الفصل الثالث

الشفرات التامة والشفرات ذات الصلة بها
Perfect & Related Codes

(٣,١) بعض الحدود على الشفرات
Some Bounds for Codes

نتناول الآن مسألة إيجاد عدد كلمات شفرة خطية طولها n ومسافتها d. هذه إحدى المسائل غير المحلولة للشفرات العامة ولكن يمكن حلها لبعض قيم n و d. سنجد بعض الحدود على سعة شفرة بمعرفة n و d.

إذا كان t و n عددين صحيحين حيث $0 \le t \le n$ فنعلم أن:

$$\binom{n}{t} = \frac{n!}{t!\,(n-t)!}$$

هو عدد المجموعات الجزئية التي عدد عناصر كل منها t التي يمكن اختيارها من مجموعة عدد عناصرها n. وبهذا نرى أن $\binom{n}{t}$ هو عدد الكلمات ذات الطول n والوزن t. وبهذا نحصل مباشرة على الحقيقة التالية:

مبرهنة (٣,١,١)

إذا كان $0 \le t \le n$ وكانت v كلمة طولها n فإن عدد الكلمات ذات الطول n والتي تبعد عن v بمسافة لا تزيد عن t هو:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}.$$ ■

بما أن عدد جميع الكلمات ذات الطول n يساوي 2^n فبوضع $t = n$ في المبرهنة (**٣,١,١**) نرى أن:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$$

تمرين

(**٣,١,٢**) لتكن $v = 10110$ و $t = 3$. تحقق من صواب المبرهنة (**٣,١,١**) بإيجاد جميع كلمات K^5 التي بُعدها عن v هو على الأكثر 3 ومن ثم تحقق من أننا نستطيع الحصول على هذا العدد من الكلمات بتطبيق المبرهنة (**٣,١,١**).

لإيجاد جميع الكلمات التي تبعد مسافة t عن كلمة معينة v نقوم بإيجاد المجاميع $v + w$ لكل الكلمات w ذات الوزن t. فإذا كان طول الشفرة C يساوي n ومسافتها هي $d = 2t + 1$ فلا توجد أي كلمة w تبعد مسافة على الأكثر t من كلمتي شفرة v_1 و v_2 مختلفتين. ولرؤية ذلك لاحظ أنه إذا كان $d(w, v_1) \leq t$ و $d(w, v_2) \leq t$ حيث $v_1 \neq v_2$ فنرى أن:

$$d(v_1, v_2) \leq d(v_1, w) + d(w, v_2) \leq 2t < d = 2t + 1$$

وهذا يناقض تعريف مسافة الشفرة C. مما سبق نرى أنه إذا كان طول الشفرة C يساوي n ومسافتها تساوي $d = 2t + 1$ فإن مجموعة جميع كلمات K^n التي تبعد مسافة t على الأكثر من كلمة شفرة v_1 لا تتقاطع مع مجموعة كلمات الشفرة التي تبعد بمسافة على الأكثر t من كلمة شفرة أخرى v_2 حيث $v_1 \neq v_2$ وبهذا نكون قد أثبتنا المبرهنة التالية:

مبرهنة (٣,١,٣) [حد هامينغ Hamming Bound]

إذا كانت C شفرة طولها n ومسافتها $d = 2t + 1$ أو $d = 2t + 2$ فإن:

$$|C|\left[\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}\right] \leq 2^n.$$

أي أن:

$$|C| \leq \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}.$$

■

إن حد هامينغ هو حد أعلى لعدد كلمات شفرة (سواء أكانت خطية أم لا) طولها n ومسافتها $d = 2t + 1$. وبما أن $t = \lfloor (d-1)/2 \rfloor$ فنجد استناداً إلى المبرهنة (**١,١٢,٩**) أن مثل هذه الشفرات تُصوّب جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن t.

مثال (٣,١,٤)

إذا كانت C شفرة خطية طولها $n = 6$ ومسافتها $d = 3$ $(d = 3 = 2(1) + 1)$ فنرى أن:

$$|C| \leq \frac{2^6}{\binom{6}{0}+\binom{6}{1}} = \frac{64}{1+6} = \frac{64}{7}.$$

وبما أن $|C|$ قوة للعدد 2 فيكون $|C| \leq 8$ وبهذا نجد أن $k = dimC \leq 3$. ▲

تمارين

(**٣,١,٥**) جد حداً أعلى لبعد الشفرة الخطية لقيم n و d المعطاة.

(أ) $n = 8$ ، $d = 3$ (ب) $n = 7$ ، $d = 3$

(ج) $n = 10$ ، $d = 5$ (د) $n = 15$ ، $d = 3$

(هـ) $n = 15$ ، $d = 5$ (و) $n = 23$ ، $d = 7$.

(**٣,١,٦**) تحقق من صحة حد هامينغ للشفرات الخطية التي لها المصفوفة المولّدة التالية:

(أ) $G = \begin{bmatrix} 1111100000000000 \\ 0000011111000000 \\ 0000011111111111 \end{bmatrix}$ (ب) $G = \begin{bmatrix} 100111 \\ 010101 \\ 001011 \end{bmatrix}$

(ج) $G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}$.

نعلم من البند (**٢,٧**) والمبرهنة (**٢,٩,١**) أن مصفوفة اختبار النوعية H لشفرة خطية من النوع (n, k, d) هي مصفوفة من الدرجة $n \times (n-k)$ بحيث يكون أي $d-1$

صفاً من صفوفها مُستقلة خطياً. وبما أن طول كل من صفوفها يساوي $n-k$ فيستحيل وجود أكثر من $n-k$ من الصفوف المُستقلة خطياً. إذن، $d-1 \leq n-k$. أي $k < n-d+1$ ونكون قد برهنا النتيجة التالية التي تسمى **حد سينغلتون (Singleton Bound) :**

مبرهنة (٣,١,٧) [حد سينغلتون Singleton Bound]

إذا كانت C شفرة خطية من النوع (n,k,d) فإن $d-1 \leq n-k$. ■

لاحظ أن حد سينغلتون أضعف من حد هامينغ، فمثلاً، إذا كان $n=15$ و $d=5$ فإن $k \leq 11$ استناداً إلى المبرهنة (٣,١,٧) وإن $k \leq 8$ استناداً إلى حد هامينغ. وعلى الرغم من ذلك، يوجد صنف مهم من الشفرات تُدعى الشفرات ذات المسافة العظمى القابلة للفصل وهذه شفرات تتحقق فيها المساواة لحد سينغلتون. نقول إن الشفرة الخطية من النوع (n,k,d) شفرة قابلة للفصل بالمسافة العظمى **(Maximum Distance Separable)** أو اختصاراً شفرة MDS إذا كان $d=n-k+1$ أو $(k=n-d+1)$.

المبرهنة التالية تزودنا ببعض التمييزات المتكافئة لشفرات MDS.

مبرهنة (٣,١,٨)

العبارات التالية متكافئة للشفرات الخطية C من النوع (n,k,d) :

(١) $d=n-k+1$.

(٢) أي $n-k$ من صفوف مصفوفة اختبار النوعية مُستقلة خطياً.

(٣) أي k من أعمدة مصفوفة مولّدة مُستقلة خطياً.

(٤) C هي شفرة MDS.

البرهان

باستخدام المبرهنة (٣,١,٧) نعلم أن $d \leq n-k+1$. ولكن $d \leq n-k+1$ إذا وفقط إذا كان $n-k$ صفاً من صفوف مصفوفة اختبار النوعية مُستقلة خطياً. إذن، (١) تُكافئ (٢). ولإثبات أن (١) تُكافئ (٣) لاحظ أنه إذا كان $d=n-k+1$ فلا توجد

كلمة شفرة غير صفرية تحتوي على أكثر من $k-1$ إحداثي صفري. ولكن من السهل إثبات أن أي k من أعمدة مصفوفة مولّدة من الدرجة $k \times n$ مرتبطة خطياً إذا وفقط إذا وجدت كلمة شفرة غير الصفرية تحتوي عدد k من الإحداثيات الصفرية في هذه المواقع (أثبت هذه العبارة). ■

نتيجة (٣,١,٩)

الشفرة الثنوية لشفرة MDS من النوع $(n, k, n-k+1)$ هي شفرة MDS من النوع $(n, n-k, k+1)$. ■

سنعطي أمثلة على شفرات MDS عند دراستنا لشفرات ريد وسولومن.

