CSM 70 Review

<3

Logistics

ADD US ON → PIAZZA

Logic

Erik

Propositions

A **proposition** is a statement that is either true or false.

"Blue is better than gold" is not a proposition

"This dog is a cat" is a proposition.

Combining propositions

and: ($P \wedge Q$) is true when both P and Q are true. false otherwise

or: ($P \vee Q$) is true when at least one of P, Q is true

not: ($\neg P$) is true when P is not true

implies: ($P \Rightarrow Q$) is true unless P is true and Q is false

Important Logic Rules

$$(P \Rightarrow Q) \Leftrightarrow ((\neg P) \vee Q)$$

$$\neg(P \vee Q) \Leftrightarrow (\neg P) \wedge (\neg Q)$$

$$\neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$$

$$(P \Rightarrow Q) \Leftrightarrow ((\neg Q) \Rightarrow (\neg P))$$

$$(P \Rightarrow Q) \Leftrightarrow (\neg P) \vee Q$$

Proposition Practice

1. Distribute negations so that negations only apply to single propositions:

$$\neg((A \Rightarrow \neg B) \vee (P \vee Q))$$

2. True or false?

$$((\neg P \Rightarrow \neg Q) \Leftrightarrow (P \Rightarrow Q))$$

3. True or false?

$$(P \Rightarrow Q) \Leftrightarrow (\neg((\neg Q) \wedge P))$$

Proposition Practice Solutions

1. Distribute negations so that negations only apply to single propositions: ¬ ((A ⇒ ¬ B) ∨ (P ∨ Q))

   ⇔ ¬((¬A ∨ ¬B) ∨ (P ∨ Q))
   ⇔(¬(¬A ∨ ¬B) ∧ ¬(P ∨ Q))
   ⇔(A ∧ B) ∧ (¬P ∧ ¬Q))

2. True or false? ((¬ P ⇒ ¬ Q) ⇔ (P ⇒ Q))

   False. Convert the LHS using the contrapositive into: Q ⇒ P. Converse is not equivalent to the original statement, therefore these two expressions are not equivalent.

3. True or false? (P ⇒ Q) ⇔ (¬ ((¬ Q) ∧ P))

   True.
   Rewrite P ⇒ Q as (¬ P) ∨ Q.
   Then distribute the NOTs on the RHS to get ((¬ P) ∨ Q

Quantifiers

For all (∀): $\forall\ x \in K$, P(x) means for every element x within the set K, P(x) is True

There exists (∃): $\exists\ x \in K \mid$ P(x) means that there exists an element x of the set K such that P(x) is True

Negating quantifiers:

$$\neg\ (\forall\ x, P(x)) \Leftrightarrow \exists\ x, \neg\ P(x)$$

$$\neg\ (\exists\ x, P(x)) \Leftrightarrow \forall\ x, \neg\ P(x)$$

Quantify These!

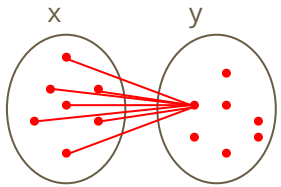
True or False?

1. $(\forall\ x, \exists\ y : P(x,y)) \Leftrightarrow (\forall\ y, \exists\ x : P(x, y))$
2. $(\forall\ x, \exists\ y : P(x,y)) \Rightarrow (\exists\ x : \exists\ y : P(x,y))$
3. $(\exists\ x : \forall\ y, P(x,y)) \Rightarrow (\forall\ y, \exists\ x : P(x,y))$
4. $(\exists\ x : \forall\ y, P(x,y)) \Leftrightarrow (\forall\ y, \exists\ x : P(x,y))$

Quantifier Solutions

1. $(\forall x, \exists y : P(x,y)) \Leftrightarrow (\forall y, \exists x : P(x, y))$

   False. Draw pictures for this!

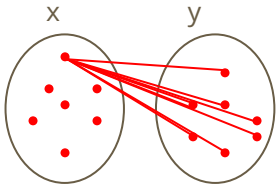


Assume the LHS is true. So all we know is that for every x, there exists a y that makes P(x, y) true. So let's say that this is the same y for every x. Does this necessarily imply that for every y, there exists an x which makes P(x, y) true? Look at the diagram, are there y's that are not paired with x by a line?

Look at the same picture from above! Since every single x is paired with some y that makes P(x, y) true, it must be true that there exists some x that is paired with a y. Just choose any x from the left circle

2. $(\forall x, \exists y : P(x,y)) \Rightarrow (\exists x : \exists y : P(x,y))$

   True.

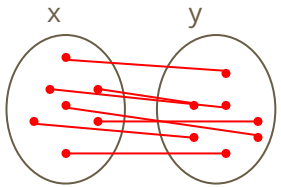


The LHS means that there is a line from one x to every single y. So every y in the right circle is connected to at least one x.

3. $(\exists x : \forall y, P(x,y)) \Rightarrow (\forall y, \exists x : P(x,y))$

   True.

The only difference here is that we must check the backwards implication. Can we draw diagram where it is not true that while every y is connected to an x, there does not exist an x that is connected to all y?



Methods of Proof

Fahad

Some Proof Techniques

Direct

Contraposition

Contradiction

Cases

Induction

Strong induction

Direct Proof

A **direct proof** proves a statement of the form (P ⇒ Q) by using a sequence of facts *without* making other assumptions.

P ⇒ K because of fact1

⇒ ...

⇒ Q Thus (P ⇒ Q)

Good to use when there is a straightforward set of facts that help prove each step

Contraposition

A proof by **contraposition** proves the contrapositive of the claim, which is equivalent to the claim

$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

$\neg Q \Rightarrow \ldots$

$\Rightarrow \neg P$ Thus $(\neg Q \Rightarrow \neg P)$ is true so $(P \Rightarrow Q)$ is true

Good to use when the contrapositive is easy to find and easier to prove than the original claim

Contradiction

Suppose that claim is false, then ..., then something that is illogical

Suppose $(P \Rightarrow Q)$ false

$\Rightarrow \ldots \Rightarrow (K \wedge (\neg K))$ true [impossible]

Good to use when the falsehood of the claim would make everything really weird

Proof by cases

Prove that we can split up the proposition into more than one case. For each case, prove that the proposition is true.

