Mathematical Reasoning and Proofs

As a computer scientist or computer engineer, one must have a high degree of certainty that the designs, algorithms, and programs that one uses will work properly. Mathematical proof is what converts today's intellectual gossip and speculation into tomorrow's textbook subject. For computer scientists and engineers, proofs have importance for many reasons, including

- **algorithm/circuit correctness:** proving that an algorithm or piece of hardware does what one claims or expects;
- **algorithm complexity:** assuming that an algorithm is correct, one must then prove that it runs in a manner that is both efficient in time and space;
- **applications:** when applying an algorithm or tool to a specific problem, one must prove that the algorithm or tool is appropriate for that problem. This may involve some analysis, and hence proof.

Differences Between Mathematical Reasoning and Propositional Logical Reasoning

Mathematical reasoning represents an extension of logical reasoning, in that the inference rules from propositional logic are still valid and used in a mathematical proof, but mathematical proofs require the following additional knowledge.

Definitions Mathematical statements that require proof usually involve the use of terms that must be understood and precisely defined.

Axioms Axioms are mathematical statements that one assumes to be true. For example, given any three numbers x, y, and z, we assume that $x + y = y + x$ (commutative), and that $x + (y + z) = (x + y) + z$ (associative), and $x(y + z) = xy + xz$ (distributive).

Background Knowledge By “background knowledge” we mean mathematical statements that we assume are true, not because they are axioms, but because they have already been proved as true.

Semi-Formal Where as logical derivation trees are constructed in a very systematic way, mathematical proofs involve a combination of formal algebraic steps and natural language. The degree of informality/formality can range anywhere from 0 to 100 percent, depending on the statement being proved. Some statements can be sucessfully proved without using any formal algebra, while others may require a presentation that mostly consists of algebraic statements.

Definitions

The following are some mathematical definitions that will be used in this and subsequent lectures.

Even/Odd An integer n is **even** iff it can be written as $n = 2k$, for some integer k. Similarly, n is **odd** iff it can be written as $n = 2k + 1$, for some integer k. Alternatively, n is even iff $n \bmod 2 = 0$ and n is odd iff $n \bmod 2 = 1$.

Prime/Composite An integer $n \geq 2$ is **prime** iff 1 and n are the only positive integers that divide evenly into n. Otherwise, n is said to be **composite**.

Prime Factor Prime number p is a **prime factor** of $n \geq 1$ iff p^e divides evenly into n, for some integer $e \geq 1$.

Rational A **rational** number is one that can be written as a fraction p/q, where p and $q \neq 0$ are integers.

Irrational An **irrational** number is one that *cannot* be written as a fraction.

Axioms

The following are some mathematical axioms that will be used in this and subsequent lectures. In what follows we assume x, y, and z are real numbers.

Identity $x + 0 = x$ and $x \cdot 1 = x$

Associative $x + (y + z) = (x + y) + z$ and $x(yz) = (xy)z$

Inverse x has an additive inverse $-x$ for which $x + (-x) = 0$, and, if $x \neq 0$, x has a multiplicative inverse $1/x$ for which $x \cdot (1/x) = 1$

Commutative $x + y = y + x$ and $xy = yx$

Distributive $x(y + z) = xy + xz$

Total Order At most one is true: $x < y$ or $x > y$ or $x = y$

Linear Order If $x < y$ and $z \neq x$ and $z \neq y$, then either $z < x$ or $x < z < y$, or $y < z$

Equations $x = y \Rightarrow x + z = y + z$ and $x = y \Rightarrow xz = yz$

Inequalities If $z > 0$, $x < y \Rightarrow xz < yz$ and if $z < 0$, $x < y \Rightarrow xz > yz$

Background Knowledge

The following are some basic mathematical results that will be used in this and subsequent lectures. In what follows we assume x, y, and z are real numbers.

Unique Prime Factorizations For every integer $n \geq 2$, there is a unique set of unique prime numbers $p_1, \ldots, p_k$, and positive-integer exponents $e_1, \ldots, e_k$ for which

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}.$$

Prime Dividing Product If prime number p divides evenly into ab, then either p divides a or p divides b.

