פתרון תרגיל בית - 4

שאלה מספר 1

האם הקוד הבא מעל $GF(5)$ ניתן לייצוג כ $G=(I\mid A)$? במידה וכן הבא אותו לצורה זו, במידה ולא, האם ישנם סימבולים היכולים להגדיר סט סימבולי אינפורמציה. מצא את המטריצה הבודקת של הקוד.

$$\begin{array}{c} \begin{array}{cccccccc} \underline{1} & \underline{2} & \underline{3} & \underline{4} & \underline{5} & \underline{6} & \underline{7} & \underline{8} \end{array} \\ \boldsymbol{G}=\begin{pmatrix} 4 & 2 & 2 & 0 & 0 & 3 & 1 & 1 \\ 0 & 1 & 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 3 & 0 \end{pmatrix} \end{array}$$

פתרון:

כיוון שבשורה השלישית יש שלושה אפסים בתחילת המילה לא נוכל להגיע למטריצת יחידה $\boldsymbol{I}_3$ בפרט ולצורה $G=(I\mid A)$ בכלל.

למרות זאת, נוכל להגדיר את עמודות 3,4,5 כעמודות האינפורמציה:

$$\boldsymbol{G}=\begin{pmatrix} 4 & 2 & 2 & 0 & 0 & 3 & 1 & 1 \\ 0 & 1 & 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 3 & 0 \end{pmatrix} \overset{I+II\to II}{\sim} \begin{pmatrix} 4 & 2 & 2 & 0 & 0 & 3 & 1 & 1 \\ 4 & 3 & 0 & 1 & 0 & 3 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 3 & 0 \end{pmatrix}$$

$$\overset{3I\to I}{\sim} \begin{pmatrix} 2 & 1 & \boldsymbol{1} & \boldsymbol{0} & \boldsymbol{0} & 4 & 3 & 3 \\ 4 & 3 & \boldsymbol{0} & \boldsymbol{1} & \boldsymbol{0} & 3 & 1 & 1 \\ 0 & 0 & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{1} & 1 & 3 & 0 \end{pmatrix}$$

המטריצה הבודקת:

$$\boldsymbol{H}=\begin{pmatrix} \boldsymbol{1}\,\boldsymbol{0}\,3\,1\,0\,\boldsymbol{0}\,\boldsymbol{0}\,\boldsymbol{0} \\ \boldsymbol{0}\,\boldsymbol{1}\,4\,2\,0\,\boldsymbol{0}\,\boldsymbol{0}\,\boldsymbol{0} \\ \boldsymbol{0}\,\boldsymbol{0}\,1\,2\,4\,\boldsymbol{1}\,\boldsymbol{0}\,\boldsymbol{0} \\ \boldsymbol{0}\,\boldsymbol{0}\,2\,4\,2\,\boldsymbol{0}\,\boldsymbol{1}\,\boldsymbol{0} \\ \boldsymbol{0}\,\boldsymbol{0}\,2\,4\,0\,\boldsymbol{0}\,\boldsymbol{0}\,\boldsymbol{1} \end{pmatrix}$$

באופן כללי ניתן להגיע למטריצת הבדיקה באופן הבא:

- החלפת סדר העמודות ב $\boldsymbol{G}$ כך שתהיה מהצורה $\boldsymbol{G}'=\left(\boldsymbol{I}_3\mid\boldsymbol{A}\right)$
- מציאת $\boldsymbol{H}'=\left(-\boldsymbol{A}^{\boldsymbol{T}}\mid\boldsymbol{I}_5\right)$
- החלפת סדר העמודות לסדר המקורי.

