تکلیف سری سوم کدینگ

پریچهر دادخواه 9601295

سوال 12 کدهای خطی $C(n,k)$ و $C'(n,k)$ ⇐ بررسی کدهای $C\cap C'$ و $C+C'=\{u+u' \mid u\in C, u'\in C'\}$ و $C\cup C'$

1) کد $C\cap C'$ ⇐ اگر کدهای C و C' خطی باشند. پس هرکدام شامل کدورد صفر و نسبت به عملگر XOR بسته می‌باشند. پس کد $C\cap C'$ نیز شامل کدورد صفر هست.

$$\text{if}\begin{cases} h_1\in C\cap C' \Rightarrow h_1\in C,\ h_1\in C' & (1)\\ h_2\in C\cap C' \Rightarrow h_2\in C,\ h_2\in C' & (2)\end{cases}$$

$(1),(2)\quad h_1\in C,\ h_2\in C \Rightarrow$ بسته بودن نسبت XOR $\Rightarrow h_1+h_2=h_3\in C$

$(1),(2)\quad h_1\in C',\ h_2\in C' \Rightarrow$ " " C' " $\Rightarrow h_1+h_2=h_3\in C'$

$\Rightarrow h_1+h_2=h_3\in C\cap C'$

همچنین ثابت کردیم اگر h_1 و h_2 در $C\cap C'$ باشند آنگاه $h_3=h_1+h_2$ نیز عضو $C\cap C'$ است و به همین علت $C\cap C'$ نسبت به عملگر XOR بسته است. پس $C\cap C'$ یک کد خطی است.

2) کد $C+C'=\{u+u' \mid u\in C, u'\in C'\}$

با انتخاب u و u' هردو کدورد صفر از C و C' داریم که $u+u'$ نیز کدورد صفر است پس کد $C+C'$ شامل کدورد صفر هست.

$$\text{if}\begin{cases} h_1\in C+C' \Rightarrow h_1=u_1+u_1'\\ h_2\in C+C' \Rightarrow h_2=u_2+u_2'\end{cases} \Rightarrow h_3=h_1+h_2=\underbrace{(u_1+u_2)}_{u_3}^{*}+\underbrace{(u_1'+u_2')}_{u_3'}^{*}\in C+C'$$

(*) به علت بسته بودن کدهای C، C' نسبت به عملگر XOR، u_3 و u_3' به ترتیب عضو کدوردهای C و C' هستند و به همین علت $u_3+u_3'=h_3$ است یک کدورد معتبر از $C+C'$ است. پس با این حساب $C+C'$ نسبت به عملگر XOR بسته و کد $C+C'$ خطی است.

3) کد $C\cup C'$ ← این کد شامل کدورد صفر است اما برای بررسی خاصیت بسته بودن نسبت به عملگر XOR داریم:

$$\text{if}\begin{cases} h_1\in C\cup C' \rightarrow h_1\in C \text{ یا } h_1\in C'\\ h_2\in C\cup C' \rightarrow h_2\in C \text{ یا } h_2\in C'\end{cases}$$

درباره‌ی h_1، h_2 نمی‌توان با قطعیت نظر داد مگر اینکه C با C' برابر باشند (یا یکی زیرمجموعه دیگری باشد) که در این صورت کد $C\cup C'$ نیز خطی خواهد شد.

سوال 6 کتاب) کد خطی (n,k) با ماتریس مولد G (با ستون‌های غیرصفر)، تمامی کدوردهای C در یک ماتریس $2^k\times n$

a) نشان دهید تمام درایه‌های یک ستون از این ماتریس صفر نیست.

اگر تمامی پیام‌ها (2^k پیام) را در یک ماتریس $2^k\times k$ بچینیم و آن را در G ضرب کنیم ماتریس مورد نظر $2^k\times n$ ساخته خواهد شد.

$$V_{2^k\times k}\cdot G_{k\times n}=U_{2^k\times n} \Rightarrow \begin{bmatrix}v_1\\v_2\\ \vdots\\ v_n\end{bmatrix}[g_1,g_2,\dots,g_n]=\begin{bmatrix}v_1g_1, & v_1g_2, & \dots, & v_1g_n\\ \vdots & & & \\ v_ng_1, & v_ng_2, & \dots, & v_ng_n\end{bmatrix}$$

g_i ها ستون‌های ماتریس G هستند که هیچ کدام برابر با صفر نیستند. بنابراین در ماتریس U ساخته شده حاصل ضرب یکی از v_iها با یکی از g_iها صفر نشده و هیچگاه ستون تماماً صفر در U نخواهیم داشت.

