

Intro to Proofs

Aamod Varma

MATH - 2106, Fall 2024

Contents

11 Relations	11
--------------	----

Real Numbers

Definition 0.1 (Properties of real numbers). Properties of \mathbb{R} are
 (d). \exists an order on \mathbb{R} which means $\forall x, y \in \mathbb{R}, x < y$ or $x > y$, or $x = y$
 Ordering follows the following properties,
 (1). $x < y, y < z \Rightarrow x < z$ (transitivity)
 (2). $x < y \Rightarrow x + z < y + z, \forall z \in \mathbb{R}$
 (3). $x < y, z > 0 \Rightarrow xz < yz$

Theorem 0.2. $xy = 0 \Leftrightarrow x = 0$ or $y = 0$

Proof. \Leftarrow Without loss of generality take, $x = 0$ Then we get,

$$0y.$$

We can write this as,

$$(0 + 0)y = 0y + 0y.$$

So,

$$0y = 0y + 0y.$$

Or, m

\Rightarrow

Assume the contrary that, $x \neq 0$ and $y \neq 0$ We have, $xy = 0$. Without loss of generality we take the multiplicative inverse of x so,

$$\frac{xy}{x} = \frac{0}{x}.$$

We showed that $0(k) = 0$ so $y = 0$

Which contradicts our assumption, hence our assumption must be wrong and $x = 0$ or $y = 0$

□

Theorem 0.3. $(-)x = -x$

Proof. We start with $(-1)x$ and add x to both sides so,

$$(-1)x + x = x(1 - 1) = 0x = 0.$$

So we showed that $(-1)x$ is the additive identity of x .
We know that the additive identity is unique for any x .
Therefore, $(-1)x = -x$ □

Theorem 0.4. $\forall x < y, z < 0$

$$xz > yz.$$

Proof. If $z < 0$ then that means $z = -k$ for some $k > 0$.

We can write $x < y$ as $x - y < 0$

Now if we multiply both sides by k we get,

$$k(x - y) < 0$$

Now if $k(x - y) = z'$ we can say that $z' < 0 \Rightarrow -z' > 0$

Or that

$$(-1)k(x - y) > 0$$

$$z(x - y) > 0$$

$$xz > yz$$

□

Theorem 0.5. $\forall x \in \mathbb{R}$ if $x \neq 0$ then $x^2 > 0$

Theorem 0.6. $x^2 = -(-x^2)$

Case 1, $x > 0$:

$$x > 0$$

$$x \times x > x$$

$$x \times x > 0x$$

$$x^2 > 0$$

Case 2, $x < 0$:

$$x < 0$$

Then the additive inverse $(-x) > 0$

$$(-x)(-x) > (-x)0$$

$$(-)(-1)x^2 > 0$$

$-(-1) = 1$ as 1 is the additive inverse of -1

$$x^2 > 0$$

Example. $\forall a, b > 0$

$$\frac{a+b}{2} \geq \sqrt{ab}$$

◇

Proof.

$$0 \leq (\sqrt{a} - \sqrt{b})^2 = a - 2\sqrt{ab} + b.$$

$$2\sqrt{ab} \leq a + b$$

$$\sqrt{ab} \leq \frac{a+b}{2}$$

□

Example. $x^2 - x + 1$

◇

Theorem 0.7. $\forall x, y \in \mathbb{R}$ we have,

$$|x| \geq x \text{ and } |x+y| \leq |x| + |y|.$$

Proof. We use proof by cases.

□

Proof related to Sets

Theorem 0.8.

$$A \cup B \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

Proof. We need to show that,

$$A \cup B \setminus (A \cap B) \subseteq (A \setminus B) \cup (B \setminus A).$$

and,

$$(A \setminus B) \cup (B \setminus A) \subseteq A \cup B \setminus (A \cap B).$$

□

Theorem 0.9. $A \subseteq B \Leftrightarrow A \cup B = B$

Proof. \Rightarrow Take $\forall x \in A \cup B$, so either

Case 1, $x \in A$:

We know that by definition if, $A \subseteq B$ then for $x \in A, x \in B$ so $x \in B$

Case 2, $x \in B$: If $x \in B$ then we don't need to go further.

