פתרון תרגיל בית - 2

שאלה מספר 1

הוכיחו את המשפטים הבאים:

א. פונקצית המרחק הינה מטריקה, היא מקיימת:

א. סימטריה $d(x,y)=d(y,x)$.

ב. אי שלילית $d(x,y)\geq 0$ ושווה ל-0 אם $x=y$.

ג. אי שוויון המשולש $d(x,y)+d(y,z)\geq d(x,z)$.

הוכחה:

יהיו $x=(x_{n-1},\dots x_0),\ y=(y_{n-1},\dots y_0),\ z=(z_{n-1},\dots z_0)$

א.

$$d(x,y)=\left|\{i\mid\ \ x_i\neq y_i,\ \ i=0\dots n-1\}\right|=\left|\{i\mid\ \ y_i\neq x_i,\ \ i=0\dots n-1\}\right|=d(y,x)$$

ב. $d(x,y)=\left|\{i\mid\ \ x_i\neq y_i,\ \ i=0\dots n-1\}\right|\geq 0$ עוצמה של קבוצה היא תמיד אי שלילית.

$$d(x,y)=\left|\{i\mid\ \ x_i\neq y_i,\ \ i=0\dots n-1\}\right|=0$$
$$\Leftrightarrow$$
$$\forall i\ :\ x_i=y_i\ \ ,i=0\dots n-1\Rightarrow x=y$$

ג. נתבונן באיבר $d(x,z)$. עבור כל $x_i\neq z_i$ לא יתכן מצב בו $x_i=y_i\ and\ y_i=z_i$

(אחרת שניהם שווים ל z_i) לכן עבור כל קידום של $d(x,z)$ אנו מקדמים גם את

$d(x,y)+d(y,z)$ בלפחות אחד. מכאן נובע כי: $d(x,y)+d(y,z)\geq d(x,z)$

ב. אם $G=(I|A)$ מטריצה יוצרת של קוד C אזי קיימת לקוד מטריצה בודקת מהצורה

$H=(-A^T|I)$.

הוכחה:

$$GH^T=(I_k|A)\begin{pmatrix}-A\\ I_{n-k}\end{pmatrix}=I_k(-A)+A(I_{n-k})=-A+A=0$$

שאלה מספר 2:

נתון כי אוסף המילים הבאות פורש קוד ליניארי מעל $GF(5)$:

$$(1,0,4,3)$$
$$(1,1,1,2)$$
$$(0,1,2,4)$$

א. מצאו פרמטרי הקוד (אורך הקוד, מימד הקוד , מספר מילות הקוד)

ב. מצאו G (מטריצה יוצרת של הקוד) האם היא יחידה? מצא G סיסטמטי

ג. תנו דוגמא לחמש מילות אינפורמציה ומילות קוד מתאימות.

ד. מצאו H (מטריצה בודקת של הקוד) האם היא יחידה?

ה. חשבו את הסינדרום של מילת הקוד $(0,1,2,4)$

ו. מצאו שלוש מילות קוד נוספות בעזרת H

ז. מהו המרחק המינימאלי של הקוד? מה מספר העמודות התלויות של H?

ח. מצאו יכולת גילוי השגיאות של הקוד ויכולת תיקון השגיאות של הקוד?

פתרון:

א. אורך הקוד הוא $n=4$. למציאת מימד הקוד נציב את מילות הקוד במטריצה, נדרג אותה ונבדוק מה מספר השורות השונות מאפס בתום הדירוג:

$$\begin{pmatrix}1&0&4&3\\1&1&1&2\\0&1&2&4\end{pmatrix}\overset{4I+II->II}{\sim}\begin{pmatrix}1&0&4&3\\0&1&2&4\\0&1&2&4\end{pmatrix}\overset{4II+III->III}{\sim}\begin{pmatrix}1&0&4&3\\0&1&2&4\\0&0&0&0\end{pmatrix}$$

בתום הדירוג קיבלנו שתי שורות השונות מאפס ולכן $k=2$.

