תרגיל בית 5

שאלה 1

$n=17$, $d=5$

$g(x) = x^8+x^3+x^6+x^4+x^2+x+1$

ניתן לתקן 2 שגיאות.

$e_1(x) = x^i$

$e_2(x) = x^i + x^j$

- ישנן 17 אפשרויות לשגיאה אחת - כולן הנגה דיקלית של x^i - לכן נבחר $e_1(x) = x^{16}$.
- ישנן $\binom{17}{2} = 136$ אפשרויות לשתי שגיאות, ושוב ישנן 16 אפשרויות לשתי שגיאות הנגמרות שאחת מהן ב-x^{16} כלומר $x^{16}+x^{16+i}$ כאשר $i=\pm1\dots\pm8$ (התקה דו mod)

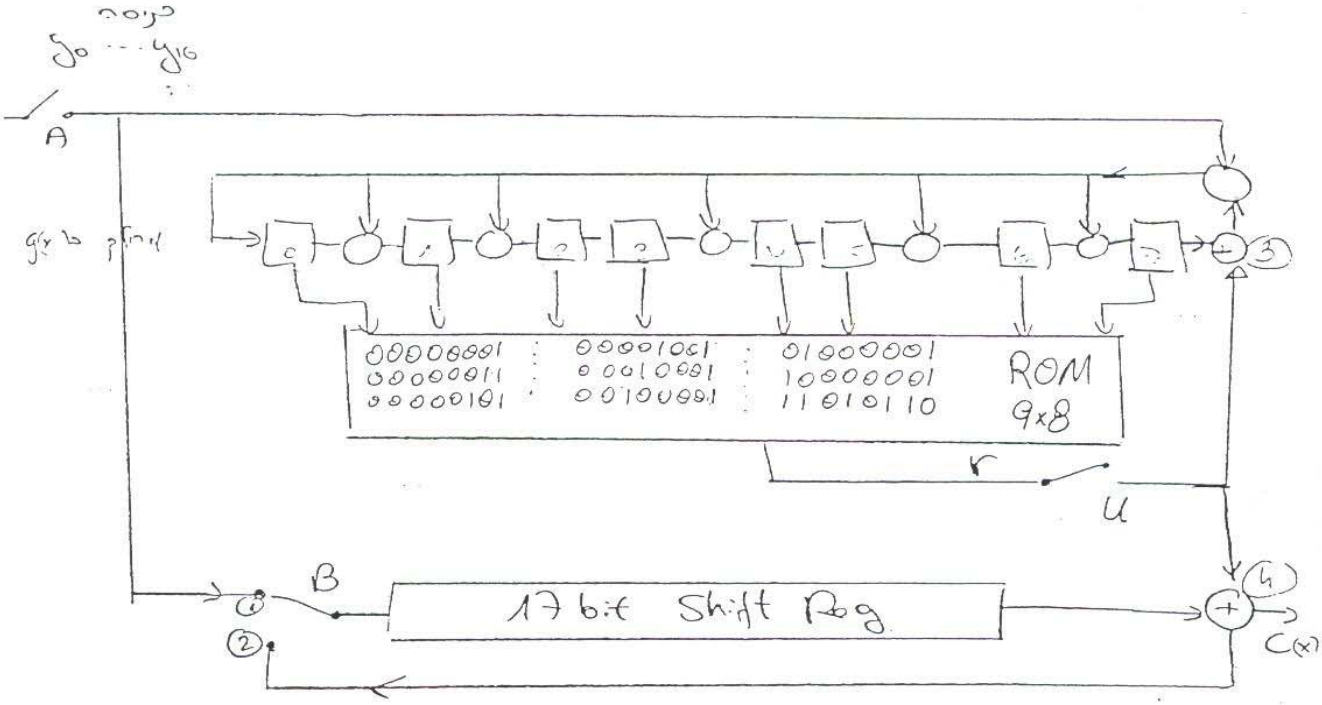
לעומת זה $x^{16}+x^{16-i}$ הינו הנגה דיקלית ב i של השגיאה $x^{16}+x^{16-i}$ לכן ישנן רק 16/2 אפשרויות (לשתי שגיאות) שאינן הנגות דיקליות.
בכך שנניח להקטין אותם בעזרת ה RAM (אך נמיר שלוש בעזרת סנכרון ו"לעבר כפל" ב shift-register)

