CS 2050: Discrete Mathematics for Computer Science

Jaeheon Shim

1 Proofs

1.1 Axioms

An argument in a proof is either an axiom or rests on an axiom. An axiom is an unproven statement, and different theorems can becom true or false depending on your choice of axioms.

The following axioms/assumptions are allowed

- The rules of algebra
  e.g. if x, y, z are real numbers and $x = y$, then $x + z = y + z$
- The set of integers is closed under addition, multiplication, and subtraction
- Every integer is either even or odd
- If x is an integer, there is no integer between x and x + 1
- The relative order of any two real numbers
  e.g. $\frac{1}{2} < 1$ or $4.2 \geq 3.7$
- The square of any number is greater than or equal to 0

1.2 Existential Instantiation

A law of logic that says if an object is known to exist, that object can be given a name as long as the name is not currently being used to denote something else.

Example
If n is an odd integer, $n = 2k + 1$ for some integer k.

1.3 Direct Proofs

In a direct proof of a conditional statement $p \rightarrow c$, the hypothesis p is assumed to be true and the conclusion c is proven as a direct result of the assumption.

If n is an odd integer, then n^2 is an odd integer.

Many theorems also have a universal quantifier such as

For every integer n, if n is odd then n^2 is odd.

1.3.1 Example

Theorem The square of every odd integer is also odd

Proof. Let n be an odd integer.
Since n is odd, $n = 2k + 1$ for some integer k.
Plug $n = 2 + 1$ into n^2 to get:

$$\begin{aligned} n^2 &= (2k+1)^2 && (1) \\ &= 4k^2 + 4k + 1 && (2) \\ &= 2(2^2 + 2k) + 1 && (3) \end{aligned}$$

Since k is an integer, $2^2 + 2$ is also an integer.
Since $n^2 = 2m + 1$, where $m = 2k^2 + 2$ is an integer, n^2 is odd. □

Two-Column Proof Format

n is odd	Assume p.	
$n = 2k + 1$, for some $k \in \mathbf{Z}$	Definition of Odd	
$n^2 = (2k+1)^2$	Square both sides	
$n^2 = 4k^2 + 4k + 1$	expand $(2k+1)^2$	
$n^2 = 2(2k^2 + 2k) + 1$	factor out 2	$\therefore$
$w = 2k^2 + 2m$	define new variable	
w is an integer	integers are closed under addition, multiplication, exponentiation	
$n^2 + 2w + 1$, w is integer	substitute w	
n^2 is odd	definition of odd	

Therefore, by direct proof, I have shown $p \rightarrow q$

1.3.2 Example

Prove that, if x and y are squares, then xy is a square

p: x and y are squares
q: xy is a square
prove $p \rightarrow q$

x and y are square integers	assume p
$x = k^2, k \in \mathbf{Z}$	definition of square
$y = j^2, j \in \mathbf{Z}$	definition of square
$xy = k^2n^2$	multiply two equations
$xy = g^2, g \in \mathbf{Z}$	

Therefore, by direct proof, I have shown $p \rightarrow q$

1.4 Proof by Contrapositive

To prove $p \rightarrow q$, we instead prove $\neg q \rightarrow \neg p$

1.4.1 Example

Prove that, for positive integers n, a, b, if $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

$$\begin{aligned}
\neg[(a \leq \sqrt{n})\text{or}(b \leq \sqrt{n})] &\to \neg(n = ab) && \\
a > \sqrt{n} \text{ and } b > \sqrt{n} & && \text{assume } \neg q \\
a \cdot b > \sqrt{n}\sqrt{n} & && \text{multiply inequalities} \\
ab > n & && \text{algebra} \\
ab \neq n & && \text{definition of ¿}
\end{aligned}$$

Therefore, we have proven the contrapositive, so the original statement is true.

1.5 Proof by Contradiction

To prove **R**

1. Assume you are wrong (**R** is false)
2. Show that eventually, **R** being false leads to some absurdity (e.g. that $1 = 2$, or that p and not p are both simultaneously, etc.)

1.6 Example

Prove $\sqrt{2}$ is irrational.

Proof by Contradiction

$$\begin{aligned}
\sqrt{2} \text{ is rational} & && \text{assume negation of original statement} \\
\sqrt{2} = \frac{a}{b}, a \in \mathbf{Z}, b \in \mathbf{Z}, b \neq 0 & && \text{definition of rational} \\
 & && \text{Let } \frac{a}{b} \text{ be the most simplified fraction for } \sqrt{2} \\
2 = \left(\frac{a}{b}\right)^2 & && \text{square both sides} \\
2 = \frac{a^2}{b^2} & && \\
2b^2 = a^2 & && \text{multiply both sides by } b^2 \\
a^2 \text{ is even} & && \text{by the definition of even} \\
a \text{ is even} & && \text{proven previously} \\
a = 2k, k \in \mathbf{Z} & && \text{definition of even} \\
a^2 = 4k^2 & && \text{square both sides} \\
2b^2 = 4k^2 & && \text{substitute} \\
b^2 = 2k^2 & && \text{divide both sides by 2} \\
k^2 \text{ is an integer} & && \text{closure of } \mathbf{Z} \\
b^2 \text{ is even} & && \text{definition of even} \\
b \text{ is even} & && \text{proven previously}
\end{aligned}$$

If a and b are not both even, then $\frac{a}{b}$ is not the most simplified form, therefore we have a contradiction. So our original assumption, that $\sqrt{2}$ is rational, is wrong. It must be the case that $\sqrt{2}$ is irrational.

