קליפ מרקני שאלות (27/2/23) ①

שרון מרכז קונינסקי
מחשב פרון, בניין 216
רחוב שטרא בהתיה
קרית ליאתי

מרכז לחלוקת | בקורס נתמקד בקליפ מרקני שאלות
1) שפת סופיות
2) שפות – חוזי הליזמים/אוקיאנוסים

1) רוצים לשפר השפה כלשהי, אבל שינוי השרשרת מקרב.
אפשר לשמור את השרשרת הישנה רוצים שהוא יהיה
קל הרבה הסופית הקרובה ביותר.

$$\underbrace{10\cdots10111101}_{\text{32 פחות 1 פחות}} \longrightarrow \underbrace{1\cdots111}_{\text{כל הפחות}}$$

קיבלנו שיש שיפור ורוצה פחות, נשתמש בשפה השלילה נקרא
שהמקור שהתחיל היה 1,
ואז אפשר לעבור בתוכנית ולהחליף את כל הפחות
למילה.

שאלת בונוס לשרון שהשאלה הקודמת מהסתיימה
ואבל אי אפשר היה לעשות בקלות יותר כמעט
כמעט בשיעור כי יש בעיה-יומה כאן ואנו יותר כמעט
למילה.

בהרצאה שלנו, ראינו שקבוע הזמן הוא $\frac{1}{001} = 2$
(יותר משתמשים להפחית).

2) נניח שרוצים לחשוב אפס פיסות שהוריק הן $a_{n-1}\cdots a_0$
סוף סוף כדי קוד, קוד לא הצליח.
נניח נתון!

נשתמש אלה $a_{n+1}a_n\cdots a_1$.

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

נוסף לאחר (בטופל) סיום a_{n+1} שהיה
$a_n\cdots a_1$ שרוצים לחשוב אפס פיסות שהוריק הן
סוף סוף כדי קוד, קוד לא הצליח.
נניח נתון!

שמתקיים לפחות אחת.

לפחות קוד אם מתקיים $R = \frac{k}{n}$ יש קידוד אלגוריתם יעיל

ולפחות שגיאה אחת.

הערה: הוכח שקוד כזה מתקן למעלה משני שגיאות

$\beta_4 - \beta_7$: מכיוון שמיפוי מופלגו 2

$\beta_3 - \beta_1$: מכיוון שזה מופלגו 2

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

נבנה מטריצה מהצורה:

ג) נניח שנקבל לשדה עם איברים $\beta_1 \beta_2 \ldots \beta_q$

כמו קוד לא מקיים לינאריות.

שזה הקוד הפלט.

ואפס היטב לתיקון השגיאות שאכן מגיעה מגישה למה

קבלה הקוד יהיה $R' = \frac{k+1}{n}$ כלומר הקבוע שקוד

שיוכח חצבת של הקוד.

אז: יהי הקוד הינארי שגיאה, נוכל לקבל, למשל,

מקודלו ב).

אזי $\Sigma = 1 \Rightarrow$ יש שגיאה (שכן $\alpha_1 + \alpha_2 + \ldots + \alpha_{k+n} \equiv 0$)

ונשאר $\alpha'_1 + \alpha'_2 + \ldots + \alpha'_{k+n} = \Sigma$.

$$\alpha_1 \ldots \alpha_n \alpha_{n+1} \ldots \alpha_{k+n} \longrightarrow \alpha'_1 \ldots \alpha'_n \alpha_{n+1} \ldots \alpha_{k+n}$$

נשאר את הקוד ונקבע

בהינתן x, y, z נאמר שd היא מטריקה אם מתקיים
לכל x, y, z וd המוגדרת עליהם, כך שd מקיימת את
התכונות הבאות

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

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

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

מרחב המינג

יהי $x \in \Sigma^n$ ו$y \in \Sigma^n$:
$x = (x_1 \dots x_n)$; $y = (y_1 \dots y_n)$

נגדיר
$d(x,y) = |\{i : x_i \neq y_i\}|$

יהי Σ אלפבית סופי.

מרחב המינג

$d(x,y) = |\{i : x_i \neq y_i\}|$ נגדיר $x, y \in \Sigma^n$.

Σ - אלפבית סופי.

$q = |\Sigma|$.

Σ^n - קבוצת כל המילים באורך n מעל Σ.

$B_r(x) = \{y \in \Sigma^n : d(x,y) \leq r\}$ - כדור סגור ברדיוס r סביב x.

$V_q(n,r) = |B_r(x)|$ - נפח הכדור ברדיוס r במרחב Σ^n.

$V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$

$B_r(x) = \{y : y \text{ נבדל מ-} x \text{ ב-} 0, 1, \dots, r \text{ מקומות}\}$

$|B_r(x)| = \sum_{i=0}^{r} |\{y : y \text{ נבדל מ-} x \text{ ב-} i \text{ מקומות}\}|$

$= \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$

$\binom{n}{i}$ - בחירת i מקומות מתוך n

$(q-1)^i$ - בחירת i אותיות שונות מ-x בכל מקום

דוגמה

$\Sigma = \{0,1\}$, $n = 3$, $r = 1$

$B_1(000) = \{000, 100, 010, 001\}$

$V_2(3,1) = \binom{3}{0} + \binom{3}{1} = 1 + 3 = 4$

משפט

$V_q(n,r) \leq q^{n - \log_q V_q(n,r)}$

הוכחה

נבנה קוד C באופן חמדני:

$C_0 = \emptyset$

$C_{i+1} = C_i \cup \{x\}$ כאשר $x \notin \bigcup_{c \in C_i} B_{2r}(c)$

נעצור כאשר $\bigcup_{c \in C} B_{2r}(c) = \Sigma^n$

$|C| \cdot V_q(n,2r) \geq q^n$

$|C| \geq \frac{q^n}{V_q(n,2r)}$

$|C| \leq q^{n - \log_q V_q(n,2r)}$

$\log_q V_q(n,2r) \geq \log_q V_q(n,r)$

$|C| \leq q^{n - \log_q V_q(n,r)}$

מסקנה

$V_q(n,r) \leq q^{n - \log_q V_q(n,r)}$

משפט

$V_q(n,r) \geq q^{n - \log_q V_q(n,2r)}$

הוכחה

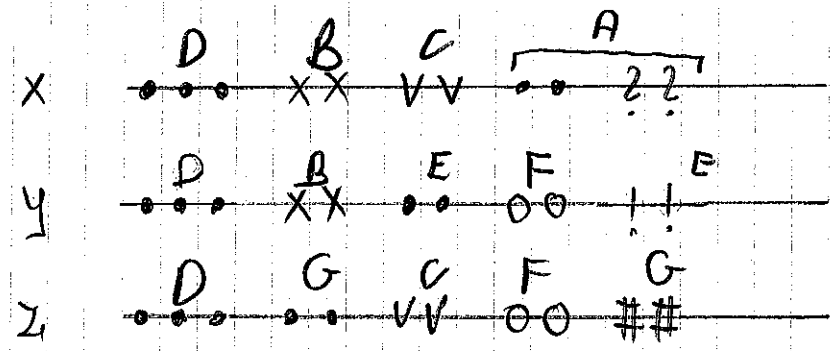
C - קוד מקסימלי עם מרחק $2r$.

$\bigcup_{c \in C} B_{2r}(c) = \Sigma^n$

$|C| \cdot V_q(n,2r) \geq q^n$

$|C| \geq \frac{q^n}{V_q(n,2r)}$

$|C| \geq q^{n - \log_q V_q(n,2



לפניך G מידה שהמרחקים בינהם מתקיים. מתקיים:

X:				
מרחק	x	xy	xz	xz,xy
אורך	A	B	C	D

$$A+B+C+D=U$$

Y:				
מרחק	y	xy	yz	xy,yz
אורך	E	B	F	D

$$E+B+F+D=U$$

Z:				
מרחק	z	xz	yz	xz,yz
אורך	G	C	F	D

$$G+C+F+D=U$$

מתקיים:

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

$$\Downarrow$$

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

הוכיחו כי d מגדירה מטריקה על U אם ורק אם לכל $x\neq y$ מתקיים $d(x,y)>0$.

1) d מגדירה מטריקה על U אם לכל $x,y,z\in U$ מתקיים (אי-שוויון המשולש) $d(x,z)\leq d(x,y)+d(y,z)$

2) יהי $c\in U$ קבוע. נגדיר $g:U\to\mathbb{R}$ על ידי $g(x)=d(x,c)$. נקרא לקבוע c נקודת המרכז של g אם $g(c)=\min_{x\neq c} g(x)$.

הוכיחו כי אם U מכיל יותר מנקודה אחת, אזי לכל נקודה $c\in U$ מתקיים $g(c)<2$.

$\frac{u}{p}=\rho$ מרחק מינימלי, ו-

לכל $\frac{u}{u}=R$ קבוע

נסמן $\mathbb{F}_{p^n}=\mathbb{F}_q$ שדה סופי עם $q=p^n$ איברים. קוד $[n,k,d]_q$ מעל $\mathbb{F}_q$:

פרמטרים של קוד

נרצה למצוא k ו-d כפונקציה של n.

$$\Leftarrow d(x,z)\geq t \text{ ולכל } d(y,z)\geq t$$

נרצה למצוא $z=(y_1,\dots,y_t,x_{t+1},\dots,x_n)$

$$x=(\underbrace{x_1,\dots,x_t}_{\text{שלושים כמו } y},x_{t+1},\dots,x_n)$$

$$y=(\underbrace{y_1,\dots,y_t}_{\text{שלושים כמו } y},y_{t+1},\dots,y_n)$$

אם $d(x,y)\geq 2t$ אז קיימות $z\neq x$ כאלו $d(x,z)=t$ ו-$d(z,y)=t$

+ שיטה:

(*) כאן n, אם $d(x,y)\geq 2t$ אז הקוד C הוא יכול לתקן t שגיאות.

כך אז אלגוריתם טוב כי הסיבוכיות היא $O(n^2)$ (אקספוננציאלי)

הגדרה

ומצאנו מינימום.

ואז עוברים על כל $y\neq x$ ומחפשים את y מינימלי

$$d(z,y)>d(x,z)$$ שמקיים

$$\{z\mid d(z,y)=1+t \text{ עבור } x\neq y\}$$

קיבלנו

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

נשים לב ש: $d(z,y)+t\geq d(x,y)\geq 1+2t$

ומכאן, הכי טוב שאפשר לקוות זה z שמרחיק את x.

לכן אלגוריתם שמקבל y מוצא את z שמרחיק את x:

נסמן ב-z את האיבר המתקבלת אחרי $t\geq x_j$.

ונסמן את x_j בשכנות הסופית ב-x, וזה $t\geq x_j$.

אם x_i שונה מכל y_i אז $1+2t\geq d(x,y)$. זה שמשאירים אותו x,

הוכחה

ושני אלו הן מקרים לשמשה קשה למצוא שלה קופים.

2) מקרה שבו ב-R יש תכונה: $\forall a,b \in R \; (ab=0 \Rightarrow a=0 \text{ או } b=0)$

1) מקרה שבו ב-R תכונה: $\exists a,b \in R \; (ab=0 \text{ ו-} a\neq 0 \text{ ו-} b\neq 0)$

קופים

על קופים מהן $a\neq 0$ $b\neq 0$

אף קשה, למן מה שנקבע בין תכונות משפחות

נקבע a,b שנקבע (נקבע שזה ווירוק יהיו, שבוע).

נקבע המבנה $a \longrightarrow a$ $b \longrightarrow b$

מציאות קרני הפרמטרים היחסיים a,b כאשר $a \to b$:

בעיות אסימפטוטיות

* יהיו a_n, b_n נתונים, הוכיחו אומן נקבע n קטן.
* מיותר (בפי להמצא כמה שמתחיל כפלי) $\Leftarrow$ נקבע a קפוץ.
* יהיו a_n, b_n נתונים, ונקבע אות הקבע הטוב קל לתקן $\Leftarrow$ נקבע a קפוץ.
* יהיו a_n, b_n נתונים, בני שהיה כמה שיותר

5) אידיאל I של $\mathbb{F}[x]$ הוא ראשי כאשר: $I=(f)$.
6) תהי $\mathbb{F}$ שדה סופי, כלומר: $\mathbb{F}[x]$ תחום ראשי, כלומר:
(שדה מקומן). $\deg(pq)=\deg p+\deg q$ $\deg(p+q)\le\max\{\deg p,\deg q\}$
פיצוי p ראשוני, נקרא: $\mathbb{F}_p=\{\overline{0},\overline{1},\dots,\overline{p-1}\}$
(מלאי סוף לכתוב, אפשר לאיפה, סוף 1 ל-1 והלאה)
7) לכל p קיים שדה יחיד $\mathbb{F}_q$ עד כדי איזומורפיזם $q=p^n$
1) שדה בן q איברים קיים אמ"מ $q=p^n$ (p ראשוני, $n\ge1$)

שאלות סמ"ם

1) $\deg(pq)=\deg p+\deg q$
2) $\deg(p+q)\le\max\{\deg p,\deg q\}$
3) $\mathbb{F}$ שדה $\Rightarrow$ $\mathbb{F}[x]$ תחום
4) $\mathbb{F}$ שדה $\Rightarrow$ $\mathbb{F}[x]$ ראשי כך ש $\deg(f)=0$
5) קיים $\mathbb{F}$ שדה כך ש: $|\mathbb{F}|=3$
6) $(x+y)+z=x+(y+z)$
7) $y+z=z+y$

כפי שראינו בקורס יש שתי פעולות בלוגיות חיבור וכפל
תכונות

* יהי $\mathbb{F}$ שדה שבו סדר $\mathbb{F}$ הוא q. אזי $\mathbb{F}=\mathbb{F}_q$
$\Leftarrow$ הוכחנו שהיחידה שהיינו היחידה אקספוננציאלי, אבל לא סגור.
אזי $\mathbb{F}$ שדה ($+$ מקומי), אז $\mathbb{F}$ יכיל תמיד $\mathbb{Z}+$ שלמות.
$R=\frac{\mathbb{Z}}{\mathbb{Z}}$, $Q=\frac{\mathbb{Z}}{\mathbb{Z}}$ קבוצה
$p=\{\exists x\ \text{שלמות}\ \ (h,x)p\}\min=(\mathbb{Z})p$
F- ט"ל. קוד C הינו $C\subseteq F^n$, ומתקיים $|C|=q^k$ כאשר $|F|=q$-

(2) (בוקר)

אידיאל – בקצרה R תחת RCR יקרא אידיאל אם:

A היא תת־חבורה חיבורית של R.

לכל $a\in A$ ו־$r\in R$ מתקיים $ra\in A$.