$U_{2^k\times n}$ یک عضو دارد $u.G=[\underline{u}\times \underline{g}_1\quad \underline{u}\times \underline{g}_2\ \cdots\ \underline{u}\times \underline{g}_n]$ ضرب داخلی / ستون G

به ازای (حداقل) یک $\underline{u}$ (که 2^k تا هستند)، در هر ستون حداقل یکی از $\underline{u}\underline{g}_i$ ها غیر صفر است که $\underline{u}=\underline{g}_i$ ...

b) نشان دهید هر ستون از ماتریس U دارای 2^{k-1} صفر و 2^{k-1} یک است.

از قسمت قبل می دانیم هر ستون حداقل شامل یک 1 می باشد. حال ستون m ام از ماتریس U را در نظر می گیریم. F_0 را مجموعه کدهایی در نظر می گیریم که در مکان ستون m ام دارای صفر هستند و F_1 را مجموعه کدهایی در نظر می گیریم که در ستون m ام دارای یک هستند (می دانیم هر ستون U یک کدورد معتبر است)، اگر x را متعلق به مجموعه ی F_1 در نظر بگیریم و x را با تمامی کدوردهای F_0 جمع کنیم مجموعه ی جدیدی حاصل می شود که به دلیل خطی بودن کد (بسته بودن نسبت به جمع) این مجموعه نیز کدوردهای معتبر هستند که در مکان ستون m ام به دلیل جمع شدن با x دارای یک هستند. این مجموعه را F_1' می نامیم. تعداد کدوردهای F_1' با F_0 به طور واضح برابر است

$|F_1'| = |F_0|$ (1) و $F_1' \subseteq F_1$ (2) (چون F_1 مجموعه ی تمامی کدوردهایی است که در مکان ستون m ام دارای 1 است و F_1' هم کدوردهایی است که در مکان ستون m ام دارای 1 هستند پس F_1' زیرمجموعه ای از F_1 است)

حال با جمع کردن x با تمامی کدوردهای F_1، کدوردهایی حاصل می شود که در مکان ستون m ام دارای صفر هستند. این مجموعه را F_0' می نامیم. مشابه حالت بالا واضح است.

$|F_0'| = |F_1|$ (3) و $F_0' \subseteq F_0$ (4)

$$(2) \Rightarrow |F_1'| < |F_1| \overset{(1)}{\Longrightarrow} |F_0| < |F_1|$$
$$(4) \Rightarrow |F_0'| < |F_0| \overset{(3)}{\Longrightarrow} |F_1| < |F_0|$$
$$\Rightarrow |F_0| = |F_1|$$

پس نتیجه می گیریم تعداد صفرها و یک های یک ستون با هم برابر و مساوی 2^{k-1} است.

c) نشان دهید مجموعه ی تمام کدوردها با صفر در یک مکان مشخص یک زیرفضا از C است. بعد این زیرفضا چقدر است؟

اگر F را مجموعه ی تمام کدوردهایی در نظر بگیریم که در مکان m ام دارای صفر هستند. اگر $x, y \in F$ باشند آنگاه $x \oplus y \in F$ است (زیرا با جمع x و y کدورد معتبری حاصل می شود (به دلیل خطی و بسته بودن کد) که این کدورد نیز در مکان m ام دارای صفر است) پس مجموعه ی F نسبت به عمل جمع بسته است. در نتیجه F یک زیرفضا از C است. از قسمت قبل می دانیم تعداد این کدوردها 2^{k-1} است پس بعد این زیرفضا $k-1$ است.

