Math 240

Dr. Evan DeCorte http://www.math.mcgill.ca/~edecorte/math240/

Intro 5

Symbols 5

Lecture 1 – 2016/09/07 6

Propositional Logic 6

Logic Laws 6

Contrapositive Examples 6

Lecture 2 – 2016/09/09 7

Conditionals 7

Lecture 3 – 2016/09/12 8

Translation Examples 8

Translation Recap 8

Equivalence, Converse, & Contrapositive 8

Lecture 4 – 2016/09/14 9

Tautologies, Contradictions, & Contingencies 9

Lecture 5 – 2016/09/16 10

Sets 10

Set operations 10

Lecture 6 – 2016/09/19 11

Order of precedence for logical connectives 11

Set Identities 11

List 11

Predicate Logic 11

Lecture 7 – 2016/09/21 12

Predicate Logic (cont) 12

Lecture 8 – 2016/09/23 13

Negations in Predicate Logic (cont) 13

Negations of existential statements 13

Lecture 9 – 2016/09/26 14

Axiomatic system 14

Lecture 10 – 2016/09/28 15
Motivation for axiomatic systems 15
First order theories 15
Applications of Logic 15
Other Logics 15
Lecture 11 – 2016/09/30 16
Mathematical Induction 16
Lecture 12 – 2016/10/03 17
Mathematical Induction (cont) 17
Direct Proof 17
Contrapositive Proof 17
Lecture 13 – 2016/10/05 18
Proof by Contradiction 18
Proof by Cases 18
Divisors 18
Euclid’s Algorithm 18
Lecture 14 – 2016/10/07 19
Euclid’s Algorithm (cont) 19
Congruences 19
Lecture 15 – 2016/10/12 20
Modular Arithmetic 20
Justification for Arithmetic Mod M 20
Fermat’s Little Theorem 20
Fundamental Theorem of Arithmetic 20
Lecture 16 – 2016/10/14 21
Cryptography Examples 21
RSA encryption 21
Lecture 17 – 2016/10/17 22
Primality Testing 22
Miller-Rabin Test 22
Lecture 18 – 2016/10/19 23
Midterm 23
Number Theory 23
Logic 23

Lecture 19 is a review 23
Lecture 20 – 2016/10/26 24
Lecture 21 – 2016/10/28 25
  Binomial Theorem 25
    Special Cases 25
    Pascal's Triangle 25
Lecture 22 – 2016/10/31 26
  Pigeonhole Principle 26
Lecture 23 – 2016/11/02 27
  Pigeonhole Principle Continued 27
  Counting Techniques 27
  Cyclic Orderings 27
Lecture 24 – 2016/11/04 28
  Principle of Inclusion-Exclusion 28
  Intersecting Set Systems 28
Lecture 25 – 2016/11/07 29
  Erdõs-Ko-Rados 29
  Graphs 29
    Examples 29
Lecture 26 – 2016/11/09 30
  Handshaking Lemma 30
  Degrees 30
  Walks & Paths 30
  The first theorem of graph theory 30
Lecture 27 – 2016/11/11 31
  Hamilton Cycles 31
    Thm: Dirac 1952 31
Lecture 28 – 2016/11/14 32
  Subgraphs 32
  Graph Isomorphism 32
  Trees 32
    Spanning Tree 32
Lecture 29 – 2016/11/16 33
  Spanning Trees (cont) 33

Counting Trees 33
Tree Encoding (Prüfer Code) 33
Lecture 30 – 2016/11/18 34
Prüfer codes (cont) 34
Lecture 31 – 2016/11/21 35
Graph Colouring 35
Greedy Algorithm for Colouring 35
Lecture 32 – 2016/11/23 36
Colouring 36
Bipartite Graphs 36
The Marriage Theorem 36
Lecture 33 – 2016/11/25 37
The Marriage Theorem 37
Proof of the Marriage Theorem 37
Planar Graphs 37
Lecture 34 – 2016/11/28 38
Euler's Theorem 38
Lecture 35 – 2016/11/30 39
Map Colouring 39

Intro

- Office hours Friday 11:30-12:30 1120 Burnside
- Math help desk burnside 911 12:00 – 5:00 every weekday
- Grading 20% homework [20% midterm 60% final] [80% final]
- 6 hw assignments, best 5 will count
    - Submit homework to mailbox at room 1005 Burnside before 4:30pm
    - Cite sources if used
- Topics
    - Symbolic Logic – abstract reasoning for true false type questions
    - Number Theory – methodical study of integers and related structures
    - Combinatorics – branch of mathematics which studies finite/discrete things
    - Graph Theory – a graph is a set V, together with another set E consisting of unordered pairs of elements from V
        - Elements of V are called vertices, elements of E are called edges

Symbols

∪	or for sets	∀	universal quantifier
∩	and for sets	∃	existential quantifier
∨	or for logic	¬	negation
∧	and for logic	|	divides
𝟙	always true (proposition)	∤	does not divide
𝟘	always false (proposition)	⊕	exclusive or

Lecture 1 – 2016/09/07

- TA Office hours Monday 11:30 – 12:30 Burnside 1032
- Tutorial tentatively Tue 10:30 – 11:30

Propositional Logic

- Suggested reading: Hammock
- A proposition or statement is an assertion which is either definitely true or definitely false
- Proposition typically denoted with letters, conventionally P, Q, R, … and are called atoms
- Propositional calculus is a language for expressing complex statements, together with a set of rules for deciding whether they are true or false
- Logical connections
  - AND – $P \cap Q$ – conjunction – both true
  - OR – $P \cup Q$ – disjunction – at least one is true
  - NOT – $\neg P$ – negation
  - $\Leftrightarrow$ – equivalence – if and only if
- Truth tables give a way to decide the truth value of a complex statement given the truth values of the atoms used to build it
- Proved that $\neg(\neg P \cup \neg Q) \Leftrightarrow P \cap Q$ and $\neg(\neg P \cap \neg Q) \Leftrightarrow P \cup Q$, known as the DeMorgan laws

Logic Laws

Double negation	$\neg\neg P \Leftrightarrow P$	
Idempotent	$P \cap P \Leftrightarrow P$	$P \cup P \Leftrightarrow P$
Absorption	$P \cup (P \cap Q) \Leftrightarrow P$	$P \cap (P \cup Q) \Leftrightarrow P$
Commutativity	$P \cap Q \Leftrightarrow Q \cap P$	$P \cup Q \Leftrightarrow Q \cup P$
Associativity	$P \cap (Q \cap R) \Leftrightarrow (P \cap Q) \cap R$	$P \cup (Q \cup R) \Leftrightarrow (P \cup Q) \cup R)$
Distributivity	$P \cap (Q \cup R) \Leftrightarrow (P \cap Q) \cup (P \cap R)$	$P \cup (Q \cap R) \Leftrightarrow (P \cup Q) \cap (P \cup R)$

- DeMorgan laws (see above)
- Jump to Set Identities

Contrapositive Examples

- Theorem – let n be an integer; if n^2 is even (P), then n is even (Q)
  - Translation: prove $P \Rightarrow Q$
  - Contrapositive: prove $\neg Q \Rightarrow \neg P$ if n is odd, n^2 is odd
  - True as the product of two odd numbers is always odd
- Theorem – where a & b $\in \mathbb{R}$; if a * b is irrational (P), then either a or b is irrational ($Q \cup R$)
  - Translation: prove $P \Rightarrow (Q \cup R)$
  - Contrapositive: prove $\neg Q \cap \neg R \Rightarrow \neg P$ if a & b are both rational, a * b is rational

- Converse – converse of $P \Rightarrow Q$ is $Q \Rightarrow P$ Not equivalent
  - Ie If a number is divisible by 6, it is even; If a number is even, it is divisible by 6

Lecture 2 – 2016/09/09

- $\mathbb{1}$, T – proposition is always true
- $\mathbb{0}$, F – proposition is always false
- Identity $P \cap T \Leftrightarrow P$ $P \cup T \Leftrightarrow T$
- Domination $P \cap 0 \Leftrightarrow \mathbb{0}$ $P \cup \mathbb{0} \Leftrightarrow P$
- Statements built up from atoms are called sentences (eg $\neg(P \Rightarrow Q) \Rightarrow K$)
- Tautology – sentence which is true for all possible truth values of the atoms
- Contradiction – sentence is false for all possible truth assignments to the atoms
- Contingency – sentence is sometimes true and sometimes false

Conditionals

- If – $P \Rightarrow Q$ – if P then Q, P implies Q, Q if P, Q whenever P, whenever P then also Q, P is sufficient for Q, Q is necessary for P, P only if Q

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

  - $P \Rightarrow Q$ is implication, P is hypothesis, Q is conclusion
  - Implication should only fail if the conclusion is false even though the hypothesis is true
  - When the hypothesis is false, the implication says nothing about the conclusion
  - Cards example E, K, 4, 7 location 1, 2, 3, 4
    - Check implication: vowel on one side ⇒ even number on other side
    - For loc2, hypothesis is false
    - For loc3, conclusion is true
    - Implications are true for loc2 and loc3, therefore we only need to turn over loc1 and loc4

Lecture 3 – 2016/09/12

Translation Examples

- If you study (S), then you will pass (P)
  - $S \Rightarrow P$
  - $P \nRightarrow S$ You can also pass without studying
- You can only make a withdrawal (W) if you have money in your account (A)
  - $W \Rightarrow A$
  - $A \nRightarrow W$ Having money in your account doesn't guarantee you can make a withdrawal
- I cry (C) whenever I see the stars (S)
  - $S \Rightarrow C$
  - $C \nRightarrow S$ You can cry without seeing stars as well
- Alfred only rides his bike (A) when it's sunny (S)
  - $A \Rightarrow S$
  - $S \nRightarrow A$ Just because it's sunny doesn't mean Alfred is riding a bike
- Alfred rides his bike (A) whenever it's sunny (S)
  - $S \Rightarrow A$
  - $A \nRightarrow S$ Alfred could also ride a bike when it's rainy
- The sun is out (S) but it's raining (R)
  - $S \cap R$
- I will cancel the trip ($\neg T$) unless Kate comes along (K)
  - $T \Rightarrow K$ $\neg K \Rightarrow \neg T$
  - $K \nRightarrow T$ If Kate decides to come, the trip may still be cancelled
- To learn logic (L), all you have to do is pay attention (P)
- Paying attention (P) is sufficient for learning logic (L)
  - $P \Rightarrow L$
  - $L \nRightarrow P$ There may be other ways to learn logic; if you learned, you might not necessarily have paid attention
- If you only study (S) when you are under pressure (P), you will not learn ($\neg L$)
  - $(S \Rightarrow P) \Rightarrow \neg L$
  - Split this into two parts when translating