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

כאן כל A הוא אידיאל של R שנוצר ע"י איבר יחיד $a=2$, כלומר $A=(2)$.

דוגמה: $R=\mathbb{F}[x]$ כאשר $\mathbb{F}$ שדה.

נתבונן בחוג המנה $R=\mathbb{F}[x]/(x^n-1)$ (עבור חוג אינו שדה, אלא רק חוג חילופי).

נשים לב כי אם $R=\mathbb{Z}$, $A=d\mathbb{Z}$ אז $R/A=\mathbb{F}_d$ (כפי שראינו בתרגול).

נשאלת השאלה, אילו $(f)/\mathbb{F}[x]$: הפולינומים g,h שקיים f כך ש־$g-h$ מתחלק ב־f ללא שארית.

לדוגמה:

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

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

בהמשך נראה כי R חוג חילופי, ולכן אידיאל מקסימלי הוא $A=(f)$ עבור f כלשהו.

המקיים שאם $f=gh$ אז g או h הוא הפיך.

כלומר $\mathbb{F}=\mathbb{F}_p$, כלומר אם $f=gh$ אז g או h הוא פולינום מדרגה 0 (קבוע שונה מ־0).

נראה כי $R=\mathbb{F}_p[x]/(f)$ הוא שדה אם"ם f אי־פריק מעל $\mathbb{F}_p$.

נניח כי f פריק מעל $\mathbb{F}_p$, כלומר $f=gh$ כאשר g,h אינם הפיכים.

נשים לב כי $gh=0$ ב־R, אך $g\neq 0$ ו־$h\neq 0$, ולכן R אינו שדה.

נניח כי f אי־פריק מעל $\mathbb{F}_p$.

נראה כי R שדה, כלומר כל איבר שונה מאפס הפיך.

יהי $g\in R$ כך ש־$g\neq 0$.

נשים לב כי $f\nmid g$ (f לא מחלק את g), שכן $\deg g<\deg f$.

מכיוון ש־f אי־פריק, $\gcd(f,g)=1$.

לפי אלגוריתם אוקלידס המורחב, קיימים $a,b\in\mathbb{F}_p[x]$ כך ש־$af+bg=1$.

כלומר $bg=1-af$, ולכן $bg\equiv 1 \pmod f$.

כלומר b הוא ההופכי של g ב־R.

לכן R שדה.

דוגמה: $\mathbb{F}=\mathbb{F}_2$, $f=x^2+x+1$.

f אי־פריק מעל $\mathbb{F}_2$ (בדיקה ישירה).

לכן $R=\mathbb{F}_2[x]/(x^2+x+1)$ שדה מגודל $2^2=4$.

איברי R הם $\{0,1,x,x+1\}$.

$x\cdot x=x^2=x+1$

$x\cdot(x+1)=x^2+x=1$

$(x+1)\cdot(x+1)=x^2+1=x$

$1\cdot 1=1$

$1\cdot x=x$

$1\cdot(x+1)=x+1$

$0\cdot a=0$ לכל $a\in R$.

דוגמה: $\mathbb{F}=\mathbb{F}_2$, $f=x^2+1$.

f פריק מעל $\mathbb{F}_2$, שכן $x^2+1=(x+1)^2$.

לכן $R=\mathbb{F}_2[x]/(x^2+1)$ אינו שדה.

$(x+1)\cdot(x+1)=x^2+1=0$ ב־R.

דוגמה: $\mathbb{F}=\mathbb{F}_3$, $f=x^2+1$.

f אי־פריק מעל $\mathbb{F}_3$ (בדיקה ישירה).

לכן $R=\mathbb{F}_3[x]/(x^2+1)$ שדה מגודל $3^2=9$.

איברי R הם $\{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}$.

$x\cdot x=x^2=-1=2$

$x\cdot(x+1)=x^2+x=x-1=x+2$

$x\cdot(x+2)=x^2+2x=2x-1=2x+2$

$(x+1)\cdot(x+1)=x^2+2x+1=2x$

$(x+1)\cdot(x+2)=x^2+3x+2=x^2+2=1$

$(x+2)\cdot(x+2)=x^2+4x+4=x+1$

$2\cdot 2=4=1$

$2\cdot x=2x$

$2\cdot(x+1)=2x+2$

$2\cdot(x+2)=2x+1$

$1\cdot a=a$ לכל $a\in R$.

$0\cdot a=0$ לכל $a\in R$.

דוגמה: $\mathbb{F}=\mathbb{F}_3$, $f=x^2+x+1$.

f אי־פריק מעל $\mathbb{F}_3$ (בדיקה ישירה).

לכן $R=\mathbb{F}_3[x]/(x^2+x+1)$ שדה מגודל $3^2=9$.

איברי R הם $\{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}$.

$x\cdot x=x^2=-x-1=2x+2$

$x\cdot(x+1)=x^2+x=-1=2$

$x\cdot(x+2)=x^2+2x=-x+2=x+2$

$(x+1)\cdot(x+1)=x^2+2x+1=x$

$(x+1)\cdot(x+2)=x^2+3x+2=x^2+2=-x-1+2=2x+1$

$(x+2)\cdot(x+2)=x^2+4x+4=x^2+x+1=0$

$2\cdot 2=4=1$

$2\cdot x=2x$

$2\cdot(x+1)=2x+2$

$2\cdot(x+2)=2x+1$

$1\cdot a=a$ לכל $a\in R$.

$0\cdot a=0$ לכל $a\in R$.

ג) $(\mathbb{F}_q,+)\cong\mathbb{F}_p^n$ משפט קיום א"א $\mathbb{F}_p$ מאופיין ע"י.

פתרון $(\mathbb{F}_q,+)=\mathrm{span}\{1,x,\dots,x^{n-1}\}$

ד) $(\mathbb{F}_q\setminus\{0\},\cdot)$ חבורה ציקלית סדר $q-1$

כי $\exists g\in\mathbb{F}_q$ כך ש $\forall f\in\mathbb{F}_q\setminus\{0\}$ מתקיים $f=g^m$

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

g נקרא "יוצר" או "איבר פרימיטיבי" של $\mathbb{F}_q$.

ה) יהי $\mathbb{F}_{p^t}$, $\mathbb{F}_{p^s}$; כך ש $t>s$.

אזי $\mathbb{F}_{p^s}\subset\mathbb{F}_{p^t}$ אם"ם $s|t$, ובמקרה

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

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

קודים לינאריים

בהינתן:

אזי $\mathbb{F}_q=F$ שדה סופי בן q איברים, ויהי $C\subseteq\mathbb{F}_q^n$ כזה

שמכנה ווקטורי, אזי $C=\mathbb{F}_q$-תת מרחב, נאמר ש-C קוד לינארי מאורך n.

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

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

בהינתן

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

כלומר $d(C)=\min\limits_{\substack{x,y\in C\\ y\neq x}} d(x,y)$

כאן d $d(x,y)=w(y-x)$ ומתקיים כי d מרחק

שהינו שקול לתכונות הבאות:

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

נגדיר $G=\begin{pmatrix}-e_1-\\ \vdots\\ -e_n-\end{pmatrix}$ המטריצה שמייצרת את C.

$x = \alpha_1 e_1 + \dots + \alpha_n e_n = (\alpha_1, \dots, \alpha_n) G$ כך ש $x \in C$ אם ורק אם x נתון ע"י הצירוף הליניארי

דוגמה

1) קוד שכל המילים בו הן בת"ל. $q = 2$, $k = n$, $C = \{(00\dots0), (11\dots1)\} \subset \mathbb{F}_2^n$

$B = \{(1\dots11)\} \Rightarrow G = (1\dots11)$

2) קוד שכל המילים בו הן בעלות משקל זוגי $C = \{(x_1, \dots, x_{n-1}, x_n) \mid x_1 + \dots + x_n = 0\} \subseteq \mathbb{F}_2^n$

כאן $q = 2$, $k = n-1$

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

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

משפט (תנאי)

2) המקודד

יהי H מטריצה מעל $\mathbb{F}_q$ בגודל $(n-k) \times n$ אזי H נותנת העתקה $H : \mathbb{F}^n \to \mathbb{F}^{n-k}$

$x \mapsto Hx^t$ ע"י

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

$\dim C = k$

H נקראת מטריצת הבדיקה של הקוד C.

דוגמה

1) יהי C קוד של כל המילים הבינאריות, $H = (1, 1, \dots, 1)$

2) C קוד של המילים: $C = \{(0,0,\dots,0), (1,1,\dots,1)\}$

כלומר כל $x_1 = x_2 = \dots = x_n$

נפרק ל- $n-1$ משוואות: $x_i + x_n = 0 \Rightarrow x_i = x_n$

שזה נותן:

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

יהי G מטריצה מגודל $n \times (n-k)$ שעמודותיה הן בסיס למרחב הפתרונות של המערכת $H^t x = 0$.

מכאן:

$$G_{n\times(n-k)}^t H^t = 0_{(n-k)\times n}$$

משוחלפת

יהי C קוד לינארי, G מטריצה יוצרת ו-H מטריצת בדיקת זוגיות. אזי

$\left.\begin{array}{l} 0=\xi_3 \Rightarrow \text{אין} \quad \text{תלויות} \quad \text{ב-} \quad x_1,x_2,x_3 \\ 0=x_2 \Rightarrow \text{אין} \quad \text{תלויות} \quad \text{ב-} \quad x_1,x_3 \\ 0=x_1 \Rightarrow \text{אין} \quad \text{תלויות} \quad \text{ב-} \quad x_3 \end{array}\right\} \Rightarrow$ מציאו מערכת בדוגמה הבאה:

$x_1=\xi_1$ $x_2=\xi_2$ $x_3=\xi_3$ נסמן $\xi=(\xi_1,\xi_2,\xi_3)$, אזי: $\xi\in[1,4]$ מתקיים $x\in\mathbb{R}$ לכל

$$\begin{aligned} \xi_3 &:= x_1+2x_2+3x_3+4x_4 \\ \xi_2 &:= 2x_1+3x_2+4x_3+5x_4 \\ \xi_1 &:= 3x_1+4x_2+5x_3+6x_4 \end{aligned}$$

נמצא את פתרון המערכת הבאה: נסמן בראשי המשתנים $x_1,\dots,x_4$

$$\begin{aligned} x_1+2x_2+3x_3+4x_4 &:= y_1 \\ 2x_1+3x_2+4x_3+5x_4 &:= y_2 \\ 3x_1+4x_2+5x_3+6x_4 &:= y_3 \end{aligned}$$

נדרג את $A=\begin{pmatrix}1&2&3&4\\2&3&4&5\\3&4&5&6\end{pmatrix}$ (בלי לכתוב במפורש)

נבחין אחרי פעולה $t=3$:

(*) אם $y_3=0$ אז יש פתרון (ראינו בהרצאה).

כי $x_4=p$ ולכן יש אינסוף.

(*) אם $y_3=5$ אז מקבלים סתירה $0=1$ לכן למערכת אין פתרון.

לסיכום אומרנו:

כי נתון כאן $\xi=p$ אחרת לקוד לא $\xi=b'h=u'$ ו-

כיצד נמצא קוד הלינארי שמרחקו $\xi=p$ ביחס $d=p$

סימון לקוד לינארי כלשהו: $b[p,u]$

קוד הנגדי

קודים לינאריים (3/2/21) ③

מתקיים $Hx=0 \Leftarrow Cx$ ומכיוון שמשקל המינימום הוא 3,
נניח ש $x \neq 0$ שמקיים $wt(x)=1$: $(0,\dots,0,1,0,\dots,0)=x$
כלומר $(i=1,\dots,n)$ $x_1h_1+x_2h_2+\dots+x_nh_n=0$

נניח בשלילה שקיים C לינארי עם מרחק 3,
כלומר $\exists x,y \in C$ שונות כך ש $d(x,y)=1$.
אז $x-y$ הוא וקטור במשקל 1 ב C בסתירה לכך ש H מטריצת הבדיקה של C.

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

$$C=\{x \mid Hx=0\}=\{(x_1,x_2,x_3,x_4,x_5,x_6,x_7) \mid x_1+x_2+x_3+x_5=0,\ x_1+x_2+x_4+x_6=0,\ x_1+x_3+x_4+x_7=0\}$$

נמצא את $G_{4\times 7}$ כאשר $GH^t=0$ (משהו כזה בערך)

$$G_{4\times 7}=\begin{pmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{pmatrix}$$

תשובה סופית מטריצת

$\Leftarrow$ קיים c_2 שמשקלו 2.
$c_3=0 \Rightarrow$ זוגי שגיאה ב x_1x_2
$c_2=0 \Rightarrow$ זוגי שגיאה ב x_1x_3
$c_1=0 \Rightarrow$ זוגי שגיאה ב x_2x_3
$c_3=1$ אי זוגי שגיאה ב $x_1x_2x_3$

הוכיחו שאם f ו-g שלמות אז גם $f+g$ שלמה.

בשאלה זו נוכיח את $Z(h)$ עבור כמה h ונסיק מכך על $Z(f)$:

1) נחשב את $Z(h)$:

נוכיח שכל מעקף מלא שייך לF_p^n אחת ויחידה:

נוכיח שכל x שייך לF_p^n אחת לכל היותר:

נניח בשלילה שx שייך לF_p^n u ולF_p^n v כאשר $u \neq v$.

נסמן $w := u - v$.

אזי $w \neq 0$ ו$x + w = x$.

$\Rightarrow$ נניח בשלילה שקיים $x \neq 0$ כך ש$x + w = x$, ומאותו טעם נקבל $x + 2w = x$, $x + 3w = x$ וכו'.

נוכיח שכל x שייך לF_p^n אחת לפחות:

נסמן $m := \min_{x \in F_p^n} \{\text{מספר המעקפים של } x\}$.

נניח בשלילה ש$m > 0$ ונסמן בx את $x \in F_p^n$ שמקיים זאת.

נסמן $y := x + w$.

נשים לב שy מקיים $m - 1$ מעקפים, שכן אם $y + w' = x$ אז $x + w + w' = x$ ו$w + w' \neq 0$ (כי $w' \neq w$).

נסיק שy מקיים $m - 1$ מעקפים, בסתירה למינימליות של m.

נסיק ש$m = 0$, כלומר כל x שייך לF_p^n אחת לפחות.

נסיק ש$Z(h) = p^n$.

2) נחשב את $Z(f)$:

נסמן $X := \{x \mid f(x) = h(x)\}$.

נסמן $Y := \{x \mid f(x) \neq h(x)\}$.

נשים לב ש$X \cup Y = F_p^n$ ו$X \cap Y = \emptyset$.

נסיק ש$|X| + |Y| = p^n$.

נסיק ש$Z(f) = |X| = p^n - |Y|$.

