MCS-236: Graph Theory Handout #A4

San Skulrattanakulchai

Gustavus Adolphus College Sep 21, 2015

Methods of Proof

- Consider a set of mathematical objects having a certain number of operations and relations defined on them. Take, for example, the natural numbers with the usual arithmetical operations $+, -, \times, \div$, and the $<$ and $=$ relations. We can state various propositions involving these objects, their operations, and their relations. For example,

  $$\forall n(2 < n \implies \neg(\exists x \exists y \exists z(x^n + y^n = z^n))).$$

  How wonderful it would be if, given any such proposition, we could always determine its truth value. Nobody knows of an algorithm for such a determination!

  The accepted method of mathematical investigation is called the *axiomatic method*. An *axiom* is a proposition that is assumed to be true. We begin by declaring a set of axioms governing our *mathematical structure*. From then on, we will accept the truth of any proposition p only when any one of the following occurs:

  1. p is an axiom,
  2. p is a tautology,
  3. p can be *logically inferred* from other true propositions.

  In the last case, p is said to be a *theorem* and the steps that were used to establish the truth of p make up a *proof* of the theorem.

  One property required of an axiom system is that it is *consistent*, i.e., no contradiction can be proved within the system. Existence of a contradiction would render the system totally useless since it allows one to prove any proposition. A desirable property of the system is that it is *complete*, i.e., there exists a proof for every true proposition, and there exists a proof for the negation of every false proposition. Gödel proved that no consistent axiom system powerful enough to include the natural numbers and arithmetic can be complete!

- Definitions are the tool we use to help us understand and communicate a proposition in English. To appreciate definitions, try expressing the following proposition in English (assuming $\mathbb{N}$ is our universe of discourse)

  $$\exists n[(n > 1) \wedge (\exists k(n = 2 \cdot k)) \wedge (\forall d[(d \neq 1 \wedge d \neq n) \implies \forall k(k \cdot d \neq n)]].$$

  As usual we define an integer n to be *even* if there is an integer k such that $n = 2 \cdot k$. Also define a natural number p to be *prime* if $p > 1$ and $p = c \cdot d$ only when $c = p$ or $d = p$. Now we see that the complicated proposition above says "there exists an even prime number," which happens to be true.

- The power of the axiomatic method comes from the general nature of axioms. The mathematical objects, their operations, and their relations that the axioms talk about are *undefined* and are subject to different interpretations. Therefore, there may exist many different *models* (or *worlds*) that satisfy the same set of axioms.

- Consider a proposition q and a set of propositions $\mathcal{P}$. We say that q *follows logically* from $\mathcal{P}$ if q is true in any possible model where all of the propositions in $\mathcal{P}$ are true. In symbol, we write $\mathcal{P} \models q$ and read $\mathcal{P}$ *logically entails* q. This concept is the basis for *inference rules* that we can use to write proofs (item 3 on our list).

- Some important inference rules.

$\frac{p\wedge q}{p}$	(and-elimination)	$\frac{p\wedge q}{q}$	(and-elimination)
$\frac{p}{p\vee q}$	(or-introduction)	$\frac{q}{p\vee q}$	(or-introduction)
$\frac{p,\ q}{p\wedge q}$	(and-introduction)	$\frac{p,\ q}{q\wedge p}$	(and-introduction)
$\frac{p\vee q,\ \neg p}{q}$	(or-elimination)	$\frac{p\vee q,\ \neg q}{p}$	(or-elimination)
$\frac{p \implies q,\ p}{q}$	(modus ponens)	$\frac{p \implies q,\ \neg q}{\neg p}$	(modus tollens)
$\frac{p \implies q,\ q \implies r}{p \implies r}$	(transitivity)		

  One way to prove an inference rule is to use logical equivalences. Another way is to inspect the truth tables and use the definition of logical entailment. (Note: do some example proofs here.)

- Two inference meta-rules not included in the above table are

  $$\emptyset \models True$$

  and

  $$\{p\} \models q$$

  whenever p is logically equivalent to q.

- Almost all proofs in mathematics we are likely to encounter are actually *informal proofs*. Such a proof presumes an intended audience. An informal proof usually skips many little steps and the readers are assumed to be able to fill out the details.

