Theory of Computation (Version 2)

William Chu

November 11, 2018

Contents

1 Mathematical Preliminaries

1.1 Set Theory

Definition 1.1.1 (Set)**.** A set is a collection of distinct elements, where the order in which the elements are listed does not matter. The size of a set S, denoted $|S|$, is known as its cardinality or order. The members of a set are referred to as its elements. We denote membership of x in S as $x \in S$. Similarly if x is not in S, we denote $x \notin S$.

Definition 1.1.2 (Set Union)**.** Let A, B be sets, Then the union of A and B, denoted $A \cup B$ is the set:

$$A \cup B := \{x : x \in A \text{ or } x \in B\}$$

Definition 1.1.3 (Set Intersection)**.** Let A, B be sets. Then the intersection of A and B, denoted $A \cap B$ us the set:

$$A \cap B := \{x : x \in A \text{ or } x \in B\}$$

Definition 1.1.4 (Symetric Difference)**.** Let A, B be sets. Then the symetric difference of A and B , denoted $A \Delta B$is the set:

$$A \Delta B := \{x : x \in A \cup B, \text{ but } x \notin A \cap B\}$$

Definition 1.1.5 (Set Complementation)**.** Let A be a set contained in our universe U. The complement of A, denoted A^C or $\overline{A}$:

$$\overline{A} := \{x \in U : x \notin A\}$$

Definition 1.1.6 (Set Difference)**.** Let A, B be sets contained in our universe U. The difference of A and B, denoted $A \backslash B$ or $A - B$ is the set:

$$A \backslash B := \{x : x \in A \text{ and } x \notin B\}$$

Definition 1.1.7 (Cartersian Product)**.** Let A, B be sets. The cartesian product of A and B, denoted $A \times B$, is the set:

$$A \times B := \{(a, b) : a \in A, \, b \in B\}$$

Definition 1.1.8 (Subset)**.** Let A, B be sets. A is said to be a subset of B if for every $x \in A$, we have $x \in B$ as well. This is denoted $A \subset B$ (equivocally, $A \subseteq B$). Note that B is a superset of A.

Definition 1.1.9 (Power Set)**.** Let S be a set. The power set of S, denoted 2^S, or $\mathcal{P}(S)$, is the set of all subsets of S. Formally:

$$2^S := \{A : A \subset S\}$$

Definition 1.1.10 (Set equality)**.** Let A, B be sets. A=B if $A \subset B$ and $B \subset A$

Proposition 1.1.1. Let $A = \{6n : n \in \mathbb{Z}\}$, $B = \{2n : n \in \mathbb{Z}\}$, $C = \{3n : n \in \mathbb{Z}\}$. So $A = B \cap C$.

Proof. We first show that $A \subset B \cap C$. Let $x \in A$. By definition of A, $x = 6k$ for some $k \in \mathbb{Z}$. We show $x \in B$ and $x \in C$. We first observe $x = 2 \cdot (3k)$. Therefore, $x \in B$. Now observe$x = 3 \cdot (2k)$. So $x \in C$. Thus $x \in B \cap C$. As x was arbitrairy, we conclude that $A \in B \cap C$. We now show that $(B \cap C) \subset A$. Let $y \in B \cap C$. Let $n_1, n_2 \in \mathbb{Z}$ such that $y = 2n_1 = 3n_2$. As 2 and 3 share no common factors, we have that $2 \cdot 3 | y$. so $6 | y$. Thus $y = 6h$ for some $h \in \mathbb{Z}$. So $y \in A$. Thus, $(B \cap C) \subset A$. We showed that $A \subset (B \cap C)$ and $(B \cap C) \subset A$. We conclude that $A = B \cap C$ by the definition of set equality. QED

Proposition 1.1.2. Let A, B, C be sets, then $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Proof. We first show $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$. Let $(x, y) \in A \times (B \cup C)$. We show that $(x, y) \in (A \times B) \cup (A \times C)$. Suppose $y \in B$. Then $(x, y) \in A \times B$. Otherwise, $y \in C$. Then $(x, y) \in A \times C$. So $(x, y) \in (A \times B)$ or $(x, y) \in A \times C$. Thus, $(x, y) \in (A \times B) \cup (A \times C)$. We conclude that $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$. We now show $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$. Let $(x, y) \in (A \times B) \cup (A \times C)$. We show that $(x, y) \in A \times (B \cup C)$. Suppose $(x, y) \in A \times B$. So $x \in A$ and $y \in B$. Thus, $(x, y) \in A \times (B \cup C)$. Otherwise, $(x, y) \in A \times C$. So $x \in A$ and $y \in C$. So $y \in B \cup C / Thus, (x, y) \in A \times (B \cup C)$. Since in both cases, $(x, y) \in A \times (B \cup C)$, we conclude that $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$. Since $A \subset (B \cap C)$ and $(B \cap C) \subset A$ and $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$, $A \times (B \cup C) = (A \times B) \cup (A \times C)$. QED

1.2 Relations

TODO: FINISH

Definition 1.2.1 (Relation)**.** Let X be a set. A k-ary relation on X is a subset $R \subset X^k$.