Translation Recap

- If A, then B; Only A if B; A is sufficient for B; $\neg A$ unless B $A \Rightarrow B$
- A whenever B; to A, do B $B \Rightarrow A$
- When finding which proposition is necessary, use the truth table
  - If A can be true while B is false, $A \nRightarrow B$
- Just because your translation is true doesn't mean it has the same meaning as the given statement

Equivalence, Converse, & Contrapositive

- Equivalence – P if and only if Q – $P \Leftrightarrow Q$ – $(P \Rightarrow Q) \cap (Q \Rightarrow P)$
- Contrapositive – for $P \Rightarrow Q$, is $\neg Q \Rightarrow \neg P$
  - The two above are equivalent; sometimes the contrapositive is easier to prove

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Lecture 4 – 2016/09/14

- Theorem – proven mathematical fact

Tautologies, Contradictions, & Contingencies

- $P \cap (P \cup Q)$ → (absorption rule) P → contingency
- Checking by truth table takes a lot of time; instead, consider using rules of logic
- $P \cup (P \cap Q) \cup (P \Rightarrow Q)$

	Rule used
$\equiv P \cup (P \cap Q) \cup (\neg P \cup Q)$	$(P \Rightarrow Q) \equiv \neg P \cup Q$
$\equiv P \cup (\neg P \cup Q)$	absorption
$\equiv (P \cup \neg P) \cup Q$	associativity
$\equiv \mathbb{1} \cup Q$	complementarity
$\equiv \mathbb{1}$	domination
Tautology	

- Island of knights & knaves – knights always tell truth; knaves always lie
  You meet two inhabitants, A & B; A says "Either I am knave, or B is knight"
  What are A & B?
    - Atoms: P – A is knight, Q – B is knight
    - Translation: $P \Leftrightarrow \neg P \cup Q$
    - From truth table: contingency

Lecture 5 – 2016/09/16

- Continuation of Knights & Knaves
- A says, “I’m a knave, but B isn’t”
- $P \Leftrightarrow \neg P \cap Q$
- $P \cap (\neg P \cap Q) \cup (\neg P \cap \neg(\neg P \cap Q))$ $X \Leftrightarrow Y \rightarrow (X \cap Y) \cup (\neg X \cap \neg Y)$
- $\equiv \mathbb{O} \cup (\neg P \cap \neg(\neg P \cap Q))$ associativity
- $\equiv \neg P \cap (\neg\neg P \cup \neg Q)$ complementarity
- $\equiv (\neg P \cap P) \cup (\neg P \cap \neg Q)$ distributivity
- $\equiv \neg P \cap \neg Q$ A and B must both be knaves

Sets

- Collection of distinct objects called elements
- Examples
  - $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$
  - $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
  - $\mathbb{Q} = \{a/b: a, b, \in \mathbb{Z}, b \neq 0\}$
  - $\mathbb{R}$ = set of real numbers
- $\emptyset = \{\}$, the empty set
- U denotes the entire universe (all things)
- $X \in A \rightarrow$ x is an element of set A $X \notin A \rightarrow$ x is not an element of set A
- Subset – $A \subseteq B$ – A is a subset of B if every element of A is an element of B
- Superset – $B \supseteq A$ – if A is a subset of B, B is a superset of A
  - $\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- Cardinality – number of elements of set
  - $|A| = \#$ $|\emptyset| = 0, |\mathbb{Z}| = \infty$

Set operations

- (of sets A and B)
- *Note $\wedge$ = and for logic, $\cap$ = and for sets
  $\vee$ = or for logic, $\cup$ = or for sets
- Intersection – set of all elements belonging to both A and B
  - $A \cap B = \{x: x \in A \wedge x \in B\}$
- Union – set of elements contained in either A or B
  - $A \cup B = \{x: x \in A \vee x \in B\}$
- Difference – set of elements in A that aren’t in B
  - $A \setminus B = A - B = \{x: x \in A, x \notin B\}$
  - $A \setminus B$ is sometimes called the complement of B in A
- Symmetric difference – set of elements contained either in A or in B, but not both (exclusive “or”)
  - $A \Delta B = \{x: x \in A \cup B, x \notin A \cap B\}$

Lecture 6 – 2016/09/19

Order of precedence for logical connectives

- No standard agreement, but the following will be used
- $\neg \gg \cup, \cap \gg \Rightarrow, \Leftarrow \gg \Leftrightarrow$
- $\neg A \cup B \Rightarrow C$ becomes $(((\neg A) \cup B) \Rightarrow C)$
- Avoid ambiguous notation such as $A \cap B \cup C$
  - Due to association, parentheses are sometimes dropped in cases like $A \cap B \cap C$

Set Identities

- Theorem $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (law of distributivity)
- Proof – to show $X = Y$, show $X \equiv Y$ and $Y \equiv X$
  - ■ is a symbol for the end of a proof
- Show $A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$
  - Take arbitrary $x \in A \cap (B \cup C)$
  - $\therefore x \in A \;\&\; x \in B \cup C$
  - Case 1 – $x \in B$ $x \in A \cap B$
  - Case 2 – $x \in C$ $x \in A \cap C$
  - Both cases result in the RHS of the theorem ■
- Show $(A \cap B) \cup (A \cap C) \equiv A \cap (B \cup C)$
  - Take arbitrary $x \in (A \cap B) \cup (A \cap C)$
  - Case 1 – $x \in A \cap B$ $x \in B \rightarrow x \in B \cup C$
  - Case 2 – $x \in A \cap C$ $x \in C \rightarrow x \in B \cup C$
  - Given that $x \in A$, both cases result in the LHS of the theorem ■

List

- Jump to logic laws
- U = universe

Identity Laws	$A \cap U = A$, $A \cup U = U$
Idempotent Laws	$A \cap A = A$, $A \cup A = A$
Complement Laws	$A \cap \neg A = \mathbb{0}$, $A \cup \neg A = U$
Domination Laws	$A \cap \mathbb{0} = \mathbb{0}$, $A \cup \mathbb{0} = A$
Commutative Laws	$A \cap B = B \cap A$, $A \cup B = B \cup A$
Associative Laws	$A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$
De Morgan's Laws	$\neg(A \cap B) = \neg A \cup \neg B$, $\neg(A \cup B) = \neg A \cap \neg B$
Double Complement Law	$\neg\neg A = A$
Absorption Laws	$A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$
Distributive Laws	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Predicate Logic

- Predicates are like T/F valued functions, with a variable as an input
- Predicates make a statement about every possible variable; is a conjunction of infinitely many statements
- Theorem: for every integer $n \geq 1$, sum $1 + 3 + 5 + \ldots + (2n + 1)$ is a perfect square

Lecture 7 – 2016/09/21

- Rules of logic example
    - $\neg Q \wedge \neg(P \Rightarrow Q)$ note that $A \Rightarrow B \equiv \neg A \vee B$
    - $\equiv \neg Q \wedge \neg(\neg P \vee Q)$
    - $\equiv \neg Q \wedge (O \wedge \neg Q)$
    - $\equiv P \wedge \neg Q$

Predicate Logic (cont)

- Recall previous lecture
- $\forall$ is the universal quantifier ("for all")
- Example
    - $C(x)$; x is cardinal, $R(x)$: x is red
        - "All cardinals are red" → $\forall x(C(x) \Rightarrow R(x))$
    - $N(x)$: x is number
        - $\forall x \forall y[N(x) \wedge N(y) \wedge y \neq 0 \Rightarrow N(x \div y)]$ → "if x & y are numbers & $y \neq 0$, then $x \div y$ is number"
    - "If it rains, every person will get wet"
        - R: it rains, $P(x)$: x is a person, $W(x)$: x will get wet
        - $R \Rightarrow \forall x(P(x) \Rightarrow W(x))$
    - "Not everything is about you"
        - $Y(x)$: x is about you
        - $\neg \forall x Y(x)$
- You can name things in universe, usually w/ lower case letters, and use them as constants
    - b: barkeeper, $B(x)$; x is busy → $B(b)$ → "the barkeeper is busy"
- Predicates can take more than one argument → called relations
    - $I(x, y)$: x asks y for ID, $W(x)$: x is person who wants wine, b: barkeeper
        - $\forall y(W(y) \Rightarrow I(b, y))$ → "if person wants wine, barkeeper will ID that person"
- $\exists$ is the existential quantifier ("there exists")
    - $E(x)$: x is even number, $P(x)$: x is prime number
        - "There exists an even number which is also prime" → $\exists x(E(x) \wedge P(x))$
    - $F(x, y)$: x & y are friends, b: barkeeper
        - "The barkeeper has a friend" → $\exists y F(b, y)$
- Predicate logic can have functions – can take anything in universe as arguments – take values in universe – can take more than one argument
    - $F(x)$: father of x, b: barkeeper
        - $F(b)$ → "father of barkeeper"
    - $P(x, y)$: $x + y$
- Negation
    - "Every even number > 2 can be written as sum of 2 prime numbers"
        - $E(x)$: x is even number, $P(x)$: x is prime number, $x > y$: x greater than y, $x + y$: $x + y$, 2: 2

Lecture 8 – 2016/09/23

Negations in Predicate Logic (cont)

- To say that $\forall x P(x)$ is false, prove that $P(x)$ is false for at least one x, where $x \in \forall$
  - $\neg\forall x P(x)$ is an existential statement $\neg\forall x S(x) \equiv \exists x \neg S(x)$
- "All cardinals are red"
  - $C(x)$: x is cardinal, $R(x)$: x is red
  - $\forall x(C(x) \Rightarrow R(x))$
  - Negation – "there is a cardinal who is not red"
    - $\exists x \neg(C(x) \Rightarrow R(x))$
    - $\exists x \neg(C(x) \wedge \neg R(x))$

Negations of existential statements

- $\neg\exists x S(x) \equiv \forall x \neg S(x)$
- "Charles has a smartphone"
  - $C(x)$; x belongs to Charles, $S(x)$: x is a smartphone
  - $\exists x(C(x) \wedge S(x))$
  - Negation – "Charles does not have a smartphone"
    - There is no x where $x \in \forall$ that fits $C(x) \wedge S(x)$
    - $\forall x \neg(C(x) \wedge S(x))$ $\forall x(S(x) \Rightarrow \neg C(x))$
- "Everyone has a friend"
  - $F(x, y)$: x and y are friends, $U = \{\text{all people}\}$
  - $\forall x \exists y F(x, y)$
  - Negation – "there exists someone with no friends"
    - $\neg\forall x \exists y F(x, y) \equiv \exists x \neg\exists y F(x, y) \equiv \exists x \forall y \neg F(x, y)$