מספר מילות הקוד בקוד ליניארי $q^k=5^2=25$.

1. $G=\begin{pmatrix}1&0&4&3\\0&1&2&4\end{pmatrix}$

שורות G מורכבות מווקטורי הבסיס הפורשים את אוסף מילות הקוד ולכן G לא יחידה.

למציאת G סיסטמטי יש לדרג את המטריצה עד לקבלת מטריצה בצורת $G=(A\,|\,I)$ או $G=(I\,|\,A)$. במקרה שלנו שני האיברים הימניים מכל שורה תלויים אחד בשני ולכן לא נוכל להגיע למטריצה מהצורה $G=(A\,|\,I)$.

המטריצה G כפי שהיא נתונה היא מהצורה $G=(I\,|\,A)$ כלומר סיסטמטית כך ש k הסימבולים הראשונים (משמאל) הם סימבולי האינפורמציה.

2. עבור מילת האינפורמציה $(m_1,m_0)=(1,0)$

$$\underbrace{(10)}_{\boldsymbol{m}}\underbrace{\begin{pmatrix}1&0&4&3\\0&1&2&4\end{pmatrix}}_{\boldsymbol{G}}=\underbrace{(1\,0\,4\,3)}_{c}$$

ובאופן דומה:

$$(\boldsymbol{m}_1,\boldsymbol{m}_0)=(1,1)\quad\Rightarrow(\boldsymbol{c}_3,\boldsymbol{c}_2,\boldsymbol{c}_1,\boldsymbol{c}_0)=(1\,1\,1\,2)$$
$$(\boldsymbol{m}_1,\boldsymbol{m}_0)=(0,4)\quad\Rightarrow(\boldsymbol{c}_3,\boldsymbol{c}_2,\boldsymbol{c}_1,\boldsymbol{c}_0)=(0\,4\,3\,1)$$
$$(\boldsymbol{m}_1,\boldsymbol{m}_0)=(0,2)\quad\Rightarrow(\boldsymbol{c}_3,\boldsymbol{c}_2,\boldsymbol{c}_1,\boldsymbol{c}_0)=(0\,2\,4\,1)$$
$$(\boldsymbol{m}_1,\boldsymbol{m}_0)=(1,2)\quad\Rightarrow(\boldsymbol{c}_3,\boldsymbol{c}_2,\boldsymbol{c}_1,\boldsymbol{c}_0)=(1\,2\,3\,1)$$

3. <u>ניעזר במשפט</u> : אם $\boldsymbol{G}=(\boldsymbol{I_k}\mid\boldsymbol{A})$ אזי קיימת מטריצה בודקת מהצורה $\boldsymbol{H}=(-\boldsymbol{A^T}\mid\boldsymbol{I_{n-k}})$

$$\boldsymbol{G}=\begin{pmatrix}1&0&4&3\\ \underbrace{0\,1}_{\boldsymbol{I_2}}&\underbrace{2\,4}_{\boldsymbol{A}}\end{pmatrix}\quad\Rightarrow\quad\boldsymbol{H}=\begin{pmatrix}-4&-2&1&0\\ \underbrace{-3\,-4}_{-\boldsymbol{A^T}}&&\underbrace{0\,1}_{\boldsymbol{I_2}}\end{pmatrix}\overset{\text{mod}5}{=}\begin{pmatrix}1&3&1&0\\2&1&0&1\end{pmatrix}$$

אם נחליף את שורות המטריצה $\boldsymbol{H}$ נקבל מטריצה בודקת נוספת ולכן אינה יחידה.

4.

$$\boldsymbol{Syndrome}=\boldsymbol{Hy^T}$$

$$\boldsymbol{S}=\begin{pmatrix}1&3&1&0\\2&1&0&1\end{pmatrix}\begin{pmatrix}0\\1\\2\\4\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$

<u>הערה</u>: סינדרום של מילת קוד שווה תמיד לאפס.

