בס"ד

בחינה II

אלפרט יונתן

סווטלנה אברהמי

302609874 260419359

(1) $GF(3^7) \supset GF(3)$

$GF(5^8) \supset GF(5^4) \supset GF(5^2) \supset GF(5^1)$

(4) קוד BCH בינארי $n=15$, $b=3$, $t=2$ ⇐ נסמן α כלשהי שורש הפולינום x^4+x+1 המגדיר את $GF(16)$.

$$H=\begin{pmatrix} 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \dots & \alpha^{11} \\ 1 & \alpha^5 & \alpha^{10} & \dots & \alpha^{10} \\ 1 & \alpha^6 & \alpha^{12} & \dots & \alpha^9 \end{pmatrix} \Rightarrow g(x)=M_{\alpha^3}(x)\cdot M_{\alpha^4}(x)\cdot M_{\alpha^5}(x)=(x^4+x^3+x^2+x+1)(x^4+x+1)(x^4+x+1)$$

ופרמטרי הקוד $[15,5,7]_2$, כל השורשים $\alpha, \alpha^2, \dots, \alpha^6$ (6 שורשים) ובמודולו 2.

(5) $t=3$, $b=11$, הפולינום היוצר כולל את השורשים: $\alpha, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}, \alpha^{15}$ ולכן,

$$g(x)=M_\alpha(x)\cdot M_{\alpha^{11}}(x)\cdot M_{\alpha^{12}}(x)\cdot M_{\alpha^{13}}(x)=(x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$

למערכת ריבוי רב של 9 שורשים $\alpha, \alpha^2, \alpha^3, \dots, \alpha^9$ ⇐ $[15,2,9]_2$

(6) $n=15$, $t=3$, $b=1$ $\alpha \in GF(16)$ שורש של x^4+x+1.

$g(x)=M_\alpha(x)\,M_{\alpha^3}(x)\cdot M_{\alpha^5}(x)$ ⇐ $[15,5,7]$

(7) אי. אוסף הקוד בשדה $GF(2^6)$ הוא 63, דרגת הפולינום היוצר יקבעת עי מספר שורשים, נתון כי: $\alpha^{32}, \alpha^{19}, \alpha^5, 1$ ול מודולים הם שורשים ולכן כדי למצוא את דרגת ושל למצוא את קבוצת המודולים הפולינומיים

$\{\alpha^{38}, \alpha^{19}, \alpha^{41}, \alpha^{52}, \alpha^{26}, \alpha^{13}\}, \{\alpha^{34}, \alpha^{17}, \alpha^{40}, \alpha^{20}, \alpha^{10}, \alpha^5\}, \{\alpha^{21}, \alpha^{42}\}$

סה"כ דרגת הפולינום היוצר הוא: $r=15$

ולסיום קבלנו: $[63, 63-15]$

ב. אוסף הקוד בשדה $GF(8^2)$ הוא 63, רשת קבוצות המודולים המכילות את השורשים. $\alpha^{32}, \alpha^{19}, \alpha^5, 1$ הן:

$\{\alpha^{21}, \alpha^{42}\}, \{\alpha^{26}, \alpha^{19}, \alpha^{52}\}, \{\alpha^{10}, \alpha^5\}, \{1\}$

סה"כ דרגת הפולינום היוצר: $r=7$, ולסיום קבלנו: $[63, 63-7]$

ג. אוסף הקוד בשדה $GF(64)$ הוא 63 ורשת קבוצות המודולים המכילות את השורשים הנתונים הם:

$\{\alpha^{42}\}, \{\alpha^{19}, \alpha^{52}, \alpha^{13}\}$ ולכן דרגת הפה היוצר $r=4$

$[63, 63-4]$

(8) אי. אוסף הקוד בשדה $GF(2^6)$ הוא 63, דרגת הפה היוצר נקבעת לפי מס' שורשים. נתון כי $\alpha^{32}, \alpha^{19}, \alpha^5, 1$ ול המודולים שהם הם שורשים, ולכן כדי למצוא את הקבוצות ושל למצוא את קבוצת המודולים הפולינומיים

$\{\alpha^{32}, \alpha^{16}, \alpha^{8}, \alpha^{4}, \alpha^{2}, \alpha^{1}\}, \{\alpha^{19}, \alpha^{37}, \alpha^{55}, \alpha^{23}, \alpha^{46}, \alpha^{29}\}, \{\alpha^{5}, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}\}$