- נשתמש בהנחה איזו כדי לקבל תיקון נאות כלומר הכפלה של השגיאה ב x^8:
ה RAM יכלל אות הטבלה הבאה

שגיאה	סנדרום	הצגה בינארית של הסינדרום
x^{16}	x^7	0 0 0 0 0 0 0 1
$x^{16}+x^{15}$	x^7+x^6	0 0 0 0 0 0 1 1
$x^{16}+x^{14}$	x^7+x^5	0 0 0 0 0 1 0 1
⋮		
$x^{16}+x^9$	x^7+x^0	1 0 0 0 0 0 0 1
$x^{16}+x^8$	$x^6+x^5+x^3+x+1$	1 1 0 1 0 1 1 0

*

$R_{gen}(x^8\cdot(x^{16}+x^8)) = x^6+x^5+x^3+x+1$



שלבי הפעולה: (המחלק מתחיל כשהוא מלא אפסים וכן גם ה shift reg)

בשלב 17 הראשונים: A סגור, B מחובר ל (1), מפסק u פועל
מתבצע החילוק של $x^8y(x)$ ב $g(x)$
ומתמלא shift reg בוקטור הקבלה

בשלב 34 אחרונים: A פתוח, B מחובר ל (2), מפסק u סגור
מתבצע חישוב הסינדרום בהנחה שקבלו את
כמילת הקוד המשודרת, הקו מוזן לתא ה"א
ומתבצע תיקון הסינדרום ותיקון הביט
המשובש. (מסלולים (3) ו (4))
הקוד shift reg מוכן בוקטור שגיאה תיקון

הוקטור המתקן יושב במחלק לה בשלב האחרון של
הפעולה. מחסרים 4.

ב) נקודה המלה:

$$y(x) = g(x)(x^4+x^4) + x + x^{16} = x^{16} + x^{14} + x^{13} + x^{11} + x^7 + x^5 + x^4 + x$$

מס'	כניסה	r_{Ram}	מלק	shift register	מוצא
אתחול			00000000	00000000000000000	
1)	1		11101011	10000000000000000	
2)	0		10011110	01000000000000000	
3)	1		10100100	10100000000000000	
4)	1		10111001	11010000000000000	
5)	0		10110111	01101000000000000	
6)	1		01011011	10110100000000000	
7)	0		11000110	01011010000000000	
8)	0		01100011	00101101000000000	
9)	0		11011010	00010110100000000	
10)	1		10000110	10001011010000000	
11)	0		01000011	01000101101000000	
12)	1		00100001	10100010110100000	
13)	1		00010000	11010001011010000	
14)	0		00001000	01101000101101000	
15)	0		00000100	00110100010110100	
16)	1		11101001	10011010001011010	
17)	0		10011111	01001101000101101	
18)		0	10100100	10100110100010110	
19)		0	01010010	01010011010001011	
20)		0	00101001	10101001101000101	
21)		0	11111111	11010100110100010	
22)		0	10010100	01101010011010001	
23)		0	01001010	10110101001101000	
24)		0	00100101	01011010100110100	
25)		0	11111001	00101101010011010	
26)		0	10010111	00010110101001101	
27)		0	10100000	10001011010100110	
28)		0	01010000	01000101101010011	
29)		0	00101000	10100010110101001	
30)		0	00010100	11010001011010100	
31)		0	00001010	01101000101101010	
32)		0	00000101	00110100010110101	
33)		1	00000010	00011010001011010	
34)		0	00000001	00001101000101101	
35)		1	00000000	00000110100010110	0
36)		0	00000000	00000011010001011	0
37)		0	00000000	10000001101000101	1
38)		0	00000000	11000000110100010	1
39)		0	00000000	01100000011010001	0
40)		0	00000000	10110000001101000	1
41)		0	00000000	01011000000110100	0
42)		0	00000000	00101100000011010	0
43)		0	00000000	00010110000001101	0
44)		0	00000000	10001011000000110	1
45)		0	00000000	01000101100000011	0
46)		0	00000000	10100010110000001	1
47)		0	00000000	11010001011000000	1
48)		0	00000000	01101000101100000	0
49)		0	00000000	00110100010110000	0
50)		0	00000000	00011010001011000	0
51)		0	00000000	00001101000101100	0

מפסק A סגור, המלה נכנסת ישירות ל shift-reg למעגל המלוקה לא מבצעים כלום מול ה Rom. בוצר מתג u פתוח.