تمارين

(٣,١,١٠) الأعمدة 5، 3، 2 من المصفوفة المولّدة مرتبطة خطياً.

$$G = \begin{bmatrix} 11001 \\ 01110 \\ 00101 \end{bmatrix}$$

عيّن كلمة شفرة تكون الإحداثيات 5، 3، 2 فيها صفرية.

(٣,١,١١) إذا كانت k من أعمدة مصفوفة مولّدة من الدرجة $k \times n$ مرتبطة خطياً فأثبت وجود كلمة شفرة غير صفرية إحداثياتها أصفار في هذه المواقع.

هدفنا الآن محاولة إنشاء شفرات لأعداد معطاة d ، k ، n. فمثلاً، إذا كان $n = 15$ و $d = 5$ فاستناداً إلى حد هامينغ لا توجد شفرة يكون بُعدها $k = 10$ ولكن هذا الحد لا يمنع وجود شفرة من النوع (15,8,5). فهل نستطيع إيجاد شفرة من النوع (15,8,5)؟ إن حل هذه المسألة بصورة عامة عادة ما يكون صعباً جداً ولكن إحدى الطرق التي يمكن اتباعها هي إيجاد مصفوفة اختبار النوعية لمثل هذه الشفرات. أي بفرض أن $r = n - k$، نحاول إيجاد عدد n من المتجهات طول كل منها r لتكون صفوفاً للمصفوفة H على شرط أن تكون أي مجموعة من المتجهات عددها $d-1$ مُستقلة خطياً.

مثال (٣,١,١٢)

لنفرض أن $n = 15$، $k = 6$، $d = 5$. عندئذ، $r = 15 - 6 = 9$. وبهذا نرغب في إيجاد 15 متجهاً غير صفري طول كل منها 9 بحيث يكون أي 4 متجهات منها مُستقلة خطياً. إيجاد المتجهات التسعة الأولى منها عملية سهلة حيث من الممكن اعتبارها صفوف المصفوفة المحايدة I_9 من الدرجة 9×9. لنفرض الآن أننا استطعنا إيجاد ثلاثة متجهات أخرى بطريقة ما ليصبح عدد المتجهات التي وجدناها يساوي 12. وبهذا تكون:

$$H = \begin{bmatrix} I_9 \\ 111100000 \\ 100011100 \\ 101000011 \\ ? \end{bmatrix}$$

قبل الشروع في محاولة إيجاد متجه آخر لاحظ أنه من الممكن إثبات وجود مثل هذا المتجه على النحو التالي: لا يمكن أن يكون هذا المتجه صفرياً أو من المتجهات الاثني عشر التي تم اختيارها سابقاً من بين جميع المتجهات والتي عددها 2^9. كما أن هذا المتجه لا يمكن أن يكون مجموع متجهين أو ثلاثة متجهات من المتجهات التي تم اختيارها؛ لأن ذلك يؤدي إلى مجموعة مرتبطة خطيّاً مكوّنة من 3 أو 4 متجهات. وهذا يستثني اختيار $\binom{12}{3} + \binom{12}{2}$ متجهاً على الأكثر.

وباستثناء الشروط السابقة يكون بإمكاننا اختيار أي متجه مما تبقى من المتجهات. وبما أن:

$$1 + \binom{12}{1} + \binom{12}{2} + \binom{12}{3} < 2^9$$

فنرى أن مثل هذا المتجه موجود. على سبيل المثال، من الممكن اختيار المتجه 010101010 ليكون الصف الثالث عشر للمصفوفة H. نترك عملية اختيار الصفين الأخيرين من المصفوفة H للتمرين (**٣,١,٢١**).

يُبيّن لنا المثال (**٣,١,١٢**) (والتمارين ذات العلاقة) وجود شفرات من النوع (15,6,5). وهذا بدوره يُزودنا بحد أدنى للسعة العظمى (أو لأكبر بُعد) لشفرة خطية تُحقق $n = 15$ ، $d = 5$. أي أن $6 \le k \le 8$.

المبرهنة التالية تعميم للمثال (**٣,١,١٢**) لإنشاء شفرات خطية (ومن ثم إيجاد حدود دُنيا) ونترك إثباتها للتمرين (**٣,١,٢٢**).

مبرهنة (٣,١,١٣) [حد جلبرت وڤارشاموف Gilbert-Varshamov Bound]

إذا كان $\binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{d-1} < 2^{n-k}$ فتوجد شفرة خطية من النوع (n, k, d). ■

نتيجة (٣,١,١٤)

إذا كان $n \neq 1$ و $d \neq 1$ فتوجد شفرة خطية C طولها n ومسافتها على الأقل d وتحقق:

$$|C| \ge \frac{2^{n-1}}{\binom{n-1}{0}+\binom{n-1}{1}+\cdots+\binom{n-1}{d-2}}.$$ ■

مثال (٣,١,١٥)

هل توجد شفرة خطية طولها $n = 9$ وبُعدها $k = 2$ ومسافتها $d = 5$ ؟

الحل

لاحظ أن:

$$\binom{n-1}{0} + \cdots + \binom{n-1}{d-2} = \binom{8}{0} + \binom{8}{1} + \binom{8}{2} + \binom{8}{3} = 93$$

وأن $2^{n-k} = 2^{9-2} = 2^7 = 128$. وبما أن $93 < 128$ فنرى استناداً إلى حد جلبرت وڤارشاموف وجود مثل هذه الشفرة الخطية. ▲

مثال (٣,١,١٦)

جد حداً أدنى وحداً أعلى لبعد الشفرة الخطية k حيث $n = 9$ و $d = 5$.

الحل

باستخدام النتيجة (**٣,١,١٤**) نجد أن حد أدنى لعدد عناصر الشفرة C هو:

$$|C| \geq \frac{2^{n-1}}{\binom{n-1}{0}+\cdots+\binom{n-1}{d-2}} = \frac{2^{9-1}}{\binom{8}{0}+\binom{8}{1}+\binom{8}{2}+\binom{8}{3}} = \frac{2^8}{93} = \frac{256}{93} = 2.75.$$

ولكن C خطية ومن ثم فإن $|C|$ قوة للعدد 2. وبهذا يكون $|C| \geq 4$.

ولإيجاد حد أعلى للعدد $|C|$ نستخدم حد هامينغ فنجد:

$$|C| \leq \frac{2^9}{\binom{9}{0}+\binom{9}{1}+\binom{9}{2}} = \frac{512}{1+9+36} = \frac{512}{46} = 11.13.$$

ولكن C شفرة خطية ومن ثم $|C|$ قوة للعدد 2. وبهذا يكون $|C| \leq 8$. مما سبق نجد أن $2^2 \leq |C| \leq 2^3$. أي أن $2 \leq k \leq 3$. وبهذا توجد شفرات خطية من النوع (9,2,5) و (9,3,5) ولكن لا توجد شفرات خطية من النوع $(9, k, 5)$ حيث $k > 3$. ▲

مثال (٣,١,١٧)

هل توجد شفرة خطية من النوع (15,7,5)؟

الحل

باستخدام حد جلبرت وڤارشاموف نرى أن:

$$\binom{n-1}{0}+\cdots+\binom{n-1}{d-2} = \binom{14}{0}+\binom{14}{1}+\binom{14}{2}+\binom{14}{3}$$
$$= 1 + 14 + 91 + 364 = 470$$

وأن $2^{n-k} = 2^{15-7} = 256$. وبما أن $256 < 470$ فنجد أن حد جلبرت وڤارشاموف غير مُحقق ومن ثم فلا نستطيع الجزم بوجود أو عدم وجود مثل هذه الشفرات. سنرى لاحقاً أن مثل هذه الشفرة موجودة وهي مثال على شفرة BCH التي تُصوّب خطأين. ▲

تمارين

(**٣,١,١٨**) لكل فقرة من فقرات التمرين (**٣,١,٣**) ضع $k = 2d$ ثم قرر وجود أو عدم وجود شفرة تحقق المطلوب. وفي حالة عدم تقييد k، جد حداً أدنى وحداً أعلى لعدد كلمات الشفرة.

