פתרון תרגיל בית 11 במבנים אלגבריים
89-214 סמסטר א׳ תשפ״ג

שאלה 1 (חימום)**.** מבלי לעשות אף פעולת חיבור או כפל, הסבירו למה הקבוצה הבאה ב-$\mathbb{Z}_2^4$ אינה קוד לינארי:

$$\{(0110),(1001),(1010),(1100)\}$$

פתרון. קוד לינארי הוא מרחב וקטורי (ובפרט חבורה), וכל מרחב וקטורי כולל את וקטור האפס. הקוד בשאלה אינו כולל את (0000), ולכן הוא לא לינארי.

שאלה 2. נקודד את $\mathbb{Z}_2^2$ לקוד ב-$\mathbb{Z}_2^8$ לפי

$$(00)\mapsto(00000000) \qquad (01)\mapsto(01010101)$$
$$(10)\mapsto(10101010) \qquad (11)\mapsto(11111111)$$

כלומר חזרנו ארבע פעמים על כל וקטור. קוד מסוג כזה נקרא קוד חזרה.

א. מצאו את המרחק המינימלי d של הקוד.

ב. מצאו את המטריצה היוצרת התקנית G ואת מטריצת בדיקת הזוגיות הקנונית H של הקוד. ודאו קודם שאתם יודעים למה זה בכלל קוד לינארי.

פתרון. ראשית נשים לב שהקידוד הזה לינארי: ניתן להגדירו לפי הנוסחה המפורשת

$$(ab)\mapsto(abababab)$$

לכל $a,b\in\mathbb{Z}_2$, שהיא אכן העתקה לינארית.

א. אפשר לבדוק לפי הגדרה מה הוא המרחק המינימלי של הקוד, מפני שיש רק $\binom{4}{2}=6$ זוגות לבדיקה. דרך קצת יותר חסכונית היא לשים לב שמדובר בקוד לינארי, ואז נוכל להסתפק בחישוב משקל המינג של $4-1=3$ מילים. משקל המינג המינימלי של מילת קוד שאינה וקטור האפס הוא 4, ולכן $d=4$.

ב. ברור שנחבר כמה פעמים (בבלוקים) את מטריצת היחידה $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. כלומר

$$G=\begin{pmatrix}1&0\\0&1\\1&0\\0&1\\1&0\\0&1\\1&0\\0&1\end{pmatrix} \qquad H=\begin{pmatrix}1&0&1&0&0&0&0&0\\0&1&0&1&0&0&0&0\\1&0&0&0&1&0&0&0\\0&1&0&0&0&1&0&0\\1&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&1\end{pmatrix}$$

באופן יותר מפורט ניזכר שבהגדרה של קוד לינארי המטריצה A היא המטריצה המייצגת של העתקת היתירות, שנסמנה φ. אצלנו מתקיים

$$\varphi\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}a\\b\\a\\b\\a\\b\end{pmatrix}$$

לכן:

$$A=\left(\varphi\begin{pmatrix}1\\0\end{pmatrix}\quad\varphi\begin{pmatrix}0\\1\end{pmatrix}\right)=\begin{pmatrix}1&0\\0&1\\1&0\\0&1\\1&0\\0&1\end{pmatrix}$$

ומציבים אותה בהגדרה שראינו של המטריצות G ו-H.

שאלה 3. יהיו $C_1, C_2 \subseteq \mathbb{Z}_2^n$ שני קודים עם מרחקים מינימליים d_1, d_2, בהתאמה.

א. מצאו דוגמה שבה $|C_1| = |C_2|$, אבל $d_2 < d_1$.

ב. הוכיחו שאם $C_1 \subseteq C_2$, אז $d_2 \leq d_1$.

פתרון.

א. נבחר $C_1 = \{(0000), (1111)\}$ ו-$C_2 = \{(0000), (0100)\}$. קל לבדוק בחישוב ישיר כי $d_2 = 1 < 4 = d_1$, ואפילו בחרנו קודים לינאריים.

ב. לפי ההגדרה, קיימים $u, v \in C_1$ כך ש-$d(u,v) = d_1$. מכיוון ש-$C_1 \subseteq C_2$ מקבלים כי $u, v \in C_2$. לכן $d(u,v) \geq d_2$ וביחד קיבלנו $d_2 \leq d(u,v) = d_1$.
למעוניינים בהוכחה שקולה שדורשת בעיקר את הקורס במתמטיקה בדידה: לכל זוג קבוצות של טבעיים A, B מתקיים שאם $A \subseteq B$, אז $\min B \leq \min A$. בפרט, נסמן שתי קבוצות

$$A = \{d(u,v) \,|\, u, v \in C_1, u \neq v\}$$
$$B = \{d(u,v) \,|\, u, v \in C_2, u \neq v\}$$

ומהנתון $C_1 \subseteq C_2$ נקבל כי $A \subseteq B$. לפי הגדרה של מרחק מינימלי נסיק

$$d_2 = \min B \leq \min A = d_1$$

שאלה 4. נתבונן במטריצה הבאה

$$H=\begin{pmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{pmatrix}$$

א. חשבו את d של הקוד הלינארי C שמגדיר מרחב האפסים של H.