So we get $\forall x \in A \cup B, x \in B$

\Leftarrow

$\forall x \in A \Rightarrow x \in A \cup B = B$

So, $x \in B$ which means that, $A \subseteq B$

□

Disproofs

If we need to show existence, $\exists x.P(x)$. We can show using,

1. Direct constructions
2. Indirectly (contradiction). For instance we can show that, $\forall x, \neg P(x)$ is false

Example. $\exists a, b, c \in R - Q$ s.t. $a^{bc} \in Q$

◇

Example. Pigeonhole principle

Suppose there are m balls in n boxes, $m > n \geq 1$ then, \exists a box where there are at least, $\frac{m}{n} + 1$ balls

◇

Proof. Assume pigeonhole is false.

Then, there are at most $\frac{m}{n}$ balls in each box.

In case 1 where $\frac{m}{n} \notin N \Rightarrow$ total balls $\leq n[\frac{m}{n}] = \frac{nm}{n} = m$ which is a contradiction.

In case 2 where $\frac{m}{n} \in N$ there are at most $\frac{m}{n} - 1$ balls in each box. So total number of balls are $\frac{nm}{n} - n = m - n$ which is contradictory.

□

To disprove $\forall x.P(x)$ we can show that, $\exists \neg P(x)$

Example. 100 can't be written as the sum of two even integers and an odd integer.

◇

Proof. Suppose it's false $\Rightarrow \exists a, b, c \in Z$ s.t. $2|a, 2|b, 2 \nmid c$ and $100 = a + b + c$

But, $2|a, 2|b \Rightarrow 2|a + b$ but $2 \nmid c \Rightarrow 2 \nmid (a + b) + c = 100$

So we get, $2 \nmid 100$ which is a contradiction.

Which means that the original statement is true.

□

Example. \nexists the smallest positive real number

The smallest positive real number is defined as $x \in R$ s.t. $x > 0$ and $\forall y > 0, x \leq y$

◇

Proof. Let's assume it is true which means that $\exists x \in R$ s.t. $x > 0$ and $\forall y > 0, x \leq y$

We know that $x > 0 \Rightarrow \frac{x}{2} > 0$

So if we set $y = \frac{x}{2}$ then we get

$$x \leq \frac{x}{2}.$$

Which is a contradiction.

Hence it cannot be the case that there exists the smallest positive number. \square

Example. $\nexists f(x)$: a polynomial with integer coefficients s.t. $\forall n, f(n)$ is prime \diamond

Proof. Consider the general form of a polynomial,

$$f(x) = a_1x^n + \dots + a_n$$

Case 1: $a_n = 0$

If $a_n = 0$ then for any $x > 1$ we can take x common and get

$$f(x) = x(a_1x^{n-1} + \dots + a_{n-1})$$

So we get a factor $x \neq 1$

Case 2: $a_n = 1$

In this case we can just plug $x = 0$ and we get $f(x)$ is neither prime or composite

Case 3: $a_n > 1$??? \square

Example. Let $f(x) = x^3 + 2x - 5$ then \exists unique $x_0 \in [1, 2]$ s.t. $f(x_0) = 0$ \diamond

Proof. Using intermediate value theorem.

$$f(1) = -2$$

$$f(2) = 7$$

So because $-2 < 0 < 7$ we know that there must exist an $x_0 \in [1, 2]$ s.t. this is the case.

To show unique we need to show its strictly increasing. Or in other words, we need to show for every $x_1, x_2 \in [1, 2], x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2)$

So we need to show that,

$$x_1^3 + 2x_1 - 5 \leq x_2^3 + 2x_2 - 5$$

$$x_1^3 + 2x_1 \leq x_2^3 + 2x_2$$

$$(x_1^3 - x_2^3) + 2(x_1 - x_2) \leq 0$$

It is enough to show that both $x_1^3 - x_2^3$ and $x_1 - x_2$ are smaller than or equal to 0.

$$x_1^3 - x_2^3 = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) = k(x_1 - x_2) \leq 0$$

Similarly,

$$2(x_1 - x_2) \leq 0 \text{ a } x_1 - x_2 \leq 0$$

So we have, $x_1^3 - x_2^3 + 2(x_1 - x_2) \leq 0$

Which tells us that our function is strictly increasing which implies that we only have a unique $x_0 \in [1, 2]$ \square

Mathematical Induction

Theorem 8.10 (Properties of Natural Numbers). (a). $1 \in N$
 (b). $\forall k \in N, \exists k + 1 \in N$
 (c). $\forall k \in N - \{1\}, \exists n \in N, \text{ s.t. } k = n + 1 \in N$
 (d). Needs to be well-ordered.