נוכיח ש$|Y| = Z(h)$:

נסמן $Y_1 := \{x \mid f(x) = 0, h(x) = 1\}$.

נסמן $Y_2 := \{x \mid f(x) = 1, h(x) = 0\}$.

נשים לב ש$Y = Y_1 \cup Y_2$ ו$Y_1 \cap Y_2 = \emptyset$.

נסיק ש$|Y| = |Y_1| + |Y_2|$.

נוכיח ש$|Y_1| = |Y_2|$:

נגדיר $\varphi : Y_1 \to Y_2$ על ידי $\varphi(x) = x + w$.

נוכיח שφ חח"ע:

נניח ש$\varphi(x) = \varphi(y)$.

נסיק ש$x + w = y + w$.

נסיק ש$x = y$.

נוכיח שφ על:

יהי $y \in Y_2$.

נסמן $x := y - w$.

נשים לב ש$x \in Y_1$ ו$\varphi(x) = y$.

נסיק ש$|Y_1| = |Y_2|$.

נסיק ש$|Y| = 2|Y_1|$.

נסיק ש$Z(f) = p^n - 2|Y_1|$.

נסיק ש$Z(f) \equiv p^n \pmod 2$.

נסיק ש$Z(f) \equiv Z(h) \pmod 2$.

נסיק ש$Z(f) \equiv 0 \pmod 2$.

נסיק שf שלמה.

ג) נשתמש את $x:=y-h$.

לכן יתכן $f(x)=g(x)$ אם ורק אם f,g שוות.

יהי C קוד ליניארי עם $n=63, k=51, d=5$

$$R\approx 0.8$$
$$|C|=2^{51}\approx 10^{15}$$
$$2^{63}-2^{51}=2^{12}\cdot 504$$

אם המילים:

והקוד מתקן את כל השגיאות

לכן הפיענוח של G הוקטורים מהמשקל $1,2$

$$m(y)=x \Leftarrow \text{קיים}$$
$$m(y)=\text{לא ידוע} \Leftarrow \text{אחרת}$$

זה נקרא מפענח לפי קרוב ביותר אותו אנו נתן

קודים בלוקיים

יהי $\mathbb{F}_q$ שדה סופי. נזכיר ש-$\mathbb{F}_q[x]$ הוא תחום (למעשה, תחום ראשי). נסמן $R=\mathbb{F}_q[x]/(1-x^n)$ (כאשר $(1-x^n)$ הוא האידיאל הנוצר ע"י $1-x^n$).

$\mathbb{F}_q^n$ הוא מודול מעל $\mathbb{F}_q[x]$ שבו הכפל בפולינום $f(x)$ משמעו הפעלת $f(T)$ על וקטורים, כאשר $T=(b\ a)$. נשים לב שמעל $\mathbb{F}_q[x]$ יש הרבה סקלרים (שאין להם הופכי) ולכן $\mathbb{F}_q^n$ אינו מרחב וקטורי. לעומת זאת, $\mathbb{F}_q^n$ הוא מודול נותרי ונותרי מעל $\mathbb{F}_q[x]$ (כלומר, כל תת-מודול נוצר סופית). לכן גם R הוא מודול נוצר סופית.

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

הפעולה הנ"ל הפיכה ומעבירה את הכפל בפולינום לפעולות הבאות:

- הזזה ימינה (כפל ב-x והצמצום מודולו $1-x^n$ משמעו לקיחת השארית)
- הזזה שמאלה (כפל ב-x^{-1})

הגדרת קודים בלוקיים

יהי $\mathbb{F}_q$ שדה סופי. קוד בלוקי הוא תת-קבוצה $C\subseteq\mathbb{F}_q^n$. אם C הוא תת-מודול של $\mathbb{F}_q^n$ מעל $\mathbb{F}_q[x]$ נאמר ש-C הוא קוד לינארי. אם C הוא תת-מודול נוצר סופית, נאמר ש-C הוא קוד מרחבי.

דוגמאות

1) C הוא קוד לינארי מעל $\mathbb{F}_2$ שיש לו מטריצה יוצרת

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

במקרה זה, הפרמטרים הם $n=4$, $|C|=q^k=2^2=4$, $q=2$, $k=2$, $n=4$.

כמו כן, מתקיים: $C=\{(0000),(1111),(1010),(0101)\}$.

2) C הוא קוד לינארי מעל $\mathbb{F}_2$ שיש לו מטריצת הבדיקות

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

(מעל $\mathbb{F}_2$).

1 2 3 4 5 6 7

כאשר שקול לקוד המינימלי (לפי ההגדרות מהשיעור הקודם).

והוא גם בלוקי (העתקה בהמשך)

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

R מתקיים $f,g\in \mathbb{F}_q[x]$ שארית של f ו g מחלקים ב-$\mathbb{F}_q[x]$ ב-x^n-1.

מתקיים, בהינתן $\bar{f},\bar{g}\in R$ נסמן $f,g\in \mathbb{F}_q[x]$

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

נוכיח את שלושת הסעיפים הנ"ל עבור R.

דוגמה $q=2$, $n=5$

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

נחשב $a\cdot b$:

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

$$a(x)b(x)=1+x+x^2+\underbrace{x^4+x^3}_{\text{מקבילים}}+\underbrace{x^4+x^5}_{\text{מקבילים}}+\underbrace{x^7+x^4}_{\text{מקבילים}}+\underbrace{x^5+x^8}_{\text{מקבילים}}=$$

(מעל $\mathbb{F}_2$)

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

נזכיר כי $R=\mathbb{F}_2[x]/(x^5-1)$:

נשים לב שלפי $f=x^5,\ g=1$ מתקיים $\bar{f}=\bar{g}$

לכן ב-R: $x^8=x^3$, $x^7=x^2$, $x^6=x$

ולכן ב-R:

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

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

לכן, מהמשך ניתן לקרוא ל c בתור קב' ב-$R=\mathbb{F}_q[x]/(x^n-1)$ משפט

קוד $R\supset C$ הוא קוד לינארי אמ"מ C הוא אידיאל.

בהצגת מקבוצה R חוג, $R\supset A$ אידיאל אמ"מ:

$$\begin{cases} 1)\ 0\in A \\ 2)\ \text{לכל } a\in A \text{ קיים } -a\in R \\ 3)\ \text{לכל } a,b\in A \text{ גם } a+b\in A \end{cases} \iff (R,+)\subset A$$ תת חבורה של

תרגיל בית לפני R תחום שלמות: הוכיח.

הוכחה

$(\Leftarrow)$ נניח ש- $R \subset C$ איזומורפי, נוכיח שהוא צפוף.

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

נתבונן ב- $xa(x)$ כלומר R:

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

(איזומורפיזם)

$\Rightarrow \exists (a_{n-2}, \dots, a_0, a_{n-1}) = a'$ ולכן C קוד צפוף.

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

ונתבונן ב- $r(x)a(x)$:

$$r(x) = r_0 + r_1 x + \dots + r_{n-1} x^{n-1}$$

מתקיים $r_0 a(x) \in C$ מקוד לינארי (צפוף $\Rightarrow$ לינארי)

$xa(x) \in C$ מהצעד

ולכן, מלינאריות וצפיפות, לכל i: $x^i a(x) \in C$

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

ולכן C אידיאל כפי שרצינו.

* מתורת החוגים ידוע:

R חוג יחידה (integral domain), תחום $\mathbb{Q}$ אידיאל R נקרא ראשי (principal ideal) אם קיים $c = g(x)$ כך ש- $\langle g \rangle = C$.

לכן, כדי להוכיח ש- C הוא אידיאל מספיק להוכיח שהוא סגור לחיבור וכפל בסקלר.

נפרק את $1 - x^n$ לגורמים אי פריקים:

$$1 - x^n = f_1(x) f_2(x) \cdots f_m(x)$$

ונקבל $g(x) = f_1(x) \cdots f_{m-1}(x)$ ($m \geq 2$) ומקבלים מענה קוד צפוף

$\langle g(x) \rangle = C$.

מהרעיון $h(x) = 1$, C שונים כך שלכל

$$H=\begin{pmatrix} h_0 & h_1 & h_2 & \cdots & h_{n-1} & 0 & \cdots & 0 \\ 0 & h_0 & h_1 & \cdots & h_{n-2} & h_{n-1} & 0 & \cdots \\ \vdots & & & & & & & \\ 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{n-1} & \\ 0 & \cdots & \cdots & 0 & h_0 & \cdots & h_{n-2} & h_{n-1} \end{pmatrix}_{n\times(n-m)}$$

ומטריצת המקדמים תהיה

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

אלגוריתם

נתון $f(x)$ פולינום יחידי $h(x)=\frac{f(x)}{g(x)}$ מקיים פולינום מוניק.
כאן בדרך $g(x)$ מקדם $c=g(x)$ מקדם בכיתה $f'''(x)$, הנגזרת
מקדמי מקדם בכיתה מוניק-שבירים. קודם בכיתה $f(x)$
כי, $f_{n-m}(x)=1-x^n$ לכאורה יש סבירות

כלומר הכפלה שלו היא 0.
יהיו שורות שהם כפולות הוא שורה קודמת כך
אפס x יהיו שורה של $F(x)$ ולכן $F(x)$
לכן $F'(x)=0$ נמצא $x=0$
$b_i=0$ $\Leftarrow$ בשדה F_q: $u\neq 0$

$$F'(x)=ux^{u-1}$$

סטיה

$$F(x)=x^u-1$$

הכנסה

$GH^t=0$ נזכיר שמתקיים

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

$$=(0\cdots0\ h_k\ h_{k-1}\cdots h_0\ 0\cdots0)\cdot(0\cdots0\ g_0\cdots g_{n-k}\ 0\cdots0)=$$

(i: $i=1$, $j=n-k$:נקבע)

נתבונן על המקדם x^k במכפלה: $g(x)h(x)=x^n-1$

$$c_k=g_0h_k+g_1h_{k-1}+\cdots$$

$$g(x)h(x)=\cdots+c_kx^k+\cdots\Rightarrow c_k=0$$

שהופך בדיוק שזה הפולינום הפולינום, כפרץ?

דוגמה $n=7$, $k=4$

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

נתבונן בקוד $g(x)=x-1\Leftarrow$ $c=(x-1)$

$$g=(1100000)$$

$$G=\begin{pmatrix}1&1&0&\cdots&0\\0&1&1&0&\cdots&0\\&&\ddots&&&\\0&\cdots&0&1&1\end{pmatrix}_{4\times7}$$

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

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

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

אזי קוד לפחות כזה.

נקבל, למשל $g(x)=c(g(x))$ כאשר $g(x)=x^3+x+1$

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

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

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

$$\uparrow\ \uparrow\ \uparrow\ \uparrow\ \uparrow\ \uparrow\ \uparrow$$

$$1\ 2\ 3\ 4\ 5\ 6\ 7$$

שקל לקוד המינג $\Leftarrow$ קוד המינג בינארי

כאן הרי $r=3$ $\quad (1+x^2+x^3)(1+x+x^3)=g(x)$ מתחלק קוד שם תיבות

משפט

הוכחה שם $\quad 2t+1\leq d$ שקיים שם $\quad m-n\geq t$

לכל w נכון $\quad \frac{d-1}{2}$ קיים קוד בינארי מאורך $n=2^w-1$

(13/4/21) ⑤

קיפים בקלות

קוד נקרא בקלי אם $C \subseteq \mathbb{F}_q[x]/(x^n-1)$ אידיאל.

ולאחר מכן, $(x)b = c \Leftarrow (x^n-1) \mid (x)b$ יתקיים פולינום יחיד $h(x) = \frac{x^n-1}{g(x)}$ יתקיים פולינום בודק.

שקילות סופיים

הגדרה

יהי $\mathbb{F}_q$ שדה סופי, $q = p^k$, ויהי $\mathbb{F}_{q^k} \supseteq \mathbb{F}_q$. נאמר ש-$\alpha \in \mathbb{F}_{q^k}$ הוא יוצר מולטיפליקטיבי אם $\mathbb{F}_{q^k}^* = \langle \alpha \rangle = \{\alpha^0, \alpha^1, \alpha^2, \dots\}$

כך שמתקיים

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

כלומר פולינום מינימלי של β הוא: $m(x) \in \mathbb{F}_p[x]$ שהוא יוצר β אחד שהוא פרימיטיבי מעל $\mathbb{F}_q$. נאמר ש- β הוא יוצר אם

$$\mathbb{F}_q^* = \{\beta^0, \beta^1, \dots, \beta^{q-2}\} = \langle \beta \rangle = \langle \beta^{-1} \rangle$$

הפולינום $m(x) = (x-\beta)(x-\beta^q)(x-\beta^{q^2})\cdots(x-\beta^{q^{d-1}})$ הוא כזה שמקיים $\beta^{q^d} = \beta$.

משפט: יהי $\mathbb{F}_{q^m}$ שדה הרחבה של $\mathbb{F}_q$ ויהי $\beta \in \mathbb{F}_{q^m}$. יהי f_i הפולינום המינימלי של β^i מעל $\mathbb{F}_q$ (כלומר $f_i \in \mathbb{F}_q[x]$). יהי $g(x) = \text{lcm}(f_1, f_2, \dots, f_r)$, כאשר r הוא הסדר הכפלי של β (כלומר $\beta^r = 1$ ו-r הוא המינימלי עם תכונה זו). אזי $g(x)$ יוצר קוד בקלי $C = \langle g(x) \rangle \subseteq \mathbb{F}_q[x]/(x^n-1)$, כאשר $n = r$.

הוכחה: נראה שמטריצת הבדיקה H מעל $\mathbb{F}_{q^m}$:

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

נראה שמתקיים $\mathbb{F}_{q^m}/\mathbb{F}_q$ מכיוון שמתקיים u. נעבור מ-$\mathbb{F}_{q^m}$ לקוד בינארי, שמתקבל מ-$\mathbb{F}_q$ כך שכל איבר ב-$\mathbb{F}_{q^m}$ מיוצג ע"י m ביטים. נסמן $\text{lcm}(m_1, \dots, m_r) = w$, ונקבל $\mathbb{F}_{q^w}$. נסמן $\beta^i \in \mathbb{F}_{q^{m_i}}$. כלומר f_i הפולינום שמוגדר ע"י β^i שלו ($i \geq 1$), $\mathbb{F}_{q^{m_i}} \ni \beta^i$.

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

הערה: הוא המספר הקטן ביותר שעבורו $\beta^r = \beta^0$.

אם נרצה ב β (ותצקודנ'ו) ל"י עקודים מאורך m המתו'מים,
נקבע m, מ"ש H' מעל $\mathbb{F}_q$.
הקוד H הינו מ"ש, מפיקות לקוד C.