P is comprised of J, K, ...

J ⇒ ... ⇒ Q

K ⇒ ... ⇒ Q

... Thus P ⇒ Q

This is useful when it is easy to split into cases and when it is difficult to prove as a single case

Induction

Useful for propositions about all values in the set of natural numbers

1. Prove **base case**: P(0) true

2. **Inductive hypothesis:** For arbitrary k, P(k) is true

3. **Inductive step:** prove that P(k) ⇒ P(k+1)

P(0) ⇒ P(1) ⇒ … ⇒ P(k) ⇒ P(k+1) ⇒ …

Thus P(x) true for all x ■

Strong Induction

Strong induction: good for proofs where it's hard to make the inductive step depend on a single value

1. **Base case**
2. Assume that P(x) is true for all values **up to and including** some arbitrary k
3. Prove that (P(x) true for base<= x <= k) ⇒ P(k+1)

Proofs for Days
Use any method of proof you think is appropriate

Even Sums

1. The sum of two even integers is even

1. The sum of two even integers is even

Consider two even integers a and b. Each can be written as a multiple of 2 times some other integer.

$a = 2i, b = 2j$

$a+b = 2i + 2j$

$= 2(i+j)$

This is an integer because the set of integers is closed under addition and multiplication and it is divisible by 2 because we have factored out a 2

Not Even

2. If x is odd, then x is not the sum of two even integers

2. If x is odd, then x is not the sum of two even integers

Consider the contrapositive of this:

If x is the sum of two even integers, then x is not odd.

We already proved this in problem 1.

Thus, the original proposition is true.

Note: It's hard to logically deduce anything if you go about it the "direct" way. Starting from the contrapositive gives you more facts to work with.

Perfect Cubes

3. Every integer that is a perfect cube is equal to, one less than, or one more than a multiple of 9

3. Every integer that is a perfect cube is equal to, one less than, or one more than a multiple of 9

Each cube number is the cube of some integer n. Every integer n is either a multiple of 3, or 1 more or 1 less than a multiple of 3. So these 3 cases are exhaustive:

- Case 1: If $n = 3p$, then $n^3 = 27p^3$, which is a multiple of 9.
- Case 2: If $n = 3p + 1$, then $n^3 = 27p^3 + 27p^2 + 9p + 1$, which is 1 more than a multiple of 9. For instance, if $n = 4$ then $n^3 = 64 = 9x7 + 1$.
- Case 3: If $n = 3p - 1$, then $n^3 = 27p^3 - 27p^2 + 9p - 1$, which is 1 less than a multiple of 9. For instance, if $n = 5$ then $n^3 = 125 = 9\times14 - 1$.

Smallest Rational

4. There is no smallest positive rational number

4. There is no smallest positive rational number

Suppose that the claim is false: There is a smallest positive rational number.
Let's consider that numer r. r can be written as a/b for some integers a,b.

$r = a/b$
consider $b' = b+1$, $r' = a/b'$
r' is positive
$r' < r$

But r is the smallest positive rational number which is a contradiction.

Algebraic Induction

5.

$$\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$$

5.

$$\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$$

Proof by Induction!

Base Case: n = 1

$P(1) \equiv 2^1 = 2^2 - 2 = 4 - 2 = 2$

Inductive Hypothesis: Assume that for an arbitrary k, $\sum_{i=1}^{k} = 2^{k+1} - 2$

Inductive Step: P(k+1)

$$\begin{aligned}\sum_{i=1}^{k+1} 2^i &= 2^1 + \ldots + 2^k + 2^{k+1} \\ &= (2^{k+1} - 2) + 2^{k+1} \\ &= (2^{k+1} + 2^{k+1}) - 2 \\ &= 2 * (2^{k+1}) - 2 \\ &= 2^{k+1+1} - 2 = 2^{k+2} - 2\end{aligned}$$

$$\sum_{i=1}^{n} 2^i = 2^1 + \ldots + 2^n$$

Package Postage

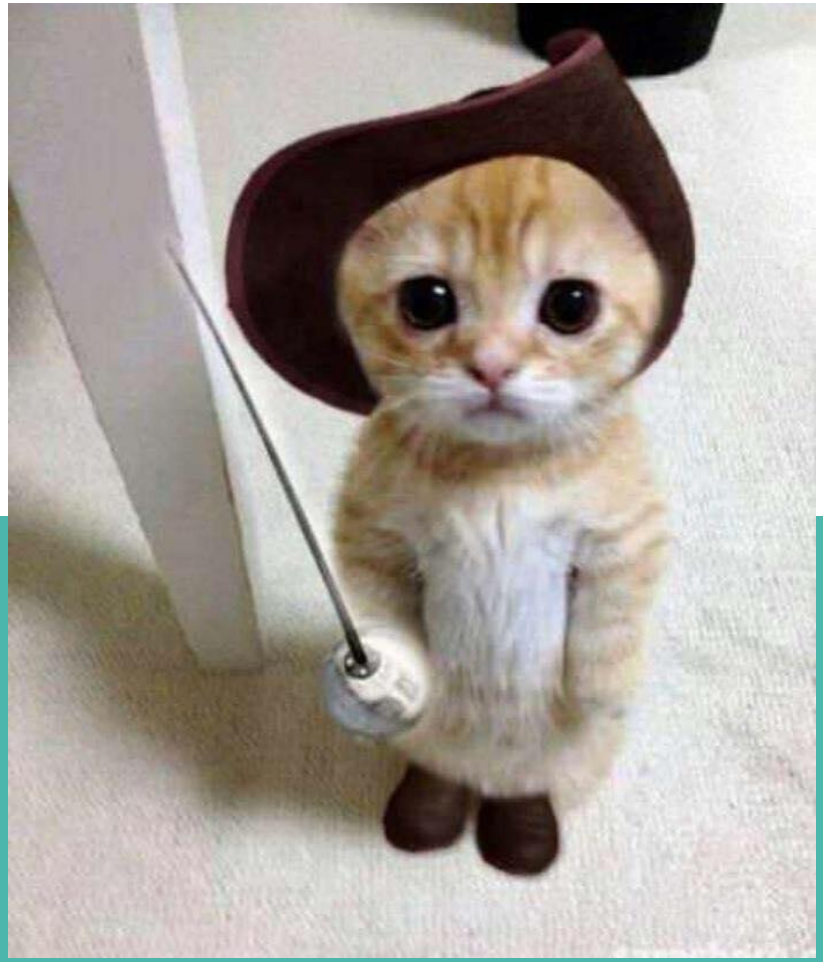
6. A package that costs 12 cents or more can be paid for with some number of 4 cent and 5 cent stamps

