

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 $f : A \rightarrow B$, $A = [0, \frac{1}{2})$, 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 $f : A \rightarrow B$, $g : B \rightarrow A$, $A = [0, 1)$, 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 $(\forall b \neq b')[g(b) \neq g(b')]$, 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 $|A| = |C|$, we have $|B| = |C|$ also.

We want to show that there exist a function f such that f is a bijection. Let $f : A \rightarrow \mathbb{R}$, 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 $f(a)$. The upper bound of $f(x)$ is $\lim_{x \rightarrow 1} f(x) \approx \infty$ and the lower bound of $f(x)$ is $\lim_{x \rightarrow -1} f(x) \approx -\infty$. So, we can cover all element in \mathbb{R} . 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: We want to show that $|2^A| = |\{0, 1\}^A|$ by direct proof. Say K and B have the same cardinality (size), denoted by $|K| = |B|$, if there exists a bijection between them. In addition, $|K| = |B|$ if and only if $|K| \leq |B|$ and $|B| \leq |K|$.

We want to show that there exist a function f such that f is a bijection. Let $f : K \rightarrow B$, $g_k : A \rightarrow \{0, 1\}$, $K = 2^A$, $a \in A$, $k \in K$ and $B = \{0, 1\}^A$. Then, let

$f(x) =$ binary array of length $|A|$ where each bit represents the presence of a in x

Besides, we say that binary array is just a tuple of $g_k(x)$.

$$f(x) = (g_k(x) | k \in A)$$

Also, let

$$g_k(x) = \begin{cases} 1 & \text{if } k \in x \\ 0 & \text{if } k \notin x \end{cases}$$

So, we have a function that map a set a and represents it in a tuple of bits like $(1, 0, \dots)$ of length $|A|$. Let $i \in K$ and $i' \in K$. From observation, $f(i)$ is unique for any arbitrary i . Besides, we can map all the permutation of binary string to each set. We have that $(\forall i \neq i')[f(i) \neq f(i')]$, so f is injective. Let $b \in B$. From observation, every b can be obtain from some $f(a)$. The upper bound of $f(x)$ is $f(A) = (1, 1, \dots, 1)$ which is a tuple of 1s with length of $|A|$ and the lower bound of $f(x)$ is $f(\emptyset) = (0, 0, \dots, 0)$ which is a tuple of 0s with length of $|A|$. So, we can cover all element in B . 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, $|A| = |B|$. Therefore, $|2^A| = |\{0, 1\}^A|$. \square .

(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 $d_1, d_2, d_3, \dots, d_8$, what is β_2 in terms of d_i 's?

Solution: $\beta_2 = p_2 \oplus d_1 \oplus d_3 \oplus d_4 \oplus d_6 \oplus d_7$

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

Solution: Hamming Code = $(p_1 p_2 d_1 p_4 d_2 d_3 d_4 p_8 d_5 d_6 d_7 d_8)$

Encode 01101010 by adding the parity bits as followed

$$p_1 = d_1 \oplus d_2 \oplus d_4 \oplus d_5 \oplus d_7 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 1 \quad (1)$$

$$p_2 = d_1 \oplus d_3 \oplus d_4 \oplus d_6 \oplus d_7 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 0 \quad (2)$$

$$p_4 = d_2 \oplus d_3 \oplus d_4 \oplus d_8 = 1 \oplus 1 \oplus 0 \oplus 0 = 0 \quad (3)$$

$$p_8 = d_5 \oplus d_6 \oplus d_7 \oplus d_8 = 1 \oplus 0 \oplus 1 \oplus 0 = 0 \quad (4)$$

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 = $(p_1p_2d_1p_4d_2d_3d_4p_8d_5d_6d_7d_8)$

(i) 010011111000

So, $p_1 = 0, p_2 = 1, p_4 = 0$, and $p_8 = 1$.

$$\beta_1 = p_1 \oplus d_1 \oplus d_2 \oplus d_4 \oplus d_5 \oplus d_7 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 1 \quad (5)$$

$$\beta_2 = p_2 \oplus d_1 \oplus d_3 \oplus d_4 \oplus d_6 \oplus d_7 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 = 1 \quad (6)$$

$$\beta_4 = p_4 \oplus d_2 \oplus d_3 \oplus d_4 \oplus d_8 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 1 \quad (7)$$

$$\beta_8 = p_8 \oplus d_5 \oplus d_6 \oplus d_7 \oplus d_8 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0 \quad (8)$$