- Order of quantification matters $\forall x \exists y S(x, y) \not\equiv \exists y \forall x S(x, y)$
  - Ie "Everyone has a friend" ≢ "There is someone who is friends with everyone"
- Vacuously true statements
  - Consider $\forall x(P(x) \Rightarrow Q(x))$, where $P(x)$ is false for all $x \in U$
    - ∵ implications w/ false hypotheses are true
    - ∴ $\forall x(P(x) \Rightarrow Q(x))$ is vacuously true

Lecture 9 – 2016/09/26

Axiomatic system

- Set of basic axioms (assumptions) which can be combined using logic to deduce theorems
- Euclidean high school geometry may be the first example of an axiomatic system
  - 300 BC – 5 axioms
  - A1 – there are at least two points
  - A2 – for any two distinct points, there is exactly one line passing through them
  - A3 – for each line L, there is a point not on L
  - A4 – if L is a line & x is a point not on L, then there is exactly one line through x parallel to L
    - Lines L and L' are parallel if they never intersect
- Proofs with axioms
  - Theorem – every point is on at least two lines
    - Take any point x
    - By A1, there is another point $y \neq x$
    - By A2, there is a line L through x and y
    - By A3, there is a point $z \notin L$
    - By A2, there Is a line L' through x and z
    - $\because z \in L' \cap z \notin L$
    - $\therefore L \neq L'$ x is on (at least) two distinct lines
  - Theorem – every line has at least two points
    - Take any line L
    - By A3, there is a point $x \notin L$
    - By previous theorem, x lies on two distinct lines L_1 & L_2
    - By A4, at most one of L_1 & L_2 can be parallel to L (Let's say $L_2 \nparallel L$)
    - By definition of parallel, there is a point y that intersects both L & L_2
    - By A3, there is a point z not on L_2
    - If $z \in L$, proof is done
    - If $z \notin L$, by A4, there is a line L' through z & $\parallel L_2$
      - $L' \nparallel L$, as otherwise there would be two lines passing through y & $\nparallel L'$
    - By definition of parallel, there is a point w that intersects both L' & L
    - $\because L' \parallel L_2 \cap w \in L' \cap y \in L_2$
    - $\therefore w \neq y$ two distinct points on L
- Russell's paradox
  - Define set R to be set of all sets which do not belong to themselves
  - $R = \{x: x \notin x\}$
  - Then $R \in R \Leftrightarrow R \notin R$
  - To avoid this, Zermelo–Fraenkel defined collection of natural axioms for set theory

Lecture 10 – 2016/09/28

Motivation for axiomatic systems

- Make proof-checking automatic (ie doable by computer)
- Automatic theorem proving
- Block paradoxes by limiting expressive power (ie Russell's paradox)

First order theories

- Essentially all of mathematics is based on Zermelo–Fraenkel axioms for set theorem.
    - Chose to formulate axiomatic system in predicate (first-order) logic
    - Has signature of ∈ (binary relation) and ∅ (empty constant)
- Usually comes with signature – list of allowed predicates, relations, constants, and functions
- Language – set of all sentences of predicates one can make from the signature
- Language of set theory example
    - $\forall x \exists y \forall u(u \in y \Leftrightarrow \exists z(z \in x \land u \in z))$ axiom of union
- Theory – set of all sentences derivable from given set of axioms
- Predicate logic comes with system of rules for formal deduction, allowing for automatically checkable proofs
- Abbreviation scheme – gives meaning to signature; not necessary in creating language, but helps other readers
- Example of formalized theory of geometry
    - Signature – P(x), L(x), I(x, y)
    - Abbreviation scheme – P(x): x is a point, L(x): x is a line, I(x, y): P(x) is on L(y)
    - Lines l & l' intersect $\exists x(P(x) \land I(x, l) \land I(x, l'))$

Applications of Logic

- AI (ie automatic theorem proving)
- Software verification
- Programming language theory (ie compiler design, translation)
- Puzzles
- Law
- Math (ie Russell's paradox)

Other Logics

- Second-order (and higher-order) logic – allows for quantification over predicates
- Modal logic (ie symbols for necessarily P, possibly P)
- Fuzzy logic – truth not 0/1, but rather values in interval [0, 1]
- Temporal logic – "I will be hungry until I eat"

Lecture 11 – 2016/09/30

Mathematical Induction

- Strategy: proving $P(n)$ for all $n \geq 1 \equiv$ proving $P(1)$ & proving $P(n) \Rightarrow P(n+1)$ for all $n \geq 1$
    - As a result, $P(n-1) \Rightarrow P(n)$, $P(n-2) \Rightarrow P(n-1)$ … $P(1) \Rightarrow P(2)$, $P(1) \equiv T$; all are true
- Theorem: for any $n \geq 1$, sum of first n odd numbers is equal to n^2
    - $P(1) = 1 = 1^2$
    - Induction $\forall n(P(n) \Rightarrow P(n+1))$
        - We can assume that the theorem is true for n (induction hypothesis)
          $1 + 3 + 5 + \ldots + (2n-1) = n^2$
        - We need to show that
          $1 + 3 + 5 + \ldots + (2n-1) + (2n+1) = (n+1)^2$
        - ↳ $n^2 + (2n+1) = (n+1)^2$ ■
- Prove that sum of first n positive integers is $n(n+1)/2$
    - Base case $1 = 1 * 2/2$
    - Induction
        - Assume $1 + 2 + 3 + \ldots + n = n(n+1)/2$
        - Prove $1 + 2 + 3 + \ldots + n + (n+1) = (n+1)(n+2)/2$
          ↳ $n(n+1)/2 + (n+1) = \frac{n(n+1)+2(n+1)}{2} = (n+1)(n+2)/2$ ■
- Prove $n(n+1)$ is odd
    - Induction
        - Assume $n(n+1)$ is odd
        - Prove $(n+1)(n+2)$ is odd
          ↳ $(n+1)(n+2) = n(n+1) + 2(n+1) =$ odd + even = odd
    - Proof is wrong, as we didn't do the base case; base case is false for all cases
- Theorem: all horses are the same colour
    - Prove that for each n, every set of n horses has the property that all the horses in it have the same colour
    - Base case $(n = 1)$ – true; only one horse
    - Induction
        - Assume that if $|H| = n$, all horses $\in H$ have same colour
        - Take set H_2 where $|H_2| = n + 1$
          ↳ $H_2 = H + h$, where h is a set of one horse
          ↳ Due to base case & assumption, all have same colour
    - Proof is wrong; problem with base case as $P(1) \nRightarrow P(2)$

Lecture 12 – 2016/10/03

Mathematical Induction (cont)

- Strong induction $\quad P(1) \wedge P(2) \wedge P(3) \wedge \ldots \wedge P(n) \Rightarrow P(n+1)$
  - You can assume any of the $P(a)$ is true when proving; where a is a constant $< n$
- Prove: every nonnegative integer n can be written as $a_k 2^k + a_{k-1} 2^{k-1} + \ldots + a_2 2^2 + a_1 2 + a_0$ With $a_i \in \{0, 1\}$ $\quad$ (prove any whole number can be written in binary)
  - Base case $n = 0$ $\quad$ binary is 0
  - Induction step – suppose n is odd; by induction hypothesis, we can write $n - 1$ as $n - 1 = a_k 2^k + a_{k-1} 2^{k-1} + \ldots + a_2 2^2 + a_1 2 + a_0$ $\quad$ with $a_i \in \{0, 1\}$ for all i
    - $\because n - 1$ is even $\quad \therefore a_0 = 0$
    - n can be written the same as $n - 1$, but with $a_0 = 1$
  - Induction step – suppose n is even; by induction hypothesis, we can write $n/2$ as $n/2 = a_k 2^k + a_{k-1} 2^{k-1} + \ldots + a_2 2^2 + a_1 2 + a_0$ $\quad$ with $a_i \in \{0, 1\}$ for all i
    - $n = 2(a_k 2^k + a_{k-1} 2^{k-1} + \ldots + a_1 2 + a_0) = a_k 2^{k+1} + a_{k-1} 2^k + \ldots + a_1 2^2 + a_0 2$ ■
- Pythagorean theorem – if triangle is a right angled triangle, then $z^2 = x^2 + y^2$
- Fermat's Last theorem – if a, b, c are positive integers & $a^n + b^n = c^n$, then $n \leq 2$
- Direct proof, contrapositive proof, proof by contradiction
- Thm = theorem $\quad$ pf = proof

Direct Proof

- To prove $P \Rightarrow Q$, assume P, deduce Q
- Thm: if $x, y \in \mathbb{R}$, then $2xy \leq x^2 + y^2$
  - Pf: assume $x, y \in \mathbb{R}$ $\quad \because 0 \leq (x - y)^2 = x^2 - 2xy + y^2$ $\quad \therefore 2xy \leq x^2 + y^2$ ■
- Thm: if $a \in \mathbb{Z}$ is odd, then a^2 is odd
  - Pf: if $a \in \mathbb{Z}$ is odd, $a = 2b + 1$ for some $b \in \mathbb{Z}$
    - $\because a^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1$
    - $\therefore a^2$ is odd $\quad$ even $\quad$ odd

Contrapositive Proof

- To prove $P \Rightarrow Q$, prove $\neg Q \Rightarrow \neg P$ $\quad$ assume $\neg Q$, deduce $\neg P$
- Thm: (Pigeonhole principle) if we drop $\geq (n + 1)$ balls into n boxes, then some box gets at least 2 balls
  - Pf: Assume $\neg Q$, every box gets < 2 balls
    - Let x_i = # of balls in box_i $\quad \because x_i \in \{0, 1\}$ $\quad \therefore \sum_{i=1}^{n} x_i \leq n$
    - $\because \sum_{i=1}^{n} x_i < n + 1$ $\quad \therefore \neg P$ ■
- Thm: let $x, y \in \mathbb{R}$ & $x, y \geq 0$; if $xy > 100$, then $x > 10$ or $y > 10$
  - Pf: Assume $\neg Q$, $x \leq 10$ and $y \leq 10$, $xy \leq 100 \rightarrow \neg P$ ■

Lecture 13 – 2016/10/05

Proof by Contradiction

- Aka indirect proofs, reductio ad absurdum
- To prove P, assume $\neg$P, derive contradiction
- Thm: $\sqrt{2}$ is irrational
    - Pf: Assume not – $\sqrt{2}$ is rational, $\therefore \sqrt{2} = p/q$ $p, q \in \mathbb{Z}$
        - Assume p/q is in lowest terms; no common factors
    - $2 = p^2/q^2$ square both sides
    - $2q^2 = p^2$ p^2 is even → p is even
    - $p = 2r$ for some $r \in \mathbb{Z}$
    - $2q^2 = 4r^2 \rightarrow q^2 = 2r^2$ q^2 is even → q is even
    - p & q are therefore not in lowest terms; contradiction ■