5. סינדרום של מילת קוד הוא אפס. נראה את החישוב בצורה אלגברית:

$$\boldsymbol{S}=\boldsymbol{Hy^T}\overset{*}{=}\boldsymbol{Hc^T}=\begin{pmatrix}1&3&1&0\\2&1&0&1\end{pmatrix}\begin{pmatrix}\boldsymbol{c}_3\\\boldsymbol{c}_2\\\boldsymbol{c}_1\\\boldsymbol{c}_0\end{pmatrix}=\boldsymbol{c}_3\begin{pmatrix}1\\2\end{pmatrix}+\boldsymbol{c}_2\begin{pmatrix}3\\1\end{pmatrix}+\boldsymbol{c}_1\begin{pmatrix}1\\0\end{pmatrix}+\boldsymbol{c}_0\begin{pmatrix}0\\1\end{pmatrix}=0$$

* $\boldsymbol{y}=\boldsymbol{c}+\boldsymbol{e}$ אך במילת קוד $\boldsymbol{e}=0$ ולכן $\boldsymbol{y}=\boldsymbol{c}$.

מציאת מילת קוד שקולה למציאת קומבינציה ליניארית של עמודות המטריצה $\boldsymbol{H}$ אשר תגרור $\boldsymbol{S}=0$. דוגמאות למילות קוד: $(1\,3\,0\,0),(1\,4\,2\,4),(2\,3\,4\,3)$.

6. המרחק המינימאלי בקוד ליניארי שקול גם למציאת המספר הקטן ביותר של עמודות תלויות ב-$\boldsymbol{H}$ במקרה שלנו שתי העמודות הראשונות תלויות ולכן המרחק המינימאלי הוא $\boldsymbol{d}=2$.

<u>הערה</u>: המרחק אינו יכול להיות אחד כיוון שאין עמודת אפסים במטריצת הבדיקה $\boldsymbol{H}$

שאלה מספר 3:

נתון כי אוסף המילים הבאות פורש קוד ליניארי מעל $GF(3)$:

$$(2,1,0,1)$$
$$(1,2,0,2)$$
$$(0,1,1,2)$$

1. מהו אורך הקוד?
2. מהו מימד הקוד? מה מספר מילות הקוד?
3. מצאו G (מטריצה יוצרת של הקוד) האם היא יחידה? מצא G סיסטמטי
4. תנו דוגמא למילת אינפורמציה ומילת קוד מתאימה.
5. מצאו H (מטריצה בודקת של הקוד) האם היא יחידה?
6. חשבו את הסינדרום של מילת הקוד $(0,1,1,2)$
7. מצאו מילת קוד נוספת בעזרת H
8. מהו המרחק המינימאלי של הקוד?
9. מהי יכולת גילוי השגיאות של הקוד?
10. מהי יכולת תיקון השגיאות של הקוד?
11. תכנן מעגל מקודד (צירופי) על פי מטריצה G
12. תכנן מעגל חישוב סינדרום (צירופי) לפי מטריצה H

פתרון:

1. $n = 4$
2. נציב את מילות הקוד במטריצה, נדרג אותה ונבדוק מה מספר השורות השונות מאפס בתום הדירוג:

$$\begin{pmatrix} 2101 \\ 1202 \\ 0112 \end{pmatrix} \overset{\text{I+II->II}}{\sim} \begin{pmatrix} 2101 \\ 0000 \\ 0112 \end{pmatrix} \overset{\text{II<->III}}{\sim} \begin{pmatrix} 2101 \\ 0112 \\ 0000 \end{pmatrix}$$

בתום הדירוג קיבלנו שתי שורות השונות מאפס ולכן $k = 2$.

<u>הערה:</u> ניתן היה מראש לראות כי שתי המילים הראשונות תלויות אחת בשנייה.

מספר מילות הקוד בקוד ליניארי $q^k = 3^2 = 9$.

