CS 70 Midterm 1 Review

Sinho Chewi, Alvin Wan

Fall 2016

Propositional Logic

- **Key Idea**: Propositional logic is the language of mathematics.
- Avoids ambiguities in common English: “time flies like an arrow”. . . “fruit flies like a banana”
- Mostly straightforward: follow the rules.

Approach 1: Truth Tables

- For simple propositional equivalences, use a truth table.
- Prove the following:

$$Q \wedge \neg(P \Rightarrow Q) \equiv F$$

Somewhat time-consuming. Next. . .

Approach 2: Use Logical Equivalences

- Save time by using logical equivalences we have already proven.
- You should know the basics:
  1. Implications: $P \Rightarrow Q \equiv \neg P \vee Q$
  2. DeMorgan's: $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
  3. DeMorgan's: $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
  4. Distributivity: $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
  5. Distributivity: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
  6. Associativity, commutativity, ...

Logical Equivalences: Example

$$Q \wedge \neg(P \Rightarrow Q) \equiv F$$

Start by rewriting the implication.

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

Use DeMorgan's to distribute the negation.

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

Get rid of the double negation, use associativity to remove parens.

$$Q \wedge P \wedge \neg Q$$

But $Q \wedge \neg Q \equiv F$. □

Quantifiers

- Universal Quantifier ($\forall$): The statement holds true for *all* elements.
- Existential Quantifier ($\exists$): The statement holds true for *at least one* element.
- DeMorgan's Laws for quantifiers: Move the negation “through” the quantifiers, “flipping” them as you go.

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

Proving Equivalences with Quantifiers

Approach 1: Use logical equivalences to make one side look like the other.
Prove the following:

$$\forall x\,\exists y\,P(x,y) \land \neg Q(x,y) \equiv \neg\exists x\,\forall y\,P(x,y) \Rightarrow Q(x,y)$$

Solution:

$$\begin{aligned}\forall x\,\exists y\,P(x,y) \land \neg Q(x,y) &\equiv \forall x\,\exists y\,\neg(\neg P(x,y) \lor Q(x,y))\\ &\equiv \neg\exists x\,\forall y\,\neg P(x,y) \lor Q(x,y)\\ &\equiv \neg\exists x\,\forall y\,P(x,y) \Rightarrow Q(x,y) \quad \square\end{aligned}$$

Proving Equivalences with Quantifiers

Approach 2: Find a counterexample.
Find a counterexample to the following:

$$\exists x\,(\forall y\, P(x,y) \land \forall z\, Q(x,z)) \equiv (\exists x\, \forall y\, P(x,y)) \land (\exists x\, \forall z\, Q(x,z))$$

One possible counterexample: $P(x,y)$ is the statement that x is an additive identity for y, and $Q(x,z)$ is the statement that x is a multiplicative identity for z.

- RHS says that an additive identity exists, and a multiplicative identity exists.
- LHS says that the additive identity and the multiplicative identity are the same!

Moving Quantifiers Around

- Danger!
- We can interchange the order of two universal quantifiers, or two existential quantifiers.
- We can **not** switch an existential quantifier and a universal quantifier!
- We can distribute existential quantifiers over disjunctions.

$$\exists x\, P(x) \vee Q(x) \equiv (\exists x\, P(x)) \vee (\exists x\, Q(x))$$

- We can distribute universal quantifiers over conjunctions.

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

Direct Proofs

To prove an implication $P \Rightarrow Q$, we **assume** P and try to prove Q.

Prove that if y satisfies $\forall x \in X \; y \cdot x = x$, then y is unique.
(Identities are unique!)

Suppose y' is any element satisfying $\forall x \in X \; y' \cdot x = x$.

$$\begin{aligned} y &= y \cdot y' && y' \text{ is an identity} \\ &= y' && y \text{ is an identity} \end{aligned}$$

Deceptively simple. □

Contraposition

Alternatively, to prove $P \Rightarrow Q$, we instead prove $\neg Q \Rightarrow \neg P$.