(**٣,١,١٩**) جد حداً أدنى وحداً أعلى لعدد كلمات الشفرات الخطية ذات الطول n والمسافة d لما يلي:

(أ) $n = 15$ ، $d = 5$ (ب) $n = 15$ ، $d = 3$

(ج) $n = 11$ ، $d = 3$ (د) $n = 12$ ، $d = 3$

(هـ) $n = 12$ ، $d = 4$ (و) $n = 12$ ، $d = 5$.

(**٣,١,٢٠**) هل من الممكن إيجاد شفرة خطية من النوع (8,3,5) ؟

(**٣,١,٢١**) جد شفرة من النوع (15,6,5) بإنشاء مصفوفة اختبار النوعية (انظر المثال (**٣,١,١٢**) ولاحظ أن وزن كل من الكلمات الثلاث الباقية يجب أن يكون على الأقل 4. لماذا ؟)

(**٣,١,٢٢**) لتكن H_i مصفوفة من الدرجة $i \times (n-k)$ حيث أي $d-1$ من صفوفها مُستقلة خطياً.

(أ) أثبت أنه يوجد على الأكثر $N_i = \binom{i}{0} + \binom{i}{1} + \cdots + \binom{i}{d-1}$ كلمة في المجموعة K^{n-k} بحيث تكون كل منها تركيباً خطياً لعلى الأكثر $d-2$ صفاً من صفوف H_i.

(ب) إذا كان $N_i < 2^{n-k}$ فبرهن أنه يمكن إضافة صف بحيث يكون أي $d-1$ من صفوف المصفوفة الناتجة عن ذلك مُستقلة خطياً.

(ج) أثبت حد جلبرت وڤارشاموف.

(د) أثبت النتيجة (**٣,١,١٤**).

(٣,٢) الشفرات التامة
Perfect Codes

نقول إن الشفرة C من الطول n والمسافة الفردية $d = 2t+1$ هي **شفرة تامة** (**Perfect Code**) إذا حققت المساواة في حد هامينغ المبين في المبرهنة (**٣,١,٣**). أي إذا كان:

$$|C| = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}.$$

على الرغم من عدم وجود عدد كبير من الشفرات الخطية التامة إلا ان لهذا العدد القليل من الشفرات الخطّيّة التامة أهمية كبيرة. الجزء الأهم في إنشاء شفرة خطية تامة يكمن في التحقق من أن العدد $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}$ هو قوة للعدد 2 ؛ (لأن $|C|$ قوة للعدد 2).

مثال (٣,٢,١)

أثبت أن $C=K^n$ شفرة تامة.

الحل

لاحظ أن مسافة K^n هي $d=1=2(0)+1$ ومن ثم فإن $t=0$. ونرى أن :

$$\frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}=\frac{2^n}{\binom{n}{0}}=2^n=|K^n|$$

وبهذا تكون K^n شفرة تامة. ▲

مثال (٣,٢,٢)

إذا كانت C شفرة تامة حيث طولها ومسافتها متساويان ويساوي كل منهما $2t+1$ فأثبت أن C تحتوي على كلمتين فقط.

الحل

لنفرض أن $n=d=2t+1$. عندئذ ،

$$\binom{n}{n-i}=\frac{ni}{(n-i)!(n-(n-i))!}=\frac{n!}{(n-i)!i!}=\binom{n}{i}.$$

وبهذا نرى أن :

$$\binom{n}{0}=\binom{n}{n},\binom{n}{1}=\binom{n}{n-1},\binom{n}{2}=\binom{n}{n-2},\cdots,$$

وبوضع $n=2t+1$ نجد :

$$\binom{n}{t}=\binom{n}{n-t}=\binom{n}{t+1}$$

وبهذا يكون:

$$\binom{n}{0}+\cdots+\binom{n}{t}=\frac{1}{2}\left(\binom{n}{0}+\cdots+\binom{n}{n}\right)=\frac{1}{2}\cdot 2^n=2^{n-1}$$

إذن، $|C|=\frac{2^n}{\binom{n}{0}+\cdots+\binom{n}{t}}=\frac{2^n}{2^{n-1}}=2$.

لاحظ أن شفرة التكرار $C=\{00,11\}$ هي الشفرة الخطية التامة الوحيدة التي تحتوي على كلمتين فقط. ▲

الشفرتان المقدمتان في المثالين **(٣,٢,١)** و **(٣,٢,٢)** هما شفرتان تامتان، ولكن لا توجد لهما فائدة تُذكر عند التطبيق العملي ولهذا السبب يُطلق عليهما **الشفرتان التامتان التافهتان (Trivial Perfect Codes)**.

مثال (٣,٢,٣)

إذا كان $n=7$ و $d=3$ فنرى أن $t=1$ وأن:

$$|C|=\frac{2^7}{\binom{7}{0}+\cdots+\binom{7}{1}}=\frac{128}{8}=16=2^4.$$

وبهذا نرى إمكانية وجود شفرة خطية تامة طولها $n=7$ ومسافتها $d=3$. هذه الشفرة موجودة وتُسمى **شفرة هامينغ (Hamming Code)** وسنقدمها في البند القادم. ▲

مثال (٣,٢,٤)

إذا كان $n=23$ و $d=7$ فإن $t=3$ وإن:

$$|C|=\frac{2^{23}}{\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}}=\frac{2^{23}}{1+23+253+1771}$$
$$=\frac{2^{23}}{2048}=\frac{2^{23}}{2^{11}}=2^{12}=4096$$

وهذا يُبين إمكانية وجود شفرة خطية تامة طولها $n=23$ ومسافتها $d=7$. سنرى في بند قادم أن مثل هذه الشفرة موجودة وتُسمى **شفرة غوليه (Golay Code)**. ▲

تمارين

(**٣,٢,٥**) إذا كان $n = 2^r - 1$ فأثبت أن $\binom{n}{0} + \binom{n}{1} = 2^r$.

(**٣,٢,٦**) هل توجد شفرة تامة للقيم n و d التالية:

(أ) $n = 15$ ، $d = 3$ (ب) $n = 31$ ، $d = 3$

(ج) $= 15$ ، $d = 5$ ؟

لقد تم إيجاد القيم والمسافات الممكنة للشفرات التامة من قبل **تيتاڤايرن وڤان لنت** (**Tietärväiren and Van Lint**) في العام ١٩٧٣م ولكن برهان ذلك يُخرجنا عن نطاق هذا الكتاب.

مبرهنة (٣,٢,٧)

إذا كانت C شفرة تامة غير تافهة طولها n ومسافتها $d = 2t + 1$ فإما أن $n = 23$ و $d = 7$ أو أن $n = 2^r - 1$ حيث $r \geq 3$ و $d = 3$. ■

مبرهنة (٣,٢,٨)

إذا كانت C شفرة خطيّة تامة طولها n ومسافتها $d = 2t + 1$ فإن C تُصوّب فقط جميع أنماط الأخطاء التي أوزانها لا تزيد عن t.

البرهان

لنفرض أن C شفرة خطية طولها n ومسافتها $d = 2t + 1$. بيّنا في المبرهنة (**١,١٢,٩**) أن C تُصوّب جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن $t = (d - 1)/2$. ولهذا فكل كلمة طولها n ووزنها لا يزيد عن t هي كلمة طليعية لمجموعة مشاركة. وعدد هذه الكلمات يساوي:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}.$$

ولكن هذا العدد ما هو إلاّ عدد المجموعات المشاركة للشفرات التامة. ■

لاحظ أنه من الممكن إعادة صياغة نص المبرهنة (**٣,٢,٨**) ليكون:

كل من كلمات K^n والتي عددها 2^n تبعد مسافة t عن كلمة شفرة واحدة فقط.

