Mathematical concepts for computer science

So far…

1. Propositional Logic
2. Applications of Propositional Logic
3. Propositional Equivalences
4. Predicates and Quantifiers

Introduction to Proofs

- A **proof** is a valid argument that establishes the truth of a mathematical statement.
- A **theorem** is a statement that can be shown to be true.
- Less important theorems sometimes are called **propositions.**
- The statements used in a proof can include **axioms (or postulates), which are statements we assume to be true,** the **premises**, if any, of the theorem, and **previously proven theorems**.

Introduction to Proofs

- A less important theorem that is helpful in the proof of other results is called a **lemma.**
- A **corollary is a** theorem that can be established directly from a theorem that has been proved.
- A **conjecture is** a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

Direct Proofs

Definition

- The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$.

(Note that every integer is either even or odd, and no integer is both even and odd.)

Two integers have the same parity when both are even or both are odd; they have opposite parity when one is even and the other is odd.

Direct Proofs

Give a direct proof of the theorem **“If n is an odd integer, then n^2 is odd.”**

- **∀n(P (n) → Q(n)),**

where **P(n) is “n is an odd integer”** and **Q(n) is “n^2 is odd.”**

- To begin a direct proof of this theorem, we **assume** that the **hypothesis of this conditional statement is true**, namely, we **assume that n is odd**.

Direct Proofs

- To begin a direct proof of this theorem, we **assume** that the **hypothesis of this conditional statement is true**, namely, we **assume that n is odd**.
- By the definition of an odd integer, it follows that

n = 2k + 1, where k is some integer.

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

$(2k^2 + 2k)$ is an integer so n^2 is odd integer

Direct Proofs

- Give a direct proof that **if m and n are both perfect squares, then nm is also a perfect square**.

(An integer a is a perfect square if there is an integer b such that $a = b^2$.)

Direct Proofs

- Give a direct proof that **if m and n are both perfect squares, then nm is also a perfect square**.

(An integer a is a perfect square if there is an integer b such that $a = b^2$.)

- we assume that the **hypothesis of this conditional statement is true**, namely, we assume that **m and n are both perfect squares**.

Direct Proofs

- we assume that the **hypothesis of this conditional statement is true**, namely, we assume that **m and n are both perfect squares**.
- By the definition of a perfect square, it follows that there are integers s and t such..

$$m = s^2$$
$$n = t^2$$

Direct Proofs

- we assume that the **hypothesis of this conditional statement is true**, namely, we assume that **m and n are both perfect squares**.
- By the definition of a perfect square, it follows that there are integers s and t such..

$$m = s^2 \qquad n = t^2$$

$$mn = s^2 t^2 = (ss)(t\,t) = (st)(st) = (st)^2$$

By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st, which is an integer.

Direct Proofs

- Direct proofs **lead from the premises of a theorem to the conclusion**.
- They **begin with the premises**, **continue with a sequence of deductions**, and **end with the conclusion**.
- However, we will see that **attempts at direct proofs often reach dead ends**. We need other methods of proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$.
- Proofs of theorems of this type that are not direct proofs, that is, **that do not start with the premises and end with the conclusion**, are called **indirect proofs.**

Direct Proofs

- Prove that if n is an integer and **3n + 2 is odd**, **then n is odd** by using direct proofs.

Direct Proofs

- Prove that if n is an integer and **3n + 2 is odd**, **then n is odd** by using direct proofs.
- Direct proof: To construct a direct proof, we first assume that 3n + 2 is an odd integer.
- This means that **3n + 2 = 2k + 1** for some integer k.
- **3n + 1 = 2k**, but there does not seem to be any direct way to conclude that n is odd. Because our attempt at a **direct proof failed**, we next try a proof by contraposition.

Proof by Contraposition

- One of the useful type of indirect proof is known as **proof by contraposition.**
- Proofs by contraposition make use of the fact that the conditional statement **$p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$**.
- This means that the conditional statement **$p \rightarrow q$ can be proved by** showing that its contrapositive,

  $\neg q \rightarrow \neg p$, is true.