Prove that if $a + b > c + d$, then $a > c$ or $b > d$.

Assume $\neg Q$: $a \leq c$ and $b \leq d$.
Add the two inequalities and we obtain $\neg P$. □

Why is it easier to use contraposition here? The goal is a disjunction, which is harder to prove. When we assume $\neg Q$, we assume a conjunction (by DeMorgan's), which is easier to use.

How do we deal with disjunctions?

Proof by Cases

When we are given $P \vee Q$, then we know *at least one* of P and Q are true. This leads naturally to the idea of a proof by cases. *Consider each case separately.*

- Make sure your cases are exhaustive!

Prove that $|xy| = |x||y|$.

- Case 1: $x \geq 0$ and $y \geq 0$. Then $xy \geq 0$, $|xy| = xy$, $|x| = x$, $|y| = y$, and $|xy| = xy = |x||y|$.
- Case 2: $x \geq 0$ and $y < 0$. Then $xy \leq 0$, $|xy| = -xy$, $|x| = x$, $|y| = -y$, and $|xy| = -xy = |x||y|$.
- You get the idea. □

Contradiction

Assume the conclusion does not hold. Show that this is absurd!

We have an 8×8 chessboard with the upper left and lower right corners removed. Prove that you cannot tile the chessboard with 2×1 pieces.

Assume, for the sake of contradiction that we *can* tile the chessboard. What can we deduce?

Idea: *Look at the black and white squares.* Each 2×1 piece covers 1 black tile and 1 white tile. If we could tile the chessboard, that would imply that the chessboard has an equal number of black and white tiles. *But this is not so*, because we removed opposite corners. □

Induction

Induction consists of two parts:

- $P(0)$
- $\forall n \in \mathbb{N}\ P(n) \Rightarrow P(n+1)$

Main Idea:

- Start with the $n+1$ case.
- Find some way to *reduce your problem* to the n case. Apply the inductive hypothesis (in other words, *assume* that $P(n)$ is true and use it).
- Now prove $P(n+1)$.
- Don't forget the base case!

Induction

Prove the formula for the sum of a geometric series.

$$\sum_{k=0}^{n} r^k = \frac{r^{n+1}-1}{r-1} \tag{1}$$

Solution: Base case is easy. Assume (1) holds for n. Prove (1) for $n+1$. (P.S. This formula will come in handy later in the semester.)

$$\begin{aligned}
\sum_{k=0}^{n+1} r^k &= \sum_{k=0}^{n} r^k + r^{n+1} \\
&= \underbrace{\frac{r^{n+1}-1}{r-1}}_{\text{Inductive Hypothesis}} + r^{n+1} \\
&= \frac{r^{n+1}-1+r^{n+2}-r^{n+1}}{r-1} = \frac{r^{n+2}-1}{r-1}
\end{aligned}$$

Strong Induction

Strong induction consists of:

- A base case. (Or possibly multiple!)
- $\forall 0 \leq k \leq n \, P(0) \wedge \cdots \wedge P(k) \implies P(k+1)$

Main Idea: While proving $P(n+1)$, we are allowed to assume that all of the statements $P(0), P(1), \ldots, P(n)$ are all true!

Strong Induction

Prove that you can pay for any amount of postage over 12 cents using only 4-cent and 5-cent stamps.

How do we form $n+1$ cents from only 4-cent and 5-cent stamps?
Idea: Let's try a proof by cases. What cases?

- Somehow, we can form n cents from only 4-cent stamps and 5-cent stamps. If we used a 4-cent stamp, we can replace it with a 5-cent stamp.
- What if we didn't use a 4-cent stamp? If we knew that $n \geq 15$, then since no 4-cent stamps were used, we must have at least three 5-cent stamps. We can replace them with four 4-cent stamps.

We're done! Almost.

Base Cases

Don't forget the base case.

In our proof of the inductive step, we had a case in which $n \geq 15$. How do we justify this assumption? Prove it!

