קוד מתקן שגיאות

הגדרה: קוד $[n,k]_2$ הוא $C \subseteq \mathbb{F}_2^n$ תת מרחב ממימד k.

הגדרה: קוד קוונטי $[n,k]_2$ הוא $\mathcal{C} \subseteq \mathcal{H}_{2^n}$ כך ש $\mathcal{C}$ תת מרחב ממימד 2^k.

דוגמה 1: $[3,1]_2$ קוד קוונטי.

$$\mathcal{C}_1 = span\{|000\rangle, |111\rangle\}$$

דוגמה 2: Shor code, $[9,1]_2$

$$|0_L\rangle = \left(\frac{1}{\sqrt{2}}\right)^3 (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1_L\rangle = \left(\frac{1}{\sqrt{2}}\right)^3 (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

$$\mathcal{C}_2 = span\{|0_L\rangle, |1_L\rangle\}$$

דוגמה 3: Steane's code $[7,1]_2$

$$|0_L\rangle = \frac{1}{\sqrt{8}}\Big[|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\Big]$$

$$|1_L\rangle = \frac{1}{\sqrt{8}}\Big[|1\ldots1\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + \ldots\Big]$$

$$= |1\ldots1\rangle \oplus |0_L\rangle$$

כל איבר ב $|0_L\rangle$ עושה xor עם $|1\ldots1\rangle$.

$$\mathcal{C}_3 = span\{|0_L\rangle, |1_L\rangle\}$$

~~הגדרה: נאמר שקוד קוונטי $[n,k]_2$, $\mathcal{C} \subseteq H_{2^n}$~~

~~מתקן שגיאות $\mathcal{E}$~~

~~אם יש פרוצדורת תיקון שגיאות R~~

~~כך שלכל ρ דמ על H_{2^n}~~

~~ולכל שגיאה $E \in \mathcal{E}$~~

~~$R(E($~~

הגדרה: יהי $\mathcal{C} \subseteq H_{2^n}$ קוד קוונטי $[n,k]_2$

נאמר ש- ρ דמ על $\mathcal{C}$

אם $\Pi_{\mathcal{C}} \rho \Pi_{\mathcal{C}} = \rho$,

כש- $\Pi_{\mathcal{C}}$ הטלה על $\mathcal{C}$.

הגדרה: נאמר שקוד קוונטי $\mathcal{C} \subseteq H_{2^n}$

מתקן שגיאות $\mathcal{E}$

אם יש פרוצדורת תיקון שגיאות R

כך שלכל ρ דמ על $\mathcal{C}$

ולכל $E \in \mathcal{E}$

$$R(E(\rho)) = \rho$$

בסקרנצה Q הגדה

נניח שאופרטורי השגיאה המותרים $\mathcal{E}$
נפרשים ע"י $E_1, \dots, E_T$

נניח הקוד Q נפרש ע"י $\psi_1, \dots, \psi_k$

ונניח R מקיימת

$$R\left(E_i(\psi_j)\right) = |\psi_j\rangle \otimes |i\rangle$$

סינדרום השגיאה

אז

$$R\left(\sum \alpha_i E_i \left(\sum \beta_j \psi_j\right)\right)$$

$$= \sum \alpha_i R\left(E_i \left(\sum \beta_j \psi_j\right)\right)$$

$$= \sum \alpha_i \beta_j \quad R(E_i(\psi_j)) = \sum \alpha_i \beta_j \quad |\psi_j, i\rangle$$

$$= \sum \beta_j |\psi_j\rangle \otimes \sum \alpha_i |i\rangle$$

ולכן אנו מוצאים ש Q מתקנת $\mathcal{E}$.

דוגמא 1! $\mathcal{C}_1$ מתקן $\mathcal{E}_1 = span\{H_1, H_2, H_3\}$

H_i [illegible] 4.7.ג [illegible]

בעצם $\mathcal{C}_1 = span\{|000\rangle, |111\rangle\}$

$R_{\#}(E_i(\Psi_j)) = |m,m,m\rangle \otimes |i\rangle$

$m = maj\{b_1, b_2, b_3\}$ [illegible]

[illegible] $\times$ Z [illegible]

$R(\|000\rangle)$	$=\|000\rangle$	$\otimes\|0\rangle$
$R(\|001\rangle)$	$=\|000\rangle$	$\otimes 3$
010	000	2
100	000	1
110	111	3
101	111	2
011	111	1
111	111	0

שגיאות ב $\mathcal{E}_i$

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ X - bit flip

$\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ Z - phase flip

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ XZ - bit & phase flip

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ I - none

נעבוד עם $\mathcal{H}_{2^n}$

שגיאה כללית $E = E_1 \otimes \dots \otimes E_n$

כאשר $E_i \in \{X, Z, XZ, I\}$

ומשקלה t אם t i-ים $E_i \neq I$.

