CMPSC 40, Section 3

TA: Jiyu Zhang

Email: jiyuzhang at ucsb dot edu

October 20, 2020

To Jiyu: remember to record the section.

1 Schedule

Quick Recap - 5 min
Practice Problems - 30-35 min
Tips & Recommendation - 10 min

2 Proof strategies recap

1. Prove conditional statement $p \to q$: direct proof; proof by contraposition: $\neg q \to \neg p$; proof by contradiction.
   - **proof by contradiction**.
   - say we want to prove conditional statement $p \to q$. i.e. if p is true, then q is true.
   - it must follow the truth table of $p \to q$. When p is false, it's always true. All we need to prove is to prove q is true.
   - we can prove $\neg q$ is false, which implies q is true.
   - assume p is true, and $\neg q$ is true. Try to prove $\neg q$ contradicts p.
2. Strategies for specific propositions.
   - proof by cases: enumerate all possible cases.
   - existence proofs:
     (a) constructive proofs. (e.g. show Alice is in the theatre.)
     (b) non-constructive proofs: proof by contradiction, **probabilistic proofs:** show the probability that a random element doesn't satisfy the properties with probability at most < 1.
   - **uniqueness proofs**: need to show two things:
     (a) existence
     (b) uniqueness: at most one element satisfies requirement.
3. more... inductions, counting, diagonalization (the halting problem), probabilistic method...

3 Practice problems

3.1

Pigeonhole principle.

Show that if k is a positive integer and $k+1$ or more balls are placed into k boxes, then there is at least one box containing two or more balls. (Hint. proof by contradition.)

Proof.

Assume for the sake of contradiction that there is no box containing more than one ball, then there are at most k balls, then we reach a contradiction because we placed more than $k+1$.

Application: suppose a box contains 2 blue balls, 1 yellow balls, 2 red balls. How many balls do you have to take out so that you can guarantee that you have a red ball?

3.2

Triangle Inequality.

Prove that for all $x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$,

where $|x|$ denotes the absolute value of x. i.e. $|x| = x$ for $x \geq 0$ and $|x| = -x$ for $x < 0$.

Proof.

First we show that $x \leq |x|$, which is an easy proof by cases: if $x \geq 0$, $x = |x|$, and if $x < 0$, $x < |x|$.

Next, without loss of generality, the same holds for y. We have $y \leq |y|$.

Consider the two cases:

i. $x + y \geq 0$.

We have $|x + y| = x + y \leq |x| + |y|$ in this case, indeed.

ii. $x + y < 0$.

We have $|x + y| = -(x + y) = -x - y \leq |x| + |y|$.

We have considered all cases and thus the proof is completed.

3.3

Sets game.

1. prove that if $A \subseteq B$, $B \subseteq C$, then $A \subseteq C$
2. let $A = \{1, 2, 3, 4\}$ $B = \{2x | x \in A\}$. Show the set B.
3. let $C = \{x \in \mathbb{N} | 0 < x < 10 \text{ and x is even}\}$. Determine the relationship between B and C?
4. what's the union of A and C?
5. let $D = \{x \in N | x \in [0, 10]\}$ be the universal set, what's the complement of $A \cup C$ with respect to D?
6. what's the difference of A and $\overline{B}$ with respect to D?
7. define the **symmetric difference** between A and B to be $A \cup B \setminus A \cap B$, denoted as $A \Delta B$, determine the set that is the symmetric difference of $\{2, 3, 4, 5\}$ and $\{3, 4, 5, 6\}$.
8. show the subsets of the set in 7.

Solutions

1. since $A \subset B$, every element in A is also an element in B. Similarly, every element in B is also an element in C, we can conclude that every element in A is also an element in C.
2. {2, 4, 6, 8}
3. $C = \{2, 4, 6, 8\}$. $B = C$.
4. $\{1, 2, 3, 4, 6, 8\}$
5. $\{0, 5, 7, 9, 10\}$
6. $\overline{B} = \{0, 1, 3, 5, 7, 9, 10\}$, $A - B = \{2, 4\}$.
7. $\{2, 6\}$
8. $\{2\}, \{6\}, \{2, 6\}, \emptyset$

3.4

Prove that every integer > 1 can be a product of primes.

(Hint. Proof by contradiction. You might want to start with assume the existence of the smallest integer $m > 1$ that is not a product of primes.)

Proof.
Let's assume there is an positive integer $m > 1$ that is the smallest integer that is not a product of primes.

Therefore there exists a, b such that $m = ab$, and $1 < a < m, 1 < b < m$, which must be a product of primes. Therefore consider ab represented by the product of primes form, m should be a product of primes, a contradiction.

Uniqueness? In fact every m can be uniquely represented by a product of primes, how to prove it? try to figure it out after class. Remember that in the above we showed the existence part, you need to prove that there is at most one product of primes representation of m.

4 Tips

- During this quarter you'll be writing a lot of proofs. Get used to it!
- It's a goal of this course to help you develop the ability to write rigorous proofs.
- Tip 1: Doubt yourself. Try to come up with examples that contradict your statement.
- Tip 2: Speak out. Try to explain your proof, as simple as possible, to yourself/friends. If you can't find any weakness in your proof, you are probably right!
- "You do not really understand something unless you can explain it to your grandmother".
- Tip 3: Slow down, play with mathematics. Mathematics has considerably more logical complexity than most other subjects (or games). Slow down when you feel certain steps are confusing. You often get upset. Be patient, be careful, be curious, and have fun.

5 Further reading for fun (Optional)

- To become an aspiring mathematician/theoretical computer scientist/theoretical cryptographer, at the first step you should learn how to write convincing proofs.
- Even no intention, you will still benefit from thinking rigorously like the professional.
- Course material by Prof. Michael Saks about mathematical reasoning.
- `https://sites.math.rutgers.edu/~saks/300S/`
- Pick whichever part that attracts you to start reading. The first two parts are highly recommended.