هذه الخاصية تساعدنا على حساب عدد كلمات الشفرة ذات الوزن الأصغر غير الصفري للشفرة التامة. الشفرة التامة التي تُصوّب جميع أنماط الأخطاء ذات الأوزان الذي لا تزيد عن t تُدعى **شفرة تامة من الدرجة t في تصويب الأخطاء (Perfect t- Error Correcting Code)**. ومن المبرهنة (**٣,٢,٧**) نجد أن قيم t الممكنة هي $t = 1$ و $t = 3$. سندرس الحالة $t = 1$ في البند التالي.

(٣,٣) شفرات هامينغ
Hamming Code

نحن الآن جاهزون لتصميم شفرة. ندرس عائلة مهمة من الشفرات التي من السهل تشفير كلماتها وفك تشفيرها والتي تُصوّب جميع أنماط الأخطاء ذات الخطأ الواحد.

لتكن C شفرة من الطول $n = 2^r - 1$ حيث $r \geq 2$ ولتكن H مصفوفة اختبار النوعية للشفرة C. إذا كانت جميع صفوف H متجهات غير صفرية من الطول r فنقول إن C **شفرة هامينغ (Hamming Code)** من الطول $2^r - 1$.

مثال (٣,٣,١)

المصفوفة H التالية هي أحد خيارات مصفوفات اختبار النوعية لشفرة هامينغ من الطول $7 (r = 3)$:

$$H = \begin{bmatrix} 111 \\ 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

وباستخدام الخوارزمية (**٢,٥,٧**) تستطيع إيجاد مصفوفة مولّدة G لشفرة هامينغ من الطول 7 وهي:

$$G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}.$$

وبهذا نرى أن بُعد الشفرة يساوي 4 وعدد كلمات الشفرة يساوي $2^4 = 16$. وبتوظيف المبرهنة (**٢,٩,١**) نجد أن مسافة الشفرة هي $d = 3$. معدل المعلومات يساوي 4/7. ولقد قمنا في التمرين (**٢,٦,١٢**) بتشفير بعض الرسائل باستخدام هذه الشفرة. كما توجد خيارات أخرى لمصفوفة اختبار النوعية لشفرة هامينغ من الطول 7 وجميعها تولّد شفرات متكافئة. ▲

بملاحظة أن مصفوفة اختبار النوعية H لشفرة هامينغ C تحتوي جميع الصفوف من الطول r التي وزن كل منها يساوي 1 (لاحظ أن عدد هذه الصفوف يساوي r)، نرى أن أعمدة H وعددها r مُستقلة خطياً. إذن، بُعد شفرة هامينغ يساوي $2^r - 1 - r$ وعدد كلماتها يساوي 2^{2^r-1-r}.

بما أن جميع صفوف H هي كلمات غير صفرية فلا يوجد صف واحد من صفوف H مرتبط خطياً. وتكون مسافة C على الأقل 2. وبما أنه لا يوجد صفان متساويان من صفوف H فنرى أن أي صفين يجب أن يكونا مستقلين خطياً. ولهذا تكون مسافة C هي على الأقل 3. ولكن H تحتوي على الصفوف:

$$100\cdots0$$
$$010\cdots0$$
$$110\cdots0$$

وهي مجموعة مرتبطة خطياً. إذن، استناداً إلى المبرهنة (**٢,٩,١**) نرى أن مسافة شفرة هامينغ هي $d = 3$. لدينا الآن، $n = 2^r - 1$ و $d = 2t + 1 = 3$ (أي أن $t = 1$). وبهذا نرى أن:

$$\frac{2^n}{\binom{n}{0}+\cdots+\binom{n}{t}} = \frac{2^n}{\binom{n}{0}+\binom{n}{1}} = \frac{2^{2^r-1}}{1+n} = \frac{2^{2^r-1}}{1+2^r-1} = 2^{2^r-1-r} = |C|.$$

وبهذا تكون شفرة هامينغ شفرة تامة. إذن، استناداً إلى المبرهنة (**٣,٢,٨**) تكون شفرة هامينغ شفرة تامة تُصوّب خطأ واحداً فقط.

من السهل أيضاً إنشاء جدول SDA لشفرة هامينغ. بما أن أي خطأ واحد يتم تصويبه فنرى أن جميع الكلمات ذات الطول $2^r - 1$ وذات الوزن 1 هي أنماط أخطاء يتم تصويبها ومن ثم فهي كلمات طليعية للمجموعات المشاركة. وإذا كان e نمط خطأ فيكون eH حاصل جمع صفوف مصفوفة اختبار النوعية H التي تقابل المواقع التي وقعت فيها الأخطاء. وبما أن عدد صفوف H يساوي $2^r - 1$ فإن جدول SDA لشفرة هامينغ يأخذ الشكل:

التناذر	الكلمة الطليعية
$000\cdots0$	$000\cdots0$
H	I_{2^r-1}

مثال (٣,٣,٢)

استخدم شفرة هامينغ المقدمة في المثال (**٣,٣,١**) لفك تشفير $w = 1101001$.

الحل

التناذُر هو $wH = 011$ وهو الصف الرابع من صفوف H. وبهذا تكون الكلمة الطليعية u هي الصف الرابع من I_7 وهي $u = 0001000$. إذن، فك تشفير w هو:

$$w + u = 1100001.$$ ▲

تمارين

(**٣,٣,٣**) جد مصفوفة مولّدة قياسية لشفرة هامينغ من الطول 15 واستخدمها لتشفير الرسالة 111111000000000.

(**٣,٣,٤**) أنشئ جدول SDA لشفرة هامينغ من الطول 7 واستخدمه لفك تشفير الكلمات التالية:

(أ) 1101011 (ب) 1111111

(ج) 0011010 (د) 0101011

(هـ) 0100011 (و) 0001011

(**٣,٣,٥**) أنشئ جدول SDA لشفرة هامينغ من الطول 15 واستخدمه لتشفير الكلمات التالية

(أ) 01000 01010 01010 (ب) 10110 00101 11110

(ج) 00111 01110 11100 (د) 00000 10110 11100

(هـ) 00110 10100 00011 (و) 11000 11001 11001.

(**٣,٣,٦**) أثبت أن كلاً من المصفوفتين التاليتين هي مصفوفة اختبار النوعية لشفرة هامينغ من الطول 7 وأن كلاً من الشفرتين تكافئ الشفرة المقدمة في المثال (**٣,٣,١**):

$$H'' = \begin{bmatrix} 100 \\ 110 \\ 111 \\ 011 \\ 101 \\ 010 \\ 001 \end{bmatrix} \quad ، \quad H' = \begin{bmatrix} 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{bmatrix}.$$

(**٣,٣,٧**) أثبت أن جميع شفرات هامينغ ذات الطول نفسه متكافئة.

(**٣,٣,٨**) هل المصفوفة التالية هي منقول مصفوفة اختبار النوعية لشفرة هامينغ من الطول 15؟

$$H^T = \begin{bmatrix} 10001 & 10111 & 01000 \\ 11100 & 10001 & 11110 \\ 01011 & 00101 & 11101 \\ 10001 & 01011 & 00111 \end{bmatrix}$$

(**٣,٣,٩**) أثبت أن شفرة هامينغ ذات الطول $2^r - 1$ حيث $r = 2$ هي شفرة تافهة.

(**٣,٣,١٠**) استخدم شفرة هامينغ من الطول 7 المقدمة في المثال (**٣,٣,١**) والتقابل بين الرسائل وحروف الهجاء المبين في المثال (**٢,٦,١٢**) لفك تشفير الرسالة التالية :

1010111 , 0110111 , 1000010 , 0010101 , 1001011 , 0010000 , 1111100.

(٣,٤) الشفرات الممتدة

Extended Codes

زيادة طول شفرة بإضافة إحداثي واحد أو بعض الإحداثيات تؤدي أحياناً إلى الحصول على شفرات جديدة تكون قدرتها على اكتشاف وتصويب الأخطاء أفضل من الشفرة الأصلية مما يستحق التضحية الناتجة عن الانخفاض في معدل المعلومات. نُقدم في هذا البند أحد التمديدات البسيطة.

لنفرض أن C شفرة من الطول n ولنفرض أن C^* شفرة من الطول $n+1$ نحصل عليها من C بإضافة إحداثي واحد لكل من كلمات الشفرة C بحيث يُصبح وزن كل من كلمات الشفرة C^* زوجياً. تُسمى C^* **امتداداً للشفرة** C (C^* **Extended Code of** C).

