מבוא לתורת הקודים - תרגיל 7

שאלה 1

ב. $GF(2^4)$ מוכלים השדות $GF(2^2)$! $GF(2)$

ג. $GF(2^7)$ אינו השדה $GF(2)$

ד. $GF(2^6)$ מוכלים השדות $GF(2^2)$, $GF(2^3)$, $GF(2)$.

שאלה 2

חלוקה לקבוצות צמודות של $GF(2^6)$

$\{1\}$

$\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}\}$

$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}\}$

$\{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}\}$

$\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}\}$

$\{\alpha^9, \alpha^{18}, \alpha^{36}\}$

$\{\alpha^{11}, \alpha^{22}, \alpha^{44}, \alpha^{25}, \alpha^{50}, \alpha^{37}\}$

$\{\alpha^{13}, \alpha^{26}, \alpha^{52}, \alpha^{41}, \alpha^{19}, \alpha^{38}\}$

$\{\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{57}, \alpha^{51}, \alpha^{39}\}$

$\{\alpha^{21}, \alpha^{42}\}$

$\{\alpha^{23}, \alpha^{46}, \alpha^{29}, \alpha^{58}, \alpha^{53}, \alpha^{43}\}$

$\{\alpha^{27}, \alpha^{54}, \alpha^{45}\}$

$\{\alpha^{31}, \alpha^{62}, \alpha^{61}, \alpha^{59}, \alpha^{55}, \alpha^{47}\}$

- הפולינום המינימלי של α $\quad M_\alpha(x) = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{32}) = x^6+x+1$
- הפולינום המינימלי של α^2 נתון לפולינום המינימלי של α, כי שניהם בעלים קבוצת צמודות זהה
- הפולינום המינימלי של α^3 $\quad M_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{48})(x-\alpha^{33})$
- הפולינום המינימלי של α^9 הינו פולינום אי פריק מדרגה 3 ולכן ישנם שתי אפשרויות: $f(x)=x^3+x+1$ או $f(x)=x^3+x^2+1$ כאשר אלו הם $x=\alpha^9$ ידוע שהינו מאופס על $f(x)=x^3+x^2+1$ ולכן זהו הפולינום המינימלי שלו.
- הפולינום המינימלי של α^{42} הינו פולינום אי פריק מדרגה 2 ולכן $M_{\alpha^{42}}(x)=x^2+x+1$
- הפולינום המינימלי של 1 הינו $M_{\alpha^0}(x)=x+1$

שאלה 3

חלוקת $GF(64)$ לקבוצות צמודות מעל $GF(8)$

מתלקים לפי קבוצות צמודות מעל $GF(2)$
8 איברים בכל אחת.

$\{1\}$

$\{\alpha, \alpha^8\}$	$\{\alpha^2, \alpha^{16}\}$	$\{\alpha^4, \alpha^{32}\}$
$\{\alpha^3, \alpha^{24}\}$	$\{\alpha^6, \alpha^{48}\}$	$\{\alpha^{12}, \alpha^{33}\}$
$\{\alpha^5, \alpha^{40}\}$	$\{\alpha^{10}, \alpha^{17}\}$	$\{\alpha^{20}, \alpha^{34}\}$
$\{\alpha^7, \alpha^{56}\}$	$\{\alpha^{14}, \alpha^{49}\}$	$\{\alpha^{28}, \alpha^{35}\}$
$\{\alpha^9\}$	$\{\alpha^{18}\}$	$\{\alpha^{36}\}$
$\{\alpha^{11}, \alpha^{25}\}$	$\{\alpha^{22}, \alpha^{50}\}$	$\{\alpha^{44}, \alpha^{37}\}$
$\{\alpha^{13}, \alpha^{44}\}$	$\{\alpha^{26}, \alpha^{19}\}$	$\{\alpha^{52}, \alpha^{38}\}$
$\{\alpha^{15}, \alpha^{53}\}$	$\{\alpha^{30}, \alpha^{51}\}$	$\{\alpha^{60}, \alpha^{39}\}$
$\{\alpha^{21}\}$	$\{\alpha^{42}\}$	
$\{\alpha^{23}, \alpha^{58}\}$	$\{\alpha^{46}, \alpha^{53}\}$	$\{\alpha^{29}, \alpha^{43}\}$
$\{\alpha^{27}\}$	$\{\alpha^{54}\}$	$\{\alpha^{45}\}$
$\{\alpha^{31}, \alpha^{59}\}$	$\{\alpha^{62}, \alpha^{55}\}$	$\{\alpha^{61}, \alpha^{43}\}$