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

נדגים את שלושת השלבים עבור המקרה שלנו:

$$\begin{array}{c} \begin{array}{cccccccc} \underline{1} & \underline{2} & \underline{3} & \underline{4} & \underline{5} & \underline{6} & \underline{7} & \underline{8} \end{array} \\ \boldsymbol{G} = \begin{pmatrix} 2 & 1 & \boldsymbol{1} & \boldsymbol{0} & \boldsymbol{0} & 4 & 3 & 3 \\ 4 & 3 & \boldsymbol{0} & \boldsymbol{1} & \boldsymbol{0} & 3 & 1 & 1 \\ 0 & 0 & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{1} & 1 & 3 & 0 \end{pmatrix} \end{array}$$

$$\begin{array}{c} \begin{array}{cccccccc} \underline{3} & \underline{4} & \underline{5} & \underline{1} & \underline{2} & \underline{6} & \underline{7} & \underline{8} \end{array} \\ \boldsymbol{G}' = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 4 & 3 & 3 \\ 0 & 1 & 0 & 4 & 3 & 3 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 3 & 0 \end{pmatrix} \end{array} \Rightarrow \begin{array}{c} \underline{3}\ \underline{4}\underline{5}\underline{1}\underline{2}\underline{6}\underline{7}\underline{8} \\ \boldsymbol{H}' = \begin{pmatrix} 31010000 \\ 42001000 \\ 12400100 \\ 24200010 \\ 24000001 \end{pmatrix} \end{array}$$

$$\begin{array}{c} \underline{1}\underline{2}\underline{3}\underline{4}\underline{5}\ \underline{6}\underline{7}\underline{8} \\ \boldsymbol{H} = \begin{pmatrix} \boldsymbol{10}310\boldsymbol{000} \\ \boldsymbol{01}420\boldsymbol{000} \\ \boldsymbol{00}124\boldsymbol{100} \\ \boldsymbol{00}242\boldsymbol{010} \\ \boldsymbol{00}240\boldsymbol{001} \end{pmatrix} \end{array}$$

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

שאלה מספר 2

סכם מתוך הספרות על קוד GOLAY - תאר כיצד הוא מוגדר, מהם הפרמטרים שלו ופרט תכונותיו. (אורך הסיכום כעמוד אחד).

פתרון:

סיכום יועלה בקובץ נפרד לאתר בהמשך הקורס.

שאלה מספר 3

א. קבע איזה מהפולינומים הבאים יכול לשמש כפולינום יוצר של קוד בינארי ציקלי באורך 9.

$$g_1(x) = 1 + x^3 + x^4$$
$$g_2(x) = 1 + x^2 + x^3 + x^5$$
$$g_3(x) = x^2 + x^5 + x^6$$
$$g_4(x) = 1 + x^2 + x^3$$
$$g_5(x) = 1 + x^2 + x^3 + x^9$$
$$g_6(x) = 1 + x^3$$

ב. מצא את מאפייני הקוד של הפולינום שבחרתם - אורך, מימד, מספר מילות הקוד, מרחק מינימאלי, קצב הקוד,יכולת גילוי ויכולת תיקון השגיאות.

ג. תן דוגמא לשלוש מילות קוד

ד. תן דוגמאות למילים שאינן מילות קוד (ללא חישובים)

ה. בעזרת הפולינום שבחרתם בסעיף א', קדד את מילת האינפורמציה $m(x) = 1 + x^2$

ו. האם המילה $v(x) = x^3 + x^6$ היא מילת קוד

ז. תן דוגמא למילת קוד השונה מ-$g(x)$ היכולה לשמש פולינום יוצר לקוד ציקלי באותו אורך – מהם פרמטרי הקוד החדש, האם הקוד החדש מכיל/שווה/מוכל בקוד המקורי

ח. תן דוגמא לקוד נוסף שהפולינום $g(x)$ יכול לשמש פולינום יוצר עבורו,מהם הפרמטרים החדשים?

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

פתרון:

א. נתבונן בפירוק של x^9-1 לגורמים:

$$x^9-1=(1+x)(1+x+x^2)(1+x^3+x^6)$$

נשים לב כי x^9-1 מתפרק לשלושה גורמים אי-פריקים. ניתן למצוא את כל הפולינומים היוצרים של קוד בינארי ציקלי באורך 9 בעזרת הפירוק לעיל.

