Today

Review for Midterm.

First there was logic...

A statement is a true or false.

Statements?

$3 = 4-1$? Statement!

$3 = 5$? Statement!

3 ? Not a statement!

$n = 3$? Not a statement...but a predicate.

Predicate: Statement with free variable(s).

Example: $x = 3$ Given a value for x, becomes a statement.

Predicate?

$n > 3$? Predicate: $P(n)$!

$x = y$? Predicate: $P(x,y)$!

$x + y$? No. An expression, not a statement.

Quantifiers:

$(\forall x)\ P(x)$. For every x, $P(x)$ is true.

$(\exists x)\ P(x)$. There exists an x, where $P(x)$ is true.

$(\forall n \in N), n^2 \geq n$.

$(\forall x \in R)(\exists y \in R) y > x$.

Connecting Statements

$A \wedge B$, $A \vee B$, $\neg A$.

You got this!

Propositional Expressions and Logical Equivalence

$(A \implies B) \equiv (\neg A \vee B)$

$\neg(A \vee B) \equiv (\neg A \wedge \neg B)$

Proofs: truth table or manipulation of known formulas.

$(\forall x)(P(x) \wedge Q(x)) \equiv (\forall x)P(x) \wedge (\forall x)Q(x)$

..and then proofs...

Direct: $P \implies Q$

Example: a is even $\implies a^2$ is even.

Approach: What is even? $a = 2k$

$a^2 = 4k^2$.

What is even?

$a^2 = 2(2k^2)$

Integers closed under multiplication!

a^2 is even.

Contrapositive: $P \implies Q$ or $\neg Q \implies \neg P$.

Example: a^2 is odd $\implies a$ is odd.

Contrapositive: a is even $\implies a^2$ is even.

Contradiction: P

$\neg P \implies$ **false**

$\neg P \implies R \wedge \neg R$

Useful for prove something does not exist:

Example: rational representation of $\sqrt{2}$ does not exist.

Example: finite set of primes does not exist.

Example: rogue couple does not exist.

...jumping forward..

Contradiction in induction:

contradict place where induction step doesn't hold.

Well Ordering Principle.

Stable Marriage:

first day where women does not improve.

first day where any man rejected by optimal women.

Do not exist.

...and then induction...

$P(0) \wedge ((\forall n)(P(n) \implies P(n+1) \equiv (\forall n \in N)\ P(n)$.

Thm: For all $n \geq 1$, $8 | 3^{2n} - 1$.

Induction on n.

Base: $8 | 3^2 - 1$.

Induction Hypothesis: Assume $P(n)$: True for some n.

$(3^{2n} - 1 = 8d)$

Induction Step: Prove $P(n+1)$

$$\begin{aligned} 3^{2n+2} - 1 &= 9(3^{2n}) - 1 \quad \text{(by induction hypothesis)} \\ &= 9(8d+1) - 1 \\ &= 72d + 8 \\ &= 8(9d+1) \end{aligned}$$

Divisible by 8.

$\square$

Stable Marriage: a study in definitions and WOP.

n-men, n-women.

Each person has completely ordered preference list
contains every person of opposite gender.

Pairing.
Set of pairs (m_i, w_j) containing all people *exactly* once.
How many pairs? n.
People in pair are **partners** in pairing.

Rogue Couple in a pairing.
A m_j and w_k who like each other more than their partners

Stable Pairing.
Pairing with no rogue couples.

Does stable pairing exist?

No, for roommates problem.

TMA.

Traditional Marriage Algorithm:

Each Day:
All men propose to favorite woman who has not yet rejected him.
Every woman rejects all but best men who proposes.

Useful Algorithmic Definitions:
Man **crosses off** woman who rejected him.
Woman's current proposer is **"on string."**

"Propose and Reject." : Either men propose or women. But not both.
Traditional propose and reject where men propose.

Key Property: Improvement Lemma:
Every day, if man on string for woman,
$\implies$ any future man on string is better.

Stability: No rogue couple.
rogue couple (M,W)
$\implies$ M proposed to W
$\implies$ W ended up with someone she liked better than M.
Not rogue couple!

Optimality/Pessimal

Optimal partner if best partner in any stable pairing.
Not necessarily first in list.
Possibly no stable pairing with that partner.

Man-optimal pairing is pairing where every man gets optimal partner.

Thm: TMA produces male optimal pairing, S.
First man M to lose optimal partner.
Better partner W for M.
Different stable pairing T.
TMA: M asked W first!
There is M' who bumps M in TMA.
W prefers M'.
M' likes W at least as much as optimal partner.
Not first bump.
M' and W is rogue couple in T.

Thm: woman pessimal.

Man optimal $\implies$ Woman pessimal.
Woman optimal $\implies$ Man pessimal.

...Graphs...

$G = (V, E)$
V - set of vertices.
$E \subseteq V \times V$ - set of edges.

Directed: ordered pair of vertices.

Adjacent, Incident, Degree.
In-degree, Out-degree.