أنشأنا في المثال (**١,٣,٣**) امتداداً للشفرة K^2 كما طلبنا من القارئ إنشاء امتداد للشفرة K^3 في التمرين (**١,٣,٥**).

إذا كانت درجة مصفوفة مولّدة G للشفرة الأصلية C هي $k \times n$ فمن الواضح أن :

$$G^* = [G \;\; b]$$

هي مصفوفة مولّدة للشفرة C^* وهي من الدرجة $k \times (n+1)$، حيث تمت إضافة العمود b بحيث يكون وزن كل من صفوف G^* زوجياً.

يمكن استخدام G^* والخوارزمية (**٢,٥,٧**) لإنشاء مصفوفة اختبار النوعية للشفرة C^* ولكن من الممكن إنشاء هذه المصفوفة بطريقة أسهل باستخدام مصفوفة اختبار النوعية H للشفرة C. في هذه الحالة تكون مصفوفة اختبار النوعية للشفرة الممتدة C^* هي :

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

حيث j هو العمود من الدرجة $n \times 1$ الذي جميع عناصره تساوي 1. لاحظ أن درجة H^* هي $(n+1) \times (n+1-k)$. وبما أن رتبة H هي $n-k$ فيضمن لنا عمود H^* الأخير أن تكون رتبة H^* هي $n-k+1$. إضافة إلى ذلك يكون:

$$G^*H^* = [G \;\; b]\begin{bmatrix} H & j \\ 0 & 1 \end{bmatrix} = [GH \quad Gj + b]$$

وبما أن $GH = 0$ وأن Gj يجمع الإحداثيات 1 من جميع صفوف G فنجد من تعريف b أن $Gj + b = 0$. وبهذا نرى أن $G^*H^* = 0$. واستناداً إلى المبرهنة (**٢,٧,٦**) نرى أن G^* و H^* هما بالفعل مصفوفة مولّدة ومصفوفة اختبار النوعية على التوالي للشفرة C^*.

مثال (٣,٤,١)

لتكن G مصفوفة مولّدة للشفرة الخطية C:

$$G = \begin{bmatrix} 10010 \\ 01001 \\ 00111 \end{bmatrix}.$$

عندئذ، تكون:

$$H = \begin{bmatrix} 10 \\ 01 \\ 11 \\ 10 \\ 01 \end{bmatrix}$$

مصفوفة اختبار النوعية للشفرة C وذلك استناداً إلى الخوارزمية (**٢,٥,٧**). وبهذا نحصل على مصفوفة مولّدة ومصفوفة اختبار النوعية للشفرة الممتدة C^* وهما:

$$G^* = \left[\begin{array}{c|c} 10010 & 0 \\ 01001 & 0 \\ 00111 & 1 \end{array}\right] \quad \text{و} \quad H^* = \left[\begin{array}{c|c} 10 & 1 \\ 01 & 1 \\ 11 & 1 \\ 10 & 1 \\ 01 & 1 \\ \hline 00 & 11 \end{array}\right]. \quad \blacktriangle$$

إذا كانت v كلمة من كلمات الشفرة الأصلية C وكانت v^* الكلمة المقابلة في الشفرة الممتدة C^* فنجد أن:

$$wt(v^*) = \begin{cases} wt(v) & \text{، إذا كان وزن } v \text{ زوجياً} \\ wt(v)+1 & \text{، إذا كان وزن } v \text{ فردياً} \end{cases}.$$

وبهذا، إذا كانت المسافة d للشفرة C فردية فتكون مسافة C^* هي $d+1$ وأما إذا كانت المسافة d زوجية فتكون مسافة C^* هي d أيضاً. ومن ثم يكون للشفرة الممتدة فائدة في الحالة التي تكون فيها مسافة الشفرة الأصلية C فردية وفي هذه الحالة فهي تُصوّب نفس عدد أنماط الأخطاء التي تُصوبها الشفرة الأصلية ولكنها تستطيع اكتشاف نمط خطأ زيادة عن الشفرة الأصلية. لاحظ أننا لن نجني أي فائدة من تمديد الشفرة مرتين.

مثال (٣,٤,٢)

لنفرض أن مسافة C هي $d=5$. عندئذ، تكون مسافة C^* هي $d^*=6$. استناداً إلى المبرهنة (**١,١١,١٤**) تكتشف C جميع أنماط الأخطاء غير الصفرية ذات الأوزان التي لا تزيد عن $d-1=4$ وتكتشف C^* جميع أنماط الأخطاء غير الصفرية ذات الأوزان التي لا تزيد عن $d^*-1=5$. واستناداً إلى المبرهنة (**١,١٢,٩**) تُصوّب C جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن $\lfloor (d-1)/2 \rfloor = \lfloor 4/2 \rfloor = 2$ وتُصوّب C^* جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن $\lfloor (d^*-1)/2 \rfloor = \lfloor 5/2 \rfloor = 2$. ▲

تمارين

(**٣,٤,٣**) جد مصفوفة مولّدة ومصفوفة اختبار النوعية لشفرة هامينغ الممتدة من الطول 8.

(**٣,٤,٤**) أنشئ جدول SDA لشفرة هامينغ الممتدة من الطول 8 واستخدمها لفك تشفير الكلمات التالية:

(أ) 10101010 (ب) 11010110 (ج) 11111111.

(**٣,٤,٥**) أثبت أن شفرة هامينغ الممتدة من الطول 8 هي ذاتية الثنوية (أي أن $C = C^{\perp}$).

(**٣,٤,٦**) جد صيغة للمسافة d^* للشفرة الممتدة C^* بدلالة مسافة الشفرة الأصلية C.

(**٣,٤,٧**) لتكن C شفرة هامينغ من الطول 15. جد عدد أنماط الأخطاء التي تضمن لنا المبرهنة (**١,١١,١٤**) أن C^* تستطيع اكتشافها وعدد أنماط الأخطاء التي تضمن لنا المبرهنة (**١,١٢,٩**) أن C^* تستطيع تصويبها. ما هو العدد الفعلي لأنماط الأخطاء التي تُصوّبها C^* ؟

(٣,٥) شفرة غوليه الممتدة
The Extended Golay Code

نقوم في هذا البند والبندين القادمين بإنشاء شفرتين تُصوّبان ثلاثة أخطاء فأقل. شفرة غوليه الممتدة التي نناقشها في هذا البند والبند الذي يليه هي الشفرة التي استخدمت في برنامج مكُوك الفضاء **فويجر (Voyager)** في بدايات الثمانينيات من القرن العشرين والذي قام بإرسال الصور القريبة لكوكبي **زحل والمشتري (Jupiter & Saturn)**.

لنفرض أن B هي المصفوفة التالية من الدرجة 12×12 :

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

ولنفرض أن $G = [I \;\; B]$ هي المصفوفة من الدرجة 24×12 حيث I المصفوفة المحايدة من الدرجة 12×12. تُسمى الشفرة الخطية C التي لها المصفوفة المولّدة G،

شفرة غوليه الممتدة (Extended Golay Code) ويُرمز لها بالرمز C_{24}. للمساعدة على تذكر المصفوفة B نفرض أن B_1 هي المصفوفة التي نحصل عليها من B بحذف الصف الأخير والعمود الأخير. عندئذ، للمصفوفة B_1 خاصية الدورية حيث الصف الأول منها هو 11011100010، ونحصل على الصف الثاني من B_1 بإزاحة كل من إحداثيات الصف الأول إلى اليسار بموقع واحد وإزاحة الإحداثي الأول ليكون الإحداثي الأخير والصف الثالث نحصل عليه من الصف الثاني بالطريقة نفسها وهكذا بقية الصفوف. وبهذا نرى أن المصفوفة B هي:

$$B = \begin{bmatrix} B_1 & j^T \\ j & 0 \end{bmatrix}$$

حيث j كلمة طولها 11 وجميع إحداثياتها تساوي 1. من الواضح أن $B^T = B$. أي أن B مصفوفة متماثلة.