כל גורם במכפלה יכול להוות פולינום יוצר. כמו כן תוצאת מכפלת מספר גורמים מניבה אף היא פולינום יוצר.

הפולינום $g_1(x)$ אינו יכול להיות פולינום יוצר באורך 9, כיוון שאין שום קומבינציה של מכפלות הגורמים שתניב פולינום עם דרגה ארבע. בצורה דומה נשלול את $g_2(x)$.

$g_3(x)$ אינו יכול להיות פולינום יוצר כיוון ש $g_0=0$.

$g_4(x)$ בעל דרגה 3. יתכן והינו פולינום יוצר כיוון ומכפלת שני הגורמים השמאליים תניב פולינום שדרגתו 3. לבדיקה האם הוא מהווה פולינום יוצר ניתן לבדוק האם x^9-1 מתחלק בו ללא שארית.

דרך נוספת לבדיקה היא הכפלת שני הגורמים הנ"ל והשוואת התוצאה ל $g_4(x)$. למטרת תרגול חלוקת פולינומים ננקוט בגישה הראשונה:

$$\begin{array}{l|l}
 & x^6+x^5+x^4+x^2 \\ \hline
x^9-1 & x^3+x^2+1 \\
 & \underline{x^9+x^8+x^6} \\
 & x^8+x^6+1 \\
 & \underline{x^8+x^7+x^5} \\
 & x^7+x^5+x^6+1 \\
 & \underline{x^7+x^6+x^4} \\
 & x^5+x^4+1 \\
 & \underline{x^5+x^4+x^2} \\
 & \boxed{x^2+1}
\end{array}$$

כלומר גם $g_4(x)$ אינו יכול להיות פולינום יוצר לקוד בינארי ציקלי באורך 9.

דרגת $g_5(x)$ היא תשע ואילו דרגה מקסימאלית של מילת קוד היא $n-1=8$ ולכן נפסל.

הפולינום היחיד שנותר הוא $g_6(x)=1+x^3$ שמורכב ממכפלת שני הגורמים השמאליים בפירוק:

$(1+x)(1+x+x^2)=1+x+x^2+x+x^2+x^3=x^3+1=g_6(x)$ ולכן מבלי שנצטרך לחלק את x^9-1 ב $g_6(x)$ יודעים שהשארית תהיה אפס.

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

ב. אורך הקוד נתון $\boldsymbol{n}=9$.

מימד הקוד הוא $\boldsymbol{k}=\boldsymbol{n}-\deg \boldsymbol{g}(\boldsymbol{x})=\boldsymbol{n}-\boldsymbol{r}=6$.

מספר מילות הקוד הוא $\boldsymbol{q}^{\boldsymbol{k}}=2^6=64$.

המרחק המינימאלי הוא 2, כיוון ויש מילת קוד במשקל Hamming 2 (הפולינום היוצר עצמו אף הוא מילת קוד). המרחק אינו יכול להיות 1 כיוון שהזזות ציקליות של כל מילה במשקל Hamming 1 בסופו של יתנו את פולינום היחידה אשר דרגתו היא אפס ולכן קטנה מדרגת הפולינום היוצר.

קצב הקוד הוא $\frac{\boldsymbol{k}}{\boldsymbol{n}}=\frac{6}{9}=\frac{2}{3}$ כלומר בכל מעבר מידע בערוץ מנוצל רק $\frac{2}{3}$ להעברת האינפורמציה ואילו השליש הנותר מוקצה לסיביות היתירות.

יכולת גילוי השגיאות היא $\boldsymbol{d}-1=1$.