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

(ii) 011101010010

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

$$\beta_1 = p_1 \oplus d_1 \oplus d_2 \oplus d_4 \oplus d_5 \oplus d_7 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 = 0 \quad (9)$$

$$\beta_2 = p_2 \oplus d_1 \oplus d_3 \oplus d_4 \oplus d_6 \oplus d_7 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 0 \quad (10)$$

$$\beta_4 = p_4 \oplus d_2 \oplus d_3 \oplus d_4 \oplus d_8 = 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0 \quad (11)$$

$$\beta_8 = p_8 \oplus d_5 \oplus d_6 \oplus d_7 \oplus d_8 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0 \quad (12)$$

Data is already correct.

4: Same Number of 0s and 1s

Consider the language $L = \{w \in \{0,1\}^* \mid w \text{ contains an equal number of 0s and 1s}\}$. 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) decidable:

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

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 accept if $L(M)$ is infinite language, else it will reject.

6: Lucky 9

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

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

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) $(\lambda z.z)(\lambda z.zz)(\lambda z.zy)$

Solution:

$$(\lambda z.z)(\lambda z.zz)(\lambda z.zy) \rightarrow_1 (\lambda z.zz)(\lambda z.zy) \quad (13)$$

$$\rightarrow_1 (\lambda z.zy)(\lambda z.zy) \quad (14)$$

$$\rightarrow_1 (\lambda z.zy)y \quad (15)$$

$$\rightarrow_1 yy \quad (16)$$

(2) $(((\lambda x.\lambda y.(xy))(\lambda y.y))w)$

Solution:

$$(((\lambda x.\lambda y.(xy))(\lambda y.y))w) \rightarrow_1 (((\lambda x.\lambda y.(xy))(\lambda y'.y'))w) \quad (17)$$

$$\rightarrow_1 (\lambda y.((\lambda y'.y')y)w) \quad (18)$$

$$\rightarrow_1 (\lambda y.(y)w) \quad (19)$$

$$\rightarrow_1 w \quad (20)$$

8: Fibonacci

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

Solution: Let `fib`(n) = `plain_fib`(`fib`, n) for all n

Define $T = \lambda zw.z$

We say `iszero` is a function that return T if the input is zero, else F .

Define `iszero` := $\lambda nxy.n(\lambda z.y)x$

Define `or` := $\lambda xy.x(T)(y)$

Define `plain_fib` := $\lambda f n. \text{if_then_else}(\text{or}(\text{iszero } n)(\text{iszero } (\text{pred } n)))(\bar{1})$
 $(\text{add}(f \text{ pred } n)(f \text{ pred } (\text{pred } n)))$

$$\overline{\text{fib}} \bar{n} \rightarrow_* (\text{plain_fib } \overline{\text{fib}}) \bar{n} \quad (21)$$

$$\rightarrow_* \text{if_then_else}(\text{or}(\text{iszero } \bar{n})(\text{iszero } (\text{pred } \bar{n}))) \quad (22)$$

$$(\bar{1})(\text{add}(\overline{\text{fib}} \text{ pred } \bar{n})(\overline{\text{fib}} \text{ pred } (\text{pred } \bar{n})))$$

Therefore,

$$\overline{\text{fib}} \bar{n} = \text{if_then_else}(\text{or}(\text{iszero } \bar{n})(\text{iszero } (\text{pred } \bar{n}))) (\bar{1})(\text{add}(\overline{\text{fib}} \text{ pred } \bar{n})(\overline{\text{fib}} \text{ pred } (\text{pred } \bar{n})))$$

9: Power Of 2

Implement a λ -term for the $\text{pow}(n) = 2^n$

Solution: $\overline{\text{pow}} \bar{n} = (\text{pow } \bar{n}) \bar{2} = ((\lambda pq. pq) \bar{n}) \bar{2}$

Substitute all church numerals, we get $\overline{\text{pow}} \bar{n} =$

$$((\lambda pq. pq) \lambda f x. f^n x) \lambda f x. f(f x)$$