نقدم الآن سبع خصائص مهمة تتمتع بها شفرة غوليه الممتدة C_{24} حيث $G = [I \quad B]$ مصفوفة مولّدة لها:

(١) C_{24} من الطول $n = 24$ والبعد $k = 12$ وعدد كلماتها يساوي $12^{12} = 4096$. وهذا واضح من المصفوفة G.

(٢) مصفوفة اختبار النوعية للشفرة C_{24} هي المصفوفة:

$$\begin{bmatrix} B \\ I \end{bmatrix}$$

من الدرجة 12×24. ونحصل على هذه الخاصية من الخوارزمية (**٢,٥,٧**).

(٣) مصفوفة اختبار نوعية أخرى للشفرة C_{24} هي المصفوفة:

$$H = \begin{bmatrix} I \\ B \end{bmatrix}$$

من الدرجة 12×24. لبرهان ذلك لاحظ أولاً أن وزن كل صف من صفوف B فردي (7 أو 11). ومن ثم فحاصل الضرب القياسي لأي صف مع نفسه يساوي 1.

ومن السهل رؤية أن الضرب القياسي للصف الأول من المصفوفة B مع أي صف آخر يساوي 0. ومن خاصية الدورية للمصفوفة B_1 نرى أن الضرب القياسي لأي صفين مختلفين من B يساوي 0. ومن ذلك نرى أن $BB^T = I$. وبما أن $B^T = B$ فنجد أن $B^2 = BB^T = I$. وبهذا نرى أن:

$$GH = [I \;\; B]\begin{bmatrix} I \\ B \end{bmatrix} = I^2 + B^2 = I + BB^T = I + I = 0$$

سوف نستخدم كلا مصفوفتي اختبار النوعية لفك تشفير C_{24}.

(٤) مصفوفة مولّدة أخرى للشفرة C_{24} هي المصفوفة $[B \;\; I]$ من الدرجة 12×24.

(٥) الشفرة C_{24} ذاتية الثنوية، أي أن $C_{24} = C_{24}^{\perp}$.

(٦) مسافة C_{24} تساوي 8.

(٧) C_{24} تُصوّب أنماط خطأ من النوع 3.

نترك برهان الفقرتين (٤) و (٥) للتمارين. أما برهان الفقرة (٧) فينتج مباشرة من الفقرة (٦)، ولذا نبرهن الفقرة (٦) حيث يحتوي برهانها على خصائص مهمة أخرى للشفرة C_{24}. وسننجز هذا البرهان على ثلاث مراحل.

المرحلة الأولى

وزن كل من كلمات الشفرة C_{24} مضاعف للعدد 4. ولرؤية ذلك، لاحظ أولاً أن أوزان صفوف G هي إما 8 أو 12. لنفرض أن $v \in C_{24}$ حيث $v = r_i + r_j$ و r_i ، r_j صفان مختلفان من G. بما أن صفوف B متعامدة فتكون صفوف G متعامدة. وبهذا يكون عدد الإحداثيات التي قيمها 1 المشتركة بين r_i و r_j هو عدداً زوجياً وليكن $2x$. إذن:

$$wt(v) = wt(r_i) + wt(r_j) - 2(2x)$$

وهذا مضاعف للعدد 4.

نفرض الآن أن $v \in C_{24}$ هي $v = r_i + r_j + r_k$ وأن $r_i \neq r_j \neq r_k$ صفوف من G. ولنفرض أن $v_1 = r_i + r_j$. وبما أن C_{24} ذاتية الثنوية نرى أن $v_1 \cdot r_k = 0$. وبهذا يشترك v_1 و r_k بعدد زوجي من الإحداثيات التي قيمها 1 وليكن $2y$. إذن:

$$wt(v) = wt(v_1) + wt(r_k) - 2(2y)$$

وهذا مضاعف للعدد 4. وبالاستمرار على هذا المنوال (أي باستخدام الاستقراء) نتوصل إلى أنه إذا كانت $v \in C_{24}$ تركيباً خطياً لصفوف من G فإن $wt(v)$ مضاعف للعدد 4 ونخلص إلى أن وزن أي $v \in C_{24}$ هو مضاعف للعدد 4.

المرحلة الثانية

الأحد عشر صفاً الأولى من G هي كلمات شفرة من C_{24} وزن كل منها 8. وبهذا تكون مسافة C_{24} إما 4 أو 8.

المرحلة الثالثة

سنبرهن الآن عدم وجود كلمات وزنها 4 في الشفرة C_{24}. ولهذا الغرض نفرض أن v كلمة غير صفرية من كلمات C_{24} حيث $wt(v) = 4$. بما أن كلاً من $[I \quad B]$ و $[B \quad I]$ مصفوفة مولّدة للشفرة C_{24}، فيوجد u_1 و u_2 بحيث يكون $v = u_1[I \quad B]$ و $v = u_2[B \quad I]$ و $wt(u_1) \leq 2$ و $wt(u_2) \leq 2$؛ (لأن نصف v يحتوي على الأكثر على إحداثيين من القيمة 1). ولكن لا يمكن أن يكون وزن مجموع صفين من B على الأكثر 3. إذن، $wt(u_i) + wt(u_iB) > 4$. وبهذا فلا يمكن أن يكون وزن v يساوي 4.

تمارين

(**٣,٥,١**) أثبت أن الكلمة التي جميع إحداثياتها 1 تنتمي إلى C_{24}. استنتج أن C_{24} لا تحتوي على كلمة وزنها 20.

(**٣,٥,٢**) أثبت الخاصية (٤) للشفرة C_{24}.

(**٣,٥,٣**) أثبت الخاصية (٥) للشفرة C_{24}.

(**٣,٥,٤**) استخدم المبرهنة (**٢,٩,١**) للتحقق من أن مسافة C_{24} تساوي 8.

(٣,٦) فك تشفير شفرة غوليه الممتدة

Decoding the Extended Golay Code

نقدم الآن خوارزمية لطريقة IMLD لفك تشفير الشفرة C_{24}. في هذا البند، w هي الكلمة المرسلة وv هي كلمة الشفرة الأقرب إلى w و $u = v + w$ نمط الخطأ. هدفنا هو تصويب جميع أنماط الأخطاء من الأوزان التي لا تزيد عن 3، ولذا سنفرض أن $wt(u) \leq 3$. سنضع علامة الفاصلة بين أول 12 إحداثي وآخر 12 إحداثي لكلمات K^{24} وسنكتب نمط الخطأ على الشكل $u = [u_1, u_2]$ حيث طول كل من u_1 و u_2 يساوي 12. هدفنا هو إيجاد كلمة طليعية u للمجموعة المشاركة التي تحتوي w دون الرجوع إلى جدول SDA للشفرة C_{24}.

بما أننا افترضنا أن $wt(u) \leq 3$ فيكون $wt(u_1) \leq 1$ أو $wt(u_2) \leq 1$. لنفرض أن s_1 هي تنادُر $w = v + u$ حيث استخدمنا عند حسابها مصفوفة اختبار النوعية.

$$.H = \begin{bmatrix} I \\ B \end{bmatrix}$$

عندئذ، $s_1 = wH = [u_1, u_2]H = u_1 + u_2B$. وبهذا نرى أنه إذا كان $wt(u_2) \leq 1$ فإما أن تكون s_1 كلمة طولها 3 على الأكثر (في الحالة $wt(u_2) = 0$) أو أن تكون صفاً من B تَغَيّر فيه إحداثيان على الأكثر (في الحالة $wt(u_2) = 1$). وبالمثل إذا كان $wt(u_1) \leq 1$. عندئذ، التنادُر:

$$s_2 = w\begin{bmatrix} B \\ I \end{bmatrix} = u_1B + u_2$$

إما أن تكون كلمة وزنها 3 على الأكثر وإما صفاً من B تغير فيه إحداثيان على الأكثر.