8 (ק) שורש הרוחב בשדה $GF(64)$ הוא 63, דרגת הפה הולם = מספר שגיאות. נניח ש $\alpha^{8}, \alpha^{15}, \alpha^{21}$ הם שגיאות, אם σ הפולינום שלהם. (מלבד אותו קבוצת הפולינומים הלוגריתמים: $\{1\}, \{\alpha^3\}, \{\alpha^5\}, \{\alpha^{21}\}$

סה"כ $V = \deg(g) = 4$, [63,63-4] זו הוא סדרת RS ולכן הפסד בכל כמות בלוק רוב.

3 (ב) נחשב את S_0 ו- S_1:

$$Y(x) = x^{14}+x^{13}+x^{11}+x^{10}+x^{7}+1$$

$$S_0 = Y(\alpha) = \alpha^{14}+\alpha^{13}+\alpha^{11}+\alpha^{10}+\alpha^{7}+1 = \cancel{\alpha^7}+\cancel{\alpha^6}+\cancel{\alpha}+\cancel{\alpha^2}+\cancel{\alpha^3}+\alpha+1 = \alpha^{10}$$

$$S_1 = Y(\alpha^3) = \alpha^{12}+\alpha^{9}+\alpha^{3}+\cancel{\alpha}+\alpha^{6}+\cancel{\alpha^3} = \cancel{\alpha^6}+\cancel{\alpha^5}+\cancel{\alpha^4}+1+\cancel{\alpha^3} = 1$$

קיבלנו ש $S_0 = \alpha^{10} \neq 0$, ולכן $S_1 = 1 = S_0^3$ ולכן שגיאה אחת במקום.

לכן ולכן המילה הוא פונקציה הזו:

$$\hat{c}(x) = Y(x) - x^{10} = x^{14}+x^{13}+x^{11}+x^{7}+1$$

2

$$Y(x) = x^{11}+x^{9}+x^{6}+x^{3}+x^{2}$$

$$S_0 = Y(\alpha) = \alpha^{11}+\alpha^{9}+\alpha^{6}+\alpha^{3}+\alpha^{2} = \alpha^2$$

$$S_1 = Y(\alpha^3) = \cancel{\alpha^{33}}+\alpha^{27}+\cancel{\alpha^{18}}+\alpha^{9}+\alpha^{6} = \cancel{\alpha^6}+1+\alpha^3 = \alpha^{14}$$

?

קיבלנו $S_0 = \alpha^2 \neq 0$ ואם $S_1 = \alpha^{14} \neq S_0^3$ ולכן (בגלל פולינום מעגלי הנשלח):

$$\Lambda(x) = x^2 + S_0 x + \left(\frac{S_1}{S_0} + S_0^2\right) = x^2 + \alpha^2 x + \left(\alpha^{14} + \alpha^4\right) = x^2 + \alpha^2 x + \alpha^{10}$$

$\Lambda(\alpha) = 0$ $\Lambda(\alpha^5) = 0$

$$e(x) = x + x^5 \Rightarrow c(x) = Y(x) - e(x) = x^{11}+x^{9}+x^{6}+x^{5}+x^{3}+x^{2}+x$$

2

$$Y(x) = x^{14}+x^{11}+x^{10}+x^{9}+x^{6}+x^{5}$$

$$S_0 = \alpha^{14}+\alpha^{11}+\alpha^{10}+\alpha^{9}+\alpha^{6}+\alpha^{5} = \cancel{\alpha^7}+\cancel{\alpha^6}+\cancel{\alpha^5} = 0$$

הסינדרום = 0 ולכן $Y(x) = c(x)$

$$S_1 = \cancel{\alpha^{21}}+\cancel{\alpha^{18}}+1+\cancel{\alpha^{12}}+\cancel{\alpha^{9}}+1 = 0$$

$$Y(x) = x^{14}+x^{13}+x^{10}+x^{7}+x^{6}+x^{2}$$

3

$$S_0 = \alpha^{14}+\alpha^{13}+\alpha^{10}+\alpha^{7}+\alpha^{6}+\alpha^{2} = \cancel{\alpha^7}+\cancel{\alpha^6}+\cancel{\alpha^2} = 0$$