יהי $c \in C$: $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$

נוכיח $c(x)$ מתלק (לכן שורש) את $b(x)$, לכן $f_b(x)$,
ב β שורש של $c(x)$ ($i \geq 1$), לכן
$$c_0 + c_1 \beta_i + \cdots + c_{n-1} \beta_i^{n-1} = 0$$
$$\Downarrow$$
$$H(c_0, c_1, \ldots, c_{n-1})^T = \vec{0}$$

כלומר
ייתכן שמטריצה H שורות ת"ל ובכך להוכיח.
פירוש: $k = b$, $n - w = m$.
יהי β איבר פרימיטיבי של $\mathbb{F}_{2^m}$. (קיים
(קוד המינ' מוגדר) $C = \{c \mid c(\beta) = 0\}$
$$H = \underset{m \times 1}{(1 \ \beta \ \cdots \ \beta^{n-1})}$$
מעל $\mathbb{F}_{2^m}$

נתון $\beta = \omega$, כלשהו $\in \mathbb{F}_{2^m}$ כאשר β איבר פרימיטיבי;
יהי, $b(x) = 1 + x + x^3$ פולינום מ"מ של β. נמצא
H-ה J-ה.
בסיס של $\mathbb{F}_{2^3}/\mathbb{F}_2$: $B = \{1, \beta, \beta^2\}$
$$\Downarrow$$
שקולן לקוד המינ' מעל $\mathbb{F}_2$ מטריצת הבדיקות:
$$H' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$
$1 \quad \beta \quad \beta^2 \quad \beta^3 \quad \beta^4 \quad \beta^5 \quad \beta^6$
$\beta^3 = 1 + \beta$
$\beta^4 = \beta \cdot \beta^3 = \beta + \beta^2$
$\beta^5 = \beta^2 + \beta^3 = 1 + \beta + \beta^2$
$\beta^6 = \beta + \beta^4 = 1 + \beta^2$

כלומר, קוד BCH משמש כלאחד מהקודים שבהם
מטריצת הבדיקה H מהצורה, ולכן $d(C)\geq 3$.
H, G ו-$\widetilde{H}$ שהוגדרו, כך $|\widetilde{H}|\neq 0$ ולכן
להגדרה כאמור, $\widetilde{H}$ שהתקבלה מ-$(n-1)$ העמודות של H.

$$\widetilde{H}=\begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \beta^4 & & \beta^{2(n-1)} \\ \vdots & & & & \vdots \\ 1 & \beta^{t-1} & \beta^{2(t-1)} & \cdots & \beta^{(t-1)(n-1)} \end{pmatrix}_{(t-1)\times(n-1)}$$

נתון $c=(c_0,c_1,\ldots,c_{n-1})\in C$, כך ש-$c\widetilde{H}^T=0$,
ונוכיח
ש-c הוא קוד BCH עבור β, כך ש-$c(\beta^i)=0$
לכל i.

נתון $w_H(c)=w<d$ (שכן C לינארי, β הוא איבר פרימיטיבי, ו-m_β/m_{β^j}
לכל j). נוכיח כי c הוא קוד BCH עבור β מסדר b.
לכל $1\leq j\leq w$, c מקיים $c(\beta^{b+j-1})=0$ (שכן β^{b+j-1} הוא
שורש של x^n-1 ולכן שייך לאחד המחלקים שם Γ_i, β שייך למחלקה
$\Gamma_{\beta^{b+j-1}}$). נסמן $g(x)=lcm(m_{\beta^b}(x),m_{\beta^{b+1}}(x),\ldots,m_{\beta^{b+w-2}}(x))$
ויהי β השורש ה-n הפרימיטיבי שלכן Γ_1, β שייך למחלקה שבה $(i=1)$
נקבל H_{BCH}

כך מתקיים קוד הגולי שעבור $w=3$ שהוא
בעצמו גולי.
$G_{4\times 11}$ שהיא מטריצה מעל השדה בין 1 ל-51
שבה $w=4$, $n=15$ נקבל:

בהינתן קוד מתקן שדה שגיאות

נתון קוד BCH מעל $q=2$, $m=4$, $\delta=5$, ו- $n=2^4-1=15$

ו- $\ell=1$, אזי $\beta\in\mathbb{F}_{16}=\mathbb{F}_{2^4}$ איבר פרימיטיבי, ונקח

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

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

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

כיוון שעל מנת שיתקיים $\delta=5$ יש לוודא שמכפלת $\beta,\beta^2,\beta^3,\beta^4$ היא פולינום מינימלי.

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

כאשר $m_1(x)$ ניתן לבחור כ פולינום מ"ל, מתוקן, מעלה 4:

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

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

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

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

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

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

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

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

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

ומתקיים כי $d=8$ מקסימלי.

2) נניח קוד BCH שהוא מעל $GF(2)$ עם $n=9$.
לא נתבונן.

1) נתון שאם נשלח את $c=2$ (כלומר, $b=4$) נקבל וקטור
r, כך ש

$$\deg = 10 \; ; \; k=4$$

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

ופ"מ אנו את מה צריך לקבל

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

לפי הגדרה $\beta \neq 2$ כלשהו שמקיים $m(\beta^4) \equiv m(\beta)$

לפי קוד המתקן שגיאות שמקיים

@ (24|4|13)

קודים ציקליים

דוגמה

מקבלים $q=2,\ m=6,\ n=2^m-1=63,\ \beta=\alpha^{63}=1$ יהי β איבר פרימיטיבי ב $\mathbb{F}_{64}$. נגדיר

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

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

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

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

ומכאן שלפחות הקוד $C[51,5,29]_2$

* נתבונן בשדה $\mathbb{F}_{q^m}$ שהוא הרחבה של $\mathbb{F}_q$, ונסמן $\Gamma=Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$. יהי $f\in\mathbb{F}_q[X]$ פולינום אי פריק ממעלה n (ונסמן $\mathbb{F}_{q^m}$ שדה הפיצול של f מעל $\mathbb{F}_q$).

יהי G חבורת גלואה של $\mathbb{F}_{q^m}/\mathbb{F}_q$:

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

(האוטומורפיזם הטריוויאלי על $\mathbb{F}_q$)

מהקשר:

1) G הבורה ציקלית: $G=\langle\sigma\rangle$ כאשר $\sigma(x)=x^q$ (האוטומורפיזם הפרובניוס, $\sigma^i=id$).

2) אוסף השורשים של f בשדה $\mathbb{F}_{q^m}$ הוא אוסף של מסלולים של G (כאשר G פועלת על השורשים של f).

דוגמה

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

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

תהי $f=x^2+1$; $\sigma(i)=-i$ ו-

נשתמש בכך שאם ζ כנ"ל אז $\zeta^{-1}=\zeta^{q-1}$ (כי $\zeta\cdot\zeta^{q-1}=\zeta^q=\zeta$).
נסמן ב- $*$ את הכפל ב- $(\mathbb{F}_{q^n})^*$, ונסמן ב- w את הסדר של q ב- $\mathbb{Z}_n^*$.
נשים לב ש- $|H|=w$, כי $\min\{s>0 \mid q^s\equiv 1 \pmod n\}=w$.
נתבונן בתת-החבורה הציקלית $H=\langle q\rangle$ של $\mathbb{Z}_n^*$.
לכל $i\in\mathbb{Z}_n^*$, $i \pmod n$ יהיה $b\in\mathbb{Z}$ כך ש- $b\equiv i \pmod n$.
נסמן $i\in Hb$ אם $b\in Hb$.
נשים לב ש- $Hb=\{\ldots,b-2q,b-q,b,b+q,b+2q,\ldots\}$.
מכאן ש- Hb מכיל את כל המספרים השלמים b' כך ש- $b'\equiv b \pmod n$.
נסמן $Hb=\{b_1,b_2,\ldots,b_w\}$.
נשים לב ש- $Hb=Hb_1=Hb_2=\ldots=Hb_w$.
נשים לב ש- $Hb_1\cup Hb_2\cup\ldots\cup Hb_w=\mathbb{Z}_n^*$.
נשים לב ש- $Hb_i\cap Hb_j=\emptyset$ אם $i\neq j$.
נשים לב ש- $|Hb_i|=w$ לכל i.
נשים לב ש- $|\mathbb{Z}_n^*|=\varphi(n)$.
נסיק ש- $\varphi(n)=w\cdot k$ עבור $k=\frac{\varphi(n)}{w}$.
נשים לב ש- k הוא מספר הקבוצות Hb_i השונות.
נשים לב ש- k הוא מספר הפתרונות של $q^s\equiv 1 \pmod n$ ב- s.
נשים לב ש- k הוא מספר הפתרונות של $q^s\equiv 1 \pmod n$ ב- s שהם כפולות של w.
נשים לב ש- k הוא מספר הפתרונות של $q^{sw}\equiv 1 \pmod n$ ב- s.
נשים לב ש- k הוא מספר הפתרונות של $(q^w)^s\equiv 1 \pmod n$ ב- s.
נשים לב ש- k הוא מספר הפתרונות של $x^s\equiv 1 \pmod n$ ב- $x=q^w$.
נשים לב ש- k הוא מספר הפתרונות של $x^s\equiv 1 \pmod n$ ב- $x\in\{q^w,q^{2w},\ldots,q^{kw}=1\}$.
נשים לב ש- k הוא מספר הפתרונות של $x^s\equiv 1 \pmod n$ ב- $x\in\{q^w,q^{2w},\ldots,1\}$.
נשים לב ש- k הוא מספר הפתרונות של $x^s\equiv 1 \pmod n$ ב- $x\in\{q^w,q^{2w},\ldots,q^{(k-1)w},1\}$.
נשים לב ש- k הוא מספר הפתרונות של $x^s\equiv 1 \pmod n$ ב- $x\in\{q^w,q^{2w},\ldots,q^{(k-1)w},q^{kw}=

הקואטה של H הן הקבוצות $\gamma^i H$ $(i-w \geq j \geq 0)$. כלומר שעות לחן
לדוגמה $H_{\text{משמאל}} = (\gamma^i)$
לפי $\gamma^i = \sum_{j=0}^{i-w} \gamma^i \gamma^j$ $(i-w \geq j \geq 0)$
לדוגמה כל הקלקות הקבוצות יותר של $\mathbb{F}_{2^w}$ כ"ל של יוצרי סט
לדוגמה מסוים של $\mathbb{F}_{2^w}/\mathbb{F}_2$: $\{1, \gamma, \gamma^2, \dots, \gamma^{w-1}\}$
לדוגמה, הקואוסות H יש שעת כ מאפ, מבחינה כיוון.
לכ"ע ש- $c = (b(x))$ הוא קוד המינ מוכלל.
ויהיו קוד מקבילי $[\gamma^w - u', n]$.
לכן כקוד מתקן שכ"ל יותר.
לכאורה כ- $b = b(x)$, אחד קוד BCH של $\gamma = \gamma^1$
$w = \deg g$; $g_w(x) = (x-\gamma)(x-\gamma^2)\cdots(x-\gamma^{w-1})$ $g_w(x)$

$$\gamma \in \mathbb{F}_{2^r} = \gamma^{w_2} = \gamma^{1-w_2} = \gamma^u$$

כי u כפי שראינו.
נקבל $b = c$, ונשכיל $w = u - w$, כי γ השורש
שקיבלנו קוד המינ

$$(1-x)(x) = 1 - x^{15} \Rightarrow$$

$$\{\gamma^{11}, \gamma^{13}, \gamma^{14}\}; \{\gamma^{10}, \gamma^{5}\}; \{\gamma^{6}, \gamma^{12}, \gamma^{9}, \gamma^{3}\}; \{\gamma^{8}, \gamma^{4}, \gamma^{2}, \gamma^{1}\}; \{\gamma^{0}\}$$

נשים לב $|H| = 4$, ומכאן כי:
שאכן הפולינום $1 - x^{15}$ כיוון $\mathbb{F}_{16}$, וגם $x^{15} - x : \mathbb{Q}$.

⊛ נתקיים תכונת האחידות מהשלילי הקודם: $n = 15 = 4 \cdot 3 = w \cdot k$

ח'ב מתקבלים מקודים שהם הפולינום $1 - x^n$ למעלות קיים שלם.
ב מתקבלים מהקודים ש- $g(x) = g$ אשר $w = |G|$

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

אלא כן שורש של $1 - x^n$. אחד מהם
ולכן $T = \{g(\gamma^i) = 0 \mid i\}$ ולכן כ תכונת ב
ב הוא יוצר כיוון שכל $1 - x^n$.

אין ניתן בדרך נוספת להגיע לקוד המתקנים שיש לשניהם.

נתון C קוד מתאים המתקן t שגיאות, $g(x)=(x-\beta)(x-\beta^2)\cdots(x-\beta^{2t})$, $\beta\in\mathbb{F}_q$ מכפל את C שורשי הפולינום המתקבל $h=n-k$.

כיוון ש H מטריצת הבדיקה של הקוד המינימלי C, $\beta\in\mathbb{F}_q$ מתקיים כי H היא מטריצה $h\times n$, $h=n-k$, ולכן $\mathrm{rank}(H)\le n-k$.

נשים לב כי H מטריצת וונדרמונד $(2t+1)\times n$, $\mathrm{rank}(H)=2t+1$.

לכן $\dim(C)=k\ge n-(2t+1)=n-2t$.

קוד ריד-סולומון (RS)

יהי $\mathbb{F}_q$ שדה סופי, $n=q-1$, β איבר יוצר של $\mathbb{F}_q^*$, $k\le n$.

$$C=\{(f(\beta),f(\beta^2),\ldots,f(\beta^{n-1}),f(1)) : f\in\mathbb{F}_q[x],\ \deg f<k\}$$

C קוד לינארי.

$$\mathrm{ev}_{\beta,n}:\mathbb{F}_q[x]_{<k}\to\mathbb{F}_q^n,\quad f\mapsto(f(\beta),\ldots,f(\beta^{n-1}),f(1))$$

$\mathrm{ev}_{\beta,n}$ העתקה לינארית.

$\ker(\mathrm{ev}_{\beta,n})=\{f\in\mathbb{F}_q[x]_{<k} : f(\beta^i)=0,\ 1\le i\le n-1\}$

$\deg f<k$ ולכן f יש לכל היותר $k-1$ שורשים.

$\ker(\mathrm{ev}_{\beta,n})=\{0\}$, $\mathrm{ev}_{\beta,n}$ חח"ע.

$\dim(C)=\dim(\mathbb{F}_q[x]_{<k})=k$.

C מרחק $n-k+1$.

C קוד MDS.

C קוד $[n,k,n-k+1]$.

C קוד $[q-1,k,q-k]$.

C קוד $[n,k,n-k+1]_q$.