6. A package that costs 12 cents or more can be paid for with some number of 4 cent and 5 cent stamps

Base: (cost=12, 12 = 4*3 + 5*0), (cost = 13 = 4*2 + 5*1),
(cost = 14 = 4*1 + 5*2),(cost = 15 = 4*0 + 5*3)

Inductive hypothesis: Suppose that we have show how to construct postage for every value from 12 up through k.

Inductive step: We need to show how to construct k + 1 cents of postage. Since we've already proved base cases up through 15 cents, we'll assume that k + 1 ≥ 16. Since k+1 ≥ 16, (k+1)−4 ≥ 12. So by the inductive hypothesis, we can construct postage for (k + 1) − 4 cents using m 4-cent stamps and n 5-cent stamps, for some natural numbers m and n. In other words (k + 1) − 4) = 4m + 5n. 3 But then k + 1 = 4(m + 1) + 5n. So we can construct k + 1 cents of postage using m+ 1 4-cent stamps and n 5-cent stamps, which is what we needed to show.



Stable Marriage

Nikhil

Definitions

Rogue Couples

Stable Pairing

Traditional SMA

Running SMA

Using the preferences listed below, run through SMA to find a stable pairing

Preferences

Male

1	A, B, C, D
2	B, A, D, C
3	A, C, B, D
4	B, C, A, D

Female

A	1, 3, 2, 4
B	1, 3, 2, 4
C	2, 1, 4, 3
D	3, 2, 1, 4

Stable Marriage Algorithm

Preferences

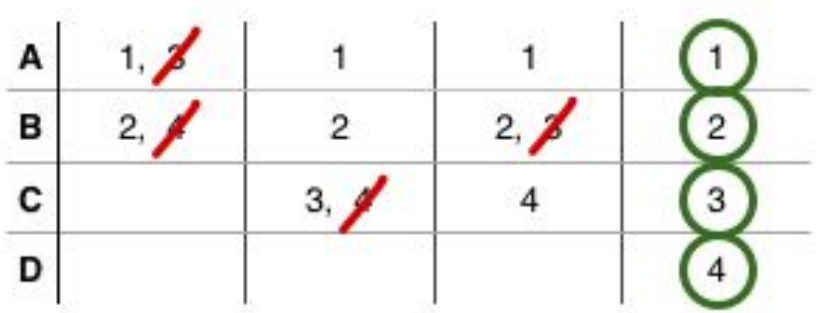
Male

1	A, B, C, D
2	B, A, D, C
3	A, C, B, D
4	B, C, A, D

Female

A	1, 3, 2, 4
B	1, 3, 2, 4
C	2, 1, 4, 3
D	3, 2, 1, 4

Algorithm



Definitions

Halting Lemma — terminates within n^2 days

Improvement Lemma

Optimality/pessimality

Question: How do we obtain a pairing that is female optimal and male pessimal?

Answer: Run the traditional SMA, with roles reversed: women propose to men

Stable Proofs

1. Prove that only one man can be rejected n - 1 times.
2. **One Man's Rejection**: Use this to prove a bound of n(n-1) + 1 on the number of proposals.
3. **Bounding SMA**: construct an example for n = 3

One Man's Rejection

Prove that only one man can be rejected n - 1 times.

Let m be the first man that is rejected n - 1 times.

This means that there are n -1 women who have men on strings.

When man m proposes to the last woman on his list (w), every man is already paired up with a woman. This means that no other man has been rejected by the last woman w that m proposes to, meaning that each other man has been rejected by a maximum of n-2 women, so no other man has been rejected n-1 times.

Bounding SMA

Use previous proof to prove a bound of n(n-1) + 1 on the number of days.

As proven previously, only one man is rejected more than n-2 times, meaning that only one man makes more than n-1 proposals. Because each man must eliminate a woman off his list each day, there is a maximum of n(n-1) days. Then, we add another because at most one man can make n proposals, so the total upper bound on number of days is n(n-1) + 1.

Challenge Solution

One possibility:

Male	
1	A, B, C
2	B, A, C
3	B, A, C

Female	
A	2, 3, 1
B	1, 2, 3
C	3, 2, 1

A	1	~~1~~, 3	3	2, ~~3~~	2
B	2, ~~3~~	2	1, ~~2~~	1	1
C					3

Proposals: 7 = 3 * (3 - 1) + 1

Days: 5 = (3 - 1) * (3 - 1) + 1

Short Exercises

1. What is the minimum number of days the algorithm can take? In what situations will this happen?

2. Construct a scenario with 4 men and 4 women that takes 5 days to run

1. What is the minimum number of days the algorithm can take? In what situations will this happen?

   Answer: 1! Each man has a distinct favorite woman. Rest of men's preference lists, and any of women's preference lists, don't matter!

