ICCS310: Assignment 4

Possawat Sanorkam
possawat2017@hotmail.com
February 24, 2021

1: Eh? They Have The Same Cardinality?

Prove the following statements using rigorous mathematical reasoning:

(1) $|[0, \frac{1}{2})| = |[0, 1)|$

Proof: We want to show that $|[0, \frac{1}{2})| = |[0, 1)|$ by direct proof. By definition, let A and B be sets. Say A and B have the same cardinality (size), denoted by $|A| = |B|$, if there exists a bijection between them.

We want to show that there exist a function f such that f is a bijection. Let $f : A \to B$, $A = [0, \frac{1}{2})$, and $B = [0, 1)$. Then, let $f(x) = 2x$. Let $a \in A$ and $a' \in A$. From observation, $f(a)$ is unique for any arbitrary a. We have that $(\forall a \neq a')[f(a) \neq f(a')]$, so f is injective. Let $b \in B$. From observation, every b can be obtain from some $f(a)$. We have that $(\forall b)(\exists a)[f(a) = b]$, so f is also surjective. According to the definition we stated before, f is a bijective function. Hence, $|A| = |B|$. Therefore, $|[0, \frac{1}{2})| = |[0, 1)|$. $\square$

(2) $|[0, 1)| = |(-1, 1)|$

Proof: We want to show that $|[0, 1)| = |(-1, 1)|$ by direct proof. By definition, let A and B be sets. Say A and B have the same cardinality (size), denoted by $|A| = |B|$, if there exists a bijection between them. In addition, $|A| = |B|$ if and only if $|A| \leq |B|$ and $|B| \leq |A|$.

We want to show that there exist functions f that is injective and g that is also injective. Let $f : A \to B$, $g : B \to A$, $A = [0, 1)$, and $B = (-1, 1)$. Then, let $f(x) = x$. Let $a \in A$ and $a' \in A$. From observation, $f(a)$ is unique for any arbitrary a. We have that $(\forall a \neq a')[f(a) \neq f(a')]$, so f is injective. Then, let $g(x) = \frac{(x+1)}{2}$. Let $b \in B$ and $b' \in B$. From observation, $g(b)$ is unique for any arbitrary b. We have that $(\forall b \neq b')[f(b) \neq f(b')]$, so g is injective. Hence, $|A| \leq |B|$ and $|B| \leq |A|$ which implies that $|A| = |B|$. Therefore, $|[0, 1)| = |(-1, 1)|$. $\square$

(3) $|[0, 1)| = |\mathbb{R}|$

Proof: We want to show that $|[0, 1)| = |\mathbb{R}|$ by direct proof. Besides, we have that $|[0, 1)| = |(-1, 1)|$ which means we can show that $|\mathbb{R}| = |(-1, 1)|$ instead. Say A and B have the same cardinality (size), denoted by $|A| = |B|$, if there exists a bijection between them. In addition, $|A| = |B|$ if and only if $|A| \leq |B|$ and $|B| \leq |A|$.

We want to show that there exist a function f such that f is a bijection. Let $f : A \to \mathbb{R}$, and $A = (-1, 1)$. Then, let $f(x) = \frac{x}{1-x^2}$. This function is continuous on domain A when $x \neq 1$ and $x \neq -1$. Let $a \in A$ and $a' \in A$. From observation, $f(a)$ is unique for any arbitrary a. We have that $(\forall a \neq a')[f(a) \neq f(a')]$, so f is injective. Let $b \in B$. From observation, every b can be obtain from some $f(a)$. We have that $(\forall b)(\exists a)[f(a) = b]$, so f is also surjective. According to the definition we stated before, f is a bijective function. So, $|A| = |\mathbb{R}|$ or $|\mathbb{R}| = |(-1, 1)|$. Hence, $|\mathbb{R}| = |(-1, 1)|$ implies that $|\mathbb{R}| = |[0, 1)|$ also. Therefore, $|[0, 1)| = |\mathbb{R}|$. $\square$

2: The Power Set of A

---

(1) Prove that $|2^A| = |\{0,1\}^A|$.

Proof:

(2) Prove that $|A| < |\{0,1\}^A|$ and conclude that $|A| < |2^A|$.

Proof:

3: Hamming Code

Consider applying the Hamming coding scheme to send 8 bits of data. This will require 4 parity bits, so an encoded code word in this scheme is 12 bits long.

(1) If the data bits are $d_1, d_2, d_3 ... d_8$, what is β_2 in terms of d_i's?

Solution: $\beta_2 = d_1 \oplus d_3 \oplus d_4 \oplus d_6 \oplus d_7$

(2) Encode the following 8-bit data: 01101010.

