CS 378 Intro to Theory of Computation **Fall 2015**

Chapter 0: Math Review

Professor Dale Skrien *Zach Schutzman*

NB: *These notes are a revised version of those taken during Dale Skrein's CS 378 course at Colby College in Fall 2015. The course followed Michael Sipser's Introduction to the Theory of Computation (3ed) text.*

0.1 Set Theory

Set theory is the foundation of modern mathematics. As such, it is relevant and important to the material in this course. We're going to move very quickly through some foundational elements (heh) of set theory to establish a mathematical language (hah) with which to precisely communicate in this course.

Definition 0.1 *A **set** is a collection of distinct objects, called **elements**.*

Definition 0.2 *A **subset** S of some set $\mathcal{A}$ is a set such that every element of S is also an element of $\mathcal{A}$. This is denoted $S \subset \mathcal{A}$.*

*We often talk about sets as being implicitly a subset of some **universal set**. For example, if I asked you to name some things that are not prime numbers, you might list $6, 14, 100$, but probably not apple or $-.5$, because you assume, possibly incorrectly, that the universe is postitive integers. In this course, the implicit universe is probably the correct one, and if there is any ambiguity, the universe will be made explicit.*

Definition 0.3 *The **empty set**, denoted $\emptyset$, is the set containing no elements. Note that it is a (vacuously) true statement that the empty set is a subset of every set.*

Definition 0.4 *A **function** f is a mapping between two sets $\mathcal{A}$ and $\mathcal{B}$, called the **domain** and **codomain**, respectively, which satisfies the following two properties:*

1. *For all $z \in \mathcal{A}$, $f(z) \in \mathcal{B}$*
2. *If $f(x) = f(y)$, then $x = y$*

Definition 0.5 *A function is an **injection** if all elements of the domain map to unique elements of the codomain. A function is a **surjection** if all elements of the codomain are equal to fx for some x in the domain. A function is a **bijection** if it is both an injection and a surjection.*

Definition 0.6 *The **cardinality** of a set is, in some sense, a measure of the number of elements of that set. For two sets $\mathcal{A}, \mathcal{B}$, we say $card(\mathcal{A}) \leq card(\mathcal{B})$ if there exists some injection from $\mathcal{A}$ to $\mathcal{B}$. Informally, this means that $\mathcal{A}$ is 'no bigger' than $\mathcal{B}$. The cardinality of a finite set is the number of elements in that set.*

Definition 0.7 *The **natural numbers**, denoted $\mathbb{N}$, is the set $0, 1, 2, 3 \ldots$. Importantly, the natural numbers can be identified by the following inductive definition (Peano Axions):*

1. 0 *is a natural number.*
2. *For any natural number* n, $n + 1$ *is a natural number.*
3. *For any non-zero natural number* m, $m = n + 1$ *for some natural number* n.

Definition 0.8 *A set* $\mathcal{A}$ *is* ***countable*** *if* $card(\mathcal{A}) \leq card(\mathbb{N})$. *All finite sets are countable. The natural numbers are* ***countably infinite****. A set* $\mathcal{B}$ *is countably infinite if there exists a bijection between* $\mathcal{B}$ *and* $\mathbb{N}$. *A set* $\mathcal{C}$ *is* ***uncountably infinite*** *if it is infinite and such a bijection does not exist.*

Definition 0.9 *The textbfpower set of a set* $\mathcal{A}$*, denoted* $\mathcal{P}(\mathcal{A})$*, is the set of all subsets of* $\mathcal{A}$.

Claim 0.10 *The real numbers (denoted* $\mathbb{R}$*) are uncountable.*

Proof:*(Cantor) Consider the interval* $[0, 1]$ *as a subset of* $\mathbb{R}$. *We will show that this subset is uncountable, therefore all of* $\mathbb{R}$ *is as well.*

Suppose, for the sake of contradiction, that this set is countable. Then we identify each real number in the interval with some natural number i. *Consider the decimal expansions of all of these real numbers. For rational numbers, which have multiple decimal representations (i.e.* $.25 = .249999\ldots$*), we consider the non-terminating one. Now, construct the following real number in the interval* $[0, 1]$. *For each natural number* i*, consider the* i^{th} *digit in the corresponding real number's decimal expansion. If this number is not a* 5*, put a* 5 *in that position. If it is already a* 5*, put a* 6 *in that position.*

By construction, this real number is not identified with a natural number, which is a contradiction, so the set of real numbers must have strictly larger cardinality than the real numbers.