2. Construct a scenario with 4 men and 4 women that takes 5 days to run

   Answer: one possibility:

Male	
1	A, B, C, D
2	A, B, D, C
3	B, C, D, A
4	C, A, D, B

Female	
A	1, 2, 3, 4
B	2, 1, 4, 3
C	2, 1, 3, 4
D	1, 4, 2, 3

Reconstruct the preference lists of the men and women involved in the following algorithm:

A	-	-	-	-	-	-	-	1
B	4	4	3, ~~4~~	3	2, ~~3~~	2	2	2
C	3	1, ~~3~~	1	1	1	1	~~1~~, 4	4
D	~~1~~, 2	2	2	~~2~~, 4	4	3, ~~4~~	3	3

You also know the following: A has the same preference list as D, and every man likes C better than A. Also, neither B nor C end up with their favorite man.

Answer:

Male

1	D, C, A, B
2	D, B, C, A
3	C, B, D, A
4	B, D, C, A

Female

A	3, 4, 2, 1
B	1, 2, 3, 4
C	2, 4, 1, 3
D	3, 4, 2, 1

Graph Theory

Shreyas, David

Definitions

Incident: edge E is incident on vertices 1 and 2

Adjacent/Neighbors: 1 and 2 are neighbors

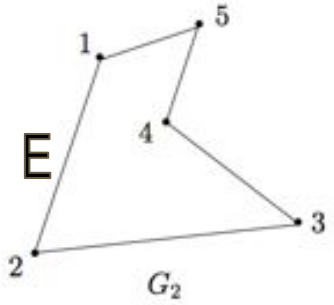
Degree of a vertex: Vertex 5 has degree 2

(Simple) Path: A sequence of edges that don't repeat vertices

Walk: Path that can repeat edges or vertices.

Cycle: (5, 4, 3, 2, 1) is a cycle

Tour: Walk that ends on the same vertex



Even Steven

Prove that the sum of the degrees of the vertices of any graph is even.

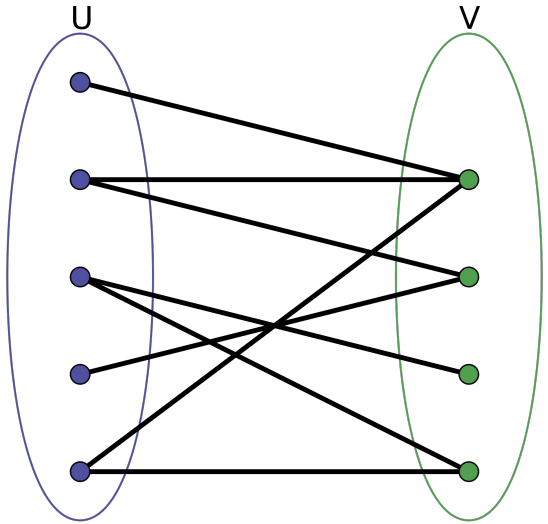
Even Steven Solution

Each edge ends at two vertices. If we begin with just the vertices and no edges, every vertex has degree zero, so the sum of those degrees is zero, an even number. Now add edges one at a time, each of which connects one vertex to another, or connects a vertex to itself (if you allow that). Either the degree of two vertices is increased by one (for a total of two) or one vertex's degree is increased by two. In either case, the sum of the degrees is increased by two, so the sum remains even.

Cycling Through Graphs

Prove that a graph is bipartite **if and only if** it contains no cycles of odd length.

Bipartite: graph where the set of vertices can be divided into two disjoint subsets, such that each edge connects a vertex from one set to a vertex from another subset



Bipartite ⇒ no cycles of odd length

Let graph G be bipartite. Let's define some notation. Let sets A and B be the partition of vertices of G such that for every edge e, one vertex is in set A and the other is in set B.

Suppose G has an odd cycle and let its length be n.

Say that cycle is $v_1, v_2, \dots, v_n, v_1$

Assume that v_1 is in A. This implies that v_2 is in B. This implies that v_3 is in A, and so on.

So every even subscript vertex is in B and every odd one is in A.

This implies v_n must be in A. Since v_1 comes right after, it must be in B.

But now we have v_1 in A and v_1 in B ⇒⇐

No odd cycles ⇒ Bipartite!

Suppose G has no odd cycles

Choose a vertex in G, let's call it v.

Define two sets, A and B. Let set A denote all vertices where the shortest distance to v has odd length. Likewise, B is the set of all vertices where the shortest distance to v has even length. These terms clearly partition the set of all vertices.

Suppose that there are two vertices in A that have an edge between them: a_1 and a_2.

Now we can construct the following cycle: v, …, a_1, a_2, …, v

Note that the length of the path from v to a_1 is odd, the length of the path from a_2 to v is also odd. So the total length of the cycle is odd + odd + 1, which is odd. So we found a cycle of odd length. Therefore no two vertices in A can share an edge. A similar argument can be repeated for the vertices in B. So the graph must be bipartite.

Definitions

Eulerian Walk: A walk that uses each edge exactly once

Eulerian Tour: A walk that uses each edge exactly once and starts and ends at the same vertex

Hamiltonian Cycle: A cycle that passes every vertex in the graph but not necessarily every edge

Walking in Cycles!

If a connected graph has **at most** two odd degree vertices, then it has an **Eulerian walk** between them.

Suppose the two odd degree vertices are A and B.
Start at A and keep following an edge until you get stuck at B.

Claim: you will get stuck at B.
Suppose you don’t. This would imply that you entered some vertex that isn’t A or B and got stuck. But each time you entered the vertex before you used up an even number of edges lying incident to it, or there was an even number from the assumption. Since you got stuck there though, that would imply that the vertex has odd degree, which contradicts our assumption.

We found a path from A to B.

