Final Review

Math 55 with Professor Stankova, GSI James Moody

December 2016

Laws of Propositional Logic

Order of precedence: Parentheses, Negation $\neg$, Conjunction $\wedge$, Disjunction $\vee$, Implication $\rightarrow$, Bi-implication $\leftrightarrow$.

Exercise: Use the order of operations for the Boolean connectives to fill in the parentheses in the following formulas:

$$P \wedge \neg Q \vee R$$

$$\neg P \rightarrow Q \wedge R$$

$$P \vee Q \wedge R \vee S \rightarrow T \vee U$$

Commutativity

$$P \wedge Q \equiv Q \wedge P$$

$$P \vee Q \equiv Q \vee P$$

Distributive Laws:

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

Associative Laws:

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$$

$$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$$

DeMorgan's Laws:

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

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

Generalized DeMorgan's Laws:

$$\neg(P_1 \wedge P_2 \wedge .... \wedge P_n) \equiv \neg P_1 \vee \neg P_2 \vee ... \vee \neg P_n$$
$$\neg(P_1 \vee P_2 \vee .... \vee P_n) \equiv \neg P_1 \wedge \neg P_2 \wedge ... \wedge \neg P_n$$

Exercise: Prove the Generalized DeMorgan's Laws by induction starting from the base case, using the OG DeMogran's Laws. (Remember, because of the order of precedence and associativity, you can omit most of the parentheses you would otherwise have to write)

Modus Ponens: If we have established P, and we have established $P \to Q$, then we have established Q.

Modus Tollens: If we have established $\neg Q$, and we have established $P \to Q$, then we have established $\neg Q$.

Resolution / Proof by Cases: If you can prove ϕ under the assumption of P, and you can prove ϕ under the assumption of $\neg P$, then you can conclude ϕ is true.

Exercise: If John likes math, then he either loves Discrete Mathematics or Calculus. If John doesn't like math, then if he doesn't like Calculus, he likes ice cream. John doesn't like calculus. Translate these statements into propositional logic, and prove that either John likes ice cream or he likes Discrete mathematics.

Hint: Try breaking up into cases, based on whether John likes math or not, and then doing a proof by cases.

Negation of Conditionals [IMPORTANT]:

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

First-order/Predicate Logic

A **predicate** names a relation between objects in a given domain. For example, the predicate"$IsEven$" with domain natural numbers could stand for the relation on the natural numbers such that $IsEven(x)$ means x is even. The binary predicate "$\leq$" with domain the real numbers names the less-than-or-equal to relation.

An existential quantifier ($\exists$) is like a giant disjunction ($\vee$) over all the elements in the domain (only one of the possibilities has to be true for the whole sentence to come out true). A universal quantifier ($\forall$) is like a giant conjunction ($\wedge$) over all the elements in the domain (all of the possibilities have to be true for the

whole sentence to come out true).

Negating Quantifiers

$$\neg\forall x\phi(x) \equiv \exists x\neg\phi(x)$$
$$\neg\exists x\phi(x) \equiv \forall x\neg\phi(x)$$

Negating Quantifiers with Inequalities

$$\neg(\forall x > y)\phi(x,y) \equiv (\exists x > y)\neg\phi(x,y)$$
$$\neg(\exists x > y)\phi(x,y) \equiv (\forall x > y)\neg\phi(x,y)$$

Notice that the inequalities do not flip!

Exercise: Find the negation of

$$\exists y\forall x < y\exists z(x + y > z \to \phi(x,y,z))$$

Recall the technique of proof by example/counter-example and proof by cases.

Proving Universal Statements: To prove a statement starting with $\forall x$, you can break up into exclusive and exhaustive cases based on the value of x, and prove each case.

Disproving Universal Statements: To disprove a statement starting with $\forall x$, you just need to a find a single value for x which serves as a counter-example

Proving Existential Statements To prove a statement starting with $\exists x$, you just need to find a single value of x making the formula true.

Proving Existential Statements To disprove a statement starting with $\exists x$, you just need to show that there is no value of x that works (proof by cases can help here).

Exercise: Decide which of these are true, and try proving or disproving them:

Every prime number strictly bigger than 2 is odd.

No negative real number is the square of another real number.

There are no integer solutions to $x^2 - x + 3 = 0$.

There are no integer solutions to $x^2 - 4x + 4$.

Modular Arithmetic

You should review the properties of divisibility and modular arithmetic (just skim through chapter 4, I won't include everything). Here are some key results:

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (That is, there is a unique positive integer $\overline{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\overline{a}$ modulo m.)

FERMAT'S LITTLE THEOREM If p is prime and a is an integer not divisible by p, then

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

Furthermore, for every integer a we have

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

THE CHINESE REMAINDER THEOREM Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Combinatorial Identities for the Soul

Pascal's Identity:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1} \text{ for } n, k \in \mathbb{N}$$

(Do you remember how to prove this? You should know two different ways: algebraic and combinatoric).

Binomial Identity:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \text{ for } n \in \mathbb{N}, x \in \mathbb{R}, y \in \mathbb{R}$$

Suggestion: Try to use this to prove that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. Is there another combinatorial proof of this fact?

Vandermonde's Identity:

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \binom{n}{k}$$

Try proving this by counting the same set in two different ways (think about picking a team of r people from m boys and n girls).

Extended Binomial Theorem:

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k$$

Do you remember what u is allowed to be here? What happens if $u < 0$. Do you know how to compute, say $\binom{-14}{4}$?

Probability and Set Theory

Do you remember:

The principle of inclusion-exclusion (both baby and full)?

Computing the complement?

How to translate statements about set membership in unions, intersections, and complements of sets into disjunctions, conjunctions, and negations?

How to compute conditional probability?

How to use Bayes' Theorem?

What can you say about the sum of the probabilities of disjoint events? (Can it be bigger than 1?)