سوال 8 کتاب) ثابت کنید هر کدورد خطی قابلیت تصحیح تعداد λ یا کمتر خطا را دارد؛ به طور همزمان قابلیت تشخیص l $(\lambda < l)$ یا کمتر خطا را دارد اگر کمترین فاصله ی کدوردهای آن در رابطه ی $d_{min} \geq \lambda + l + 1$ صدق کند.

کدوردی با d_{min} دارای قدرت تصحیح حداکثر $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ است یعنی $\lambda < \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$. می دانیم تمامی الگوهای خطا با طول کمتر مساوی λ می توانند به عنوان coset leader در روش standard array استفاده شوند و بنابراین قابل تصحیح اند. برای اینکه الگوی خطا با طول l قابل تشخیص باشد باید نشان دهیم l هر چقدر باشد با الگوهای تولید شده در coset های با leader $\lambda < \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ وجود نداشته باشد. زیرا اگر این الگوی خطا در این coset ها وجود داشته باشد تصحیح می شوند و تشخیص داده نمی شوند. بنابراین اگر x را الگوی خطایی با طول l در نظر بگیریم و این الگو بخواهد در coset با y leader باشد که $w(y) < \lambda$ است باید:

$$w(x+y) \leq w(x) + w(y) \leq l + \lambda < d_{min}$$

پس اگر $d_{min} > \lambda + l$ یا $(d_{min} \geq \lambda + l + 1)$، دیگر الگوی x در coset با y leader اتفاق نخواهد افتاد و قابل تشخیص خواهد بود.

سوال ۱۰ کتاب) کد (8,4) مطرح شده در سوال ۱ کتاب دارای $d_{min}=4$ است و به همین سبب تنها ۱ خطا را می‌تواند اصلاح کند. $\left(\left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{3}{2} \right\rfloor = 1\right)$ و بطور همزمان 2 خطا را می‌تواند شناسایی کند. $\left(\boxed{l=2} \Leftarrow d_{min} \geq \lambda + l + 1 \right)$

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

یک دکدر برای این کد بسازید که این ویژگی‌ها را داشته باشد.

مراحل decode کردن بر اساس Standard array :

۱- ابتدا S را حساب می‌دهیم $S = r \cdot H^T$ (r بردار دریافتی است)

2- بررسی می‌کنیم Coset متناظر با S را، هرگاه ei دارای یک خطا باشد (در 8 حالت اتفاق می‌افتد) خطا را اصلاح می‌کنیم و در غیر این صورت $(2^4 - 8 = 8)$ حالت که ei دارای دو خطا است خطا را تشخیص می‌دهیم.

3- برای اصلاح خطا $r' = r + e_i$ و سپس r' را کدگشایی می‌کنیم و در حالت تشخیص تقاضای ارسال دوباره می‌کنیم.

syndrome	ei
1 0000	00000000
2 1000	10000000
3 0100	01000000
4 0010	00100000
5 0001	00010000
6 1101	00001000
7 0110	00000100
8 1110	00000010
9 1011	00000001
10 1100	11000000
11 1010	10100000
12 1001	10010000
13 0101	10001000
14 0011	10000001
15 0111	00010100
16 1111	00010010

قابل تصحیح $\binom{8}{1} = 8$

قابل تشخیص

لازم به ذکر است بقیه دو خطاها در جمع این Coset leader ها با کد دوهای متناظر در همین دو مسطر ظاهر خواهند شد

درصورتی که ei ها دارای وزن یک هستند و با توجه به اینکه کد دارای 16 کد دو با وزن 4، کد دو با وزن 8 و کد دو 0 است تمامی کدهای ساخته شده توسط این ei ها دارای وزن بزرگتر از 3 هستند و لذا هیچ کد ساخته شده دارای وزن دو نمی‌باشد و تمامی کلمات دارای وزن دو در دسته دوم قرار خواهند گرفت

سوال 13 کتاب) اگر c_1 یک کد خطی سیستماتیک (n_1, K) با فاصله‌ی مینیمم d_1 و ماتریس مولد $G_1 = [P_1 \; I_K]$ باشد و فرض کنید C_2 یک کد خطی سیستماتیک (n_2, K) با فاصله‌ی مینیمم d_2 و ماتریس مولد $G_2 = [P_2 \; I_K]$ باشد. یک کد خطی (n_1+n_2, K) را با ماتریس Parity زیر در نظر بگیرید.

$$H = \left[I_{n_1+n_2-K} \;\middle|\; \begin{matrix} P_1^T \\ I_K \\ P_2^T \end{matrix} \right]$$

نشان دهید این کد دارای مینیمم فاصله $d_1 + d_2$ است.