Proof by Cases

- Sometimes $P \Rightarrow Q$ breaks up into cases: $(P_1 \lor P_2 \lor P_3 \lor \dots \lor P_k) \Rightarrow Q$
    - Suffice to prove $(P_1 \Rightarrow Q) \land (P_2 \Rightarrow Q) \land (P_3 \Rightarrow Q) \land \dots \land (P_k \Rightarrow Q)$
    - Binary example from last lecture
- Thm: if $n \in \mathbb{Z}$ is not divisible by 3, then $n^2 + 2$ is divisible by 3
    - Pf: if 3 does not divide n, then $n = 3m + 1$ or $n = 3m + 2$, for some $m \in \mathbb{Z}$
    - Case 1 – $n = 3m + 1$
        - $n^2 + 2 = (3m + 1)^2 + 2 = 9m^2 + 6m + 1 + 2 = 3(3m^2 + 2m + 1)$
    - Case 2 – $n = 3m + 2$
        - $n^2 + 2 = (3m + 2)^2 + 2 = 9m^2 + 12m + 4 + 2 = 3(3m^2 + 4m + 2)$
    - All cases are divisible by 3 ■

Divisors

- Let $a, b \in \mathbb{Z}$ if b is multiple of a ($b = ax$ for some $x \in \mathbb{Z}$), then we say "a divides b": $a|b$
- If $a \nmid b$, then there exists an $r \in \mathbb{Z}$, where $1 \leq r < a$ such that $b = ax + r$
    - We say r is the remainder
- If $d|a$ and $d|b$, then d is a common divisor of a and b

Euclid's Algorithm

- Possibly the oldest known algorithm – used to find greatest common divisor (GCD)
- Thm: if $b = ax + r$ $(a, b, x, r \in \mathbb{Z})$ $(0 \leq r < a)$ then $\gcd(b, a) = \gcd(a, r)$
- Pf: $b = ax + r$
    - Show that every divisor of a and r is also a divisor of a and b – $\gcd(a, r) \leq \gcd(a, b)$
        - Suppose $d|a$ & $d|r \rightarrow a = md$ & $r = nd$ $m, n \in \mathbb{Z}$
        - $b = ax + r = mdx + nd = d(mx + n)$ $\therefore d|b$
    - Show that every divisor of a and b is also a divisor of a and r – $\gcd(a, r) \geq \gcd(a, b)$
        - Suppose $d|a$ * $d|b \rightarrow b = md$ & $a = nd$ $m, n \in \mathbb{Z}$
        - $b = ax + r \rightarrow b - ax = r \rightarrow md - ndx = r \rightarrow r = d(m - nx)$ $\therefore d|r$ ■

Lecture 14 – 2016/10/07

Euclid's Algorithm (cont)

- Given number a & b, switch a for b is $b < a$ (a should be the smaller number)
- If $a > 0$, divide b by a for r. Replace b by r and loop again
- If $a = 0$, return b as gcd
- Example: gcd(300, 18)
    - $a = 18, b = 300$ $b/a = 16r12$ → $a = 18, b = 12$
    - $a = 12, b = 18$ $b/a = 1r6$ → $a = 12, b = 6$
    - $a = 6, b = 12$ $b/a = 2r0$ → $a = 6, b = 0$
    - $a = 0, b = 6$ return gcd 6
- Question: which numbers can be written as $ma + nb$ with $a, b, m, n \in \mathbb{Z}$
    - If $x = ma + nb$ & $d = \gcd(a, b)$, then $d|x$
        - If $a = a'd$ & $b = b'd$, $x = ma + nb = ma'd + nb'd = d(ma' + mb')$
        - $\therefore$ divisibility by gcd(a, b) is a necessary condition
    - gcd(a, b) is also a sufficient condition
        - Euclid's algorithm shows how to write gcd(a, b) as $ma + nb$
- Example: find gcd(62, 28) & express as $62m + 28n$ with $m, n \in \mathbb{Z}$
    - $\gcd(62, 28) \to (a, b) \to (28, 62) \to (6, 28) \to (4, 6) \to (4, 2) \to (0, 2) \to$ gcd is 2
    - Do Euclid's algorithm backwards, write r in terms of a and b
        - $62 - 2 * 28 = 6$, $28 - 4 * 6 = 4$, $6 - 4 = 2$
        - $\gcd = 2 = 6 - 4 = 6 - (28 - 4 * 6) = 5 * 6 - 28 = 5(62 - 2 * 28) - 28$
          $= 5 * 62 - 11 * 28$ → $m = 5, n = -11$
    - Note: since gcd = 2, any even number can be written as $62m + 28n$ with $m, n \in \mathbb{Z}$
- If $\gcd(a, b) = 1$, a & b are "relatively prime" or "coprime"
    - If a & b are relatively prime, any integer can be written as $ma + nb$ for $m, n \in \mathbb{Z}$

Congruences

- If a & b give same remainder when divided by m, we say that a & b are congruent modulo m
    - Notation $a \equiv b \pmod{m}$
- If $a \equiv 0 \pmod{b}$, then a is divisible by b
- Thm: $a \equiv b \pmod{m} \Leftrightarrow a - b \equiv 0 \pmod{m}$
    - Pf $\Rightarrow$: if $a = mp + r$, $b = mq + r$, then $a - b = m(p - q)$, $m|(a - b)$
    - Pf $\Leftarrow$: assume $a - b \equiv 0 \pmod{m}$
        - If $a = mp + r$, $b = mq + r'$ with $0 \leq r, r' < m$, then $a - b = m(p - q) + r - r'$
        - $\because m|(a - b)$ $\therefore m|(a - b) - m(p - q)$, $m|(r - r')$
        - $\because 0 \leq r, r' < m$, we have $-m < r - r' < m$, so $r - r' = 0$ ■
- Thm: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
    - Pf: $ac - bd = (a - b)c + b(c - d)$
    - $\because a \equiv b \pmod{m}$ $\therefore a - b \equiv 0 \pmod{m}$
    - $\because c \equiv d \pmod{m}$ $\therefore c - d \equiv 0 \pmod{m}$
    - $\therefore m|ac - bd$, $ac \equiv bd \pmod{m}$ ■

Lecture 15 – 2016/10/12

Modular Arithmetic

- Can be thought of as "arithmetic on the clock"
- Ie It's now 11 o'clock in the morning; what time of the day will it be in 89 hours?
    - $11 + 89 \equiv 4 \pmod{24}$ → it would be 4am
- Ie Today is Wednesday; what day of the week will it be in 104 days
    - Assume Monday = 0 → Wednesday = 2
    - $2 + 104 \equiv 1 \pmod{7}$ → it would be Tuesday
- Can show that equations have no solutions in integers
- Ie Show that $x^2 + y^2 = 211$ has no solutions for $x, y \in \mathbb{Z}$
    - Observe that $0^2 \equiv 0 \pmod{4}$, $1^2 \equiv 1 \pmod{4}$, $2^2 \equiv 0 \pmod{4}$, & $3^2 \equiv 1 \pmod{4}$
    - $\because x^2 \equiv 0$ or $1 \pmod{4}$, $y^2 \equiv 0$ or $1 \pmod{4}$ $\therefore x^2 + y^2 \equiv 0, 1$, or $2 \pmod{4}$
    - $\because 211 \equiv 3 \pmod{4}$ ∴ the equation has no solution

Justification for Arithmetic Mod M

- We know $2 \equiv 7 \pmod{5}$
- Thm: if $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
    - Proved last class; justifies multiplication of congruences
- Thm: if $a\equiv b(\text{mod } m)$ & $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
    - Pf: $(a + c) – (b + d) = (a – b) + (c – d)$ → both divisible by m → $0 \pmod{m}$

Fermat's Little Theorem

- Thm: if p is any prime and a is any integer, then $a^p \equiv a \pmod{p}$
- Useful for computing large powers modulo p
- Ie Find $4762^{5367} \pmod{13}$
    - Note $4762 \equiv 4 \pmod{13}$ → $4762^{5367} \equiv 4^{5367} \pmod{130}$
    - $5367 = 13 * 412 + 11$, using FLT, $4^{5367} \equiv (4^{13})^{412} * 4^{11} \pmod{13}$
    - $\equiv (4^{412})(4^{11}) \pmod{13} \equiv 4^{423} \pmod{13}$
    - $423 = 13 * 32 + 7 \rightarrow (4^{13 * 32 + 7}) \pmod{13} \equiv 4^{39} \pmod{13} \equiv 4^3 \pmod{13}$
    - $\equiv 12 \pmod{13}$ (FLT) (FLT)
- Ie Find $2^{39674} \pmod{523}$
    - Note 523 is prime
    - $39674 = 523 * 75 + 449$ → $\equiv 2^{75 + 449} \pmod{523} \equiv 2^{524} \pmod{523}$
    - $524 = 523 + 1$ → $\equiv 2^{1 + 1} \pmod{523} \equiv 4 \pmod{523}$

Fundamental Theorem of Arithmetic

- Thm: every positive integer can be written as product of primes, and factorization is unique up to the order of the prime factors
- Ie What is the prime factorization of 511? $511 = 7 * 73$
- Ie 8085? $8085 = 3 * 5 * 7^2 * 11$
- How many primes are there? Infinitely many
    - Pf: say we have a finite number of primes; multiplying all of them and adding one would yield in a new prime (it would have remainder 1 when divided by any prime) Contradiction to Fundamental Theorem of Arithmetic ■

Lecture 16 – 2016/10/14

- Applications of number theory – primality testing, cryptography, random number generation

Cryptography Examples

- Substitution cipher – all items get switched with another item (ie a → n, b → c, c → b …)
    - Can be defeated with frequency analysis – matching frequency of common encrypted letters with frequency of actual English letters
        - Most common letters are e, t, a, o, i, …
    - Must use same encrypting permutation for decryption
- Public key cryptography – encryption key is sent to those who need it, but only receiver has decryption key