Unique Quotient and Divisor Given integers a and b, $b \neq 0$, there are unique integers q, called the **quotient**, and r, called the **remainder**, for which

$$a = bq + r$$

where $0 \leq r < b$.

Mathematical Proof Strategies

Name of Strategy	**Goal**	**Strategy**
Direct proof	prove $p \to q$	assume p, show q
Indirect proof	prove $p \to q$	assume $\neg q$, show $\neg p$
Proof by contradiction	prove $p \to q$	assume $\neg q, p$, show a contradiction
Proof by cases	prove $p_1 \vee \cdots \vee p_n \to q$	$\forall i \in \{1, \ldots, n\}$ prove $p_i \to q$
Counterexample	prove $\forall n(p(n) \to q(n))$	provide a value for n for which $p(n)$ evaluates to `true` but $q(n)$ evaluates to `false`

Example 1. Give both a direct and indirect proof that the square of an odd number is odd.

Example 2. A **rational number** is any number that can be represented as a fraction p/q, where p and $q \neq 0$ are integers. Otherwise the number is called **irrational**. Use a proof by contradiction to show that the sum of an irrational number and a rational number equals a number that is irrational.

Example 3. Use a proof by contradiction to prove that $\sqrt{2}$ is irrational.

Example 4. Use a proof by cases to prove that, for any two real numbers x and y, $\min(x, y) + \max(x, y) = x + y$.

Example 5. Provide a counterexample that $2^n - 1$ is a prime number whenever $n > 4$.

Set Containment Proofs

At times it becomes necessary to prove that two sets A and B are equal. In the Sets lecture we showed that one way of accomplishing this to create a membership table. But this only works if A and B are related via a set identity. A more general method is to use a **set containment proof**. This requires the following two symmetric steps.

1. Prove that $A \subseteq B$. Do this by showing that, for arbitrary member $x \in A$, x is also a member of B.
2. Prove that $B \subseteq A$. Do this by showing that, for arbitrary member $x \in B$, x is also a member of A.

Example 6. Use a set containment proof to prove that the greatest common divisor of two positive integers a and b is equal to the greatest common divisor of b and r, where r is the remainder when dividing a by b.

The following are some common pitfalls that arise when writing a proof.

1. Generalizing from examples, such as asserting $\forall n p(n)$ is true when having shown $p(n)$ is true for only a proper subset of $\text{dom}(n)$
2. Not showing all the steps
3. Assuming what is to be proved
4. Assuming facts that are not true

Exercises

1. Give a direct proof that the square of an even number is even. Provide the statement(s) that may be assumed. Provide the statement that must be proved.

2. Give a direct proof that product of two odd numbers is odd. Provide the statement(s) that may be assumed. Provide the statement that must be proved.

3. Prove that if n is an even number then $7n+4$ is even. Also, prove or disprove that the converse is also true.

4. Give an indirect proof that the square of an even number is even. Provide the statement(s) that may be assumed. Provide the statement that must be proved.

5. Give an indirect proof of the statement n is odd provided $5n+6$ is odd. Provide the statement(s) that may be assumed. Provide the statement that must be proved.

6. Give an indirect proof that at least 10 days of any 64 calendar days must fall on the same day of the week. Write the statement as a conditional statement of the form $p \to q$, and identify both p and q. Then Provide the statement(s) that may be assumed. Provide the statement that must be proved.

7. Prove that $\min(a, \min(b, c)) = \min(\min(a, b), c)$ using a proof by cases. Provide each of the case statements, and prove the result for each case.

8. Using proof by cases, show that, for all real numbers x and y
$$|x + y| \leq |x| + |y|.$$
List all of the cases that are needed in order to ensure that the absolute value from each term can be removed. Hint: there are more than four cases. Prove the statement for each case.

9. Show how to use case reasoning to determine the solutions to the equation $|5x+1| = 7$. Clearly state the cases that are being considered.

10. Use a proof by contradiction to prove that $\sqrt{3}$ is irrational. Provide the assumption that this proof strategy allows for.

