}$ with inverse $f^{-1} : S_{n-1,k-1} \to A_1 : T \mapsto T \cup \{n\}$. Then, $|A_1| = \left|S_{n-1,k-1}\right| = \binom{n-1}{k-1}$.

Claim $A_2 \rightleftharpoons S_{n-1,k}$ under $g = \mathrm{id}_{A_2}$ with $g^{-1} = \mathrm{id}_{S_{n-1,k}}$. Then, $|A_2| = \left|S_{n-1,k}\right| = \binom{n-1}{k}$.

Finally, $\binom{n}{k} = \left|S_{n-1,k}\right| = \binom{n-1}{k} + \binom{n-1}{k-1}$. ☐

Example 4.2. $\binom{n}{k} = \sum_{i=k}^{n} \binom{i-1}{k-1}$ for all $n \geq k \geq 1$

Proof (informal). Subsets of $[n]$ of size exactly k come in $n-k+1$ types, namely, classify by their maxima. Then, if i is largest, we have to chose $k-1$ remaining elements from $[i-1]$. This goes down to k being largest by the pigeonhole principle where we have $k-1$ elements from $[k-1]$. ☐

Proof. By Theorem 1.5, $\left|S_{n,k}\right| = \binom{n}{k}$.

Then, since the maximum of a set is unique, we can partition $S_{n,k}$ into the disjoint union $A_k \cup \cdots \cup A_n$ where for each i, $A_i = \{S \in S_{n,k} : \max S = i\}$. Thus, $\left|S_{n,k}\right| = \sum_{i=k}^{n} |A_i|$

Claim $A_i \rightleftharpoons S_{i-1,k-1}$ under the bijection $f : A_i \to S_{i-1,k-1} : S \mapsto S \setminus \{i\}$ with inverse $f^{-1} : S_{i-1,k-1} \to A_i : T \mapsto T \cup \{i\}$ from above. Then, $|A_i| = \binom{i-1}{k-1}$.

Finally, $\binom{n}{k} = \left|S_{n,k}\right| = \sum_{i=k}^{n} \binom{i-1}{k-1}$, as desired. ☐

Chapter 2

Generating Series

Lecture 5 (09/16)

Definition (*weight function*)

$w : A \to \mathbb{N}$ such that $\left|\operatorname{preim}_w(n)\right|$ is finite for all $n \in \mathbb{N}$. Call $w(a)$ the weight of a.

In general, answer questions of the form "how many elements of A have weight n?"

Definition (*generating series*)

$\Phi_A^w(x) = \sum_{a \in A} x^{w(a)}$ for a set A and weight function w.

This is not a polynomial but a formal power series with infinite terms. We do not ever evaluate $\Phi_A^w(x)$ so convergence is irrelevant.

Basically, take the sequence $(\left|\operatorname{preim}_w(0)\right|, \left|\operatorname{preim}_w(1)\right|, \dots)$ and make it into coefficients.

Notate $[x^n]f(x)$ for the coefficient of x^n in $f(x)$.

Example 5.1. For $A = \mathcal{P}([n])$, $w = |\cdot|$, we have $\Phi_A^w(x) = \sum_{k=0}^n \binom{n}{k} x^k = (1+x)^n$

Proposition

The number of elements of weight i is the ith coefficient in $\Phi_A^w(x)$. Equivalently, $\Phi_A^w(x) = \sum_{n \geq 0} a_n x^n$ where $a_n = \left|\operatorname{preim}_w(n)\right|$.

Example 5.2. For set of multisets with t types A and w size of the multiset, $\Phi_A^w(x) = \sum_{n \geq 0} \binom{n+t-1}{t-1} x^n = \frac{1}{(1-x)^t}$.

Example 5.3. For set of binary strings A and w length, $\Phi_A^w(x) = \sum_{n \geq 0} 2^n x^n = \sum_{n \geq 0} (2x)^n = \frac{1}{1-2x}$.

Example 5.4. For set of compositions A and w size, $\Phi_A^w(x) = 1 + x + 2x^2 + 4x^3 + \cdots = 1 + x(1 + 2x + 4x^2 + \cdots)$. This is $1 + x(\frac{1}{1-2x}) = \frac{1-x}{1-2x} = \frac{1}{1-\frac{x}{1-x}}$.

Definition (*formal power series*)

$A(x) = \sum_{n \geq 0} a_n x^n$ where a_n is finite for all $n \in \mathbb{N}$

We define addition, subtraction, and equality of formal power series akin to polynomials: $[x^n](A(x) + B(x)) = a_n + b_n$, $[x^n](A(x) - B(x)) = a_n - b_n$, $A(x) = B(x) \iff \forall n (a_n = b_n)$.

Lecture 6 (09/19)

Define multiplication of formal power series: $A(x)B(x) = \sum_{n\geq 0}(\sum_{k=0}^{n} a_k b_{n+k})x^n$.

Define division using inverses: $\frac{1}{A(x)}$ is the power series $C(x)$ such that $A(x)C(x) = 1$ where we consider the unit power series $1 + 0x + 0x^2 + \cdots$.

If $A(x)C(x) = 1$, then each coefficient $\sum_{k=0}^{n} a_k c_{n-k} = 0$ for $n \geq 1$ and $a_0 c_0 = 1$.

Solving, $c_0 = \frac{1}{a_0}$, $c_1 = -\frac{a_1 c_0}{a_0} = -\frac{a_1}{a_0^2}$, $c_2 = -\frac{1}{a_0}(a_1 c_1 - a_2 c_0)$, etc.

In general, $c_0 = \frac{1}{a_0}$ and $c_n = -\frac{1}{a_0}\sum_{k=0}^{n-1} a_k c_{n-k}$ for $n \geq 1$.

Theorem

$A \in \mathbb{R}[[x]]$ has an inverse $C = A^{-1}$ if and only if $a_0 \neq 0$. If $C(x)$ exists, $c_0 = a_0^{-1}$ and $c_n = -a_0^{-1}\sum_{k=1}^{n} a_k c_{n-k}$.

Given these four operations, we have the ring $\mathbb{R}[[x]]$ of power series. This is a superring of the polynomials $\mathbb{R}[x]$.

Theorem

$A \circ B \in \mathbb{R}[[x]]$ exists if and only if $A \in \mathbb{R}[x]$ or $b_0 = 0$

Lecture 7 (09/21)

Lemma (*Sum Lemma*)

Let C be the disjoint union $A \cup B$. Let w be a weight function of C. Then, $\Phi_C^w(x) = \Phi_A^w(x) + \Phi_B^w(x)$.
Note: Since $w : C \to \mathbb{N}$, we implicitly let $\Phi_A^w = \Phi_A^{w|_A}$ and $\Phi_B^w = \Phi_B^{w|_B}$

Proof. We will show equality by the coefficient definition, i.e., $[x^n]\Phi_C^w(x) = [x^n](\Phi_A^w(x) + \Phi_B^w(x)) = [x^n]\Phi_A^w(x) + [x^n]\Phi_B^w(x)$. The LHS is just the number of elements in $C = A \cup B$ of weight n and the RHS is the sum of the elements in A and B of weight n. These must be equal because $A \cap B = \varnothing$. $\square$

Proof. Expand:

$$\Phi_C^w(x) = \sum_{c\in C} x^{w(c)} = \sum_{a\in A} x^{w(a)} + \sum_{b\in B} x^{w(b)} = \Phi_A^w(x) + \Phi_B^w(x)$$

where we can divide the sum because every $c \in C$ is in exactly one of A or B. $\square$

Lemma (*Infinite Sum Lemma*)

Let C be the disjoint union $\bigcup A_i$ of countably infinite sets. Let w be a weight function of C. Then, $\Phi_C^w(x) = \sum \Phi_{A_i}^w(x)$.

Proof. Since w is a weight function, the preimage is finite. That is, $[x^n]\Phi_C^w(x)$ is finite and we can decompose the finite set $\{c \in C : w(c) = n\}$ into finitely many $\{c \in A_i : w(c) = n\}$, which gives us what we want as above. $\square$

Note: The proof must go in this direction. For weight functions $w_i : A_i \to \mathbb{N}$, $\text{preim}_{w_i}(n)$ is finite but $\bigcup \text{preim}_{w_i}(n)$ is not guaranteed to be finite.

Lemma (*Product Lemma*)

Let A and B be sets and w_A and w_B be weight functions. Define $w_{A\times B} : A \times B \to \mathbb{N} : (a,b) \mapsto w_A(a) + w_B(b)$. Then, $\Phi_{A\times B}^{w_{A\times B}} = \Phi_A^{w_A} \cdot \Phi_B^{w_B}$.

Proof. Recall by definition $\Phi_{A\times B}^{w_{A\times B}} = \displaystyle\sum_{(a,b)\in A\times B} x^{w_{A\times B}((a,b))}$.

But this is $\displaystyle\sum_{(a,b)\in A\times B} x^{w_A(a)+w_B(b)} = \sum_{(a,b)\in A\times B} x^{w_A(a)}x^{w_B(b)} = \sum_{a\in A}\sum_{b\in B} x^{w_A(a)}x^{w_B(b)}$.

We split the sum to get $\left(\sum_{a\in A} x^{w_A(a)}\right)\left(\sum_{b\in B} x^{w_B(b)}\right) = \Phi_A^{w_A}(x) \cdot \Phi_B^{w_B}(x)$. □

Corollary (Finite Products). Define $w(a_1, \dots, a_k)$ on $A_1 \times \cdots \times A_k$ by $\sum_{i=1}^{k} w_{A_i}(a_i)$. Then,

$$\Phi_{A_1 \cdots \times A_k}^{w}(x) = \prod_{i=1}^{k} \Phi_{A_i}^{w_{A_i}}(x)$$

Corollary (Cartesian Product Lemma). For set A with weight function w, $\Phi_{A^k}^{w_k}(x) = (\Phi_A^w(x))^k$ where $w_k((a_i)) = \sum w(a_i)$.

Definition (*strings*)

$A^* = \bigcup_{i=0}^{\infty} A^i$ where $A^0 = \{\varepsilon\}$ with the empty string $\varepsilon = \varnothing$. That is, A^* is the set of all strings (sequences) with entries from A.

Example 7.1. For $A = \mathbb{N} \setminus \{0\}$, then A^* is the set of all compositions. For $A = \{2, 4, 6, \dots\}$, then A^* is the set of all compositions with even parts.

Lecture 8 (09/23)

Lemma (*String Lemma; 2.14*)

Given A and w on A, define $w^* : A^* \to \mathbb{N} : (a_i) = \sum w(a_i)$ with $w^*(\varepsilon) = 0$. Also, there are no elements of A with weight 0. Then, $\Phi_{A^*}^{w^*}(x) = \frac{1}{1-\Phi_A^w(x)}$.

Proof. By definition, $A^* = A^0 \cup A^1 \cup \cdots$ and this is a disjoint union.

Then, since w^* is a weight function of A^* becaues A has no weight 0 elements, we apply the Infinite Sum Lemma. This gives $\Phi_{A^*}^{w^*}(x) = \sum \Phi_{A^i}^{w^*}(x)$.

By the Product Lemma, $\Phi_{A^i}^{w*}(x) = (\Phi_A^w(x))^i$. That is, $\Phi_{A^*}^{w^*}(x) = \sum(\Phi_A^w(x))^i$. Now, we can compose the geometric series $\frac{1}{1-x}$ with $\Phi_A^w(x)$ so long as $[x^0]\Phi_A^w(x) = 0$ which is true by supposition.

Therefore, we get $\Phi_{A^*}w^*(x) = \sum(\Phi_A^w(x))^i = \frac{1}{1-\Phi_A^w(x)}$. □

Example 8.1. Let $A = \mathbb{N}_{\geq 1}$. Then, A^* is the set of all compositions. Define $w = \mathrm{id}$, so A has no elements of weight 0 and we have w^* is a weight function. Namely, w^* gives the size of a composition.

By the String Lemma, $\Phi_{A^*}^{w*}(x) = \frac{1}{1-\Phi_A^w(x)}$. By inspection, $\Phi_A^w(x) = x + x^2 + \cdots$. By the geometric series, we have $x(1 + x + \cdots) = \frac{x}{1-x}$ so $\Phi_{A^*}^{w^*}(x) = \frac{1}{1-\frac{x}{1-x}} = \frac{1-x}{1-2x} = 1 + \frac{x}{1-2x}$ and we can write this as $1 + x + 2x^2 + 4x^3 + \cdots$ or

$$[x^n]\Phi_{A^*}^{w^*}(x) = \begin{cases} 1 & n = 0 \\ 2^{n-1} & n \geq 1 \end{cases}$$

Example 8.2. Let $A = 2\mathbb{N}_{\geq 1}$. Then, A^* is the set of all compositions with even parts and as above we can define $w = \text{id}$ and w^* is a weight funciton giving the size.

By inspection, $\Phi_A^w(x) = x^2 + x^4 + x^6 + \cdots = x^2(1 + (x^2) + (x^2)^2 + \cdots) = \frac{x^2}{1-x^2}$.

Then, $\Phi_{A^*}^{w^*}(x) = \frac{1}{1-\frac{x^2}{1-x^2}} = \frac{1-x^2}{1-2x^2} = 1 + \frac{x^2}{1-2x^2}$ and we can write

$$[x^n]\Phi_{A^*}^{w^*}(x) = \begin{cases} 1 & n = 0 \\ 2^{\frac{n}{2}-1} & n \text{ even} \\ 0 & n \text{ odd} \end{cases}$$

Example 8.3. $A = \{1, 2, 3, 4\}$, $w = \text{id}$, A^* is the set of all compositions with parts 1 to 4. Again, $\Phi_A^w(x) = x + x^2 + x^3 + x^4$ and $\Phi_{A^*}^{w^*} = \frac{1}{1-x-x^2-x^3-x^4}$.

Example 8.4. $A = \{1, 2\}$, $w = \text{id}$, $\Phi_A^w(x) = x + x^2$, $\Phi_{A^*}^{w^*}(x) = \frac{1}{1-x-x^2}$ which is the Fibonacci series.

Example 8.5. $A = \{6, 7, 8, \ldots, 100\}$, $\Phi_A^w(x) = x^6 + x^7 + \cdots + x^{100}$. By the Finite Geometric Series, this is $\frac{x^6 - x^{101}}{1-x}$. Then, $\Phi_{A^*}^{w^*}(x) = \frac{1}{1-\frac{x^6-x^{101}}{1-x}} = \frac{1-x}{1-x^6+x^{101}}$.

Chapter 3

Binary Strings

Lecture 9 (09/26)

Definition (*binary string*)

A sequence of 0's and 1's. The *length* of a binary string is the total number of 0's and 1's. We notate the *empty string* by $\varepsilon = \varnothing$. Formally, it is an element of $\{0,1\}^*$ written without parentheses and commas.