- For this class we will not develop all the mathematics we need from scratch. We assume an axiom system powerful enough to include arithmetic on the real numbers. This means you may use facts you have learned up to the materials typically covered in a precalculus course without proving them.

- **Proving an Existentially Quantified Statement $\exists x.\varphi(x)$.** This is straightforward. We simply pick an element x from our universe of discourse (perhaps after a long period of pondering), and then show that $\varphi(x)$ is true. Let's look at an example.

  Theorem. *Some prime number is even.*

  Proof. Consider the number 2. We have $2 = 2 \cdot 1$ and 1 is an integer. Hence, 2 is even by the definition of evenness. Moreover, the only divisors of 2 are 1 and 2. Therefore, 2 is a prime by the definition of prime. Thus, 2 is both a prime number and even. □

- **Proving a Universally Quantified Statement $\forall x.\varphi(x)$.** We begin by saying, "Let x be any arbitrary element from our universe of discourse," and then proceed to show that φ(x) is true. Our proof will be valid as long as we do not use any properties except those that are known to hold for every element in our universe of discourse. Let's look at an example.

  Theorem. *Every natural number is smaller than some natural number.*

  Proof. Let n be any natural number. It is an arithmetic fact that $n+1$ is a natural number and that $n < n+1$.

  We have shown that for any natural number n there exists a number, specifically the natural number $n+1$, such that n is smaller than it.

  Thus, every natural number is smaller than some natural number. □

  In the formal language, this theorem says $\forall n \exists m(n < m)$. That is, it is of the form $\forall n.\varphi(n)$ where $\varphi(n)$ is $\exists m.\psi_n(m)$, i.e., $\psi_n(m)$ depends on n. The order of quantifiers is important. That's why we pick an arbitrary number n first, and then judiciously pick another number m that is greater than that specific n second.

- **Proving an Implication.** An implication is the most important type of proposition we will be dealing with. Suppose we have to show that $p \implies q$ is true in our axiom system. This means we want to prove that in any model where our axioms and p hold, q also holds. There are three proof methods we can use: **direct proof**, **proof by contrapositive**, and **proof by contradiction**.

  In a direct proof, we assume that the hypothesis p is true in addition to the axioms. We then write a series of valid statements (axioms, tautologies, statements using inference rules) having the conclusion q as the last statement.

  The proof by contrapositive is based on the fact that an implication is logically equivalent to its contrapositive, i.e.,

  $$(p \implies q) \equiv (\neg q \implies \neg p).$$

  It is the direct proof of the contrapositive.

  We will describe the proof by contradiction later.

- **Direct Proof of a Universally Quantified Implication** $\forall x(\varphi(x) \implies \psi(x))$**.**

  Theorem. *For every integer n, if n is even then n^2 is even.*

  Proof. Let n be an even integer. By definition of even integer, $n = 2k$ for some integer k. By the rule of arithmetic, we have $n^2 = (2k)^2 = 2k2k = 2(k2k)$. Since k is an integer and 2 is an integer, and the set of integers is closed under multiplication, we have that $k2k$ is an integer. Thus, n^2 is even (because it can be written as 2 times the integer $k2k$). □

- **Proof by Contrapositive of a Universally Quantified Implication** $\forall x(\varphi(x) \implies \psi(x))$**.**

  Theorem. *For every integer n, if n^2 is even then n is even.*

  Proof. Let n be any integer that is not even. Thus n is odd. By definition of odd integer, $n = 2k + 1$ for some integer k. By the rule of arithmetic, we have $n^2 = (2k + 1)^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since k is an integer and 2 is an integer, and the set of integers is closed under multiplication and addition, we have that $2k^2 + 2k$ is an integer. Thus, n^2 is odd (because it can be written as twice the integer $2k^2 + 2k$, plus 1). Therefore, n^2 is not even. □

- **Proof by Contradiction.** This proof method is based on the fact that any proposition p is logically equivalent to the proposition $\neg p \implies False$. So instead of proving p, we directly prove that $\neg p \implies False$. Let's look at an example.

