CS 50010 Module 1

Ben Harsha

Apr 12, 2017

Course details

- Course is split into 2 modules
  - Module 1 (this one): Covers basic data structures and algorithms, along with math review.
  - Module 2: Probability, Statistics, Crypto
- Goal for module 1: Review basics needed for CS and specifically Information Security
  - Review topics you may not have seen in awhile
  - Cover relevant topics you may not have seen before

IMPORTANT

This course **cannot** be used on a plan of study except for the IS Professional Masters program

Administrative details

- Office: HAAS G60
- Office Hours: 1:00-2:00pm in my office
    - Can also email for an appointment, I'll be in there often

- Course website
    - cs.purdue.edu/homes/bharsha/cs50010.html
    - Contains syllabus, homeworks, and projects

Grading

- Module 1 and module are each 50% of the grade for CS 50010
- Module 1
  - 55% final
  - 20% projects
  - 20% assignments
  - 5% participation

Boolean Logic

- **Variables/Symbols:** Can only be used to represent 1 or 0
- **Operations:**
  - Negation
  - Conjunction (AND)
  - Disjunction (OR)
  - Exclusive or (XOR)
  - Implication
  - Double Implication

- **Truth Tables**: Can be defined for all of these functions

Operations

- Negation ($\neg p$, $\overline{p}$, p^C, not p) - inverts the symbol. 1 becomes 0, 0 becomes 1
- Conjunction ($p \land q$, p && q, p and q) - true when both p and q are true. False otherwise
- Disjunction ($p \lor q$, p || q, p or q) - True if at least one of p or q is true
- Exclusive Or (p xor q, $p \veebar q$, $p \oplus q$) - True if exactly one of p or q is true
- Implication ($p \rightarrow q$) - True if p is false or q is true ($q \lor \neg p$)
- Double implication ($p \leftrightarrow q$) true if p and q are the same

Translating from English

- We often need to represent an idea logically to work with it
- “If it is raining then the ground is wet”
- p = it is raining
- q = the ground is wet

- p -> q

- Identify the variables
- Identify the relationship
- Combine

4	E	7	K

Each card has a number on one side and a letter on the other side.

Which card(s) must you turn over in order to test the truth of the proposition that if a card has an even number on one face, then its opposite face has a vowel?

https://www.menti.com/114f94

De Morgan’s Laws

- Allows you to apply negation to and and or statements

- De Morgan’s Laws:
  - $\neg (p \vee q) = \neg p \wedge \neg q$
  - $\neg (p \wedge q) = \neg p \vee \neg q$

- All ands become ors and vice versa

De Morgans examples

- p -> q
- (p v q) -> a
- (p v q v a) ^ b

Quantifiers

- Universal quantifier “For all” - ∀
- Means that a statement applies to any possible choice
- ∀ real x, 2x is also real

- Existential quantifier “There exists” - ∃
- Means that there is at least one example where the statement is true
- ∃ x such $x^2 = x$

- ∃ ! - Shows up sometimes. Means “Exists a unique”, as in there exists exactly one item

- ∀ ∀ ∃ ∃

Negating quantifiers

- During negation ∃ becomes ∀ and vice versa
- “There is a person who has been to Indianapolis
- ∃ p , p has been to Indy
  Negated: ∀ p, p has not been to Indy
- “Someone has taken a flight on every airline in the world”
- ∃ p ∀ a, p has taken a flight on all airlines
  Negated: ∀ p ∃ a, p has not taken a flight on a

Logical Equivalence

- Often need to show that two things are the same
- Most basic way to show this: truth tables
- Example on the board
- (p -> q) ^ (q -> p) = p <-> q

Contraposition

- The following is true for all implications
- If p -> q then ¬q -> ¬p
  - Proof is by truth table, on board
- If it is raining then the ground is wet
- If the ground is not wet, then it is not raining
- Used often in proofs - if you prove the contraposition you have proven the original statement

Contraposition examples

- $(p \vee q) \rightarrow a$

- If x and y are two integers for which x+y is even, then x and y have the same parity (oddness/evenness)

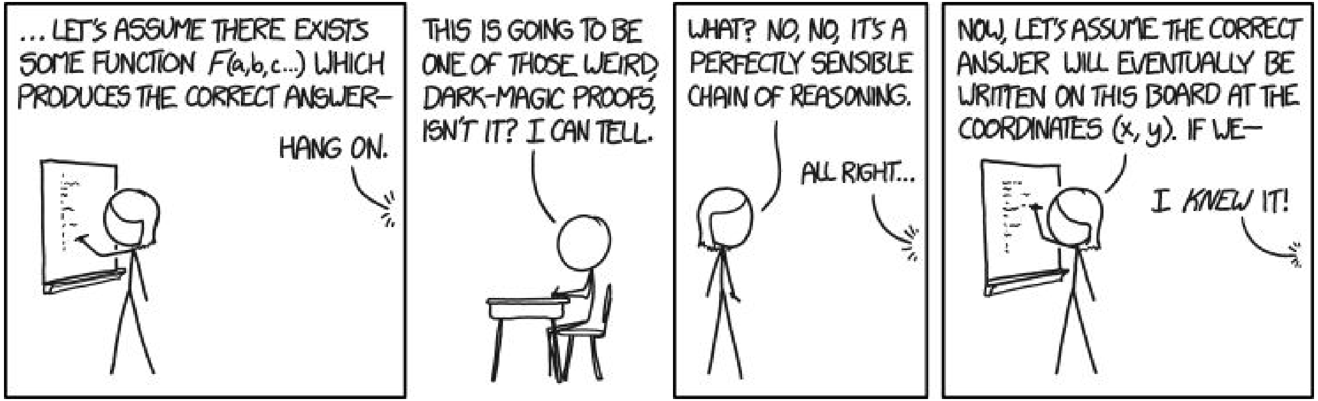
Solving more complicated logic problems

- Break the problem into parts - treat groups of logical statements as “chunks”. Work on the larger chunks first, then solve for smaller parts

- (p^q)v(z^y) ➔ (a v b v c)

Proofs

- Slides adapted from TAMU
- Relevant XKCD



A **theorem** is a statement that can be shown to be true.