Remark. Define a weight function for $\{0,1\}^*$ to get the length. Let $A = \{0,1\}$. Define $w(a) = 1$. Then if we apply Lemma 2.13, w^* is a weight function and by the String Lemma, $\Phi_{A^*}^{w^*}(x) = \frac{1}{1-\Phi_A^w(x)} = \frac{1}{1-2x}$.

Definition (*regular expression*)

A string of finite length that is, up to parentheses, any one of:

- ε, 0, and 1;
- $\mathsf{R} \smile \mathsf{S}$ for regular expressions R and S;
- RS for regular expressions R and S; or
- $\mathsf{R}*$ for regular expression R

Definition (*concatenation product*)

For binary strings $\alpha = \alpha_1 \ldots \alpha_n \in \{0,1\}^*$ and $\beta = \beta_1 \ldots \beta_n \in \{0,1\}^*$, define $\alpha\beta = \alpha_1 \ldots \alpha_n \beta_1 \ldots \beta_n$

For sets of binary strings $A, B \subseteq \{0,1\}^*$, define $AB = \{\alpha\beta : \alpha \in A, \beta \in B\}$.

Remark. The concatenation product acts like a flatten over the Cartesian product. That is, $((1,0),1) \neq (1,(0,1))$ but $(1,0)(1) = (1)(0,1)$. It follows that $|AB| \leq |A||B|$.

Definition (*rational language*)

$\mathcal{R} \subseteq \{0,1\}^*$ produced by a regular expression R:

- ε, 0, and 1 produce themselves;
- $\mathsf{R} \smile \mathsf{S}$ produces $\mathcal{R} \cup \mathcal{S}$;
- RS produces the concatenation product $\mathcal{RS}$; and
- R^* produces $\bigcup\limits_{k\geq 0} \mathcal{R}^k$ where $\mathcal{R}^k$ is the concatenation power.

Example 9.1. What languages do $(1)^*$, $(1 \smile 11)^*$, $(0 \smile 1)^*$, $1(11)^*$, $(01)^*$ produce?

Solution. $(1)^*$ produces the set of binary strings of only ones, i.e., $\{1\}^*$.

$(1 \smile 11)^*$ produces the same set.

$(0 \smile 1)^*$ produces $\{0,1\}^*$, the set of all binary strings.

$1(11)^*$ produces the set of all odd numbers of ones.

$(01)^*$ produces $\{\varepsilon, 01, 0101, 010101, \dots\}$. □

Example 9.2. Not every set is a rational language. The set $\{\varepsilon, 01, 0011, 000111, 0^i1^i\}$ is not a rational language because it cannot be produced by a regular expression.

Lecture 10 (09/28; from Bradley)

Definition (*unambiguity*)

Regular expression R that produces every element in the corresponding rational language $\mathcal{R}$ exactly once.

Lemma

The following regular expressions are unambiguous:

- ε, 0, and 1
- $\mathsf{R} \smile \mathsf{S}$ given $\mathcal{R} \cap \mathcal{S} = \varnothing$
- RS given either (1) $|\mathcal{RS}| = |\mathcal{R}||\mathcal{S}|$, (2) for all $t \in \mathcal{RS}$, there is a unique $r \in \mathcal{R}$, $s \in \mathcal{S}$ such that $rs = t$, or (3) there does not exist $r_1, r_2 \in \mathcal{R}$, $s_1, s_2 \in \mathcal{S}$ such that $r_1s_1 = r_2s_2$.
- R^* given R unambiguous and either (1) all of ε, $\mathcal{R}$, and $\mathcal{R}^2$ are disjoint or (2) all of the $\mathcal{R}^i$ are unambiguous as products

Example 10.1. Consider the following:

- 1^* is unambiguous because ε, 1, 1^2, etc. are all disjoint meaning that 1^k is unambiguous for all k.
- $(1 \smile 11)^*$ is ambiguous because we can produce 11 as either $(11)^1$ or 1^2.
- $(0 \smile 1)^*$ produces all binary strings and is unambiguous. The union is clearly disjoint. The binary strings of lengths k are clearly disjoint.
- $(101)^*$ produces $\{\varepsilon, 101, 1011101, \dots\}$ and is unambiguous.
- $(1 \smile 10 \smile 01)^*$ is ambiguous because 101 is produced by $1^1(01)^1$ and $(10)^11^1$.

Definition

R leads to a rational function $R(x)$ according to its structure:

- ε leads to 1
- 0 leads to x
- 1 leads to 1
- $R \smile S$ leads to $R(x) + S(x)$
- RS leads to $R(x) \cdot S(x)$
- R^* leads to $\frac{1}{1-R(x)}$

Example 10.2. Consider the same regular expressions:

- 1^* leads to $\frac{1}{1-x}$
- $(1 \smile 11)^*$ leads to $\frac{1}{1-(x+x^2)} = \frac{1}{1-x-x^2}$
- $(0 \smile 1)^*$ leads to $\frac{1}{1-2x}$.
- $(101)^*$ leads to $\frac{1}{1-x^3}$

- $(1 \smile 10 \smile 01)^*$ leads to $\frac{1}{1-x-2x^2}$
- $0^*(11^*00^*)^*1^*$ leads to $\frac{1}{1-x}\frac{1}{1-\frac{x^2}{(1-x)^2}}\frac{1}{1-x} = \frac{1}{1-2x}$

Lemma

> Let R be a regular expression, $\mathcal{R}$ its rational language, $R(x)$ the rational function it leads to, and w the length weight function on binary strings.
> If R is unambiguous, then $\Phi^w_{\mathcal{R}}(x) = R(x)$.

Proof. Proceed by structural induction on the above unambiguity lemma:

Notice that $\Phi^w_{\{e\}}(x) = 1$, $\Phi^w_{\{0\}}(x) = x$, and $\Phi^w_{\{1\}}(x) = x$.

If $\mathsf{R} = \mathsf{S} \smile \mathsf{T}$ and is unambiguous, then R produces $\mathcal{S} \cup \mathcal{T}$ and

$$\Phi^w_{\mathcal{S}\cup\mathcal{T}}(x) = \Phi^w_{\mathcal{S}}(x) + \Phi^w_{\mathcal{T}}(x) = S(x) + T(x) = R(x)$$

by the Sum Lemma.

Likewise by the Product Lemma, if $\mathsf{R} = \mathsf{ST}$ we can write

$$\Phi^w_{\mathcal{S}\mathcal{T}}(x) = \Phi^w_{\mathcal{S}\times\mathcal{T}}(x) = \Phi^w_{\mathcal{S}}(x) \cdot \Phi^w_{\mathcal{T}}(x) = S(x) \cdot T(x) = R(x)$$

because $\mathcal{S}\mathcal{T} = \mathcal{S} \times \mathcal{T}$ by unambiguity.

The case for $\mathsf{R} = \mathsf{S}^*$ goes similarly by the Infinite Sum Lemma and Product Lemma. □

Be careful to distinguish between:

- A regular expression R
- A rational language $\mathcal{R} \subseteq \{0,1\}^*$ it *produces*
- A rational function $R(x) \in \mathbb{Z}[[x]]$ it *leads to*, equal to $\Phi_{\mathcal{R}}(x)$ when R is unambiguous

Lecture 11 (09/30; from Bradley)

Definition (*block*)

> A maximal subsequence of a binary string with the same digit.

Lemma (*Block Decompositions*)

> The set of all binary strings is unambiguously produced by $0^*(11^*00^*)^*1^*$ and $1^*(00^*11^*)^*0^*$.

Proof. WLOG consider the second regular expression. We decompose every binary string after each block of 0s.

This means each string is of the form (a (possibly empty) initial block of 0s, first pair of blocks of 1s, second pair of 0s, ..., last pair, (possibly empty) terminal block of 1s). Moreover, first/last pair may not exist.

This decomposition is unique and we can express it as a regular expression of the form $\mathsf{I}(\mathsf{M})^*\mathsf{T}$ where

- I is a regular expression for the initial (possibly empty) block of 0s
- M is a regular expression for a middle pair of blocks, non-empty block of 1s followed by non-empty block of 0s

- T is a regular expression for the terminal (possibly empty) block of 1s

Then, we can unambiguously write $\mathsf{I} = 0^*$, $\mathsf{M} = (11^*00^*)^*$, and $\mathsf{T} = 1^*$. Using the extra 1/0 ensures each block is non-empty. □

Example 11.1. Write an unambiguous regular expression for "the set of binary strings where each block of 0s has length at least 2 and each block of 1s has even length".

Solution. Follow the $\mathsf{I}(\mathsf{M})^*\mathsf{T}$ pattern beginning with a block of 0s.

To get either no 0s or at least two 0s, set $\mathsf{I} = \varepsilon \smile (000^*)$.

To get either no 1s or an even number of 1s, set $\mathsf{T} = (11)^*$.

Combine these ideas to get $\mathsf{M} = 11(11)^*000^*$.

Altogether, write $(\varepsilon \smile (000^*))(11(11)^*000^*)^*(11)^*$. □

Example 11.2. Write an unambiguous regular expression for "the set of all binary strings where each block of 0s has length at least 5 and congruent to 2 (mod 3) and each block of 1s has length at least 2 and at most 8".

Solution. Follow the $\mathsf{I}(\mathsf{M})^*\mathsf{T}$ pattern beginning with a block of 0s.

To get either no 0s or $5 + 3k$ 0s, set $\mathsf{I} = \varepsilon \smile (00000(000)^*)$.

To get either no 1s or between two and eight 1s, set $\mathsf{T} = (11 \smile 111 \smile \cdots \smile 1^8 \smile \varepsilon)$.

Combine to get $\mathsf{M} = (11 \smile 111 \smile \cdots \smile 1^8)(00000(000)^*)$. Altogether,

$$(\varepsilon \smile (00000(000)^*))((11 \smile 111 \smile \cdots \smile 1^8)(00000(000)^*))^*(11 \smile 111 \smile \cdots \smile 1^8 \smile \varepsilon)$$

□

Example 11.3. Same as example 11.2 with the additional restriction that the string is non-empty and starts with 0.

Solution. $(0^5(000)^*)((1^2 \smile 1^3 \smile \cdots \smile 1^8)(0^5(000)^*))^*(1^2 \smile 1^3 \smile \cdots \smile 1^8 \smile \varepsilon)$.

If we wanted it to start with 1 instead, decompose the blocks beginning with 1s to get a similar answer: $(1^2 \smile 1^3 \smile \cdots \smile 1^8)((0^5(000)^*)(1^2 \smile 1^3 \smile \cdots \smile 1^8))^*(0^5(000)^* \smile \varepsilon)$. □

Example 11.4. Starts with 0 and at least 2 blocks

Solution. $(0^5(000)^*)(1^2 \smile \cdots \smile 1^8)((0^5(000)^*)(1^2 \smile \cdots \smile 1^8))^*(0^5(000)^* \smile \varepsilon)$. □

Example 11.5. Starts with 0 and ends with 0

Solution. $(0^5(000)^*)((1^2 \smile 1^3 \smile \cdots \smile 1^8)(0^5(000)^*))^*$. □

Lecture 12 (10/03)

Instead of decomposing after every block of 1s, we could instead decompose after every 1. This leads to prefix decompositions: the regular expression $\mathsf{M}^*\mathsf{T}$ where $\mathsf{M} = 0^*1$ and $\mathsf{T} = 0^*$ unambiguously produces the set of all binary strings.

As a sanity check, notice that $(M^*T)(x) = \frac{1}{1-\frac{1}{1-x}x}\frac{1}{1-x} = \frac{1}{1-2x}$ which we expect as the generating series for all binary strings.

Example 12.1. Write an unambiguous regular expression for binary strings without k consecutive zeroes.

Solution. $((\varepsilon \smile 0^1 \smile \cdots \smile 0^{k-1})1)^*(\varepsilon \smile 0^1 \smile \cdots \smile 0^{k-1})$.

This leads to $\frac{1}{1-(1+\cdots+x^{k-1})x} \cdot (1+\cdots+x^{k-1}) = \frac{1+\cdots+x^{k-1}}{1-x-\cdots-x^k} = \frac{1-x^k}{1-2x+x^{k+1}}$ □

Similarly, decompose before every 1. This leads to postfix decompositions: the regular expression IM^* where $\mathsf{I} = 0^*$ and $\mathsf{M} = 10^*$ unambiguously produces the set of all binary strings.

Definition (*recursive expression*)

A regular expression R which may contain itself. The rational function $R(x)$ that R leads to is identical to if it were a regular expression except R leads to $R(x)$.

Example 12.2. Interpet $\mathsf{S} = \varepsilon \smile (0 \smile 1)\mathsf{S}$.

Solution. Clearly, ε is in $\mathcal{S}$. Also, $0\varepsilon = 0$ and $1\varepsilon = 1$ are in $\mathcal{S}$. Onward, by induction, $\mathcal{S}$ contains all binary strings.

The rational function $S(x) = 1 + (x + x)S(x) = 1 + 2xS(x) \implies S(x) = \frac{1}{1-2x}$ which matches the generating series for binary strings. □

Example 12.3. Interpret $\mathsf{S} = \varepsilon \smile 1\mathsf{S}$.

Solution. This produces the set of all binary strings with no 0s.

It leads to $S(x) = 1 + xS(x) \implies S(x) = \frac{1}{1-x}$. □

Example 12.4. Write the prefix decomposition as a recursive expression.

Solution. $\mathsf{S} = 0^* \smile (0^*1)\mathsf{S}$ □

Example 12.5. Write example 12.1 as a recursive expression.

Solution. $\mathsf{S} = (\varepsilon \smile 0 \smile \cdots \smile 0^{k-1}) \smile ((\varepsilon \smile 0 \smile \cdots \smile 0^{k-1})1)\mathsf{S}$.

This leads to $S(x) = (1+\cdots+x^{k-1}) + (1+\cdots+x^{k-1})S(x) \implies S(x) = \frac{1+\cdots+x^{k-1}}{1-(1+x+\cdots+x^{k-1})x}$ as in example 12.1. □

Example 12.6. Write example 9.2 as a recursive expression.

Solution. $\mathsf{S} = \varepsilon \smile 0\mathsf{S}1$. Recall that this is not possible with ordinary regular expressions.

Then, the generating series $S(x) = 1 + xS(x)x = 1 + x^2S(x) \implies S(x) = \frac{1}{1-x^2}$. □

Recursion allows us to solve a wider range of problems.

Definition (*containment*)

A binary string σ contains κ if there exist binary strings α and β such that $\sigma = \alpha\kappa\beta$.

We want to solve the general problem: given κ a fixed binary string and $\mathcal{S}_\kappa$ the set of all binary strings that do not contain κ, determine $\Phi_{\mathcal{S}_\kappa}(x)$.

We just did this for $\kappa = 0^k$ in examples 12.1 and 12.5, but what about arbitrary κ?

Lecture 13 (10/05)

Definition (*avoidance*)

A binary string α excludes a binary string κ if α does not contain κ.

We are solving the general problem: given a binary string κ, let A_κ be the set of binary strings avoiding κ. Determine $\Phi_{A_\kappa}(x)$.