Proof by Contraposition

- In a proof by contraposition of $p \rightarrow q$, we take **$\neg q$ as a premise**, and using axioms, definitions, and previously proven theorems, together with rules of inference, **we show that $\neg p$ must follow**.
- Prove that if n is an integer and **3n + 2 is odd**, **then n is odd** by using proof by contraposition.

Proof by Contraposition

- Prove that if n is an integer and **3n + 2 is odd**, **then n is odd** by using proof by contraposition.
- **Step 1:Assume** that the conclusion of the conditional statement "**If 3n + 2 is odd, then n is odd**" is **false**;
- Step 2: By the **definition of an even integer, n = 2k** for some integer k. Substituting 2k for n, we find that

3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1).

3n + 2 is even (because it is a multiple of 2), and therefore not odd.

Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true.

Proof by Contraposition

- Prove that **if n = ab**, where a and b are positive integers, then **$a \le \sqrt{n}$ or $b \le \sqrt{n}$**.

Proof by Contraposition

- Prove that **if $n = ab$**, where a and b are positive integers, then **$a \le \sqrt{n}$ or $b \le \sqrt{n}$**.
- Step 1: Assume that the conclusion of the conditional statement "If $n = ab$, where a and b are positive integers, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$" **is false**.

Proof by Contraposition

- Prove that **if $n = ab$**, where a and b are positive integers, then **$a \leq \sqrt{n}$ or $b \leq \sqrt{n}$**.
- Step 1: Assume that the conclusion of the conditional statement "If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$" **is false**.
- That is, we assume that the statement **$(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$** is **false**.

Proof by Contraposition

- Prove that **if $n = ab$**, where a and b are positive integers, then **$a \leq \sqrt{n}$ or $b \leq \sqrt{n}$**.
- **$(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$ $=F$**
- **$a > \sqrt{n}$ and $b > \sqrt{n}$**
- **$ab > \sqrt{n} \times \sqrt{n} = n$**
- **$ab > n$**
- **$ab \neq n$**, which contradicts the statement,

$$n = ab.$$

Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded;

VACUOUS AND TRIVIAL PROOFS

- We can quickly prove that a conditional statement **p → q is true** when we know that **p is false**, because **p → q must be true** when p is false.
- Consequently, **if we can show that p is false**, then we have a proof, **called a vacuous proof**, **of the conditional statement p → q**.
- Vacuous proofs are often used to establish **special cases of theorems** that state that a conditional statement is **true for all positive integers.**

VACUOUS AND TRIVIAL PROOFS

- Show that the proposition P(0) is true, where P(n) is "**If n > 1, then** n^2 **> n**" and the domain consists of all integers.

VACUOUS AND TRIVIAL PROOFS

- We can also quickly prove a conditional statement $p \rightarrow q$ if we know that the conclusion q is true. By showing that q is true, it follows that $p \rightarrow q$ must also be true.
- A proof of $p \rightarrow q$ that uses the fact that q is true is called a **trivial proof.**

VACUOUS AND TRIVIAL PROOFS

- Let P(n) be "If a and b are positive integers with a ≥ b, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that P(0) is true.

VACUOUS AND TRIVIAL PROOFS

- Let P(n) be "If a and b are positive integers with a ≥ b, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that P(0) is true.
- The proposition P(0) is "If a ≥ b, then $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the conditional statement "If a ≥ b, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is P(0), is true.
- **The statement "a ≥ b," was not needed in this proof.**

A LITTLE PROOF STRATEGY

- First evaluate whether a direct proof looks promising.
- If a direct proof does not seem to go anywhere, try the same thing with a proof by contraposition.

PROOF STRATEGY

- Prove that the sum of two rational numbers is rational.
- **Definition**

The real number r is rational if there exist integers p and q with p and q $\neq$ 0 such that r = p/q. A real number that is not rational is called irrational.

Direct proof

- Prove that the sum of two rational numbers is rational.

To begin, suppose that **r** and **s** are rational numbers.