RSA encryption

- Named after Rivest, Shamir, Adleman
- Receiver generates two prime numbers, p, q, and sets $m = pq$ (More info later)
- Receiver finds two numbers e, d such that $(p - 1)(q - 1)|(ed - 1)$
    - Use Euclidean algorithm to find random e which is relatively prime to $(p - 1)(q - 1)$
    - Find u, v such that $u(p - 1)(q - 1) + ve = 1$
    - Let $d = v \rightarrow de - 1 = -u(p - 1)(q - 1)$ so $(p - 1)(q - 1)|(ed - 1)$
- Receiver publishes m & e; keeps d private
- A “message” in this context is simply a number x, where $0 \leq x < m$
    - So p and q should be sufficiently large
    - Larger messages can be split up into smaller blocks and sent piece by piece
- Sender computes $x^e \pmod{m}$ & sends it
    - More on how to compute x^e later
- Receiver gets $r \equiv x^e \pmod{m}$ and computes $r^d \pmod{m}$
    - $r^d \equiv x \pmod{m}$

Explanation

- Need to show $r^d \equiv x^{ed} \equiv x \pmod{m}$ or $m|x^{ed} - x$
- Fact – for all integers $a > 2$ & $n \geq 1$, $a - 1|a^n - 1$
- Enough to show that $p|x^{ed} - x$ & $q|x^{ed} - x$ [Fundamental theorem of arithmetic]
    - $x^{ed-1} - 1 = x^{l(p-1)} - 1$ for some l Note that $p - 1|ed - 1$
    - $x^{p-1} - 1|x^{l(p-1)} - 1$ Due to fact above
    - $x^p - x|x(x^{l(p-1)} - 1)$ Multiply both sides by x
    - $p|x(x^{l(p-1)} - 1)$ Fermat’s Little Theorem: $p|x^p - x$
    - $p|x^{ed} - x$ $x(x^{l(p-1)} - 1) = x^{ed} - x$
    - Same similarity for $q \rightarrow m|x^{ed} - x \rightarrow x^{ed} \equiv x \pmod{m}$

Dynamic Programming Algorithm for 2^n

- If n is even, take $2^{n/2}$ and square it
- If n is odd, take 2^{n-1} and double it
- If n has k binary bits, 2^n can be found with $\leq 2k$ multiplications
- Note that all exponentiation is mod m

Lecture 17 – 2016/10/17

- RSA security relies on complexity – if you can factor integers quickly, you can crack RSA

Primality Testing

- Idea #1: For $a < n$, check $a|n$ (really slow)
- Idea #2: Fermat's Little Theorem – using contrapositive, if $a^{n-1} \not\equiv 1 (\text{mod } n)$, n is composite
    - Ie 9: $9 \nmid 2^8 - 1 = 255$
    - If it fails the test, it is composite, but if it passes, it isn't necessarily prime
        - Ie $341 \mid 2^{240} - 1$, but $341 = 11 * 31$
- Thm: Positive integer $n > 1$ is prime if and only if it passes the Fermat test for every base a = 1, 2, 3, …, n – 1 (slow as well)

Miller-Rabin Test

- Recall that $a^{2n} - b^{2m} = (a^n - b^m)(a^n + b^m)$
- $a^{560} - 1 = (a^{280} - 1) (a^{280} + 1) (a^{560} + 1) = (a^{140} - 1) (a^{140} + 1) (a^{280} + 1) (a^{560} + 1) = \ldots$
- If 561 were prime, it would divide $a^{560} - 1$ (FLT), so it would divide one of the factors
- Test: for odd integer $n > 1$, pick integer a at random with $0 < a \leq n - 1$; factor $a^{n-1} - 1$
    - Factor using $a^{2n} - b^{2m} = (a^n - b^m)(a^n + b^m)$
    - For each factor, check divisibility by n
    - If n does not divide; it is composite
    - Unfortunately, there are still false positives, but better than idea #2
- Thm: if n is composite, Millar-Rabin test fails with probability ≥ ¾
    - To be more certain, do test many times

- More deterministic method – AKS (Agrawal-Kangal-Saxena)
    - $O(n) = (\log(n))^6$ still too slow, Miller-Rabin faster in practice

- Extra – how many squares are there among 11, 111, 1111, 11…1, …
    - Notice that $11 \equiv 3 \ (\text{mod } 4)$ and 3 is not a square mod 4
    - All numbers have the form $100m + 11$ for some $m \in \mathbb{Z}$
    - $100m + 11 \equiv 3 \ (\text{mod } 4)$
    - Therefore, none of the numbers are squares

Lecture 18 – 2016/10/19

Midterm

- Two problems – logic & number theory – each with a few parts
- Samples here
- Mostly based on homework – make sure you can do all the hw exercises
- If you have time, read Book of Proof – Hammack

- **Core**, Very Important, *Important*

Number Theory

- **Euclidian algorithm, GCD**
- Modular arithmetic, congruences
- **Fermat's Little theorem**
- **Induction**
- Proof strategy/proof structures
- *Primality testing*
- *Cryptography (RSA)*
- Fundamental theorem of arithmetic (factorization into primes)
- Exponentiation
- *Infinitude of primes*

Logic

- Set theory/proving set identities
- **Translation/symbolization (predicate & propositional logic)**
- Negations, especially in predicate logic
- **Rules of logic**
- *Axiomatic systems*
- **Truth tables**
- *Knights and knaves*
- *Venn diagrams*
- Tautologies, contradictions, contingencies

- Uniqueness – $\exists x[P(x) \wedge \forall y(P(y) \Rightarrow y = x)]$

- Let there be $x, m \in \mathbb{Z}$ – when does there exist y such that (*) $xy \equiv 1 \pmod{m}$?
  - $\because$ (*) $= xy - 1 = km$ for some $k \in \mathbb{Z}$
  - $\therefore$ (*) $\Leftrightarrow \exists k \in \mathbb{Z}\ (xy + km = 1)$
  - So (*) has a solution if and only if x and m are relatively prime
  - In this case, we say x is invertible module m, and if y satisfies (*), it's the inverse of x, usually denoted x^{-1}
  - Ie is there a y such that $3y \equiv 1 \pmod{6}$? O, 3 & 6 are not relatively prime

Lecture 19 is a review

Lecture 20 – 2016/10/26

- f is surjective (onto) if every y ∈ Y is a value f(x) for some x ∈ X (every output has an input)
- f is injective if it's one-to-one (every output has at most one input)
- f is bijective (1-1 and onto) if every y ∈ Y is a value f(x) for exactly one x ∈ X (every input has one output, and vice versa)
- We can compose a function f:X → Y with a function g:Y → Z to get a function h:X → Z
    - h(x) = g(f(x)) = g ∘ f(x)
- f: X → Y is invertible if it has inverse function g: Y → X such that g ∘ f(x) = x for all x ∈ X and f ∘ g(y) = y for all y ∈ Y. In this case, we denote g by f^{-1}
    - Bijections are invertible
- Recall |X| means cardinality (size) of X
- Observe that f:X → Y ⇔ …
    - |X| ≥ |Y| for surjections
    - |X| ≤ |Y| for injections
    - |X| = |Y| for bijections
    - Useful for combinatorics
- Ie: Given an alphabet with k letters, say [k] (all integers i → k), how many sequences of length n can you make
    - k^n since we have k choices for each of the n letters
    - Note that we have just counted the number of functions f[n] → [k]
- Subsets: take an n-set X; how many subsets does it have?
    - 2^n since for each element, it can either be in or out of the subset
- Permutations: A permutation of a set x is a bijection from f:X → X (itself)
    - How many permutations are there of an n-set?
        - Without loss of generality, X = {1, 2, 3, …, n}
        - We have n choices for f(1), n – 1 choices for f(2), etc
            - n(n – 1)(n – 2)…(3)(2)(1) = n!
- How many subsets of k does an n-set have?
    - $\binom{n}{k}$ = n!/(k!(n – k)!) = "n choose k"
    - For every set of size m, there are n + 1 – m choices → (n)(n – 1)….(n – k + 1) = n!/(n – k)! for sets sized 1 to k. As every set k can be ordered k! ways and order does not matter for subsets, we must divide the answer by k!.

Lecture 21 – 2016/10/28

Binomial Theorem

- Let n ≥ 0 be an integer, and consider the polynomial $(x + y)^n$
- $(x + y) = x + y$ $(x + y)^2 = x^2 + 2xy + y^2$
- In general, $(x + y)^n$ is the sum of terms of degree n, ie they all have the form $x^k y^{n-k}$ for some k, $0 \leq k \leq n$; every $x^k y^{n-k}$ also has a coefficient equal to the number of ways to pick k objects from a set of n objects: $\binom{n}{k}$ the numbers $\binom{n}{k}$ are called the binomial coefficients
- $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Special Cases

- x = y = 1
    - $(1 + 1)^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n}$
    - LHS: the $^{\#}$subsets of an n-set
    - RHS: the $^{\#}$k-subsets of an n-set summed over all k
    - So the last identity actually has two proofs: an algebraic one (via binomial theorem), and a combinatorial one
- x = -1, y = 1
    - $0 = (-1 + 1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots$
    - Combinatorically: "The number of odd subsets of an n-set is equal to the number of even subsets."

Pascal's Triangle

- The outside numbers are 1 and each other entry is the sum of the two above it
- Thm: Entry k of row n is $\binom{n}{k}$
    - Pf: By induction on n
        - Base case: n = 0, $\binom{0}{0} = 1$ by definition
        - Induction: for k = 0 or k = n, $\binom{n}{k} = 1$

          Assuming 0 < k < n, we want to show that $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
            - Combinatorial proof:
                - LHS: $^{\#}$k-subsets of an n-set
                - RHS: $^{\#}$k-subsets of {1, 2, 3, …, n} containing n <u>plus</u> $^{\#}$k-subsets of {1, 2, 3, …, n – 1}
- Observation: Pascal's triangle is symmetrical about the vertical line which goes through the apex → $\binom{n}{k} = \binom{n}{n-k}$
    - Combinatorically: choosing a k-subset of an n-set is equivalent to choosing its (n-k)-element complement → $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

Lecture 22 – 2016/10/31

- $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \ldots + \binom{n}{k}^2 = \binom{n}{k}^2$
  - LHS = $\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \binom{n}{2}\binom{n}{n-2} + \ldots + \binom{n}{n}\binom{n}{0}$
  - RHS = # ways to choose an n-set out form a 2n-set
  - LHS: to select an n-subset from {1, 2, 3, …, 2n}, we could select k elements from {1, …, n} and n – k elements from {n + 1, …, 2n}
  - This can be done in $\binom{n}{k}\binom{n}{n-k}$ ways. Summing over all k gives the result. ■
- Question: Suppose we've got n identical coins, and k children. How many ways can we distribute the n coins among the k children? In other words, how many nonnegative integers $d_1, \ldots, d_k$ are there with $d_1 + d_2 + \ldots + d_k = n$
  - Add k – 1 new coins to the set of n. Line up all n + k – 1 coins.
  - Select k – 1 coins to act as "walls". Child 1 gets all the coins to the left of the first wall. Child 2 gets the coins between the first and second wall, …, and the last child gets the coins to the right of the last wall.
  - How many ways can we pick k – 1 walls from n + k – 1 coins? $\binom{n+k-1}{k-1}$