Theorem *(3.26)*

Let κ be a fixed binary string, $\mathcal{A} = \mathcal{A}_\kappa$ be the set of binary strings avoiding κ, and $A(x) = \Phi_{\mathcal{A}_\kappa}(x)$. Then,

$$A(x) = \frac{1 + C(x)}{(1-2x)(1+C(x)) + x^{\ell(\kappa)}}$$

where $C(x) = \Phi_{\mathcal{C}}(x)$ where $\mathcal{C}$ is the set of non-empty proper suffixes γ of κ such that there exists a non-empty proper prefix η such that $\kappa\gamma = \eta\kappa$.

Example 13.1. $\kappa = 0^k$. Then, $\mathcal{C} = \{0, 0^2, \dots, 0^{k-1}\}$ because $0^k 0^i = 0^i 0^k$.

Example 13.2. $\kappa = 11011$. Then, $\mathcal{C} = \{011, 1011\}$ because we can write $(11011)(011) = (110)(11011)$ and $(11011)(1011) = (1101)(11011)$ but not with 1 or 11.

Proof. Let $\mathcal{B}$ be the set of all binary strings with exactly one occurence of κ and that occurence is at the end. Let $B(x) = \Phi_{\mathcal{B}}(x)$.

Claim. The following are unambiguous recursive expressions relating $\mathcal{A}$ and $\mathcal{B}$:

$$\mathsf{A} \smile \mathsf{B} = \varepsilon \smile \mathsf{A}(0 \smile 1) \qquad\qquad \mathsf{A}\kappa = \mathsf{B} \smile \smile_{\gamma\in\mathcal{C}} \mathsf{B}\gamma$$

For (1): We know $\varepsilon \in \mathcal{A}$ and $\mathsf{A}(0 \smile 1)$ generates the strings of length at least 1 that are either in $\mathcal{A}$ (by adding a bit that does not complete κ) or in $\mathcal{B}$ (by adding a bit that does). In the other direction, notice that deleting a bit from $\mathcal{A}$ or $\mathcal{B}$ is in $\mathcal{A}$.

For (2): If $\sigma \in \mathcal{A}\kappa$, then σ has an occurence of κ at the end.

Let σ' be the substring of σ with the same start and ending at the first occurence of κ. This exists since there exists at least one occurence of κ.

Thus, $\sigma' \in \mathcal{B}$ and $\sigma = \sigma'\gamma = \sigma''\kappa$ and hence $\kappa\gamma = \eta\kappa$ and $\gamma \in \mathcal{C}$ where γ is the suffix of κ of length $w(\sigma) = w(\sigma')$.

Converting the expressions to equations gives

$$A(x) + B(x) = 1 + A(x)2x \qquad\qquad \begin{aligned} A(x)x^{w(\kappa)} &= B(x)\left(1 + \sum_{\gamma\in\mathcal{C}} x^w(\gamma)\right) \\ &= B(x)(1 + C(x)) \end{aligned}$$

and solving gives us $A(x) = \frac{1+C(x)}{(1+2x)(1+C(x))+x^{w(\kappa)}}$ by eliminating $B(x)$. $\square$

Chapter 4

Recurrence Relations

Lecture 14 (10/07; from Bradley)

Theorem (*4.12*)

> Let $P(x)$ and $Q(x)$ be polynomials such that $\deg P < \deg Q$. Suppose we can write $Q(x) = \prod(1-\lambda x)^{d_i}$, i.e., Q has inverse roots λ_i with multiplicity d_i. Then, there exist complex numbers $c_i^{(1)}, \dots, c_i^{(d_i)}$ for each root λ_i such that $P(x) = \sum_i \sum_{j=1}^{d_i} \frac{c_i^{(j)}}{(1-\lambda_i x)^j}$.

Proof (sketch). One can show that the polynomials $\frac{1}{(1-\lambda_i x)^j}$ form a basis of the subspace of rational functions $P(x)/Q(x)$ with $\deg P < \deg Q$. □

Example 14.1. Write $\frac{1}{(1-x)(1+x)}$ using partial fractions.

Solution. By 4.12, there exist a and b such that $\frac{1}{(1-x)(1+x)} = \frac{a}{1-x} + \frac{b}{1+x} = \frac{a(1+x)+b(1-x)}{(1-x)(1+x)}$. Setting numerators equal, $a(1+x)+b(1-x) = 1 \implies (a+b)+(a-b)x = 1+0x$. Setting coefficients equal, $a+b=1$ and $a-b=0$. This gives $a=b=\frac{1}{2}$. □

This allows us to write any rational function as the sum of negative binomials, which we know how to extract coefficients from. That is, we can extract coefficients from arbitrary series.

Example 14.2. Find the coefficients in example 14.1.

Solution. Write:

$$\begin{aligned}
[x^n]\frac{1}{1-x^2} &= [x^n]\frac{1/2}{1-x} + [x^n]\frac{1/2}{1+x} = \frac{1}{2}[x^n]\frac{1}{1-x} + \frac{1}{2}[x^n]\frac{1}{1+x} = \frac{1}{2}(1)^n + \frac{1}{2}(-1)^n \\
&= \begin{cases} \frac{1}{2}+\frac{1}{2} = 1 & n \equiv 0 \pmod 2 \\ \frac{1}{2}-\frac{1}{2} = 0 & n \equiv 1 \pmod 2 \end{cases}
\end{aligned}$$

which agrees with the known power series $\frac{1}{1-x^2} = 1 + x^2 + x^4 + \cdots$ □

Example 14.3. Find the coefficients of $\frac{1+x}{(1-2x)(1+3x)} = \frac{a}{1-2x} + \frac{b}{1+3x}$.

Solution. Since the degree of the numerator is strictly smaller than the degree of the denominator $(1 < 2)$, we can apply partial fractions.

Write $\frac{1+x}{(1-2x)(1+3x)} = \frac{a(1+3x)+b(1-2x)}{(1-2x)(1+3x)} + \frac{(a+b)+(3a-2b)x}{(1-2x)(1+3x)}$.

Equate coefficients of the numerator:

$$\begin{aligned} a + b &= 1 \\ 3a - 2b &= 1 \end{aligned}$$

Solving gives $a = \frac{3}{5}$, $b = \frac{2}{5}$. To find coefficients, use the negative binomial series:

$$\begin{aligned} [x^n]\frac{1+x}{(1-2x)(1+3x)} &= [x^n]\frac{3/5}{1-2x} + [x^n]\frac{2/5}{1+3x} \\ &= \frac{3}{5}[x^n]\frac{1}{1-2x} + \frac{2}{5}[x^n]\frac{1}{1-3x} \\ &= \frac{3}{5}2^n + \frac{2}{5}(-3)^n \end{aligned}$$

which is a closed-form, non-recursive expression. □

Example 14.4. Find the coefficients of $\frac{1+x}{(1-2x)^2}$.

Solution. Since the root has multiplicity 2, we have to use all its powers:

$$\frac{1+x}{(1-2x)^2} = \frac{a}{1-2x} + \frac{b}{(1-2x)^2} = \frac{a(1-2x)+b}{(1-2x)^2} = \frac{(a+b)-2ax}{(1-2x)^2}$$

Equating coefficients,

$$\begin{aligned} a + b &= 1 \\ -2a &= 1 \end{aligned}$$

which gives $a = -\frac{1}{2}$, $b = \frac{3}{4}$. Then,

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

applying the negative binomial series. □

In summary, we have that $[x^n]\frac{P(x)}{Q(x)} = \sum f_i(n)\lambda_i^n$ for some polynomials $f_i(n)$ with $\deg f_i < d_i$.

Note that all this works only when $\deg P < \deg Q$. If it is not, then we must divide. Recall the polynomial division algorithm lemma from MATH 135:

Lemma (*Division Algorithm*)

For all polynomials $\deg P \geq \deg Q$, there exists polynomials P_1 and P_2 such that $\frac{P(x)}{Q(x)} = P_1(x) + \frac{P_2(x)}{Q(x)}$ where $\deg P_2 < \deg Q$.

Example 14.5. $\frac{1+x^2}{1-x^2} = \frac{x^2-1+1+1}{1-x^2} = \frac{x^2-1}{1-x^2} + \frac{2}{1-x^2} = -1 + \frac{2}{1-x^2}$

Example 14.6. $\frac{x^3+x^2+5x+1}{1-x-x^2} = \frac{-x(1-x-x^2)-x^2-x+x^2+5x+1}{1-x-x^2} = -x + \frac{4x+1}{1-x-x^2}$

This means that when $\deg P \geq \deg Q$, we have $[x^n]\frac{P(x)}{Q(x)} = [x^n]P_1(x) + \sum f_i(n) + \lambda_i^n$. Notice $[x^n]P_1(x)$ will be some constant for $n \leq \deg P_1 \leq \deg P - \deg Q$ and 0 otherwise.

Definition (*recurrence relation*)

A sequence $a_0, \dots, a_n, \dots$ where there exists n_0 and constants $c_1, \dots, c_{n_0-1}$ such that for all $n \geq n_0$, $a_n = \sum_{i=1}^{n_0} c_i a_{n-i}$. The terms $a_0, \dots, a_{n_0-1}$ are the initial conditions.

Example 14.7. $a_0 = 1$, $a_n = a_{n-1}$ for $n \geq 1$. This solves to $a_n = 1$.

Example 14.8. $a_0 = 1$, $a_n = 2a_{n-1}$ for $n \geq 1$. This gives $a_n = 2^n$.

Example 14.9. $a_0 = 1$, $a_1 = 3$, $a_n = 2a_{n-2}$ for $n \geq 2$. Then, $a_n = \begin{cases} 2^{n/2} & n \text{ even} \\ 3 \cdot 2^{\frac{n-1}{2}} & n \text{ odd} \end{cases}$

Example 14.10. Fibonacci: $a_0 = 1$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$ for $n \geq 2$. What is the closed form solution for a_n?

Solution. Recall that rational functions yield recurrence relations because we defined division of power series using recurrently-defined inverses. This procedure is reversible to return recurrence relations to rational functions.

To find $A(x) = \sum a_i x^i$, write out $a_0 x^0 = 1$, $a_1 x^1 = x$, $a_2 x^2 = (a_1 + a_0)x^2$, etc. Then,

$$\begin{aligned} A(x) &= 1 + x + a_0 x^2 + a_1 x^3 + a_1 x^2 + a_2 x^3 + \cdots \\ &= 1 + x + x^2 A(x) + (xA(x) - a_0 x) \\ &= 1 + x + x^2 A(x) + xA(x) - x \\ &= 1 + (x + x^2)A(x) \end{aligned}$$

Solving, $A(x) = \frac{1}{1-x-x^2}$. □

Lecture 15 (10/17)

Theorem (*Case 1*)

TFAE: (1) $A(x) = \frac{P(x)}{Q(x)}$ is a rational function (i.e., P and Q are polynomials and $\deg P < \deg Q$).
(2) The coefficients a_n of $A(n) = \sum_{n \geq 0} a_n x^n$ satisfy initial conditions $a_0, \dots, a_k$ and recurrence relation $a_n = \sum_{i=1}^{k-1} c_i a_{n-i}$ for all $n \geq k+1$ where $k = \deg Q - 1$.
(3) The coefficients a_n have a closed form solution $a_n = \sum_{\text{roots } r_i} p_i(n) - (r_i)^n$ where $p_i(n)$ is a polynomial of degree equal to the multiplicity of r_i minus 1.

Proof. (1) implies (2) by extracting the infinitely many equations of coefficients.

(2) implies (1) by reversing the extraction process (multiply recurrence equation by x^n and sum).

(1) implies (3) by method of partial fractions.

(3) implies (1) by reversing partial fractions (i.e., use the negative binomial series). □

Theorem (*Case 2*)

TFAE: (1) $A(x) = \frac{P(x)}{Q(x)}$ (with no conditions on $\deg P$, $\deg Q$)
(2) Any number of initial conditions $a_0, \dots, a_r$ and recurrence $\sum_{i=1}^{k+1} c_i a_{n-i}$ for all $n > r$ where $k = \deg Q - 1$.
(3) $a_n = C_n + \sum_{\text{roots } r_i} p_i(n)(r_i)^n$ with extra constants C_n (for $n > r$, $C_n = 0$).

Definition (*auxiliary (characteristic) polynomial*)

Given $a_n = \sum_{i=1}^{k+1} c_i a_{n-i}$ is a recurrence relation, replace a_n by x^{k+1}, a_{n-1} by x^k, ..., down to $a_{n-(k+1)}$ by 1.

Example 15.1. Fibonacci: $a_0 = 1$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$ for all $n \geq 2$.

Find the coefficients directly (without using partial fractions).

Solution. We apply Case 1 and know that $a_n = \sum_{r_i} p_i(n) r_i^n$.

The characteristic polynomial is $x^2 = x + 1$, i.e, $0 = x^2 - x - 1$. This is $Q(\frac{1}{x}) \cdot x^{\deg Q}$, i.e., keep the coefficients but reverse the order.

The r_i in Case 1 are *not* the roots of $Q(x)$, but the roots of the characteristic polynomial (the "inverse roots" of Q). In fact, r_i^{-1} is a root of Q.

The roots here are $r_1 = \frac{1-\sqrt{5}}{2}$ and $r_2 = \frac{1+\sqrt{5}}{2}$.

So $a_n = p_1(n) r_1^n + p_2(n) r_2^n$ where p_1 and p_2 have degree 0. That is, $a_n = c_1 r_1^n + c_2 r_2^n$.

Use our initial conditions to solve:

$$\begin{aligned} a_0 &= 1 = c_1 r_1^0 + c_2 r_2^0 = c_1 + c_2 \\ a_1 &= 1 = c_1 r_1 + c_2 r_2 \end{aligned}$$

Then, $c_1 = 1 - c_2$, so $1 = (1-c_2) r_1 + c_2 r_2 = r_1 + c_2(r_2 - r_1) \implies r_2 = \sqrt{5} c_2 \implies c_2 = \frac{1+\sqrt{5}}{2\sqrt{5}}$ and $c_1 = \frac{\sqrt{5}-1}{2\sqrt{5}}$. Finally, $a_n = \frac{\sqrt{5}-1}{2\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n + \frac{1-\sqrt{5}}{2\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n$.

Notice also that $|r_1| < 1$ so $r_1^n \to 0$ and a_n is the closest integer to $\frac{1+\sqrt{5}}{2\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n$. $\square$

Example 15.2. $a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3}$, $a_0 = 1$, $a_1 = 2$, $a_2 = 3$.

Solution. The characteristic polynomial is $x^3 - 3x^2 + 3x - 1$. It factors as $(x-1)^3$ so it has one root $r_1 = 1$ with multiplicity 3.

So $a_n = p_1(n) r_1^n$ where p_1 has degree $3 - 1 = 2$, so $a_n = (c_1 n^2 + c_2 n + c_3)(1)^n = c_1 n^2 + c_2 n + c_3$.

By the initial conditions, $c_3 = 1$.

