1 Preliminaries

Let $\mathbb{Z}$ denote the set of all integer numbers (positive and negative). The set of natural numbers, denoted by $\mathbb{N} = \{1, 2, \ldots\}$, are all the integer numbers which are positive.

**Theorem 1.1 (Unique factorization theorem)** Let $n \in \mathbb{N}$ be a natural number. Then $n$ can be written as a product of prime numbers $n = (p_1)^{\alpha_1}(p_2)^{\alpha_2}\cdots(p_r)^{\alpha_r}$, where $\alpha_1 \geq 1$. Furthermore, this factorization is unique. Namely, if $n = (p_1)^{\alpha_1}(p_2)^{\alpha_2}\cdots(p_r)^{\alpha_r}$ and $n = (p_1)^{\beta_1}(p_2)^{\beta_2}\cdots(p_r)^{\beta_r}$, then $\alpha_j = \beta_j$, for $j = 1, \ldots, r$.

2 Countable sets

**Definition 2.1** A set $S$ is countable if there exists a bijection $f : S \rightarrow \mathbb{N}$, where $\mathbb{N}$ is the set of natural numbers. We denote this fact, by $|S| = \aleph_0$.

**Lemma 2.2** If there exists an injection (i.e., one-to-one) mapping $f$ between a set $S$ and $\mathbb{N}$, and $S$ is infinite, then $S$ is countable.

**Proof:** We need to show a bijection between $S$ and $\mathbb{N}$. To that end, consider the set $A = f(S) = \{f(s) \mid s \in \mathbb{N}\}$. For an element $u \in A$, let $r(u)$ be the number of elements in $A$ smaller or equal to $u$ in $A$. Thus, $r(u) \geq 1$ for all elements $u \in A$, $r(u)$ is an integer number, and furthermore, for any $a \neq b \in A$, we have $r(a) \neq r(b)$. Since $S$ is infinite, it follows that $A$ is infinite. Thus, for any natural number $n$, there exists $c \in A$ such that $r(c) = n$. Namely, $r : A \rightarrow \mathbb{N}$ is a bijection. Thus, the combined mapping $r(f(x))$ is a bijection between $S$ and $\mathbb{N}$.

**Claim 2.3** The integer numbers $\mathbb{Z}$ are countable.

**Proof:** Let $f : \mathbb{Z} \rightarrow \mathbb{N}$, which is the following

$$f(x) = \begin{cases} 2x + 1 & x \geq 0 \\ -2x & x < 0. \end{cases}$$
This mapping is clearly an injection and onto. As such it is a bijection, and the claim follows.

\textbf{Claim 2.4} The rational numbers \( \mathbb{Q} \) are countable.

\textit{Proof:} Let \( f : \mathbb{Q} \to \mathbb{N} \) be the mapping, such that for \( a, b \in \mathbb{N} \), the rational number \( a/b \) is mapped to \( 5^a7^b \). The rational number \( -a/b \) is mapped to \( 2 \cdot 5^a7^b \). Since two natural numbers have unique factorization into primes, it follows that \( f \) is an injection. Thus, \( \mathbb{Q} \) is countable by Lemma 2.2.

\textbf{Claim 2.5} \( \mathbb{N} \times \mathbb{N} \) is countable. \( \mathbb{N}^r = \underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{r \text{ times}} \) is countable for an integer \( r \). In fact, \( \mathcal{X} = \bigcup_{r \in \mathbb{N}} \mathbb{N}^r \) is countable (this is the set of all finite sequences of integer numbers).

\textit{Proof:} Consider the mapping \( f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \), where \( f((a, b)) = 2^a3^b \). Clearly, \( f \) is an injection and the claim holds by Lemma 2.2.

In general, let \( p_i \) denote the \( i \)-th prime number (we remind the reader that there are infinite number of prime numbers), for \( i = 1, 2, \ldots \). Thus, given \( (a_1, a_2, \ldots, a_r) \in \mathbb{N}^r \), let \( g : \mathbb{N}^r \to \mathbb{N} \) be

\[ g(a_1, a_2, \ldots, a_r) = (p_1)^{a_1}(p_2)^{a_2}\cdots(p_r)^{a_r}. \]

By the unique factorization of natural numbers, it follows that \( g \) is an injection, and it follows that the set \( \mathbb{N}^r \) is countable.

Finally, consider any element of \( (b_1, b_2, \ldots, b_m) \in \mathcal{X} \). Similarly to the above, we define

\[ h((b_1, b_2, \ldots, b_m)) = (p_1)^{b_1-1}(p_2)^{b_2-1}\cdots(p_r)^{b_r-1}(p_{r+1})^{b_{r+1}-1}\cdots(p_m)^{b_m-1}. \]

This is an injection, by the unique prime factorization theorem. But in fact, \( h \) is a bijection. Thus \( \mathcal{X} \) is countable.

\textbf{Definition 2.6} A real number \( x \) in the range \([0, 1]\) is a sequence \( a_1, a_2, \ldots \) of digits, where \( x = \sum_{i=1}^{\infty} a_i/10^i \).

\textbf{Theorem 2.7} The set of real numbers in the interval \([0, 1]\) are not countable.

\textit{Proof:} Assume for the sake of contradiction that they are countable, and let \( h : \mathbb{N} \to [0, 1] \) be the bijection realizing this fact. Let \( \alpha_i \) be the \( i \)-th digit after the period of \( h(i) \) (i.e., if \( h(2) = 0.234 \), then \( \alpha_2 = 3 \)). Finally, let \( U : \{0, 1, \ldots, 9\} \to \{0, 1\} \), where \( U(0) = 1 \), and \( U(i) = 0 \), for \( i = 1, \ldots, 9 \).