יכולת תיקון השגיאות היא $\boldsymbol{t}=\left\lfloor\frac{\boldsymbol{d}-1}{2}\right\rfloor=0$

ג. דוגמאות למילות קוד ניתן למצוא למשל על ידי הזזה ציקלית של הפולינום היוצר:

$$\boldsymbol{c}_1=\boldsymbol{x}\cdot\boldsymbol{g}_6(\boldsymbol{x})\bmod\left(\boldsymbol{x}^9-1\right)=\boldsymbol{x}\cdot\left(1+\boldsymbol{x}^3\right)\bmod\left(\boldsymbol{x}^9-1\right)=\boldsymbol{x}+\boldsymbol{x}^4$$
$$\boldsymbol{c}_2=\boldsymbol{x}\cdot\boldsymbol{c}_1\bmod\left(\boldsymbol{x}^9-1\right)=\boldsymbol{x}\cdot\left(\boldsymbol{x}+\boldsymbol{x}^4\right)\bmod\left(\boldsymbol{x}^9-1\right)=\boldsymbol{x}^2+\boldsymbol{x}^5$$
$$\boldsymbol{c}_3=\boldsymbol{x}\cdot\boldsymbol{c}_2\bmod\left(\boldsymbol{x}^9-1\right)=\boldsymbol{x}\cdot\left(\boldsymbol{x}^2+\boldsymbol{x}^5\right)\bmod\left(\boldsymbol{x}^9-1\right)=\boldsymbol{x}^3+\boldsymbol{x}^6$$

ד. דרגת הפולינום היוצר היא 3 ולכן נובע מתכונות הפולינום היוצר כי כל מילה בדרגה קטנה מ3 אינה מילת קוד. כמו כן כל מילה בדרגה 3 אשר שונה מהפולינום היוצר גם היא אינה מילת קוד כיוון והפולינום היוצר הוא הפולינום היחיד עם דרגה 3 בקוד.

דוגמאות למילים שאינן מילות קוד: $\boldsymbol{x}^2+\boldsymbol{x}+1\ ,\ \boldsymbol{x}\ ,\ 1\ ,\ \boldsymbol{x}^3+\boldsymbol{x}+1$

ה. $\boldsymbol{c}(\boldsymbol{x})=\boldsymbol{m}(\boldsymbol{x})\cdot\boldsymbol{g}_6(\boldsymbol{x})=\left(1+\boldsymbol{x}^2\right)\left(1+\boldsymbol{x}^3\right)=1+\boldsymbol{x}^3+\boldsymbol{x}^2+\boldsymbol{x}^5=\boldsymbol{x}^5+\boldsymbol{x}^3+\boldsymbol{x}^2+1$

ו. $\boldsymbol{x}^3+\boldsymbol{x}^6$ היא מילת קוד כפי שראינו כבר בסעיף ג'. ניתן גם לחלק בפולינום היוצר ולראות שהשארית המתקבלת היא אפס.

ז. בקוד הספציפי שבחרנו לא קיימת מילה כזו. נסו למצוא קוד בו מתקיימת תכונה זו.

ח. כפי הוכחנו בתרגול כיתה 4, הפולינום היוצר יכול לפרוש קוד גם עבור $\boldsymbol{n}$ שהוא כפולה של 9. למשל עבור $\boldsymbol{n}=18$. הפרמטרים החדשים יהיו: $\left(\boldsymbol{n}=18,\boldsymbol{k}=18-3=15,\boldsymbol{d}=2\right)_2$

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

שאלה מספר 4

א. האם הפולינום $g(x)=1+x+x^3$ יוצר קוד ציקלי באורך 8 מעל $GF(3)$?

ב. אם כן, מצא את מאפייני הקוד של הפולינום שבחרתם - אורך, מימד, מספר מילות הקוד, חסם למרחק מינימאלי, קצב הקוד. אם לא מצא פולינום כזה ואת מאפייני הקוד שלו.