11. Use a proof by contradiction to prove that if x is irrational, then $1/x$ is irrational.

12. Use a proof by contradiction to prove that if n is an integer and $n^3 + 5$ is odd, then n is even. Provide all the statements that may be assumed.

13. Find a counterexample to the statement that every positive integer can be written as the sum of the squares of three integers.

14. Prove that at least one real number from $a_1, \ldots, a_n$ must be greater than or equal to the average of the numbers $a_1, \ldots, a_n$.

15. Prove or disprove that if a and b are rational numbers, then a^b is also rational.

16. Prove or disprove that there is no positive integer n such that $n^2 + n^3 = 100$.

17. Provide (unique) prime factorizations for the numbers 300, 65, 113, and 315.

18. If a and b are positive integers having respective prime factorizations $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, then provide a prime factorization for $\gcd(a, b)$.

19. Use a set containment proof and proof by cases to show that $(B - A) \cup (C - A) = (B \cup C) - A$.

20. Let $f : A \to B$ be a function from set A to set B; and let S and T be subsets of B. Use a set containment proof to prove that i) $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$, and ii) $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$.

21. Prove or disprove each of the statements about the floor and ceiling functions. Assume x and y are both real numbers.

    - **a.** $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$.
    - **b.** $\lfloor 2x \rfloor = 2\lfloor x \rfloor$.
    - **c.** $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil = 0$ or 1.
    - **d.** $\lceil xy \rceil = \lceil x \rceil \lceil y \rceil$.

22. If $(g \circ f)$ is one-to-one, prove that f must be one-to-one. Hint: use a proof by contradiction.

23. If $(g \circ f)$ is onto, prove that g must be onto.

24. Prove or disprove the following statements about arbitrary sets A, B, and C.

    (a) If $A \cup C = B \cup C$, then $A = B$.

    (b) If $A \cap C = B \cap C$, then $A = B$.

    (c) If $A \cup C = B \cup C$ and $A \cap C = B \cap C$, then $A = B$.

Exercise Solutions

1. **Assume**: Integer n is even. **Prove**: n^2 is even. **Proof.** Since n is even, we may write $n = 2k$, where k is an integer. Then

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

   which is even. □

2. **Assume**: Integers m and n are odd. **Prove**: mn is odd. **Proof.** Since m and n are odd, we may write $m = 2k_1 + 1$ and $n = 2k_2 + 1$, where k_1 and k_2 are integers. Then

   $$mn = (2k_1 + 1)(2k_2 + 1) = 4k_1k_2 + 2k_1 + 2_k2 + 1 = 2(2k_1k_2 + k_1 + k_2) + 1,$$

   which is odd. □

3. Since n is even, we may write $n = 2k$, where k is an integer. Then

   $$7n + 4 = 7(2k) + 4 = 2(7k + 2),$$

   which is even.

   Conversely, suppose $7n + 4$ is even. Then $7n + 4 = 2k$ for some integer k. Then $7n = 2k - 4 = 2(k - 4)$, which means that $7n$ is even. Therefore, by Exercise 2, n must be even, since the product of two odd numbers must be odd.

4. **Assume**: Integer n^2 is odd. **Prove**: n is odd. **Proof.** Since n^2 is odd, we may write $n^2 = 2k+1$, where k is an integer. Then

   $$n^2 - 1 = (n - 1)(n + 1) = 2k$$

   is even. Moreover both $n - 1$ and $n + 1$ are either both even or both odd, since they differ by 2. Finally, both must be even by Exercise 2, since the product of two odd numbers is odd. Therefore, n must be odd. □

5. **Assume**: Integer n is even. **Prove**: $5n + 6$ is even. **Proof.** Since n is even, we have $n = 2k$ for some integer k. But then we have that

   $$5n + 6 = 5(2k) + 6 = 10k + 6 = 2(5k + 3)$$

   is even. □

6. P: there are 64 distinct calendar days. Q: at least 10 of those days fall on the same day of the week. **Assume**: $\neg Q$: any day of the week has at most 9 of the 64 calendar days. **Prove**: $\neg P$: it's not the case that there are 64 distinct calendar days. **Proof.** If each day of the week has at most 9 of the calendar days, then there would be at most $9 \times 7 = 63 < 64$ calendar days. Therefore, it's not the case that there are 64 calendar days. □