Definition 1.2.2 (Function)**.** Let X and Y be sets. A function f is a subset (or 1-place relation) of $X \times Y$ such that for every $x \in X$, $\exists! y \in Y$ where $(x, y) \in f$.

Definition 1.2.3 (Injection)**.** A function $f : X \to Y$ is said to be an injection if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. Equivocally, f is an injection if $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

Definition 1.2.4 (Surjection)**.** Let X and Y be sets. A function $f : X \to Y$ is a surjection if $\forall y \in Y$, $\exists x \in X$ s.t. $f(x) = y$.

Definition 1.2.5 (Bijection)**.** Let X and Y be sets. A bijection is a function$f : X \to Y$ that is both an injection and a surjection.

Definition 1.2.6 (Reflexive Relation)**.** A relation R on the set X is said to be reflexive if $(a, a) \in R$ for every $a \in X$.

Definition 1.2.7 (Symmetric Relation)**.** A relation R on the set X is said to be symmetric if $(a,b) \in R$ if and only if $(b,a) \in R$ for every $a, b \in X$.

Definition 1.2.8 (Transitive Relation)**.** A relation R on the set X is said to be transitive if for every $a, b, c \in X$ satisfying $(a,b),(b,c) \in R$, then $(a,c) \in R$.

Definition 1.2.9 (Equivalence Relation)**.** An equivalence relation is a reflexive, symmetric, and transitive relation.

Definition 1.2.10 (Congruence Relation)**.** Let $n \leq 1$ be an integer. The congruence relation modulo n is a binary relation on $\mathbb{Z}$ given by: $a \equiv b (\text{mod } n)$ (read as: a is congruent to b modulo n) if and only if $n|(b-a)$.

Proposition 1.2.1. The congruence relation modulo n is an equivelence relation.

Proof. We show that the congruence relation modulo n is reflexive, symmetric, and transitive.

Reflexivity: We show that $\forall a \in \mathbb{Z}$, $a \equiv a \pmod{n}$. Observe that $a - a = 0$. So $n \times 0 = 0 = a - a$. Thus $n|a - a$. So $a \equiv a \pmod{n}$. We conclude that the congruence relation modulo n is reflexive.

Symmetry: We show that $b \equiv a \pmod{n}$. Let $q \in \mathbb{Z}$ such that $nq = a - b$. Thus, $n(-q) = b - a$, so $n|(b-a)$. Thus, $b \equiv a \pmod{n}$. So the congruence relation modulo n is symmetric.

Transitive: Let $a, b, c \in \mathbb{Z}$ s.t. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. We show that $a \equiv c \pmod{n}$. By the definition of the congruence relation, $n|(a-b)$ and $n|(b-c)$. Let $h, k \in \mathbb{Z}$ s.t. $nh = a - b$ and $nk = b - c$. So $nh + nk = n(h+k) = a - c$. Thus, $n|(a-c)$, so $a \equiv c \pmod{n}$. It follows that the congruence relation modulo n is transitive.

We conclude that the congruence relation modulo n is an equivalence relation. QED

1.3 Induction

TODO

1.4 Asymptotics

1.5 Combinatorics

TODO

1.6 Countability

TODO

1.7 Graph Theory

TODO

2 Autonoma Theory

2.1 Regular Expressions

TODO

2.2 Finite State Automata

TODO

2.3 Pumpng Lemma

TODO

2.4 Closure Propertoes

TODO

2.5 Myhill-Nerode and DFA Minimization

TODO

3 Group Theory

TODO

3.1 Brzozowski Algebraic Method

TODO

3.2 Dihedral Groups

TODO

3.3 Symmetry Groups

TODO

4 Turing Machines and Decidability

4.1 Standard Deterministic Turing Machine

TODO

4.2 Undecidability

TODO

4.3 Reducibility

TODO

5 Complexity Theory

5.1 $\mathcal{P}$ and $\mathcal{NP}$

TODO

5.2 $\mathcal{NP}$-Completeness

TODO