3. $G = \begin{pmatrix} 2101 \\ 0112 \end{pmatrix}$

שורות G מורכבות מווקטורי הבסיס הפורשים את אוסף מילות הקוד ולכן G לא יחידה.

למציאת G סיסטמטי יש לדרג את המטריצה עד לקבלת מטריצה בצורת $G = (A \mid I)$:

$$\begin{pmatrix}2101\\0112\end{pmatrix}\overset{II\leftrightarrow I}{\sim}\begin{pmatrix}0112\\2101\end{pmatrix}\overset{II+I\to I}{\sim}\underbrace{\begin{pmatrix}2210\\2101\end{pmatrix}}_{systematic}$$

4. עבור מילת האינפורמציה $(\boldsymbol{m}1,\boldsymbol{m}0)=(1,2)$

$$\underbrace{(12)}_{\boldsymbol{m}}\underbrace{\begin{pmatrix}2101\\0112\end{pmatrix}}_{\boldsymbol{G}}=\underbrace{(2022)}_{c}$$

5. <u>ניעזר במשפט</u> : אם $\boldsymbol{G}=(\boldsymbol{I}\mid\boldsymbol{A})$ אזי קיימת מטריצה בודקת מהצורה $\boldsymbol{H}=(-\boldsymbol{A}^{\boldsymbol{T}}\mid\boldsymbol{I})$

ראשית נדרג את $\boldsymbol{G}$ לצורת $\boldsymbol{G}=(\boldsymbol{I}\mid\boldsymbol{A})$:

$$\boldsymbol{G}=\begin{pmatrix}2101\\0112\end{pmatrix}\overset{2*II+I\to I}{\sim}\begin{pmatrix}2022\\0112\end{pmatrix}\overset{2*I\to I}{\sim}\begin{pmatrix}1011\\0112\end{pmatrix}$$

$$\Rightarrow$$

$$\boldsymbol{H}=\begin{pmatrix}-1&-1&1&0\\-1&-2&0&1\end{pmatrix}\overset{mod3}{=}\begin{pmatrix}2210\\2101\end{pmatrix}$$

אם נחליף את שורות המטריצה $\boldsymbol{H}$ נקבל מטריצה בודקת נוספת ולכן אינה יחידה.

6.

$$\boldsymbol{Syndrome}=\boldsymbol{Hy^T}$$

$$\boldsymbol{S}=\begin{pmatrix}2210\\2101\end{pmatrix}\begin{pmatrix}0\\1\\1\\2\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$

<u>הערה</u>: סינדרום של מילת קוד שווה תמיד לאפס.

7. סינדרום של מילת קוד הוא אפס. נראה את החישוב בצורה אלגברית:

$$\boldsymbol{S}=\boldsymbol{Hy^T}\overset{*}{=}\boldsymbol{Hc^T}=\begin{pmatrix}2210\\2101\end{pmatrix}\begin{pmatrix}\boldsymbol{c}_3\\\boldsymbol{c}_2\\\boldsymbol{c}_1\\\boldsymbol{c}_0\end{pmatrix}=\boldsymbol{c}_3\begin{pmatrix}2\\2\end{pmatrix}+\boldsymbol{c}_2\begin{pmatrix}2\\1\end{pmatrix}+\boldsymbol{c}_1\begin{pmatrix}1\\0\end{pmatrix}+\boldsymbol{c}_0\begin{pmatrix}0\\1\end{pmatrix}=0$$

* $\boldsymbol{y}=\boldsymbol{c}+\boldsymbol{e}$ אך במילת קוד $\boldsymbol{e}=0$ ולכן $\boldsymbol{y}=\boldsymbol{c}$.

מציאת מילת קוד שקולה למציאת קומבינציה ליניארית של עמודות המטריצה $\boldsymbol{H}$ אשר תגרור $\boldsymbol{S}=0$. דוגמא למילת קוד: 1011.

8. המרחק המינימאלי בקוד ליניארי שקול למשקל Hamming המינימאלי מבין כל מילות הקוד.