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu}.$$

Because q ≠ 0 and u ≠ 0, it follows that qu ≠ 0.

PROOF STRATEGY

- Prove that if n is an integer and n^2 is odd, then n is odd.

Direct Proof

$$n^2 = 2k + 1$$

$$n = \pm\sqrt{2k + 1}$$

which is not terribly useful

PROOF STRATEGY

- Prove that if n is an integer and n^2 is odd, then n is odd.

proof by contraposition

We take as our hypothesis the statement that n is not odd. Because every integer is odd or even, this means that n is even. This implies that there exists an integer k such that n = 2k . To prove the theorem, we need to show that this hypothesis implies the conclusion that n2 is not odd, that is, that sqr(n) is even.

$$n^2 = 4k^2 = 2(2k^2)$$

Proved

Proofs by Contradiction

- Suppose we want to prove that a **statement p is true**.
- Furthermore, suppose that we can **find a contradiction q** such that **¬p → q** is **true**. **Because q is false, but ¬p → q is true**, we can conclude that ¬p is false, which means that p is true.

Proofs by Contradiction

- Because the statement **$r \wedge \neg r$ is a contradiction** whenever **r is a proposition**, we can prove that **p is true if** we can show that **$\neg p \rightarrow (r \wedge \neg r)$** is true for some proposition r.
- Show that at least four of any 22 days must fall on the same day of the week.

Proofs by Contradiction

P: “At least four of 22 chosen days fall on the same day of the week.”

¬p: “At most three of the 22 days fall on the same day of the week.”

Assume ¬p is true

- Because there are seven days of the week, this implies that at most 21 days could have been chosen, as for each of the days of the week, at most three of the chosen days could fall on that day.
- This **contradicts** the premise that we have 22 days under consideration.

Proofs by Contradiction

P: "At least four of 22 chosen days fall on the same day of the week."

¬p: "At most three of the 22 days fall on the same day of the week."

Assume ¬p is true

if **r** is the statement that **22 days are chosen**, then we have shown that $\neg p \rightarrow (r \wedge \neg r)$. Consequently, we know that p is true.

Proofs by Contradiction

- Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

P :"$\sqrt{2}$ is irrational."

$\neg p$:"It is not the case that $\sqrt{2}$ is irrational"

$\neg p$: "$\sqrt{2}$ is rational"

Assume $\neg p$ is true

Proofs by Contradiction

$\neg p$: "$\sqrt{2}$ is rational"

Assume $\neg p$ is true

- If $\sqrt{2}$ is rational, there exist integers a and b with

$\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors *(so that the fraction a/b is in lowest terms.)*

(Here, we are using the fact that every rational number can be written in lowest terms.)

Proofs by Contradiction

¬p: "√ 2 is rational"

Assume ¬p is true

Because √2 = *a/b, when both* sides of this equation are squared, it follows that

$$2 = \frac{a^2}{b^2}.$$

Hence,

$$2b^2 = a^2.$$

Proofs by Contradiction

¬p: "√ 2 is rational"

Assume ¬p is true

By the definition of an even integer it follows that a^2 *is even.*

If a^2 is even, *a* must also be even

By the definition of an even integer, *a = 2c* for some integer *c*.

$$2b^2 = 4c^2$$

Proofs by Contradiction

¬p: "√ 2 is rational"

Assume ¬p is true

$$2b^2 = 4c^2$$

Dividing both sides of this equation by 2 gives

$$b^2 = 2c^2$$

b^2 **is even and we conclude that b must be even as well.**

Proofs by Contradiction

$\neg p$: "√ 2 is rational"

Assume **$\neg p$ is true**

r: **√2 = a/b, where a and b have no common factors**

$\neg r$: **√2 = a/b, where a and b have a common factor 2.**

$\neg p \rightarrow (r \wedge \neg r)$: **T → T is true**

We have now shown that the assumption of $\neg p$ leads to the equation **√2 = a/b, where a and b have no common factors**, but **both a and b are even, that is, 2 divides both a and b**.

