מבוא לתורת הצפינה – תשס"ח

פתרון תרגיל בית - 3

שאלה מספר 1

נתון קוד ליניארי מעל $GF(2)$ הנפרש על ידי המטריצה היוצרת $G = \begin{pmatrix} 0111100 \\ 1011010 \\ 1101001 \end{pmatrix}$

מצאו את מאפייני הקוד - אורך, מימד, מספר מילות הקוד, מרחק מינימאלי, קצב הקוד,יכולת גילוי ויכולת תיקון השגיאות.

פתרון:

אורך הקוד זהה למספר העמודות ב G כלומר $n = 7$. מימד הקוד זהה למספר השורות ב G כלומר $k = 3$.

מספר מילות הקוד הוא $q^k = 2^3 = 8$

המרחק המינימאלי בקוד ליניארי שקול למספר הקטן ביותר של עמודות תלויות ב H.

נמצא את H:

$$G = \begin{pmatrix} 0111100 \\ 1011010 \\ \underbrace{1101}_{A}\underbrace{001}_{I_3} \end{pmatrix} \quad \Rightarrow \quad \mathrm{H} = \begin{pmatrix} 1000011 \\ 0100101 \\ 0010110 \\ \underbrace{0001}_{I_4}\underbrace{111}_{-A^T} \end{pmatrix}$$

רואים כי מספר העמודות הבלתי תלויות הוא 4 ולכן $d = 4$.

את המרחק המינימאלי ניתן למצוא גם בעזרת פרישת כל שבע המילים (כולן חוץ ממילת האפס השקולה לקידוד מילת האינפורמציה (000)) ובחירת המשקל המינימאלי.

שלוש מילים מתוך השבע כבר נתונות במטריצה היוצרת G (זכרו כי שורות G עצמן הן מילות קוד השקולות לקידוד מילות האינפורמציה $(001),(010),(100)$). לכן נותר לפרוש עוד ארבע מילים.

<u>הפרישה יכולה להתבצע באופן הבא:</u>

סכום שתי השורות הראשונות ב G - שקול לקידוד מילת האינפורמציה (110):

$$(0111100)+(1011010)=(1100110)$$

סכום השורה הראשונה עם השורה השלישית ב G - שקול לקידוד מילת האינפורמציה (101):

$$(0111100)+(1101001)=(1010101)$$

סכום שתי השורות האחרונות ב G - שקול לקידוד מילת האינפורמציה (011):

$$(1011010)+(1101001)=(0110011)$$

סכום שלוש המילים ב G - שקול לקידוד מילת האינפורמציה (111):

$$(0111100)+(1011010)+(1101001)=(0001111)$$

סה"כ רואים כי המשקל המינימאלי הוא 4 ולכן $d=4$.

יכולת גילוי השגיאות היא $d-1=3$. יכולת תיקון השגיאות היא $t=\left\lfloor \frac{d-1}{2} \right\rfloor=1$.

קצב הקוד הוא $\boldsymbol{R}=\frac{\boldsymbol{k}}{\boldsymbol{n}}=\frac{3}{7}$

לסיכום, התקבל הקוד $[7,3,4]_2$ עם קצב קוד - $\frac{3}{7}$ בעל יכולת גילוי של 3 שגיאות ותיקון שגיאה אחת.

<u>שאלה מספר 2</u>

נתונים שני קודים $[\boldsymbol{n}_1,\boldsymbol{k},\boldsymbol{d}_1],[\boldsymbol{n}_2,\boldsymbol{k},\boldsymbol{d}_2]$ המוגדרים בעזרת המטריצות היוצרות $\boldsymbol{G}_1,\boldsymbol{G}_2$.

א. הראו שהקוד המוגדר ע"י $\boldsymbol{G}=\begin{pmatrix}\boldsymbol{G}_1 & 0\\ 0 & \boldsymbol{G}_2\end{pmatrix}$ הוא קוד $[\boldsymbol{n}_1+\boldsymbol{n}_2,2\cdot\boldsymbol{k},\min(\mathrm{d}_1,\mathrm{d}_2)]$.

ב. הראו שהקוד המוגדר על ידי $\boldsymbol{G}=(\boldsymbol{G}_1\,|\,\boldsymbol{G}_2)$ הוא קוד $[\mathrm{n}_1+\mathrm{n}_2,\boldsymbol{k},\boldsymbol{d}]$ כאשר

$$\boldsymbol{d}\ge\boldsymbol{d}_1+\boldsymbol{d}_2$$

<u>**פתרון**</u>:

א. ב G יש $k+k$ שורות לכן המימד החדש הוא $2k$. כמו כן ב G יש n_1+n_2 עמודות לכן המימד החדש הוא n_1+n_2.

המרחק המינימאלי בקוד ליניארי הוא המשקל המינימאלי של כל מילות הקוד מלבד מילת האפס. נשים לב לפי הגדרת G כי התוספת לכל מילת קוד מקורית היא אפס.

ניתן לרשום את הקוד החדש באופן הבא:

$$C=\{c=\ c_i\,|\,c_j:\forall c_i,c_j\ \ c_i\in C_1,c_j\in C_2\}$$

נחשב את המרחק המינימאלי ונקבל:

$$\min(d)=\min\{\min wt(c_i\,|\,0),\min wt(0\,|\,c_j)\}\,c_i\in C_1,c_j\in C_2$$

אבל נתון ש $\min wt(c_i\,|\,0)=d_1\quad,\min wt(0\,|\,c_j)=d_2$

ולכן $\min(d)=\min(d_1,d_2\ )$

ב. ב G יש k שורות לכן המימד החדש הוא k. כמו כן ב G יש n_1+n_2 עמודות לכן המימד החדש הוא n_1+n_2.

ניתן לרשום את הקוד החדש באופן הבא:

$$C=\{c=\ c_i\,|\,c_j\ :\ c_i=mG_1\,,c_j=mG_2\ \ \forall m\}$$

אם קיים m עבורו $wt(mG_1)=d_1\quad and\quad wt(mG_2)=d_2$ אזי $d=d_1+d_2$

אחרת $d>d_1+d_2$

נשלול את האפשרות ש $(c_i=0\ and\ c_j\neq 0)\ or\ (c_i\neq 0\ and\ c_j=0)$ כלומר

$d=d_1\ or\ d_2$

$\begin{cases} m=0\Leftrightarrow c_i=0 \\ m=0\Leftrightarrow c_j=0 \end{cases}\Leftarrow c_i=0\Leftrightarrow c_j=0$ כלומר אם c לא מילת האפס משקלה

$d\geq d_1+d_2$.

<u>שאלה מספר 3</u>

האם הקודים הבינאריים הבאים אפשריים:

1) n=7, k=2, d=5
2) n=63, k=31, t=17
3) n=63, k=45, d=7
4) n=127, k=109, d=7

<u>רמז</u>: היעזרו בחסמים הנמצאים בקובץ חסמים על קודים

<u>פתרון:</u>

כל הקודים שהוצגו אינם אפשריים.

הקוד הראשון אינו מקיים את חסם Plotkin וכן לא מקיים את חסם GV

הקוד השני אינו מקיים את חסם Singleton (שימו לב כי $d=2t+1=35$)

הקוד השלישי אינו מקיים את חסם GV

הקוד הרביעי אינו מקיים את חסם Hamming וכן לא מקיים את חסם GV.