במקרה שלנו $\boldsymbol{d}=3$.

<u>מסקנה</u>: המרחק המינימאלי בקוד ליניארי שקול גם למציאת המספר הקטן ביותר של עמודות תלויות ב- $\boldsymbol{H}$.

9. יכולת גילוי השגיאות של הקוד היא $d-1=2$

10. יכולת תיקון השגיאות של הקוד היא $t=\left\lfloor \frac{d-1}{2} \right\rfloor=1$

11. תכנון מקודד לפי $G=\begin{pmatrix}2101\\0112\end{pmatrix}$ מעל $GF(3)$:

<u>משתני כניסה</u>: M_1, M_0 כאשר כל אחד מהם בגודל שני ביטים (לפי המיפוי להלן).

<u>משתני יציאה</u>: C_3, C_2, C_1, C_0 כאשר כל אחד מהם בגודל שני ביטים (לפי המיפוי להלן).

כניסות ויציאות המערכת נקבעות על פי המיפוי הבא:

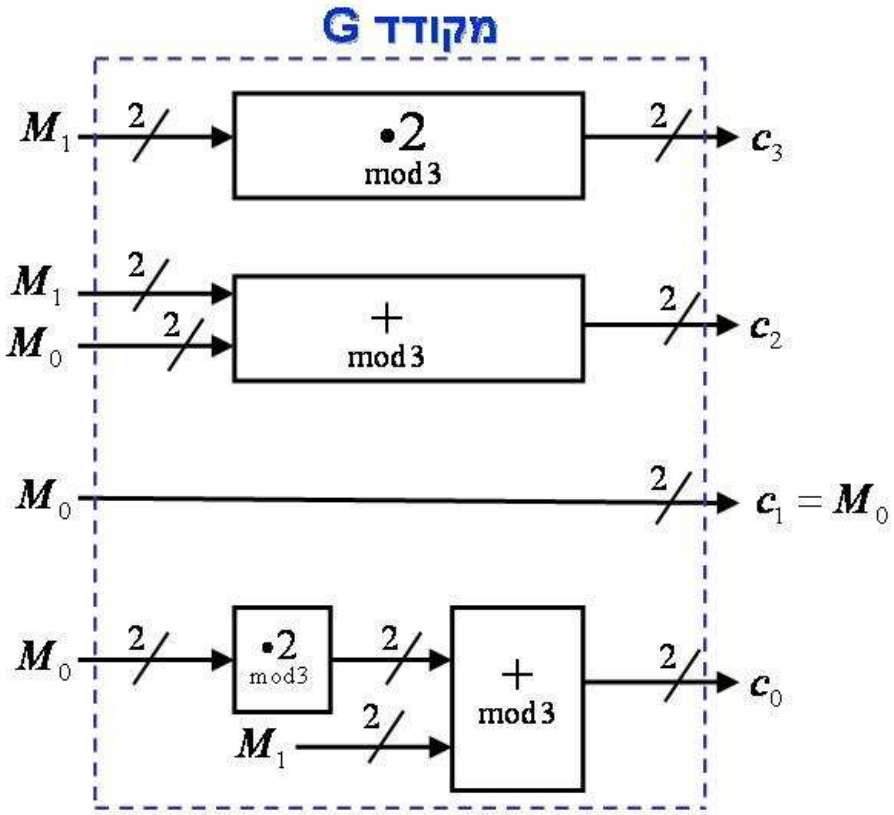
מיפוי	סימבול
00	0
01	1
10	2

<u>תיאור המערכת:</u>

<u>מימוש</u>:

פעולת הקידוד היא מכפלת מילת הכניסה $M_1 M_0$ במטריצה היוצרת G כלומר:

$$\left(M_1\ M_0\right)\begin{pmatrix}2101\\0112\end{pmatrix}=\left(2M_1, M_1+M_0, M_0, M_1+2M_0\right)$$