ג. קדד את מילת האינפורמציה $m(x)=2+2x^2$

ד. האם המילה $v(x)=2x^4+2x^2+2x$ היא מילת קוד

פתרון:

א. הפולינום הוא מוני כלומר המקדם של החזקה הגבוהה ביותר הוא 1

וכן $g_0 \neq 0$ כלומר הLSB שונה מאפס. לכן נותר רק לבדוק האם $g(x) \mid x^8-1$:

$$
\begin{array}{l|l}
 & x^5+2x^3+2x^2+x+2 \\
\hline
x^8-1 & x^3+x+1 \\
 & \underline{x^8+x^6+x^5} \\
 & 2x^6+2x^5+2 \\
 & \underline{2x^6+2x^4+2x^3} \\
 & 2x^5+x^4+x^3+2 \\
 & \underline{2x^5+2x^3+2x^2} \\
 & x^4+2x^3+x^2+2 \\
 & \underline{x^4+x^2+x} \\
 & 2x^3+2x+2 \\
 & \underline{2x^3+2x+2} \\
 & \boxed{0}
\end{array}
$$

<u>מסקנה</u>: כל התנאים מתקיימים ולכן $g(x)=1+x+x^3$ יוצר קוד ציקלי באורך 8 מעל $GF(3)$.

ב. אורך הקוד נתון - $n=8$.

דרגת הפולינום היוצר שווה למספר סימבולי היתירות (r). במקרה שלנו $r=3$ ולכן $k=n-r=5$.

מספר מילות הקוד הוא $q^k=3^5=243$.

באופן כללי למציאת חסם למרחק המינימאלי ניעזר בחסם סינגלטון האומר כי $d \le n-k+1=4$. במקרה שלנו, משקל הפולינום $g(x)$ הוא 3 ולכן $d \le 3$.

קצב הקוד הוא $\frac{k}{n}=\frac{5}{8}$.

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

ג.
$$c(x)=m(x)\cdot g(x)=\left(2+2x^2\right)\cdot\left(1+x+x^3\right)$$
$$=2+2x+\underline{2x^3}+2x^2+\underline{2x^3}+2x^5$$
$$=2+2x+2x^2+\underline{x^3}+2x^5$$

ד.
$$\begin{array}{l|l} & 2x \\ \hline 2x^4+2x^2+2x & x^3+x+1 \\ \underline{2x^4+2x^2+2x} & \\ \boxed{0} & \end{array}$$
ולכן המילה הינה מילת קוד.

<u>שאלה מספר 5</u>

רשום את כל הקודים הבינאריים הציקליים האפשריים באורך 9 ובאורך 3. עבור כל אחד מהקודים קבע את הפולינום היוצר את האורך והמימד.

<u>פתרון:</u>

<u>עבור קוד באורך 9:</u>

$$x^9-1=(1+x)\left(1+x+x^2\right)\left(1+x^3+x^6\right)$$

כפי שהוסבר בפתרון תרגיל 3, הפולינומים היוצרים האפשריים הם:

$$g_1(x)=1$$
$$g_2(x)=1+x$$
$$g_3(x)=1+x+x^2$$
$$g_4(x)=1+x^3+x^6$$
$$g_5(x)=(1+x)\left(1+x+x^2\right)=1+x^3$$
$$g_6(x)=(1+x)\left(1+x^3+x^6\right)=1+x+x^3+x^4+x^6+x^7$$
$$g_7(x)=\left(1+x+x^2\right)\left(1+x^3+x^6\right)=1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8$$

<u>עבור קוד באורך 3:</u>

$$x^3-1=(1+x)\left(1+x+x^2\right)$$

הפולינומים היוצרים האפשריים הם:

$$g_1(x)=1$$
$$g_2(x)=1+x$$
$$g_3(x)=1+x+x^2$$

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

שאלה מספר 6

נתונים שני קודים ציקליים באותו האורך n. הקוד C_1 מוגדר ע"י הפולינום היוצר $g_1(x)$, והקוד C_2 מוגדר ע"י $g_2(x)$.

א. האם הקוד $C_1 \cap C_2$ המכיל את אוסף המילים המשותפות לשני הקודים הוא ציקלי ? אם כן מהו הפולינום היוצר שלו ? מהם האורך והמימד של הקוד החדש ?