שאלה 5

קוד BCH כאלה כי.

נסמן ב M_{α^i} את הפולינום המינימלי
של α^i

נחלק את המחלקות לקבוצות 3 מוגדרות

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\} \longrightarrow M_\alpha$$
$$\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\} \longrightarrow M_{\alpha^3}$$
$$\{\alpha^5, \alpha^{10}\} \longrightarrow M_{\alpha^5}$$
$$\{\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}\} \longrightarrow M_{\alpha^7}$$

$t=1 \longrightarrow M_\alpha \longrightarrow [15, 11, 3]$

$t=2 \longrightarrow M_\alpha M_{\alpha^3} \longrightarrow [15, 7, 5]$

$t=3 \longrightarrow M_\alpha M_{\alpha^3} M_{\alpha^5} \longrightarrow [15, 5, 7]$

$\left.\begin{array}{l} t=4 \\ t=5 \\ t=6 \\ t=7 \end{array}\right\} \longrightarrow M_\alpha M_{\alpha^3} M_{\alpha^5} M_{\alpha^7} \longrightarrow [15, 1, 15]$

שאלה 7

קוד BCH בשדה באורך 15 על $GF(4)$. $t=1$:

$$H = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{14} \\ 1 & \alpha^2 & \dots & \alpha^{13} \end{pmatrix}$$

$$g(x) = M_\alpha(x)\, M_{\alpha^2}(x) = \left((x-\alpha)(x-\alpha^4)\right)\left((x-\alpha^2)(x-\alpha^8)\right) = x^4+x+1$$

פרמטרי הקוד $[15, 11, 5]$ מספר מילות הקוד 4^{11} .

מילות קוד :

$$c(x) = 0$$
$$c(x) = 2\, g(x) = 2x^4+x+1$$
$$c(x) = (2x+3)\, g(x)$$

שאלה 8

קוד RS באורך 31 יכולת תיקון של שגיאה אחת

הקוד מוגדר מעל $GF(32)$ ($GF(2^5)$)

כאשר α הוא שורש הפולינום x^5+x^2+1

$$H = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{30} \\ 1 & \alpha^2 & & \end{pmatrix}$$

$$g(x) = (x-\alpha)(x-\alpha^2) = x^2+\alpha^{19}x+\alpha^3$$

פרמטרי הקוד $[31, 29, 3]$.

מילות קוד

$$c(x) = g(x)$$
$$c(x) = \alpha^7\, g(x)$$
$$c(x) = (x^{13}+\alpha^{14}x^7+\alpha^2x+\alpha^{25})\, g(x)$$

שאלה 9

קוד בינארי ציקלי באורך 15 ומימד 9 $\Longrightarrow$ פולינום יוצר מדרגה $15-9=6$.

פולינום היוצר שורשים α^9 ! יש לכם הרי מתחלק בפולינום המינימלי שלה

$$M_{\alpha^5} = x^2+x+1 \mid g(x)$$
$$M_{\alpha^9} = x^4+x^3+x^2+x+1 \mid g(x)$$
$$\Longrightarrow g(x) = M_{\alpha^5}(x)\cdot M_{\alpha^9}(x)$$

ולכן $\deg(g(x)) = 6$.