Then, $2 = a_1 = c_1 + c_2 + c_3 = c_1 + c_2 + 1 \implies c_1 + c_2 = 1$.

Also, $3 = a_2 = 4c_1 + 2c_2 + c_3 = 4c_1 + 2c_2 + 1 = 2c_1 + 3 \implies c_1 = 0$ and $c_2 = 1$.

Finally, we have $a_n = n + 1$. $\square$

Lecture 16 (10/19)

Recall: if $W(x) = \frac{P(x)}{Q(x)}$ is a rational function, then the coefficients w_i satisfy a linear recurrence relation $w_n = \sum_{i=1}^{k+1} c_i w_{n-i}$.

We can write rational functions as $Q(x)W(x) - P(x) = 0$ as a linear equation over the field of polynomials. This is why linear recurrence relations relate to rational functions.

Definition (*quadratic recurrence*)

$A(x)W(x)^2 + B(x)W(x) + C(x) = 0$ for polynomials A, B, and C.

We can in fact apply the quadratic formula and say $W(x) = \frac{-B(x) \pm \sqrt{B(x)^2 - 4A(x)C(x)}}{2A(x)}$.

To do this, we must calculate the square roots of polynomials.

Definition (*complex binomial coefficients*)

For $\alpha \in \mathbb{C}$, define $\binom{\alpha}{k} = \frac{1}{k!}(\alpha)(\alpha - 1) \cdots (\alpha - k + 1)$

Theorem (*General Binomial Theorem*)

For all $\alpha \in \mathbb{C}$, $(1+x)^\alpha = \sum\limits_{k=0}^{\infty} \binom{\alpha}{k} x^k$

Corollary. $\sqrt{1-4x} = 1 - 2\sum_{k \geq 1} \frac{1}{k}\binom{2k-2}{k-1} x^k = 1 - 2\sum_{k \geq 0} \frac{1}{k+1}\binom{2k}{k} x^{k+1}$

Proof. Use the General Binomial Theorem with $\alpha = \frac{1}{2}$ so $(1-4x)^{1/2} = \sum_{k \geq 0} \binom{1/2}{k}(-4)^k x^k$. Algebra bashing gives the result we want. □

Definition (*Catalan numbers*)

$C_n = \frac{1}{n+1}\binom{2n}{n}$

Example 16.1. Calculate the first 5 Catalan numbers.

Solution. $C_0 = \frac{1}{1}\binom{0}{0} = 1$, $C_1 = \frac{1}{2}\binom{2}{1} = 1$, $C_2 = \frac{1}{3}\binom{4}{2} = 2$, $C_3 = \frac{1}{4}\binom{6}{3} = 5$, $C_4 = 14$, $C_5 = 42$. □

The Catalan numbers are interesting because they count many different objects: the number of full binary trees with $n+1$ leaves, the number of triangulations of $(n+2)$-gons, the number of well-formed parenthesizations, etc.

Proposition

$\sum_{k \geq 0} C_k x^k = \frac{1 - \sqrt{1-4x}}{2x}$

Proof. Apply the corollary above and isolate the power series. □

Since this is not a rational function, the Catalan numbers do not form a rational language.

Definition (*Well-formed Parenthesization*)

A sequence of n opening and closing parentheses that "match". That is, for any starting subsequence, the number of opens is at least the number of closes.

Example 16.2. List all WFPs when $n = 3$.

Solution. ()()(), (())(), ()(()), ((())), (()()). Notice there are 5, which is exactly C_3. □

Theorem

The number of WFPs with size n is C_n. Equivalently, the generating series for WFPs with respect to size is $W(x) = \sum w_n x^n = \frac{1-\sqrt{1-4x}}{2x}$.

Proof. We find a recursive unambiguous expression for the set of WFPs $\mathcal{W}$. Let ε be the "empty" WFP, then write

$$\mathsf{W} = \varepsilon \smile (\mathsf{W})\mathsf{W}$$

This is unambiguous because we are always decomposing using the first open parenthesis. This expression leads to the equation

$$\begin{aligned}
W(x) &= 1 + xW(x)^2 \\
0 &= 1 - W(x) + xW(x)^2 \\
W(x) &= \frac{1 \pm \sqrt{(-1)^2 - 4(x)(1)}}{2(x)} \\
&= \frac{1 \pm \sqrt{1-4x}}{2x}
\end{aligned}$$

by the quadratic equation. We must take the negative solution because in the positive solution,

$$W(x) = \frac{1}{2x} + \frac{1}{2x}\left(1 + 2\sum_{k\geq 0} C_k x^{k+1}\right) = \frac{1}{x} - \sum_{k\geq 0} C_k x^k$$

which is not well-defined because $\frac{1}{x}$ has no power series. But the negative solution is exactly the generating series for Catalan numbers. □

Theorem

bradley was bored in class out of his mind today and wanted to say hi to the readers :)

Part II

Graph Theory

Chapter 4

Introduction to Graph Theory

Note: In the notes, there are two chapter 4's (Recurrence Relations and Introduction to Graph Theory). This numbering is maintained.

Lecture 17 (10/21; from Bradley)

Definition (*graph*)

A graph $G = (V, E)$ is a finite set of vertices V and a set[1] of unordered[2] pairs[3] of distinct[4] vertices E called edges. Denote the set of vertices $V(G)$ and edges $E(G)$.

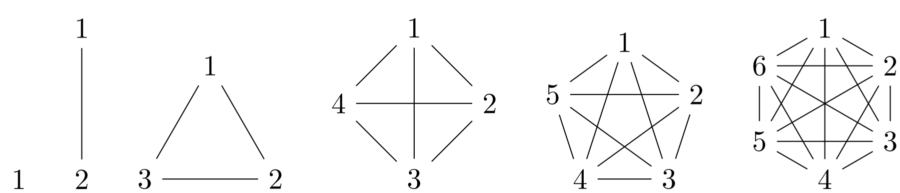
Note: if the graph includes loops and/or parallel edges, it is a multigraph.

Definition (*complete graph on n vertices*)

The graph K_n given by $V(K_n) = [n]$ and $E(K_n) = \{S \subseteq [n] : |S| = 2\}$.

Example 17.1. Draw K_1 through K_6.

Solution. Connect every node in a n-gon:



as desired. □

Definition (*path on n vertices*)

The graph P_n given by $V(P_n) = [n]$ and $E(P_n) = \{\{i, i+1\} : i \in [n-1]\}$.

Definition (*cycle on n vertices*)

The graph C_n for $n \geq 3$ given by $V(C_n) = [n]$ and $E(C_n) = E(P_n) \cup \{1, n\}$.

---

[1] if we allow multisets, they are multiple or parallel edges
[2] if ordered, the graph is directed
[3] if larger tuples, it is a hypergraph
[4] if not, the edge is a loop

Definition (*bipartite*)

> Given a graph G, there exists a partition (A, B) of $V(G)$ such that every edge has exactly one element in A and one element in B.

Example 17.2. Which of the above graphs are bipartite?

Solution. K_1 and K_2 are bipartite, but K_n for $n \geq 3$ is note.

In general, P_n is bipartite with bipartition $A = \{i \in [n] : i \text{ odd}\}$ and $B = \{i \in [n] : i \text{ even}\}$.

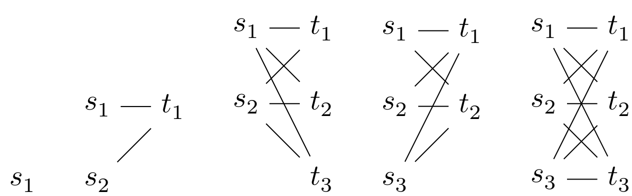
In general, C_n is bipartite when n is even (under the same bipartition as P_n) and not when n is odd. □

Definition (*complete bipartite graph*)

> The graph $K_{m,n}$ described by $V(K_{m,n}) = \{s_i : i \in [m]\} \cup \{t_j : j \in [n]\}$ and $E(K_{m,n}) = \{\{s_i, t_j\} : i \in [n], j \in [m]\}$.

Example 17.3. Draw $K_{1,0}$, $K_{2,1}$, $K_{2,3}$, $K_{3,2}$, and $K_{3,3}$.

Solution. Connect m nodes with n nodes:



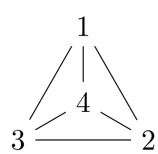
Notice that $K_{2,3}$ and $K_{3,2}$ have the same structure. □

Definition (*planar*)

> A graph that can be drawn on the plane such that no two edges cross

Example 17.4. Which of K_n, P_n, C_n, and $K_{m,n}$ are planar?

Solution. Obviously, K_1, K_2, and K_3 are planar.

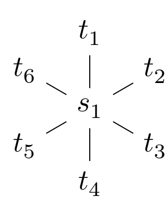
We can redraw K_4 like 

to make it planar.

However, K_5 can't do that.

P_n and C_n are planar for all n.

For $K_{m,n}$, when $m = 0$, we just have n unconnected vertices, which is planar.

When $m = 1$, we have a star (e.g. 

).

When $m = 2$, put s_1 on the left and s_2 on the right and connect (e.g. $\begin{array}{ccccc} & \diagup & t_1 & \diagdown & \\ s_1 & — & t_2 & — & s_2 \\ & \diagdown & t_3 & \diagup & \end{array}$)

When $m \geq 3$, this doesn't work. So $K_{m,n}$ is planar if $m \leq 2$ or $n \leq 2$. □

Lecture 18 (10/24; from Bradley)

Definition

Given vertices u, v and an edge e in G:
- If $uv \in E(G)$, then u and v are adjacent
- If $e = uv$, then e joins the endpoints u and v
- If $v \in e$, then e is incident with v
- If u and v are adjacent, u is a neighbour of v
- The neighbourhood of v $N_G(v)$ is the set of neighbours of v

Definition (*degree*)

The number of neighbours $\deg_G(v) = |N_G(v)|$ of a vertex v in a graph G.

Definition (*k-regularity*)

A graph where every vertex has degree exactly k.

Example 18.1. What are the degrees for K_n, P_n, C_n, and $K_{m,n}$?

Solution. Every vertex in K_n connects to the other $n-1$, so they all have degree $n-1$ and K_n is $(n-1)$-regular.

Every vertex $v \in V(C_n)$ has $\deg(v) = 2$, so C_n is 2-regular.

For P_n, the endpoints $\deg(v_1) = \deg(v_n) = 1$ and the middle vertices $\deg(v_i) = 2$ for $2 \leq i \leq n-1$. Edge case: in P_0, $\deg(v_1) = 0$.

In $K_{m,n}$, $\deg(s_i) = |N(s_i)| = |\{t_i\}| = n$ and $\deg(t_i) = |N(t_i)| = |\{s_i\}| = m$. □

Definition (*degree sequence*)

An ordering $d_1 \geq d_2 \geq \cdots \geq d_n$ of degrees of vertices.

Theorem (*Handshaking Lemma*)

If G is a graph, then $2|E(G)| = \sum_{v \in V(G)} \deg_G(v)$.

Proof (Informal). Every edge is a "handshake" betwen two "people". The number of hands is twice the number of handshakes, since each handshake takes two hands. □

Proof (Formal). Let $S = \{(e, v) : e \in E(G), v \in V(G), v \text{ incident with } e\}$. Counting edges,

$$|S| = \sum_{e \in E(G)} |\{(e, v) \in S\}| = \sum_{v \in V(G)} 2 = 2|E(G)|$$

since every edge has exactly two endpoints. Counting vertcies,

$$|S| = \sum_{v \in V(G)} |\{(e, v) \in S\}| = \sum_{v \in V(G)} \deg_G(v)$$

by definition of $N_G(v)$. Therefore, $2|E(G)| = |S| = \sum_{v\in V(G)} \deg_G(v)$. ☐

Corollary (4.3.2). The number of vertices of odd degree in a graph is even.

Proof. Let $\mathcal{O}(G)$ be the set of odd degree vertices. Let $\mathcal{E}(G)$ be the set of even degree vertices. By the Handshaking Lemma,

$$2|E(G)| = \sum_{v\in V(G)} \deg_G(v) = \sum_{v\in \mathcal{O}(G)} \deg_G(v) + \sum_{v\in \mathcal{E}(G)} \deg_G(v)$$

Take the congruence modulo 2:

$$0 \equiv \sum_{v\in \mathcal{O}(G)} 1 + \sum_{v\in \mathcal{E}(G)} 0 \equiv |\mathcal{O}(G)| + 0 \pmod 2$$

which means that $|\mathcal{O}(G)|$ is even, as desired. ☐

Corollary (4.3.3). The average degree for a graph G is $\frac{2|E(G)|}{|V(G)|}$.

Proof. Average degree is $\frac{\sum_{v\in V(G)} \deg_G(v)}{|V(G)|} = \frac{2|E(G)|}{|V(G)|}$. ☐

Corollary. If G is a k-regular graph, then $|E(G)| = \frac{k}{2}|V(G)|$.

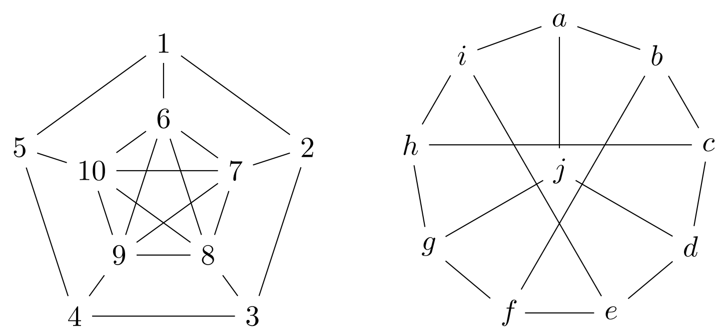
Proof. By the Handshaking Lemma, $2|E(G)| = \sum_{v\in V(G)} \deg_G(v) = \sum_{v\in V(G)} k = k|V(G)|$. ☐

Definition (*isomorphism*)

Graphs G and H are isomorphic if there exists a (graph) isomorphism between them, i.e., a bijection $f : V(G) \to V(H)$ such that $uv \in E(G)$ if and only if $f(u)f(v) \in E(H)$.

Example 18.2. K_1 is isomorphic to P_1, K_2 to P_2, and K_3 to C_3.

Example 18.3. The following are isomorphic representations of the Peterson graph:



under the isomorphism $(a, b, c, d, e, f, g, h, i, j) \mapsto (1, 6, 9, 7, 10, 8, 3, 4, 5, 2)$.

Lecture 19 (10/26)

Definition (*subgraph*)

Graph H of a graph G where $V(H) \subseteq V(G)$ and $E(H) \subseteq \{uv \in E(G), u, v \in V(H)\}$.

Equivalently, a subgraph is obtained from G by deleting a subset of $V(G)$ and the edges incident with those vertices and then deleting a subset of remaining edges.