An ordered set S is well-ordered if,

$$\forall A \in S \text{ s.t. } A \neq \phi, \exists x = \min A$$

$$\text{Or, } \exists x \in A \text{ s.t. } y \in A, x \leq y$$

Example. \mathbb{Q} is not well-ordered as it does not have a minimum ◇

Example. \mathbb{Z} is not well-ordered as it does not have a minimum ◇

Axiom 8.11. N is well-ordered

Theorem 8.12. If $A \subseteq S$ and S is a well-ordered set then A is well-ordered.

Proof. Let $B \subseteq A$ and $B \neq \phi \Rightarrow B \subseteq S$
 So B has a min x which means that A is well-ordered by definition. □

Example. $[1, \infty)$ is not well-ordered because a subset $(1, \infty)$ does not have a min ◇

Theorem 8.13. $\forall a \in \mathbb{Z}, d \in \mathbb{N}, \exists q, r \in \mathbb{Z} \times \{0, 1, \dots, d-1\} \text{ s.t.}$

$$a = dq + r$$

Proof. Let $S = \{a - nd : n \in \mathbb{Z}, a - nd \in \mathbb{N}\}$
 First we can see that S is non-empty as we can take

$$n = -|a| - 1 \Rightarrow a - nd > 0$$

Now because this is a subset of \mathbb{N} it follows the well-ordering principle implying that $\min S = a - nd = m$

$m \in S \Rightarrow \exists l \in \mathbb{Z} \text{ s.t. } m = a - ld$

Case 1: If $m > d$ then

$$a - (l+1)d > 0$$

$$a - (l+1)d \in S \Rightarrow a - (l+1)d < m$$

Which is a contradiction. This means that $m \not> d$

Case 2: $m = d$

Let $q = l+1, r = 0$

$$m = d \Rightarrow a - ld = d \Rightarrow a - (l+1)d = 0$$

Case 3: $0 < m < d$

Let $q = l, r = m \Rightarrow a = dq + r$

Now to show uniqueness,

Suppose, $(q, r), (q', r') \in \mathbb{Z} \times \{0, 1, \dots, d-1\}$ and

$$a = qd + r = q'd + r'$$

We have,

$$(q - q')d = r' - r$$

$$0 - (d-1) \leq r' - r \leq d-1$$

And,

$$d|r' - r \Rightarrow r' - r = 0$$

□

Definition 8.14. Let $a, b \in \mathbb{N}, d = \text{GCD}(a, b) \in \mathbb{N}$ if

(a). $d|a$ and $d|b$ and

(b). If $d' \in \mathbb{N}$ s.t. $d'|a$ and $d'|b$ then $d \geq d'$

Theorem 8.15. $\forall a, b \in \mathbb{N}, \exists p, q \in \mathbb{Z} \text{ s.t. } \text{GCD}(a, b) = ap + bq$

Proof. Let $S = \{a_m + b_n : m, n \in \mathbb{Z}, a_m + b_n \subseteq \mathbb{N}\}$

We know S is non-empty as $m, n = 1$ makes it $a + b > 0$ as $a, b \in \mathbb{N}$

So by well-ordering principle we know that $\exists \min S = d$ and $p, q \in \mathbb{Z} \text{ s.t.}$

$$d = ap + bq$$

If $d' \in \mathbb{N}$ s.t. $d'|a$ and $d'|b \Rightarrow d'|ap + bq = d$

So, $d \in \mathbb{N} \Rightarrow d \geq d'$

$$d \in \mathbb{N} \Rightarrow \exists m \in \mathbb{Z}, r \in \{0, \dots, d-1\} \text{ s.t. } a = md + r$$

Which means $r = a - md = a - m(ap + bq) = a(1 - mp) + b(-mq)$

$r < d$ but $d = \min S \Rightarrow r \notin S \Rightarrow r = 0$

So $a = md$ so $d|a$. Similarly, $d|b$

This means d is the greatest common divisor.