1.7 Proof by Cases

Split the domain into cases and prove each case. The cases must cover the entire domain.

2 Sets

A set is an unordered collection of distinct objects. Below is an excerpt from my MATH 3012 notes regarding sets.

2.1 Set Basics

A set is a collection of objects. Below are two examples of sets:

$$A = \{1, 2, 3\}$$
$$B = \{A, -2.7, ARTICHOKE\}$$

- The order of elements does not matter
- Repeated elements are not allowed

The $\emptyset$ symbol denotes the empty set. The empty set is the set containing no elements.

Below are some symbols related to sets.

- $\mathbf{b} \in \mathbf{A}$ - element b is a member of set A

$$1 \in \{1, 2, 3\}$$
$$7 \notin \{1, 2, 3\}$$
$$\emptyset \in \{1, 2, 3\}$$

- $\mathbf{A} \subseteq \mathbf{B}$ - A is a subset of B (Every element of A is also in B)
- $\mathbf{A} \nsubseteq \mathbf{B}$ - A is not a subset of B (There exists an element of A that is not in B
- $\exists$ - "there exists"

$$\exists x \in \{7, 8\} \text{ such that } x > 5$$

- $\forall$ - "for all"

$$\forall x \in \{7, 8, 9\}, x \geq 4$$

- $\mathbf{B = \{x \in A \mid x > 4\}}$ - An example of set builder notation. "The set containing every element in A that is greater than 4"

- $\cup$ - Set Union: Elements in either set or both

$$\{1,2,3,4\} \cup \{3,4,5,6\} = \{1,2,3,4,5,6\}$$

- $\cap$ - Set Intersection: Elements in both sets

$$\{1,2,3,4\} \cap \{3,4,5,6\} = \{3,4\}$$

- $|\mathbf{A}|$ - Cardinality: The size of a set

$$A = \{1,2,3,4\} \qquad |A| = 4$$

2.2 The Cartesian Product

The cartesian product is an operation that can be applied to two sets.

Example
Let $A = \{1,2\}, \quad B = \{3,4\}$

$$\begin{aligned} A \times B &= \{(x,y) \mid x \in A, y \in B\} \\ &= \{(1,3),(1,4),(2,3),(2,4)\} \end{aligned}$$

More formally,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \forall i \in 1,2,\ldots,n\}$$

Notice the elements of the set produced by the cartesian product are contained in parentheses '()' instead of curly brackets '{}'. This denotes that they are a tuple. In a tiple, **order matters** and **repeates are allowed**

2.3 Set Proofs

2.3.1 Proving $x \in A \to x \in B$

Can be proven by conventional methods (direct proof, contrapositive, etc.)

2.3.2 Proving $A \subset B$

1. Prove $A \subseteq B$
2. Prove $A \neq B$

Disproving
Either show $A \nsubseteq B$ or $A = B$. There is an element in A that is not in B, or vice versa.

2.3.3 Proving $A = B$

You need to prove that $A \subseteq B$ AND $B \subseteq A$

1. Prove $x \in A \to x \in B$ $(A \subseteq B)$
2. Prove $x \in B \to x \in A$ $(B \subseteq A)$

2.3.4 Proof of transitivty of $\subset$

It is true that $A \subset B, B \subset D \rightarrow A \subset D$
Direct Proof
Assume $A \subset B, B \subset D$

1. $x \in A \rightarrow x \in D \quad (A \subset D)$
   (a) $x \in A$ assumption
   (b) $x \in A \rightarrow x \in B$ (defn of $A \subset B$)
   (c) $x \in B$ modus ponens
   (d) $x \in B \rightarrow x \in D$ (defn of $B \subset D$)
   (e) $x \in D$ modus ponens
2. $A \neq D$
   We assume $B \subset D$. Let q be something in D but not in B. Can q be in A? No, because $A \subseteq B$. (So if it was in A it would also HAVE to be in B).

3 Functions

$f : A \rightarrow B$ f is a function from A to B
$f(a) = b$ f assigns b to a
A is the domain of f
B is the codomain (the range is not the codomain)

To be a well defined function, each preimage must be assigned exactly one image

- preimage: a in $f(a) = b$
- image: b in $f(a) = b$

Is square root a well defined function?

$$\sqrt{25} = 5 \qquad \sqrt{25} = -5$$

It depends on what domain and codomain you give it. We can disallow negative outputs (principal square root), in which case the square root function is well defined.

3.1 Combining functions

If f and g are functions with the same domain and codomain, we can define things like

$$f(x) + g(x) \qquad f(x) \cdot g(x) \qquad f(x) \circ g(x) = f(g(x))$$

3.2 Properties of functions

There are 3 properties of functions we would like to define

- One-to-One (Injection)
  A function is one-to-one if "different inputs have different outputs". $\forall a \forall b (f(a) = f(b) \rightarrow a = b)$. Multiple different inputs do not map to the same input.

  Is $x \mapsto x^2$ one-to-one? It depends on the domain. For $\mathbb{Z}$, no (e.g. 7 and -7 both map to 49). For $\mathbb{N}$, yes.

  Examples of functions

  - $x \mapsto x^0$ Not one-to-one: everything maps to 1
  - $x \mapsto -x$ One-to-one: No way for two different real numbers to map to same negative
  - $x \mapsto |x|$ Not one-to-one: e.g. 5 and -5 both map to 5
  - $x \mapsto \frac{1}{x}$ One-to-one
  - $S \mapsto P(S)$ One-to-one
  - $S \mapsto |S|$ Not one-to-one (two sets can have the same size without having the same elements
  - $S \mapsto S^c$ One-to-one