$\mathcal{E}$ זה כל שגיאה עם משקל לכל היותר t + צירופים

טענה: Shor's code מתקן $\mathcal{E}_1$.

אלגוריתם התיקון R:

שלב 1: יש לנו 3 קבוצות של אחד.
בכל קבוצה הפעל את אלגוריתם התיקון של bit-flip.

שלב 2: מדוד $|m_1,m_1,m_1\rangle \otimes |m_2,m_2,m_2\rangle \otimes |m_3,m_3,m_3\rangle$
ל $|m_1, m_2, m_3\rangle$

הפעל $H^{\otimes 3}$ שלושה
ואז הפעל תיקון של bit-flip שוב.

נראה מה קורה עם E שגיאה

כלומר $E = E_1 \otimes \dots \otimes E_q$ רק לכל היותר אחד מה E_i אינו I

ו $E_1 \in \{I, X, Z, XZ\}$

ועוד Ψ אינו $\Psi \in \{|0_L\rangle, |1_L\rangle\}$

השלב ה-1 מתקן ה bit-flip ובסיכום לא מזיקים לסינדרום הבאים.

לכן - נשאר רק phase flip (אם יש).

המצב הנכון $|0_L\rangle = (|+\rangle)^{\otimes 3} = |+\rangle \otimes |+\rangle \otimes |+\rangle$

ועם phase flip בביט $i=1$: $|-\rangle \otimes |+\rangle \otimes |+\rangle$

אחרי הפעלת $H^{\otimes 3}$ מקבלים $|1\rangle \otimes |0\rangle \otimes |0\rangle$

ואחרי התיקון (לשיטת הסינדרום) מקבלים $|0\rangle \otimes |0\rangle \otimes |0\rangle$

כנ"ל עבור 2, 3. $\square$

מעט על קודים קוונטים

מטריצה יוצרת

יהי $C \subseteq \mathbb{F}_2^n$ קוד לינארי ממימד k

אז יש $G: \mathbb{F}_2^k \to \mathbb{F}_2^n$ כך ש- $C = Im(G)$,

$$\begin{pmatrix} G \end{pmatrix}_{n \times k}$$

המטריצה G נקראת המטריצה היוצרת של הקוד.

parity check matrix

נגדיר $C^{\perp} = \{y \in \mathbb{F}_2^n \mid \forall c \in C \;\; c \cdot y = 0\}$

אז $C^{\perp} \subseteq \mathbb{F}_2^n$ הוא ממימד $n-k$

ולכן אפשר לתאר אותו ע״י parity check matrix

שהיא מטריצה

$$H_{(n-k)\times n}$$

כך ש $\forall c \in C: \; Hc = 0$

ובעצם מתקיים: $C = \{y \mid Hy = 0\}$

($\Rightarrow$ $C \subseteq \underbrace{\{y \mid Hy = 0\}}_{\text{הוא ממימד } k}$ ולכן שוויון.)

Syndrom decoding

הגדרה: המרחק של הקוד C הוא d

$$d = \min_{x_1 \neq x_2} d(C(x_1), C(x_2))$$

($C(x_1)$ – מילת קוד של x_1; $C(x_2)$ – מילת קוד של x_2)

מרחק מינימלי בין 2 מילות קוד.

אם $c \in C$, ו- $e \in \{0,1\}^n$ כך ש- $w(e) < d$

משקל מינימלי $= d(e, 0)$

אז $H(c+e) = H(c) + H(e)$ (כאשר $H(c) = 0$)

ו- $H(e)$ נקרא סינדרום השגיאה.

נניח כי קיימים $e_1 \neq e_2$, ו- $w(e_1), w(e_2) \le \frac{d-1}{2}$

אז אם e_1 ו- e_2 מייצרים אותה שגיאה

כ- $H(e_1) = H(e_2) \Rightarrow$

$$H(e_1+e_2) = H(e_1) + H(e_2) = 0$$

$w(e_1+e_2) < d$

אבל $e_1+e_2 \notin C$, סתירה.

דוגמא: $C_1 = [7, 4, \underset{\text{מרחק}}{3}]_2$ Hamming code

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$ זו p.c.m

מכאן $n=7$, $k=7-3=4$

לפי המרחק, אם קרתה שגיאה אחת $e = e_i = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$

$He_i = \begin{pmatrix} \vdots \end{pmatrix}$ (עמודה i), רק אז ניתן לתקן שגיאה אחת, רק אחת.