A **proof** is a valid argument that establishes the truth of a theorem.

A **direct proof** (of $p \rightarrow q$ or $\forall x\ P(x) \rightarrow Q(x)$) assumes the antecedent (p) and uses the rules of inference to show that the consequent (q) must also be true.

Theorem: If x, y are odd integers, then $x \cdot y$ is odd

Proof:

- **Indirect proofs** are not direct.

Proof by Contraposition

Want to prove $p \to q$

Show $\neg q \to \neg p$

Proof by Contradiction

Want to prove p

Show $\neg p \to (r \land \neg r)$

Theorem: If $n^3 + 13$ is an odd integer, then n is an even integer.

Proof:

- To prove $\neg\forall x\ P(x)$, find any example (**counterexample**) that satisfies $\neg P(x)$.

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

A kind of *existence proof*.

Example: Show that not every positive integer is the sum of the squares of 2 integers.

Proof:

Exhaustive Proof: prove for every element in the universe of discourse.

Proof by Cases: divide universe of discourse into cases and prove for every case.

Forward Reasoning

Start with premises, plug and chug to the conclusion.

Direct proof

Start with negation of conclusion, plug and chug to negation of premises

Indirect proof

Backward Reasoning

Work backwards from the conclusion to find the correct steps for a direct proof

Proof by Contradiction

- Start with some claim
- Assume the claim is false
- Show that some impossible thing arises

- Example: You cannot divide by zero

Football Prediction

@

by 3.

Ben's Note: Final score was 29-16

Intermission

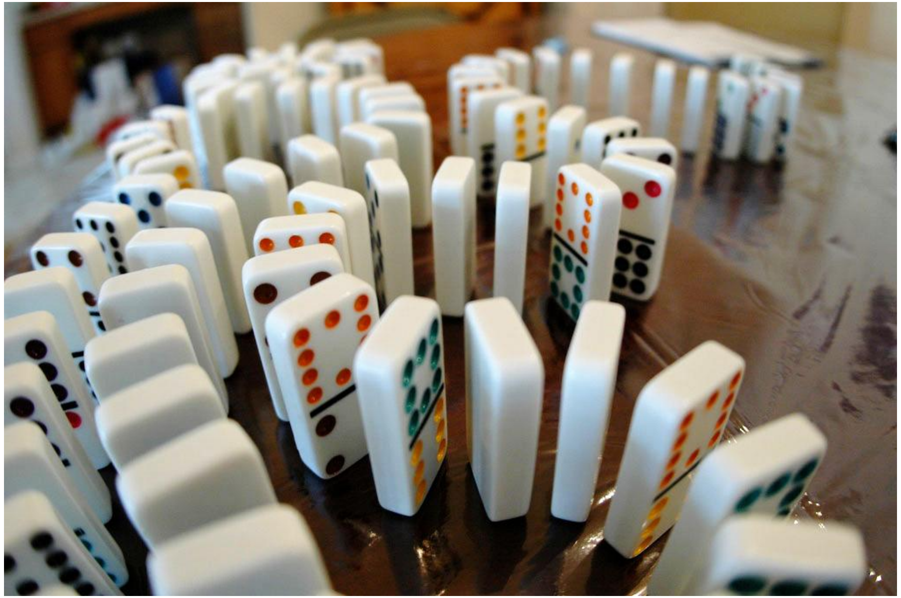
- Questions?

Sample questions

- For all integers n, if n^2 is odd, then n is odd. (Contradiction)
- Prove that if n^2 is even then n is even (Direct)
- If x*y is even then at least one of the two is even(Contrapositive)

Induction

- Final method for today
- Very common in computer science (as it will relate to recursion)
- Start with a base case, show that it is true
- Assume it is true for n, show that it is true for n+1



How to prove something by induction

- Sum from i=1 to n of $2^i = 2^{n+1} - 2$
- Step 1: Establish a base case
- Step 2: Assume that it is true for n
- Step 3: Prove that if it is true for n, it is true for n+1

Examples

- Prove that $1+2+3+...+n-1+n = (n(n+1))/2$
- Prove that $n! > 3^n$ for all $n >= 7$
- $1^2 + 2^2 + 3^2 + .. + n^2 = n(n+1)(2n+1) / 6$

Assignments

- First assignment is posted, it is due in one week.
- Download from cs.purdue.edu/homes/bharsha/cs50010.html
- Can also just go to cs.purdue.edu/homes/bharsha and follow links
- 2-3 questions per lecture, recommended to work as we go

End of lecture 1

If time remaining: See if we can work through the blue-eyed island puzzle

Also - survey to fill out