Pinter Chapters 2-4

Owen Wang

2.D. Automata: The Algebra of Input/Output Sequences

1. Concatenation of input sequences is associative. We start by fixing some arbitrary $\boldsymbol{a}$ and $\boldsymbol{b}$, and aim to show that:

   $$(\boldsymbol{ab})\boldsymbol{c} = \boldsymbol{a}(\boldsymbol{bc})$$

   For the base case where $\boldsymbol{c} = \lambda$,

   $$(\boldsymbol{ab})\lambda = \boldsymbol{ab} = \boldsymbol{a}(\boldsymbol{b}\lambda)$$

   Then, if $\boldsymbol{c}$ is a non-empty sequence, then it may be broken down into the subsequence $\boldsymbol{c} = \boldsymbol{d}a$ where $a \in A$.

   $$\begin{aligned}
   (\boldsymbol{ab})\boldsymbol{c} &= (\boldsymbol{ab})(\boldsymbol{d}a) \\
   &= ((\boldsymbol{ab})\boldsymbol{d})a && \text{Def. of concatenation} \\
   &= (\boldsymbol{a}(\boldsymbol{bd}))a && \text{Inductive hypothesis} \\
   &= (\boldsymbol{a}(\boldsymbol{b}(\boldsymbol{d}a))) && \text{Def. of concatenation} \\
   &= (\boldsymbol{a}(\boldsymbol{bc}))
   \end{aligned}$$

2. Concatenation is not commutative. Order explicitly matters in the definition of concatenation. As a brief example, let $A = \{0, 1\}$ and then let $\boldsymbol{a} = 1$ and $\boldsymbol{b} = 0$. Then,

   $$\boldsymbol{ab} = a_1 b_1 = 10 \neq 01 = b_1 a_1 = \boldsymbol{ba}$$

3. To show that there is an identity element, let $\boldsymbol{e} = \lambda$. Then, for any arbitrary $\boldsymbol{a}$,

   $$\begin{aligned}
   \boldsymbol{ae} &= a_1 ... a_n = \boldsymbol{a} \\
   \boldsymbol{ea} &= a_1 ... a_n = \boldsymbol{a}
   \end{aligned}$$

   Thus, λ is the identity element.

3.G. Maximum-Likelihood Decoding

1.

codeword	a_4	$a_1 + a_3$	a_5	$a_1 + a_2 + a_3$
00000	0	$0 + 0 = 0$	0	$0 + 0 + 0 = 0$
00111	1	$0 + 1 = 1$	1	$0 + 0 + 1 = 1$
01001	0	$0 + 0 = 0$	1	$0 + 1 + 0 = 1$
01110	1	$0 + 1 = 1$	0	$0 + 1 + 1 = 0$
10011	1	$1 + 0 = 1$	1	$1 + 0 + 0 = 1$
10100	0	$1 + 1 = 0$	0	$1 + 0 + 1 = 0$
11010	1	$1 + 0 = 1$	0	$1 + 1 + 0 = 0$
11101	0	$1 + 1 = 0$	1	$1 + 1 + 1 = 1$

2. a. 000000, 001001, 010111, 011110, 100011, 101010, 110100, 111101

   b. 2

   c. A single error can be detected. Because the minimum distance between any two codewords is 2 and the distance between a codeword and a codeword with a single error is 1, a codeword with a single error will never be recognized as a different codeword.

3. Let $a_3 = a_1, a_4 = a_1 + a_2 + a_3$.

   a. 0000, 0110, 1010, 1111

   b. The minimum distance between any two codewords is 2.

4.

word	codeword(s)
11111	11101
00101	00111
11000	11010
10011	10011
10001	10011
10111	10011, 00111

5. We aim to prove the contrapositive: if a codeword has m errors, it may not always be detected.

   By definition of m, there must exist two codewords x and y such that $d(x, y) = m$. Suppose x is transmitted and the errors occur in exactly the m positions that it differs with y. Then, the word received is y, which is another valid codeword, so it is undetectable.

6. Assume that there exists $x \in S_t(a)$ and $x \in S_t(b)$ such that $a \neq b$. Then, $d(a,x) \leq t$ and $d(b,x) \leq t$. Then, because the distance function satisfies the triangle inequality, $d(a,b) \leq d(a,x) + d(b,x)$. Thus,

$$d(a,b) \leq d(a,x) + d(b,x) \leq 2t = m - 1$$

However, this leads to a contradiction, as m is defined to be the minimum distance between two codewords.

7. Part 6 indicates that $\forall a : \forall b : (a \neq b) \rightarrow (S_t(a) \perp S_t(b))$, as it is true for any arbitrary a, b. Then, a word with less than t errors can be decoded by finding the unique sphere of radius t that it is contained in.

8. The textbook is incorrect in its claim. However, as $m = 2$, a single error may be detected.

4.A. Solving Equations in Groups

1. $axb = c$

$$\begin{aligned} xb &= a^{-1}c && \text{left multiplication by } a^{-1} \\ x &= a^{-1}cb^{-1} && \text{right multiplication by } b^{-1} \end{aligned}$$

2. $x^2b = xa^{-1}c$

$$\begin{aligned} xb &= a^{-1}c && \text{left multiplication by } x^{-1} \\ x &= a^{-1}cb^{-1} && \text{right multiplication by } b^{-1} \end{aligned}$$

3. It is given that $x^2a = bxc^{-1}$ and $acx = xac$.

$$\begin{aligned} x^2ac &= bx && \text{right multiplication by } c \\ xacx &= bx && \text{substitute equation 2} \\ xac &= b && \text{right multiplication by } x^{-1} \\ xa &= bc^{-1} && \text{right multiplication by } c^{-1} \\ x &= bc^{-1}a^{-1} && \text{right multiplication by } a^{-1} \end{aligned}$$

4. It is given that $ax^2 = b$ and $x^3 = e$.

$$\begin{aligned} x^2 &= a^{-1}b && \text{left multiplication by } a^{-1} \\ x^3 &= xa^{-1}b && \text{left multiplication by } x \end{aligned}$$

By the second equation, $x^3xa^{-1}b = e$. Thus,

$$\begin{aligned} xa^{-1}b &= e \\ xa^{-1} &= b^{-1} && \text{right multiplication by } b^{-1} \\ x &= b^{-1}a && \text{right multiplication by } a \end{aligned}$$

5. It is given that $x^2 = a^2$ and $x^5 = e$.

$$\begin{aligned} x^4 &= a^4 && \text{squaring} \\ x^5 &= xa^4 && \text{left multiplication by } x \end{aligned}$$

By the second equation,

$$\begin{aligned} xa^4 &= e \\ x &= a^{-4} && \text{right multiplication by } a^{-4} \end{aligned}$$

6. It is given that $(xax)^3 = bx$ and $x^2a = (xa)^{-1}$.

$$xax^2ax^2ax = bx$$

Then, substituting using equation 2,

$$
\begin{aligned}
xa(xa)^{-1}(xa)^{-1}x &= bx \\
xaa^{-1}x^{-1}a^{-1}x^{-1}x &= bx \\
xx^{-1}a^{-1} &= bx \\
a^{-1} &= bx \\
x &= b^{-1}a^{-1}
\end{aligned}
$$