Example 19.1. $\begin{array}{ccc} & 1 & \\ 2 & \text{—} & 5 \\ \backslash & & / \\ 3 & \text{—} & 4 \end{array}$ has a subgraph $\begin{array}{ccc} 2 & \text{—} & 5 \\ \backslash & & / \\ 3 & & 4 \end{array}$

Definition (*types of subgraphs*)

A subgraph H of G is spanning if $V(H) = V(G)$ (only edge deletions), proper if $H \neq G$, and induced if $E(H) = \{uv \in E(G) : u, v \in V(H)\}$ (only vertex deletions).

Definition (*walk*)

A sequence $W = (v_0, e_1, v_1, \dots, e_k, v_k)$ where $v_i \in V(G)$ and $e_i = v_{i-1}v_i \in E(G)$ is a walk from v_0 to v_k. If $v_0 = v_k$, then W is closed. Call k the length of the walk.

Example 19.2. In the graph G $\begin{array}{ccccccc} u_1 & & & & & & u_5 \\ | & > & u_3 & \text{—} & u_4 & < & | \\ u_2 & & & & & & u_6 \end{array}$, the sequence $(u_5, u_5u_6, u_6, u_6u_5, u_5, u_5u_4, u_4, u_4u_3, u_3, u_3u_1)$ is a walk.

Definition (*path*)

A walk $W = (v_0, \dots, v_k)$ where all the v_i are distinct. Then, the distinct v_0 and v_k are the ends of the path.

We call this a path because the subgraph H formed by $V(H) = \{v_0, \dots, v_k\}$ and $E(H) = \{e_1, \dots, e_k\}$ is isomorphic to P_{k+1}.

Example 19.3. In the graph from example 19.2, $(u_5, u_5u_4, u_4, u_4u_3, u_3, u_3u_1, u_1)$ is a path.

We can abbreviate paths (and walks) as $v_0v_1v_2 \dots v_k$ since it is unambiguous.

Theorem (*4.6.2*)

Given a graph G and there exists a walk from u to v, then there exists a path from u to v.

Proof (informal). If W has no repeat vertices, then W is already a path.

Otherwise, there exists a vertex that repeats twice. Remove the subsequence between these two instances (and repeat). □

Proof. Let $W = v_0, \dots, v_k$ be the shortest walk from u to v. If W has no repeated vertices, then we are done.

Otherwise, there exists a subsequence starting and ending with a repeated node $v_i = v_j$, so we delete e_i through v_j. This is a strictly shorter path W', so W is not the shortest. Contradiction. □

Lecture 20 (10/28)

Corollary (4.6.3). Let G be a graph. If there exists a path from u to v in G and there exists a path from v to w in G, then there exists a path from u to w in G.

Proof. Append the two paths together to get a walk from u to w in G. Then, by 4.6.2 there exists a path from u to w in G. □

Definition (*cycle*)

A subgraph isomorphic to C_k for some $k \geq 3$. The length of a cycle k is the number of edges in it and the girth of a graph is the length of its largest cycle. A Hamilton cycle is a spanning cycle and a Hamiltonian graph contains one.

Theorem (*4.6.4*)

If G is a graph and every vertex of G has degree at least 2, then G contains a cycle.

Proof (algorithmic sketch). We give an algorithm that always finds such a cycle.

Let $P = v_0 \cdots v_k$ be a path in G with $k \geq 2$.

The node v_k has at least two neighbours, so there is one other than v_{k-1}. If the other neighbour $v_i \in V(P)$, then $v_i \cdots v_k$ is a cycle. Otherwise, the neighbour $v_{k+1} \notin V(P)$. Set $P \leftarrow v_0 \cdots v_k v_{k+1}$ and repeat.

We have to prove correctness (that it generates a path and finds cycles) and that it terminates (since length increases and $V(G)$ finite). □

Proof. Let $P = v_0 \cdots v_k$ be a longest path in G. Since a vertex has degree at least 2, $k \geq 2$.

Suppose v_k has a neighbour $v_i \in V(P)$ where $0 \leq i \leq k-2$. Then, $C = v_i \cdots v_k$ is a cycle, as desired.

Otherwise, $N(v_k) \cap V(P) = \{v_{k-1}\}$. Since v_k has degree at least two, $|N(v_k)| \geq 2$. Therefore, $N(v_k) \setminus V(P) \neq \varnothing$. Select $v_{k+1} \in N(v_k) \setminus V(P) \neq \varnothing$. But then $P' = v_0 \cdots v_k v_{k+1}$ is a path in G with length longer than P. Contradiction. □

Corollary (cycle corollary). Let G be a graph. TFAE: (1) G contains a cycle; and (2) G contains a subgraph where every vertex has degree at least 2.

Proof. If G contains a cycle, then the cycle is indeed such a subgraph. If G contains such a subgraph, then by 4.6.4 it contains a cycle. □

Corollary (no cycle corollary). Let G be a graph. Then, TFAE: (1) G does not contain a cycle; (2) all subgraphs of G contain a vertex with degree at most 1; and (3) there exists an ordering $v_1, \ldots, v_n$ of $V(G)$ such that $|N(v_i) \cap \{v_1, \ldots, v_{i-1}\}| \leq 1$ for all $i \in [n]$.

Proof. (1) and (2) are equivalent by the last corollary.

(2) implies (3) by induction on $V(G)$. By assumption, G has a vertex $\deg v_n \leq 1$. Let $G' = G$ without v_n. By assumption, every subgraph of G' has a vertex with degree at most 1 since G does. By induction, there exists the desired ordering $v_1, \ldots, v_{n-1}$ of $V(G')$ but then just let $v_1, \ldots, v_n$ as desired.

(3) implies (2): let H be a subgraph of G and i be the largest index such that $v_i \in V(H)$. Then, $|N_H(v_i)| \leq |N_G(v_i) \cap \{v_1, \ldots, v_{i-1}\}| \leq 1$ by assumption. □

Consider now the question: can we decide efficiently whether a graph G contains a cycle?

Definition (*polynomial time*)

A decision problem is in polynomial time if it can be solved in $O(|V(G)|^k)$ for some $k \in \mathbb{N}$. Denote the set of such problems by P.

Then, ask if the decision problem "does G contain a cycle?" lies in P.

Lecture 21 (10/31)

Definition (*nondeterministic polynomial time*)

A decision problem is in NP if the problem of verifying a certificate of correctness for "yes" results is in P.
Equivalently, a nondeterministic algorithm can solve "yes" instances in P.

Definition (*co-NP time*)

A decision problem is in $\mathsf{co\text{-}NP}$ if verification of "no" instances is in P.

Remark. Clearly, $\mathsf{P} \subseteq \mathsf{NP}$ and $\mathsf{P} \subseteq \mathsf{co\text{-}NP}$.

It is simple to verify a cycle exists after finding one, so this is in NP.

Point (3) of the no cycle corollary is a sufficient "no" certificate, so this is also in $\mathsf{co\text{-}NP}$.

It is not obvious that this problem is in P or not in P.

Conjecture

$\mathsf{P} \neq \mathsf{NP}$

Conjecture

$\mathsf{P} = \mathsf{NP} \cap \mathsf{co\text{-}NP}$

Definition (*NP-complete*)

A problem in NP and, if it is in P, implies that $\mathsf{P} = \mathsf{NP}$. Informally, a problem in NP that is as hard as possible.

We can use the no cycle corollary to find whether a cycle exists in G:

1. $i \leftarrow |V(G)|$
2. $G_n \leftarrow G$
3. **while** $\exists v_i \in V(G)$, $\deg v_i \leq 1$ **do:**
   $G_{i-1} \leftarrow G_i \setminus \{v_i\}$
   $i \leftarrow i - 1$
4. **if** $i = 0$ **then** NO **else** YES

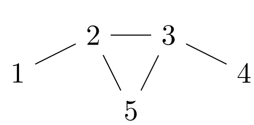
Definition (*connectedness*)

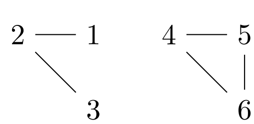
For every $u, v \in V(G)$, there exists a path from u to v.

Example 21.1. K_n, C_n, and P_n are all connected for every n (trivial). $K_{m,n}$ is connected as long as either $m \neq 0$ or $n \neq 0$.

Definition (*component*)

A non-empty subset X of $V(G)$ such that the graph induced by X is connected and X is maximal with respect to this property.

Example 21.2. The graph  is connected and has one component.

Example 21.3. The graph  has two unconnected components.

Theorem

The components of a graph are pairwise disjoint and partition $V(G)$.

Definition (*equivalence relation*)

A binary relation $\sim$ if it is (1) reflexive, i.e., $x \sim x$, (2) symmetric, i.e., $x \sim y \implies y \sim x$, and (3) transitive, i.e., $x \sim y \sim z \implies x \sim z$.

Definition (*equivalence class*)

The set $[x]_\sim := \{y : x \sim y\}$.

Proposition

Given equivalence relation $\sim : S \to S$, the equivalence classes of $\sim$ partition S.

Lecture 22 (11/02)

Theorem (*path equivalence*)

Let $\sim_G$ be a binary relation on $V(G)$ such that $x \sim_G y$ if a path exists from x to y in G. Then, $\sim_G$ is an equivalence relation.

Proof. Show reflexivity, symmetry, and transitivity. Let $x, y, z \in V(G)$.

Notice that a path from x to x exists, namely, the path $\mathbf{p} = (x)$. Then, $x \sim_G x$.

Suppose $x \sim_G y$. Then, there exists a path $(x, xv_1, \dots, v_k y, y)$ from x to y. But then $(y, yv_k, \dots, v_1 x, x)$ is a path from y to x. Therefore, $y \sim_G x$.

Suppose $x \sim_G y \sim_G z$. Then, there exist paths from x to y and y to z. By Corollary 4.6.3, there exists a path from x to z. Therefore, $x \sim_G z$.

Thus, $\sim_G$ is an equivalence relation. $\square$

Corollary. A subset of $V(G)$ is an equivalence class of $\sim_G$ if and only if it is a component.

Proof. Exercise. $\square$

The immediate consequence is the theorem

Theorem

The components of a graph G partition $V(G)$.

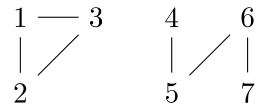
Consider the decision problem if a graph G is connected. Is this in P? NP? $\mathsf{co\text{-}NP}$?

Given a set of paths from every pair of vertices (x, y), it will take $O(|V(G)|^3)$ time to verify that all the paths exist. This is polynomial, so we are in NP.

Definition (*cut*)

For graph G and $X \subseteq V(G)$, the <u>cut induced by X</u> is $\delta(X) = \{xy \in E(G) : x \in X, y \notin X\}$.

Example 22.1. In $\begin{array}{ccccccc} 1 & — & 3 & — & 4 & — & 5 \\ & / & & & & \diagdown & \\ 2 & & & & & & 6 \end{array}$, $\delta(\{1,2,4\}) = \{13, 23, 43, 45, 46\}$.

Example 22.2. In , $\delta(\{1,3,7\}) = \{12, 23, 67\}$ and $\delta(\{1,2,3\}) = \varnothing$.

Theorem (*4.8.5*)

> A graph G is connected if and only if there does not exist non-empty $X \subsetneq V(G)$ with $\delta(X) = \varnothing$.

Proof. Suppose G is not connected. Then, G has at least two components. Let X be one of them, so that $X \subseteq V(G)$ and $X \neq V(G)$. Then, $\delta(X) = \varnothing$ because if $u \in X$ and $uv \in \delta(X)$, then $u \sim_G v$, so $v \in X$ and $uv \notin \delta(X)$.

Conversely, there exists non-empty $X \subsetneq V(G)$ with $\delta(X) = \varnothing$. Then, pick $x \in \delta(X)$ and $y \in V(G) \setminus \delta(X)$.

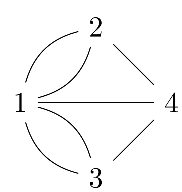
Notice that for there to be a path $xv_1 \cdots v_k y$ from x to y, we must cross between X and $V(G) \setminus X$. This is because either (1) $v_1, \ldots, v_k$ are all in X, meaning $v_k y \in \delta(X)$ or (2) some v_i is the first that is not in X, meaning $v_{i-1}v_i \in \delta(X)$.

Since $\delta(X)$ is empty, there cannot be a path from x to y. Therefore, G is not connected. $\square$

With this theorem, connectivity is in co-NP. Given a component $\varnothing \neq X \subsetneq V(N)$, we need only examine $\delta(X)$ and find it is empty. This runs in $O(|V(G)| + |E(G)|)$.

Lecture 23 (11/04)

Recall the Seven Bridges of Königsberg across the Pregel: there is a bridge between the islands of Kneiphof and Lomse, two bridges from each bank of the Pregel to Kneiphof and one bridge from each bank to Lomse. Is it possible to start and end in the same place and traverse each bridge once?

Recast as a graph theory problem: given the graph  is there a closed walk that uses every edge exactly once? Generalize.

Definition (*Eulerian circuit*)

> A closed walk in G that uses every edge exactly once.

Finding an Eulerian circuit is in NP: given an Eulerian circuit, traverse it to verify correctness.

Theorem (*4.9.2*)

> Let G be a connected graph. Then, G has an Eulerian circuit if and only if every vertex of G has even degree.

Proof. Suppose an Eulerian circuit exists. Let $v \in V(G)$. Every appearance of v in the circuit has an incoming and outgoing edge. Then, since the circuit uses all edges, $|\delta(v)| = \deg v$ is even.

Conversely, suppose that G is connected and every vertex has even degree.

Proceed by induction on $|E(G)|$.

If there exists a vertex with degree 0, then since G is connected, it is the only vertex and G has no edges. Then, the empty walk is an Eulerian circuit.

If every vertex has degree at least 2, then by Theorem 4.6.4, G contains a cycle C.

Let G' be the subgraph of G without $E(C)$. Note that every vertex of G' still has even degree, since we either leave it alone or remove two edges. Let C_i be the components of G'. Inductively, each component C_i has an Eulerian circuit W_i since $|E(C_i)| < |E(G)|$.

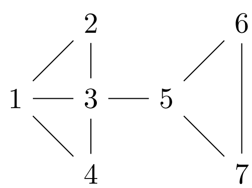
Finally, for each C_i, there is a $v_i \in V(C_i) \cap V(C)$ since G is connected. Insert at v_i the circuit W_i to create an Eulerian circuit of G. $\square$

Corollary. Let G be a graph. Then G has an Eulerian circuit if and only if every vertex has even degree and all edges are in the same component.

Now, it is obvious that finding an Eulerian circuit is in co-NP: either an odd degree vertex or an empty cut with an edge on both sides. We can also show it is in P, analyzing the algorithm.

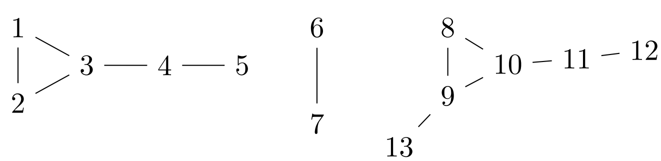
Definition (*bridge*)

An edge $e \in E(G)$ such that $G - e$ has more components than G.