Proofs by Contradiction

- Proof by contradiction can be used to prove conditional statements.
- In such proofs, we **first assume** the **negation of the conclusion**.
- We then use the premises of the theorem and the negation of the conclusion to arrive at a contradiction.

Proofs by Contradiction

- Give a proof by contradiction of the theorem "If 3n + 2 is odd, then n is odd."

  $p \rightarrow q$

p: 3n + 2 is odd

q: n is odd

Assume that **p**, **$\neg$q is true**

That is, assume that **3n + 2 is odd** and that **n is not odd means n is even**.

Proofs by Contradiction

- Because n is even, there is an integer k such that $n = 2k$.
- $\mathbf{3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1).}$
- $\mathbf{3n + 2 = 2t}$, where $\mathbf{t = 3k + 1}$, **3n + 2 is even= ¬p**.
- Because **both p and ¬p are true**, we have a contradiction.

Taxonomy of Proof: if and only if

- ***A* IF AND ONLY IF *B***
- we physically **break an IF AND ONLY IF proof into two proofs**, the ``forwards'' and ``backwards'' proofs.
- To prove a theorem of the form ***A* IF AND ONLY IF *B***, you first prove IF *A* THEN *B*, then you prove IF *B* THEN *A*, and that's enough to complete the proof.

Taxonomy of Proof: if and only if

- Let x be a number. Let $\lfloor x \rfloor$ be the greatest integer less than x, and $\lceil x \rceil$ be the smallest integer greater than x. Prove that $\lfloor x \rfloor = \lceil x \rceil$ if and only if x is an integer.
- **Proof:**

  forwards : IF *A* THEN *B*

Taxonomy of Proof: if and only if

- Let x be a number. Let $\lfloor x \rfloor$ be the greatest integer less than x, and $\lceil x \rceil$ be the smallest integer greater than x. Prove that $\lfloor x \rfloor = \lceil x \rceil$ if and only if x is an integer.
- **Proof:**
  forwards : IF *A* THEN *B*
- Assume $\lfloor x \rfloor = \lceil x \rceil$ if upper bound and lower bound are equal it will be an integer. Hence proved

Taxonomy of Proof: if and only if

- Let x be a number. Let $\lfloor x \rfloor$ be the greatest integer less than x, and $\lceil x \rceil$ be the smallest integer greater than x. Prove that $\lfloor x \rfloor = \lceil x \rceil$ if and only if x is an integer.
- **Proof:**
  backwards : IF *B* THEN *A*
- Assume x is an integer

$$\lfloor x \rfloor = x \qquad \lceil x \rceil = x \qquad \lfloor x \rfloor = \lceil x \rceil$$

Hence proved

What is wrong with this “proof?”

What is wrong with this famous supposed “proof” that 1 = 2?

Step	**Reason**
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

What is wrong with this “proof?”

“Theorem:” If *n2 is positive, then n is positive.*

“Proof:"

Suppose that n^2 is positive. Because the conditional statement “If n is positive, then n^2 is positive” is true, we can conclude that n is positive.

What is wrong with this “proof?”

“Theorem:” If n^2 *is positive, then n is positive.*

“Proof:"

Suppose that n^2 is positive. Because the conditional statement “**If n is positive, then** n^2 **is positive**” is true, we can conclude that n is positive.

What is wrong with this "proof?"

- It supposedly shows that *n is an even integer whenever* n^2 *is* an even integer.

Suppose that n^2 *is even. Then* $n^2 = 2k$ *for some integer k. Let n = 2l for some integer l.* This shows that *n is even.*

What is wrong with this “proof?”

- It supposedly shows that *n is an even integer whenever* n^2 *is* an even integer.

Suppose that n^2 *is even. Then* $n^2 = 2k$ *for some integer k. Let n = 2l for some integer l.* This shows that *n is even.*

Reference

- **Rosen, Kenneth H., and Kamala Krithivasan. Discrete mathematics and its applications: with combinatorics and graph theory. Tata McGraw-Hill Education, 2016.**