7. **Case 1:** $a \leq b \leq c$. Then

   $$\min(a, \min(b, c)) = \min(a, b) = a,$$

   and

   $$\min(\min(a, b), c) = \min(a, c) = a.$$

Case 2: $a \leq c \leq b$. Then

$$\min(a, \min(b, c)) = \min(a, c) = a,$$

and

$$\min(\min(a, b), c) = \min(a, c) = a.$$

The remaining four cases (what are they?) are proved similarly. □

8. **Case 1:** $x, y \geq 0$. Then

$$|x + y| = x + y = |x| + |y|.$$

Case 2: $x, y \leq 0$. Then

$$|x + y| = -(x + y) = -x + -y = |x| + |y|.$$

Case 3: $x \geq 0$, $y \leq 0$, and $x \geq |y|$. Then

$$|x + y| = x + y = |x| + y \leq |x| + |y|.$$

Case 4: $x \geq 0$, $y \leq 0$, and $x < |y|$. Then

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

The remaining two cases (what are they?) are, by symmetry, identical to the last two cases. □

9. **Case 1:** $5x + 1 = 7$, Then $x = 6/5$.

Case 2: $5x + 1 = -7$, Then $x = -8/5$.

10. Let P denote the statement "$\sqrt{3}$ is irrational". **Assume:** $\neg P$: $\sqrt{3}$ is rational. Show a contradiction.

Proof. Since $\sqrt{3}$ is rational, we have $\sqrt{3} = p/q$ where p and q are integers, $q \neq 0$, and $\gcd(p, q) = 1$. Then we have

$$3q^2 = p^2 \Rightarrow 3|p^2 \Rightarrow 3|p \Rightarrow p = 3k,$$

for some integer k. Then we have

$$3q^2 = (3k)^2 = 9k^2 \Rightarrow q^2 = 3k^2.$$

But this implies that $3|q$ and so $\gcd(p, q) \geq 3$, a contradiction. □

11. Let P denote the statement "x is irrational", while Q denotes the statement "$1/x$ is irrational". Then we must prove $P \to Q$.

Assume: P: x is irrational, and $\neg Q$: $1/x$ is rational. Show a contradiction. □

Proof. Since x is irrational we know that $x \neq 0$. Also, if $1/x$ is rational, then we have $1/x = p/q$, with $p \neq 0$ and $q \neq 0$ both integers. Thus, $x = q/p$ is rational, a contradiction. □

12. Let P denote the statement "n^3+5 is an odd integer", while Q denotes the statement "n is an even integer". Then we must prove $P \to Q$.

    Assume: P: n^3+5 is an odd integer, and $\neg Q$: n is an odd integer. Show a contradiction. □

    Proof. Since n is odd, $n = 2k+1$, for some integer k. Thus,

    $$n^3+5 = (2k+1)^3 = (8k^3+3(4k^2)+3(4k)+1)+5 = 8k^3+3(4k^2)+3(4k)+6 = 2(4k^3+6k^2+6k+3)$$

    is even, a contradiction. □

13. The number 7 serves as a counterexample.

14. Proof by contradiction. **Assume:** $\mu = (a_1+a_2+\cdots+a_n)/n$ and $a_i < \mu$ for every $i = 1, \ldots, n$.

    Proof. Since $a_i < \mu$ for every $i = 1, \ldots, n$, it follows that

    $$a_1+a_2+\cdots+a_n < (\mu+\mu+\cdots+\mu) = n\mu,$$

    which implies

    $$(a_1+a_2+\cdots+a_n)/n < \mu,$$

    a contradiction. □

15. The statement is false for rational numbers $a = 2$ and $b = 1/2$ is since $\sqrt{2} = 2^{\frac{1}{2}}$. □

16. The statement is false, since the only numbers not exceeding 100 of the form n^2+n^3, where n is a positive integer, are 2, 12, 36, and 80.