Thm: Sum of degrees is $2|E|$.
Edge is incident to 2 vertices.
Degree of vertices is total incidences.

Pair of Vertices are Connected:
If there is a path between them.

Connected Component: maximal set of connected vertices.

Connected Graph: one connected component.

Graph Algorithm: Eulerian Tour

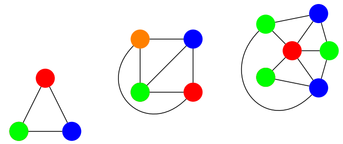
Thm: Every connected graph where every vertex has even degree has an Eulerian Tour; a tour which visits every edge exactly once.

Algorithm:
Take a walk using each edge at most once.
Property: return to starting point.
Proof Idea: Even degree.

Recurse on connected components.
Put together.
Property: walk visits every component.
Proof Idea: Original graph connected.

Graph Coloring.

Given $G = (V, E)$, a coloring of a G assigns colors to vertices V where for each edge the endpoints have different colors.

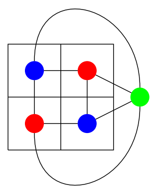


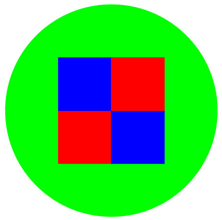
Notice that the last one, has one three colors.
Fewer colors than number of vertices.
Fewer colors than max degree node.

Interesting things to do. Algorithm!

Planar graphs and maps.

Planar graph coloring $\equiv$ map coloring.





Four color theorem is about planar graphs!

Six color theorem.

Theorem: Every planar graph can be colored with six colors.

Proof:
Recall: $e \leq 3v - 6$ for any planar graph.
From Euler's Formula.

Total degree: $2e$
Average degree: $\leq \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v}$.

There exists a vertex with degree < 6 or at most 5.

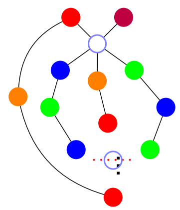
Remove vertex v of degree at most 5.
Inductively color remaining graph.
Color is available for v since only five neighbors...
and only five colors are used. □

Five color theorem

Theorem: Every planar graph can be colored with five colors.

Preliminary Observation: Connected components of vertices with two colors in a legal coloring can switch colors.

Proof:
Again with the degree 5 vertex. Again recurse.



Assume neighbors are colored all differently.
Otherwise done.
Switch green to blue in component.
Done. Unless blue-green path to blue.
Switch red to orange in its component.
Done. Unless red-orange path to red.

Planar. $\Longrightarrow$ paths intersect at a vertex!

What color is it?
Must be blue or green to be on that path.
Must be red or orange to be on that path.

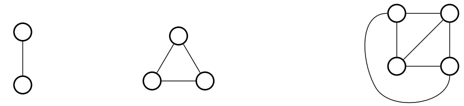
Contradiction. Can recolor one of the neighbors.
And recolor "center" vertex. □

Four Color Theorem

Theorem: Any planar graph can be colored with four colors.

Proof: Not Today!

Graph Types: Complete Graph.

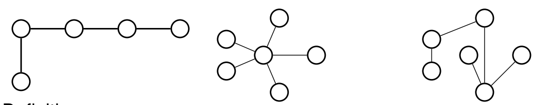


K_n, $|V| = n$

every edge present.
degree of vertex? $|V| - 1$.

Very connected.
Lots of edges: $n(n-1)/2$.

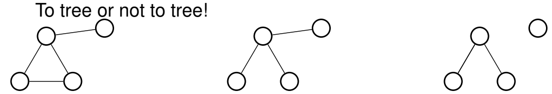
Trees.



Definitions:

A connected graph without a cycle.
A connected graph with $|V| - 1$ edges.
A connected graph where any edge removal disconnects it.
An acyclic graph where any edge addition creates a cycle.

To tree or not to tree!



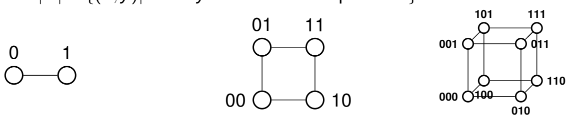
Minimally connected, minimum number of edges to connect.

Property:
Can remove a single node and break into components of size at most $|V|/2$.

Hypercube

Hypercubes. Really connected. $|V|\log|V|$ edges!
Also represents bit-strings nicely.

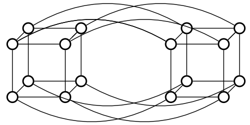
$G=(V,E)$
$|V|=\{0,1\}^n$,
$|E|=\{(x,y)|x$ and y differ in one bit position.$\}$



Recursive Definition.

A 0-dimensional hypercube is a node labelled with the empty string of bits.

An n-dimensional hypercube consists of a 0-subcube (1-subcube) which is a $n-1$-dimensional hypercube with nodes labelled $0x$ ($1x$) with the additional edges $(0x,1x)$.



Hypercube:properties

Rudrata Cycle: cycle that visits every node.
Eulerian? If n is even.