Example 23.1. In the graph 

, the edge 35 is a bridge.

Example 23.2. In the graph



the edges 34, 45, 67, 913, 1011, and 1012 are bridges.

Lemma (*4.10.2*)

Let G be a connected graph.
If $e = xy$ is a bridge of G, then $G - e$ has exactly two components and x and y are in different components of $G - e$.

Proof. Let $A = \{v \in V(G) : v \sim_{G-e} x\}$ and $B = \{v \in V(G) : v \sim_{G-e} y\}$.

Claim that $V(G) = A \cup B$. Since G is connected, there exists a path P from x to v. If $y \notin V(P)$, then P is a path from x to v in $G - e$, hence $v \in A$.

Assume $y \in V(P)$. Then, the subpath P' of P from y to v does not use e and hence $v \in B$. This completes the proof of the claim.

If $A \cap B = \varnothing$, then all of $G - e$ is in one equivalence class of $\sim_{G-e}$, contradicting that $G - e$ has at least 2 components.

Therefore, A and B partition $V(G)$ and indeed are the components of $G - e$. $\square$

Lecture 24 (11/07)

Proposition (*converse of 4.10.2*)

Let $e = xy \in E(G)$. If x and y are in different components of $G - e$, e is a bridge.

Proof. First, note that if $u \nsim_G v$, then $u \nsim_{G-e} v$. This implies that $G/\sim_G \subseteq G_{G-e}/\sim_{G-e}$. Then, since $x \sim_G y$ (i.e., $[x] = [y]$) but $x \nsim_{G-e} y$ (i.e., $[x] \neq [y]$), $G/\sim_G$ must be a strict subset. Since $G - e$ has more components than G, e is a bridge. □

Theorem (*4.10.3*)

Let $e = xy \in E(G)$. Then, TFAE,
(1) e is a bridge of G;
(2) x and y are in different components of $G - e$;
(3) there does not exist a path from x to y in $G - e$;
(4) there does not exist a cycle of G containing e

Proof. (1) and (2) are equivalent by Lemma 4.10.2 and the converse of 4.10.2.

(2) and (3) are equivalent since a component of $G - e$ is exactly an equivalence class of $\sim_{G-e}$, so being in different components means that there is no path.

(3) and (4) are equivalent since if there is a path P from x to y in $G - e$, then $P + e$ is a cycle in G. Conversely, if C is a cycle in G containing e, then $C - e$ is a path from x to y in $G - e$.

Note: (1) $\iff$ (4) is Theorem 4.10.3. □

Corollary (4.10.4). Let G be a graph and $u, v \in V(G)$. If there exist two distinct paths from u to v in G, then G contains a cycle.

Proof. Let $P_1 = ux_1 \cdots x_k v$ and $P_2 = uy_1 \cdots y_\ell v$.

Since $P_1 \neq P_2$, there exists i such that $x_i \neq y_i$ and for all $j < i$, $x_j = y_j$.

Notice that $P_2' = y_{i-1} y_i \cdots y_\ell v$ is a path from y_{i-1} to v in $G - x_{i-1}x_i$. Also, $P_1' = x_i x_{i+1} \cdots x_k v$ is a path from x_{i+1} to v in $G - x_{i-1}x_i$. That is, $x_i \sim_{G-e} v \sim_{G-e} y_{i-1} = x_{i-1}$. Therefore, x_i and x_{i-1} are in the same component of $G - x_i x_{i-1}$.

By Theorem 4.10.3, there exists a cycle of G containing $x_i x_{i-1}$. □

Chapter 5

Trees

Definition (*tree*)

A connected graph that has no cycles.

Definition (*forest*)

A graph that has no cycles.

Notice that every tree is a forest. Also, the components of a forest are trees. Taking a subgraph cannot induce a cycle, so subgraphs of forests are forests and subgraphs of trees are forests. Finally, every forest is the disjoint union of trees (namely, its components).

Lemma (*5.1.3*)

If u and v are vertices of a tree T, then there is a unique u,v-path in T.

Proof. There exists at least one such path since T is connected. But there is at most one path by Corollary 4.10.4 since T has no cycle by definition. □

Lemma (*5.1.4*)

Every edge of a tree T is a bridge.

Proof. There are no cycles in T, so by Theorem 4.10.3, every edge is a bridge. □

Definition (*leaf*)

A vertex in a tree of degree exactly 1.

Theorem (*leaf existence*)

Every tree T with at least two vertices has a leaf.

Solution. Since T has no cycle, then T has a vertex $\deg(v) \leq 1$ by the no cycle corollary.

If $\deg(v) = 0$, then v is a component by itself. But since $|V(T)| \geq 2$, there is another component, contradicting that T is a tree.

Therefore, v is a leaf. □

Lecture 25 (11/09)

Theorem

TFAE:

1. G is a tree
2. G is connected and every connected subgraph of G with at least two vertices has a leaf
3. There exists an ordering $(v_i, \ldots, v_n)$ such that $|N(v_i) \cap \{v_1, \ldots, v_{i-1}\}| = 1$ for all $2 \leq i \leq n$

Theorem (*very useful theorem*)

Let T be a tree and v a leaf of T. Then, $T - v$ is a tree.

Proof. Clearly, $T - v$ is a forest (removal cannot create a cycle).

By Lemma 5.1.4, every edge of T is a bridge.

Let u be the unique neighbour of v and $e = uv$. Then, e is a bridge.

Since T is connected, $T - e$ has exactly two components and u and v are in different components. Since v now has degree 0 in a component on its lonesome, $V(T) \setminus \{v\}$ is a component of $T - e$ and in fact of $T - v$.

Therefore, $T - v$ is connected and $T - v$ is a tree ☐

Notice that induction on this theorem proves equivalence of (1) and (3) above.

Theorem (*5.1.8*)

Every tree with at least two vertices has at least two leaves.

Proof (Postle). Proceed by induction on $|V(T)|$.

If $|V(T)| = 2$, then $T = K_2$ with both vertices being leaves.

Otherwise, if $|V(T)| \geq 3$, by leaf existence, T has at least one leaf v. Then, by the very useful theorem, $T - v$ is a tree where $|V(T - v)| = |V(T)| - 1$. By induction, $T - v$ has at least two leaves v_1 and v_2.

Let u be the neighbour of v. Then, u cannot be both v_1 and v_2, so either v_1 or v_2 is another leaf in $T - v$ and in T, as desired. ☐

Proof (Book). Let $P = v_1 \cdots v_k$ be a longest path in T. Then, v_1 and v_k are leaves of T (if not, then there is either a longer path or a cycle). ☐

Theorem (*5.1.5*)

If T is a tree, then $|E(T)| = |V(T)| - 1$.

Proof. Proceed by induction on $|V(T)|$. If $|V(T)| = 1$, then $E(T) = 0 = |V(T)| - 1$.

Assume $|V(T)| \geq 2$. Then, T has a leaf by Theorem 5.1.8. But $T - v$ is a tree by the very useful theorem. Since $T - v$ removed a leaf, it removed only one edge. That is, by induction, $|E(T)| = |E(T - v)| + 1 = (|V(T - v)| - 1) + 1 = |V(T)| - 1$ as desired. ☐

Corollary (5.1.6). If G is a forest with exactly k components, then $|E(G)| = |V(G)| - k$.

Proof. Let $T_1, \ldots, T_k$ be the components of G. Then, T_i are trees. By Theorem 5.1.5, $|E(T_i)| = |V(T_i)| - 1$.

Then, $\sum |E(T_i)| = \sum (|V(T_i)| - 1) = |V(T)| - k$. ☐

Proposition

If T is a tree with at least two vertices and $n_r = \{v \in V(T) : \deg(v) = r\}$, then we can write $n_1 = 2 + \sum_{r\geq 3}(r-2)n_r$.

Proof. By Theorem 5.1.5, $|E(T)| = |V(T)|-1$. But by the Handshaking Lemma, $2|E(T)| = \sum \deg(r) = \sum n_r r$. Combining, $2(|V(T)|-1) = 2|E(T)| = \sum n_r r$.

This gives $2(\sum n_r r) - 2 = \sum r n_r$, so that $2n_1 + 2n_2 + \cdots - 2 = n_1 + 2n_2 + \cdots$ and we can write $n_1 = 2 + \sum_{r\geq 3}(r-2)n_r$. □

This proposition gives another altnernate proof for Theorem 5.1.8.

Definition (*spanning tree*)

A spanning subgraph of G that is a tree.

Theorem (*5.2.1*)

A graph G is connected if and only if G has a spanning tree.

Proof. If G has a spanning tree, then G is clearly connected since paths exist by walking along the connected spanning tree.

If G is connected, then we proceed by induction on $|E(G)|$. If G is a tree, then we are done.

Since G is connected, it contains a cycle C by Theorem 4.6.4. Let $e \in C$. Then, by Theorem 4.10.3, e is not a bridge. Hence, $G - e$ has the same number of components.

But $|E(G-e)| = |E(G)| - 1 < |E(G)|$. By induction, $G - e$ has a spanning tree T. Since we deleted only an edge, T is a spanning tree for G. □

Lecture 26 (11/11)

Consider again the forwards (hard) direction of Theorem 5.2.1.

Proof ("grow a tree"). Let T be a tree in G such that $|V(T)|$ is maximized. Such a T exists as G has a single vertex. If $V(T) = V(G)$, then T is spanning and we are done.

Assume $V(T) \neq V(G)$. Then, since G is connected, there exists a non-empty cut $\delta(V(T))$ because $\varnothing \neq V(T) \neq V(G)$. Therefore, there exists an edge $e \in \delta(V(T))$. Then, $T' = T + e$ is a tree with $|V(T')| = |V(T)| + 1 > |V(T)|$ contradicting the choice of T. □

Proof ("grow a forest"). Let F be a spanning forest such that $|E(F)|$ is maximized. This exists since F with all vertices, no edges is such a graph.

If $|E(F)| = |V(G)| - 1$, then F is a spanning tree.

Assume $|E(F)| \leq |V(G)| - 1$ so that F is not a tree.

Let F_1 be a component of F. Since G is connected, $\delta(F_1) \neq \varnothing$ so $\exists e \in \delta(F_1)$. Then, $F' = F + e$ is a spanning forest with more edges. □

Proof (cute). Induct on $|V(G)|$. Let $v \in V(G)$. Then $G - v$ has components $H_1, \ldots, H_k$ for $k \geq 1$. These components are connected with fewer vertices, so by induction, spanning trees $T_1, \ldots, T_k$ exist. Then, since G is connected, there exist $u_i \in V(H_i)$ where $vu_i \in E(G)$. Finally, $\bigcup(T_i + vu_i)$ is a spanning tree of G. □

Corollary (5.2.2). If G is connected and $|E(G)| = |V(G)| - 1$, then G is a tree.

Proof. By Theorem 5.2.1, G has a spanning tree T where $V(G) = V(T)$. By Theorem 5.1.5, $|E(T)| = |V(T)| - 1 = |V(G)| - 1$. Since $E(T) \subseteq E(G)$, we have that $E(G) = E(T)$ and G is the tree T. □

Theorem (*5.2.3*)

If T is a spanning tree of G and e is an edge of G not in T, then $T + e$ contains exactly one cycle C.[1] Also, if $e' \in E(C)$, then $T + e - e'$ is a spanning tree of G.

Proof. Since T is a tree, every cycle of $T + e$ must contain e.

Let C be a cycle containing $e = uv$. Then, $C - e$ is a path in T from u to v. By Lemma 5.1.3, $C - e$, and indeed C, is unique.

Suppose $e' \in E(C)$. Then, by Lemma 4.10.2, e' is not a bridge. That is, $T + e - e'$ has the same number of components as $T + e$, i.e., it is connected. But $|E(T + e - e')| = |E(T)|$ so by Corollary 5.2.2, it is a tree. □

Theorem (*5.2.4*)

If T is a spanning tree of G and $e \in E(T)$, then $T - e$ has two components. If e' is in the cut induced by one of the components, $T - e + e'$ is a spanning tree.

Proof. The first part is obvious by Lemma 4.10.2.

Let X and Y be the components of $T - e$. Since $e' \in \delta(X) = \delta(Y)$,[2] we have that X and Y are the same component in $T - e + e'$, meaning that it is connected. As above, by Corollary 5.2.2, it is a tree. □

Equivalently, if we *add* an edge e to T, then *deleting* an edge in its fundamental cycle yields a spanning tree; and if we instead *delete* the edge, *adding* from its fundamental cut gives a spanning tree.

Lemma (*5.3.1*)

An odd cycle is not bipartite.

Proof. See Example 17.2.

Let $V(C_n) = \{v_1, \dots, v_n\}$. Suppose for a contradiction there exists a bipartition (A, B) of $V(C_n)$ with $E(C_n) \subseteq \delta(A)$.

We assume WLOG that $v_1 \in A$. Given $v_1v_2 \in E(G)$, this means $v_2 \in B$. Likewise up to $v_n \in A$. But then $v_1v_n \notin \delta(A)$. Contradiction. □

Proposition

If G is bipartite, then every subgraph of G is bipartite.

Proof. There exists a bipartition of G. If we restrict it to a subgraph, it is stil valid. □

Lecture 27 (11/14)

[1]This is the fundamental cycle of e with respect to T

[2]The fundamental cut of e with respect to T

Theorem (*5.3.2*)

A graph is not bipartite if and only if it has no odd cycles.

Proof. The forwards direction follows from the above proposition and by Lemma 5.3.1.

Suppose G has no odd cycles. By the proposition, G is bipartite if and only if its components are bipartite.

Then, we may assume G is connected. By Theorem 5.2.1, there exists a spanning tree T. Let $v \in V(T)$. Partition (A, B) based on the parity of the distance from v.

If this is not the desired bipartition, then there exists $u_1u_2 \in E(G)$ with u_1 and u_2 both in either A or B. Let w be the vertex of the unique (u_1, u_2)-path P whose (w, v)-path has minimum length.

Then, let P_1 be the (u_1, v)-path in T, P_2 be the (u_2, v)-path, P_1' be the (u_1, w)-path, P_2' be the (u_2, w)-path, and Q be the (v, w)-path. By path uniqueness, $|E(P_1)| = |E(P_1')| + |E(Q)|$ and $|E(P_2)| = |E(P_2')| + |E(Q)|$.

But since u_1 and u_2 are in the same partition, $|E(P_1)| \equiv |E(P_2)| \pmod 2$. It follows that $|E(P_1')| \equiv |E(P_2')| \pmod 2$. Therefore, $|E(P)| = |E(P_1')| + |E(P_2')| \equiv 0 \pmod 2$.

Therefore, P has an even number of edges, so $P + u_1u_2$ is an odd cycle in G. □

Consider the decision problem of whether G is bipartite.

It is in NP, since we can just give the bipartition. By Theorem 5.3.2, it is also in co-NP, since we can give an odd cycle.