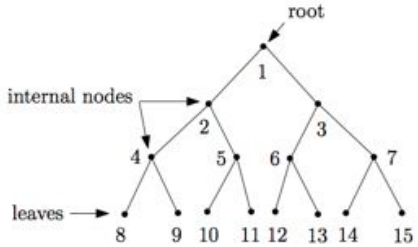
Take the path found in the previous slide. If it contains all the edges we are done. If it doesn’t then remove all edges used on the path. We are left with connected components of the graph. Note that each of these components is of even degree. By Euler’s Theorem, there exists an Eulerian tour in each of these components. Connecting these with the original path gives us an Eulerian path from A to B.

Definitions

Planarity: A graph is planar if it can be drawn on a piece of paper with no edges crossing

Connected: A graph is connected if there exists a path between any two vertices.

Tree: A minimally connected graph



Hypercube:

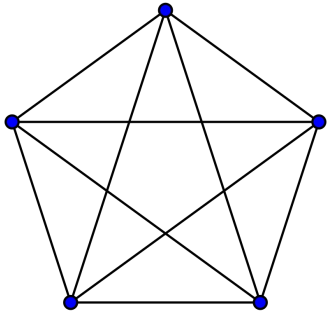
The bit definition: Two vertices x and y are neighbors if and only if x and y differ in exactly one bit position.

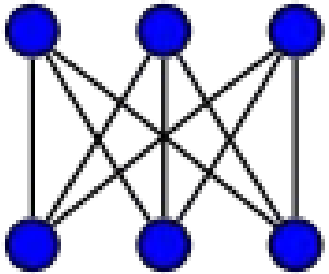
Recursive definition: Define the 0-subcube as the (n-1) dimensional hypercube with vertices labeled 0x. Do the same for the 1-subcube with vertices labeled 1x. Then an n dimensional hypercube is created by placing an edge between 0x and 1x in the 0-subcube and 1-subcube respectively.

Euler's Formula and Graph Planarity

Euler's Formula: **v - e + f = 2** ~~($e^{\pi i} = -1$)~~

2 aplanar graphs: K_5 and $K_{3,3}$





Kuratowski's Theorem: A graph is aplanar iff it has K_5 or $K_{3,3}$ as a subgraph.

Tree's Degrees

Show that if G is a tree with maximum degree greater than or equal to k, then G has at least k leaves.

Tree's Degrees Solution

Draw a vertex of degree k. The k edges incident to this vertex cannot connect to each other. Therefore they must eventually become leaves. So there are at least k leaves.

Alternate solution: Suppose that G has n total nodes and m nodes with degree 1 and at least one node of degree k.
n - 1 - m nodes must have degree at least 2. The sum of all degrees of all vertices is 2n - 2
k + 2(n - 1 - m) + m <= 2n - 2
k + 2n - 2 - 2m + m <= 2n - 2
k - m <= 0
k <= m

Paths and Degrees

Let G be a graph where all vertices have degree at least d. Prove that G contains a path of length d.

Paths and Degrees Solution

Let the longest path have length p. Consider the last vertex in the path. It has degree at least d, therefore, they must all be in the path otherwise we can make a longer path by adding any of those. Therefore, the longest path must include at least d + 1 vertices, meaning the longest path must be at least length d, so a path of length d can be found by taking a subpath of the longest path.

Collapsing Bridges

Edge e is a bridge if the the graph G’ with edge e removed has more connected components than the original graph G. Prove that if each vertex has even degree then there are no bridges.

Collapsing Bridges Solution

Can also be solved using Euclid's Theorem. Since every vertex has even degree, a Euclidian Tour must exist. So when we remove any edge, there must still be a way to get to all other points. So the graph is still connected.

Alternate solution: We may assume that G is connected, for otherwise the lemma could be applied to each component separately. For contradiction, suppose that an edge {v1, v2} = e is a bridge of G. The graph G0 = (V, E \ {e}) has exactly 2 components. Let G1 be the component containing v1. All vertices of G1 have an even degree except for v1 whose degree in G1 is odd. But this is impossible by the handshake lemma.

Disjoint Cycles

Prove that given a connected graph G = (V, E), the degrees of all vertices of G are even if and only if there is a set of edge-disjoint cycles in G that cover the edges of G. (That is, the edge set of G is the disjoint union of the edge sets of these cycles.)

Disjoint Cycles Solution

We would prove this by strong induction on the number of vertices. For the induction basis, consider a graph with with a single vertex and the proposition holds trivially. Assume that this holds for all graphs with up to n vertices for $n \geq 2$. Now consider a graph G with n + 1 vertices. Since each vertex in G is even and of degree at least 2, so G is not a tree (no vertex of degree 1). Thus, there is at least one cycle C in the graph. If G is not this cycle, let G0 be the subgraph (possibly disconnected) obtained from G by deleting all the edges belonging to C. Since every vertex in a cycle is of degree 2 and every vertex in G0 is also even, by the induction hypothesis G0 has a set of edges that is the disjoint union of edge sets of cycles.

Thus, the set of edges of G will be the disjoint union of edge sets of G0 and the deleted cycle. Conversely, consider a graph with a single vertex (set of edges is empty). Obviously, the vertex has an even degree. Assume that this holds for all graphs with up to n vertices for $n \geq 2$. Now consider a connected graph G with n + 1 vertices such that the set of edges in G is the disjoint union of m cycles. Consider any one of these cycles, say C. Since G is connected, there is a vertex in common between C and the rest of the graph G0 , obtained by omitting the edges in cycle C from the set of edges of G. Since every vertex in a cycle has degree 2, and by our induction hypothesis all vertices in G1 have even degrees, all vertices in G will have even degrees. This concludes the proof.

Party Planning

Prove that every set of 6 people contain at least three mutual acquaintances or three mutual strangers.

Party Planning Solution

Let v be a vertex in G. v has 5 potential neighbors. It must have at least 3 neighbors or at least 3 non-neighbors. If v has 3 neighbors then they either form an independent set or two of them are adjacent and these two together with v form a clique of order 3.

If v has 3 non-neighbors, then either they form a clique or two of them are not adjacent and these two together with v form an independent set of order 3.