Pigeonhole Principle

- Fact. There are two people in Montreal who have the exact same number of hairs on their head.
  - Reason: No one has more than 0.5 million hairs on their head. (Scientific fact) For each i = 0 1, 2, …, 500 000, create a group G_i, where each G_i contains all the Montrealers having exactly i hairs. Since there are 500 001 groups and > 500 001 Montrealers, one of the groups must have at least two people.
- Principle: If we have n boxes and more than n objects, and we place all the objects into the boxes, then some box must contain ≥ 2 objects.
- Ie: Suppose $S \subset \{1, 2, \ldots, 2n\}$ consists of n + 1 elements. Show that S contains two numbers summing to 2n + 1
  - Our boxes will be labelled with pairs of numbers summing to 2n + 1:
    - {1, 2n}, {2, 2n – 1}, {3, 2n – 2}, … , {n, n+1}
  - There are n boxes, and each element of S goes into the box showing the corresponding label. One of the boxes must get two numbers; these two numbers will sum to 2n + 1.
- Ie: Consider a set X of 90 integers, each with 25 digits. There must be two subsets of X having the same sum.
  - Reason: The sum of all elements in any subset is $\leq 90 * 10^{25} \leq 10^{27}$
    - Also an upper bound on the number of possible sums
    - The number of subsets is 2^{90}, which is $> 10^{27}$
    - Pigeonhole principle implies there must be two subsets having the same sum

Lecture 23 – 2016/11/02

Pigeonhole Principle Continued

- Ie: If 16 people sit down in a row of 18 chairs, then there is a sequence of 6 consecutive chairs all being used
  - Block 1 {1, …, 6}
  - Block 2 {7, …, 12}
  - Block 3 {13, …, 18}
  - To avoid getting 6 occupied chairs in a row, then none of the blocks can be full.
  - Each block would have at most 5 people, meaning that there are at most 15 people in total.
- Take a set X of 5 points on the infinite 2D grid
  - There exists two points $x, y \in X$ such that the midpoint $((x + y)/2)$ of the connecting line segment is also a grid point
  - Let $S =$ set of even integers, $T =$ set of odd integers
  - We'll have four boxes: odd x odd, odd x even, even x odd, even x even
  - Since $|x| = 5$, two points $x, y \in X$ must be in the same box
  - Then $x + y \in$ even x even, so each coordinate of $x + y$ is divisible by 2, which means $(x + y)/2$ is a grid points

Counting Techniques

- How many "words" can you make by arranging the letters in MATHEMATICS?
- Had the question been for MATH, the answer would be 4! (permutation for distinct items)
- MATHEMATICS has 11 letters, but there are duplicates. → For every letter with k occurrences, divide 11! by k!. M, A, T all occur twice → Answer is $11!/(2! * 2! * 2!) = 11!/8$

Cyclic Orderings

- How many ways can we arrange the numbers around a circle?
- Each permutation gives n circular orderings
  → # circular orderings = # permutations/n = (n – 1)!

Lecture 24 – 2016/11/04

Principle of Inclusion-Exclusion

- Suppose we've got a bunch of students. 18 are enrolled in math 240, 16 in phys 131, and 12 in comp 250. How many students are there in total? → not enough info
  - $A_1 = \{\text{students in math 240}\}$, $A_2 = \{\text{in phys 131}\}$, $A_3 = \{\text{in comp 250}\}$
  - Let's say we know: $|A_1 \cap A_2| = 7$, $|A_1 \cap A_3| = 5$, $|A_2 \cap A_3| = 3$, $|A_1 \cap A_2 \cap A_3| = 2$
  - $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$

Intersecting Set Systems

- Suppose that F is a family of subsets of $[n] = \{1, 2, \ldots, n\}$, having the property that $x \cap y \neq \emptyset$ for all $x, y \in F$. Such an F is called an intersecting family
- How big can an intersecting family be?
  - Let's take F to be the collective of all subsets containing some fixed element, say 1. Then $|F| = 2^{n-1}$
  - It's the best you can do, because if $x \in F$, $[n] \setminus x \notin F$
  - So $|F| \leq 2^{n-1}$
- What if we insist that all subsets in F have the same size k?
  - Assume $2k \leq n$: $\binom{n-1}{k-1}$, all k subsets containing same fixed element
- Theorem: (Erdõs-Ko-Rado, 1961) – if F is an intersecting family of k-subsets of $[n] = \{1, 2, \ldots, n\}$, and $n \geq 2k$, then $|F| \leq \binom{n-1}{k-1}$
  - Lemma Let $\sigma:[n] \to [n]$ be a permutation
    - For $0 \leq s \leq n - 1$, set $A_s = \{\sigma(s), \sigma(s + 1), \ldots, \sigma(s + k - 1)\}$ Where addition within σ is modulo n
    - Then an intersecting family F in [n] can contain at most k of the sets A_s
    - Suppose we have $A_s \in F$. There are $2(k - 1)$ other sets A_t intersecting A_s, namely A_{s-i} and A_{s+i} for $s = 1, 2, \ldots, k - 1$
    - But if I pick A_{s-i} to be in F, I cannot pick A_{s+k-i}.
    - So F can contain $\leq k - 1$ other sets A_t ■
  - R^i of $2kR_i$
    - Let F be an intersecting family. Consider pairs of the form (σ, t)
    - There are n!xn such pairs
    - We map each such pair to the k-subset of [n] as follows
    - $S(\sigma, t) := \{\sigma(t + 1), \sigma(t + 2), \ldots, \sigma(t + k)\}$ (arithmetic again is modulo n)
    - Given a permutation σ, there can be at most k values of $t \in \{0, 1, \ldots, n - 1\}$ for which $S(\sigma, t) \in F$, by the lemma
    - So $|\{(\sigma, t) : S(\sigma, t) \in F\}| \leq kn!$
  - How many pairs get mapped to each k-subset?
    - Answer does not depend on the subset, so $n!xn/\binom{n}{k}$
    - Therefore, $|\{(\sigma, t) : S(\sigma, t) \in F\}| = |F|n!xn/\binom{n}{k} \leq kn!$
    - $|F| \leq \binom{n}{k}k/n = \binom{n-1}{k-1}$ ■

Lecture 25 – 2016/11/07

Erdõs-Ko-Rados

- Q: Given integers n and k, n ≥ 2k, how large can we make a family F of K-subsets of [n] if we require x ∩ y ≠ ∅ for all x, y ∈ F?
- We can get $|F| = \binom{n-1}{k-1}$ by taking all the k-subsets containing some fixed element
- Theorem (Erdõs-Ko-Rados): $\binom{n-1}{k-1}$ is the best you can do
- Lemma: For any way you place the numbers around the circle, the family F can contain no more than K of the arcs
- Note: Choosing a way to get the numbers around the circle is the same as choosing a permutation; and choosing the arc of length k is equivalent to choosing a number from {0, 1, …, n – 1}
- We estimate in two ways, the number of permutation-arc pairs, which produce a k-subset inside F
- There are n! * n permutation-arc pairs in total
- The number of pairs which produce any fixed k-subset is just $\frac{n! * n}{\binom{n}{k}}$
- So the number of permutation-arc pairs producing a k-subset in F is $\frac{n! * n}{\binom{n}{k}} * |F|$
- But by the lemma, this number is ≤ n! * k
- So $\frac{n! * n}{\binom{n}{k}} * |F| \leq n! * k$ → $|F| \leq \binom{n}{k}\frac{k}{n} = \binom{n-1}{k-1}$

Graphs

- A graph is an ordered pair (ν, ϵ) consisting of a set of vertices V (or nodes), with some pairs of vertices being connected by edges. The elements of E are unordered pairs {u, v}, with u, v ∈ V, u ≠ v. We have {u, v} ∈ E if and only if an edge joins u and v.
- Graphs can model just about anything

Examples

- Networks
  - V = {people on Facebook}, Join two people with an edge when they are friends.
  - V = {nodes in network}, An edge between two nodes indicates a direct connection
- Conflicts
  - V = {radio transmitting stations}, Connect two station with edge if they might interfere with each other
  - V = {k-subsets of [n]}, Join two k-subsets with edge if they are disjoint
- Routing/logistics
  - V = {cities}, E = {roads}

- If two vertices are joined with an edge, they are adjacent
- When an edge e is attached to a vertex v, we say e is incident to v
- The number of edges incident to a vertex v is its degree, usually denoted d(v)

Lecture 26 – 2016/11/09

Handshaking Lemma

- If there are n people at a meeting and everyone shakes hands with everyone exactly once, how many handshakes take place?
- We can represent this situation with a graph; Answer: $\binom{n}{2}$
- The graph drawn is called the compete graph on n vertices, denoted K_n

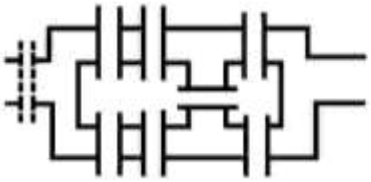
Degrees

- Recall: the degree of a vertex v is the number of edges incident to v.
- Q: Can there be a graph with 5 vertices, having degrees 1, 2, 3, 4, 5?
- Observation: by adding up all the vertex degrees, we count double the number of edges
    - Each endpoint is counted once
- A: $\because 1 + 2 + 3 + 4 + 5 = 15$, which isn't even $\therefore$ degree sequence is impossible

Walks & Paths

- Let $G = (\nu, \epsilon)$ be a graph.
- A walk in G is a sequence of vertices $v_0, v_1, v_2, \ldots, v_k$ so that v_i is adjacent to v_{i-1}.
    - A closed walk is a walk in which $v_0 = v_k$ (endpoints are the same)
- A path is a walk in which no vertex gets repeated.
    - A closed path is a walk in which $v_0 = v_k$ and no other vertex gets repeated.
- A connected graph is a graph in which every $u, v \in V$ has a path starting at u and ending at v.

