Boolean Product

Wednesday, March 9, 2022 12:44 PM

Recall: relation representation
- matrix
- digraphs

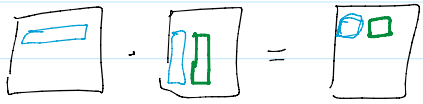
Missing: on Quiz 2

1] Matrix for composition of $R_1 \circ R_2$

Given M_1 for R_1 and M_2 for R_2

Then M_3 for $R_1 \circ R_2$ is computed by:

$$M_3 = M_2 \odot M_1$$

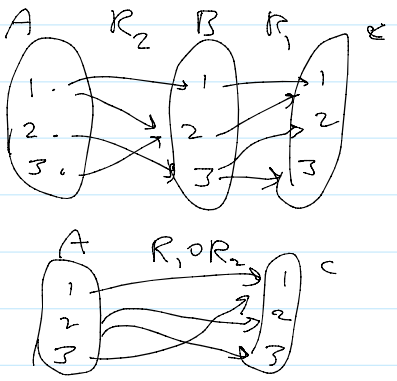


Note: $1+0+1+1 = 3 \longrightarrow 1$

e.g.

$$M_3 = M_1 \odot M_2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

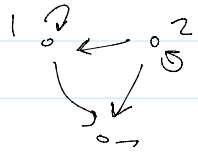


$$M_3 = M_2 \odot M_2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

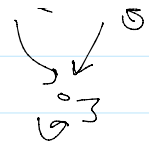
2] Matrix for R^n

$$M_{R^n} = [M_R]^n$$

e.g. $M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$



e.g. $M_R = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$



$$M_R^2 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

End of §9.3

Review

Quiz #1.

Q1. $-13 = (-3) \cdot 5 + 2$

$q = -3$, $r = 2$

Q2.
$$\begin{array}{r} {\scriptstyle 1} \\ 422 \\ 431 \\ \hline 1403 \end{array}$$

Q3.

$$(3926\,02 \times 25989 + 3941^2) \equiv 2 \cdot (-11) + 2^2 \equiv 2 \cdot 2 + 4 \equiv 8 \pmod{13}$$

(26000 − 11), 2^2

13, 26, 39, 52, 65

HW 3

#24. RSA A–Z → 0–25 (mod 26)

ATTACK

n = 2537

00 19, 19 00, 02 10

0 1 2 3 ... 10 ... 19 ... 25

a b c e f g h i j k l m n o p q r s t a v w x y z

key = (e = 13, n = 2537) →

$(0019^{13} \bmod 2537)$

$d = e^{-1} \pmod{\phi(n)}$

n = 77

$\phi(n) = 8 \cdot 10 = 60$

e = 11

$d = 11^{-1} \pmod{60}$

Quiz 2

#1.

$x_1 = 6$

$x_2 = 9$

#2.

$3^{50} \bmod 23$

$\equiv 3^6$ by F.L.T.

$\equiv (3^3)^2 \equiv (4)^2 \equiv 16 \pmod{23}$

F.L.T.

$a^{p-1} \equiv 1 \pmod p$

$a^{50} \equiv (a^{22})^2 \cdot a^6$

$\equiv 1^2 \cdot a^6$

#3.

$C = M^e \pmod n$

$$C = M^{e} \pmod{n}$$

$$\equiv 4^{3} \pmod{33}$$

$$\equiv 64$$

$$\equiv -2 \equiv 31 \pmod{33}$$