  Theorem. $\sqrt{2}$ *is an irrational number.*

  Proof. Suppose for the sake of contradiction that $\sqrt{2}$ is rational. By the definition of rational number, there exist integers n and m such that their only common positive divisor is 1 and that

  $$\sqrt{2} = n/m.$$

  By the rule of arithmetic, we can then square both sides to get

  $$2 = n^2/m^2$$

  and again by the rule of arithmetic, we can then multiply both sides by m^2 to get

  $$2m^2 = n^2.$$

  The above equality says that n^2 is an even number by the definition of even number. By the last theorem we proved, we conclude that n is even. So by the definition of even integer, $n = 2k$ for some integer k. Replacing n by $2k$ in the last equality we get

  $$2m^2 = (2k)^2$$

  which gives

  $$2m^2 = 4k^2.$$

  By the rule of arithmetic, we can divide both sides by 2 to get

  $$m^2 = 2k^2.$$

  The above equality says that m^2 is an even number by the definition of even number. By the last theorem we proved, we conclude that m is even.

  We have now proved that both n and m are even integers, that is, they have 2 as a common divisor. This contradicts our assumption that n and m have 1 as their only common positive divisor. □

- **Proof by Contradiction of a Universally Quantified Implication** $\forall x(\varphi(x) \implies \psi(x))$**.**

  By the foregoing discussion, we have to show that

  $$\neg[\forall x(\varphi(x) \implies \psi(x))] \implies False$$

  which is logically equivalent to

  $$\exists x[\neg(\varphi(x) \implies \psi(x))] \implies False$$

  which is logically equivalent to

  $$\exists x[\neg(\neg\varphi(x) \vee \psi(x))] \implies False$$

  which is logically equivalent to

  $$\exists x[\neg\neg\varphi(x) \wedge \neg\psi(x)] \implies False$$

  which is logically equivalent to

  $$\exists x[\varphi(x) \wedge \neg\psi(x)] \implies False,$$

  and this is the form that we will use. Let's look at an example.

  Theorem. *For all integer n, if n is even then n^2 is even.*

  Proof. Suppose there exists an even integer n such that its square n^2 is odd. This means, by definition of even and odd integers, that there exist integers k and ℓ such that $n = 2k$ and $n^2 = 2\ell + 1$. We thus have

  $$2\ell + 1 = n^2 = (2k)^2 = 4k^2.$$

  Subtracting 2ℓ from both sides we get

  $$1 = 4k^2 - 2\ell$$

  which further yields

  $$1 = 2(2k^2 - \ell)$$

  which says that 1 is an even integer, a contradiction. □

- **Proof by Cases.** This proof method is based on the fact that any proposition q is logically equivalent to the proposition $(p \implies q) \wedge (\neg p \implies q)$, where p is any proposition. Instead of trying to prove q, we prove $(p \implies q) \wedge (\neg p \implies q)$. We will now give an example of a beautiful proof by cases.

Theorem. *There exist irrational numbers x and y such that x^y is rational.*

Proof. Consider the number $\sqrt{2}^{\sqrt{2}}$. It is either rational or irrational. We consider each case in turn.

Case 1. $\sqrt{2}^{\sqrt{2}}$ is rational. We then let $x = \sqrt{2}$ and let $y = \sqrt{2}$. We then have both x and y irrational but x^y rational.

Case 2. $\sqrt{2}^{\sqrt{2}}$ is irrational. We then let $x = \sqrt{2}^{\sqrt{2}}$ and let $y = \sqrt{2}$. We thus have $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$, a rational number. Again we have both x and y irrational but x^y rational.

This completes the proof. □

Notice that even after the proof we still don't know whether Case 1 above is true or Case 2 is true. The proof helps absolutely nothing in determining the rationality of $\sqrt{2}^{\sqrt{2}}$.

- **Exercises.**

1. Prove *it is not the case that for every natural number n, the number $n^2 + 41n + 41$ is prime.*
2. Prove *it is not the case that there exists a natural number m such that for every natural number n we have $m = n + 1$.*
3. Prove directly that *for any integers m and n, if $m + n$ is odd then m is odd or n is odd.*

   Hint: Use the fact that $p \vee q \equiv \neg p \implies q$.
4. Prove it again by contrapositive.
5. Prove it again by contradiction.
6. Prove by contrapositive that for all integers m, n, if mn is odd then both m and n are odd.

   Hint: Use the fact that $p \vee q \implies r \equiv (p \implies r) \wedge (q \implies r)$.
7. Prove it again by contradiction.
8. Prove (by cases) that the product of any three consecutive integers is divisible by 3.