C קוד $[n,k,n-k+1]$ מעל $\mathbb{F}

פתרון

נבדוק תחילה שאי שוויון $\Rightarrow$ נקבל $5=2\cdot 2+1$. לכן

$$5 \le 2t+1 = n-k$$

אז k

קבל k הטוב ביותר נקח $t=2$, ונקבל $d=5$.

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

נסה $\xi=3 \Rightarrow 3^2=2$, אינו פרימיטיבי. נסה $\xi=3$ פרימיטיבי.

$\xi=3 \Rightarrow \xi^2=2$, $\xi^3=6$, וכן הלאה... לכן $\xi=3$ פרימיטיבי.

נקבע $g(x)=(x-\xi)(x-\xi^2)(x-\xi^3)(x-\xi^4)$

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

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

ומתקיים $n=6$, לכן אם נקלף $[5,2,6]$

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

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

נקלף:

מספרים $[6,2,5]$ קוד לינארי. מצא $\mathbb{F}_7$, ומצא $n-k$ פולינום

מספרים $n-k$ מתקיים $d=5$ קוד $[6,2,5]$

מספרים $n-k=6-2=4$

ב-$\mathbb{F}_q^{n+1}$ נתון הקוד הלינארי C שמוגדר ע"י $C=\{(c_1,\dots,c_n,c_{n+1})\in\mathbb{F}_q^{n+1} \mid c_1+c_2+\dots+c_n=0\}$.

קוד המשלים $C^\perp$ הוא קוד לינארי $[n+1,n]$ שמורכב מכל הוקטורים $(c_1,\dots,c_n,c_{n+1})\in\mathbb{F}_q^{n+1}$ כך שלכל $(x_1,\dots,x_n,x_{n+1})\in C$ מתקיים $c_1x_1+\dots+c_nx_n+c_{n+1}x_{n+1}=0$.

תכונות

1) $C^\perp$ הוא $[n+1,n,2]$ קוד MDS.

2) $C^\perp$ הוא קוד הפוך לקוד החזרה $[n+1,1]$: מתקיים $C=[n+1,1]$ כי $(1,\dots,1)\in C$.

3) הקוד $C^\perp$ הוא בעל מילת קוד יחידה $(1,\dots,1,-(n-1))$ ומתקיים $d(C^\perp)=2$.

קודים מוכתבים

יהי C קוד לינארי $[n,k]$ מעל $\mathbb{F}_q$. נסמן: $\mathbb{F}_q^{n+1}\ni\bar{c}=\{(c_1,\dots,c_n,c_{n+1}) \mid (c_1,\dots,c_n)\in C\}$

1) $\bar{C}$ הוא קוד לינארי $[n+1,k]$ שמורכב מכל הוקטורים $(c_1,\dots,c_n,c_{n+1})$ כך ש-$(c_1,\dots,c_n)\in C$ ו-$c_1+c_2+\dots+c_n=c_{n+1}$.

2) $\bar{C}$ הוא קוד MDS.

3) $\bar{C}$ הוא קוד הפוך לקוד $[n+1,1]$ שמורכב מהוקטורים $(1,\dots,1,-(n-1))$ ומתקיים $d(\bar{C})=2$.

קודים מורחבים

1. $\bar{C}$ נקרא ההרחבה הכללית של C, אם $\bar{C}=\{(c_1,\dots,c_n,c_{n+1}) \mid (c_1,\dots,c_n)\in C, c_1+c_2+\dots+c_n=c_{n+1}\}$.

2. $\bar{C}$ נקרא ההרחבה הרגילה של C אם $\bar{C}=\{(c_1,\dots,c_n,c_{n+1}) \mid (c_1,\dots,c_n)\in C, c_1+c_2+\dots+c_n+c_{n+1}=0\}$.

משפט (משפט הסנדלון)

יהי קוד לינארי $C=[n,k,d]_q$ אז קיים קוד לינארי $[n+1,k,d]_q$ אם ורק אם $d\le q^k$.

הוכחה

$\Leftarrow$ נוסיף ל-C שורה של 1-ים ונקבל H שמגדירה קוד $[n+1,k,d]_q$.

$\Rightarrow$ נסמן ב-w את מספר האפסים של שורות H שהן קומבינציה לינארית של $d-1$ שורות אחרות. אז $w=p-1$.

$$p-1\le\left(\begin{matrix}\text{מספר שורות}\\ H\end{matrix}\right)\dim=\operatorname{rank}(H)-d$$

אחרת, $d\le n-k$ (מספר העמודות).

לכן,
$$p\le n-k+1$$
$$n+k-d\ge p$$

נוכיח עתה בצורה שונה משהו את חסם הסינגלטון.

יהי קוד לינארי $C=[n,k,d]_p$ מעל $\mathbb{F}_p$, p ראשוני. $n+k-d\ge p$

הוכחה

נסמן $C=[n,k]$ קוד MDS.

נבחר d עמודות בת"ל ב-H ונסמן H' את המטריצה המתקבלת.

H' מייצגת העתקה $\varphi:\mathbb{F}_p^k\to\mathbb{F}_p^d$ חח"ע ועל.

φ מקבלת כל וקטור ב-$\mathbb{F}_p^d$ לכל היותר פעם אחת.

φ מקבלת כל וקטור ב-$\mathbb{F}_p^d$ בדיוק פעם אחת.

φ מקבלת את 0 בדיוק פעם אחת.

φ מקבלת את 0 לכל היותר

לכל k שלמה. לכן $n=2^k-1$ הוא מספר טבעי. נוכיח באינדוקציה

בסיס

$k=1$ אזי $n=1$ ו-$H_1=(1)$ שלמה.

הנחה

H_k שלמה.

צעד

$H_{k+1}=\begin{pmatrix} 0 & 1\cdots1 \\ 0 & \\ \vdots & H_k \\ 0 & \end{pmatrix}$

נוכיח ש-H_{k+1} שלמה.

יהי $x\in\mathbb{Z}_2^n$, ונסמן $y=Hx$. נראה שניתן לחשב את x מתוך y.

נסמן $x=(z_1,z_2,z_3,z_4,\vec{z})$ כאשר $\vec{z}\in\mathbb{Z}_2^{n-4}$.

$y=Hx=(z_1+z_2+z_4,\ z_1+z_3+z_4,\ z_2+z_3+z_4,\ s(z_1,z_2,z_3,z_4),\ \vec{z})$

נחשב את $s(z_1,z_2,z_3,z_4)$ מתוך y.

אם $z_1+z_2+z_3+z_4=0$ אזי $s(z_1,z_2,z_3,z_4)=0$.

אם $z_1+z_2+z_3+z_4=1$ אזי $s(z_1,z_2,z_3,z_4)=1$.

נסמן $z_1+z_2+z_3+z_4=t$.

נחשב את z_1,z_2,z_3,z_4 מתוך y.

$z_1=y_1+y_2+t$

$z_2=y_1+y_3+t$

$z_3=y_2+y_3+t$

$z_4=t+z_1+z_2+z_3$

נחשב את $\vec{z}$ מתוך y.

$\vec{z}=\vec{y}$

נחשב את x מתוך y.

$x=(z_1,z_2,z_3,z_4,\vec{z})$

x מתוך y.

H_{k+1} שלמה.

$n=2^k-1$ לכל k טבעי.

דוגמה

$H_3=\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & & & & & & \\ 0 & & H_3 & & & & \\ 0 & & & & & & \end{pmatrix}$

$C=[7,4,3]_2$ קוד המינג מגודל

H_3 מטריצת בקרת זוגיות של C.

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

כאשר להוספת שורת אפסים וסיבית זוגיות בסוף כל מילה של H_3 נקבל מטריצת בקרת זוגיות של C.

מטריצת יוצרת שלו 3 מילות שיוצרות אותו שזה H_3 כן בת"ל.

נראה, שכל מילה של הקוד היא צירוף של המילות מטריצת יוצרת

$0\neq1+1+1$

במקרה ש- $k=p$, הקוד C יכול לגלות שגיאות אבל

להקוד מרחק $d=4$.

נסמן $H=H_p$, ויהי $x\in C$, ונניח h מילה שגויה.

נניח $y=Hx=z$

נחשב $\vec{e}\neq(z_1,z_2,z_3,z_4)$ אזי $s(z_1,z_2,z_3,z_4)$ שווה למשקל

אם $\vec{e}=(z_1,z_2,z_3,z_4)$: אז 0 או 4 שגיאות

$z_4\neq0\Rightarrow$ יש שגיאות.

$z_4=0\Rightarrow$ אין שגיאות

לכל k שלמה.

הוכחה: ראינו בהרצאה כי $n=2^k-1$, אזי בקוד n יש

קודי RS מורחבים

משפט

יהי $\mathbb{F}_q$ שדה סופי, $q=p^m$. יהי R קוד RS מעל $\mathbb{F}_q$, ויהי C קוד בR המוגדר ע"י $b[z,z^{-1}b,\dots,z^{-k}b]=C$.

מוכחה. נוכיח $b[1+z,z^{-k}b]=C$.

יהי

$$c\in C \iff c(x)=c_nx^n+\dots+c_1x+c_0$$

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

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

נניח ש-

$$w(c_0,c_1,\dots,c_n,c_{n+1})\le 1+z$$

נכתוב

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

ונשתמש משפט

$$c(1)=a(1)g(1)$$

נבדוק למקרים:

1) $c_{n+1}\neq 0$, נוכיח מהוכח.

$$w(c_0,c_1,\dots,c_n,c_{n+1})\le 1+z \implies w(c_0,c_1,\dots,c_n)\le z$$

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

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

לכן $c(x)$ מתחלק ב-

$$(x-1)(x-\beta^{1+z})\cdots(x-\beta^2)(x-\beta)$$

כלומר BCH עם z תיקון שמקיים לכן $1+z\ge p$

משפט

קוד RS מעל $\mathbb{F}_q$ שדה סופי עם קוד בסיס $b=1+z$ ו-$1+(z-b)-b=1+z$

בניה מקורית לקוד כיף סופית

יהי $b=1$ - נשתמש ב$\mathbb{F}_q$ בלבד השורש:

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

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

$$C=\{[f(\alpha_0),\dots,f(\alpha_{q-1})] \mid f\in T\}$$

שזה בדיוק

הערות

1) $c \in \mathbb{F}_q$

2) c קבוע לינארי (כי T מ"ו מעל $\mathbb{F}_q$)

3) $\dim \ker T = k$:

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

φ הוא מ"ל של מ"ו, והגרעין שלה הוא לכן:

$$\ker \varphi = \{f \mid \varphi(f) = 0 \text{ (כלומר } f \text{ מעל } \mathbb{F}_q)\}$$

כי $f \equiv 0$ הוא הפולינום היחיד ממעלה $\leq k-1$ שמתאפס בכל $\alpha_0,\dots,\alpha_{q-1}$.

לכן הגרעין מתקבל.

4) נוכיח את p: נקח $c = (f(\alpha_0),\dots,f(\alpha_{q-1})) \in c$

ונראה ש $w(c)$.

אם הפולינום של c = אם כמות השורשים של $f \leq k-1$, לכן

$$w(c) \geq q - (k-1) = q-k+1 = n-k+1 = d$$

הסבר: מציאת קוד עם שקול לקוד RS מהסוג

נתבונן ב- $\mathbb{F}_q$ $\alpha_0,\dots,\alpha_{q-1}$ כנ"ל של הקו הישר $\mathbb{A}^1$

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

(∞ הוספת נק' אינסופית)

מתוך הגדרת ההומוגניזציה, נק' של הישר הפרויקטיבי הן $(\mathbb{k}:\eta)$

כך שלפחות אחת מהן אינו שפס, ושם

$$(\mathbb{k}\gamma:\eta\gamma) = (\mathbb{k}:\eta)$$

כיוון הפרויקטיבי כולל הנק'

$$\mathbb{P}^1 = \{P_0, P_1, \dots, P_{q-1}, P_q, P_\infty\} = \{(\alpha_0:1), (\alpha_1:1), (\alpha_2:1), \dots, (\alpha_{q-1}:1), (1:0)\}$$

↑ נק' אינסופית

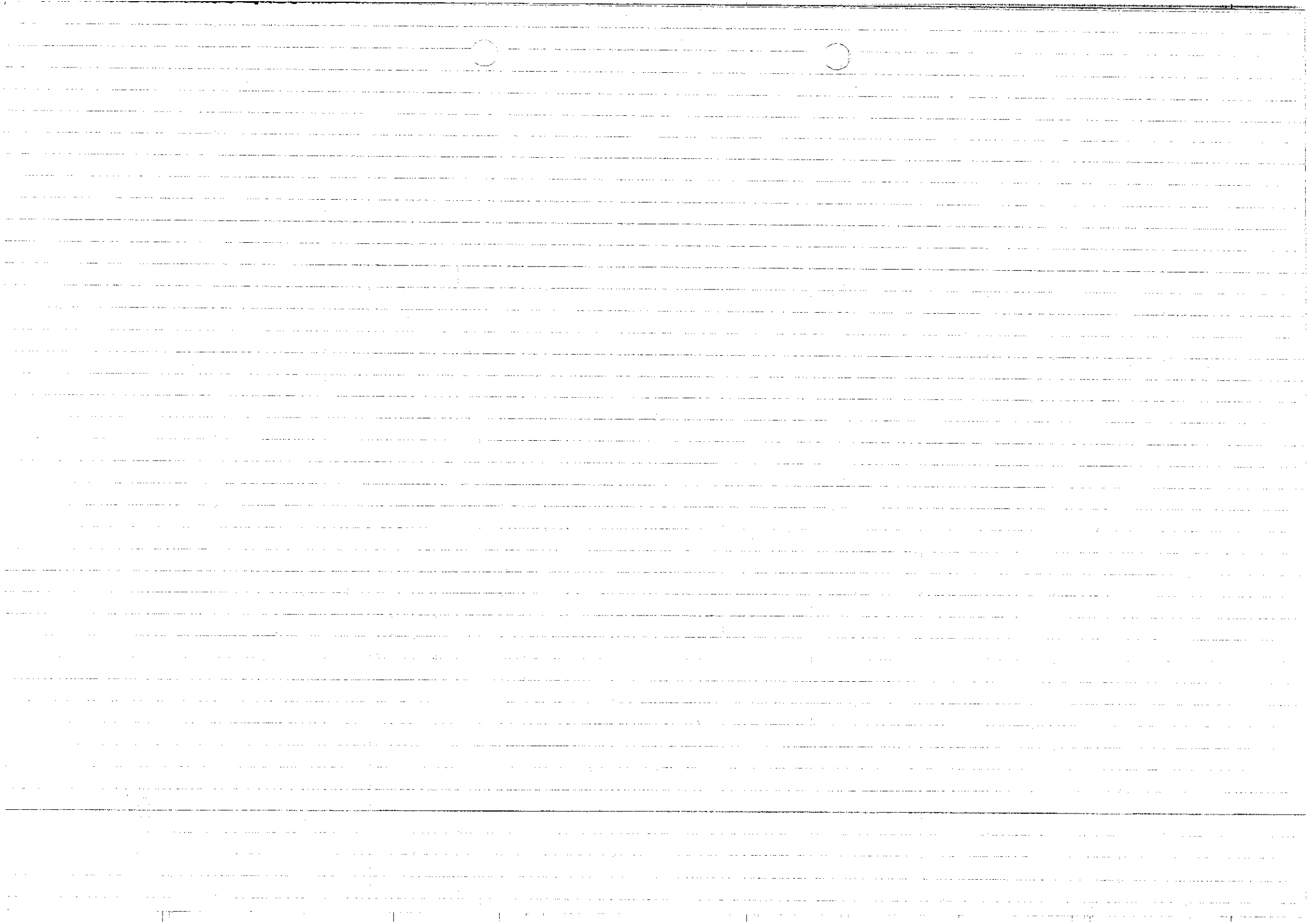
$\mathbb{F}_q$ הוא שדה סופי בגודל q, $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ הרחבה מדרגה m.