- $P(12)$: Use three 4-cent stamps.
- $P(13)$: Use one 5-cent stamp and two 4-cent stamps.
- $P(14)$: Use two 5-cent stamps and one 4-cent stamp.
- $P(15)$: Use three 5-cent stamps.

Now we're done. □

Key Idea: The base cases in strong induction depend on what you assume in the proof of your inductive step.

Stable Marriage

It's all about the definitions!

- A **matching** assigns each man to exactly one woman, and vice versa.
- A **rogue couple** is a pair (m, w) such that m prefers w over his current partner in the matching, and w prefers m over her current partner in the matching.
- A matching is **stable** if there are no rogue couples.
- We say w is m's **optimal partner** if m prefers w over his partners in all other *stable* matchings. *Important*: We are only considering stable pairings!
- We say a stable pairing is **male-optimal** if every man is paired with his optimal partner.

Proof Intuitions

We will go over all of the proven results, giving the *intuition* behind the proofs instead of the proofs themselves.

The idea is that when you go over the slides, you should be able to fill in the details on your own, given the intuitions.

Let's begin!

Termination

Why does the algorithm terminate?

Proof Intuition: Every day, either a man gets rejected, or the algorithm terminates. Each rejection crosses off a woman on some man's preference list, and their preference lists are only so big.

Okay, actually that was the entire proof. □

Improvement Lemma

Every day, the women are at least as happy as they were the day before.

Proof Intuition: Induction. On day *n*, either a woman has no one, or she has a man. If she has no one, of course things can only get better for her! But if she has a man on a string, he'll come back the next day.

The statement of the lemma is pretty intuitively clear already. Still useful, though.

Completeness

How do we know every man is matched with a woman at the end?

Proof Intuition: Improvement Lemma. If there is some man who is not matched at the end, he was rejected by n women. By the Improvement Lemma, each of those n women has someone better on their strings. But now we count $n + 1$ men…whoops!

Stability

How do we know the pairing given by the algorithm is stable?

Proof Intuition: Keep track of definitions. If (m, w) is a rogue couple, then m must have proposed to w first (he likes her better than his current partner). But he's not together with w right now, which means...she rejected him! So w would actually not rather be with m after all. Not a rogue couple.

Male-Optimality

Can we show that the pairing given by the algorithm is male-optimal?

Proof Intuition: Well-Ordering Principle. Let *m* be the first man who got rejected by his optimal partner. The woman he asked out must like some other man better. . . and that man must like her a lot too, since *m* was supposed to be the first one rejected by his optimal partner! Rouge couple?

Small Counterexamples

Approach 1: Always try small counterexamples first.

Prove or disprove: Suppose all men have the same preference lists. The women that every man likes the least must be matched with the man she likes the least.

Not so.

$$M_1 : W_1 > W_2 \qquad W_1 : M_1 > M_2$$
$$M_2 : W_1 > W_2 \qquad W_2 : M_2 > M_1$$

Trying out this small counterexample can save you a lot of time/frustration, compared to immediately trying to prove the statement.

Rogue Couples

Approach 2: Many stable marriage questions require proof by contradiction: specifically, find a rogue couple (m, w) which contradicts the stability of a pairing.

Homework question: R and R' are stable pairings. Suppose (m, w) are a couple in R, but not in R'. Prove that if m prefers R, then w prefers R', and vice versa.

Suppose that both m and w prefer R over R'. This means that both m and w prefer each other over their partners in R', which is the definition of a rogue couple. This contradicts the stability of... R? R'? (The answer is R'.)

Graphs

- A graph $G = (V, E)$ has vertices and edges.
- The **degree** of a vertex is the number of edges incident to it.
- A graph is **connected** if from any vertex, you can reach any other.
- An **Eulerian tour** visits every edge exactly once. Sufficient and necessary conditions for the existence of an Eulerian tour? Every vertex must have even degree and the graph is connected.
- Paths, cycles, walks, tours. . . Make sure to read the clarifying Piazza post about graph theory definitions.