The first theorem of graph theory



- Leonhard Euler 1736
- Q: Is it possible to tour the city in a way that you cross each bridge exactly once?
- A: During such a tour, each region of land would need to be entered and exited the same number of times. Therefore, each region would need an even number of bridges connected to it, which is not the case.
- Let $G = (\nu, \epsilon)$ be a graph. An Euler tour in G is a closed walk in which each edge gets used exactly once. Graphs with an Euler tour are Eulerian
- Q: Which graphs are Eulerian?
- Thm: (Euler 1736): A connected graph is Eulerian if and only if all the vertices have even degrees
    - Pf: We've already checked the necessity of having even degrees; let's do sufficiency
    - Let $W = v_0, v_1, v_2, v_3, \ldots, v_l$ be a longest possible walk in which no edge gets used more than once.
    - If there were an unused edge incident to v_l, we could take it, so all edges incident to v_l have been used.
    - At the end of the walk, we entered v_l but never exited; since v_l has even degree, v_l must equal v_0 (all other vertices have been entered and exited the same number of times)
    - Suppose G has an edge not used in W; since G is connected, there must be an unused edge incident to some v_i. Then $v_i, v_{i+1}, \ldots, v_0 = v_l, v_1, v_2, \ldots, v_i$ is a longer walk → contradiction ■

Lecture 27 – 2016/11/11

Hamilton Cycles

- Last time we found a simple characterization of Eulerian graphs, ie graphs which admit a closed walk which uses each edge exactly once.
- What if instead we ask that each vertex gets used exactly once?
- Cycle – a closed path of length ≥ 3
- Hamilton cycle – a cycle which uses each vertex exactly once
    - A graph which admits a Hamilton cycle is Hamiltonian
- A Hamilton path is a path which uses each vertex exactly once – like the cycle, but without the last edge connecting back to the start point
- No simple characterization (necessary and sufficient condition) known, and evidence that none exists. (P vs NP)
- Nevertheless, we have the following useful sufficient condition

Thm: Dirac 1952

- If $G = (V, E)$ is a graph with ≥ 3 vertices and $d(v) \geq |V|/2$ for each $v \in V$, then G is Hamiltonian
- Pf: Contradiction: Let $G = (V, E)$ be a non-Hamiltonian graph with $d(v) \geq |V|/2$ for all $v \in V$
- Add edges to G until addition of just one more edge would introduce a Hamilton cycle
- Claim: G must contain a Hamilton path
    - If it is not a Hamilton path then its length is $< |V| - 1$, so we could add another edge without introducing a Hamilton cycle.
- Say our Hamilton path is $v_1, v_2, v_3, \ldots, v_n$ ($n = |V|$)
- We know v_1 is adjacent to more than half of the vertices $v_3, v_4, \ldots, v_{n-1}$, and v_n is adjacent to more than half of the vertices $v_2, v_3, \ldots, v_{n-2}$
- By the pigeonhole principle, there is an index i such that v_1 is adjacent to v_{i+1} and v_n is adjacent to v_i
- $v_1, v_2, \ldots, v_i, v_n, v_{n-1}, \ldots, v_{i+1}, v_1$ is a Hamilton cycle ■

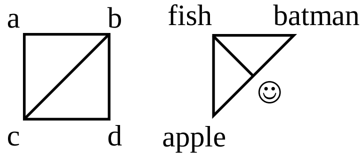
Lecture 28 – 2016/11/14

Subgraphs

- Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$. We say that G_2 is a subgraph of G_1 if $V_2 \subseteq V_1$ and $E_2 \subseteq E_1$.
- If $V_2 \subseteq V_1$ and E_2 consists of every edge in E_1 that has both endpoints in V_2, then we say G_2 is an induced subgraph

Graph Isomorphism

- When are 2 graphs the same?
- If we do not care about the names of the vertices, then $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are "the same" if $\exists$ bijection $f{:}V_1 \rightarrow V_2$ such that $\{i, j\} \in E_1 \Leftrightarrow \{f(i), f(j)\} \in E_2$
- Note: isomorphisms always send vertices to vertices of the same degree
- Bijections: $f(a) = \text{apple}$, $f(b) =$ ☺, $f(c) = \text{fish}$, $f(d) = \text{batman}$



Trees

- A tree is a connected graph with no cycles
- Vertices of degree 1 are leaves; all other vertices are internal vertices
- Fact: Every tree with ≥ vertices has ≥ 2 leaves
  - Pf: Take a largest possible path. The two endpoints must have degree 1, otherwise the path could be made longer
  - Note that no other edge on one of the endpoints can go back to the path
- Fact: Every pair of vertices in a tree is connected with a unique path
  - Pf: Supposed P_1 and P_2 are two different paths from a to b with at least two points in common, namely the endpoints a and b (there may be more points in common)
    - Take two consecutive common points x and y, Walk from x to y along P_1 and walk back to x along P_2. This is a cycle, and trees don't have cycles
    - Contradiction ■
- Thm: Every tree on $n \geq 1$ vertices has $n - 1$ edges
  - Pf: By induction on n
    - Base case: 1 vertex, 0 edges
    - Induction step: Let T be a tree with $n + 1$ vertices. Let v be a leaf (exists by an earlier fact). Let $T' = T - v$. T' is still connected and is still noncyclic
      ∴ T' is a tree on n vertices; by induction, it has $n - 1$ edges
      ∴ T has $n - 1 + 1 = n$ edges ■

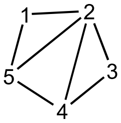
Spanning Tree

- Every connected graph contains a tree as a subgraph which uses all the vertices
  → such a graph is a spanning tree

Lecture 29 – 2016/11/16

Spanning Trees (cont)

- A spanning tree of a connected graph G is a tree T which is a subgraph of G and which has all the vertices of G
- One way to see that every connected graph has a spanning tree is with a breadth-first search (a way to enumerate the vertices)
- Start by inserting 1 into the queue (shown on right)
    - Remove next vertex v from queue and mark v as "visited"
    - Look at neighbours of v & discard the ones marked "visited"; mark remaining as "visited" and add them to the queue
    - Repeat
- To get spanning tree
    - Do BFS. Each time you add a vertex to the queue, remember the edge connecting it to the last vertex removed. Discard all other edges



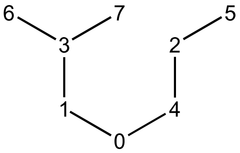
~~1~~		~~2~~		~~5~~		~~3~~		~~4~~
2		5		3		4		
5		3		4				
		4						

Counting Trees

- How many trees are there on a set of n vertices? 2 ways to interpret this question
    - We could ask for the number of isomorphism classes of trees (no simple formula)
    - We could ask for the number of labelled trees. In this case, isomorphic trees would be different. → but there is a nice answer: n^{n-2} (Cayley's theorem)

Tree Encoding (Prüfer Code)

- Fix n = # of vertices. Consider a sequence of length n – 2 made with numbers from {0, 1, …, n – 1}, ie (n = 8) 2 4 0 3 3 1
- Claim: we can turn every such sequence into a labelled tree with vertices from {0, …, n – 1}
- Procedure
    - Add 0 to end of sequence 2 4 0 3 3 1 0
    - Construct row of numbers (L → R) above existing row
      Find smallest # in {0, 1, …, n – 1} not already listed in 5 2 4 6 7 3 1
      top row nor in the bottom row below or after it 2 4 0 3 3 1 0
        - Every number in top row is smallest possible number not on top row to its left and bottom row starting from its position and going right
    - Build the tree
        - Start with 0, read table (R → L) and connect each top-bottom pair with edge, creating new vertex whenever it does not already exist. Result on right.



Lecture 30 – 2016/11/18

Prüfer codes (cont)

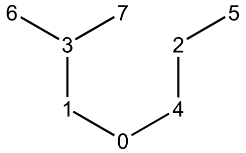
- Recall the function we defined last time.
- V = {0, 1, ..., n – 1}
- f: V^{n-2} → {graphs on V}
- f(2 4 0 3 3 1) = ?

Edge table
5 2 4 6 7 3 1
2 4 0 3 3 1 0

- Suppose $u_1, u_2, \ldots, u_{n-2}, u_{n-1}$ is the edge table;
  v_1 $v_2, \ldots, v_{n-2}, 0$

note that by the way the top row is constructed, all of u's are distinct; so each number from {1, 2, ..., n – 1} occurs exactly once

- Now we use induction
- Clearly the graph on {u_{n-1}, o) with just one edge is a tree. After adding edges $\binom{u_{n-1}}{o}, \binom{u_{n-2}}{v_{n-2}}, \ldots, \binom{u_{i+1}}{v_{i+1}}$
- To add $\binom{u_i}{v_i}$, we create the new vertex u_i and join it to v_i
  - v_i has already been created, since it cannot be among $u_{,1}, u_2, \ldots, u$, therefore adding $\binom{u_i}{v_i}$ produces another tree ■
- So actually f: V^{n-2} → {trees on V}; in fact, f is a bijection
- Surjective
  - Let T be a given tree on V = {0, 1, ..., n – 1}; we create a sequence in V^{n-2} as follows
  - Go to the smallest nonzero leaf u in T; say its neighbour is v
  - Add v to sequence (sequence is constructed left to right)
  - Delete u from T along with edge uv
  - Go back to first step until there is only 0 remains
  - Delete 0 from end of sequence
  - Sequence for tree on the right: 2 4 0 3 3 1 ~~0~~



  - Suppose we get the sequence $v_1, v_2, \ldots, v_{n-2}$
  - Do we have $f(v_1, v_2, \ldots, v_{n-2})$ = T?
  - First build the edge table

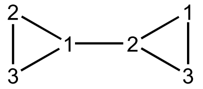
Edge table
$u_1, u_2, \ldots, u_{n-2}, u_{n-1}$
$v_1, v_2, \ldots, v_{n-2}, 0$

  - All the nonzero numbers in the bottom row are internal vertices of T. So u_1 is the smallest number which is not an internal vertex of T. In other words, u_1 is the smallest leaf in T; $\binom{u_i}{v_i}$ is an edge
  - In general {$v_{i+1}, \ldots, v_{n-2}$} is the set of nonzero internal vertices of $T_i := T - u_1 - u_2 - \ldots - u_i$ and u_{i+1} is the smallest leaf ■
- Injective
  - Let T be a given tree on V = {0, 1, ..., n – 1}
  - For each i = 1, 2, ..., n – 2, the following statement holds
  - After removing the first i leaves in the procedure, the nonzero internal vertices must be $v_{i+1}, \ldots, v_{n-2}$ as defined in the surjective proof, and their multiplicity is their degree minus one. This completely determines the sequence $v_1, v_2, \ldots, v_{n-2}$ ■
- Thm (Cayley's theorem): the number of labelled trees on n vertices is n^{n-2}

Lecture 31 – 2016/11/21

Graph Colouring

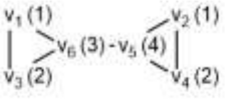
- A vertex colouring of a graph is a function c:V → N. A vertex colouring is called proper if c(x) ≠ c(y) wherever xy ∈ E
- The chromatic number of G, denoted X(G), is the smallest number of colours you can use to properly colour the vertices of G
- Example on the right (numbers denote colour):



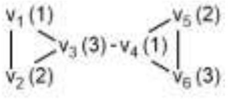
- In fact, X(G) = 3. To prove this…
- No way to properly 2-colour this (triangle graph, three vertices)
- Graph colouring gets used in many ways
    - Schedule problems
        - Colours are rooms, vertices are lectures, edges join vertices whose lecture times are scheduled to overlap
        - Proper colouring gives room assignment with no conflicts
    - Telecommunications
        - Colours are rooms, vertices are transmitters, edges join vertices whose transmitters are close enough to interfere with each other
        - Proper colouring corresponds to frequency assignment with no interference.