ב. האם הקוד $C_1 + C_2$ המכיל את אוסף המילים מהצורה $m_1(x)g_1(x) + m_2(x)g_2(x)$, הוא ציקלי ? אם כן מהו הפולינום היוצר שלו ומה הם האורך והמימד של הקוד החדש.

הערה: כדי לקבוע האם קוד הוא ציקלי יש לבדוק האם מתקיימות כל התכונות.

פתרון:

א. הקוד ציקלי. ראשית נראה ליניאריות של הקוד החדש $C_1 \cap C_2$.

מספיק להראות:

$$\left(\boldsymbol{u}\cdot\vec{\boldsymbol{x}} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2 \quad \textbf{and} \quad \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2\right) \Rightarrow \left(\boldsymbol{u}\cdot\vec{\boldsymbol{x}} + \boldsymbol{v}\cdot\vec{\boldsymbol{y}}\right) \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2$$
$$\forall \boldsymbol{u},\boldsymbol{v} \in \boldsymbol{GF}\left(\boldsymbol{q}\right)$$

ואכן:

$$\boldsymbol{u}\cdot\vec{\boldsymbol{x}} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2 \Rightarrow \boldsymbol{u}\cdot\vec{\boldsymbol{x}} \in \boldsymbol{C}_1 \textbf{ and } \boldsymbol{u}\cdot\vec{\boldsymbol{x}} \in \boldsymbol{C}_2$$
$$\boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2 \Rightarrow \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_1 \textbf{ and } \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_2$$

$$\begin{aligned}
&\left(\boldsymbol{u}\cdot\vec{\boldsymbol{x}} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2 \textbf{ and } \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2\right)\\
&\Rightarrow \left(\boldsymbol{u}\cdot\vec{\boldsymbol{x}} \in \boldsymbol{C}_1 \textbf{ and } \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_1\right) \textbf{ and } \left(\boldsymbol{u}\cdot\vec{\boldsymbol{x}} \in \boldsymbol{C}_2 \textbf{ and } \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_2\right)\\
&\Rightarrow \boldsymbol{u}\cdot\vec{\boldsymbol{x}} + \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_1 \textbf{ and } \boldsymbol{u}\cdot\vec{\boldsymbol{x}} + \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_2\\
&\Rightarrow \boldsymbol{u}\cdot\vec{\boldsymbol{x}} + \boldsymbol{v}\cdot\vec{\boldsymbol{y}} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2
\end{aligned}$$

כלומר הקוד ליניארי.

שנית נראה ציקליות של הקוד:

צריך להראות שאם $\boldsymbol{x} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2$ אזי גם כל ההזזות שלו שייכות לחיתוך.

נסמן את ההזזות של הווקטור $\vec{\boldsymbol{x}}$ באות $\boldsymbol{S}$.

מהגדרת חיתוך מקבלים: $\vec{\boldsymbol{x}} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2 \;\Rightarrow\; \vec{\boldsymbol{x}} \in \boldsymbol{C}_1 \cap \vec{\boldsymbol{x}} \in \boldsymbol{C}_2$

אבל אם $\vec{\boldsymbol{x}} \in \boldsymbol{C}_1$ גם כל ההזזות שלו שייכות ל $\boldsymbol{C}_1$ ($\boldsymbol{C}_1$ קוד ציקלי) נסמן $\boldsymbol{S} \in \boldsymbol{C}_1$.

וכן אם $\vec{\boldsymbol{x}} \in \boldsymbol{C}_2$ גם כל ההזזות שלו שייכות ל $\boldsymbol{C}_2$ ($\boldsymbol{C}_2$ קוד ציקלי) נסמן $\boldsymbol{S} \in \boldsymbol{C}_2$

לכן לפי הגדרת חיתוך נקבל שההזזות שייכות ל $\boldsymbol{C}_1 \cap \boldsymbol{C}_2$ כלומר $\boldsymbol{S} \in \boldsymbol{C}_1 \cap \boldsymbol{C}_2$.

כלומר הראינו כי הקוד הוא ציקלי.