$\mathbb{F}_{q^m}$ הוא מ"ו מעל $\mathbb{F}_q$ מממד m.

$\mathbb{F}_q$ הוא מ"ו מעל $\mathbb{F}_q$ מממד 1.

$\mathbb{F}_q^n$ הוא מ"ו מעל $\mathbb{F}_q$ מממד n.

$\mathbb{F}_q^n$ הוא מ"ו מעל $\mathbb{F}_q$ מממד n.



לפי משפט לגרנז', מכאן שכל תת-חבורה H של $\mathbb{Z}_p^*$ מקיימת $|H| = 1$ או $|H| = p-1$. לכן $H = \{1\}$ או $H = \mathbb{Z}_p^*$.

נניח בשלילה ש-g יוצר של תת-חבורה H שאינה טריוויאלית. אז $g^{p-1} = 1$, ולכן g הוא שורש של הפולינום $x^{p-1} - 1$ בשדה $\mathbb{Z}_p$. אבל לפי משפט לגרנז' לפולינום ממעלה d מעל שדה יש לכל היותר d שורשים, ולכן $|H| \leq p-1$. מכאן $H = \mathbb{Z}_p^*$, בסתירה להנחה.

מסקנה $|\mathbb{Z}_p^*| = \varphi(p) = p-1$.

הוכחה נסמן $\mathbb{Z}_p^* = \{g_1, \ldots, g_{p-1}\}$. אז $\{g_1^k, \ldots, g_{p-1}^k\} = \mathbb{Z}_p^*$ לכל k שזר ל-$p-1$. לכן $\prod_{i=1}^{p-1} g_i = \prod_{i=1}^{p-1} g_i^k$. מכאן $\prod_{i=1}^{p-1} g_i = 1$.

משפט (וילסון) $(p-1)! \equiv -1 \pmod{p}$.

הוכחה נסמן $Q = \{1, 2, \ldots, p-1\}$. נגדיר יחס שקילות $\sim$ על Q באופן הבא: $a \sim b$ אם $a = b$ או $a = p-b$. נסמן ב-N את מספר מחלקות השקילות, וב-A את אוסף המחלקות שאיבריהן שקולים לעצמם ($a \sim a$).

מתקיים $|Q| = p-1 = 2N + |A|$.

נתבונן ב-$\mathbb{Z}_p^*$, ונסמן $\mathbb{Z}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$. מכיוון ש-$g^{p-1} = 1$ ו-g יוצר של $\mathbb{Z}_p^*$, נובע ש-$g^{\frac{p-1}{2}} = -1$. נסמן $x = g^{\frac{p-1}{2}}$, ולכן $x^2 = 1$. מכאן $x^2 - 1 = 0$, ולכן $(x-1)(x+1) = 0$. מכאן $x = 1$ או $x = -1$.

נניח בשלילה ש-$x = 1$. אז $g^{\frac{p-1}{2}} = 1$, ולכן $g^{p-1} = 1$. מכאן $|\mathbb{Z}_p^*| \leq \frac{p-1}{2}$, בסתירה לכך ש-$|\mathbb{Z}_p^*| = p-1$. לכן $x = -1$.

נסמן $A = \{a_1, \ldots, a_k\}$. אז $k = |A|$. נגדיר $B = \{a_1, \ldots, a_k, p-a_1, \ldots, p-a_k\}$. מתקיים $B = Q$, ולכן $|B| = p-1$.

נסמן $N = \{b_1, \ldots, b_N\}$. אז $Q = \{b_1, p-b_1, \ldots, b_N, p-b_N\}$.

נגדיר $\mathbb{Z}_p^* = \{g^0, g^1, \ldots, g^{p-2}\}$, אז $|\mathbb{Z}_p^*| = p-1$. נשים לב ש-$g^{\frac{p-1}{2}} = -1$, ולכן $g^{\frac{p-1}{2}} \neq 1$. מכאן $g^{\frac{p-1}{2}} = -1$.

נסמן $x = g^{\frac{p-1}{2}}$, ולכן $x^2 = 1$. מכאן $x = 1$ או $x = -1$.

מסקנה

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

נגדיר $Q = \{ i^2 \mid 1 \le i \le \frac{n-1}{2} \}$

הוכחה: $(n-i)^2 \equiv i^2 \pmod n$

נניח בשלילה שלא: $i^2 \equiv j^2 \pmod n$

אז $i^2 - j^2 \equiv 0 \pmod n$

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

$1 \le i, j \le \frac{n-1}{2} \Rightarrow i+j \neq 0 \pmod n \Rightarrow n \mid i-j \Rightarrow i \equiv j \pmod n$ סתירה.

סימן לז'נדר

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & n \mid a \\ 1 & a \text{ שארית ריבועית} \\ -1 & a \text{ לא שארית ריבועית} \end{cases}$$

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 $a \equiv b \pmod n$ אז $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

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 קובע שאם n, m אי-זוגיים זרים אז:

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

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

1) הפולינומים $g_Q = \prod_{a \in Q} (x - \zeta_a)$; $g_N = \prod_{q \in N} (x - \zeta_q)$ שייכים ל-$\mathbb{F}_q[x]$

2) $N_b \in \mathbb{F}_q[x]$: $N_b g_Q b (1-x) = 1 - v_x$

יהי v מס' כאשר x לוקי ו-b שו"מ מודולו v. אזי

$$\dim C_Q = n - \frac{2}{1-v} = \frac{2}{1+v} \quad ; \quad C_Q(v,b) = (g_Q)$$

$$\dim C'_Q = \frac{2}{1-v} \quad ; \quad C'_Q(v,b) = (g_Q(1-x)) \quad \text{(קוד } QR\text{)}$$

$$\dim C_N = \frac{2}{1+v} \quad ; \quad C_N(v,b) = (N_b)$$

$$\dim \hat{C}_N = \frac{2}{1-v} \quad ; \quad \hat{C}_N(v,b) = (N_b(1-x))$$

נרצה

הבסיס של $C_Q(z^4)$ שקול לקוד המתקן.

נשפט

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

הבסיס

אומרים שקוד לינארי C הוא קוד שבו כל שלה שני מילים

מרחק קוד.

אשפט

אי. $(\text{mod } p)$ $v \equiv \pm 1$, אזי $C_Q(v,b)$; $C_N(v,b)$ הם קו"מ.

הוכחה

נניח תחילה $\hat{C}_Q$. מתקיים $(x)c/(1-x)$, לכן $c(1) = 0$

$$\Leftarrow c_0 + c_1 + \cdots \pm c_{n-1} = 0$$

נניח ש-b ש"מ מודולו v. אזי:

יהי v מתקיים $v \equiv \pm 1$, כלומר $\frac{1}{2}$ שורש יחיד מריאציה מתקיים

תרגיל 5

1) $d(C_Q(n,2))$ ראינו בכיתה.

2) $d(C_Q(n,q)) = d(C_Q(n,q)) + 1$

תרגיל 6

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 $N \in \mathbb{N}$ כך ש- $g = g_Q$ ו- $\tilde{g} = g_N$

נקבע $a \in \mathbb{Z}_n$, נסמן $\lambda = \alpha^a$.

אם $j \in Q$, אזי $a \in N$.

אם $j \in N$, אזי $a \in Q$.

נקח $c(x) \in C$ מינימלי כך ש- $w(c) = d$, נסמן $p = w(c)$.

$$c(x) = a(x)b(x)$$

לכן $c(x) = c(x^s) \pmod{(x^n - 1)}$

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

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

נסמן ב- ζ את הפרימיטיבי מסדר $q^k - 1$ ב- $\mathbb{F}_q$.

אם $j \in Q$ אזי $\exists k \in N$ כך ש- $g(\zeta^{jk}) = 0$

אם $j \in N$ אזי $\forall k \in Q$ מתקיים $g(\zeta^{jk}) = c \neq 0$

לכן $\tilde{g}(x) = g(x^s)$

לכן $\tilde{c}(x)$ $(\pmod{x^n - 1})$ מתאפס ב- ζ ו- $\tilde{g} \Rightarrow$ מתאפס ב- g.

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

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

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

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

2 טענה $n \equiv 3 \pmod 4$

נקח $\zeta = -1$, ונקבל ש"כ n אי-זוגי.

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

לכן $1+p-d^2 \geq n$

$1+d(d-1) \geq \omega$

בכיתה: $c \neq 0$, $c \in C_Q(n,2)$, $p = w(c)$

נסמן $c_0, c_1, \dots, c_{n-1}$ כמילים שאינן אפס.

הרעיון הוא לספור בי"ד כמה:

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

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

יש בדיוק d זוגות סדורים מהצורה (u,u), (v,v)

אך יש בדיוגונלים גם $(u,v), (v,u)$

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

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

יש d^2 בסך הכל;

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

$$n = 1+d^2-p$$

p הוא ריבוע $\pmod 4$ $d \equiv 1,3 \pmod 4$

נניח $d \equiv 1 \pmod 4$, אז $n \equiv 1 \pmod 4$

מסתירה, לכן $d \equiv 3 \pmod 4$ מקבלים

⑧ (22/5/13)

קודים QR

הגדרה $\mathbb{F}_q$ שדה סופי, n טבעי, $b(1-x)\in\mathbb{F}_q[x]$ פולינום מתוקן מדרגה n שאינו מתחלק ב-x.

$\mathbb{F}_q$ פולינום הדוגמא ל-b שאינו $(x-\xi_i)$ $\prod_{i=1}^{n}$ מדרגה n $=N_b$

$\mathbb{F}_q$ פולינום מדרגה n שאינו מתחלק ב-$(x-\xi_i)$ $\prod_{i=1}^{n}$ $=N_b$

יהי $u\neq v$ וכתוב: b שאינו מתחלק ב-u, v

$\langle N_b(1-x)\rangle = (b,u)_q^1 c_N$; $\langle N_b\rangle = (b,u)_N c_N$

$\langle B_b(1-x)\rangle = (b,v)_q^1 c_q$; $\langle B_b\rangle = (b,v)_q c_q$

משפט יהי $n\mid q-1$, $\gcd(n,p)=1$, $b\in\mathbb{F}_q$ שאינו שורש של x^n-1, $\deg b\leq n-1$.

1) $\deg g_b \leq n-\deg b$

2) אם $\deg b \leq n-1-2t$ אז $g_b \mid x^n-1$

3) אם $n\equiv -1 \pmod q$ אז $n=2^m-1$ עבור $m\in\mathbb{N}$

דוגמאות של קודים (Hamming)

$n=2^m-1$, $q=2$, $\deg b=m$ אז $g_b \mid x^n-1$ $\Leftrightarrow$ b פולינום פרימיטיבי מדרגה m

$\deg g_b \leq n-m$

$d\geq 3$ אז $t=1$ אז $n-m=2^m-1-m$

$[n,k,d]_2$ הוא הקוד הדואלי של $[n,n-m,3]_2$ (משום ש $\overline{G_{23}}$, מוגדרת ע"י הוספת שורת אחדות ל-G_{23} מתחת ל-G_{23})

$G_{23}=c_Q(23,2)$

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

n	k	
7	4	$G_{11}=[11,9,6]_3$
15	11	$G_{24}=[24,12,8]_2$
23	12	$G_{23}=[23,12,7]_2$

הקודים

n הגדול ביותר כך ש $2^n-1\equiv -1 \pmod 3$ הוא $n=11$ ולכן 2 ו"ר

$\mathbb{F}_{2^{11}}$ מוגדר ע"י $\{0,1,2,3,4,5,6,7,8,9,10\}=\mathbb{F}_{2^{11}}$

$\deg b_0 \leq 5$

$n=\frac{2^{11}-1}{23}=89$ ולפי BCH נוצר $(\deg b_0 \geq n-11)$

$\deg b_0 \leq 1+p-2p$ ניתן לתקן $t=p$ שגיאות ע"י קוד מעל $\mathbb{F}_p$ ואורכו הוא $p-1$.

אפשר לכתוב β כשורש של הפולינום הזה מעל $\mathbb{F}_3$: x^5+x^2+x+1

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

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

כלומר β שורש של פולינום ממעלה 5 (מעל $\mathbb{F}_3$).
המתקיים $\beta^{11}=1$.

נקח γ כך ש- $\gamma^{242}=1$ כי $\mathbb{F}_{243}^\times$, כיוון ש- $243=3^5$

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

לכן β הוא $(1-d)$.

(מקדימים תחילה $a_0=1$). $a_d \neq 1 \pmod d$ ואז מוסיפים עוד

אפשר למשל $m=5$ ואז ω יהיה $\omega^{11}=1$ (אך ω^{11} לא 1 מודולו m)

$$\omega^3 = 1 \pmod{11}$$

$$\Rightarrow (1-x)m_{\beta^{-1}}(x)m_\beta(x) = 1-x^{22}$$

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

כלומר $\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{32}, \beta^{64}, \beta^{128}, \beta^{256}, \beta^{512}, \beta^{1024}\}$ אותיות 11

נתון $\beta = g^{89}$ כאשר $g^{23}=1$

$$\gamma^{2047}=1 \text{ ולכן } \gamma^k \neq 1 \text{ לכל } 1 \leq k < 2047$$

נשאלת השאלה האם קיים איבר γ ב- $\mathbb{F}_{2^{11}}$ כך ש-

$$\gamma^{2047}=1 \text{ אבל } \gamma^k \neq 1 \text{ לכל } 1 \leq k < 2047$$

$2047 = 23\cdot 89$; $2^{11}=2048$ נסמן $\omega = 2$

$$2^{11} \equiv 1 \pmod{23}$$

איבר g_{23} נמצא, נסמן w כאיבר

תרגילים בקוד אלו

נתבונן עם $p=5$ מעל השדה $\mathbb{F}_3$ ונמצא H, G.