Vicious Cycle

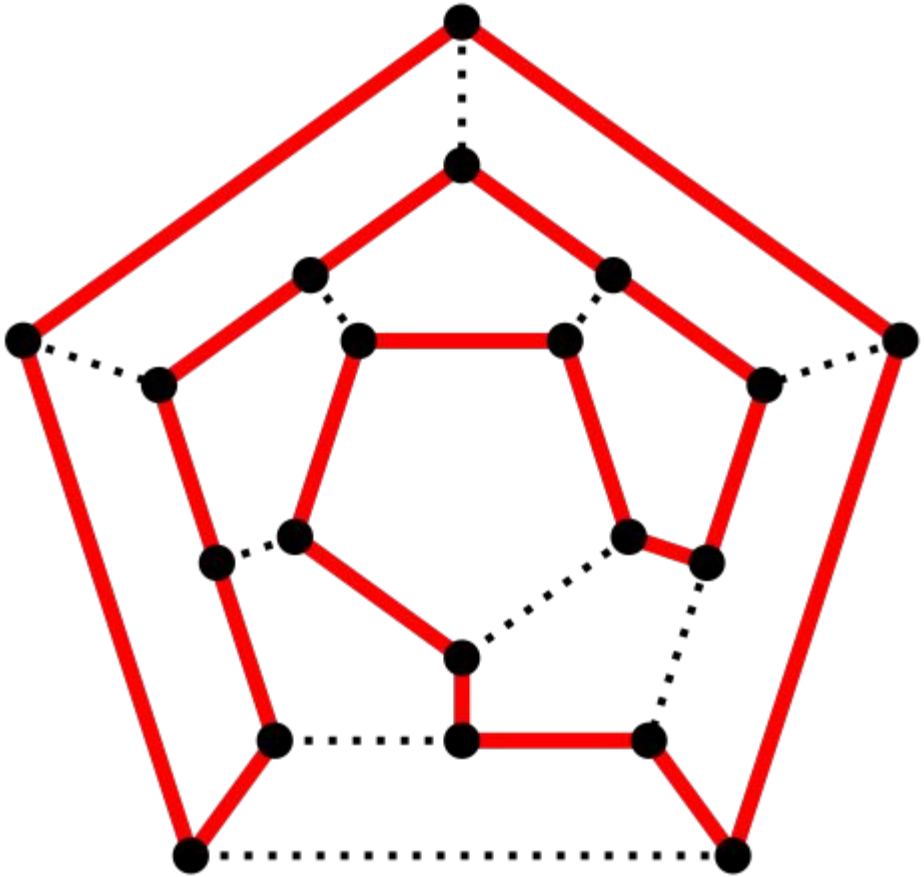
Prove that every graph with n vertices and at least n edges must have a cycle.

Vicious Cycle Solution

Induction on order of G.
Base case: n = 1 → we have a loop
Inductive Hypothesis: Assume that for G of order k we have that every graph with k vertices and at least k edges must have a cycle
Inductive Step: Examine graph G' with k+1 vertices and k+1 edges.
Case 1: There is a vertex with degree 1
We can remove this vertex and the edge incident to it. Since we removed on edge and one vertex we have a graph with k vertices and k edges and can apply the inductive hypothesis.
Case 2: Every vertex has degree at least 2. We have shown in Worksheet 3 that every graph where every vertex has degree at least 2 contains a cycle.

Hamilton and Cubes

For any $n \geq 2$, the n-dimensional hypercube has a Hamiltonian cycle.

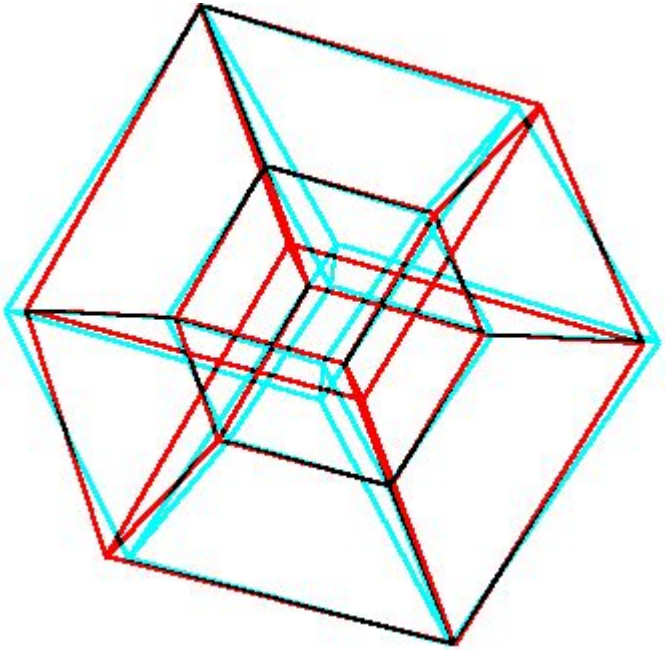


Worksheet 3

Hamilton and Cubes Solution

Solution Redacted (on hw03)