Greedy Algorithm for Colouring

- Finding a vertex colouring of G using X(G) colours is a hard (NP) computational problem Even finding X(G) is hard; would be nice to have an algorithm that gives some proper colouring with a not too large number of colours
- We have a set of colours 1, 2, 3, 4, …
- Consider the vertices in any order v_1, v_2, v_3, …
- When considering v_i, colour with the smallest colour not used by neighbours; order matters



4 colours; not optimal



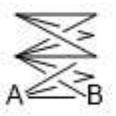
- Maximum number of colours used by the greedy algorithm is ≤ Δ(G) + 1 Where Δ(G) ≔ max {deg(v) : v ∈ V} is the maximum degree of G = (V, E)
- Thm: If G = (V, E) has max degree Δ = Δ(G), then
    - (i) X(G) ≤ Δ + 1 (ii) X(G) ≤ Δ if G is not regular (all vertices have same degree)
- Pf
    - We've already proven (i); just apply greedy algorithm
    - For (ii), we may suppose without loss of generality that G is connected
        - Otherwise just apply this proof separately to each connected component
        - ∵ G is not regular ∴ ∃v ∈ V with deg(v) ≤ Δ – 1
        - Set v_n = v; starting from v_1, do breadth-first search
        - G is connected, so every vertex gets listed
        - Now, apply greedy algorithm with ordering v_1, v_2, …, v_n
        - By construction, each vertex (except v_n) has at least one neighbour which gets considered after it, so when the greedy algorithm is colouring v_i, at most Δ – 1 colours have been used by the neighbours of v_i. One colour from 1, 2, …, Δ is always usable ■

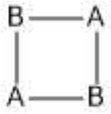
Lecture 32 – 2016/11/23

Colouring

- A stronger theorem is true compared to last lecture's greedy algorithm.
- Thm: (Brooks 1941)
    - Let G be a connected graph. If G is neither complete, nor an odd cycle, then $X(G) \leq \Delta(G)$ Pf not given in class.

Bipartite Graphs

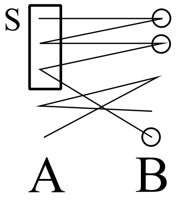




- A graph $G = (V, E)$ is bipartite if there is a partition $A \cup B = V$ of V such that every edge has one end in A and the other end in B
- Examples on the right (ignore the gap for overlapping lines)
- Observation: A graph is bipartite if and only if it is properly colourable with just 2 colours
- Thm: A graph $G = (V, E)$ is bipartite if and only if it contains no odd cycle
- Pf: If G has an odd cycle, it cannot be bipartite
    - We may suppose without loss of generality that G is connected
    - Take a spanning tree T of G, and fix some vertex r ("the root")
    - For each $v \in V$, there is a unique path in T from r to v. The path length is either odd or even; this defines a bipartition of V. We show that G is bipartite with this bipartition.
    - Assume there is an edge $e \in E$ between the vertices x, y. If e is in T, then x and y have different parities. (Only one edge in between)
    - If e is not in T, let P be the path in T from x to y. Then $P + e$ is a cycle, which must be even. So P has odd length, and the vertices in P must alternate between odd and even; x and y have different parities ■

The Marriage Theorem

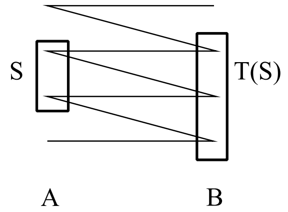
- In a village, there are 50 males and 50 females. We are the matchmaker, and our job is to pair up boys with girls. Is it possible to do this so that no one gets paired with a stranger?
- We represent this situation with a bipartite graph → put males on one side, females on the other, and draw an edge between male and female if there is an acquaintance
- A **perfect matching** in a graph is a set of edges M such that every vertex is incident with exactly one edge in M
- Our marriage problem is to decide whether there is a perfect matching in a given bipartite graph.
- Let G be a bipartite graph whose partition has parts A and B
- For any $S \subseteq A$, let $T(S)$ be the set of vertices in B adjacent to at least one vertex in S (see graph on right; vertices in $T(S)$ are circled)



- Thm: (The marriage theorem) G has a perfect matching if and only if $|A| = |B|$ and $|T(S)| \geq |S|$ for every $S \subseteq A$

Lecture 33 – 2016/11/25

The Marriage Theorem

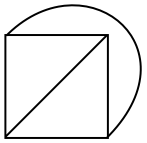


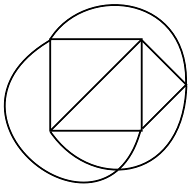
- G: A bipartite graph with bipartition A, B. For $S \subseteq A$, let $T(S)$ be the set of vertices in B adjacent to at least one vertex in S
- Thm (the marriage theorem): G has a perfect matching if and only if $|A| = |B|$ and $|T(S)| \geq S$
- Observation: The necessary condition in the marriage theorem goes "left to right", but a similar condition going right to left is equivalent
- Pf: If $T \subseteq B$, then $T(A \setminus T(T)) \cap T = \emptyset$, so $T(A \setminus T(T)) \leq |B| - |T|$, and $|T(A \setminus T(T))| \geq |A \setminus T(T)| = |A| - |T(T)|$ (since G satisfies the left-right condition) so $|A| - |T(T)| \leq |B| - |T| \Rightarrow |T| \leq |T(T)|$ ■

Proof of the Marriage Theorem

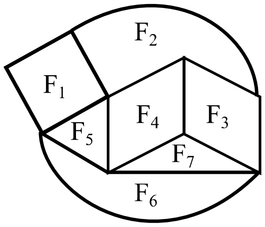
- Necessity: easy
- Sufficiency: induction on $|A| = |B|$
    - Base case $|A| = |B| = 1$
    - Induction step: Call a bipartite graph "good" if it satisfied the necessary conditions of the theorem
    - Take $a \in A$ and $b \in B$, where a and b are adjacent vertices
    - If $G - a - b$ is good, then we're done by induction
    - Otherwise, there is an $S \subseteq A \setminus \{a\}$ such that $|T(S) \setminus \{b\}| < |S|$
    - Since G was good, this can only happen if $b \in T(S)$ and $|S| = T(S)|$
    - Now, the graph induced on vertices S, T(S) is good, so it has perfect matching by induction
    - We'll be done by induction if we can show the graph G' induced on vertices $A = A \setminus S$, $B' = B \setminus T(S)$ [the unmatched vertices] is also good
    - For this, we use the "right to left" definition of goodness. If $T \subseteq B'$, then $T(T) \subseteq A'$, so G' is good because G was good ■

Planar Graphs


K_4 is planar


K_5 is not planar

- A graph G is planar if it can be drawn on a plane such that no pair of edges cross
- The regions of the plan cut out by the edges Y are called faces in a planar drawing of a graph
- The unbounded face of the drawing is called the outer face
- Let f = # face, v = # vertices, e = # edges
- Thm (Euler 1752): A connected planar graph satisfies $v + f - e = 2$
    - Observe that Euler's formula implies that while a graph may have different planar drawings, they all have the same number of faces



F_0 [outer loop]

Lecture 34 – 2016/11/28

- Question: You've got a pile of 8 batteries. You know 4 are full, and 4 are empty. You've got a flashlight which takes 2 batteries, and they both have to be full for the flashlight to turn on. How many times must you try turning on the flashlight in order to decide whether it is broken? Answer is 7

Euler's Theorem

- A connected planar graph satisfied v + f – e = 2
  where v = #vertices, e = #edges, f = #faces
    - Pf: induction on e
        - Base case: G is a tree; in this case f = 1, e = v – 1, formula holds
        - Induction: if G is not a tree, then it has a cycle. Pick an edge in same cycle, and delete it; call the resulting graph G'. G' therefore has one less edge and one less face that G; by induction, 2 = v + (f – 1) – (e – 1) = v + f – e
- Euler's formula also allows us to upper bound the number of edges in any planar graph
- Thm: If e ≥ 3 in any planar graph, then e ≤ 3v – 6
    - Pf: in any planar graph, each edge touches ≤ 2 faces. But each face touches ≥ 3 edges.
      So the #pairs (e, f) where e touches f satisfies 2e ≥ #pairs ≥ 3f
      By Euler's formula, 3(e + 2) = 3v + 3f ≤ 3v + 2e; 3e + 6 ≤ 3v + 2e; e ≤ 3v – 6 ■
    - From this wee see K_5 is not planar: v = 5, e = $\binom{5}{2}$ = 10, and 15 – 6 < 10

Lecture 35 – 2016/11/30

- Last time we proved…
- Thm: In a planar graph, if $e \geq 3$, then $e \leq 3v - 6$
- If we know the graph is bipartite, we can strengthen the last theorem
- In a bipartite graph, a face must touch ≥ 4 edges. So let's redo the estimate from the last proof
- $2e \geq \#(e, f) \geq 4f$
- From Euler's formula
  - $4(e + 2) = 4(v + f)$
  - $4e + 8 \leq 4v + 2e$
- Thm: If G is a bipartite planar graph, with ≥ 4 edges, then $e \leq 2v - 4$
- Cor: $K_{3,3}$ is not planar

Map Colouring

- Suppose we want to colour a map so that when two countries touch, they get different colours. We can turn map colouring into graph colouring by giving a vertex to each country and joining two vertices with an edge when the corresponding countries touch.
- Thm (Four colour theorem, Appel-Haken 1976)
  - Every planar graph can be properly coloured with just four colours
    - No human-readable proof currently exists (proof is done by computation)
- Thm (Five colour theorem)
  - Every planar graph can be properly coloured with just five colours (easier to prove)
  - Lemma: Every planar graph has a vertex with degree ≤ 5
    - Pf: by contradiction, assume every vertex has degree ≥ 6
    - Recall #edges $= \frac{1}{2}\sum_{v \in V} \deg(v)$, so #edges $\geq 6/2$ #vertices $= 3$ #vertices
    - But we know #edges ≤ 3 #vertices – 6, so there are too many vertices