Graph Induction

Avoid build-up error. Start with a graph of $n+1$ vertices (or $n+1$ edges) and *remove one*. The resulting graph is smaller, so apply the inductive hypothesis to the smaller graph. *Add the vertex/edge back to the graph.* Now, prove your statement!

Graph Proofs

Show that every graph (with $|V| \geq 2$) has two vertices of the same degree.

Solution: For a graph of n vertices, what is the range of values that its degree can be?

$$\{0, \ldots, n-1\}$$

(Why not n?) There are n possible values, and n vertices. If we want the vertices to all have different degrees, then for each $i \in \{0, \ldots, n-1\}$, there is a vertex with that degree. (Pigeonhole Principle) A vertex with degree 0, in the same graph as a vertex with degree $n-1$... Contradiction! □

Graph Proofs

Prove that the edges of a graph with maximum degree d can be colored with $2d-1$ colors, such that no two edges which share a vertex also share the same color.

Solution: Induction (on the number of edges).

- A graph with one edge can indeed be colored with 1 color.
- Take a graph with $n+1$ edges and remove an edge. By the inductive hypothesis, the resulting graph with n edges has degree at most d and can be colored by $2d-1$ colors. Add the edge back in: the edge was touching two vertices u and v. Since the maximum degree of the vertices was d, then u and v are each incident to at most $d-1$ other edges, for a total of $2d-2$ other edges which share a vertex with (u, v). We can use the $(2d-1)$th color for the edge we just added back! □

Special Graphs

- **Trees** have many equivalent characterizations.
  - Acyclic and connected.
  - Connected with $n-1$ edges (where n is the number of vertices).
  - Between any vertices u and v, there is a unique path from one to the other.
- **Complete graphs** have every possible edge. How many? $n(n-1)/2$.
- **Hypercubes**: remember the bit-string representation! A hypercube of dimension n has a vertex for each length-n bit-string.
  - When is there an edge between two vertices? When the vertices differ by 1 bit.
  - How many edges in a hypercube? $n2^{n-1}$.

Modular Arithmetic

- Performing computations *modulo n* effectively means setting $n = 0$. For example, what is 30 mod 7? Answer: $30 = 4 \cdot 7 + 4$, so $30 \equiv 4 \pmod 7$.
- Addition, subtraction, and multiplication work in the same way as before, except take the result modulo n at the end.
- Division...trickier.
  - A number x has a multiplicative inverse ($x^{-1} \pmod n$) if and only if $\gcd(x, n) = 1$.
  - Why do we like primes? For a prime p, $\gcd(x, p) = 1$ *for every* $x \neq 0$.

Division Modulo n

Solve:

$$9x \equiv 12 \pmod{11}$$

Test tip: It's probably faster to just list all of the multiples of 9 until we find one which equals $1 \pmod{11}$. Why does this work?

9, 18, 27, 36, 45 ... but 45 mod 11 = 1, so we're done. $9 \cdot 5 \equiv 1 \pmod{11}$, so $9^{-1} \pmod{11} = 5$. Multiply both sides of the equation by 5.

$$5 \cdot 9x \equiv 5 \cdot 12 \pmod{11}$$

$$x \equiv 5 \pmod{11}$$

Repeated Squaring

Compute

$$11^{56} \bmod 7$$

Uh-oh. We're going to be here for a while. Not really! Use repeated squaring.

$$\begin{aligned}
11 \bmod 7 &= 4 \\
11^2 \bmod 7 &= 4^2 \bmod 7 = 2 \\
11^4 \bmod 7 &= 2^2 \bmod 7 = 4 \\
11^8 \bmod 7 &= 4^2 \bmod 7 = 2 \\
11^{16} \bmod 7 &= 2^2 \bmod 7 = 4 \\
11^{32} \bmod 7 &= 4^2 \bmod 7 = 2
\end{aligned}$$

How is this useful?

$$11^{56} \equiv 11^{32+16+8} \equiv 2 \cdot 4 \cdot 2 \equiv 2 \pmod{7}$$

Good Luck!

Get plenty of rest, too!