Cube is Life



Any cycle in an n-dimensional hypercube must have even length

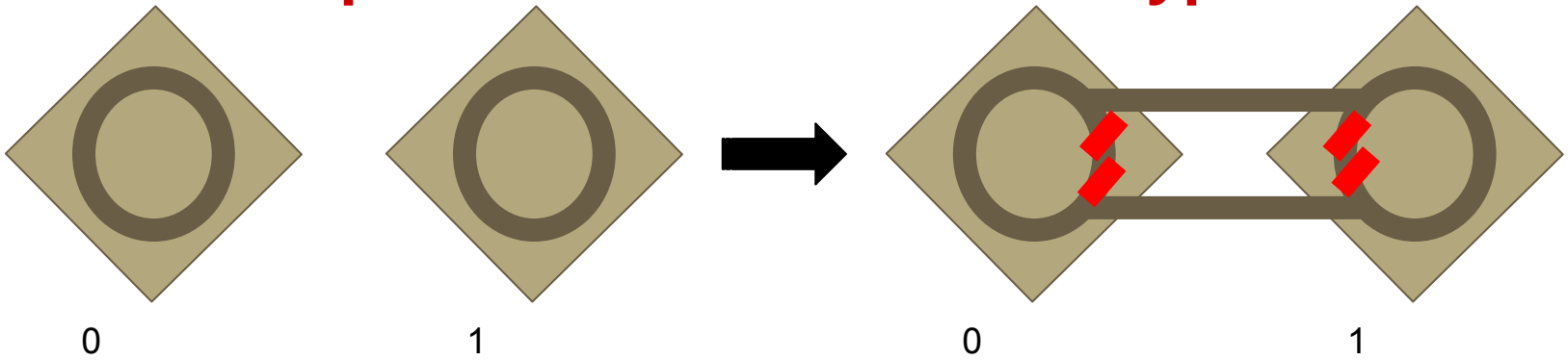
THE WRONG SOLUTION

Induction on dimension n.

Base case: n = 1. Trivially true.

Inductive Hypothesis: Assume that any cycle in an n-1 dimensional hypercube has even length.

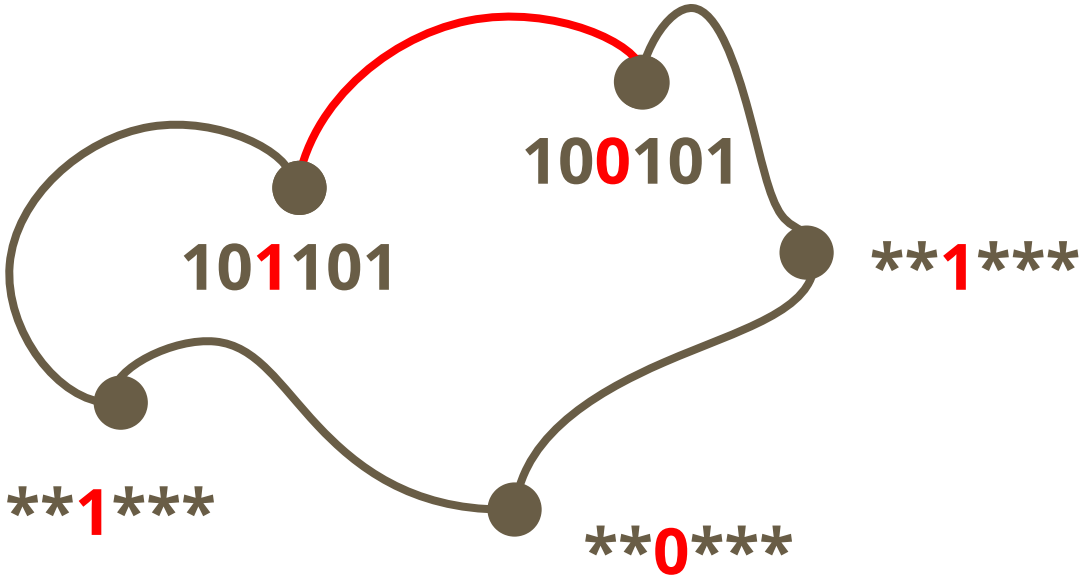
Inductive Step: Draw the n dimension hypercube:



WHAT WENT WRONG?

Cube is Life Bit Solution

Full credit was given for this problem for informal proofs, as long as you had the right idea. Instead of working with the recursive definition of hypercubes, work with the bit definition:

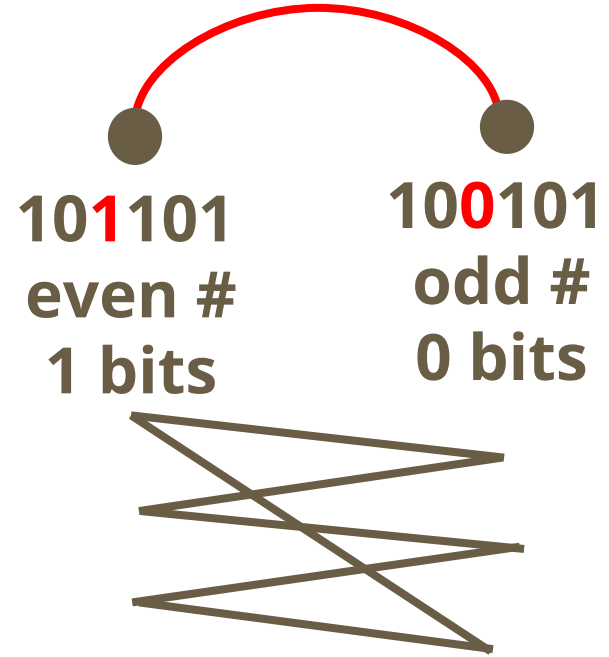


Cube is Life Parity Solution

Claim: Every time you move you go either odd → even or even → odd

There are an even number of the zig-zag edges.

Formally this would be an induction on the length of the path.




gifbin.com

Modular Arithmetic

Anwar

Definitions

congruence: Two integers are congruent if they simplify to the same number in that mod space

x = x + 5 (mod 5). Therefore 2 = 7 (mod5) in the mod 5 space

relatively prime: x and y are relatively prime if GCD(x,y) = 1

multiplicative inverse: y is the multiplicative inverse of x in mod q if xy = 1 (mod q)

Euclidean GCD Algorithm: How to find the multiplicative inverse

Fermat's Little Theorem: Makes doing mod arithmetic easier

Rules/Tips of modular arithmetic

- You can distribute the mod across multiplication (Associative Property)

  `(3*3*3)mod5 = (((3mod5)*3mod5)*3mod5 )`

  - `= (((3mod5)(3mod5))*3)mod5`

- It's easier to work with numbers that are smaller. Use subtraction/addition to write the numbers you are working with in the range of your mod

  Ex: -25 = -25 + (7)*4 = 3 (mod 7)

- **exponents:** Simplify terms by applying the same rules before computing

  Ex: 3^4(mod 5) = 1 (mod 5)

Another tip

- Use repeated squaring to perform heavy computations
- Ex: $3^{21} \pmod 5$
  - $3^2 \pmod 5 = 4$
  - $3^4 = (3^2)^2 = 4^2 \pmod 5 = 1$
  - $3^8 = (3^4)^2 = 1$ since squaring 1 gives us 1
  - $3^{16} = 1$ since squaring 1 gives us 1
  - $3^{21} = 3^{16+4+1} = 3^{16} * 3^4 * 3^1 = 1 * 1 * 3 =$ **$3 \pmod 5$**


BUT CAN YOU DIVIDE?