■

Claim 0.11 $\mathcal{P}(\mathbb{N})$ *is uncountable.*

Proof: *We will show there exists a bijection between* $\mathcal{P}(\mathbb{N})$ *and the interval* $[0, 1] \subset \mathbb{R}$.

Consider binary decimal representations of the elements of $[0, 1]$ *and the indicator function on the subsets of natural numbers where the digit in the* i^{th} *position is a* 1 *if and only if* i *is in the corresponding subset. We can therefore map between subsets of* $\mathbb{N}$ *and real numbers in* $[0, 1]$. *Because this map is invertible, it is a bijection and the power set of* $\mathbb{N}$ *is uncountable.*

■

0.2 Relations

Relations are a way to formalize a way of comparing elements of a set.

Definition 0.12 *An* ***equivalence relation*** $\sim$ *on a set* $\mathcal{A}$ *is a binary relation satisfying three properties, for* $x, y, z \in \mathcal{A}$:

1. ***Reflexive****:* $x \sim x$*, for all* $x \in \mathcal{A}$.

2. ***Symmetric**: if $x \sim y$, then $y \sim x$.*
3. ***Transitive**: if $x \sim y$ and $y \sim z$, then $x \sim z$.*

Definition 0.13 *A **total order** $\leq$ on a set $\mathcal{B}$ is a binary relation satisfying three properties, for $x, y, x \in \mathcal{B}$:*

1. ***Reflexive**: $x \leq x$, for all $x \in \mathcal{B}$.*
2. ***Antisymmetric**: either $x \leq y$, or $y \leq x$, for all $x, y \in \mathcal{B}$.*
3. ***Transitive**: if $x \leq y$ and $y \leq z$, then $x \leq z$.*

Equality of rational numbers ($\frac{1}{2} = \frac{3}{6} = \frac{34}{68}$) is a commonly understood equivalence relation, and the ordering of the integers is a commonly understood total order.

Definition 0.14 *An **equivalence class** of some element $x \in \mathcal{A}$ under some equivalence relation $\sim$, denoted $[x]$ is the subset of $\mathcal{A}$ such that every element of $[x]$ is equivalent to x under the relation*

Claim 0.15 *Equivalence classes partition a set. That is, for all elements $x, y \in \mathcal{A}$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.*

Proof: *Consider some equivalence class $[x]$ and some element $[y]$. If $x \sim y$, then $y \in [x]$ and $y \sim z$ for all $z \in [x]$. Therefore, by transitivity, $[y] = [x]$. Otherwise, x and y are not equivalent, so $[x] \neq [y]$. If there existed some w in both $[x]$ and $[y]$, then it must be $w \sim x$ and $w \sim y$. But by transitivity, that implies $y \sim x$, so their equivalence classes must be equal. Therefore, no such w exists and $[x]$ is disjoint from $[y]$.* ■

0.3 Graphs

Definition 0.16 *A **graph** $G = \langle V, E \rangle$ is a pair of sets V, the vertex set, and E, the edge set. An edge $e \in E$ is a pair of vertices $u, v \in V$. In an **undirected graph**, u and v are an unordered pair. In a **directed graph**, u and v are an ordered pair, corresponding to an edge (often called an **arc**) from u into v.*

Definition 0.17 *A **subgraph** $H = \langle V', E' \rangle$ of a graph $G = \langle V, E \rangle$ is a graph such that $V' \subset V$ and $E' \subset E$.*

Definition 0.18 *The **degree** of a vertex v is the number of edges e such that $e = v, a$ for some $a \in V$. In a directed graph, the **indegree** is the number of arcs into v and the **outdegree** is the number of arcs leaving v.*