□

Theorem 8.16 (Induction principle). Suppose $k \in \mathbb{N}, S \subseteq \mathbb{N}$ satisfy,

- (a). $k \in S$
 - (b). if $n \in S$ then $n + 1 \in S$
- then $\{k, k + 1, \dots\} \subseteq S$

Proof. Let $A = \{n \in \mathbb{N}, n \geq k : n \notin S\}$

Suppose $A \neq \emptyset \Rightarrow n_0 = \min A$ exists

Which means $n_0 \geq k$ but $k \notin A$ due to (a). So, $n_0 > k \Rightarrow n_0 - 1 \geq k$ and $n_0 - 1 \notin A$ as $n_0 = \min A$

(b). and $n_0 - 1 \notin A \Rightarrow n_0 \notin A$ contradiction which implies that $A = \emptyset$

□

Corollary 8.17. If a statement $P(n), n \in \mathbb{N}$ satisfies

- (a) $P(k)$ is true
 - (b) $P(n) \Rightarrow P(n + 1)$
- Then $P(n)$ is true for all $n \geq k$

Theorem 8.18. $\sum_{k=1}^n k = \frac{n+1}{2}n$

Proof. Proof by induction.

If $n = 1$, then (1) holds.

If $n = k$ then we have,

$$1 + \dots + k = k \frac{k+1}{2}$$

Now we need to show that $1 + \dots + k + k + 1 = (k + 1) \frac{k+2}{2}$

Using the statement for $n = k$ we can do,

$$k \frac{k+1}{2} + k + 1 = (k + 1) \frac{k+2}{2}$$

Simplifying the left hand side we get,

$$(k + 2) \frac{k+1}{2} = (k + 1) \frac{k+2}{2}$$

It is trivial to see that this is true.

Hence by induction our statement is true.

□

Definition 8.19. $C_n^m = \binom{n}{m} = \frac{n!}{m!(n-m)!}$ if $n \geq m \geq 0$ and 0 otherwise

Remark. $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$ is a stronger definition of factorial

Theorem 8.20. $\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m+1}, \forall n, m \in \mathbb{Z}$

Proof. We prove by cases.

Case 1: $m \leq -2$ or $m > n$

Case 2: $n = m = -1$

Case 3: $n > m = -1$

Case 4: $m \geq 0$ and $m \leq n$

□

Theorem 8.21. $\forall n \in N \cup \{0\}, a, b \in \mathbb{R}$

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

Chapter 11

Relations

Theorem 11.1. Relatoin from A to B is described by a subset of $A \times B$ which is a graph of the relation.

Theorem 11.2 (Equivalence Relation). R on A is an equivalence relation if it is, reflexive, symmetric and transitive.

Definition 11.3 (Equivalence Classes). $[a]_R = \{x \in A : aRx\}$

Property. $a \in [a]_R$ since R is reflexive

Theorem 11.4. Let R be an equivalence relatoin on A then,

1. aRb
2. $[a]_R = [b]_R$
3. $[a]_R \cap [b]_R \neq \phi$

Definition 11.5. A partition of A is a family of subsets, $(A_i)_{i \in I}$ where $A_i \subseteq A$. We have,

1. $A_i \neq \phi, \forall i \in I$
2. $\cup A_i = A$
3. If $i_1 \neq i_2$ then $A_{i_1} \cap A_{i_2} = \phi$

Definition 11.6. Let R be an equivalence relation on A , $A/R = \{\text{equivalence classes of } R\}$

Theorem 11.7. Let R be an equivalence relation on A then $A/R = \{\dots\}$ form a partiiton of A .

Proof. (i) $\forall \alpha \in A/R, \exists a \in A, s.t. \alpha = [a]_R$

$\Rightarrow a \in \alpha \Rightarrow \alpha \neq \phi$

(ii) $\forall a \in A, a \in [a]_R \Rightarrow a \in U$

(iii) Suppose, $\alpha, \beta \in A/R, \alpha \neq \beta$

$\Rightarrow \exists a, b \in A, s.t. \alpha = [a]_R, \beta = [b]_R$

So, $\alpha \cap \beta \neq \phi$

Therefore, A/R form a partition of A □

Example. $A = \mathbb{Z}, n \in \mathbb{N} R \equiv_n$

$\mathbb{Z}/ \equiv_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$ ◇

Example. $A \neq \phi$ and $R =$ then R is not equivalent because of reflexivity ◇

Theorem 11.8. Let $A \neq \phi$ and $\{S_i\}_{i \in I}$ is a partition of A then \exists equivalence relation R on A s.t. $A/R = \{S_i\}_{i \in I}$

Proof. Let $R = \{(a, b) \in A \times A : \exists i \in I, s.t. a, b \in S_i\}$

(a) $\forall a \in A = \bigcup S_i \Rightarrow \exists i \in I$ s.t. $a \in S_i$

Since, $a, a \in S_i \Rightarrow (a, a) \in R$. So it is reflexive

(b). Suppose $(a, b) \in R \Rightarrow \exists i \in I$ s.t. $a, b \in S_i \Rightarrow b, a \in S_i \Rightarrow (b, a) \in R$

So, it is symmetric.