Solution: Hamming Code = $(\beta_1\beta_2 d_1\beta_4 d_2 d_3 d_4\beta_8 d_5 d_6 d_7 d_8)$

Encode 01101010 by adding the parity bits as followed

$$\begin{aligned}
\beta_1 = d_1 \oplus d_2 \oplus d_4 \oplus d_5 \oplus d_7 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 &= 1 && (1)\\
\beta_2 = d_1 \oplus d_3 \oplus d_4 \oplus d_6 \oplus d_7 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 &= 0 && (2)\\
\beta_4 = d_2 \oplus d_3 \oplus d_4 \oplus d_8 = 1 \oplus 1 \oplus 0 \oplus 0 &= 0 && (3)\\
\beta_8 = d_5 \oplus d_6 \oplus d_7 \oplus d_8 = 1 \oplus 0 \oplus 1 \oplus 0 &= 0 && (4)
\end{aligned}$$

Therefore, encoded bits are 100011001010

(3) Assuming that at most a single single bit flip, decide the following codewords (indicate also whether there was any error):

Solution: Hamming Code = $(\beta_1\beta_2 d_1\beta_4 d_2 d_3 d_4\beta_8 d_5 d_6 d_7 d_8)$

(i) 010011111000

So, $\beta_1 = 0, \beta_2 = 1, \beta_4 = 0$,and $\beta_8 = 1$.

$$\begin{aligned}
\beta_1 \oplus d_1 \oplus d_2 \oplus d_4 \oplus d_5 \oplus d_7 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 &= 1 && (5)\\
\beta_2 \oplus d_1 \oplus d_3 \oplus d_4 \oplus d_6 \oplus d_7 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 &= 1 && (6)\\
\beta_4 \oplus d_2 \oplus d_3 \oplus d_4 \oplus d_8 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 &= 1 && (7)\\
\beta_8 \oplus d_5 \oplus d_6 \oplus d_7 \oplus d_8 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 &= 0 && (8)
\end{aligned}$$

Error Position is $0111_2 = 7$. Corrected Data is 010011011000.

(ii) 011101010010

So, $\beta_1 = 0, \beta_2 = 1, \beta_4 = 1$,and $\beta_8 = 1$.

$$\begin{aligned}
\beta_1 \oplus d_1 \oplus d_2 \oplus d_4 \oplus d_5 \oplus d_7 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 &= 1 && (9)\\
\beta_2 \oplus d_1 \oplus d_3 \oplus d_4 \oplus d_6 \oplus d_7 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 &= 1 && (10)\\
\beta_4 \oplus d_2 \oplus d_3 \oplus d_4 \oplus d_8 = 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 &= 0 && (11)\\
\beta_8 \oplus d_5 \oplus d_6 \oplus d_7 \oplus d_8 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 &= 0 && (12)
\end{aligned}$$

Possawat Sanorkam
possawat2017@hotmail.com

Error Position is $0011_2 = 3$. Corrected Data is 010101010010.

4: Same Number of 0s and 1s

Consider the language $L = \{w \in \{0,1\}^* |$ w contains an equal number of 0s and 1s $\}$. Show that L is (Turing) decidable by providing a TM that decides it (a medium-level detail is preferred).

Proof:

5: Infinite DFA

Show that the following language is (Turing) decideable:

$$\text{IDFA} = \{\langle M \rangle | \text{ M is a DFA and L(M) is an infinite language } \}.$$

Proof: We want to show that IDFA is decidable. So, we will construct a TM T that decides IDFA. For all DFAs M, we want $T(\langle M \rangle)$ to accepts if $L(M)$ is infinite language, else it will reject.

6: Lucky 9

(1) Let $L_1 \subseteq \Sigma^*$ be defined as

$$L_1 = \begin{cases} \varnothing & \text{if } 2^{74207281} - 1 \text{ is prime} \\ \{99\} & \text{if } 2^{74207281} - 1 \text{ is not prime} \end{cases}$$

Prove that L_1 is (Turing) decidable.

Proof:

(2) Let $L_2 \subseteq \Sigma^*$ be defined as

$w \in L_2 \iff w$ appears somewhere (not necessarily consecutively) in the decimal expansion of π

Prove that L_2 is (Turing) decidable.

Proof:

7: β-reduction

(1)

Solution:

(2)

Solution:

8: Fibonacci

Possawat Sanorkam
possawat2017@hotmail.com

Using the functions we have developed (e.g., pred, if_then_else, mult, add, etc.), write down an explicit λ-term fib such that $\overline{fib}\ \overline{n} =_\beta \overline{f(n)}$.

Solution:

9: Power Of 2

Implement a λ-term for the $pow(n) = 2^n$

Solution: