קודים מתקני שגיאות

(1) (27/2/13)

kunyav@gmail.com

פרופ' בוריס קוניאבסקי

חדר 9, בניין 216

חומר פתוח בבחינה

צריך לדעת:

1) שדות סופיים

2) חוגים – חוגי פולינומים/אידיאלים

בקורס נתמקד בקודים מתקני שגיאות

דוגמות

1) רוצים לשדר תשובה כן/לא, מבלי שהיא תשתבש בדרך. אפשר לשדר את התשובה פעמים רבות, כך שגם יש רעש התוצאה הסופית תתקבל בקלות.

$$\underbrace{111\cdots1}_{100 \text{ פעמים}} \longmapsto 10111101\cdots01$$

1 – 68 פעמים

0 – 32 פעמים

קיבלנו ש-1 מופיע יותר פעמים, ולכן בשלב הפענוח נחליט שהמקור שהועבר הוא 1.

אבל מה אם הרעש גדול ונקבל בתוצאה יותר אפסים מאחדים? נרצה לדרוש שהשגיאה תקרה בהסתברות נמוכה.

אבל בשיטה זו יש בעיה – לוקח יותר זמן וגם יותר כסף? (יותר משאבים להעביר).

במקרה שלנו, נאמר שקצב הקוד הנו $R=\frac{1}{100}$

זה נמוך!

סוג קוד זה קרוי קוד עם חזרות.

2) נניח שרוצים להעביר מספר ביטים באורך n: $a_1\cdots a_n$, נוסיף למסר (בסוף) סימן a_{n+1} שיהיה

$$a_{n+1}=a_1+\dots+a_n \pmod 2$$

ונשדר את $a_1\cdots a_n a_{n+1}$.

נשדר את הקוד ונקבל

$$\alpha_1\cdots\alpha_n\alpha_{n+1} \longmapsto \alpha'_1\cdots\alpha'_n\alpha'_{n+1}$$

נחשב $S=\alpha'_1+\dots+\alpha'_n+\alpha'_{n+1}$.

אם $S=1$ $\Leftarrow$ יש שגיאה (שכן $\alpha_1+\dots+\alpha_n+\alpha_{n+1}\equiv 0$ מודולו 2).

קוד זה מגלה שגיאה אחת (כלשהי) אבל לא אומר מה: אם הקוד החזיר שגיאה, ניתן לבקש, למשל, שידור חוזר של הקוד.

קצב הקוד יהיה $R=\frac{n}{n+1}$, כלומר הקצב גבוה אבל היכולת לתקן השגיאות נמוכה בניגוד למה שהיה בקוד הקודם.

זהו קוד עם בדיקת זוגיות.

3) נניח שנרצה לשדר מסר באורך 9 $\alpha_1\alpha_2\cdots\alpha_9$.

נבנה מטריצה מהצורה:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \beta_1 \\ \alpha_4 & \alpha_5 & \alpha_6 & \beta_2 \\ \alpha_7 & \alpha_8 & \alpha_9 & \beta_3 \\ \beta_4 & \beta_5 & \beta_6 & \beta_7 \end{pmatrix}$$

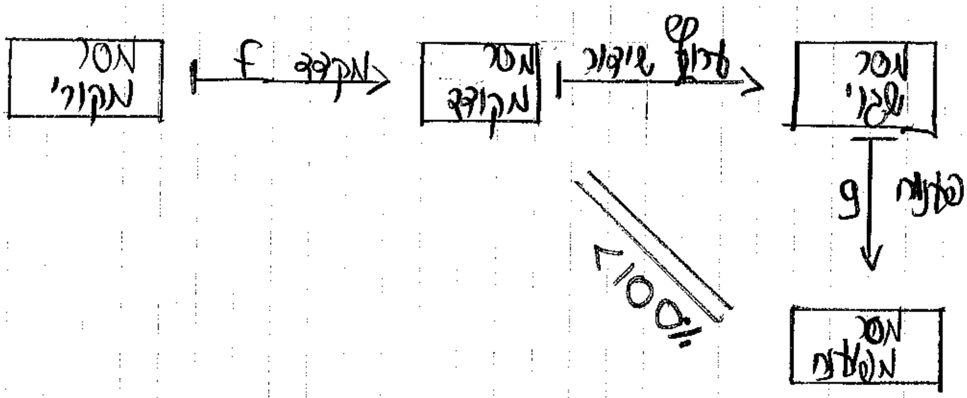
$\beta_1-\beta_3$: סכום שורה מודולו 2

$\beta_4-\beta_7$: סכום עמודה מודולו 2

תרגיל: הראה שקוד זה מסוגל למצוא שתי שגיאות ולתקן שגיאה אחת.

לגבי קוד זה מתקיים $R=\frac{9}{16}$. יש קודים יעילים יותר שמסוגלים לתקן שגיאה אחת.

סכמה כללית של קידוד



נרצה שוויון בין המסר המקודד למסר המפוענח, אבל זה לא קורה בהסתברות של 100%.

הגדרות

A – א"ב: קבוצה סופית של אותיות שנעביר, ונסמן $|A|=q$.

M_k – קב' מסרים מקוריים (מאותיות A) מאורך k, $|M_k|=q^k$.

C – אוסף של מסרים מקודדים מאורך n, $k<n$, מתקיים $C\subsetneq M_n$.

(למשל, בדוגמה הטריוויאלית שנתנו $C=\{\underbrace{00\ldots0}_{100\text{ פעמים}},\underbrace{11\ldots1}_{100\text{ פעמים}}\}$).

נרצה $|C|=q^k$.

$f: M_k\to C$ – העתקת קידוד, שהיא חח"ע.

$g: M_n\to C$ – העתקת פענוח, ונרצה שאם $x\in C$ אז $x=g(x)$.

מרחק המינג

הגדרה

יהיו $x,y\in M_n$: $x=(x_1\ldots x_n)$; $y=(y_1\ldots y_n)$

נגדיר
$$d(x,y)=|\{i: x_i\neq y_i\}|$$

זהו המרחק מהמילה x למילה y.

תכונות

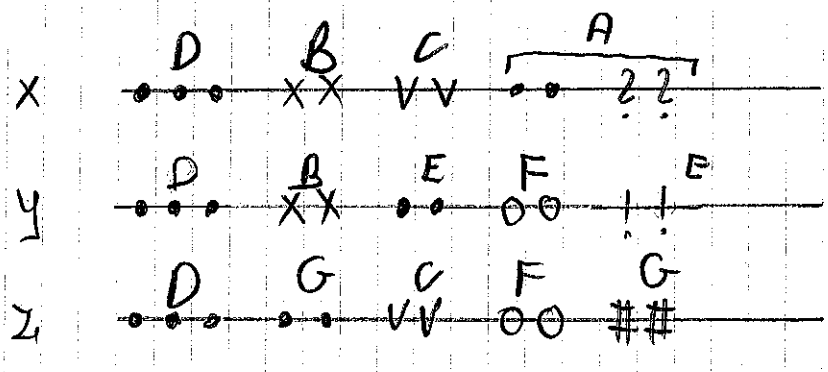
1) $d(x,y)\geq 0$ וגם $d(x,y)=0$ אמ"מ $x=y$.

2) $d(x,y)=d(y,x)$

3) $d(x,y)+d(y,z)\geq d(x,z)$

הוכחת תכונה 3

בה"כ, נניח שכל מופעי האותיות שמשותפים לשלוש המילים בהתחלה, ונמיין את x,y,z בצורה הבאה



נחלק כל מילה לאזורים [illegible] מרחקיים

x:

אזור	A	B	C	D
מופיע ב	x	x,y	x,z	x,y,z

$A+B+C+D=n$

y:

אזור	E	B	F	D
מופיע ב	y	x,y	y,z	x,y,z

$E+B+F+D=n$

z:

אזור	G	C	F	D
מופיע ב	z	x,z	y,z	x,y,z

$G+C+F+D=n$

מרחקים:

$d(x,y)=A+C=E+F$

$d(y,z)=E+B=G+C$

$d(x,z)=A+B=G+F$

$\Downarrow$

$$d(x,y)+d(y,z)=A+C+E+B\geq A+B=d(x,z)$$

הגדרה

1) תת קב' $C\subseteq M_n$ מגודל q^k ($k\leq n$) נקרא קוד.

2) יהי $C\subseteq M_n$ קוד. נגדיר $d(C)=\min_{\substack{x,y\in C\\ x\neq y}} d(x,y)$

$d(C)$ נקרא המרחק המינימלי של C.

משפט

אם C קוד עבורו $d(C)>2t$ (t הגדול ביותר המתאים), אזי C יכול לתקן עד t שגיאות.

הוכחה

אם $x,y\in C$, שונים אזי $d(x,y)\ge 2t+1$. נניח ששודרה מילה x,
ונסמן את מס' השגיאות בשידור ב-r_x, ונניח $r_x\le t$,
נסמן ב-z את המילה המתקבלת אזי $d(x,z)=r_x\le t$.
נציג אלגוריתם שמקבל כקלט את z ומחזיר את x:
ואכן, הרי $y\in C$ כלשהי שאינה x.
נשים לב שמתקיים: $2t+1\le d(x,y)\le d(x,z)+d(z,y)\le t+d(z,y)$

$$t+1\le d(z,y)$$

קיבלנו שמתקיים $\begin{cases} d(x,z)\le t \\ d(z,y)\ge t+1 \end{cases}$ לכל $x\ne y\in C$;

לכן לכל $x\ne y\in C$: $d(z,x)<d(z,y)$

ולכן אפשר למצוא את x ע"י מעבר על כל מילות C, ומציאת מינימום.

הערה

זה לא אלגוריתם טוב כי הסיבוכיות היא q^k (אקספוננציאלי)

(*) כמו כן, אם $d(C)=2t$ אזי הקוד C לא יכול לתקן t שגיאות:

אם $d(C)=2t$ אז קיימות $x\ne y\in C$ כך ש $d(x,y)=2t$

$$x=(x_1\cdots x_t\, x_{t+1}\cdots x_{2t}\, x_{2t+1}\cdots x_n)$$

$$y=(\underbrace{y_1\cdots y_t\, y_{t+1}\cdots y_{2t}}_{\text{טורים שונים}}\, \underbrace{y_{2t+1}\cdots y_n}_{\text{טורים זהים}})$$

נתבונן במילה $z=(x_1\dots x_t\, y_{t+1}\dots y_{2t}\, x_{2t+1}\dots x_n)$

$\Rightarrow d(z,x)=t$ וגם $d(z,y)=t$

ולכן לא נוכל לפענח את z.

פרמטרים של קוד

נסמן, אם C הוא קוד, $|C|=q^k$ עם מרחק מינ' d: $C=[n,k,d]_q$

נגדיר גם: $R=\frac{k}{n}$ קצב

$\delta=\frac{d}{n}$ מרחק מינימלי יחסי

⊛ יהיו q,n,M נתונים, כדי שיהיה כמה שיותר קל לתקן ⇐ נרצה d גדול.

⊛ יהיו q,n,d נתונים, ונרצה את הקצב הטוב ביותר (כדי להבטיח כמה שפחות כפל) ⇐ נרצה M גדול.

⊛ יהיו q,n,d נתונים, באותו אופן נרצה n קטן.

בעיות אסימפטוטיות

מציאות ערכי הפרמטרים היחסיים R,δ כאשר $n\to\infty$:

נרצה למצוא $\delta\to\delta_0$ $\quad R\to R_0$

נרצה R_0,δ_0 גדולים (קצב גדול ומרחק יחסי גדול).

זה קשה, לכן מה שנרצה זה לבנות משפחות של קודים בהן $\delta_0\neq 0$ $\quad R_0\neq 0$

דוגמאות

1) בקוד עם n חזרות: $R=\frac{1}{n}\to 0$; $\delta=1$

2) בקוד עם בדיקת זוגיות: $R=\frac{n}{n+1}\to 1$; $\delta=\frac{2}{n+1}\to 0$

ושני אלו לא מקיימים [illegible] קשה למצוא כאלו קודים,

קודים מתקני שגיאות

F – ש״ב. קוד C הוא $C\subset F^n$, ונניח $|C|=q^k$ כאשר $q=|F|$.

$$d(C)=\min\{d(x,y) \mid x,y\in C \text{ שונות}\}$$

$R=\frac{k}{n}$ קצב, $\delta=\frac{d}{n}$

אם $d\geq 2t+1$ (t מקסימלי), אז C יכול לתקן עד t שגיאות.

$\Leftarrow$ האלגוריתם שהראנו הוא אקספוננציאלי, וזה לא טוב.

⊛ נניח שהש״ב F הוא שדה סופי מגודל q: $F=\mathbb{F}_q$

עוד נניח שC מ״ו מעל $\mathbb{F}_q$.

תזכורת

V ״קטר מ״ו אם מוגדרות עליו שתי פעולות: חיבור וקטורים, כפל בסקלר

כך שמתקיימות האקסיומות הבאות:

1) $u+v=v+u$
2) $(u+v)+x=u+(v+x)$
3) קיים $0\in V$ כך שלכל $v\in V$: $v+0=v$
4) לכל $v\in V$ קיים $-v\in V$ כך ש $v+(-v)=0$
5) $1\cdot v=v$
6) $(\alpha+\beta)v=\alpha v+\beta v$
7) $\alpha(u+v)=\alpha u+\alpha v$

שדות סופיים

1) שדה בן q איברים קיים אם״ם $q=p^t$ (p ראשוני, $t\geq 1$).

2) לכל $q=p^t$ קיים שדה יחיד $\mathbb{F}_q$ עד כדי איזומורפיזם (מעביר סכום לסכום, מכפלה למכפלה, 0 ל-0, 1 ל-1 (והפוך))

דוגמא $q=p$ ראשוני, נקח: $\mathbb{F}_p=\{\bar{0},\bar{1},\bar{2},\dots,\overline{p-1}\}$

(שדה מודולו). $\bar{a}+\bar{b}=\overline{a+b}$ $\bar{a}\cdot\bar{b}=\overline{ab}$

3) אם $\mathbb{F}$ שדה כלשהו, אז $\mathbb{F}[x]$ חוג ראשי, כלומר:

כל אידיאל A של $\mathbb{F}[x]$ הוא אידיאל ראשי: $A=(f)$.

אידיאל - בהנתן R חוג, $A\subset R$ יקרא אידיאל אם:

א. A חבורה חיבורית

ב. לכל $a\in A$ ולכל $r\in R$ מתקיים $ra\in A$.

למשל: $R=\mathbb{Z}$, $A=2\mathbb{Z}$.

כמו כן, $A=(f)$ אם לכל $a\in A$ קיימת הצגה $a=gf$ כאשר $g\in F[x]$ כלשהו.

4) נתבונן בחוג $R=\mathbb{F}[x]/(x^n-1)$ (עבור חוג מנה,
למשל אם $R=\mathbb{Z}$, $A=p\mathbb{Z}$ $\Leftarrow$ $R/A=\mathbb{F}_p$) עבור p ראשוני,

למעשה, איברי $\mathbb{F}[x]/(f)$: הפולינומים g,h "יקראו" שקולים אם"ם $h-g$ מתחלק ב-f ללא שארית.

דוגמה

$R=\mathbb{F}[x]/(x^3-1)$; $g=x+1$ $h=x^3+x$

$g-h=1-x^3 \Rightarrow g\sim h$.

במקרה כזה, R חוג ראשי: לכל אידיאל קיים וקטור f $A=(f)$ המקיים גם $f|(x^n-1)$.

5) יהי $F=\mathbb{F}_p$, ויהי $g\in F[x]$ אי פריק מעלה t
(אז g יקרא פריק אם"ם קיימים h_1,h_2 מעלות שונות מ-0 עבורם $g=h_1h_2$).

עובדה: $\mathbb{F}_p[x]/(g)$ שדה מגודל p^t.

תרגיל

מצאו פולינום אי פריק $g\in\mathbb{F}_2[x]$ מעלה 3 ומצאו לוח חיבור וכפל ל-$\mathbb{F}_8$.

נזכר שמצאנו לכל $g=p^t$ פולינום אי פריק $g\in\mathbb{F}_p[x]$ מעלה t
כך שקיים l של המקדמים השונים מאפס, מינימלי: $l=l(p,t)$
זה יקרא הוום כאשר $t\to\infty$: $l\to\infty$.

6) $(\mathbb{F}_q,+)\cong\mathbb{F}_p^t$ משום כך מ"ו מעל $\mathbb{F}_p$ ממימד t.

דוגמה $(\mathbb{F}_8,+)=span\{1,x,x^2\}$

7) $(\mathbb{F}_q\setminus\{0\},\cdot)$ היא חבורה ציקלית, כלומר קיים $g\in\mathbb{F}_q$ כך שלכל $0\neq f\in\mathbb{F}_q$ מתקיים $f=g^m$

$$\Rightarrow\mathbb{F}_q=\{0,1,g,\dots,g^{p-2}\}$$

g כנ"ל יקרא איבר פרימיטיבי של $\mathbb{F}_q$.

8) יהיו $\mathbb{F}_{p^t}$, $\mathbb{F}_{p^s}$; כך ש- $s<t$.
אם $\mathbb{F}_{p^s}\subset\mathbb{F}_{p^t}$ אזי $s|t$, ולהפך.

9) אם $q=p^t$, $F=\mathbb{F}_q$. אזי לכל $a,b\in F$ מתקיים $(a+b)^p=a^p+b^p$

לכן $f\in\mathbb{F}_q[x]$ אזי $(f(x))^q=f(x^q)$

קודים לינאריים

הגדרה:

אם $F=\mathbb{F}_q$ שדה סופי בן q איברים, ויהי $C\subset\mathbb{F}_q^n$ תת מרחב וקטורי, אם $\dim_{\mathbb{F}_q}C=k$, נאמר ש-C קוד לינארי ממימד k.

כמו כן, לכל $x\in\mathbb{F}_q^n$; $x=(x_1,x_2,\dots,x_n)$, נגדיר את המשקל של x ע"י

$$w(x)=|\{i|x_i\neq 0\}|$$

הערה

אם C קוד לינארי, אזי $d(C)=\min\{w(x)|0\neq x\in C\}$

הוכחה

$$d(C)=\min_{\substack{x,y\in C\\ x\neq y}} d(x,y)$$

כמו כן $d(x,y)=w(x-y)$ וממ"ו הטענה מתקבלת.

שתי שיטות להגדרת C:

1) יהי $B=\{e_1,\dots,e_k\}$ בסיס ל-C: $e_i=(a_{i1},\dots,a_{in})$; $a_{ij}\in\mathbb{F}_q$

$$G=\begin{pmatrix} — e_1 — \\ \vdots \\ — e_n — \end{pmatrix}$$

נקרא למטריצה יוצרת של C.

אם $x\in C$, אזי x ניתן להצגה יחידה

$$x=\alpha_1 e_1+\dots+\alpha_n e_n=(\alpha_1,\dots,\alpha_k)G$$

דוגמה

1) קוד עם חזרות: $q=2$, $k=1$, $C=\{(00\dots0),(11\dots1)\}\subset\mathbb{F}_2^n$

$B=\{(11\dots1)\}\Leftarrow$ $G=(11\dots1)$

2) קוד עם בדיקת זוגיות $C=\{(x_1,\dots,x_{n-1},x_n)\mid x_1+\dots+x_n=0\}\subset\mathbb{F}_2^n$

כאן $q=2$, $k=n-1$

$$e_i=(0,\dots,\underset{i}{1},\dots,0,1)$$

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

<u>שיטה שנייה</u>

2) הגדרה

תהי H מטריצה מגודל $n\times(n-k)$ מעל שדה $\mathbb{F}_q$, מדרגה $n-k$.

נסמן גם ב-H העתקה: $H:\mathbb{F}^n\longrightarrow\mathbb{F}^{n-k}$

ע"י $x\longmapsto Hx^t$

נסמן $C=\ker(H)\subset\mathbb{F}^n$ $\Leftarrow$ $C=\{x\in\mathbb{F}^n\mid Hx^t=0\}$

$\dim C=k$

H נקראת מטריצת הבדיקה של הקוד C.

דוגמה

1) יהי C קוד עם בדיקת זוגיות, $H=(1,1,\dots,1)$

2) C קוד עם חזרות: $C=\{(0,0,\dots,0),(1,1,\dots,1)\}$

הנוסחה היא $x_1=x_2=\dots=x_n$

נפרק ל-$n-1$ משוואות: $x_i-x_n=x_i+x_n=0$ (שדה בינארי)

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

משפט

אם C קוד ליניארי, G מטריצה יוצרת ו-H מטריצת בדיקות, אזי

מתקיים: $G_{k\times n}H^t_{n\times(n-k)}=0$

הוכחה

שורה $x\in C \iff Hx^t=0 \iff xH^t=0$

לכן מתקיים גם ל- $x=e_i$ $(1\le i\le k) \Leftarrow e_iH^t=0$

$$\Downarrow$$

$GH^t=0$ כנדרש

(3) (13/3/13)

קודים לינאריים

קוד המינג

סימון קוד ליניארי q-ארי: $[n,k,d]_q$

נרצה לבנות קוד המתקן שגיאה אחת: צריך $d\ge 3$

הכי נוח כבר דוגמא לקוד עם $n=?, k=4, q=2, d=3$

נשפר אותו:

(*) אם $n=5$ מוסיפים רק סימן אחד ⇐ קוד לבדיקת זוגיות כי $d=2$, ולא זה לא מתאים.

(*) אם $n=6$ זה בלתי אפשרי (נוכיח בהמשך).

נבנה דוגמא עם $n=7$:

נתחיל מ-a_1,a_2,a_3,a_4 (נגדיר עבור הקידוד)

$$a_5:=a_2+a_3+a_4$$
$$a_6:=a_1+a_3+a_4$$
$$a_7:=a_1+a_2+a_4$$

עבור הפענוח: נסמן המילה המתקבלת $a_1',\dots,a_7'$

נחשב את סדרת הביטויים הבאים:

$$z_1:=a_4'+a_5'+a_6'+a_7'$$
$$z_2:=a_2'+a_3'+a_6'+a_7'$$
$$z_3:=a_1'+a_3'+a_5'+a_7'$$

טענה: נסמן $\bar{z}=(z_3,z_2,z_1)$, אזי: (נניח שהעברה בערוץ הכרה לכל היותר שגיאה אחת)

א. $\bar{z}=\bar{0}$ אמ"מ אין שגיאות

ב. אם $\bar{z}$ כבסיס הצגה הבינארית של מס' שהוא ב-$[1,7]$ אזי השגיאה במקום ה-z.

הוכחה

א. $z_1=0$ ⇐ אין שגיאות ב- a_4,a_5,a_6,a_7

$z_2=0$ ⇐ אין שגיאות ב- a_2,a_3,a_6,a_7

$z_3=0$ ⇐ אין שגיאות ב- a_1,a_3,a_5,a_7

⇐ אין שגיאות בכלל. בכיוון ההפוך ברור.

ב. נניח $s=2$ השאר באותו אופן:

$S_1=0 \Rightarrow$ אין שגיאה ב- a_4,a_5,a_6,a_7

$S_2=1 \Rightarrow$ יש שגיאה באחד מ- a_2,a_3,a_6,a_7

$S_3=0 \Rightarrow$ אין שגיאה ב- a_1,a_3,a_5,a_7

$\Downarrow$

יש שגיאה ב- a_2.

תיאור הקוד בעזרת מטריצה

$$G_{4\times7}=\begin{pmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{pmatrix}$$

נחשב את $H_{3\times7}$, אפשר בשתי דרכים;

א. ממשפט $GH^t=0$ (עשה צורת הבית)

ב. $C=\{x \mid Hx^t=0\}=\{x \mid a_4+a_5+a_6+a_7=a_2+a_3+a_6+a_7=a_1+a_3+a_5+a_7=0\}$

$\Downarrow$

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

משפט

יהי C קוד לינארי ותהי H מטריצת הבדיקות שלו. אזי $d_C \geq s+1$ אם"ם כל s עמודות של H בת"ל.

הוכחה

($\Leftarrow$) נניח בשלילה שב-H יש s עמודות ת"ל, ונניח $s \geq d_C$. נניח בה"כ s העמודות הראשונות ת"ל;

$$a_1v_1+a_2v_2+\dots+a_sv_s=0 \qquad (\exists i: a_i\neq 0)$$

נגדיר $0\neq x\in C$ עבורו $w(x)\leq s$; $0\neq x=(a_1\ a_2 \dots a_s\ 0\ 0 \dots 0)$

מתקיים $Hx^t=0 \Rightarrow x\in C$ וברור $w(x)\leq s$ בניגוד הנדרש.

($\Leftarrow$) נניח בשלילה שקיים $0\neq x\in C$ עבורו $w(x)\leq 2$ אזי
נניח בה"כ $x=(x_1, x_2, 0 \dots 0)$, ובאותו אופן נקבל הנדרש.

מסקנה
אם C קוד לינארי בינארי ($q=2$), אזי:
$d_C\geq 3 \iff$ כל שתי עמודות של H שונות זו מזו ואין עמודות אפסים.

מסקנה בקוד המינג $d_C=3$

הוכחה
מהמסקנה הקודמת $d_C\geq 3$, וגם יש ב-H 3 עמודות שסכומן 0 (למשל: 1,2,3).

<u>פענוח לפי תסמונת</u>

יהי $C\subseteq \mathbb{F}_q^n$ קוד לינארי, ותהי H מטריצת הבדיקות של C.
נגדיר את התסמונת של: $s(y)=yH^t\in \mathbb{F}_q^{n-k}$
מתקיים $s(y)=0$ אם"ם $y\in C$.
יהי y וקטור מתקבל
x וקטור נשלח
e וקטור שגיאות
אזי $y=x+e \Rightarrow s(y)=(x+e)H^t=\overbrace{xH^t}^{0}+eH^t=eH^t=s(e)$

נסמן $C_e:=e+C$
ונעשה $\mathbb{F}_q^n=\bigcup_{e\in \mathbb{F}_q^n}(e+C)$
בכל מחלקה נבחר וקטור e_i עבורו $w(e_i)=\min_{y\in e_i+C} w(y)$ (משקל מינימלי).
ונחשב $s(e_i)$.

אם מקבלים מילה שגויה $y\in \mathbb{F}_q^n$ אזי:
1) מחשבים $s(y)$
2) משווים את $s(y)$ עם התסמונות $s(e_i)$ ולפי זה מחליטים
$y\in e_i+C$ ("קפ" המקום בו יש שוויון).

3) משפרים את x: $x := y - e_i$.

הערה

לא ייתכן $S(e_i)=S(e_j)$ כי e_i, e_j ממחלקות שונות.

דוגמה:

יהי C קוד עם $q=2, n=63, k=51, d=5$

$R \approx 0.8$

$M = 2^{51} \approx 10^{15}$

מס' המחלקות: $2^{63-51} = 2^{12} = 4096$

והקוד מתקן עד שתי שגיאות

לכן נתבונן על G הווקטורים ממשקלים 1,2

$w(e_i)=1 \Rightarrow 63$ כאלה

$w(e_i)=2 \Rightarrow \frac{n(n-1)}{2} = 1953$ כאלה

לא תמיד

לא נקבל מכל מחלקה שקל לבודד איזה מה-e_i הנ"ל

$\Rightarrow$ יש יותר משתי שגיאות

(4) (10/4/13)

קודים ציקליים

הגדרה

קוד ליניארי $C \subseteq \mathbb{F}_q^n$ ייקרא ציקלי אם לכל מילה $c=(c_0,c_1,\dots,c_{n-1}) \in C$
גם המילה $c'=(c_{n-1},c_0,\dots,c_{n-2}) \in C$

דוגמאות

1) C קוד ליניארי מעל $\mathbb{F}_2$ עם מטריצה יוצרת

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

למעשה, הפרמטרים הם $n=4,\ k=q=2,\ |C|=q^k=4$

כלומר, למעשה: $C=\{(0000),(1111),(1010),(0101)\}$
ולכן זהו קוד ציקלי.

2) C קוד עם מטריצת הבדיקות

$$H=\begin{pmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\end{pmatrix} \quad (\text{מעל } \mathbb{F}_2)$$

$$\begin{matrix}\uparrow&\uparrow&\uparrow&\uparrow&\uparrow&\uparrow&\uparrow\\4&6&7&3&5&2&1\end{matrix}$$

הוא שקול לקוד המינג (לפי ההמרה מבינארי לעשרוני)
והוא גם ציקלי (הוכחה בהמשך)

<u>בדיקת ציקליות</u>

לשם כך נרצה לעבור מווקטורים לפולינומים:

$$\mathbb{F}_q^n \ni (c_0,c_1,\dots,c_{n-1}) \longmapsto \sum_{i=0}^{n-1} c_i x^i \in \{p(x) \mid p\in\mathbb{F}_q[x],\ \deg p<n\} =: F_n[x]_q$$

וזהו איזומורפיזם של מרחבים וקטוריים: $\mathbb{F}_q^n$ עם $F_n[x]_q$.

נשים לב שב-$F_n[x]_q$ יש גם פעולת כפל (שאין ב-$\mathbb{F}_q^n$) אבל אין בה סגירות.

ובכן, נניח $(n,q)=1$. נגדיר את החוג: $R:=\mathbb{F}_q[x]/(x^n-1)$
(חוג מנה).

(האידיאל הנוצר ע"י x^n-1)

תזכורת $(x^n-1)=\{g(x)\cdot(x^n-1) \mid g(x)\in \mathbb{F}_q[x]\}$

ב-R למעשה יש שאריות של חלוקה של כל פולינום מ-$\mathbb{F}_q[x]$ עם הפולינום x^n-1.

למעשה, בעבור $f,g\in\mathbb{F}_q[x]$ נסמן $\bar f,\bar g\in R$ ומתקיים

$$\bar f=\bar g \iff \exists h\in\mathbb{F}_q[x]:\ f-g=(x^n-1)h$$

וכך את פעולות הכפל אנו נבצע ברינג R.

דוגמה $n=5,\ q=2$

$a=(11101)\qquad b=(10011)$

נבצע חישוב $a\cdot b$:

$a(x)=1+x+x^2+x^4\qquad b(x)=1+x^3+x^4$

$$a(x)b(x)=1+x+x^2+x^4+x^3+x^4+x^5+x^7+x^4+x^5+x^6+x^8=$$

מצטמצמים (נשאר מופע 1)   מצטמצמים

$$=1+x+x^2+x^3+x^4+x^6+x^7+x^8\in\mathbb{F}_2[x]$$

עכשיו, ב- $R=\mathbb{F}_2[x]/(x^5-1)$:

נשים לב שעבור $f=x^5,\ g=1 \Leftarrow \bar f=\bar g$

לכן ב-R: $x^6=x,\ x^7=x^2,\ x^8=x^3$

ולכן ב-R:

$$\overline{a(x)}\,\overline{b(x)}=1+x+x^2+x^3+x^4+x+x^2+x^3=1+x^4\in R$$

$\Rightarrow\quad a\cdot b=(10001)$

לכן, בהמשך נתייחס לקוד C כתת קב' ב-$R=\mathbb{F}_q[x]/(x^n-1)$

משפט

קוד $C\subset R$ הוא ציקלי אמ"מ C הוא אידיאל.

תזכורת בעבור R חוג, $A\subset R$ אידיאל אם:

1) $0\in A$
2) אם $a\in A$ אז $-a\in R$
3) אם $a,b\in A$ אז $a+b\in A$

$\Leftarrow A<(R,+)$ תת חבורה חיבורית

4) לכל $a\in A$ ולכל $r\in R$: $ra\in A$.

הוכחה

($\Leftarrow$) נניח ש- $C\subset R$ אידיאל, נוכיח שהוא ציקלי.

יהי $a=(a_0\dots a_{n-1})\Leftrightarrow a(x)=\sum_{i=0}^{n-1}a_ix^i\in C$

נתבונן ב- $xa(x)$ כאיבר ב R:

$$xa(x)=\sum_{i=1}^{n-1}a_{i-1}x^i+a_{n-1}x^n=a_{n-1}+\sum_{i=1}^{n-1}a_{i-1}x^i=:a'(x)\in C$$

(אידיאל)

$\Leftarrow a'=(a_{n-1},a_0,\dots,a_{n-2})\in C$ ולכן C קוד ציקלי.

($\Rightarrow$) נניח ש- $C\subset R$ קוד ציקלי. יהי $a(x)\in C$, $r(x)\in R$,

נתבונן ב- $r(x)a(x)$:

$$r(x)=r_0+r_1x+\dots+r_{n-1}x^{n-1}$$

מתקיים $r_0a(x)\in C$ מקוד לינארי (ציקלי $\Leftarrow$ לינארי)

$xa(x)\in C$ מהגדרה

לכן, מלינאריות וציקליות, לכל i: $r_ix^ia(x)\in C$

מלינאריות נקבל: $\Leftarrow r(x)a(x)\in C$

ולכן זה אידיאל כנדרש.

✻ מתורת החוגים ידוע:

R חוג ראשי (principal ideal domain), כלומר כל אידיאל ב R נוצר ע"י פולינום אחד ($C=(g(x))$) כאשר $g|x^n-1$.

לכן, כדי למצוא את הקודים הציקליים מאורך n, צריך לפרק את x^n-1 למכפלת גורמים אי פריקים

$$x^n-1=f_1(x)\cdots f_\ell(x)$$

ולקחת $g(x)=f_{i_1}(x)\cdots f_{i_m}(x)$ ($m\le\ell$) ומקבלים ממנו קוד ציקלי $C=(g(x))$.

הערה

מהרצאה: $(n,q)=1$, כל $f_i(x)$ שונים זה מזה.

הוכחה

נסמן
$$F(x)=x^n-1$$
$$F'(x)=nx^{n-1}$$

$(n,q)=1 \Leftarrow$ ב-$\mathbb{F}_q$: $n\not\equiv 0$

לכן $F'(x)=0$ אמ"ם $x=0$

אבל $x=0$ אינו שורש של $F(x)$ ולכן ל-$F(x)$ אין שורשים כפולים (אם שורש שהוא כפול, הנגזרת שלו הייתה 0).

הגדרה

יהי
$$x^n-1=f_1(x)\cdots f_\ell(x)$$
פירוק של x^n-1 לגורמים אי פריקים. קוד ציקלי $(f_i(x))$ ייקרא קוד ציקלי אי-פריק.

כמו כן, אם $C=(g(x))$ קוד ציקלי הנוצר ע"י $g(x)$, g ייקרא פולינום יוצר ו- $h(x)=\frac{x^n-1}{g(x)}$ ייקרא פולינום בודק.

הערה

יהיו
$$g(x)=g_0+g_1x+\dots+g_{n-k}x^{n-k}$$
$$h(x)=h_0+h_1x+\dots+h_kx^k$$
אזי, המטריצה היוצרת של $C=(g(x))$ היא:

$$G=\begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & & & 0 & g_0 & \cdots & & g_{n-k} \end{pmatrix}_{k\times(n-k)}$$

ומטריצת הבדיקות תהיה

$$H=\begin{pmatrix} 0 & \cdots & 0 & h_k & \cdots & h_2 & h_1 & h_0 \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 \\ & & & & \vdots & & & \\ h_k & \cdots & h_0 & 0 & \cdots & & & 0 \end{pmatrix}_{(n-k)\times n}$$

נבדוק שמתקיים $GH^t=0$

$$(GH^t)_{ij}=(\text{שורה } i \text{ ב-} G)\cdot(\text{עמודה } j \text{ ב-} H^t)=(\text{שורה } i \text{ ב-} G)\cdot(\text{שורה } j \text{ ב-} H)=$$

$$=(0\ldots0\ g_0\cdots g_{n-k}\ 0\ldots0)\cdot(0\ldots0\ h_k h_{k-1}\ldots h_0\ 0\ldots0)$$

(g_0 במקום i)

נתבונן על המקרה הפרטי: $i=1,\ j=n-k$: נקבל

מצד אחד $g(x)h(x)=x^n-1$

ומצד שני: $d_k=g_0h_k+g_1h_{k-1}+\ldots$

$$g(x)h(x)=\ldots+d_kx^k+\ldots \Rightarrow d_k=0$$

באופן דומה שאר המכפלות הן אפס, כנדרש.

דוגמה $n=7,\ k=7$

$$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1)$$

נתבונן בקוד $C=(x-1)$

$$g(x)=x-1 \Rightarrow g=(1100000)$$

$$G=\begin{pmatrix}1&1&0&\cdots&&0\\0&1&1&0&\cdots&0\\&&\ddots&\ddots&&\\0&\cdots&&0&1&1\end{pmatrix}_{6\times7}$$

$$h(x)=\frac{x^7-1}{x-1}=(x^3+x+1)(x^3+x^2+1)=x^6+x^5+x^4+x^3+x^2+1$$

$$H=(1\ 1\ \ldots\ 1)_{1\times7}$$

$$\Rightarrow C=\{(x_1,\ldots,x_7)\mid Hx^t=0\}=\{(x_1\ldots x_7)\mid x_1+\ldots+x_7=0\}$$

זהו קוד לבדיקת זוגיות.

כעת, עבור $C=(g(x))$ כאשר $g(x)=x^3+x+1$

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

$h(x)=(x+1)(x^3+x^2+1)=x^4+x^2+x+1$

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

$$\begin{matrix} \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 1 & 2 & 5 & 3 & 7 & 6 & 4 \end{matrix}$$

שקול לקוד המינג! $\Leftarrow$ קוד המינג ציקלי!

כמו כן, ל- $g(x)=(x^3+x+1)(x^3+x^2+1)$ מתאים קוד עם חזרות.

משפט

לכל m ולכל $t<\frac{2^m-1}{2}$ קיים קוד ציקלי מאורך $n=2^m-1$ המתקן עד t שגיאות עם $k\geq n-mt$

(3) (17/4/13)

קודים ציקליים

קוד נקרא ציקלי אם $C \triangleleft \mathbb{F}_q[x]/(x^n-1)$ אידיאל.
למעשה, $C=(g(x))$ כש- $g(x) \mid (x^n-1)$ יקרא פולינום יוצר,
$h(x)=\frac{x^n-1}{g(x)}$ יקרא פולינום בודק.

שדות סופיים

הגדרה

יהי $\mathbb{F}_q$ שדה סופי, $q=p^n$, ויהי $\beta\in\mathbb{F}_q$. נאמר ש-β איבר פרימיטיבי אם $\mathbb{F}_q^*=\langle\beta\rangle=\{1,\beta,\dots,\beta^{q-2}\}$

הגדרה

יהי β איבר פרימיטיבי של שדה $\mathbb{F}_q$. נאמר ש-$m(x)\in\mathbb{F}_p[x]$ הנו פולינום מינימלי ל-β אם:

1) $m(x)$ מתוקן.
2) $m(\beta)=0$
3) m פולינום אי פריק.

עובדה

$$m(x)=(x-\beta)(x-\beta^p)(x-\beta^{p^2})\cdots(x-\beta^{p^{s-1}})$$

כש-s הוא המס' השלם הקטן ביותר עבורו $\beta^{p^s}=\beta$.

הצגה אלטרנטיבית של קודים ציקליים

יהי $C=(g(x))\triangleleft\mathbb{F}_q[x]/(x^n-1)$, $g(x)=f_1(x)\cdots f_r(x)$

לכל f_i נבחר שורש β_i שלו $(1\le i\le r)$, $\beta_i\in\mathbb{F}_{q^{m_i}}$.

נסמן $m=\text{lcm}(m_i)$, אזי $\beta_i\in\mathbb{F}_{q^m}$,
$\mathbb{F}_{q^m}/\mathbb{F}_q$ מרחב וקטורי ממימד m.

נבחר בסיס של מרחב וקטורי זה, ונתבונן ב-β_i כוקטור עמודה מאורך m של רכיבים מ-$\mathbb{F}_q$.

נגדיר את המט' H מעל $\mathbb{F}_{q^m}$:

$$H=\begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \beta_r & \beta_r^2 & \cdots & \beta_r^{n-1} \end{pmatrix}_{r\times n/\mathbb{F}_{q^m}}$$

אם נרחיב את β_i (וצמודיו) ע"י וקטורים מאורך m המתאימים,
נקבל מט' $H'_{mr\times n}$ מעל $\mathbb{F}_q$.
הערה H היא מט' בדיקות לקוד C.

אם $c\in C$: $c(x)=c_0+c_1x+\dots+c_{n-1}x^{n-1}$
אזי $c(x)$ מתחלק (ללא שארית) ע"י $g(x)$, לכן לכל
β_i שורש של $c(x)$ $(1\le i\le r)$, לכן
$$c_0+c_1\beta_i+\dots+c_{n-1}\beta_i^{n-1}=0$$
$$\Downarrow$$
$$H(c_0,c_1,\dots,c_{n-1})^t=\vec{0}$$

הערה
ייתכן שבמטריצה H' שורות ת"ל וצריך להוריד.
דוגמא $q=2$, $n=2^m-1$.
יהי β איבר פרימיטיבי של $\mathbb{F}_{2^m}$. נגדיר
$C=\{c(x) \mid c(\beta)=0\}$ (קוד המינג מוכלל)
$H=(1\ \beta\ \cdots\ \beta^{n-1})_{1\times n}$ מעל $\mathbb{F}_{2^m}$

נקח $m=3$, אזי $n=7$. יהי $\beta\in\mathbb{F}_8$ איבר פרימיטיבי;
יהי פולינום מינ' של β $g(x)=x^3+x+1$. נעבור
מ-H ל-H'.
בסיס של $\mathbb{F}_8/\mathbb{F}_2$: $B=\{1,\beta,\beta^2\}$
$$\Downarrow$$
$$H'=\begin{pmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{pmatrix}$$
מתרגום לבינארי; שקול לקוד המינג

1, β, β^2, $\beta^3=-\beta-1$, $\beta^4=\beta^2+\beta$, $\beta^5=\beta^3+\beta^2=\beta+1+\beta^2$

דוגמא: קוד המתקן שלוש שגיאות

נקבל $z=7$ לפי הבנייה שהכרנו!

$m(\beta^4) \equiv m(\beta)$

$m(\beta^5)(x) = (x-\beta^5)(x-\beta^{10})$

וסימנו את מה צריך! נקח

$$g(x) = m_1(x) m_3(x) m_5(x)$$

$$\beta^5 = \beta^2 + \beta; \quad \beta^{10} = \beta^2 + \beta + 1$$

$$m_5(x) = x^2 - (\beta^5 + \beta^{10})x + \beta^{15} = x^2 + x + 1$$

$$\Rightarrow g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

$$deg = 10; \quad k = 5$$

הערות:

1) הערה שאם נמשיך עם $t=4$ (ארבע שגיאות, $z=9$) נקבל קוד עם חזרות.

2) בנה קוד BCH טוב במקרה $q=2$, $m=6$.

שם $m=4$, $n=15$ נקבל:
$H'_{4\times15}$ שגם היא מורכבת מכל המס' בין 1 ל-15
בצורה בינארית.

כך מקבלים קוד המינג מוכלל ל-m כלשהו.

<u>קודי BCH</u>

הגדרה

יהי β השורש ה-n פרימיטיבי של 1 ($\beta^n=1$), β שייך להרחבה של $\mathbb{F}_q$. נסמן
$$g(x)=\text{lcm}(m(\beta^l), m(\beta^{l+1}),\dots,m(\beta^{l+z-2}))$$
כש- $m(\beta^i)$ הינו הפולינום המינ' של β^i.
יהי $C=(g(x))\triangleleft\mathbb{F}_q[x]/(x^n-1)$ קוד ציקלי מאורך n.
C ייקרא קוד BCH מעל q עם מרחק מעוצב z.
אם $l=1$, C ייקרא קוד BCH מצומצם.
ואם $n=q^m-1$ (m שלם), C ייקרא קוד BCH פרימיטיבי.
הערה במקרה האחרון, β הוא איבר פרימיטיבי של $\mathbb{F}_{q^m}/\mathbb{F}_q$

משפט

אם C קוד BCH (מצומצם) עם מרחק מעוצב z, אזי $z\le d(C)$.

הוכחה

אם $c=(c_0,c_1,\dots,c_{n-1})\in C$ אזי $Hc^t=0$, כש
$$H=\begin{pmatrix}1 & \beta & \beta^2 & \cdots & \beta^{n-1}\\ 1 & \beta^2 & \beta^4 & & \beta^{2(n-1)}\\ \vdots & \vdots & & & \vdots\\ 1 & \beta^{z-1} & \beta^{2(z-1)} & & \beta^{(z-1)(z-1)}\end{pmatrix}_{n\times(z-1)}$$
נתבונן במטר' $\tilde{H}$ שמורכבת מ-$(z-1)$ עמודות H.
$\tilde{H}$ מטר' ונדרמונדה, לכן $|\tilde{H}|\neq0$ ולכן כל $z-1$
עמודות H בת"ל, ולכן $z\le d(C)$.

הערה קוד BCH שמאפשר פענוח יעיל יותר מאשר פענוח לפי הטבלה

דוגמה (קוד מתקן שתי שגיאות)

נבנה קוד BCH עם $\delta=5$, $q=2$, $m=4$, $n=2^4-1=15$.

יהי $\beta\in\mathbb{F}_{16}=\mathbb{F}_{2^4}$ איבר פרימיטיבי, וניקח $l=1$

$$m(\beta)(x)=(x-\beta)(x-\beta^2)(x-\beta^4)(x-\beta^8)$$

$$m(\beta^2)(x)=(x-\beta^2)(x-\beta^4)(x-\beta^8)(x-\underset{\beta^{16}}{\beta})$$

$$m(\beta^3)(x)=(x-\beta^3)(x-\beta^6)(x-\beta^{12})(x-\underset{\beta^{24}}{\beta^9})$$

קיבלנו עד סוף את $\beta,\beta^2,\beta^3,\beta^4$ לכן עם $\delta=5$ עוקבים.

$$\Rightarrow g(x)=m(\beta)(x)\cdot m(\beta^3)(x)=m_1(x)m_3(x)$$

כ-$m_1(x)$ ניתן לקחת כל פולינום אי"פ, מתוקן, ממעלה 4:

$$m_1(x)=x^4+x+1$$

$$\beta^4+\beta+1=0$$

$$\Rightarrow \beta^6=\beta^3+\beta^2$$

$$\beta^9=\beta^6+\beta^5=\beta^3+\beta^2+\beta^2+\beta=\beta^3+\beta$$

$$\beta^{12}=\beta^6+\beta^4=\beta^3+\beta^2+\beta+1$$

$$\Rightarrow m_3(x)=x^4+x^3+x^2+x+1$$

$$\Rightarrow g(x)=m_1(x)m_3(x)=x^8+x^7+x^6+x^4+1\;;\quad \deg g=8$$

$$k=n-\deg g=7$$

$$G=\begin{pmatrix}1&0&0&0&1&0&1&1&1&0&0&0&0&0&0\\0&1&0&0&0&1&0&1&1&1&0&0&0&0&0\\&&&&&&\vdots\end{pmatrix}_{7\times 15}$$

ומתקיים $d\geq 5$ כנדרש.

(6) (24/4/13)

קודים ציקליים

דוגמה

עבור $q=2,\ m=6,\ n=2^m-1=63$

יהי β איבר פרימיטיבי של $\mathbb{F}_{64}$. נגדיר

$$g(x)=\underbrace{m_1(x)}_{\text{עבור } \beta}\cdot\underbrace{m_3(x)}_{\text{עבור } \beta^3}$$

$$m_1(x)=(x-\beta^1)(x-\beta^2)(x-\beta^4)(x-\beta^8)(x-\beta^{16})(x-\beta^{32})$$

$$m_3(x)=(x-\beta^3)(x-\beta^6)(x-\beta^{12})(x-\beta^{24})(x-\beta^{48})(x-\beta^{33})$$

($33 = 96-63$)

$\Rightarrow \deg g=12 \Rightarrow k=n-\deg g=51\ ;\ R=\frac{k}{n}=\frac{51}{63}\approx 0.8$

וצפוי למעשה הקוד $[63,51,5]_2$

* נתבונן על n של $\mathbb{F}_q$ כאשר $(n,q)=1$ של $f\in\mathbb{F}_q[X]$,
יהי $\mathbb{F}_{q^m}$ שדה הפיצול של f (השדה הקטן ביותר המכיל את כל שורשי f).
תהי G חבורת גלואה של $\mathbb{F}_{q^m}/\mathbb{F}_q$:

$$G=\{\sigma\in \mathrm{Aut}(\mathbb{F}_{q^m})\mid \forall x\in\mathbb{F}_q:\ \sigma(x)=x\}$$

(Aut: העתקה חח"ע ועל)

מתקיים:

1) G חבורה ציקלית: $G=\langle\sigma\rangle$ כאשר $\sigma(x)=x^q$ אוטומורפיזם פרובניוס, $\sigma^m=id$.

2) החבורה G פועלת על אוסף שורשי הפולינום f, כלומר אם α שורש של f, גם $\sigma(\alpha)$ שורש של f.

דוגמה

תהי $\mathbb{C}/\mathbb{R}$ כאשר $\mathbb{C}=\mathbb{R}[\sqrt{-1}]=\{a+bi\mid a,b\in\mathbb{R}\}$.

$G=Gal(\mathbb{C}/\mathbb{R})=\{id,\sigma\}\ ;\ \sigma: a+bi\longrightarrow a-bi$

עבור $f=x^2+1$: $\sigma(i)=-i$ וכו'.

בהמשך לתרגול 2, נתבונן במסלול

$$O(\alpha)=\{\alpha,\alpha^{q},\alpha^{q^2},\dots\}$$

מתקיים $m_\alpha(x)=\prod_{\gamma\in O(\alpha)}(x-\gamma)$.

קל לראות ש-$m_\alpha(x)$ אינווריאנטי תחת פעולות G, ולכן, כנ"ל, $m_\alpha\in\mathbb{F}_q[x]$.

הגדרה

יהי n טבעי, $(n,q)=1$. הסדר של q הוא

$$\text{ord}_n(q)=m=\min\{s\mid q^s\equiv 1 \pmod n\}$$

למה

יהי $m=\text{ord}_n(q)$. אזי:

1) מעל $\mathbb{F}_{q^m}$ הפולינום x^n-1 מתפרק באופן הבא:
$$x^n-1=\prod_{i=1}^{m}(x-\beta^i)$$
כש-β האיבר הפרימיטיבי של $\mathbb{F}_{q^m}$

2) $O(\beta^i)=\{\beta^i,\beta^{iq},\beta^{iq^2},\dots,\beta^{iq^{v-1}}\}$
כאשר v הטבעי המינימלי עבורו $iq^v\equiv i \pmod n$

3) $m_{\beta^i}(x)=\prod_{\alpha\in O(\beta^i)}(x-\alpha)$

4) $x^n-1=\prod_{\beta^i\in T} m_{\beta^i}(x)$

כאשר T היא הקבוצה שקיבלנו לאחר בחירה של נציג מכל מסלול של G על אוסף השורשים.

הוכחה

$(n,q)=1 \Leftarrow$ קיימים $a,b\in\mathbb{Z}$ עבורם $an+bq=1$
$$bq\equiv 1 \pmod n$$

לכן, ב-$\mathbb{Z}_n$, $\bar{q}\equiv q \pmod n$ הוא איבר הפיך. בפרט $\bar{q}\in\mathbb{Z}_n^*$.
נתבונן בתת החבורה הציקלית הנוצרת ע"י $\bar{q}$, $H=\langle\bar{q}\rangle\subset\mathbb{Z}_n^*$.
נסמן $m=|H|$, ולכן $m=\min\{s\mid q^s\equiv 1 \pmod n\}$.
נתבונן ב-$(\mathbb{F}_{q^m})^*$, זאת חבורה ציקלית מגודל q^m-1.
נבחר ζ יוצר שלה, ויהי $\beta=\zeta^{\left(\frac{q^m-1}{n}\right)}$

β הוא איבר פרימיטיבי, ולכן β שורש של x^n-1.
ולכן גם $(\beta^i)^n=(\beta^n)^i=1$ ולכן כל חזקות β
גם הן שורשים של x^n-1. אזי נקבל

$$x^n-1=\prod_{i=1}^{n}(x-\beta^i)$$

2 מתקבל מהעובדה ש- $G=\langle\sigma\rangle$ וגם $m=|G|$
3,4 מתקבלים מחלוקת שורשי הפולינום x^n-1 למסלולים ביחס ל-G.

(*) נחזור לאחת הדוגמאות מהשיעור הקודם: $q=2, m=4 \Rightarrow n=15$
שדה הפיצול של $x^{15}-1$ הינו $\mathbb{F}_{16}$, ויש $\sigma: x\to x^2$.
נשים לב $|G|=4$, והמסלולים הם:

$$\{1\};\ \{\beta,\beta^2,\beta^4,\beta^8\};\ \{\beta^3,\beta^6,\beta^{12},\beta^9\};\ \{\beta^5,\beta^{10}\};\ \{\beta^7,\beta^{14},\beta^{13},\beta^{11}\}$$

$$\Downarrow$$

$$x^{15}-1=(x-1)m_1(x)m_3(x)m_5(x)m_7(x)$$

דוגמה- קוד המינג
עבור $q=2$, m טבעי ו- $2^m-1=n$, יהי β השורש
ה-n פרימיטיבי.

$$\beta^n=\beta^{2^m-1}=1 \Rightarrow \beta^{2^m}=\beta\in\mathbb{F}_{2^m}$$

$$m_\beta(x)=(x-\beta)(x-\beta^2)\cdots(x-\beta^{2^{m-1}});\quad \deg m_\beta(x)=m$$

נבחר ב- $g(x)=m_\beta(x)$, זהו קוד BCH עם $\delta=3$,
ולכן הקוד מתקן שגיאה אחת.
וזהו קוד מהצורה $[n,n-m,3]$.
נוכיח ש- $C=(g(x))$ הוא קוד המינג מוכלל.
(כלומר, בעמודות H יש את כל המס' בכתיב בינארי).
נבחר בסיס של $\mathbb{F}_{2^m}/\mathbb{F}_2$: $\{1,\beta,\beta^2,\dots,\beta^{m-1}\}$
נרשום כל החזקות הגבוהות יותר של β כצירוף של איברי הבסיס
כך: $\beta^j=\sum_{i=0}^{m-1}\alpha_{ij}\beta^i \quad (0\le j\le n-1)$
נגדיר מטריצה $H_{m\times n}=(\alpha_{ij})$
העמודות של H הן הצגת ל- β^j $(0\le j\le n-1)$. כולן שונות ולכן

H אכן מטריצת בדיקות קוד המינג מוכלל.

שוב יהי $c\in C=(g(x))$ נרצה להראות $c\in C$ אמ"מ $Hc^t=0$,

אמ"מ ⊛ $\sum_{j=1}^{n-1}\alpha_{ij}c_j=0$ (לכל $0\le i\le m-1$),

נכפיל את ⊛ ב-β^i ונחשב את סכום כל השוויונות.

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\alpha_{ij}c_j\beta^i=0$$

$$\sum_{j=1}^{n-1}c_j\left(\sum_{i=0}^{m-1}\alpha_{ij}\beta^i\right)=\sum_{j=0}^{n-1}c_j\beta^j$$

נתבונן ב- $c=(c_0,\dots,c_{n-1})$ כאל פולינום

$$c(x)=c_0+c_1x+\dots+c_{n-1}x^{n-1}$$

$c(x)\in C$ אמ"מ $c(\beta)=0$ אמ"מ β שורש של c.

אבל $g(x)$ הוא הפולינום המינ' של β, ומכאן כיוון זה.

אם β שורש של $c(x)$, אזי $c(x)\in C$.

לכן $C=(m_\beta(x))$ כנדרש ($m_\beta(x)=g(x)$)

קוד ריד-סולומון (RS)

הגדרה:

עבור $n=q-1$, קוד ה-BCH מעל $\mathbb{F}_q$, יקרא קוד ריד-סולומון.

ב-BCH $n=q^m-1$, ולכן ב-RS: $m=1$.

$\beta\in\mathbb{F}_q$ במקרה זה, ולכן כל הפולינומים המינ' של β וחזקותיו הם לינאריים.

כלומר, $\mathbb{F}_q$ מכיל את כל שורשי היחידה מסדר $n=q-1$.

$C=(g(x))$, $g(x)=(x-\beta)(x-\beta^2)\cdots(x-\beta^{z-1})$

אז C קוד עם המרחק המינ' המתוכנן z

זה נותן דרך נוספת לבניית קודים המתקנים שתי שגיאות.

דוגמה

נרצה תיקון שתי שגיאות ⇐ נרצה $\delta=5$. לכן

$$q-1=n\geq\delta=5$$

$$q\geq 6$$

נרצה q ראשוני ולכן נקח $q=7$ ונקבל $n=6$.

נתבונן על $\mathbb{F}_7$, ונמצא איבר פרימיטיבי שלו.

ננסה $\beta=2 \Rightarrow 2^3=1$, ולכן $\beta=2$ אינו פרימיטיבי

$\beta=3 \Rightarrow 3^2=2$, $3^3=6$, וכך הלאה... לכן $\beta=3$ פרימיטיבי

נקבל $g(x)=(x-3)(x-3^2)(x-3^3)(x-3^4)$

$$g(x)=(x-3)(x-2)(x-6)(x-4)=x^4-x^3+3x^2-5x+4=x^4+6x^3+3x^2+2x+4$$

$$\Rightarrow G=\begin{pmatrix}4&2&3&6&1&0\\0&4&2&3&6&1\end{pmatrix}$$

ומתקיים $k=2$, ולכן זהו קוד $[6,2,5]_7$

$$h(x)=(x-3^5)(x-3^6)=(x-5)(x-1)=x^2+x+5$$

$$\Rightarrow H=\begin{pmatrix}0&0&0&1&1&5\\0&0&1&1&5&0\\0&1&1&5&0&0\\1&1&5&0&0&0\end{pmatrix}$$

הערה

בדוגמה $5=6-2+1$

משפט לכל קוד RS מתקיים $d=n-k+1$

משפט (סינגלטון)

אם $C=[n,k,d]_q$ קוד לינארי מעל $\mathbb{F}_q$, אזי $d\leq n-k+1$ (חסם סינגלטון)

הגדרה קוד C כך ש $d=n-k+1$ נקרא קוד MDS.

(11/5/13)

קוד ריד סולומון

בעבור $n=q-1$, מתבוננים ב $C=(g(x))$

$$g(x)=(x-\beta)(x-\beta^{2})\cdots(x-\beta^{s-1})$$

וזהו למעשה הקוד $[q-1,q-s,s]_q$

$$s=(q-1)-(q-s)+1$$

ולמעשה שוויון $d=n-k+1$

קודי MDS (קודים עם הפרדה מירבית)

משפט חסם סינגלטון

אם C קוד ליניארי $C=[n,k,d]_q$ מתקיים $d\leq n-k+1$

הוכחה

אם נסמן ב-m את המס' המקס' של עמודות H שהן בת"ל, אזי $d=m+1$. כל $d-1$ עמודות של H הן בת"ל.

$$rank(H)=\dim\begin{pmatrix}\text{מרחב עמודות} \\ H \quad \text{של}\end{pmatrix}\geq d-1$$

מצד שני, $rank(H)\leq n-k$ (מספר השורות).

קיבלנו $n-k\geq d-1$

$$d\leq n-k+1$$

תרגיל הוכח בצורה שונה ע"י שימוש במט' היוצרת G.

הגדרה

קוד ליניארי $C=[n,k,d]_q$ שבו $d=n-k+1$, נקרא קוד MDS.

דוגמאות

1) קוד RS.
2) קוד עם חזרות $C=[n,1,n]_2$: מתקיים $n=n-1+1$.
3) קוד עם בדיקת זוגיות $C=[n,n-1,2]_2$; מתקיים $2=n-(n-1)+1$.

קודים מורחבים

יהי C קוד ליניארי, $C=[n,k,d]_q$, נגדיר: $\bar{C}\subseteq \mathbb{F}_q^{n+1}$

בקוד המורחב ע"י $\bar{C}=\{(c_1,\dots,c_n,c_{n+1}) \mid (c_1,\dots,c_n)\in C,\ c_1+\dots+c_n+c_{n+1}=0\}$

ל-c_{n+1} נקרא בדיקת הזוגיות הכללית.

דוגמה (קוד המינג מורחב)

נתחיל מקוד המינג רגיל $C=[7,4,3]_2$

$$H_{\bar C}=\left(\begin{array}{c|ccccccc} 1&1&1&1&1&1&1&1\\ \hline 0& & & & & & & \\ 0& & & & H_C & & & \\ 0& & & & & & & \end{array}\right)_{4\times 8}$$

(עמודות: 8, 1, 2, 3, 4, 5, 6, 7)

$\bar C=[8,4,4]_2$

כדי להראות שהמרחק אכן 4 נראה שכל שלוש עמודות של $H_{\bar C}$ הן בת"ל.

מספיק לבדוק שאין 3 עמודות שסכומן שווה לאפס, וזה נכון בגלל הרכיב הראשון של העמודות

$1+1+1\neq 0$

הערה

בגלל ש- $d=4$, הקוד $\bar C$ יכול לגלות שתי שגיאות אבל לתקן שגיאה אחת.

נסמן $\bar H=H_{\bar C}$, ויהי $x\in\bar C$, ותהי y מילה שגויה.

נחשב $S=\bar H y^t=(S_1,S_2,S_3,S_4)^t$

אם $(S_1,S_2,S_3)\neq\vec{0}$ אזי יש שגיאה אחת, ואפשר לתקן.

אם $(S_1,S_2,S_3)=\vec{0}$: יש 0 או 2 שגיאות

$S_4=0 \Rightarrow$ אין שגיאות

$S_4\neq 0 \Rightarrow$ יש שגיאות.

תרגיל

הוכח את הטענה הבאה, אם $d_c=2t$, אזי הקוד c יכול לגלות עד t שגיאות.

קודי RS מורחבים

משפט

יהי $c=[q-1,q-s,s]_q$ קוד RS מעל $\mathbb{F}_q$, ויהי $\bar{C}$ קוד RS מורחב. אזי $\bar{C}=[q,q-s,s+1]_q$.

הוכחה

יהי $c(x)=c_0+c_1x+\dots+c_nx^n\in C$

$$c_{n+1}+c_0+\dots+c_n=0$$

נסמן ב- $g(x)$ את הפולינום היוצר של C.

$$g(x)=(x-\beta)(x-\beta^2)\cdots(x-\beta^{s+1})$$

נוכיח ש- $w(c_0,c_1,\dots,c_n,c_{n+1})\geq s+1$

נכתוב $c(x)=a(x)g(x)$

ולמעשה מתקיים $c(1)=a(1)g(1)$

נחלק למקרים:

1) $c_{n+1}\neq 0$, אזי הוכחנו:
$$w(c_0,c_1,\dots,c_n)\geq s \Rightarrow w(c_0,\dots,c_n,c_{n+1})\geq s+1$$

2) $c_{n+1}=0$, אזי $c(1)=c_0+c_1+\dots+c_n=0$.

לכן $c(x)$ מתחלק ב- $x-1$, וגם ב- $g(x)$;

לכן $c(x)$ מתחלק ב-

$$(x-1)g(x)=(x-\beta^0)(x-\beta^1)\cdots(x-\beta^{s-1})$$

זהו BCH עם s חזקות עוקבות, לכן $d\geq s+1$

מסקנה

קוד RS מורחב הוא גם קוד MDS: $s+1=q-(q-s)+1$

גישה מקורית לקוד ריד סולומון

יהי $n=q$. נרשום את $\mathbb{F}_q$ בצורה הבאה:

$$\mathbb{F}_q=\{\alpha_i=\alpha^i \mid 0\leq i\leq q-1,\ \alpha_{q-1}=0\}$$

נגדיר
$$L=\{f(x)\in\mathbb{F}_q[x] \mid \deg f<k\}$$

עוד נגדיר
$$C=\{f(\alpha_0),\dots,f(\alpha_{q-1}) \mid f\in L\}$$

תכונות

1) $C \subset \mathbb{F}_q^{\,q}$

2) C קוד לינארי (כי L מ"ו מעל $\mathbb{F}_q$)

3) $k = \dim L$:

נגדיר $\varphi: L \to C$ ע"י $f \mapsto (f(\alpha_0),\dots,f(\alpha_{q-1}))$

φ היא ה"ל של מ"ו, והיא גם חח"ע ולכן:

$\dim C = \dim(\operatorname{im}\varphi)$; $\underline{\ker\varphi = 0}$

כי $f \equiv 0$ אמ"ם $\varphi(f)=0$ (שכן f מעל $\mathbb{F}_q$).

לכן הנדרש מתקבל.

4) נחשב את d: ניקח $c=(f(\alpha_0),\dots,f(\alpha_{q-1}))\in C$

ונחשב $w(c)$.

מס' האפסים של c = מס' השורשים של f $\le k-1$, לכן

$w(c) \ge n-(k-1) = n-k+1$ כי $d = n-k+1$

תרגיל

הסבר מדוע קוד צב שקול לקוד RS מוכלל.

הכללה

נתבונן ב- $\alpha_0,\dots,\alpha_{q-1}\in\mathbb{F}_q$ כנק' של הקו הישר $\mathbb{A}^1$,

נעבור לקו הישר הפרויקטיבי $X=\mathbb{P}^1$

(ע"י הוספת נק' אינסופית).

מבחינה אלגברית, נק' של הישר הפרויקטיבי הן $(\alpha:\beta)$

כך שלפחות אחד מהם אינו אפס, וגם

$(\alpha:\beta)=(c\alpha:c\beta)$

הישר הפרויקטיבי כולל הנק'

$$\mathbb{P}^1=\{P_0,P_1,\dots,P_{q-1},P_q,P_\infty\}=\{(1:1),(1:\alpha),(1:\alpha^2),\dots,(1:\alpha^{q-2}),(1:0),(0:1)\}$$

↑ נק' אינסופית

נגדיר את L אוסף כל הפונק' $F=\frac{f}{g}$, כאשר f,g פולינומים הומוגניים מאותה דרגה וכך של-F אין קטבים ב- $P_0,\dots,P_q$, ובנק' P_∞ יש קוטב מריבוי $\le k-1$.

עוד נגדיר

$$C=\{(F(P_0),\dots,F(P_{q-1}))\mid F\in L\}$$

בשדה גדול יותר יש להחליף את P^1 לעקום כלשהו, ואת L,C בונים בצורה דומה.

<u>קודי שאריות ריבועיות (QR)</u>

יהי n מס' ראשוני אי זוגי, ונתבונן בשדה השאריות $\mathbb{Z}_n$.

נסמן בהתאמה: $z\in\mathbb{Z}\longmapsto \bar{z}=z \pmod n\in\mathbb{Z}_n$ $\left(z=sn+\bar{r},\ 0\le\bar{r}\le n-1;\ \bar{z}=\bar{r}\right)$

נתבונן בהתאמה אחרת: $z\in\mathbb{Z}\longmapsto \underline{r}$

כאשר $z=sn+\underline{r}$, $-\frac{n-1}{2}\le\underline{r}\le\frac{n-1}{2}$

הגדרה

נאמר ש-$i\in\mathbb{Z}$ ריבוע מודולו n, אם קיים $z\in\mathbb{Z}$ עבורו $i\equiv z^2 \pmod n$. במקרה כזה i ייקרא שארית ריבועית. אחרת נאמר שהוא אינו שארית ריבועית.

נסמן ב-Q את אוסף השאריות הריבועיות, וב-N את אוסף האיברים שאינם שאריות ריבועיות ($0\notin N\cup Q$).

טענה $|Q|=|N|=\frac{n-1}{2}$

הוכחה

נכתוב $\mathbb{Z}_n^*=\langle\beta\rangle$, $|\mathbb{Z}_n^*|=n-1$ אזי

$Q=\{\beta^{2m}\}$; $N=\{\beta^{2m+1}\}$

אם נקח איבר פרימיטיבי אחר γ, ונניח בשלילה ש-

$$x=\beta^{2m}=\gamma^{2k+1}$$

$$\Rightarrow \gamma=(\underbrace{\beta^m\gamma^{-k}}_{\delta})^2 \Rightarrow \gamma=\delta^2$$

וגם $\delta^{n-1}=1$. לכן $\gamma^{\frac{n-1}{2}}=\delta^{n-1}=1$ בסתירה לפרימיטיביות, ומכאן הנדרש.

מסקנה

$$Q\cdot Q=Q;\ N\cdot N=Q;\ Q\cdot N=N$$

למה $Q=\left\{ i^2 \;\middle|\; 1\le i\le \frac{n-1}{2} \right\}$

הוכחה $(n-i)^2\equiv i^2 \pmod n$

נוכיח שכל האיברים שונים:

נניח $i^2\equiv j^2 \pmod n$

$$i^2-j^2\equiv 0 \pmod n$$

$$(i-j)(i+j)\equiv 0 \pmod n$$

$1\le i,j\le \frac{n-1}{2} \Rightarrow i+j\not\equiv 0 \pmod n \Rightarrow i\equiv j \pmod n$ בפרט.

הגדרה סימן לג'נדר

$$\left(\frac{a}{n}\right)=\begin{cases}0 & n\mid a\\ 1 & a \text{ ש"ר} \\ -1 & a \text{ אינו ש"ר}\end{cases}$$

משפט אוילר $\left(\frac{a}{n}\right)\equiv a^{\frac{n-1}{2}} \pmod n$

תכונות

1) $\left(\frac{a^2}{n}\right)=1$

2) אם $a\equiv b \pmod n$ אזי $\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$

3) $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

4) $\left(\frac{-1}{n}\right)=\begin{cases}1 & n\equiv 1 \pmod 4\\ -1 & n\equiv 3 \pmod 4\end{cases}$

5) $\left(\frac{2}{n}\right)=\begin{cases}1 & n\equiv \pm 1 \pmod 8\\ -1 & n\equiv \pm 3 \pmod 8\end{cases}$

6) חוק ההדדיות הריבועית של גאוס: יהיו n,m ראשוניים אי"ז

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{(m-1)(n-1)}{4}}$$

$$\Rightarrow \left(\frac{m}{n}\right)=\pm\left(\frac{n}{m}\right);\ \begin{cases}- & m\equiv n\equiv 3 \pmod 4\\ + & \text{else}\end{cases}$$

למה

יהי n ראשוני אי זוגי, ויהי ζ שורש יחידה פרימיטיבי מסדר n.
נניח ש-q ש"ר מודולו n. אזי:

1) הפולינומים $g_Q=\prod_{\bar a\in Q}(x-\zeta^{\bar a})$; $g_N=\prod_{\bar b\in N}(x-\zeta^{\bar b})$ שייכים ל-$\mathbb{F}_q[x]$.

2) מעל $\mathbb{F}_q[x]$:

$$x^n-1=(x-1)g_Q g_N$$

הגדרה

יהי n מס' ראשוני אי זוגי ויהי q ש"ר מודולו n. נגדיר

$$C_Q(n,q)=(g_Q);\qquad \dim C_Q=n-\frac{n-1}{2}=\frac{n+1}{2}$$

$$\hat{C}_Q(n,q)=((x-1)g_Q);\qquad \dim \hat{C}_Q=\frac{n-1}{2}$$

(קוד QR)

$$C_N(n,q)=(g_N);\qquad \dim C_N=\frac{n+1}{2}$$

$$\hat{C}_N(n,q)=((x-1)g_N);\qquad \dim \hat{C}_N=\frac{n-1}{2}$$

תרגיל

הוכח ש- $C_Q(7,2)$ שקול לקוד המינג.

משפט

C_Q שקול ל- C_N, וגם $\hat{C}_Q$ שקול ל- $\hat{C}_N$.

הגדרה

אומרים שקוד לינארי C הוא זוגי אם כל מילה שלו בעלת משקל זוגי.

משפט

יהי $n\equiv\pm1 \pmod 8$, אזי $\hat{C}_Q(n,2)$; $\hat{C}_N(n,2)$ הם זוגיים.

הוכחה

נניח $c\in\hat{C}_Q$. מתקיים $(x-1)|c(x)$, ולכן $c(1)=0$

$$\Rightarrow c_0+c_1+\dots+c_{n-1}=0$$

ולכן $w(c)$ זוגי.

משפט

1) $d(C_Q(n,2))$ אי זוגי.

2) $d(\hat{C}_Q(n,q))=d(C_Q(n,q))+1$

משפט

יהי $C=C_Q(n,q)$, אזי:

1) $d^2\geq n$

2) אם $n\equiv 3 \pmod 4$, אזי $d^2-d+1\geq n$

3) אם $q=2$, $n\equiv 7 \pmod 8$, אזי $d\equiv 3 \pmod 4$.

הוכחה

1) נקבע $s\in N$ ונסמן $\tilde{g}=g_N$; $g=g_Q$

נקח $a\in\mathbb{Z}_n$, ונסמן $a=js$.

אם $j\in Q$, אזי $a\in N$.

אם $j\in N$, אזי $a\in Q$.

נקח $c(x)\in C$ מילה משקל מינימלי, ונסמן $w(c)=d$.

$$c(x)=a(x)g(x)$$

נגדיר $\tilde{c}(x)=c(x^s) \pmod{(x^n-1)}$

$$\tilde{c}(x)=a(x^s)g(x^s) \pmod{(x^n-1)}$$

$$w(\tilde{c})=d$$

נסמן ב-ζ את האיבר הפרימיטיבי של $\mathbb{F}_q$.

אם $j\in Q$ אזי $js\in N$ ולכן $g(\zeta^{js})\neq 0$

אם $j\in N$ אזי $js\in Q$ ולכן $g(\zeta^{js})=0$

לכן $g(x^s)=\tilde{g}(x)$

לכן $c(x)\tilde{c}(x) \pmod{(x^n-1)}$ מתחלק ב-g וב-$\tilde{g}$ ⇐ מתחלק ב-$g\tilde{g}$.

$$x^n-1=(x-1)g(x)\tilde{g}(x)$$

$$\Rightarrow g(x)\tilde{g}(x)=\frac{x^n-1}{x-1}=x^{n-1}+x^{n-2}+\dots+1$$

$$\deg(c\tilde{c})=\deg(x^{n-1}+\dots+1)=n-1$$

$$\underbrace{\underbrace{\tilde{c}}_{w=d}\cdot\underbrace{c}_{w=d}}_{w\leq d^2}=\underbrace{x^{n-1}+\dots+1}_{w=n}\Rightarrow n\leq d^2$$

(2) נניח $n \equiv 3 \pmod{4}$

נקח $\lambda = -1$, אז אינו ש"ר מודולו n

$$c(x)c(x^{-1}) = \beta(1+x+\dots+x^{n-1}) \qquad (\beta \neq 0)$$

נקבל

$$w \le d(d-1)+1$$
$$n \le d^2-d+1$$

(3) תהי $0 \neq c \in C_\lambda(n,2)$, $w(c)=d$

נסמן $c_0, c_1, \dots, c_{d-1}$ כרכיבים שאינם אפס.

ונשים לב ש-d אי זוגי.

$$1+x+\dots+x^{n-1} \equiv c(x)\cdot c(x^{-1}) \equiv \left(\sum_{u=0}^{d-1} x^{i_u}\right)\left(\sum_{v=0}^{d-1} (x^{-1})^{i_v}\right) \equiv$$

$$\equiv \sum_{\substack{u,v \\ 0\le u,v\le d-1}} x^{i_u-i_v} \equiv \underbrace{1+1+\dots+1}_{d \text{ פעמים}} + \sum_{\substack{u\neq v \\ 0\le u,v\le d-1}} x^{i_u-i_v}$$

יש צמצומים לזוגות מהצורה $(u,v),(y,z)$

אז יש ההפוכים גם $(v,u),(z,y)$

$$i_u - i_v = i_z - i_y \Rightarrow i_u - i_z = i_v - i_y \quad (u,z),(y,v)$$
$$i_v - i_u = i_y - i_z \Rightarrow i_z - i_u = i_y - i_v \quad (z,u),(v,y)$$

יש $4l$ צמצומים:

$$1+x+\dots+x^{n-1} \equiv 1+d(d-1)-4l$$
$$n = 1+d^2-d-4l$$

d אי זוגי לכן $d \equiv 1,3 \pmod{4}$

נניח בשלילה $d \equiv 1 \pmod{4}$, אזי $n \equiv 1 \pmod{4}$

בסתירה, לכן $d \equiv 3 \pmod{4}$ כנדרש.

⑧ (22/5/13)

קודי QR

נניח $x^n-1=(x-1)g_Q g_N$, ויהי ζ איבר פרימיטיבי

g_Q פולינום המתאים לשאריות $g_Q=\prod_{a\in Q}(x-\zeta^a)$ (אוסף הריבועים)

g_N פולינום עבור שאר האיברים $g_N=\prod_{b\in N}(x-\zeta^b)$

⊛ עבור $n\neq 2$ ראשוני, q שארית מודולו n, מגדירים:

$C_Q(n,q)=\langle g_Q\rangle;\quad C_Q^1(n,q)=\langle (x-1)g_Q\rangle$

$C_N(n,q)=\langle g_N\rangle;\quad C_Q^1(n,q)=\langle (x-1)g_N\rangle$

משפט

1) $d\geq\sqrt{n}$

2) אם $n\equiv 3 \pmod 4$ אזי $d^2-d+1\geq n$

3) אם $q=2$, $n\equiv -1 \pmod 8$ אזי $d\equiv 3 \pmod 4$

הקודים של גולאי (Golay)

הגדרה $G_{23}=C_Q(23,2)$

G_{24} הוא ההרחבה של G_{23} (מסומן גם $\overline{G_{23}}$, מורחב ע"י הוספת שורת אחדות ל-H)

$G_{11}=C_Q(11,3)$

משפט

א. $G_{23}=[23,12,7]_2$

ב. $G_{24}=[24,12,8]_2$

ג. $G_{11}=[11,6,5]_3$

הוכחה

א. נשים לב $n=23$, $23\equiv -1 \pmod 8$ ולכן 2 ש"ר עבור מודולו 23:

$Q=\{1,2,3,4,6,8,9,12,13,16,18\}$

מתי איברים של קודי BCH נובע $d\geq 5$ (מ-1,2,3,4)

ולמעשה $k=\frac{n+1}{2}=12$ $(k=n-\deg g_Q)$

נשתמש בסעיף 2 של המשפט הקודם: $d^2-d+1\geq 23$

מסעיף 3 נקבל $d\geq 7$ ומחסם המינג (בהמשך השיעור) $d=7$.

ב. נוכיח מתכונות של קוד מורחב (הראינו בשיעור הקודם)

ג. $k=6$ ברור.

עבור $\mathbb{Z}_{11}$; $Q=\{1,3,4,5,9\}$

$d\geq 4$

שאלות 2,3 של כמשפט הקודם לא עוזרות לנו.
ההוכחה של $d=5$ מתקבלת משימוש בתכונות המט' G,H.

<u>חישובים בקודים אלו</u>

עבור G_{23} למשל, נמצא m עבורו $2^m\equiv 1 \pmod{23}$
צפי למשל עבור $m=11$; $2^{11}=2048$; $2047=23\cdot 89$

בשדה $\mathbb{F}_{2048}$ נקח איבר פרימיטיבי α:
$\alpha^{2047}=1$ ולכל $n<2047$ אז $\alpha^n\neq 1$

נגדיר $\alpha^{89}=\beta$ אז $\beta^{23}=1$

המסלול של β: $\{\beta,\beta^2,\beta^4,\beta^8,\beta^{16},\beta^9,\beta^{18},\beta^{13},\beta^3,\beta^6,\beta^{12}\}$ ⇐ אורך 11

$\deg m_\beta(x)=11$; $\deg m_{\beta^{-1}}(x)=11$

$$\Rightarrow x^{23}-1=(x-1)m_\beta(x)m_{\beta^{-1}}(x)$$

עבור G_{11} נמצא m עבורו $3^m\equiv 1 \pmod{11}$
צפי למשל עבור $m=10$ או $m=5$:
(מקבלים עבור $(a,p)=1$: $a^{p-1}\equiv 1 \pmod p$ ואז מספיקים את גורמים של $p-1$).

$3^5=243\equiv 1 \pmod{11}$, $242=11\cdot 22$

נקח α כך ש- $\alpha^{242}=1$ ב-$\mathbb{F}_{243}$, נגדיר $\beta=\alpha^{22}$
ומתקיים $\beta^{11}=1$.

המסלול של β יהיה: $\{\beta,\beta^3,\beta^9,\beta^5,\beta^4\}$ (מאורך 5).

$\deg m_\beta=\deg m_{\beta^{-1}}=5$

$$\Rightarrow x^{11}-1=(x-1)m_\beta(x)m_{\beta^{-1}}(x)$$

אפשר לקחת β כשורש של הפולינום הבא מעל $\mathbb{F}_3$: $x^5-x^3+x^2-x+1$

(8) (22/5/13)

חסמים לקודים

חסם המינג

יהי $|F|=q$, $C\subset F^n$, $|C|=q^k$, $k=\log_q|C|$.

השאלה היא האם קיים C קוד $[n,k,d]_q$.

הגדרה נסמן

$$A(n,d)_q=\max\{|C| : C=[n,k,d]_q\}$$

קוד C שעבורו $|C|=A(n,d)_q$ נקרא אופטימלי

הגדרה

יהי $C\subset F^n$, $c\in C$ מילה. יהי e מס' טבעי. נסמן

$B(c,e)=\{x\in F^n \mid d(c,x)\le e\}$ כדור המינג עם מרכז c ורדיוס e.

טענה

אם $e\le\frac{d-1}{2}$, $c_1\neq c_2$, אזי $B(c_1,e)\cap B(c_2,e)=\emptyset$

מסקנה

נניח $e\le\frac{d-1}{2}$. אזי $\sum_{c\in C}|B(c,e)|\le q^n$

למה

$$|B(c,e)|=\sum_{i=0}^{e}\binom{n}{i}(q-1)^i$$

הוכחה

תהי $c\in C$ מילה, נסמן $Z_k=\{x\in F^n \mid d(c,x)=k\}$

נסמן $c=(c_1,\dots,c_n)$; $x=(x_1,\dots,x_n)$.

אזי

$$|Z_k|=\binom{n}{k}(q-1)^k$$

(בחירת k מקומות שונים / בהינתן $x_i\neq c_i$ כמות האפשרויות לבחור x_i)

מתקיים: $B(c,e)=\bigcup_{i=0}^{e}Z_i$

לכן $\Rightarrow |B(c,e)|=\sum_{i=0}^{e}\binom{n}{i}(q-1)^i$

מסקנה עבור $e=\lfloor\frac{d-1}{2}\rfloor$:

$$A(n,d)_q\le q^n\cdot\left[\sum_{i=0}^{e}\binom{n}{i}(q-1)^i\right]^{-1}$$

מסקנה - חסם המינג

$$\frac{k}{n}=R\le 1-\frac{\log_q\left(\sum_{i=0}^{e}\binom{n}{i}(q-1)^i\right)}{n}$$

הגדרה

אם באי השוויון יש שוויון, C ייקרא קוד מושלם

דוגמה

יהי C קוד המינג: $q=2, n=7, k=4, |C|=2^4=16; d=3, e=1$

$$\sum_{i=0}^{e}\binom{n}{i}(q-1)^i=8 \;;\quad R=\frac{k}{n}=\frac{4}{7}=1-\frac{\log_2 8}{7}$$

ולכן קוד המינג הוא מושלם.

הערה

אי אפשר לשפר את קוד המינג ע"י בניית קוד $[6,4,3]_2$. כיון $R=\frac{4}{6}$ אבל אי"ש המינג לא מתקיים ולכן זה יותר טוב.

דוגמה קוד גולאי (G_{23}) $G_{23}=[23,12,7]_2$

מתקיים $d=7 \Rightarrow e=3$:

$$\sum_{i=0}^{3}\binom{23}{i}1^i=2048$$

$$R\le 1-\frac{\log_2 2048}{23}=\frac{12}{23}$$

ולכן G_{23} מושלם.

נשים לב שעבור $d>8$ אי"ש לא מתקיים, אבל $d=8$ לא אפשרי כי d צריך להיות אי זוגי (ללא הוכחה)

דוגמה

נראה שלא קיים קוד בינארי מאורך 4 המתקן שגיאה אחת. חלק מקוד עם חזרות. נניח בשלילה שיש קוד: $d\ge 3$; אם $d=4$ זה קוד עם חזרות $\Leftarrow d=3$.

$$A(4,3)\le 3\cdot 2 \Rightarrow A(4,3)\le 3$$

אם $A(4,3)=2$ נקבל קוד עם חזרות ולכן נצטרך להראות $A(4,3)\ne 3$

ובכן, נניח בשלילה $|C|=3$: $C=\{x,y,z\}$.

$x=(x_1,\dots,x_4)$; $y=(y_1,\dots,y_4)$; $z=(z_1,\dots,z_4)$

$d=3$ אזי $d(x,y), d(y,z), d(x,z) \geq 3$

נסמן $A=\{i \mid x_i \neq y_i\}$ $B=\{j \mid x_j \neq z_j\}$

$|A| \geq 3$; $|B| \geq 3$ $\Rightarrow$ $|A \cap B| \geq 2$

$A \cap B = \{k \mid x_k \neq y_k \wedge x_k \neq z_k\}$

בגלל הא"ב הוא 2 אזי $A \cap B \subseteq \{k \mid y_k = z_k\}$

$|A \cap B| \geq 2$ וזו סתירה ל- $d(y,z) \geq 3$!

מכאן מתקבל הנדרש.

(4) (29/5/13)

חסמים לקודים

חסם פלוטקין

משפט

אם $C\sim[n,k,d]_q$, אזי $d\le\frac{n\cdot q^k(q-1)}{(q^k-1)q}$

הוכחה:

נסמן $|F|=q$, $C\subset F^n$, ונסמן $M=|C|=q^k$. מתקיים

$$d\le d_{average}=\frac{1}{M(M-1)}\sum_{\substack{x,y\in C\\ x\ne y}} d(x,y)$$

נסמן $X_{i,j}=\{x=(x_1,\dots,x_n)\in C \mid x_i=j\}$; $m_{i,j}=|X_{i,j}|$

וגם לכל $1\le i\le n$ מתקיים $\sum_{j\in F} m_{i,j}=M$

$$dM(M-1)\le d_{average}M(M-1)=\sum_{\substack{x,y\in C\\ x\ne y}} d(x,y)=\sum_{i=1}^{n}\sum_{x,y\in C}(1-\delta_{x_i,y_i})=$$

$$=\sum_{i=1}^{n}\sum_{j,l\in F}(1-\delta_{j,l})m_{i,j}m_{i,l}\underset{\text{פתיחה}}{=}\sum_{i=1}^{n}\left[\left(\sum_{j\in F}m_{i,j}\right)^2-\sum_{j\in F}m_{i,j}^2\right]=$$

$$=\sum_{i=1}^{n}\left(M^2-\sum_{j\in F}m_{i,j}^2\right)$$

תזכורת: אי שוויון קושי שוורץ:

אם V ממ"פ $(\langle\cdot,\cdot\rangle)$ ואם $\|\cdot\|$ הנורמה המושרית, אזי

$$|\langle x,y\rangle|\le\|x\|\cdot\|y\|$$

אם נקח $y=(1,\dots,1)$ נקבל: $(x_1+\dots+x_n)^2\le n(x_1^2+\dots+x_n^2)$

$$\frac{1}{n}(x_1+\dots+x_n)^2\le x_1^2+\dots+x_n^2$$

$$\Rightarrow dM(M-1)\le\sum_{i=1}^{n}\left[M^2-\frac{1}{q}\left(\sum_{j\in F}m_{i,j}\right)^2\right]=\sum_{i=1}^{n}\left(M^2-\frac{1}{q}M^2\right)=nM^2\left(1-\frac{1}{q}\right)=\frac{nM^2(q-1)}{q}$$

$$\Rightarrow d\le\frac{n(q-1)M}{q(M-1)}=\frac{nq^k(q-1)}{(q^k-1)q}$$

⊛ נשים לב: חסם פלוטקין נותן $d\le\frac{nq^k(q-1)}{(q^k-1)q}$

חסם סינגלטון נותן $d\le n-k+1$

נעדן עבור פרמטרים האסימפטוטיים $R=\frac{k}{n}$ $\delta=\frac{d}{n}$

מסינגלטון נקבל $\delta \le 1-R+\frac{1}{n}$ ובאסימפטוטיקה: $\delta \le 1-R$

מפלוטקין נקבל $\delta \le \frac{q^n}{q^n-1}\cdot\frac{q-1}{q}$

באסימפטוטיקה: $\delta \le \frac{q-1}{q}$

פענוח לפי רוב קולות

דוגמה

נקח c קוד ציקלי עם $n=7$:

$$g(x)=(x+1)(x^3+x+1)=x^4+x^3+x^2+1$$

$$h(x)=\frac{x^7-1}{g(x)}=x^3+x^2+1$$

$$H=\begin{pmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{pmatrix}\begin{matrix}r_1\\r_2\\r_3\\r_4\end{matrix}$$

(העמודות: $x_0, x_1, x_2, x_3, x_4, x_5, x_6$)

נניח ש- $x=(x_0,\dots,x_6)$ מילה מתקבלת. אם אין שגיאות אזי $x\in C$, ולכן $Hx^T=0$ או

r_1: $x_0=x_1+x_3$

$r_1+r_2+r_3$: $x_0=x_4+x_5$

$r_1+r_2+r_4$: $x_0=x_2+x_6$

אם אין שגיאות, אזי מתקיימות שלוש המשוואות.

אם יש שגיאה אחת אזי אחת מהמשוואות לא מתקיימת.

אופן התיקון: לעשות, נתבונן בארבעת המס׳ $x_0, x_1+x_3, x_4+x_5, x_2+x_6$.

אם רובם 0, נקבע $x_0=0$.

אם רובם 1 נקבע $x_0=1$.

אם יש אותו מס׳, יש לפחות שתי שגיאות ואין דבר.

לגבי x_1, נבצע הזזה ציקלית ונקבל: $x_1=x_2+x_4$; $x_1=x_5+x_6$; $x_1=x_0+x_3$

ונשתמש באותה הדרך ונקבע את x_1 לפי רוב קולות וכך הלאה.

באופן כללי, אפשר להשתמש באלגו' שפענוח לפי רוב קולות אם לכל x_j קיימת מערכת משוואות מהצורה הבאה

$$x_j = \sum_{k\neq j} a_{1k} x_k$$
$$\vdots$$
$$x_j = \sum_{k\neq j} a_{Zk} x_k$$

כך שבצד ימין של כל משוואה כל סמל שונה מ-x_j מופיע מקס' פעם אחת (מערכת נפרדת)

בפענוח, אנו מחליטים על הערך של x_j לפי רוב ערכי

$$\{x_j, \sum_{k\neq j} a_{1k}x_k, \dots, \sum_{k\neq j} a_{Zk}x_k\}$$

אפשר במקרה זה לתקן $\frac{1+Z}{2}$ שגיאות.

הגדרה

אומרים שהקוד $C^\perp$ דואלי לקוד הליניארי C אם המט' היוצרת של $C^\perp$ היא מט' הבדיקות של C (ולהפך).

דוגמא

עבור C קוד המינג מורחב: $C=[8,4,4]_2$

$$H=\begin{pmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \end{pmatrix}=G \qquad \begin{matrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{matrix}$$

ומתקיים $HG^t=HH^t=0 \Rightarrow$ C דואלי לעצמו.

לכל מילה $x=(x_0,\dots,x_7)\in C$ נכתוב:

$$x=\sum_{i=0}^{3} a_i g_i \qquad (a_i\in\{0,1\})$$

סכום של שני האיברים הראשונים בשורות 2-0 הוא 0 בשורה 3 הוא 1

$$\Rightarrow a_3 = x_0+x_1$$

באותו אופן: $a_3=x_2+x_3$, $a_3=x_4+x_5$, $a_3=x_6+x_7$

ונחליט את הערך של a_3 בעזרת הצבעה בין
$\{x_0+x_1, x_2+x_3, x_4+x_5, x_6+x_7\}$

עבור a_2 נקבל באותו אופן שצריך להחליט לפי
$\{x_0+x_2, x_1+x_3, x_4+x_6, x_5+x_7\}$

עבור a_1: $\{x_0+x_4, x_1+x_5, x_2+x_6, x_3+x_7\}$

עבור a_0 נצטרך לסיבוב שני:
נתבונן ב- $\bar{x}' = a_0\bar{g}_0$

אם אין שגיאות אז $\bar{x}'$ הוא $(0...00)$ או $(1...11)$
ולמסקנה מחליטים את הערך של a_0 לפי רוב קולות ב-$\bar{x}'$.

דוגמה

נניח שקיבלנו מילה $(0,1,1,1,0,1,1,0)$

נקבל $a_3=1$, $a_2=1$, $a_1=0$, $a_0=0$

$\Rightarrow x_0 = \bar{g}_2 + \bar{g}_3 = (0,1,1,0,0,1,1,0)$

(10) (5/6/13)

פענוח לפי רוב קולות

עבור קוד דואלי להמינג עם $G: m\times(2^m-1)$ מרחיבים את הקוד המורחב עם: מט' מגודל $2^m\times(m+1)$, אומר: (נקרא קוד RM מספר ראשון)

$n=2^m \quad k=m+1 \quad d=4$

ולמעשה מבטיחים גם תיקון של שגיאה אחת וגילוי של 2 שגיאות

דוגמה- $m=4$ המט' $G:5\times 16$ היא:

$$G=\begin{pmatrix} 1 & 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0 & 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0 & 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0 & 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0 & 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix} \begin{matrix} \bar{g_0} \\ \bar{g_1} \\ \bar{g_2} \\ \bar{g_3} \\ \bar{g_4} \end{matrix}$$

שאר החלקים מקוד מורחב

דואליות להמינג

כל מילה מהקוד מתקבלת ע"י: $\bar{x}=\sum_{i=0}^{4} a_i \bar{g_i}$

מסתכלות על זוגות סמוכים בכל השורות

(זוגות עם אינדקסים 0,1 ; 2,3 וכו...).

מכאן נקבל, עבור a_4, מהתבוננות על שתי הקואורדינטות הראשונות

$a_4=\{x_0+x_1, x_2+x_3, x_4+x_5, x_6+x_7, x_8+x_9, x_{10}+x_{11}, x_{12}+x_{13}, x_{14}+x_{15}\}$

(מתקבל מסכום איברי עמודות $i, i+1$ בכל אחת מן השורות עבור $i\in\{0\}\cup$ זוגיים).

אם אין שגיאות נקבל שכל הקודים זהים.

אם יש שגיאה אחת נקבל שאחד שונה מהשאר.

אם יש 2,3 שגיאות נקבל ש-2,3 שונים מהשאר (בהתאמה)

אם יש 4 שגיאות יש בעיה, אי אפשר לתקן.

$\Downarrow$

כך מתקנים שלוש שגיאות ומתקנים ארבע שגיאות.

באותו אופן, עבור האחרים:

$a_3=\{x_0+x_2,\ x_1+x_3,\ x_4+x_6,\ x_5+x_7,\ x_8+x_{10},\ x_9+x_{11},\ x_{12}+x_{14},\ x_{13}+x_{15}\}$

$a_2=\{x_0+x_4,\ x_1+x_5,\ x_2+x_6,\ x_3+x_7,\ x_8+x_{12},\ \dots\}$

$a_1=\{x_0+x_8,\ x_1+x_9,\ \dots\}$

ואז מסיימים עם הסיבוב הראשון.

לסיבוב השני נגדיר

$$\bar{x}'=\bar{x}-a_1\bar{g_1}-\dots-a_4\bar{g_4}=$$

$$=a_0\bar{g_0}=\begin{cases}(0\dots0)\\(1\dots1)\end{cases}$$

רוב ← אם

אם בפועל יש וקטור משולב עם אפסים ואחדים, מחליטים על הערך של a_0 לפי רוב הקולות בקרב איברי $\bar{x}'$.

כאן, קיבלנו שמתקנים 3 שגיאות ומגלים 4, ולכן $d=8$.

(*) למעשה קוד RM מסדר אחד (כמו הנ"ל) מתקן $2^{m-2}-1$ שגיאות ומגלה 2^{m-2} שגיאות

$\Rightarrow d=2^{m-1}$

כלומר הפרמטרים של הקוד הם $[2^m, m+1, 2^{m-1}]_2$.

<u>קודי RM מסדר גבוה</u>

נגדיר כפל מילים בינאריות כך:

בהינתן $\bar{x}=(x_1,\dots,x_n)$ ו- $\bar{y}=(y_1,\dots,y_n)$ אזי:

$\bar{x}\circ\bar{y}=(x_1y_1,\dots,x_ny_n)$

יהי $r>1$, נגדיר קוד RM מסדר r כך:

נתחיל מקוד RM מסדר 1, עם פרמטר m עם

$$G_1=\begin{pmatrix}-\bar{g_0}-\\-\bar{g_1}-\\\vdots\\-\bar{g_m}-\end{pmatrix}_{(m+1)\times 2^m}$$

נבנה את G: המכפלות של לכל היותר r שורות של G_1 ונוסיף אותן ל-G_1.
G המתקבל מתוך G_r ע"י מחיקת השורות הזהות.
G המתקבלת יוצרת את קוד RM מסדר r.

בקוד זה הקצב משתפר (כי יש מילה), שאר הפרמטרים
נשארים זהים אבל כושר תיקון השגיאות יורד.

⊛ נשים לב: נסמן באופן כללי: $RM(m,r)$

דוגמה - $RM(4,2)$
מתווספות לכל היותר $6=\binom{4}{2}$ שורות (כל לא מתכפלת
במכפלות כי לא ייתן שום דבר חדש.

$G=$

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	$\overline{g_0}$
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	$\overline{g_1}$
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	$\overline{g_2}$
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	$\overline{g_3}$
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	$\overline{g_4}$
0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	$\overline{g_{12}}$
0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	$\overline{g_{13}}$
0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	$\overline{g_{14}}$
0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	$\overline{g_{23}}$
0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	$\overline{g_{24}}$
0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	$\overline{g_{34}}$

מקבלים קוד $[16,11,4]_2$
(4 ← חישוב לפי משקל מינ' של השורות)

עבור הפענוח, נציג $\overline{X}\in C$ באופן הבא:

$$\overline{X}=a_0\overline{g_0}+\dots+a_4\overline{g_4}+a_{12}\overline{g_{12}}+\dots+a_{34}\overline{g_{34}}$$

נבצע הצבעה מרובת סיבובים, עם $3=r+1$ סיבובים:
a_{ij} ⇐ סיבוב ראשון, a_i ⇐ סיבוב שני, a_0 ⇐ סיבוב שלישי.

מהשורה g_{34} נתבונן על 4 סמלים ונקבל

$$a_{34}=\{x_0+x_1+x_2+x_3,\ x_4+x_5+x_6+x_7,\ x_8+x_9+x_{10}+x_{11},\ x_{12}+x_{13}+x_{14}+x_{15}\}$$

$\Leftarrow$ אפשר לתקן שגיאה אחת ולגלות 2.

באותו אופן עבור המשך הסיבוב הראשון.

עבור הסיבוב השני:

$$\overline{x'}=\overline{x}-a_{12}\overline{g_{12}}-\dots-a_{34}\overline{g_{34}}=(x'_0,\dots,x'_{15})$$

אם אין שגיאות אזי $\overline{x'}=a_0\overline{g_0}+\dots+a_4\overline{g_4}$

ואפשר להשתמש באותה שיטת בדיקה ל-RM מסדר 1

משום ש- $d=4$ ואפשר לתקן רק שגיאה אחת ולגלות שתיים, בסיבובים הבאים כבר לא תהיה אפשרות של רוב הכרעה.

(*) באופן כללי עבור $RM(r,m)$, יתקיים:

$n=2^m$

$k=1+m+\binom{m}{2}+\dots+\binom{m}{r}$

מס' סיבובים $= r+1$

מס' בדיקות בסיבוב ראשון 2^{m-r}

הקוד מתקן $2^{m-r-1}-1$ שגיאות ומגלה 2^{m-r-1} שגיאות.

<u>קונסטרוקציה אלטרנטיבית</u>

עבור $\mathbb{F}=\mathbb{F}_q$, $m\geq 1$ נתבונן ב:

$$L_m=\{f\in\mathbb{F}_q[x_1,\dots,x_m] \mid f \text{ לינארי}\}$$

L הוא מ"ו מעל $\mathbb{F}_q$, ומתקיים

$$\dim_{\mathbb{F}_q} L=m+1$$

תהי $P=\{\overline{y_1},\dots,\overline{y_n}\}$ אוסף של m-יות של איברי F.

נניח ש $f\in L$ אינו מתאפס בכל איברי P.

מתקיים: (מס' האפסים של $f\in L$) $\leq q^{m-1}$

אם נבחר $n=q^{m}$ זה יתקיים.

נגדיר העתקה $\varphi: L_m \to \mathbb{F}_q^n$ ע"י
$$\varphi(f) = (f(\bar{y}_1), \dots, f(\bar{y}_n))$$
ו- φ לין. נגדיר $C = Im(\varphi) \subset \mathbb{F}_q^n$.

φ חח"ע (לפי ההנחה) אמ"ם $\ker\varphi = 0$ עבור איזה q.

לכן:
$$k = \dim C = \dim L_m = m+1$$
$$d \geq n - q^{m-1}$$

נקח $n = q^m$ ונקבל
$$C = [q^m, m+1, \geq q^m - q^{m-1}]$$

אם $q=2$ אנו נקבל $C = [2^m, m+1, 2^{m-1}] \Leftarrow$ דואלי להמינג.

כך יש לנו הכללה של RM מסדר ראשון ל-q כלשהו.

<u>גרסה הומוגנית של קונסטרוקציה זו</u>

נסמן $L'_m = \{f \in \mathbb{F}_q[x_1, \dots, x_{m+1}] \mid$ לינארי הומוגני $f = \alpha_1 x_1 + \dots + \alpha_{m+1} x_{m+1}\}$

$L'_m / \mathbb{F}_q$ הוא מרחב וקטורי, ומתקיים $\dim L'_m = m+1$

נבחר קב' $P = \{\bar{y}_1, \dots, \bar{y}_n\} \subset \mathbb{F}_q^{m+1}$ ש $\bar{0} \notin P$ ומתקיים:

אם $\bar{y}_i \in P$ אז לכל $\alpha \neq 1$: $\alpha \bar{y}_i \notin P$.

נגדיר: $\varphi: L'_m \to \mathbb{F}_q^n$ ע"י $\varphi(f) = (f(\bar{y}_1), \dots, f(\bar{y}_n))$

מספר האפסים של $f \in L'_m$ $\leq q^m$

$0 \notin P$ וגם אם $f(\bar{y}_i) = 0$ אזי $f(\alpha \bar{y}_i) = 0$

לכן
$$\text{מס' האפסים של } f \text{ בתוך } P \leq \frac{q^m - 1}{q-1}$$

נגדיר $C := Im(\varphi) \subseteq \mathbb{F}_q^n$, אם n מספיק גדול אזי φ חח"ע

ולכן
$$K = \dim C = \dim L'_m = m+1$$

$$C = [n, m+1, \geq n - \frac{q^m - 1}{q-1}]$$

נקח $n = \frac{q^{m+1}-1}{q-1}$ ונקבל
$$C = \left[\frac{q^{m+1}-1}{q-1}, m+1, q^m\right]_q$$

אם $q = m = 2$:
$$C = [7, 3, 4]_2$$