Large Cuts: Cutting off k nodes needs $\geq k$ edges.
Best cut? Cut apart subcubes: cuts off 2^n nodes with 2^{n-1} edges.

FYI: Also cuts represent boolean functions.

Nice Paths between nodes.
Get from 000100 to 101000.
$000100 \to 100100 \to 101100 \to 101000$
Correct bits in string, moves along path in hypercube!

Good communication network!

...Modular Arithmetic...

Arithmetic modulo m.
Elements of equivalence classes of integers.
$\{0,\ldots,m-1\}$
and integer $i\equiv a \pmod m$
if $i=a+km$ for integer k.
or if the remainder of i divided by m is a.

Can do calculations by taking remainders
at the beginning,
in the middle
or at the end.

$58+32=90=6 \pmod 7$
$58+32=2+4=6 \pmod 7$
$58+32=2+-3=-1=6 \pmod 7$

Negative numbers work the way you are used to.
$-3=0-3=7-3=4 \pmod 7$

Additive inverses are intuitively negative numbers.

Modular Arithmetic and multiplicative inverses.

$3^{-1} \pmod 7$? 5
$5^{-1} \pmod 7$? 3

Inverse Unique? Yes.
Proof: a and b inverses of $x \pmod n$
$ax=bx=1 \pmod n$
$axb=bxb=b \pmod n$
$a=b \pmod n$.

$3^{-1} \pmod 6$? No, no, no....

$\{3(1),3(2),3(3),3(4),3(5)\}$
$\{3,6,3,6,3\}$

See,... no inverse!

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m)=1$.

Group structures more generally.

Proof Idea:
$\{0x,\ldots,(m-1)x\}$ are distinct modulo m if and only if $gcd(x,m)=1$.

Finding gcd.
$gcd(x,y)=gcd(y,x-y)=gcd(y,x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0)=x$.

Extended-gcd(x,y) returns (d,a,b)
$d=gcd(x,y)$ and $d=ax+by$

Multiplicative inverse of (x,m).
egcd$(x,m)=(1,a,b)$
a is inverse! $1=ax+bm=ax \pmod m$.

Idea: egcd.
gcd produces 1
by adding and subtracting multiples of x and y

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned} 7(0)+60(1) &= 60 \\ 7(1)+60(0) &= 7 \\ 7(-8)+60(1) &= 4 \\ 7(9)+60(-1) &= 3 \\ 7(-17)+60(2) &= 1 \end{aligned}$$

Confirm: $-119+120 = 1$

$d = e^{-1} = -17 = 43 = \pmod{60}$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod p$,

$a^{p-1} \equiv 1 \pmod p$.

Proof: Consider $T = \{a \cdot 1 \pmod p, \ldots, a \cdot (p-1) \pmod p\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

$$a^{(p-1)}(1 \cdots (p-1)) \equiv (1 \cdots (p-1)) \mod p.$$

Each of $2, \ldots (p-1)$ has an inverse modulo p,
mulitply by inverses to get...

$$a^{(p-1)} \equiv 1 \mod p. \quad \square$$

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod N$

Proof:
$x^{ed} - x$ is divisible by p and q $\implies$ theorem!

$x^{ed} - x = x^{k(p-1)(q-1)+1} - x = x((x^{k(q-1)})^{p-1} - 1)$

If x is divisible by p, the product is.
Otherwise $(x^{k(q-1)})^{p-1} = 1 \pmod p$ by Fermat.
$\implies (x^{k(q-1)})^{p-1} - 1$ divisible by p.

Similarly for q. $\square$

RSA, Public Key, and Signatures.

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m.$

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

Verify: Check $C = E(C)$.

$E(D(C,k),K) = (C^d)^e = C \pmod N$

Midterm format

Time: 120 minutes.

Some short answers.
Get at ideas that you learned.

Know material well:	fast, correct.
Know material medium:	slower, less correct.
Know material not so well:	Uh oh.

Some longer questions.
Proofs, algorithms, properties.
Not so much calculation.

Will post midterm from 4 years ago to get an idea.
Back when I was younger.

Fermat/RSA

$3^6 \pmod 7$? 1. Fermat: $p = 7$, $p-1 = 6$
$3^{18} \pmod 7$? 1.
$3^{60} \pmod 7$? 1.
$3^{61} \pmod 7$?3.

$2^{12} \pmod{21}$? 1.
$21 = (3)(7)$ $(p-1)(q-1) = (2)(6) = 12$
$gcd(2,12) = 1$, $x^{(p-1)(q-1)} = 1 \pmod{pq}$ $2^{12} = 1 \pmod{21}$.

$2^14 \pmod{21}$? 4. Technically $4 \pmod{21}$.

Wrapup.

If you sent me email about Midterm conflicts
- Other arrangements.
- Should have recieved an email from me.

Other issues....
- satishr@cs.berkeley.edu
- Private message on piazza.

Good (sort of last minute)
Studying!!!!!!!!!!!!!!!!!