وبهذا نرى في كل من الحالتين أنه إذا كان وزن u على الأكثر 3 فيكون تحديدها أمراً سهلاً ؛ لأنه يمكن إيجاد 3 صفوف على الأكثر من إحدى مصفوفتي اختبار النوعية ومن ثم جمعها لنحصل على التناذر المقابل. باستخدام هذه الملحوظات والحقائق $B^2 = I$ و

$$\begin{aligned} s_1 &= u_1 + u_2 B = wH \\ s_2 &= u_1 B + u_2 \\ &= (u_1 + u_2 B)B = s_1 B \end{aligned}$$

نستطيع تقديم خوارزمية لفك التشفير للشفرة C_{24}. سنستخدم في هذه الخوارزمية مصفوفة اختبار النوعية :

$$H = \begin{bmatrix} I \\ B \end{bmatrix}$$

فقط وهذا ممكن من الحقائق المقدمة في الفقرة السابقة. وكما هي العادة، فبمجرد إيجاد u يكون فك تشفير w هو كلمة الشفرة $v = w + u$. نستخدم الرمز e_i ليكون لكلمة من الطول 12 التي تحتوي على الإحداثي 1 في الموقع i والإحداثيات 0 في المواقع الأخرى. ونرمز للصف i من المصفوفة B بالرمز b_i.

خوارزمية (٣,٦,١) [فك تشفير شفرة غوليه الممتدة]

(١) احسب التناذُر $s = wH$.

(٢) إذا كان $wt(s) \leq 3$ فإن $u = [s\ , 0]$.

(٣) إذا كان $wt(s + b_i) \leq 2$ حيث b_i أحد صفوف B فإن $u = [s + b_i\ , e_i]$.

(٤) احسب التناذُر الثاني sB.

(٥) إذا كان $wt(sB) \leq 3$ فإن $u = [0\ , sB]$.

(٦) إذا كان $wt(sB + b_i) \leq 2$ حيث b_i أحد صفوف B فإن :

$$u = [e_i\ , sB + b_i]$$

(٧) إذا لم تتمكن من تحديد u فاطلب إعادة إرسال.

يحتاج تنفيذ الخوارزمية (**٣,٦,١**) إلى حساب 26 وزناً على الأكثر أثناء عملية فك التشفير (لاحظ أنه إذا تم تحديد u في أي من خطوات الخوارزمية فإننا نتوقف ولا نحتاج لتنفيذ باقي الخطوات).

مثال (٣,٦,٢)

فُك تشفير $w = 101111101111\,,010010010010$.

الحل

التنادُر هو:

$$\begin{aligned} s = wH &= 101111101111 + 001111101110 \\ &= 10000000000 \end{aligned}$$

ونرى أن وزنه يساوي 2. وبما أن $wt(s) \leq 3$ فنجد:

$$u = [s\,, 0] = 100000000001\,, 000000000000$$

ومن ثم نخلص إلى أن:

$$v = w + u = 001111101110\,, 010010010010$$

هي كلمة الشفرة المرسلة. ▲

بما أن $G = [I \quad B]$ مصفوفة قياسية وأنه من الممكن تشفير أي كلمة من كلمات K^{12} على أنها رسالة (بُعد C_{24} يساوي 12) فنرى أن الرسالة المرسلة هي أول 12 إحداثي من كلمة فك التشفير v. ولذا فالرسالة المرسلة في المثال (**٣,٦,٢**) هي 001111101110.

مثال (٣,٦,٣)

فُك التشفير $w = 001001001101\,, 101000101000$.

الحل

التنادُر هو:

$$s = wH = 001001001101 + 111000000100 = 110001001001$$

ونرى أن وزن s يساوي 5. ننتقل الآن إلى الخطوة (٣) من الخوارزمية (**٣,٦,١**) فنجد:

$$s + b_1 = 000110001100$$
$$s + b_2 = 011111000010$$
$$s + b_3 = 101101011110$$
$$s + b_4 = 001001100100$$
$$s + b_5 = 000000010010$$

وبما أن $wt(s + b_5) \leq 2$ فنرى:

$$u = [s + b_5 , e_5] = 000000010010 , 000010000000$$

وبهذا نخلص إلى أن:

$$v = w + u = 001001011111 , 101010101000$$

هي كلمة الشفرة المرسلة. ▲

مثال (٣,٦,٤)

فُك التشفير $w = 000111000111 , 011011010000$.

الحل

التنادُر هو:

$$\begin{aligned} s = wH &= u_1 + u_2 B \\ &= 000111000111 + 101010101101 \\ &= 101101101010 \end{aligned}$$

ووزن s يساوي 7. وبتنفيذ الخطوة (٣) نجد أن $wt(s + b_i) \geq 3$ لكل صف b_i من صفوف B. ننتقل الآن إلى الخطوة (٤) ونحسب التنادُر الثاني فنجد:

$$sB = 111001111101$$

ووزن sB يساوي 9. ولذا ننتقل إلى الخطوة (٥) لنجد:

$$sB + b_1 = 001110111000$$
$$sB + b_2 = 010111110110$$
$$sB + b_3 = 100101101010$$
$$sB + b_4 = 000001010000$$

وبما أن $wt(sB + b_4) \leq 2$ فنرى أن:

$$u = [e_4 , sB + b_4] = 000100000000 , 000001010000$$

ونستنتج أن:

$$v = w + u = 000011000111 , 011010000000$$

هي كلمة الشفرة المرسلة. ▲

تمارين

(**٣,٦,٥**) للشفرة C_{24}، جد نمط الخطأ المرجح (إذا أمكن ذلك) لكل من الكلمات w المستقبلة التالية:

(أ) 111 000 000 000,011 011 011 011

(ب) 111 111 000 000,100 011 100 111

(ج) 111 111 000 000,101 011 100 111

(د) 111 111 000 000,111 000 111 000

(هـ) 111 000 000 000,110 111 001 101

(و) 110 111 001 101,111 000 000 000

(ز) 000 111 000 111,101 000 101 101

(ح) 110 000 000 000,100 100 100 000

(ط) 110 101 011 101,111 000 000 000.

(**٣,٦,٦**) جد نمط الخطأ الأرجح لكل من الكلمات ذات التناذرات التالية:

(أ) $s_1 = 010010000000, s_2 = 011111010000$

(ب) $s_1 = 010010100101, s_2 = 001000110000$

(ج) $s_1 = 111111000101, s_2 = 111100010111$

(د) $s_1 = 111111111011, s_2 = 010010001110$

(هـ) $s_1 = 001101110110, s_2 = 111110101101$

(و) $s_1 = 010111111001, s_2 = 100010111111$.

(**٣,٦,٧**) إذا كان وزن s أو sB يساوي 4 فأثبت أن طريقة IMLD تطلب إعادة إرسال الكلمة.

(٣,٧) شفرة غوليه
The Golay Code

يمكن الحصول على شفرة أخرى مهمة تُصوّب أنماط الأخطاء من النوع 3 بحذف أحد إحداثيات كلمات الشفرة C_{24} (يتم حذف الإحداثي من الموقع نفسه لجميع كلمات الشفرة). سنحذف في شفرتنا هذه الإحداثي الأخير من كلمات الشفرة C_{24}.

لنفرض أن $\hat{B}$ هي المصفوفة من الدرجة 11×12 التي نحصل عليها بحذف العمود الأخير من المصفوفة B. ولنفرض أن $G = [I_{12} \quad \hat{B}]$ المصفوفة من الدرجة 23×12. تُسمى الشفرة الخطية ذات المصفوفة المولّدة G، **شفرة غوليه (Golay Code)** ويُرمز لها بالرمز C_{23}.

طول C_{23} هو $n = 23$ وبُعدها هو $k = 12$ وعدد كلماتها هو $2^{12} = 4096$. لاحظ أن الشفرة الممتدة C_{23}^* هي بالفعل C_{24}. وبهذا تكون مسافة C_{23} هي $d = 7$ (انظر التمرين (**٣,٤,٦**)). ومن الممكن أيضاً إثبات ذلك باستخدام المبرهنة (**٣,٢,٨**) أو بأسلوب مماثل للبرهان المقدم في إثبات أن مسافة C_{24} تساوي 8.