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

חישוב הפולינום היוצר החדש:

בחיתוך נמצאות כל המילים שהן כפולה של $g_1(x)$ וגם של $g_2(x)$ כלומר כל המילים הן מהצורה $m(x)\bullet\left[lcm\left(g_1(x),g_2(x)\right)\right]$. לכן הפולינום היוצר הוא $lcm\left(g_1(x),g_2(x)\right)$

הערת אגב:

$lcm\left(g_1(x),g_2(x)\right)$ הוא הגורם המשותף המינימאלי של שני הפולינומים. לדוגמא:

$$g_1(x)=(1+x)\left(1+x+x^3\right)$$
$$g_2(x)=(1+x)$$
$$lcm\left(g_1(x),g_2(x)\right)=(1+x)\left(1+x+x^3\right)$$

עבור הדוגמא הזו רואים שקוד החיתוך שווה לקוד שיוצר $g_1(x)$ (קוד C_1). במילים אחרות, הקוד C_2 מכיל את הקוד C_1 (שרטטו דיאגראמת ואן להמחשה או חשבו את מימד הקודים וראו מי הגדול מבין השניים).

פרמטרי הקוד החדש

$$\left(n,k=n-\deg\left[lcm\left(g_1(x),g_2(x)\right)\right]\right)$$

ב. הקוד ציקלי. ראשית נראה ליניאריות של הקוד החדש C_1+C_2 .

מספיק להראות:

$$\left(u\cdot\vec{x}\in C_1+C_2 \quad and \quad v\cdot\vec{y}\in C_1+C_2\right)\Rightarrow\left(u\cdot\vec{x}+v\cdot\vec{y}\right)\in C_1+C_2$$
$$\forall u,v\in GF(q)$$

ואכן:

$$u\cdot\vec{x}\in C_1+C_2\Rightarrow u\cdot\vec{x}=m_1(x)g_1(x)+m_2(x)g_2(x)$$
$$v\cdot\vec{y}\in C_1+C_2\Rightarrow v\cdot\vec{y}=m_3(x)g_1(x)+m_4(x)g_2(x)$$
$$\Rightarrow u\cdot\vec{x}+v\cdot\vec{y}=\underbrace{\left[m_1(x)+m_3(x)\right]g_1(x)}_{\in C_1}+\underbrace{\left[m_2(x)+m_4(x)\right]g_2(x)}_{\in C_2}$$
$$\Rightarrow u\cdot\vec{x}+v\cdot\vec{y}\in C_1+C_2$$

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

שנית נראה ציקליות של הקוד:

צריך להראות שאם $\vec{x} \in C_1 + C_2$ אזי גם כל ההזזות שלו שייכות לחיתוך.

$$\vec{x} \in C_1 + C_2 \Rightarrow \vec{x} = m_1(x)g_1(x) + m_2(x)g_2(x)$$
$$\left(x^i\right)\vec{x} \bmod \left(x^n - 1\right) = \left(x^i\right)\left[m_1(x)g_1(x) + m_2(x)g_2(x)\right] \bmod \left(x^n - 1\right)$$

$$= \left(x^i\right)m_1(x)g_1(x) \bmod \left(x^n - 1\right) + \left(x^i\right)m_2(x)g_2(x) \bmod \left(x^n - 1\right)$$

$$\overset{g(x) \bmod \left(x^n - 1\right) \equiv g(x)}{=} \underbrace{\left(x^i\right)m_1(x)g_1(x)}_{\in C_1} + \underbrace{\left(x^i\right)m_2(x)g_2(x)}_{\in C_2}$$

$$\Rightarrow \left[\left(x^i\right)\vec{x} \bmod \left(x^n - 1\right)\right] \in C_1 + C_2$$

חישוב הפולינום היוצר החדש:

בקוד החדש נמצאות כל המילים מהצורה

$$a(x) \bullet \left[\gcd\left(g_1(x), g_2(x)\right)\right] =$$
$$\left(m_1(x)\frac{g_1(x)}{\gcd\left(g_1(x), g_2(x)\right)} + m_2(x)\frac{g_2(x)}{\gcd\left(g_1(x), g_2(x)\right)}\right)\left[\gcd\left(g_1(x), g_2(x)\right)\right]$$

לכן הפולינום היוצר הוא $\gcd\left(g_1(x), g_2(x)\right)$.