נקח $C_2 = C_1^\perp$

אז

$$C_2 = [7, 3, ?]_2$$

המטריצה היוצרת של $G_2 = H^t_{7\times3}$

p.c.m של

$$H_2 = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]_{4\times7}$$

$$= \left[\begin{array}{c|c} I & A \end{array}\right]$$

כי נתון ש- $H_2 G_2 = 0_{4\times3}$ (H_2 בגודל 4×7, G_2 בגודל 7×3)

שורה 1 של H = שורה מוספת של H_2

שורה 2 - שורה II+III של H_2

3 - I+III

רק $H_2 y = 0 \Leftarrow Hy = 0 \Leftarrow$ $\boxed{C_2 \subseteq C_1}$

ולכן, זהו הקוד שמוכל C_2 שהוא
קוד לשאלה הבאה מסתמכת על זה
ורק C_2 מכיל מינימאלי, מרחק ≥ 3

$$c_1^{\perp} = c_2 = [7, 3, 3]_2$$

Calderbank, Shor, Steane — CSS codes

נקח $C_2 \subseteq C_1 \subseteq \mathbb{F}_2^n$, $\dim C_1 = k_1$

כך ש C_1, $C_2^{\perp}$ מתקנים t שגיאות

(בתור קוד מרחק $2t+1$).

יש $\frac{|C_1|}{|C_2|}$ cosets של C_2 ב- C_1

לכל coset נגדיר מילת-קוד

לכל coset $y+C_2$ נגדיר:

$$|y+C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{c \in C_2} |y+c\rangle$$

(א) מגדיר ש-הקוד $= \mathrm{Span}\{\,|y+C_2\rangle \mid y \in C_1\}$

(ב) קוד קוו' $[n, k_1-k_2]_2$

כי ממד הקוד $\frac{|C_1|}{|C_2|} = \frac{2^{k_1}}{2^{k_2}} = 2^{k_1-k_2}$

⊖ תיקון כתוצאת מילה קוד ואחרי שגיאה

שגיאות כאלו $E_1 \otimes \cdots \otimes E_n$

$E_i \in \{X, Z, XZ, I\}$, מספר ה-i כך ש $E_i \neq I \le t$.

זה אומר תת-קבוצה עליה הפעלנו Z

ותת-קבוצה " " X

ולכן יש $e_1, e_2 \in \{0,1\}^n$ ש $w(e_1), w(e_2) \le t$

כך ש

$$\frac{1}{\sqrt{C_2}} \sum_{c \in C_2} | y + c \rangle$$

עובר [illegible]:

$$\frac{1}{\sqrt{C_2}} \sum_{c \in C_2} (-1)^{(y+c) \cdot e_2} | y + c + e_1 \rangle$$

אלגוריתם הפתרון:

① מפעילים את H_1 על $y+c$ לקבלת סופרפוזיציה רגע
ומודדים את הרגע e_1
ומקבלים.

המצב שלך כה $|y+c\rangle$ $\frac{1}{\sqrt{C_2}} \sum_{c\in C_2} (-1)^{(y+c)\cdot e_2}$

② מפעילים $H^{\otimes n}$ מקבלים

$$\frac{1}{\sqrt{N}} \frac{1}{\sqrt{C_2}} \sum_{c\in C_2} (-1)^{(y+c)\cdot e_2} \sum_{z} (-1)^{(y+c)\cdot z} |z\rangle$$

$$= \frac{1}{\sqrt{N}} \frac{1}{\sqrt{C_2}} \sum_{z} \underbrace{\left(\sum_{c\in C_2} (-1)^{(y+c)\cdot(e_2+z)} \right)}_{(-1)^{y(e_2+z)} \cdot \sum_{c\in C_2} (-1)^{c\cdot(e_2+z)}} |z\rangle$$

אם z כך $\forall_{c\in C_2}$ $c\cdot(e_2+z)=0$ מקבלים C_2
z " $\exists c\in C_2$: $c\cdot(e_2+z)\neq 0$

אז לכל $\alpha\in C_2$
$\alpha(e_2+z) \neq (\alpha+c)(e_2+z)$

אז $\frac{1}{2}$ שלהם 0, ו-$\frac{1}{2}$ שלהם 1
סכומם $\underline{\underline{0}}$

לכן נשארים רק אם z כך ש $c(e_2+z)=0$ $\forall c\in C_2$

$$e_2+z\in C_2^{\perp}$$
$$z\in C_2^{\perp}+e_2$$

כלומר:

$$n\sum_{z\in C_2^{\perp}+e_2}(-1)^{y(z+e_2)}|z\rangle$$

③ מפעילים הפוך על $C_2^{\perp}$
מסכמים על e_2
ומצמצמים

מקבלים

$$n\sum_{w\in C_2^{\perp}}(-1)^{y\cdot w}|w\rangle$$
$$w=z+e_2$$

④ מפעילים $H^{\otimes n}$
ומקבלים

$$\frac{1}{\sqrt{|C_2|}}\sum_{c\in C_2}|y+c\rangle$$

□