We can give a polynomial-time algorithm to find the bipartition/odd cycle:

```
for H_i component of G do:
    T_i ← spanning tree of H_i
    pick v_i ∈ V(T_i)
    construct A_i and B_i as in the proof
    if there are no edges with both ends in A_i or B_i then:
        continue
    else:
        return NO
return YES
```

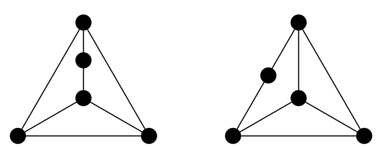
Chapter 7

Planar Graphs

Definition (*planar graph*)

A graph that can be drawn in the plane without edges crossing, i.e., vertices are distinct points and edges are continuous, non-interescting curves connecting those points. This drawing is a planar embedding. A plane graph is a planar graph with a planar embedding.

Example 27.1. These two distinct planar embeddings embed the same graph:



Definition (*face*)

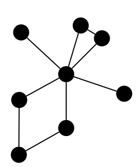
A connected region of $\mathbb{R}^2 - (E(G) \cup V(G))$. Let $F(G)$ be the set of faces of G.

Definition (*boundary walk*)

A sequence $v_0, e_1, v_1, \ldots, v_0$ which traverses the edges on the boundary of a face.[1]

Note: a vertex may appear multiple times in a boundary walk.

Example 27.2. In the graph



the central vertex appears 4 times in the boundary walk of the "outside".

An edge appears twice if and only if that edge is a bridge.

Definition (*degree (length) of a face*)

The length of the boundary walk, counting multiplicity.

If the boundary is not connected, then the boundary walk is the union of the boundary

[1] i.e., "incident" to the face

walks with respect to each component.

Lemma (*Faceshaking Lemma*)

Let G be a plane graph. Then,

$$\sum_{f \in F(G)} \deg(f) = 2|E(G)|$$

(by analogy to the Handshaking Lemma)

Proof. Each edge contributes exactly 2 to this sum. If it is a bridge, 2 to the one face it is incident with; otherwise, 1 to each of the 2 faces it is incident with. ☐

Corollary. There are an even number of odd-degree faces.

Corollary. The average degree of a face is $\frac{2|E(G)|}{|F(G)|}$.

Lecture 28 (11/16; from Bradley)

Theorem (*Euler's Formula*)

Let G be a connected planar graph. Then, $|V(G)| - |E(G)| + |F(G)| = 2$.

Proof. Proceed by induction on $|E(G)|$.

If G is a tree, the number of edges is minimized. Then, $|V(G)| = |E(G)| - 1$ by Corollary 5.2.2 and there is one face, so $|V(G)| - |E(G)| + |F(G)| = 1 + 1 = 2$.

Otherwise, G is not a tree. Then, G contains a cycle C. Let $e \in C$ and $G' = G - e$.

Then, $|V(G')| = |V(G)|$ and $|E(G')| = |E(G)| - 1$. Since e was in a cycle, it was incident to two faces that are now joined, so $|F(G')| = |F(G)| - 1$. Finally, since e is a bridge, G' is connected. Therefore, by induction, since $|E(G')| < |E(G)|$, we have $|V(G')| - |E(G')| + |F(G')| = 2$. Substituting, $|V(G)| - |E(G)| + |F(G)| = 2 + 1 - 1 = 2$ as desired. ☐

Corollary (Euler's Formula for unconnected graphs). Let G be a graph with k components. Then, $|V(G)| - |E(G)| + |F(G)| = 1 + k$.

Proof. Do the same thing but with the base case of a forest instead of a tree. Alternatively, add the minimum $k-1$ edges to connect the components and apply the ordinary formula. ☐

Lemma (*7.5.1*)

Let G be a planar graph. If G contains a cycle, the boundary of any face contains a cycle.

Proof. Since G contains a cycle, there are at least two faces. Then, a face f is incident to at least one other face g. Pick an edge e on the boundary of f and g. Consider the component of the boundary of f that e lies in and consider the boundary walk. Since e is incident to two faces, e appears once in the walk. Therefore, there is a cycle in the component since e is not a bridge. ☐

Lemma (*7.5.2*)

Let G be a planar graph. If each face of G has degree at least g, then $|E(G)| \leq \frac{g}{g-2}(|V(G)| - 2)$.

Proof. By the Faceshaking Lemma, $2|E(G)| = \sum \deg(f) \geq g|F(G)|$. Then, by Euler's Formula for unconnected graphs,

$$\begin{aligned}
|V(G)| - |E(G)| + |F(G)| = 1 + k &\leq 2 \\
|V(G)| - 2 + |F(G)| &\leq |E(G)| \\
g(|V(G)| - 2) + g|F(G)| &\leq g|E(G)| \\
g(|V(G)| - 2) + 2|E(G)| &\leq g|E(G)| \\
g(|V(G)| - 2) &\leq (g-2)|E(G)| \\
\frac{g}{g-2}(|V(G)| - 2) &\leq |E(G)|
\end{aligned}$$

as desired. □

Theorem (*7.5.3*)

Let G be a planar graph with $|V(G)| \geq 3$. Then, $|E(G)| \leq 3|V(G)| - 6$.

Proof. Suppose G does not contain a cycle. Then, it is a forest and by Corollary 5.1.6, $|E(G)| = |V(G)| - k \leq |V(G)| - 1 \leq |V(G)| - 6$ since there is at least 1 component and 3 vertices.

Otherwise, G contains a cycle. By Lemma 7.5.1, every face contains a cycle in its boundary. Since a cycle has at least 3 edges, the degree of every face is at least 3. So by Lemma 7.5.2, $|E(G)| \leq \frac{3}{3-2}(|V(G) - 2|) = 3|V(G)| - 6$, as desired. □

Corollary (7.5.4). K_5 is not planar.

Proof. Notice that $|E(K_5)| = \binom{5}{2} = 10$ but $3|V(G)| - 6 = 9$. □

Theorem (*7.5.6*)

Let G be a planar graph with $|V(G)| \geq 3$. If G is triangle-free, then $|E(G)| \leq 2|V(G)| - 4$.

Proof. Follow the proof of Theorem 7.5.3 but notice that cycles will have length at least 4, so $|E(G)| \leq \frac{4}{4-2}(|V(G)| - 2) = 2|V(G)| - 4$. □

Lemma (*7.5.7*)

$K_{3,3}$ is not planar.

Proof. First, notice that since $K_{3,3}$ is bipartite, it is triangle-free. But $|E(G)| = 9$ and $2|V(G)| - 4 = 8$. □

Lecture 29 (11/18)

Recall Euler's formula: $V - E + F = 2$ if connected or in general $V - E + F = k + 1$ for k components.

If $V \geq 3$ and G planar, then $E \leq 3V - 6$. Thus, K_5 and $K_{3,3}$ are non-planar.

Consider the decision problem of whether G is planar. We cannot certify planarity by giving equations of curves, since showing no intersections is not efficient and the equations can be arbitrarily complex. However, a planar embedding is equivalently a list of boundary walks of faces. To certify, assert that every edge appears twice, Euler's formula holds, and edges cut a vertex cone in a clockwise order. Therefore, planarity is in NP.

Proposition

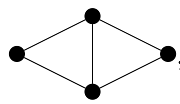
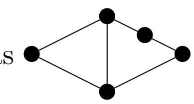
If G is a planar graph and H is a subgraph of G, then H is planar.

Proof. Obvious (delete from the planar embedding of G until you get H). ☐

Corollary. If G contains K_5 or $K_{3,3}$ as a subgraph, then G is not planar.

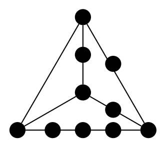
Definition (*edge subdivision*)

Let $e = uv \in E(G)$ and $z \notin V(G)$. Obtain G' as $V(G') = V(G) \cup \{z\}$ and $E(G') = E(G) \setminus \{e\} \cup \{uz, zv\}$.

Example 29.1. If G is , we can draw G' as 

Definition (*subdivision*)

A graph obtained from G by any number (including none) of repeated edge subdivisions.

Example 29.2. If $G = K_4$, then G' could be 

Proposition

If G is a planar graph and H is a subdivision of G, then H is planar.

Proof. Subdivide the planar embedding of G and notice it is still planar. ☐

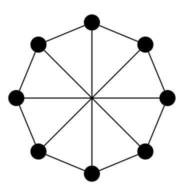
Corollary. If G is a subdivision of $K_{3,3}$ or a subdivision of K_5, then G is not planar.

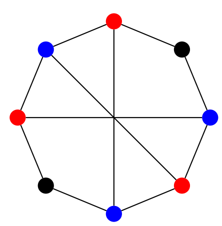
Theorem (*Kuratowski's Theorem*)

A graph G is planar if and only if it does not contain a subdivision of $K_{3,3}$ or a subdivision of K_5.

Proof. Very hard. See CO 342. ☐

Now, we can say that planarity is in co-NP because we can give by Kuratowski a subgraph that is a subdivision of $K_{3,3}$ or a subdivision of K_5.

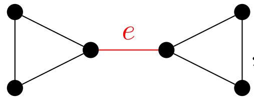
Example 29.3. Is the graph  planar?

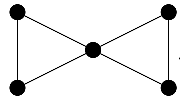
Solution. No. We can highlight $K_{3,3}$ as a subgraph:  ☐

We can show that planarity is in P with an $O(|V(G)|^3)$ algorithm.

Definition (*contraction*)

Let $e = uv \in E(G)$ and $z \notin V(G)$. Obtain $G' = G/e$ as $V(G') = V(G) \setminus \{u, v\} \cup \{z\}$ and $E(G') = E(G \setminus \{u, v\}) \cup \{wz : w \in N_G(u) \cup N_G(v)\}$.

Example 29.4. If G is 

, then G/e is .

Definition (*minor*)

A graph H is a minor of a graph G if it can be obtained from a subgraph of G by contracting edges.

Proposition

If G is planar and H is a minor of G, then H is planar.

Corollary. If G contains K_5 or $K_{3,3}$ as a minor, then G is not planar.

Lecture 30 (11/21)

We can equivalently state Kuratowski's Theorem in terms of minors due to Wagner:

Theorem (*Kuratowski's Theorem for minors*)

A graph G is planar if and only if G does not contain $K_{3,3}$ or K_5 as a minor.

Proof (sketch). We must show that containing $K_{3,3}$ or K_5 as a subdivision is equivalent to containing $K_{3,3}$ or K_5 as a minor.

In fact, claim that K_5 subdivisions give K_5 minors and $K_{3,3}$ subdivisions give $K_{3,3}$ minors. If we contract the paths in subdivisions to single edges, we get the respective minors.

Conversely, a $K_{3,3}$ minor will give a $K_{3,3}$ subdivision. But a K_5 minor can give either a K_5 or $K_{3,3}$ subdivision (depending on if a vertex in the minor is the result of contracting). □

Theorem (*Graph Minors Theorem*)

Every minor-closed property is characterized by a finite list of forbidden minors.

Definition (*colouring*)

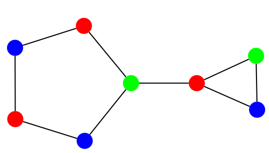
Assignment of one of k colours to the vertices of G such that no two adjacent vertices have the same colour. If G has a k-colouring, it is <u>k-colourable</u>.

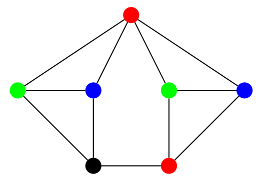
Equivalently, partition $V(G)$ into k sets such that for all edges $uv \in E(G)$, u and v are in different sets. When $k = 2$, this is bipartiteness.

Clearly, every graph is $|V(G)|$-colourable, so we are interested in the minimum k such that G is k-colourable.

Definition (*chromatic number*)

The minimum $\chi(G)$ such that G is $\chi(G)$-colourable.

Example 30.1.  has chromatic number 3.

Example 30.2.  is clearly not bipartite (has triangle) and trying to 3-colour gives a contradiction, so $\chi(G) \geq 4$ and in fact we can colour it to get $\chi(G) = 4$.

If we fix k, consider the decision problem of k-colourability. This is in NP, since we can just show the colouring. It is probably not in $\mathsf{co\text{-}NP}$ because if it were, we could show $\mathsf{P} \neq \mathsf{NP}$ because it is NP-complete.

Theorem (*Four-Colour Theorem*)

Every planar graph is 4-colourable.

Proof. Pain. □

We settle for the next best things: the Six- and Five-Colour Theorems.

Lemma (*7.5.5*)

Every planar graph has a vertex of degree at most 5.

Proof. Suppose a planar graph G exists where every vertex has degree 6 or greater. Then, $|V(G)| \geq 7$. By Theorem 7.5.3, since $|V(G)| \geq 3$, we have $|E(G)| \leq 3|V(G)| - 6$, i.e., $2|E(G)| \leq 6|V(G)| - 12$.

But by the Handshaking Lemma, $2|E(G)| = \sum_{v \in V(G)} \deg(v) \geq 6|V(G)|$, a contradiction. □

Theorem (*Six-Colour Theorem*)

Every planar graph is 6-colourable.

Proof. Proceed by induction on $|V(G)|$.

If $|V(G)| = 1$, then G is 1-colourable.

Suppose $|V(G)| \geq 2$. Then, by Lemma 7.5.5, there exists a vertex v of G with $\deg(v) \leq 5$.

Let $G' = G - v$. Note that $|V(G')| < |V(G)|$ and G' is planar.

Then, by induction, there exists a 6-colouring $\phi : V(G') \to [6]$ of G'. But since $\deg(v) < 6$, there exists $c \in [6] \setminus \{\phi(u) : u \in N_G(v)\}$. Define $\phi(v) = c$ and ϕ is a 6-colouring for G.

Therefore, by induction, every planar graph is 6-colourable. □

Lecture 31 (11/23)

Theorem (*Five-Colour Theorem*)

Every planar graph is 5-colourable.

Proof. Proceed by induction on $|V(G)|$.

If $|V(G)| = 1$, then G is 1-colourable.

Suppose $|V(G)| \geq 2$. Then, by Lemma 7.5.5, G has a vertex v with $\deg(v) \leq 5$.

If $\deg_G(v) \leq 4$, let $G' = G - v$. Since $|V(G')| = |V(G)| - 1 < |V(G)|$, by induction, G' is 5-colourable. Let ϕ be a 5-colouring of G' and extend it so that $\phi(v) \in [5] \setminus \operatorname{im}_\phi(N_G(v))$ which exists since $|N_G(v)| \leq 4$. Then, ϕ is a 5-colouring of G.

Otherwise, $\deg_G(v) = 5$. Since G is planar, G does not contain K_5 as a subgraph. Therefore, of the five neighbours of v, there exist two, a and b, that are not adjacent in G.

Let $G' = G/\{av, bv\}$, i.e., merge a, b, and v into a new vertex z. Then, $|V(G')| = |V(G)| - 2 < |V(G)|$ and since planarity is closed under contraction, we have by induction that G' is 5-colourable.