ماتریس مولد کد (n_1+n_2, K) از روی ماتریس H به صورت زیر بدست می‌آید.

$$G = \left[P_1 \; I_K \; P_2 \;\middle|\; I_K \right] = [G_1, G_2]$$

$$u_{(1,K)} \, G_{(K, n_1+n_2)} = V_{(1, n_1+n_2)} \Rightarrow u \cdot [G_1, G_2] = [uG_1, uG_2] = [V_1, V_2]$$

این کد در واقع Cascade دو کد G_2, G_1 است. یعنی با کنار هم قرار دادن کلمات کد G_2, G_1 کد G حاصل خواهد شد. پس:

$$\min \omega(V) = \min \omega(V_1, V_2) = \min \omega(V_1) + \min \omega(V_2) = d_1 + d_2$$

سوال ۱۰ کتاب) کد (8,4) مطرح شده در سوال ۱ کتاب دارای $d_{min}=4$ است و به همین سبب تنها ۱ خطا را می‌تواند اصلاح کند.

$\left(\left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{3}{2} \right\rfloor = 1\right)$ و به طور همزمان 2 خطا را می‌تواند شناسایی کند. $\left(\boxed{l=2} \Leftarrow d_{min} \geq \lambda + l + 1 \right)$

یک decoder برای این کد بسازید که این ویژگی‌ها را داشته باشد.

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

مراحل decode کردن بیت از ساختار standard array :

۱- ابتدا S را محاسبه می‌دهیم $S = r \cdot H^T$ (r بردار دریافتی است)

2- سپس سطری از Coset متناظر با S را پیدا می‌کنیم. اگر e_i دارای یک خطا باشد (در 8 حالت امکان دارد) خطا را اصلاح می‌کنیم و در غیر این صورت ($2^4 - 8 = 8$) حالت که e_i دارای دو خطا است خطا را تشخیص می‌دهیم.

3- برای اصلاح خطا $r' = r + e_i$ و سپس r' را decode می‌کنیم و در هنگام تشخیص تقاضای ارسال دوباره می‌کنیم.

syndrome	e_i
1 0000	00000000
2 1000	10000000
3 0100	01000000
4 0010	00100000
5 0001	00010000
6 1101	00001000
7 0110	00000100
8 1110	00000010
9 1011	00000001
10 1100	11000000
11 1010	10100000
12 1001	10010000
13 0101	10001000
14 0011	10000001
15 0111	00010100
16 1111	00010010

قابل تصحیح $\binom{8}{1} = 8$

قابل تشخیص

لازم به ذکر است بقیه دو خطاها در جمع این leader Coset‌ها با کدهای مذکور در همین دو سطر ظاهر خواهند شد

در حقیقت e_i خطاهای دارای وزن یک هستند و با توجه به اینکه کد دارای 16 کد و با وزن 4، ۱ کد و با وزن 8 و ۱ کد صفر است تمامی کدهای ساخته شده توسط این e_i خطاها دارای وزن ۳ یا ۵ هستند و لذا هیچ کد ساخته شده دارای وزن دو نمی‌باشد و تمامی حالات دارای وزن دو در دسته دوم قرار خواهند گرفت.

سوال 13 کتاب) اگر C_1 یک کد خطی سیستماتیک (n_1, K) با فاصله‌ی مینیمم d_1 و ماتریس مولد $G_1 = [P_1 \; I_K]$ باشد و فرض کنید C_2 یک کد خطی سیستماتیک (n_2, K) با فاصله‌ی مینیمم d_2 و ماتریس مولد $G_2 = [P_2 \; I_K]$ باشد. یک کد خطی (n_1+n_2, K) را با ماتریس Parity زیر در نظر بگیرید.

$$H = \begin{bmatrix} I_{n_1+n_2-K} & \begin{matrix} P_1^T \\ I_K \\ P_2^T \end{matrix} \end{bmatrix}$$

نشان دهید این کد دارای مینیمم فاصله‌ی $d_1 + d_2$ است.