(c). Suppose $(a, b), (b, c) \in R \Rightarrow \exists i_1, i_2 \in I$ s.t. $a, b \in S_{i_1}, b, c \in S_{i_2} \Rightarrow b \in S_{i_1} \cap S_{i_2} \Rightarrow S_{i_1} \cap S_{i_2} \neq \phi \Rightarrow S_{i_1} = S_{i_2} \Rightarrow a, c \in S_{i_1} \Rightarrow (a, c) \in R$

So we have R is an equivalence relation.

(d) $\forall i \in I, S_i \neq \phi \Rightarrow \exists a \in S_i$. If $b \in [a]_R \Rightarrow (a, b) \in R \Rightarrow \exists j \in I, s.t. a, b \in S_j$.

$a \in S_i \Rightarrow S_i \cap S_j \neq \phi \Rightarrow S_j = S_i$ so,

$a, b \in S_i \Rightarrow [a]_R \subseteq S_i$

$\forall c \in S_i$ by definition of $R, aRc \Rightarrow c \in [a]_R \Rightarrow S_i \subseteq [a]_R$

Hence $S_i = [a]_R$

(e) Now we show that $A/R \subseteq \{S_i\}_{i \in I}$ □

Consider \equiv_n where $n \in \mathbb{N}$ and let $[z]_n = z/ \equiv_n$. Where,

$$[z]_n = \{[0]_n, \dots, [n-1]_n\}$$

Lemma 11.9. Suppose $a, b, a', b' \in z$ satisfying,

$$a \equiv_n a', b \equiv_n b'$$

then,

$$a + b \equiv_n a' + b'$$

and

$$a - b \equiv_n a' - b'$$

and

$$a'b' \equiv_n ab$$

Definition 11.10. For any $\alpha, \beta \in [z]_n \exists a, b \in z$ s.t. $\alpha = [a]_n, \beta = [b]_n$ then,

$$\alpha + \beta = [a + b]_n, \alpha - \beta = [a - b]_n, \alpha\beta = [ab]_n$$

Example. $n = 12$ then

1. $[2]_n[3]_n = [6]_n$
2. $[5]_n + [8]_n = [1]_n$
3. $[5]_n - [8]_n = [-3]_n = [9]_n$
4. $[5]_n[8]_n = [40]_n = [4]_n$
5. $[8]_n[9]_n = [0]_n$

◇

Theorem 11.11. Suppose $n \in N - \{1\}, a \in N$

- (i). $GCD(a, n) = 1$
- (ii). $\forall b, c \in Z, [a]_n[b]_n = [a]_n[c]_n \Rightarrow [b]_n = [c]_n$

Proof. $\Rightarrow GCD(a, n) = 1 \Rightarrow \exists, d, q \in \mathbb{Z}$ s.t.

$$ad + nq = 1 \Rightarrow [a]_n[d]_n = [1]_n$$

$$[a]_n[b]_n = [a]_n[c]_n \Rightarrow [d]_n[a]_n[b]_n = [d]_n[a]_n[c]_n$$

$$\Rightarrow [1]_n[b]_n = [1]_n[c]_n \Rightarrow [b]_n = [c]_n$$

←

□

Definition 11.12. A relation on a set $A \neq \phi$ is an order if it is reflexive, antisymmetric and transitive.

Definition 11.13. We say that $a, b \in A$ are comparable if $a \preccurlyeq b$ or $b \preccurlyeq a$

Definition 11.14. If $\forall a, b \in A$ are comparable then " \preccurlyeq " is a total order

Example.

$$(\mathbb{Z}, \leq), (\mathbb{R}, \leq), (\mathbb{Q}, \leq)$$

◇

Example. $U \neq \phi, (P(U), \subseteq)$

◇