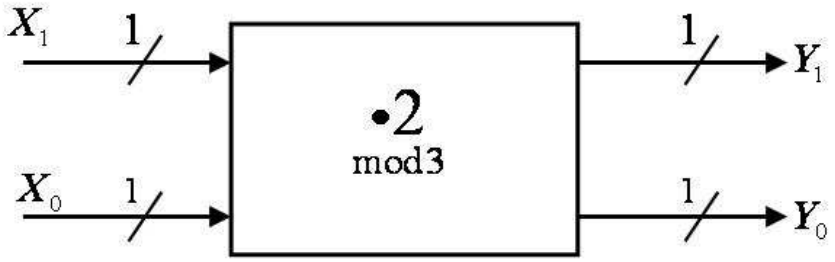
פעולות החיבור והכפל מבצעות במודול 3 לכן נתכנן בנפרד את הרכיבים הללו:

<u>נממש מכפל ב-2 מעל $GF(3)$</u>:

<u>משתני כניסה</u>: X_1, X_0 כאשר כל אחד מהם בגודל ביט אחד.

<u>משתני יציאה</u>: Y_1, Y_0 כאשר כל אחד מהם בגודל ביט אחד.

<u>תיאור המערכת</u>:



טבלת אמת:

X_1, X_0	Y_1, Y_0
00	00
01	10
10	01
**	**

מטבלת האמת מתקבלות משוואות המערכת:

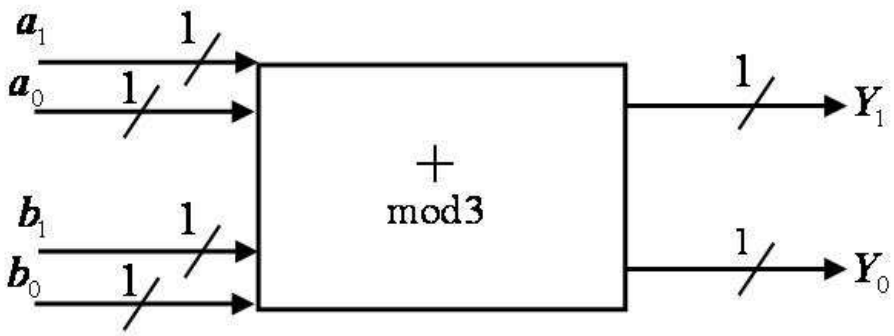
$$Y_1 = X_0 \qquad Y_0 = X_1$$

<u>נממש מסכם מעל $GF(3)$:</u>

<u>משתני כניסה</u>: a_1, a_0, b_1, b_0 כאשר כל אחד מהם בגודל ביט אחד.

<u>משתני יציאה</u>: Y_1, Y_0 כאשר כל אחד מהם בגודל ביט אחד.

<u>תיאור המערכת:</u>



<u>טבלת אמת</u>

a_1, a_0	b_1, b_0	Y_1, Y_0
00	00	00
	01	01
	11	**
	10	10
01	00	01
	01	10
	11	**
	10	00
10	00	10
	01	00
	11	**
	10	01
11	00	**
	01	**
	11	**
	10	**

<u>נבצע מינימיזציה בעזרת מפת קרנו:</u>

עבור Y_1 מתקבל:

b_1, b_0 \ a_1, a_0	00	01	11	10
00	0	0	*	1
01	0	1	*	0
11	*	*	*	*
10	1	0	*	0

$$Y_1 = \bar{a}_1\bar{a}_0 b_1 + a_0 b_0 + a_1\bar{b}_1\bar{b}_0$$

עבור Y_0 מתקבל:

b_1,b_0 \ a_1,a_0	00	01	11	10
00	0	1	*	0
01	1	0	*	0
11	*	*	*	*
10	0	0	*	1

$$Y_0 = a_1 b_1 + a_0 \bar{b}_1 \bar{b}_0 + \bar{a}_1 \bar{a}_0 b_0$$

12. תכנון מעגל חישוב סינדרום לפי $H = \begin{pmatrix} 2\,2\,1\,0 \\ 2\,1\,0\,1 \end{pmatrix}$

<u>משתני כניסה</u>: Y_3, Y_2, Y_1, Y_0 כאשר כל אחד מהם בגודל שני ביטים (לפי המיפוי להלן).

