

פתרון תרגיל בית 10 במבנים אלגבריים 89-214 סמסטר א' תש"ף

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 ל- $\mathbb{Z}_2^8$ לפי

$$\begin{array}{ll} (00) \mapsto (00000000) & (01) \mapsto (01010101) \\ (10) \mapsto (10101010) & (11) \mapsto (11111111) \end{array}$$

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

א. מצאו את המרחק המינימלי $d_{\min}$ 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.

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 המינימום של $4 - 1 = 3$ מילים. משקל המינימום המינימלי של מילת קוד שאינה וקטור האפס הוא 4, ולכן $d_{\min} = 4$.

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

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

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

א. הוכיחו על ידי מציאת דוגמה כי ייתכן שמתקיים $|C_1| = |C_2|$, 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 לחשב כי $d_2 = 1 < d_1 = 4$, ואפילו בחרנו קודים לינאריים. בשני הקודים האלו בדיוק שתי מילות קוד כמובן.

ב. לכל זוג קבוצות של טבעיים A, B מתקיים שאם $A \subseteq B$, אז $\min B \leq \min A$. בפרט, נסמן שתי קבוצות

$$A = \{d(u, v) \mid u, v \in C_1, u \neq v\}$$

$$B = \{d(u, v) \mid u, v \in C_2, u \neq v\}$$

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 $d_{\min}$ 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 $d_{\min} \leq 3$. לפי (מסקנה של) טענה שראינו בכיתה בקוד לינארי מתקיים $d_{\min} \geq 3$ אם ורק אם אין ב- H עמודת אפסים ואין בה עמודות זהות. זה בדיוק המצב אצלנו ולכן $d_{\min} = 3$.

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 $\deg r(x) < \deg g(x)$.

א. $\mathbb{Q}[x]$ בחוג $f(x) = x^4 + 5x^3 + 3x^2 + 3x + 2, g(x) = x^2 + 5x - 1$.

ב. $\mathbb{Z}_2[x]$ בחוג $f(x) = x^4 + 5x^3 + 3x^2 + 3x + 2, g(x) = x^2 + 5x - 1$.

ג. $k \in \mathbb{N}$ כאשר $\mathbb{Z}_2[x]$ בחוג $f(x) = x^{4k}, g(x) = x^4 + 1$.
רמז: בחישוב סכום סדרה הנדסית מוכיחים $(q-1)|(q^k - 1)$.

פתרון.

א. מחשבים $f(x) = (x^2 + 4)g(x) + (-17x + 6)$ כלומר $r(x) = -17x + 6$ וכן $q(x) = x^2 + 4$.

ב. במקרה זה $f(x) = x^4 + x^3 + x^2 + x + 1$ 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- $q(x) = x^2$.

ג. לפי הרמז $(q-1)|(q^k - 1)$, ואנחנו יודעים לחשב סכום של סדרה הנדסית

$$q^k - 1 = (q - 1)(q^{k-1} + q^{k-2} + \dots + q + 1) = (q - 1) \sum_{i=0}^{k-1} q^i$$

אז בהצבה $q \mapsto x^4$ נקבל כי $(x^4 - 1)|(x^{4k} - 1)$. לכן

$$x^{4k-1} - 1 = (x^4 - 1)(x^{4(k-1)} + x^{4(k-2)} + \dots + x^4 + 1) = (x^4 - 1) \sum_{i=0}^{k-1} x^{4i}$$

ונקבל $x^{4k} = \sum_{i=0}^{k-1} x^{4i}(x^4 - 1) + 1$ נזכר שבחוג $\mathbb{Z}_2[x]$ מתקיים $x^4 + 1 = x^4 - 1$ ונסיק $r(x) = 1$ ו- $q(x) = \sum_{i=0}^{k-1} x^{4i}$.

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

א. הוכיחו או הפריכו האם C הוא קוד ציקלי.

ב. קודדו את הוקטור $x = (110011)$ למילת קוד ב- C .

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

$$v_1 = (110011101) \quad v_2 = (000101101) \quad v_3 = (110010110)$$

פתרון.

א. כן, זה קוד ציקלי. הרי $x^3 + 1$ מחלק את $x^9 - 1$. 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 $f(x) = x^5 + x^4 + x + 1$. נכפיל אותו ב- x^m ונחסיר את השארית בחלוקה ב- $g(x)$, כפי שעשינו בכיתה:

$$f(x) \cdot x^3 = x^8 + x^7 + x^4 + x^3 = (x^5 + x^4 + x^2 + 1)g(x) + (x^2 + 1)$$

$$f(x) \cdot x^3 - (x^2 + 1) = x^8 + x^7 + x^4 + x^3 + x^2 + 1$$

ולכן מילת הקוד המבוקשת היא (110011101) .

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!