שלושת $2^2, 2^3$ על כשמסתכלים בו עלולים לא לעבוד.

$$Q = \{\underbrace{2, 5, 4, 3, 1}_{k \geq 4}, 1\}$$

מצוי $\mathbb{Z}_{11}$;

$n=4$ כלומר.

ב- $\mathbb{F}_{11}$ מתקיים $2^5 = 10 = -1$ (כי אלו השלמים הקלים)

סיכום הרצאה

יהי $F=\mathbb{F}_q$, כאשר $q=p^k$, p ראשוני. $|F|=q$, $\log_p|F|=k$.

השאלה היא האם קיים n עבורו $[n,k,d]_q$ הוא מהיר.

נסמן $A_q(n,d)=\max\{|C|: C\subseteq F^n, d_H(C)=d\}$

נקבע n ונרצה לחסום את $|C|$ עבור $A_q(n,d)$

הגדרה: יהי F^n מ"ו. $x\in F^n$ נסמן $B(x,r)=\{y\in F^n \mid d(x,y)\le r\}$ כדור סביב x ורדיוס r.

למה: יהי F^n מ"ו. $x_1\neq x_2$, אז $B(x_1,e)\cap B(x_2,e)=\emptyset$ אמ"מ $d(x_1,x_2)\ge 2e+1$.

הוכחה: נניח $B(x_1,e)\cap B(x_2,e)\neq\emptyset$, אז $\exists y\in B(x_1,e)\cap B(x_2,e)$.

$d(x_1,x_2)\le d(x_1,y)+d(y,x_2)\le e+e=2e$

למה: יהי F^n מ"ו. $|B(x,e)|=\sum_{i=0}^{e}\binom{n}{i}(q-1)^i$

הוכחה: נסמן $Z_i=\{y\in F^n \mid d(x,y)=i\}$, נסמן $x=(x_1,\dots,x_n)$, $y=(y_1,\dots,y_n)$.

$|Z_i|=\binom{n}{i}(q-1)^i$

$\binom{n}{i}$ בחירת i מקומות שונים / $(q-1)^i$ בחירת i אותיות שונות מאותיות x

מסקנה: $|B(x,e)|=\sum_{i=0}^{e}|Z_i|$

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

מסקנה חלשה: $A_q(n,d)\ge q^k\cdot\left[\sum_{i=0}^{\frac{d-1}{2}}\binom{n}{i}(q-1)^i\right]^{-1}$ כאשר $e=\frac{d-1}{2}$

ומכאן, נניח בשלילה $|C|=3$. לפי $[4,3]$ אם $A(4,3)=2$ נקבע קוד לא טריוויאלי $C\subseteq\{0,1\}^4$ כך ש$C\subseteq C(4,3)$.

$C\subseteq C(4,3)$ ו$|C|=3$. אבל C לא יכול להכיל שני איברים שונים x,y כך ש$d(x,y)\geq 3$.

טענה: אם $n=p$ כך שקיים קוד לינארי C עם $d=3$ ו$|C|=2^{n-p}$ אזי $A(n,3)=2^{n-p}$.

הוכחה: נראה שקיים קוד לינארי C עם $d=3$ ו$|C|=2^{n-p}$ ולכן $A(n,3)\geq 2^{n-p}$. נשים לב שלכל $d<p$ אי"ש לא מתקיים, אבל $d=p$ לא שולל כי p בהכרח להיות אי זוגי (למשל $p=2$).

לכן C_{23} מושלם.

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

מתקיים $n=p=23$ ו$|C|=2^{23-11}=2048$:

$$\sum_{i=0}^{3}\binom{23}{i}=1+23+\frac{23\cdot 22}{2}+\frac{23\cdot 22\cdot 21}{6}=2048$$

הוכחה: נראה ש$C_{23}=[23,12,7]_2$ קוד לינארי.

מתקיים $n=p=23$ ו$|C|=2^{23-11}=2048$:

$$\sum_{i=0}^{3}\binom{23}{i}=1+23+\frac{23\cdot 22}{2}+\frac{23\cdot 22\cdot 21}{6}=2048$$

לכן C_{23} מושלם.

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

מסקנה – חסם המינג

אם C הוא קוד לינארי שמתקן e שגיאות אזי

$$R=\frac{k}{n}\geq 1-\frac{\log_2(\sum_{i=0}^{e}\binom{n}{i}(q-1)^i)}{n}$$

$X=(x_1,\dots,x_4)$; $Y=(y_1,\dots,y_4)$; $Z=(z_1,\dots,z_4)$

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

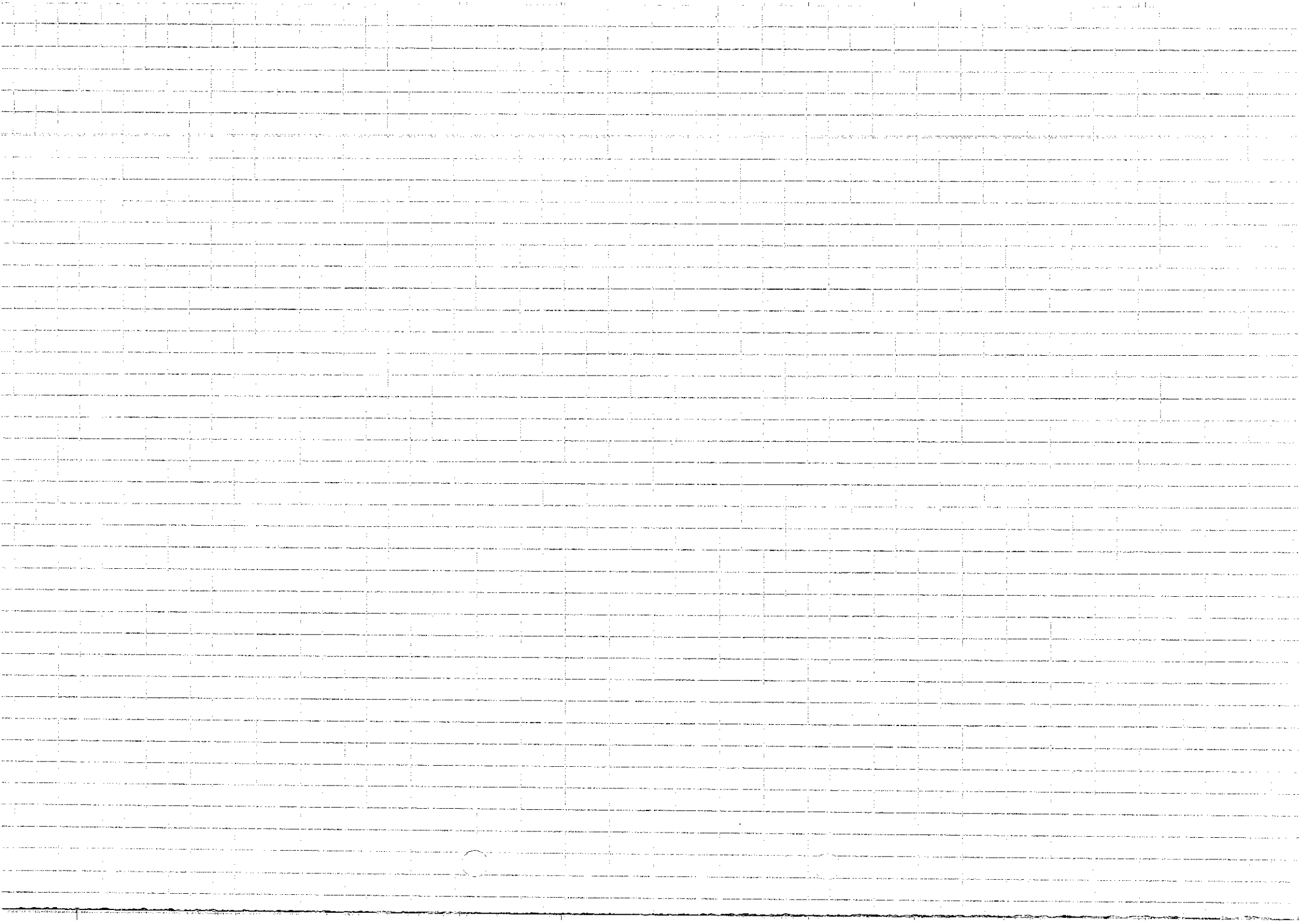
$A=\{i \mid x_i \neq y_i\}$ $B=\{j \mid x_j \neq z_j\}$ לכן

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

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

$A\cap B=\{k \mid y_k = z_k\}$ לכן $|A\cap B|\geq 2$ וזה סתירה כי $d(y,z)\geq 3$!

משל מוטעם הקבוצה



(4) (29/5/13)

תרגול 5 – קודים לינאריים

חסם הילברט

משפט

אם $C \subseteq [q]^n$, $|C| = M$, $d = d_q[n,k]$ אזי $\frac{q^k(q-1)}{(q^k-1)q} \cdot n \geq d$

הוכחה:

נסמן $|F| = q$, $C \subseteq F^n$, $|C| = M = q^k$. אנחנו יודעים ש

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

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

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

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

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

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

נרצה להראות שזה קטן שווה למשהו:

נגדיר Λ מרחב $(\cdot,\cdot)$ ואת $\|\cdot\|$ הנורמה המושרית, אז

$$|\langle h, x \rangle| \leq \|h\| \cdot \|x\|$$

את נקח $h = (1,\dots,1)$ נקבל: $(x_1 + \dots + x_q)^2 \leq q(x_1^2 + \dots + x_q^2)$

$$\frac{1}{q}(x_1 + \dots + x_q)^2 \leq x_1^2 + \dots + x_q^2$$

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

$$\Rightarrow d \leq \frac{\frac{q-1}{q} n M^2}{M(M-1)} = \frac{(q-1)nM}{q(M-1)} = \frac{(q-1)q^k n}{q(q^k-1)}$$

* נשאר לבדוק: מסה של הקודים נותן $\frac{q(1-\mu_q)}{(1-\mu_q)\mu_q n} \geq \rho$

מסה של $\rho \leq 1 - \mu_q$ נותן $\frac{\mu_q}{\rho} = R$ כאשר $\rho = \delta$

נשתמש באותה השיטה כדי לחשב את x_1. אבל הפעם נקבל שתי משוואות שונות: $x_4+x_5+x_6+x_7=1$, ו- $x_1+x_2+x_3+x_7=1$. לכן, נוסיף משוואה שלישית, שתהיה בלתי תלויה לינארית בשתי הראשונות. נבחר למשל $x_5=0$. נקבל את המערכת הבאה:

$$\begin{cases} x_4+x_5+x_6+x_7=1 \\ x_1+x_2+x_3+x_7=1 \\ x_5=0 \end{cases}$$

אפשר לבדוק, למשל בעזרת דירוג, שהמטריצה המתאימה למערכת זו הפיכה. לכן, קיים פתרון יחיד למערכת. אבל, אין שום משוואה שנוכל להוסיף כדי לקבל את x_1 בלבד. אם נוסיף משוואה שבה $x_1=1$, נקבל סתירה. אם נוסיף משוואה שבה $x_1=0$, נקבל סתירה. אם נוסיף משוואה שבה x_1 לא מופיע, נקבל סתירה. אם נוסיף משוואה שבה x_1

בדוגמה אפשר: $x_1+x_2=c_3$, $x_3+x_4=c_3$, $x_4+x_5=c_3$

$\Leftarrow$ $x_3+x_4=c_3$

משמעות 3 היא 1 וסיבות שני האיברים הראשונים בשורות 2-ם הוא 0

$$(\{0,1\}\ni i)\quad \sum_{i=0}^{n} i\cdot b_i = \chi$$

לכן $\exists c(x_1,\dots,x_n)=\chi$ כאשר:

המקיים $0=+H=\frac{1}{2}GH \Rightarrow c$ אזי נקבל.

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

מטריצת בדיקת זוגיות

לפיכך c הוא בעל מרחק $[A,V,8]=c$

שים $\exists c$ כי $\mathbb{F}_2$ המילות של c (להסבר).

אומרים שהקוד $\exists c$ בגודל לכל היותר c אם הוא $\mathbb{F}_2$-תת

אפשר במקרה כזה לתקן $\frac{c}{2}$ שגיאות.

$\{x_n\sum_{i=0}^{n} b_i,\dots,x_n\sum_{i=0}^{n} b_i\}$ כלומר, אין אפשרות לדעת מה היה x שלי היה

מקס, סמס את (מלבד הסבר)

$\exists$ שבעצם ימין של $\mathbb{F}_2$ משוואה כל סעיף שונה $n-i$ מיפוי

$$x_n \sum_{i=0}^{n} b_i = \chi$$

$$\vdots$$

$$x_{n-1}\sum_{i=0}^{n} b_i = \chi$$

אם לכל x קיימת אלגוריתם משוואות מהצורה הבאה

באופן כללי, אפשר להשתמש באלגוריתם שלנו כדי כדי קבוצת

ועבור על כולן שם a_3 מקבלת הפעולה בין
$\{x_7+x_6, x_5+x_4, x_3+x_2, x_1+x_0\}$

לעומת a_2 נקבל תמונה אחרת שתביא להתנגשות ל-
$\{x_7+x_5, x_6+x_4, x_3+x_1, x_2+x_0\}$

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

לעומת a_0 נקבל הסימטריה שכן:
$a_0 \overline{x} = \overline{x}'$ בהתאם ל-

אם אין שוויונות אל $\overline{x}'$ הוא $(1,\dots,1)$ או $(0,\dots,0)$
ולכן מגדירים על קלט שם a_0 לפי כמה קלות ב-x.

דוגמה

נניח שקיבלנו עבור $(0,1,1,1,0,1,1,0)$
נקבע $a_3=1$, $a_2=1$, $a_1=0$, $a_0=0$

$x_0 = \overline{x_7+x_3} = \overline{(0,1,1,0,0,1,1,0)}$

שלמות לפי רמת קלות

שאלה קוד פואל, למעלה עם $G: m \times (2^m - 1 - m)$ מאפיינים על

בקוד המוכלה עם: מס' מילים 2^m ← $m \times (1+m)$ גודל: מספר ראשון

$p = 4$ $1+m = 4$ $n = 2^m$ ← בעל קוד שלם

ולמעשה מטרתם ל תיקון של שגיאה אחת ולגלות של 2 שגיאות

פה למשל- $m = 4$ המטרי $G: 4 \times 15$ הוא:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{matrix}$$

שורה מיותרת

מיקום שגיאה

וכן מילה מהקוד אינה אלא $\sum_{i=0}^{4} b_i a_i = x$ כלשהי.