ماتریس مولد کد (n_1+n_2, K) از روی ماتریس H به طریق زیر بدست می‌آید.

$$G = \left[P_1 \; I_K \; P_2 \; \vdots \; I_K \right] = \left[G_1, G_2 \right]$$

$$u_{(1,K)} \, G_{(K, n_1+n_2)} = V_{(1, n_1+n_2)} \Rightarrow u \cdot [G_1, G_2] = [uG_1, uG_2] = [V_1, V_2]$$

این کد در واقع Cascade دو کد G_1, G_2 است. یعنی با کنار هم قرار دادن کلمات کد G_1, G_2 کد G حاصل خواهد شد. پس:

$$\min \omega(V) = \min \omega(V_1, V_2) = \min \omega(V_1) + \min \omega(V_2) = d_1 + d_2$$

سوال ۱) اگر ماتریس مولد کد خطی سیستماتیک به صورت زیر باشد.

$$G=\begin{bmatrix}0&0&1&1&1&0&1\\0&1&0&0&1&1&1\\1&0&0&1&1&1&0\end{bmatrix}_{3\times7}$$

الف) ماتریس H (Parity check) متناظر را بیابید.

با تعویض ستون اول و ستون سوم یک کد سیستماتیک می‌سازیم

$$G'=\left[\begin{array}{ccc|cccc}1&0&0&1&1&0&1\\0&1&0&0&1&1&1\\0&0&1&1&1&1&0\end{array}\right] \Rightarrow H'=\left[\begin{array}{ccc|cccc}1&0&1&1&0&0&0\\1&1&1&0&1&0&0\\0&1&1&0&0&1&0\\1&1&0&0&0&0&1\end{array}\right]$$

حال برای به دست آوردن ماتریس H باید ستون اول و سوم ماتریس H' را جابجا کنیم ⇐

$$H=\left[\begin{array}{ccc|cccc}1&0&1&1&0&0&0\\1&1&1&0&1&0&0\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{array}\right]$$

ب) کمترین فاصله در این کد چه میزان است؟ کمترین تعداد ستون‌های H' که جمع آن‌ها برابر صفر می‌شود که برابر ۴ است.

$d_{min}=4$

ستون اول + ستون دوم + ستون چهارم + ستون سوم = 0

ج) جدول سندرم را برای این کد رسم کنید.

سندرم	Coset leaders 000	001	010	100	011	101	110	111
0 0000	0000000 0	1001110	0100111	0011101	1101001	1010011	0111010	1110100
1 0001	0000001 1	1001111	0100110	0011100	1101000	1010010	0111011	1110101
2 0010	0000010 2	1001100	0100101	0011111	1101011	1010001	0111000	1110110
4 0100	0000100 4	1001010	0100011	0011001	1101101	1010111	0111000	1110000
8 1000	0001000 8	1000110	0101111	0010101	1100001	1011011	0110010	1111100
13 1101	0010000 16	1011110	0110111	0001101	1111001	1000011	0101010	1100100
7 0111	0100000 32	1101110	0000111	0111101	1001001	1110011	0011010	1010100
14 1110	1000000 64	0001110	1100111	1011101	0101001	0010011	1111010	0110100
3 0011	0000011 3	1001101	0100100	0011110	1101010	1010000	0111001	1110111
6 0110	0000110 6	1001000	0100001	0011011	1101111	1010101	0111100	1110010
12 1100	0001100 12	1000010	0101011	0010001	1100101	1011111	0110110	1111000
5 0101	0011000 24	1010110	0111111	0000101	1110001	1001011	0100010	1101100
10 1010	0110000 48	1111110	0010111	0101101	1011001	1100011	0001010	1000100
9 1001	1100000 96	0101110	1000111	1111101	0001001	0110011	1011010	0010100
15 1111	1000001 65	0001111	1100110	1011100	0101000	0010010	1111011	0110101
11 1011	0101100 44	1100010	0001011	0110001	1000101	1111111	0010110	1011000