הערת אגב:

$\gcd\left(g_1(x), g_2(x)\right)$ הוא המחלק המשותף המקסימאלי של שני הפולינומים. לדוגמא:

$$g_1(x) = (1 + x)\left(1 + x + x^3\right)$$
$$g_2(x) = (1 + x)\left(1 + x^2 + x^3\right)$$
$$\gcd\left(g_1(x), g_2(x)\right) = (1 + x)$$

פרמטרי הקוד החדש $\left(n, k = n - \deg\left[\gcd\left(g_1(x), g_2(x)\right)\right]\right)$

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com

שאלה מספר 7

נתון קוד ציקלי C באורך n המוגדר ע"י פולינום יוצר $g(x)$. נסמן מילת קוד של C כ- $(c_0,c_1,\cdots,c_{n-1})$. מקוד זה יוצרים קוד חדש C' באורך 2n ע"י שכפול מילת הקוד פעמיים, מילת הקוד החדשה מוגדרת כ- $(c_0,c_1,\cdots c_{n-1},c_0,c_1,\cdots c_{n-1})$. הראה כי C' הוא ציקלי וקבע את הפולינום היוצר שלו.

פתרון:

כיוון שהזזה n מקומות שקולה להכפלה ב x^n, נשים לב שמילה בקוד החדש ניתנת לכתיבה כך:

$$c'(x)=c(x)+x^n c(x) \overset{c(x)=m(x)g(x)}{=} m(x)\left(1+x^n\right)g(x)$$

נראה ליניאריות של הקוד החדש:

$$c_1'(x)=m_1(x)\left(1+x^n\right)g(x)$$
$$c_2'(x)=m_2(x)\left(1+x^n\right)g(x)$$
$$c_1'(x)+c_2'(x)=\left[m_1(x)+m_2(x)\right]\left(1+x^n\right)g(x)=m_3(x)\left(1+x^n\right)g(x)$$

נראה ציקליות של הקוד החדש:

בהזזה ציקלית של הקוד החדש נקבל

$$\underline{(c_0,c_1,\ldots,c_{n-1},c_0,c_1,\ldots,c_{n-1})\rightarrow\left(\underbrace{c_{n-1},c_0,\ldots,c_{n-2}}_{C_{new}\in C'(x)},\underbrace{c_{n-1},c_0,\ldots,c_{n-2}}_{C_{new}}\right)}$$

לאחר הזזה רואים כי החלק השמאלי של המילה המוזזת הוא מילת של הקוד המקורי והחלק הימני שלה הוא שכפול מילת הקוד הזו. לכן הקוד ציקלי.

הפולינום היוצר של קוד זה הוא $g'(x)=\left(1+x^n\right)g(x)$

שאלה מספר 8

נתון קוד ציקלי C באורך j המוגדר ע"י פולינום יוצר $g(x)$. בהסתמך על המשפט שהוכח בתרגול כיתה (4), הראה שניתן להאריך קוד זה לקוד ציקלי C' באורך n , (נתון כי j | n) עם אותו פולינום יוצר $g(x)$. קבע את הפרמטרים של הקוד החדש.

פתרון:

בתרגול כיתה 4 הוכחנו כי אם j מחלק את n, אז x^j-1 מחלק את x^n-1.

לכן אם $g(x)\mid x^j-1$ הרי $g(x)\mid x^n-1$ ולכן ניתן להגדיר קוד ציקלי עם פולינום יוצר $g(x)$ בעל הפרמטרים $\left(n,n-\deg g(x)\right)$.

PDF Created with deskPDF PDF Writer - Trial :: http://www.docudesk.com