Consider the sequence \( \beta_i = U(\alpha_i) \), for \( i \geq 0 \). Observe that \( \beta_i \neq \alpha_i \) for all \( i \in \mathbb{N} \). Consider the real number \( y = \sum_{i \in \mathbb{N}} \beta_i/10^i \). Clearly, \( y \) is a real number in the interval \([0, 1]\).

We claim, however, that there is no \( i \) such that \( h(i) = y \). This would contradict the fact that \( h \) is onto. Indeed, let assume that there exists \( k \), such that \( h(k) = y \). Note that the \( k \)-th digit of \( y \) is \( \beta_k \). On the other hand, the \( k \)-th digit of \( h(k) \) is \( \alpha_k \). But we know that \( \beta_k \neq \alpha_k \). As such, \( h(k) \) and \( y \) can not be equal. A contradiction.

The above ingenious proof is due to Cantor\footnote{Georg Ferdinand Ludwig Philipp Cantor Born: 3 March 1845 in St Petersburg, Russia Died: 6 Jan 1918 in Halle, Germany} it is a clever \textit{diagonalization} argument. Indeed, write the numbers explicitly in a table.
\[ h(1) = | 0 \ 1 \ 2 \ 3 \ 4 \ 2 \ 1 \]
\[ h(2) = | 0 \ 7 \ 4 \ 4 \ 2 \ 7 \ 9 \]
\[ h(3) = | 0 \ 3 \ 3 \ 0 \ 3 \ 1 \ 5 \]
\[ h(4) = | 0 \ 5 \ 2 \ 9 \ 4 \ 9 \]
\[ h(5) = | 0 \ 6 \ 1 \ 6 \ 5 \ 9 \ 1 \]

\[ \vdots \]  

In this case, \( \alpha_1 = 1, \alpha_2 = 4, \alpha_3 = 0, \alpha_4 = 9 \) and \( \alpha_5 = 9 \). This represents the number 0.14099... Next, we “mixed” the digits and got the number \( y = \sum_i \beta_i / 10^i = 0.00100... \). The important thing is that \( y \) can not appear as a row in the above infinite matrix, because it would disagree on what should be written in the diagonal digit.

We thus conclude, that the “number” (or more precisely the cardinality) of real numbers is much bigger than the number of natural numbers. We denote this infinite cardinality by \( \aleph \). Formally, \( |\mathbb{R}| = |[0, 1]| = \aleph \).

**Exercise 2.8** Prove that \( (0, 1] \) has the same cardinality as \([0, 1]\).

**Exercise 2.9** Prove that \((0, 1)\) has the same cardinality as \((0, 1]\).

**Exercise 2.10** Prove that \((-1, 1) \setminus \{0\}\) has the same cardinality as \((0, 1]\).

**Exercise 2.11** Prove that \(\mathbb{R} \setminus \{0\}\) has the same cardinality as \((-1, 1) \setminus \{0\}\).

**Exercise 2.12** Prove that \(\mathbb{R} \setminus \{0\}\) has the same cardinality as \(\mathbb{R}\).

**Exercise 2.13** Prove that \(\mathbb{R}\) has the same cardinality as \([0, 1]\).

### 3 Applications for theory of computations

**Claim 3.1** Let \( \Sigma \) be a finite alphabet. The set \( \Sigma^* \) is countable.

**Proof:** We can consider the alphabet in \( \Sigma \) to be the numbers 1, \ldots, |\Sigma|. Thus, given a word \( w = a_1 a_2 \ldots a_k \in \Sigma^* \), we can interpret it as the number \( f(w) = \sum_{i=1}^{k} a_i |\Sigma|^i \). Clearly, \( f \) is a bijection into the natural numbers. 

**Claim 3.2** Let \( \mathcal{L} = \{ L \mid L \subseteq \Sigma^* \} \) be the set of all languages. Then, \( |\mathcal{L}| = \aleph \).

**Proof:** Let \( X \) be the set of all binary sequences. Clearly, given a sequence \( \langle a_i \rangle \in X \), it corresponds to the language \( \alpha(\langle a_i \rangle) = \{ w_i \mid a_i = 1, i \geq 0 \} \), where \( w_i \) is the \( i \)th word in \( \Sigma^* \). (More formally, \( \Sigma^* \) is countable, and let \( f : \mathbb{N} \to \Sigma^* \) be a bijection. Then \( w_i = f(i) \).

Thus, \( \alpha : X \to \mathcal{L} \) is a bijection. However, consider the mapping \( \beta : X \to [0, 1] \), which maps \( \langle a_i \rangle \) to the real number \( \sum_{i=1}^{\infty} a_i / 2^i \). Clearly, this is a bijection. Thus \( |\mathbb{R}| = |[0, 1]| = |X| = |\mathcal{L}|. \)

3
A Turing machine, can always be encoded as a large integer number. For a Turing machine $M$, we consider its encoding to be $\langle M \rangle$. Consider the set $L_M = \{ \langle M \rangle \mid M \text{ is a valid turing machine} \}$. Clearly, $L_M$ is countable. Every machine in $L_M$ recognizes at most one language in $L$. However, $L$ is uncountable. It follows:

**Theorem 3.3** There exists a language $L$, that no Turing machine accepts.

But are there any natural languages that on Turing machine can accept?