קיבלנו $S_0 = 1 \neq 0$ ואם $S_1 = \alpha^6 \neq S_0^3$

$$S_1 = \alpha^{12}+\alpha^{9}+1+\cancel{\alpha^{6}}+\alpha^{3}+\cancel{\alpha^{6}} = \alpha^2+1+\alpha^3 = \alpha^6$$

?

$$\Lambda(x) = x^2 + S_0 x + \left(\frac{S_1}{S_0} + S_0^2\right) = x^2 + x + (\alpha^6 + 1) = x^2 + x + \alpha^{13}$$

$\alpha^{8}+\alpha^{3}+\alpha^{13}$ $\alpha^{9}+\alpha^{3}+\alpha^{13}$ $\alpha^{8}+\alpha^{5}+\alpha^{13}$ $\alpha^{6}+\alpha^{12}+\alpha^{13}$

$\alpha^{12}+\alpha^{9}+\alpha^{13}$ $\alpha^{8}+\alpha^{4}+\alpha^{13}$ $\alpha^{7}+\alpha^{14}+\alpha^{13}$

$\alpha^{13}+\alpha^{11}+\alpha^{13}$ $\alpha^{11}+\alpha^{7}+\alpha^{13}$ $\alpha^{10}+\alpha^{5}+\alpha^{13}$

$\alpha^{14}+\alpha^{13}+\alpha^{13}$

קיבלנו $S_0 = 0$ ו $S_1 \neq 0$ ולכן אפשר לפענח את המילה.

בס"ד

בקרה 11. אלפרט ונעמה.

(2) נחפש m כך ש: $20 \mid 3^m - 1 \Leftarrow \boxed{m=4}$ ונקבל $b=0$, $t=3 \Leftarrow d=7$ מינימלי, מאפשר.

רוצים נמצא רוטס בקלוטומי: $\{1,3,9,7\}, \{2,6,18,14\}, \{4,12,16,8\}$ וגם

$\{5,15\}, \{10\}, \{11,13,19,17\}$

לכן בשביל 20 שורות - נבחר בכל מה קטן - יהיה פחות:

$$H = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{19} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{38} \\ \cancel{1} & \cancel{\alpha^3} & \cancel{\alpha^6} & \cancel{\alpha^9} & & \cancel{\alpha^{57}} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \cdots & \alpha^{76} \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \cdots & \alpha^{95} \end{pmatrix} \Rightarrow H = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{19} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{38} \\ 1 & \alpha^4 & \alpha^8 & \cdots & \alpha^{76} \\ 1 & \alpha^5 & \alpha^{10} & \cdots & \alpha^{95} \end{pmatrix}$$

$$g(x) = \mathrm{LCM}(M_{\alpha^0}, M_{\alpha^1}, M_{\alpha^2}, M_{\alpha^3}, M_{\alpha^4}, M_{\alpha^5})$$

$$= (x-1)(x-\alpha)(x-\alpha^3)(x-\alpha^9)(x-\alpha^7)\cdot(x-\alpha^2)(x-\alpha^6)(x-\alpha^{18})(x-\alpha^{14})(x-\alpha^4)(x-\alpha^{12})(x-\alpha^{16})(x-\alpha^8)(x-\alpha^5)(x-\alpha^{11})(x-\alpha^{15})$$

דרגת $g(x) = 15$ ולכן $r=15$.

(ב) $d=7$ אפשרי, אבל בפועל צריך $d=9$ כי חייבים לקחת את 3 α שנמצאים בשורה רוטס בקלוטומי. $\alpha^0 \ldots \alpha^{16}$

(ג) הקוד $R=\frac{k}{n}$ ולכן $R=\frac{5}{20}=\frac{1}{4}$

(ד) אם היינו בוחרים $b=7$, אז היינו לוקחים את השורשים: $\alpha^7 - \alpha^{12}$

והיינו משיגים: $g(x) = M_{\alpha^7} \cdot M_{\alpha^8} \cdot M_{\alpha^{10}} \cdot M_{\alpha^{11}}$

ודרגת $g(x)$ הינה 13, ולכן $k=7$, והקוד המשופר הוא $R=\frac{7}{20}$ מ.ש.ל.