NO!

Multiplicative Inverses

FIND X: $5 = 7x \pmod 3$

How would you solve this using algebra?

Divide by 7 on both sides

BUT YOU CAN'T DIVIDE!!!!

HOW IT WORKS:

$(7^{-1})5 = x \pmod 3$

$(1)5 = x \pmod 3$

$x = 5 \pmod 3$

CAUTION: DON'T REDUCE! $10/2 \pmod 7$

$\rightarrow 10(2^{-1})(\text{mod } 7) = 3(4) = 5(\text{mod } 7)$

EGCD Algorithm

1. First do Euclid's Algorithm:

$11 = 8 * 1 + 3$
$8 = 3 * 2 + 2$
$3 = 2 * 1 + 1$
$2 = 1 * 2 + 0$

2. Rewrite the above equations putting the remainder on the LHS

$3 = 11 - 8 * 1$
$2 = 8 - 3 * 2$
$1 = 3 - 2 * 1$

What is the inverse of 8 mod 11?

Remember what our goal is: write down 1 as a sum of 8 and 11!

3. Now we need to start with the bottom equation from step 3 and plug in the equation for **2**.

$1 = 3 - 2 * 1$
$1 = 3 - (8 - 3 * 2) * 1 = 3 - (8 - 3 * 2) = 3 * 3 - 8$

Repeat for **3**.

$1 = 3 * 3 - 8$
$= 3 * (11 - 8 * 1) - 8$
$= 3 * 11 - 3 * 8 - 8$
$= 3 * 11 - 4 * 8$

Therefore the inverse of 8 mod 11 is -4, or **7**

Divide by K

Prove that the product of any k>=1 consecutive integers is divisible by k.

Solution

Notice that there are only k different integers in mod k space, and since theses particular k integers are consecutive, they must cover all integers from 0 to k-1 in mod k space. Because one of these numbers is 0 mod k, the product of all of these numbers is always going to be 0. As an example, consider: 4, 5, 6, 7, 8.

We want to show that 4 * 5 * 6 * 7 * 8 mod 5 = 0. When distributed, we have 4 * 0 * 1 * 2 * 3 mod 5 = 0. Just like in this example, the k numbers completely cover the mod space, so there will always be a 0.

More EGCD

Find integers x and y in the range 0,1,…,42 satisfying the following two equations:

$$12x \equiv y+3 \pmod{43}$$

$$x+y \equiv 1 \pmod{43}$$

Solution

Turn 2nd equation into : $y \equiv -x+1 \pmod{43}$

Substituting into the 1st equation: $12x \equiv -x+4 \pmod{43}$

$13x \equiv 4 \pmod{43}$

$x \equiv 13^{-1} \cdot 4 \pmod{43}$

Use the Extended Euclidean algorithm to find $13^{-1} \pmod{43}$:

$\gcd(43,13)\ 1 = 1 \cdot 13 - 3 \cdot (43 - 3 * 13) = -3 \cdot 43 + 10 \cdot 13$

$= \gcd(13,4)\ 1 = 0 \cdot 4 + 1 \cdot (13 - 3 \cdot 4) = 1 \cdot 13 - 3 \cdot 4$

$= \gcd(4,1)\ 1 = 0 \cdot 4 + 1 \cdot 1 = 1$

$13^{-1} \equiv 10 \pmod{43}$

$x \equiv 10 \cdot 4 \equiv 40 \pmod{43}$

Substituting back for y, we have $y \equiv -x+1 \equiv -39 \equiv 4 \pmod{43}$.

We check that $x = 40$, $y = 4$ satisfies the two equations.

FLT (Fermat's Little Theorem)

The rule states that $x^{n-1} \pmod n = 1$ for prime n

This also means that $x^{n} \pmod n = x$ for prime n (do you see why?)

PROOF:

{x·1, x·2, …, x·(p − 1)} is congruent to **{1, 2, … , p − 1} (mod p)**

Multiply elem's of each list together & equate them:

$\mathbf{x^{p-1} \cdot 1 \cdot 2 \cdot \cdots (p-1) \equiv 1 \cdot 2 \cdot \cdots (p-1)}$.

Multiply both sides by $\mathbf{(1)^{-1}, \ldots, (p-1)^{-1}}$

$x^{p-1} \equiv 1 \pmod p$

So You Think You Can FLT?

1) $4^{10} \pmod{11}$

2) $4^{275} \pmod{11}$

Solution:

$4^{10} \pmod{11}$ is a vanilla application of FLT. 11 is prime, so we get 1.

Solution:

$4^{275} \pmod{11} = ((4^{10}) \pmod{11})^{27} \pmod{11} * 4^5 \pmod{11}$

$= 1^{27} \pmod{11} * 4^5 \pmod{11}$

$= (\{[(4 * 4) \pmod{11} * 4] \pmod{11}\} * 4 \pmod{11}) * 4 \pmod{11}$

$= 5 \pmod{11} * 4 * \ldots = 9 \pmod{11} * 4 * \ldots = 3 \pmod{11} * 4$

$= 1 \pmod{11}$

Good luck! :)

HAVE YOU ADDED US ON → PIAZZA ?


MAKE GIFS AT GIFSOUP.COM


coub.com/v/61nvg6g0
COUB