מסקנות על קוד מאופיינים כמו הטענות

(שלמות אי אינדקסים 1 ו0 בלבד וכו...)

מכאן נקבע, לכאורה a_4, מהתפלגות על שתי הקואורדינטות הראשונות

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

(מהנקבע מסכימות אלגברי לאחדות $i+j$ בכל זאת מן השורות לגבי a_i ו a_j בהתאמה).

אם אין שגיאות נקבע שכל הקודים כאלה.

אם יש שגיאה אחת נקבע שאחד שונה מהשאר.

אם יש 2,3 שגיאות נקבע ש-2,3 שונים מהשלו (בהתאמה)

אם יש 4 שגיאות יש מקרה, אי אפשר לתקן.

כך מתקנים שגיאות ומתקנים אחת שגיאות,

באופן אופן, קלות האחרים:

$$a_3=\{x_0+x_2, x_1+x_3, x_4+x_6, x_5+x_7, x_8+x_{10}, x_9+x_{11}, x_{12}+x_{14}, x_{13}+x_{15}\}$$
$$a_2=\{x_0+x_4, x_1+x_5, x_2+x_6, x_3+x_7, x_8+x_{12}, \dots\}$$
$$a_1=\{x_0+x_8, x_1+x_9, \dots\}$$

נאלץ מס"מ לפי הסימה הראשון.
לסימה השני נגדיר

$$\overline{x}'=\overline{x}-a_1\overline{g_1}-\dots-a_4\overline{g_4}=$$
$$=a_0\overline{g_0}=\begin{cases}(0\dots0)\\(1\dots1)\end{cases}\overset{\text{אם כן}}{\Leftarrow}$$

אם כפלנו ב a_0 לפי הוא הקלות בקה אחרי x.
על ידנו של a_0 לפי הוא הקלות בקה אחרי x.
כאן קיבלנו שאנקים ב שיאות ואנלוים ל ולכן $g=p$.

⊛ סמלנלה קוד RM מסדר אחד (כאן תיל) אורך 2^m שיאות ואנלה 2^{m} שיאת $1+m+\binom{m}{2}$.

טענה: הפרמטרים של הקוד הם $[2^m, 1+m+\binom{m}{2}]$.

קוד RM מסדר אחרון

נגדיר עבו מילים הינאריות כך:
הכינוס $\overline{x}=(x_1,\dots,x_n)$ + $(y_1,\dots,y_n)=\overline{y}$ אנו:
$\overline{y}\circ\overline{x}=(x_1,y_1,\dots,x_n,y_n)$

יהי $k<r$, נגדיר קוד RM מסדר r ע"י:
נתונים מקוד RM מסדר r עם פרמטרים m ל

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

$x_i=0 \Rightarrow$ סיבה ראשונה, $x_i=1 \Rightarrow$ סיבה שנייה, סיבה שלישית,
נסכם השלכה מרשת סיבתית, לפי $i+j=3$ סיבות:

$$\overline{q_{34}}a_{34}+\dots+\overline{q_{12}}a_{12}+\overline{q_4}a_4+\dots+\overline{q_0}a_0=\overline{X}$$

לפניך השלכות, בצבע ג $\overline{\exists x}$ באופן הבא:

ניתוח זה מעלה כי השורות
מקבלים קוד $\in C[4,11,3]$

q_{34}	1	0	0	1	0	0	0	1	0	0	0	1	0	0	0
q_{24}	1	0	1	0	0	0	0	1	0	1	0	0	0	0	0
q_{23}	1	1	0	0	0	0	0	1	1	0	0	0	0	0	0
q_{14}	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0
q_{13}	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0
q_{12}	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
q_4	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
q_3	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
q_2	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0
q_1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
q_0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

$=G$

מתוספות כי לא ייתכן שום דבר חפש.
מתוספות לכל היותר $\binom{4}{2}=6$ שורות לפי לא מתכוונים
לחיצה- $RM(2,4)$

* נשים לב: ניתן באופן כללי: $RM(m,r)$

נשאיר כמים ונמן כאשר תיקון השגיאות יורד.
נקוד כי נקבל אשתמר (כי יש d_{min}) שזו הסתברות
ג המתקבלת יוצרת את קוד RM מספר r.
ג תתקבל מתוך G ע"י מחיקת השורות הנותרות.
נסמן את G המטריצה של C שהיא ע"י ונוסיף אותן $r-g$.

אז יש q^{w-1} מקרים כך שיתקיים
מקרים. $\geq q^{w-1}$ (עם כפל בסקלר של קוד)
נניח שיש קוד C שאינו מהאפסקלארי d.
כלומר, $\{v_1,\dots,v_k\}=B$ בסיס של C שמכיל F.
$\dim_{\mathbb{F}_q} C = w+1$
C הוא מ"ו מעל $\mathbb{F}_q$, ומתקיים
$\{f : U \to \mathbb{F}_q \mid f(x_1,\dots,x_{w-1})=0\} = C$
לפיכך $|\mathbb{F}_q| = q$, $C \subseteq U$ ומתקיים:

קומבינטוריקה אלגברית

קיבלנו מתקן $w-1-k$ שיש q^{w-1-k} שיאות.
אם מקיימות בסיבוכיות כל שהן $k-w$
אם סטודנטים $= 1+k$

$$\binom{w}{0}+\dots+\binom{k}{w}+w+1-k = \sum_{m=0}^{w} \binom{m}{w}$$

* באופן כללי, עבור $RM(m,w)$, יתקיים:
שפע גדול מספיק.
שניתן, בסיבוכיות הגבוה כמו כן לא תמיד אפשרות
משום ש- $p=2$ ואפשר לתקן כך שיאפס את הלמידה
ואפשר להשתמש באותה מילה בקידוד RM מסדר m,
אם אין שיאות אז $\overline{b_1 v_1 + \dots + b_k v_k} = \overline{x}$
$(b_1 x_1, \dots, b_k x_k) = \overline{b_1 v_1} - \dots - \overline{b_k v_k} - \overline{x} = |x|$
לדוגמה הסימון הבא:
באותו אופן לדוגמה במשך הסימנים הראשון.
$\Leftarrow$ אפשר לתקן שיאה את הלמידה 2.
$\{x_1+x_4+x_7+x_{11}, x_1+x_5+x_8+x_{12}, x_2+x_4+x_9+x_{13}, x_3+x_4+x_5+x_{14}, x_6+x_7+x_8+x_9\} = a_{34}$
מתשמה $\overline{b_{34}}$ נתבוון לפי 4 סמלים ונקבל

הוכיחו שהעתקה

$$\varphi(f)=(f(\gamma_1),\dots,f(\gamma_{q^w-1})) \quad \varphi: T'_w \to \mathbb{F}_{q^b}^{q^w-1}$$

היא חח"ע. (הבהרה: $\mathbb{F}_{q^b}^{q^w-1}$ מסמן את $\mathbb{F}_{q^b}$ בחזקת q^w-1.)

פתרון:

$$\dim_{\mathbb{F}_q} T'_w = w+1 \Rightarrow \dim_{\mathbb{F}_q} C \le w+1 = k$$

$$d \ge n-q^b-q^w+2$$

נקבע $b=w$ ונקבל $d \ge q^w-q^w-q^w+2 = q^w-2q^w+2$

אם $q \ge 3$ אזי $d \ge 1$ ולכן C הוא קוד מעל.

אם $q=2$ אזי $d \ge 0$ ולכן $C=[2^w-1, w+1, 0]$ אינו קוד מעל.

שדה המורחבות של קודים מעגליים כלליים

יהי T קוד מעגלי מעל $\mathbb{F}_q$ ויהי $g(x)$ פולינום היוצר של T. נסמן $T'_w = \{f \in \mathbb{F}_{q^w}[x] \mid f(x)g(x) \in T\}$

T'_w הוא קוד לינארי, $\dim_{\mathbb{F}_{q^w}} T'_w = w+1$

נסמן ב $\gamma_1,\dots,\gamma_{q^w-1}$ את כל איברי $\mathbb{F}_{q^w}$ שאינם שורשים של g.

אם d הוא המרחק של T אז המרחק של T'_w הוא לפחות d.

נגדיר $\varphi: T'_w \to \mathbb{F}_{q^b}^{q^w-1}$ ע"י

$$\varphi(f)=(f(\gamma_1),\dots,f(\gamma_{q^w-1}))$$

φ היא חח"ע אם $\ker\varphi=0$ (כלומר $\dim_{\mathbb{F}_{q^b}} \operatorname{Im}(\varphi)=C$.

$$\dim C \le \dim T'_w = w+1 = k$$

נסמן: d המרחק של C.

אם $b \ge 2$ אזי $C=[q^w-1, w+1, \ge q^w-q^b]$ ונקבל $d \ge q^w-q^b$.

אם $b=w$ אזי $C=[2^w-1, w+1, \ge 2^{w-1}] \Rightarrow$ קוד לינארי.

אם $q \ge 3$ אזי $d \ge 1$ ולכן $C=[q^w-1, w+1, \ge 1]$ אינו קוד מעגלי.

אם $q=2$ אזי $d \ge 0$ ולכן $C=[2^w-1, w+1, 0]$ אינו קוד מעגלי.

שדה המורחבות של קודים מעגליים כלליים

יהי T קוד מעגלי מעל $\mathbb{F}_q$ ויהי $g(x)$ פולינום היוצר של T. נסמן $T'_w = \{f \in \mathbb{F}_{q^w}[x] \mid f(x)g(x) \in T\}$

T'_w הוא קוד לינארי, $\dim_{\mathbb{F}_{q^w}} T'_w = w+1$

נסמן ב $\gamma_1,\dots,\gamma_{q^w-1}$ את כל איברי $\mathbb{F}_{q^w}$ שאינם שורשים של g.

אם d הוא המרחק של T אז המרחק של T'_w הוא לפחות d.

נגדיר $\varphi: T'_w \to \mathbb{F}_{q^b}^{q^w-1}$ ע"י

$$\varphi(f)=(f(\gamma_1),\dots,f(\gamma_{q^w-1}))$$

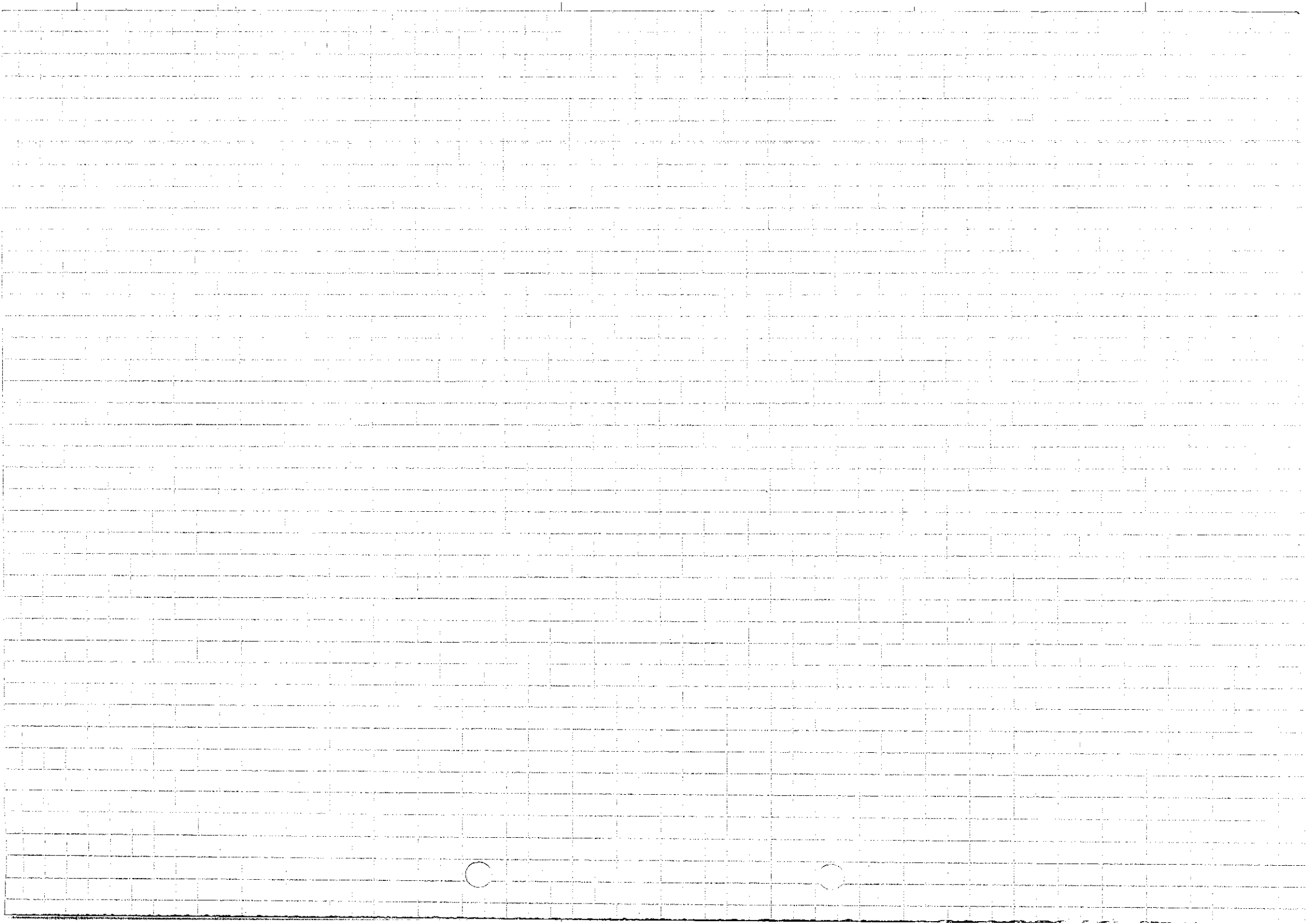
φ היא חח"ע אם $\ker\varphi=0$ (כלומר $\dim_{\mathbb{F}_{q^b}} \operatorname{Im}(\varphi)=C$.

$$\dim C \le \dim T'_w = w+1 = k$$

נסמן: d המרחק של C.

אם $b \ge 2$ אזי $C=[q^w-1, w+1, \ge q^w-q^b]$ ונקבל $d \ge q^w-q^b$.

אם $b=w$ אזי $C=[2^w-1, w+1, \ge 2^{w-1}] \Rightarrow$ קוד לינארי.

אם $q \ge 3$ אזי $d \ge 1$ ולכן $C=[q^w-1, w+1, \ge 1]$ אינו קוד מעגלי.

אם $q=2$ אזי $d \ge 0$ ולכן $C=[2^w-1, w+1, 0]$ אינו קוד מעגלי.