Let ϕ be a 5-colouring of G'. Construct $\phi' : G \to [5]$:

$$\phi'(x) = \begin{cases} \phi(x) & x \in V(G) \setminus \{a, b, v\} \\ \phi(z) & x \in \{a, b\} \\ c \in [5] \setminus \operatorname{im}_{\phi'}(N_G(v)) & x = v \end{cases}$$

and verify this is a colouring.

Let $e = xy \in E(G)$.

If $x, y \in V(G) \setminus \{a, b, v\}$, then $\phi'(x) = \phi(x) \neq \phi(y) = \phi'(y)$ since ϕ is a colouring on G'.

If $x \in V(G) \setminus \{a, b, v\}$ and $y \in \{a, b\}$ then $\phi'(x) = \phi(z) \neq \phi(y) = \phi'(y)$.

If $x = v$ and $y \in N_G(v)$, then $\phi'(x) \neq \phi'(y)$ by construction.

Note that $e \neq ab$ because we chose a and b not adjacent. $\square$

Generalizing the Four-Colour Theorem (NOT COURSE CONTENT)

Is there a generalization of the Four-Colour Theorem to all graphs?

Notice that $\chi(K_n) \leq n$ since every vertex can get at most one colour and $\chi(K_n) \geq n$ since any vertex is adjacent to all others. Then, $\chi(K_n) = n$.

Hajós' Conjecture. If G does not contain a subdivision of K_t as a subgraph, then G is $(t-1)$-colourable.

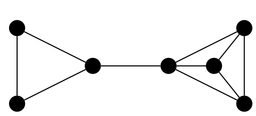
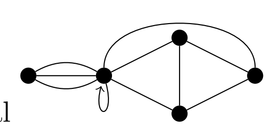
This was proven false for all $t \geq 7$ and almost every graph is a counterexample. In fact, $\frac{t^2}{\sqrt{\log t}} \leq \max \chi(G) \leq t^2$ so not even on the right order of magnitude.

Hadwiger's Conjecture. If G does not contain K_t as a minor, then G is $(t-1)$-colourable.

This is proved for $t \leq 6$ but open for $t \geq 7$. For general t, $\max \chi(G) \leq t(\log \log t)$ due to Delcourt–Postle.

Definition (*dual*)

Given a planar graph G, G^* is a planar multigraph where $V(G^*) = F(G)$ and then for every $e \in E(G)$, draw an edge e^* in G^* crossing e and connecting the faces of G to the left and right of e in G.

Example 31.1.  has a dual 

Note: this is a multigraph, so loops can be created by crossing bridges and parallel edges if two faces share more than one edge.

It is planar, so it satisfies Euler's Formula.

Observe that handshaking for G^* is equivalent to faceshaking for G.

If G is connected, then $(G^*)^* = G$.

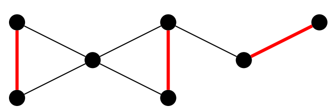
Chapter 8

Matchings

Lecture 32 (11/25)

Definition (*matching*)

On a graph G, a set of edges $M \subseteq E(G)$ such that no two edges share a common endpoint.

Example 32.1.  is a matching.

Definition

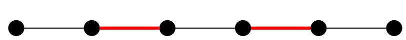
M saturates v if v is an end of an edge in M.
M is perfect if every vertex of G is saturated by M.
The size of M is the number of edges it contains, i.e., $|M|$.
M is a maximum matching if it has maximum size over all matchings of G.

Notice that a perfect matching obviously cannot exist for components an odd number of vertices.

Finding a perfect matching is in NP (just give the matching), co-NP (since CO 250 expresses this as a linear program), and P (for proof, take CO 342).

Definition (*alternating*)

Given a matching M of G, a path P in G is M-alternating if every other edge of P is in M. Equivalently, all $v \in V(P)$ are saturated by M.

Example 32.2. The path  is M-alternating.

Definition (*augmenting*)

A path P which is M-alternating and whose ands are not saturated by M.

Lemma (*8.1.1*)

Let G be a graph with matching M. If there exists an M-augmenting path, then M is not a maximum matching.

Proof. Let P be an M-augmenting path. Then, $M' = M \triangle E(P)$ is a larger matching of G. This is because, starting from the unsaturated ends, flip the exactly one incident edges to the other incident edge which exists because the degree of vertices on a path are exactly two. Finally, $|M'| > |M|$ because $|E(P) \setminus M| > |E(P) \cap M|$ by definition of M-augmenting. $\square$

Lemma (*converse of Lemma 8.1.1*)

Let G be a graph with matching M. If M is not a maximum matching, then there exists an M-augmenting path of G.

Proof. Let M' be a maximum matching of G. Consider $M \triangle M'$. For example, the matchings M and M'

have symmetric difference $M \triangle M'$

Observe that since M and M' are matchings, then $M \triangle M'$ is a disjoint union of M-alternating paths (or M'-alternating paths).

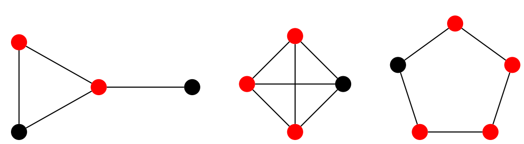
Let $P_1, \dots, P_k$ be the components of $M \triangle M'$. If the ends of P_i are saturated by M' (i.e., $|E(P_i) \cap M'| > |E(P_i) \cap M|$), then P_i is an M-augmenting path as desired.

Otherwise, $|M'| = |M' \cap M| + \sum |E(P_i) \cap M'| \leq |M' \cap M| + \sum |E(P_i) \cap M| = |M|$, a contradiction. $\square$

Lecture 33 (11/28)

Definition (*cover*)

A set $X \subseteq V(G)$ such that every edge of G has at least one end in X.

Example 33.1.  have covers in red.

Every graph has the obvious cover $X = V(G)$.

Definition (*minimum cover*)

A cover of minimum size (i.e., $|X|$), which exists because $V(G)$ is a cover.

Notice that in Example 33.1, the first and second covers are minimal.

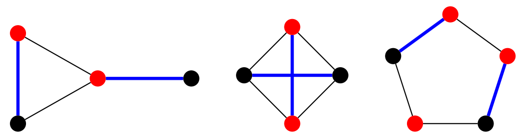
Determining if a graph has a cover of size k is obviously in NP. It is in fact NP-complete, so it is not in $\mathsf{co\text{-}NP}$ or P (assuming $\mathsf{P} \neq \mathsf{NP}$).

Lemma (*8.2.1*)

Let M be a matching and C be a cover of the graph G. Then, $|M| \leq |C|$.

Proof. Let e_i be the edges of M. For each edge, at least one of the two incident vertices must be covered by C. Therefore, $|C| \geq \sum |C \cap e_i| \geq \sum 1 = k = |M|$. $\square$

Corollary. Let G be a graph, M be a maximum matching of G, and C be a minimum cover of G. Then, $|M| \leq |C|$.

Example 33.2.  have minimum covers in red and maximum matchings in blue.

How many graphs have the property that $|M| = |C|$? We must exclude subgraphs of C_{2n+1} since the minimum cover is $n+1$ but the maximum matching is n.

Theorem (*König's Theorem*)

Let G be a bipartite graph, M be a maximum matching of G, and C be a minimum cover of G. Then, $|M| = |C|$.

Lemma (*8.2.2*)

Let G be a graph, M be a matching of G, and C be a cover of G. If $|M| = |C|$, then M is a maximum matching and C is a minimum cover.

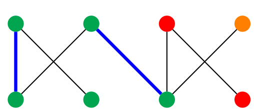
Proof. Let M' be a matching of G. Since C is a cover, then by Lemma 8.2.1, $|M'| < |C|$. Since $|C| = |M|$, then $|M'| < |M|$ and M is maximum, as desired.

Likewise, let C' be a covery of G. Then, by Lemma 8.2.1, $|M| \leq |C'|$. Since $|M| = |C|$, then $|C| \leq |C'|$ and $|C| \leq |C'|$ for all covers, meaning C is minimum, as desired. $\square$

Lecture 34 (11/30)

Definition (*reachability*)

Given a graph G with matching M and $v \in V(G)$, a vertex u is M-reachable from v if there exists an M-alternating u, v-path of G. For a set $S \subseteq V(G)$, u is M-reachable from S if there exists a $v \in S$ such that u is M-reachable from v.

Example 34.1.  has a set of vertices that are M-reachable from v. and a set of M-unreachable vertices.

Recall König's Theorem.

Proof. Let G be a graph with bipartition (A, B).

Let M be a maximum matching of G and U be the set of M-unsaturated vertices of G.

Let $X_0 = U \cap A$.

First, suppose $X_0 = \varnothing$. Let $C := A$. Then, A is a cover of G because every edge has exactly one end in A. Also, since $X_0 = \varnothing$, we have that $|C| = |A| = |M|$ because every vertex of A is M-saturated.

By Lemma 8.2.2, it follows that M is maximum, C is minimum, and $|M| = |C|$ as desired.

Assume $X_0 \neq \varnothing$. Let $X \subseteq A$ and $Y \subseteq B$ be the M-reachable vertices from X_0. Define $C := (A \setminus X) \cup Y$. We claim that (1) C is a cover and then that (2) $|C| = |M|$.

Suppose for a contradiction C is not a cover, i.e., there exists $e = uv \in E(G)$ where $u, v \notin C$. WLOG assume $u \in A$, $v \in B$. Then, since $u, v \notin C$, we have $u \notin A \setminus X$, so $u \in X$. That is, u is M-reachable from X_0. We also have $v \notin Y$, so v is not M-reachable from X_0.

Let P be an M-alternating u, x-path for some $x \in X_0$. Then, since v is not M-reachable, $v \notin V(P)$.

Let $P' = P + uv$. The edge of P incident with x is not in M since $x \in X_0$ is M-unsaturated. Then, $|E(P)|$ is even because $u, x \in A$, so we know that the edge of P incident with u is in M. Therefore, P' is an M-alternating u, v-path, so $v \in Y$. This is a contradiction, giving us (1).

Claim now (2a) that $Y \cap U = \varnothing$. Suppose that $Y \cap U \neq \varnothing$. Let $w \in Y \cap U$. Since $w \in Y$, there is an M-alternating w, x-path P for some $x \in X_0$. But then $w \in U$ and $x \in U$ and hence P is M-augmenting, contradicting Lemma 8.1.1 since M is a maximum matching. Therefore, every vertex of Y is M-saturated, i.e., (2a).

Finally, suppose there exists $e = ab \in M$ where $b \in Y$ and $a \in A \setminus X$. Then, there exists an M-alternating b, x-path P for some $x \in X_0$. This path has odd length because it goes from A to B. It starts on $x \in U$, so the last edge is not in M. Again, we can now take $P' = P + ba$ to get a contradicting M-alternating path. Therefore, (2b) no edge from $A \setminus X$ to Y exists.

Now, recall that $(A \setminus X) \cap U = \varnothing$ since $U \cap A = X_0 \subseteq X$. That is, every vertex in $A \setminus X$ is M-saturated. Finally (actually this time), by (2b), notice that all edges from $A \setminus X$, i.e., the saturated edges of the matching, must then go to $B \setminus Y$.

Let $M_1 \subseteq E(M)$ have ends in Y and $M_2 \subseteq E(M)$ have ends in $A \setminus X$. From before, there does not exist edges from $A \setminus X$ to Y, so $M_1 \cap M_2 = \varnothing$. Yet $C = (A \setminus X) \cup Y$ is a cover. So $M \subseteq M_1 \cup M_2$ and in fact $M = M_1 \cup M_2$. But by (2a), $Y \cap U = \varnothing$, so $|M_1| = |Y|$. Similarly $|M_2| = |A \setminus X|$.

Finally (for the third time), $|M| = |M_1| + |M_2| = |Y| + |A \setminus X| = |C|$, i.e., (2).

Then, since (1) and (2) hold, by Lemma 8.2.2, it follows that M is maximum and C is minimum, as desired. □

Lecture 35 (12/02; missing)

XY Algorithm

Lecture 36 (12/05)

Theorem (*Hall's Theorem*)

> Let $G = (A, B)$ be a bipartite graph. Then, G has a matching saturating every vertex of A if and only if $\forall D \subseteq A, |D| \leq |N(D)|$ where $N(D) = \bigcup_{v \in D} N(v)$.

Proof. Suppose G has a matching M saturating every vertex of A. Let $D \subseteq A$. Then, let $X := \{u \in B : \exists v \in A, uv \in M\}$. Since M is a matching, $|X| = |D|$. But $X \subseteq N(D)$, so $|D| \leq |N(D)|$, as desired.

Suppose that there exists a matching saturating A. Recall that by König's Theorem, the size of a maximum matching is equal to the size of a minimum cover.

Let C be a (possibly minimum) cover of G. Then, because G is bipartite, there does not exist an edge $e = ab$ where $a \in A \setminus C$ and $b \in B \setminus C$. It follows that $N(A \setminus C) \subseteq B \cap C$.

Then, $|A \setminus C| \leq N(A \setminus C) \leq |B \cap C|$ because $A \setminus C$ is a subset of A.

Finally, $|A| = |A \cap C| + |A \setminus C| \leq |A \cap C| + |B \cap C| = |C|$. Therefore, a minimum cover has size at least $|A|$. By König's, a maximum matching has size at least $|A|$ and the matching saturates all of A by bipartiteness. $\square$

Note: König's and Hall's theorems show that for a bipartite graph $G = (A, B)$, deciding if there exists a matching saturating all of A is in co-NP.

Corollary (8.6.1). A bipartite graph $G = (A, B)$ has a perfect matching if and only if $|A| = |B|$ and $\forall D \subseteq A, |D| \leq |N(D)|$.

Proof. Suppose G has a perfect matching M. Then, $|A| = |B|$ by bipartiteness and $\forall D \subseteq A, |D| \leq |N(D)|$ as in Hall's Theorem.

Suppose $|A| = |B|$ and $\forall D \subseteq A, |D| \leq |N(D)|$. Then, by Hall's Theorem, there exists a matching saturating A. But since $|A| = |B|$, M must be perfect by bipartiteness. $\square$

Theorem (*8.6.2*)

All k-regular bipartite graphs with $k \geq 1$ have perfect matchings.

Proof. By Corollary 8.6.1, it suffices to show that $|A| = |B|$ and $\forall D \subseteq A, |D| \leq |N(D)|$. Since G is bipartite,

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

But by k-regularity,

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

and $|A| = |B|$ since $k \geq 1$.

Let $D \subseteq A$. Then, $\sum_{v \in D} \deg(v)$ is the number of edges with one end in D, which is at least the number of edges with one end in $N(D)$, i.e., $\sum_{v \in N(D)} \deg(v)$. As above, this gives us $k|D| \leq k|N(D)| \implies |D| \leq |N(D)|$, as desired. $\square$

Theorem

Given a bipartite graph $G = (A, B)$ and integer $k \geq 1$ such that every vertex in A has degree at least k and every vertex in B has degree at most k, then G has a matching saturating A.