ב. בדקו האם המילים הבאות הן מילות קוד של C, ואם לא הניחו שאירעה שגיאה אחת ותקנו אותה:

$$v_1 = (0110100) \quad v_2 = (1000100) \quad v_3 = (1011100) \quad v_4 = (1010111)$$

פתרון.

א. סכום העמודות השנייה, השישית והשביעית של H הוא וקטור האפס, ולכן $d \le 3$. לפי (מסקנה של) טענה שראינו בכיתה בקוד לינארי מתקיים $d \ge 3$ אם ורק אם אין ב-H עמודת אפסים ואין בה עמודות זהות. זה בדיוק המצב אצלנו ולכן $d = 3$.

ב. נחשב $Hv_1 = 0$, ולכן v_1 היא מילת קוד.
לעומת זאת כשנחשב Hv_2 נקבל את וקטור העמודה (111), ולכן v_2 אינה מילת קוד. השגיאה שאירעה הייתה בסיבית השישית, כי זו העמודה המתאימה ב-H. לכן מילת הקוד שנשלחה הייתה

$$v_2 + e_6 = (1000110)$$

נחשב $Hv_3 = 0$, ולכן v_3 היא מילת קוד.
לבסוף נחשב Hv_4 ונקבל את וקטור העמודה (100), ולכן v_4 אינה מילת קוד. השגיאה שאירעה הייתה בסיבית הראשונה, כי זו העמודה המתאימה ב-H. לכן מילת הקוד שנשלחה הייתה

$$v_4 + e_1 = (0010111)$$

שאלה 5. לכל זוג פולינומים $f(x), g(x)$ בצעו חלוקה אוקלידית של פולינומים ומצאו פולינומים $q(x), r(x)$ כך ש-$f(x) = q(x)g(x) + r(x)$ עם $r(x) < g(x)$.

א. $f(x) = x^4 + 3x^3 + 3x^2 + 3x + 2,\ g(x) = x^2 + x - 5$ בחוג $\mathbb{R}[x]$.

ב. $f(x) = x^4 + 3x^3 + 3x^2 + 3x + 2,\ g(x) = x^2 + x - 5$ בחוג $\mathbb{Z}_2[x]$.

פתרון.

א. מחשבים $f(x) = (x^2 + 2x + 6)g(x) + (7x + 32)$. כלומר $r(x) = 7x + 32$ וכן $q(x) = x^2 + 2x + 6$.

ב. במקרה זה $f(x) = x^4 + x^3 + x^2 + x$ ו-$g(x) = x^2 + x + 1$. נקבל כי $f(x) = x^2 \cdot g(x) + x$, וזה מתאים לתשובה מהסעיף הקודם, כאשר מתייחסים למקדמים כאיברים של $\mathbb{Z}_2$. כלומר $r(x) = x$ ו-$q(x) = x^2$.

שאלה 6. יהי $g(x) = x^3 + 1 \in \mathbb{Z}_2[x]$. נגדיר לפי $g(x)$ קוד פולינומי C מ-$\mathbb{Z}_2^6$ ל-$\mathbb{Z}_2^9$ (כלומר כאן $m = 3$, $k = 6$ ו-$n = 9$).

א. הוכיחו או הפריכו האם C הוא קוד ציקלי.

ב. קודדו את הוקטור $x = (101011)$ למילת קוד ב-C.

ג. בדקו מי מבין המילים הבאות היא מילת קוד של C:

$$v_1 = (101011110) \qquad v_2 = (000101101) \qquad v_3 = (110010110)$$

פתרון.

א. כן, זה קוד ציקלי. הרי x^3+1 מחלק את x^n-1. באופן מפורש

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

ולפי טענה מן ההרצאה זה אומר ש-C הוא קוד ציקלי.

ב. הוקטור x מתאים לפולינום $f(x)=x^5+x^3+x+1$. נכפיל אותו ב-x^m ונחסיר את השארית בחלוקה ב-$g(x)$, כפי שעשינו בכיתה:

$$f(x)\cdot x^3=x^8+x^6+x^4+x^3=(x^5+x^3+x^2+x)g(x)+(x^2+x)$$
$$f(x)\cdot x^3-(x^2+x)=x^8+x^6+x^4+x^3+x^2+x$$

ולכן מילת הקוד המבוקשת היא (101011110).

ג. נשים לב כי v_1 היא מילת הקוד שקיבלנו בסעיף הקודם, ולכן התשובה ברורה.
המילה v_2 מתאימה לפולינום $x^5+x^3+x^2+1$, שמתחלק ב-$g(x)$:

$$x^5+x^3+x^2+1=(x^2+1)g(x)$$

ולכן זו מילת קוד. לעומת זאת, המילה v_3 מתאימה לפולינום שאינו מתחלק ב-$g(x)$:

$$x^8+x^7+x^4+x^2+x=(x^5+x^4+x^2)g(x)+x$$

ולכן v_3 אינה מילת קוד.

בהצלחה!