<u>משתני יציאה</u>: S_1, S_0 כאשר כל אחד בגודל שני ביטים (לפי המיפוי להלן).

כניסות ויציאות המערכת נקבעות לפי המיפוי הבא:

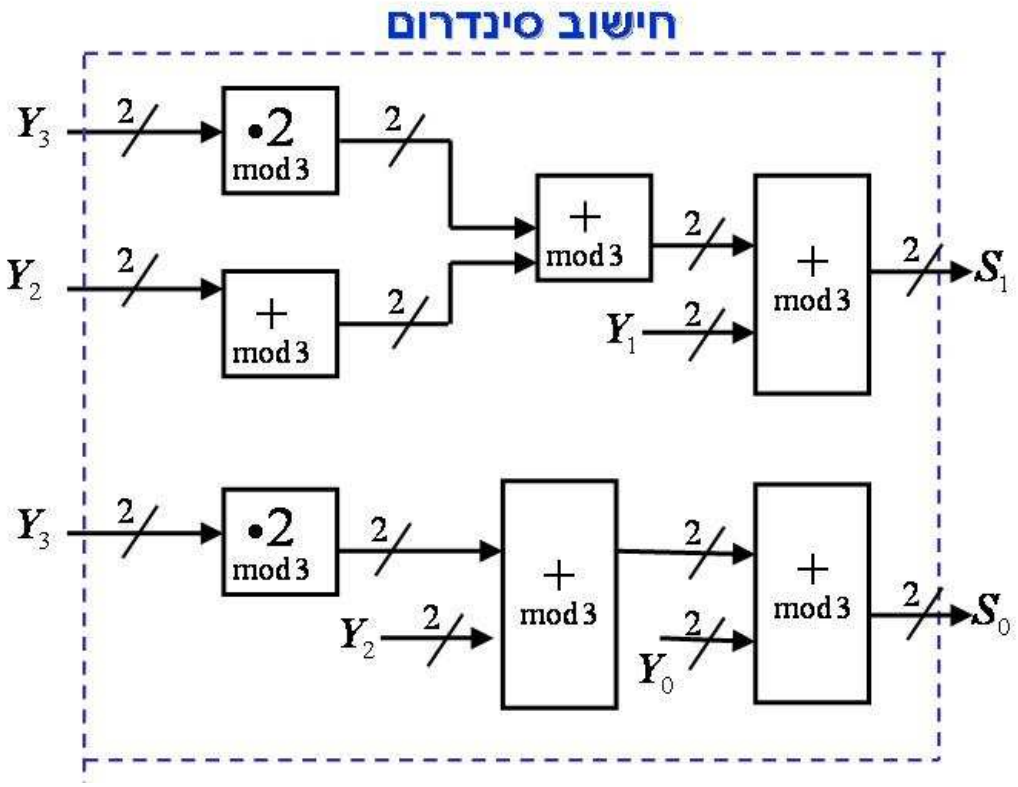
<u>מיפוי</u>	<u>סימבול</u>
00	0
01	1
10	2

<u>תיאור המערכת:</u>

מימוש:

פעולת חישוב הסינדרום היא מכפלת הווקטור המתקבל (Y_3,Y_2,Y_1,Y_0) במטריצה הבודקת H כלומר:

$$\begin{pmatrix} 2210 \\ 2101 \end{pmatrix} \begin{pmatrix} Y_3 \\ Y_2 \\ Y_1 \\ Y_0 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_0 \end{pmatrix}$$

$$S_1 = 2Y_3 + 2Y_2 + Y_1$$

$$S_1 = 2Y_3 + Y_2 + Y_0$$