17. $300 = 2^2 \cdot 3 \cdot 5^2$, $65 = 5 \cdot 13$, $113 = 113^1$, and $315 = 3^2 \cdot 5 \cdot 7$.

18. If a and b are positive integers having respective prime factorizations $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, then

    $$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}.$$

19. **Part 1:** Show $(B-A) \cup (C-A) \subseteq (B \cup C) - A$. Assume $x \in (B-A) \cup (C-A)$. **Case 1:** $x \in (B-A)$. Then $x \in B$ and $x \notin A$. Then $x \in B \cup C$. Therefore, $x \in (B \cup C) - A$. **Case 2:** $x \in (C-A)$. The proof is similar to Case 1.

    Part 2: Show $(B \cup C) - A \subseteq (B-A) \cup (C-A)$. Assume $x \in ((B \cup C) - A)$. Then $x \in B \cup C$ and $x \notin A$. **Case 1:** $x \in B$. Then $x \in B - A$ which implies $x \in (B-A) \cup (C-A)$. **Case 2:** $x \in C$. The proof is similar to Case 1.

20.

21. We have

    - **a.** $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$ is true since $\lfloor x \rfloor$ is an integer, and $\lceil n \rceil = n$ for any integer n.
    - **b.** $\lfloor 2x \rfloor = 2\lfloor x \rfloor$ is not always true since, for $x = 0.6$,

      $$\lfloor 1.2 \rfloor = 1 \neq 2\lfloor 0.6 \rfloor = 2 \cdot 0 = 0.$$

    - **c.** $\lceil x \rceil + \lceil y \rceil - \lceil x+y \rceil = 0$ or 1 is true and can be proved by cases on the distances between the ceiling values compared with the original values.

- **d.** $\lceil xy \rceil = \lceil x \rceil \lceil y \rceil$ is not always true since, for $x = y = -0.1$,

$$\lceil (-0.1)(-0.1) \rceil = 1 \neq (\lceil -0.1 \rceil)^2 = 0^2 = 0.$$

22. Given functions $f : A \to B$ and $g : B \to C$ suppose $(g \circ f) : A \to C$ is one-to-one, and f is not one-to-one. Then there are $a_1, a_2 \in A$ and $b \in B$ such that $f(a_1) = f(a_2) = b$. Furthermore, suppose $g(b) = c \in C$. But then

$$(g \circ f)(a_1) = g(f(a_1)) = g(b) = c = g(b) = g(f(a_2)) = (g \circ f)(a_2),$$

and so $g \circ f$ maps both a_1 and a_2 to c, contradicting the fact that $g \circ f$ is one-to-one.

23. Given functions $f : A \to B$ and $g : B \to C$ suppose $(g \circ f) : A \to C$ is onto. Then we have the image of A under $g \circ f$ equal to

$$(g \circ f)(A) = g(f(A)) = C,$$

which means that every $c \in C$ is in the range of g. In other words, g is onto.

24. Prove or disprove the following statements about arbitrary sets A, B, and C.

(a) If $A \cup C = B \cup C$, then $A = B$. Sometimes false: Let $A = \emptyset$, $B = \{1\}$, $C = \{1\}$. Then $A \cup C = B \cup C$, but $A \neq B$

(b) If $A \cap C = B \cap C$, then $A = B$. Sometimes false: Let $A = \{1, 2\}$, $B = \{1, 3\}$, $C = \{1\}$. Then $A \cap C = B \cap C$, but $A \neq B$.

(c) Always true. Proof: suppose $x \in A$ is true. If $x \notin B$, then, since we're assuming $A \cup C = B \cup C$, it must be true that $x \in C$ since, otherwise, x would not be a member of $B \cup C$, even though it is a member of $A \cup C$. But if $x \in C$, then $x \in A \cap C$. But this contradicts $A \cap C = B \cap C$, since $x \in B \cap C$ contradicts $x \notin B$. Therefore, we must have $x \in B$, and so $A \subseteq B$. Similarly, we may prove that $B \subseteq A$, and so $A = B$.