מתג A פתוח: נכנסה המלה. מתג B על מצב 2. מתפצל מעבר סנדרום ומעבר מלה לפי הערך של הביט המוצא מה - Rom (מתג u סגור)

17 מחזורים אחרונים לא המוצא

$$c(x) = x^{14} + x^{13} + x^{11} + x^7 + x^5 + x^4$$

$$c(x) = y(x) - (x + x^{16})$$

וקבלנו במוצא את המלה ואכן מתקיים

שאלה 2

נתבונן במפענח מגיט המתקן שגיאה בודדת עם עדכון סנדרום
ואז בהקרה והיתה יותר משגיאה אחת אני לא נדע
תיקון והסנדרום הסופי יהיה שונה מ-0 לעם בעצמו
תיקון בודד אי עדכון הסנדרום יאפס את הסנדרום.
כלומר, כדי שהגלוי יעלה צריך שבדיקה הלא הסנדרום הסופי
אינו מאופס.

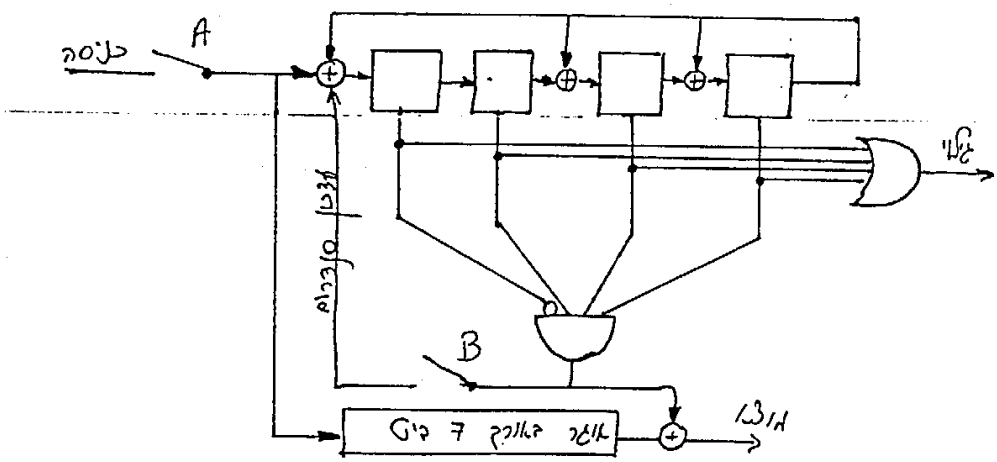
נמצא מפענח מגיט המאוחן משמעלה המתקן שגיאה בודדת:

$$g(x) = (1+x)(1+x+x^3) = x^4+x^3+x^2+1$$

השגיאות הבודדות מהצורה x^i יתקנו עי הסנדרום המתאים לשגיאה
בכוח הפולינום: $e(x)=x^6 \Leftarrow$

$$x^4 = x^3+x^2+1 \quad (\bmod g(x))$$
$$x^5 = x^4+x^3+x = x^2+x+1$$
$$x^6 = x^3+x^2+x = R_{g(x)}(x^6)$$

ואכן, המפענח:



A סיבוב ↔ 7 צעדים כאשר הגיעה לכניסה לאוגר ומאפס התקבלה.
B סיבוב ↔ 7 צעדים נוספים הביטים באוגר יוצאים ומוזרמים תיקון
(אם יש צורך) וכן מתבצע עדכון סנדרום.
בסך הכל 14 צעדים, אם ביט הגלוי דלוק אני היתה
שגיאה מרובה!

שאלה 3

$\gcd(492, 1599) = 123$

$g_0 = 1599$
$g_1 = 492$
$g_2 = 1599 \bmod 492 = 123$
$g_3 = 492 \bmod 123 = 0$

$\gcd(245, 370) = 5$

$g_0 = 370$
$g_1 = 245$
$g_2 = 370 \bmod 245 = 125$
$g_3 = 245 \bmod 125 = 120$
$g_4 = 125 \bmod 120 = 5$
$g_5 = 120 \bmod 5 = 0$