شفرة غوليه C_{23} هي شفرة تامة (انظر المثال (**٣,٢,٤**)) وتُصوّب فقط جميع أنماط الأخطاء من الوزن 3 فأقل (انظر المبرهنة (**٣,٢,٨**)). وبهذا تكون المسافة بين أي كلمة مستقبلة w وبين كلمة شفرة واحدة فقط هي على الأكثر 3. ونرى أنه بإضافة إحداثي 0 أو1 إلى الكلمة w بحيث يكون وزن الكلمة $w0$ أو$w1$ الناتجة عن ذلك فردياً نحصل على كلمة مسافتها على الأكثر 3 من كلمة شفرة c من كلمات C_{24} (انظر التمرين (**٣,٧,١٠**)). وباستخدام الخوارزمية (**٣,٦,١**) لفك تشفير الكلمة المرسلة

لتكون كلمة الشفرة c ومن ثم حذف الإحداثي الأخير من c يؤدي إلى الحصول على أقرب كلمة شفرة من كلمات C_{23} إلى الكلمة w.

خوارزمية (٣,٧,١) [فك تشفير شفرة غوليه]

(١) جد الكلمة $w0$ أو $w1$ (أيهما ذات وزن فردي).

(٢) فُك تشفير wi ($i = 0$ أو $i = 1$) باستخدام الخوارزمية (**٣,٦,١**) لنحصل على كلمة شفرة c من كلمات C_{24}.

(٣) احذف الإحداثي الأخير من c.

عند التطبيق العملي تكون الكلمة المستقبلة w عادة كلمة شفرة ولكن wi الناتجة من الخطوة (١) لا يمكن أن تكون كلمة شفرة (لماذا ؟). إذا كانت w كلمة شفرة فإن تنادُر wi هو الصف الأخير من المصفوفة H (لماذا ؟). ويمكن التحقق من ذلك بسهولة قبل الشروع بتنفيذ الخوارزمية (**١,٦,١**).

مثال (٣,٧,٢)

فُك التشفير $w = 001001001001\,,\,11111110000$.

الحل

بما أن وزن w فردي فنأخذ:

$$w0 = 001001001001\,,\,111111100000$$

وبهذا نرى أن $s_1 = 100010111110$. ومن ثم يكون $s_1 = b_6 + e_9 + e_{12}$. ويكون فك تشفير $w0$ هو $001001000000\,,\,111110100000$. ونخلص إلى أن فك تشفير w هو $001001000000\,,\,11111010000$. ▲

تمارين

(**٣,٧,٣**) فُك تشفير كل من الكلمات المستقبلة التي تم تشفيرها باستخدام الشفرة C_{23}:

(أ) $101011100000\,,\,10101011011$

(ب) $101010000001\,,\,11011100010$

(ج) $100101011000\,,\,11100010000$

(د) $011001001001\,,\,01101101111$.

(**٣,٧,٤**) أثبت أن مسافة C_{23} هي $d = 7$.

(**٣,٧,٥**) احسب موثوقية C_{23} عند إرسالها عبر قناة BSC باحتمال p.

(**٣,٧,٦**) أي من C_{23} و C_{24} لها موثوقية أكبر عند استخدام قناة BSC نفسها ؟

(**٣,٧,٧**) استخدم حقيقة أن كل كلمة وزنها 4 تبعد مسافة مقدارها 7 عن كلمة شفرة واحدة (لماذا ؟) لحساب عدد الكلمات ذات الوزن 7 في شفرة غوليه [**إرشاد :** لكل كلمة شفرة c، عدد الكلمات ذات الوزن 4 التي تبعد مسافة مقدارها 3 عن c هو $\binom{7}{3}$].

(**٣,٧,٨**) استخدم التمرين (**٣,٧,٧**) لإثبات أن C_{24} تحتوي بالضبط 759 كلمة شفرة من الوزن 8. [**إرشاد :** كل كلمة وزنها 5 تبعد مسافة مقدارها 3 عن كلمة شفرة واحدة فقط].

(**٣,٧,٩**) استخدم التمرين (**٣,٥,١**) والتمرين (**٣,٧,٨**) للتحقق من جدول توزيع أوزان الشفرة C_{24} التالي :

الوزن	0	4	8	12	16	20	24
عدد الكلمات	1	0	759	2576	759	0	1

(**٣,٧,١٠**) لتكن w هي الكلمة المستقبلة المشفّرة بالشفرة C_{23}. أضف إحداثي i إلى w لتكوين كلمة wi وزنها فردي. أثبت أن بُعد wi عن كلمة شفرة من كلمات C_{24} يساوي 3 [**إرشاد :** جميع أوزان كلمات C_{24} زوجية].

(٣,٨) شفرات ريد ومولر
Reed-Muller Codes

نقدم في هذا البند دراسة مختصرة لصنف مهم من الشفرات يحتوي كحالة خاصة على شفرة هامينغ الممتدة التي درسناها سابقاً (انظر أيضاً الفصل التاسع). يرمز **لشفرة ريد ومولر من الطول 2^m والدرجة r (The rth Order Reed-Muller Code of Length 2^m)** بالرمز $RM(r,m)$ حيث $0 \le r \le m$ وتُعرف استقرائياً على النحو التالي:

(١) $RM(0,m) = \{00\cdots0\,, 11\cdots1\}$ و $RM(m,m) = K^{2^m}$.

(٢) $RM(r,m) = \{(x, x+y): x \in RM(r,m-1),\ \ y \in RM(r-1,m-1)\}$

حيث $0 < r < m$.

مثال (٣,٨,١)

$$RM(0,0) = \{0,1\}$$
$$RM(0,1) = \{00,11\}$$
$$RM(1,1) = K^2 = \{00,01,10,11\}$$
$$RM(0,2) = \{0000,1111\}$$
$$RM(2,2) = K^4$$

$RM(1,2) = \{(x, x+y): x \in \{00,01,10,11\}, y \in \{00,11\}\}$. ▲

نقدم الآن تعريفاً استقرائياً لمصفوفة مولّدة $G(r,m)$ لشفرة $RM(r,m)$ ونستخدم هذه المصفوفة عوضاً عن الوصف المقدم في بداية البند. تُعرف $G(r,m)$ على النحو التالي:

(١) $G(0,m) = [11\cdots1]$.

(٢) لكل $0 < r < m$ تكون:

$$G(r,m) = \begin{bmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \end{bmatrix}.$$

(٣) $G(m,m) = \begin{bmatrix} G(m-1,m) \\ 0\cdots01 \end{bmatrix}$.

مثال (٣,٨,٢)

$G(0,1) = [1 \quad 1]$ هي مصفوفة مولّدة للشفرة $RM(0,1)$ و $G(1,1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ مصفوفة مولّدة للشفرة $RM(1,1)$. ▲

مثال (٣,٨,٣)

إذا كان $m = 2$ فنرى أن طول الشفرة هو $n = 2^2 = 4$. والمصفوفات المولّدة عندما $r = 1,2$ هي:

$$G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{bmatrix} = \begin{bmatrix} 11 & 11 \\ 01 & 01 \\ 00 & 11 \end{bmatrix}$$ و $$G(2,2) = \begin{bmatrix} G(1,2) \\ 0001 \end{bmatrix} = \begin{bmatrix} 1111 \\ 0101 \\ 0011 \\ 0001 \end{bmatrix}.$$ ▲

مثال (٣,٨,٤)

إذا كان $m = 3$ فإن $n = 2^3 = 8$ ويكون:

$$G(0,3) = [11111111]$$

$$G(3,3) = \begin{bmatrix} G(2,3) \\ 00000001 \end{bmatrix}$$

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{bmatrix} = \begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0000 & 1111 \end{bmatrix}$$

$$G(2,3) = \begin{bmatrix} G(2,2) & G(2,2) \\ 0 & G(1,2) \end{bmatrix}.$$ ▲

تمارين

(٣,٨,٥) جد المصفوفة المولّدة $G(2,3)$.

(٣,٨,٦) جد مصفوفة مولّدة $G(r,4)$ للشفرة $RM(r,4)$ والقيم $r = 0,1,2$.

من الممكن الآن توظيف التعريف الاستقرائي وطريقة البرهان بالاستقراء الرياضي لإثبات بعض الخصائص الأساسية لشفرة ريد ومولر.

مبرهنة (٣,٨,٧)

تتمتع شفرة ريد ومولر $RM(r,m)$ من الدرجة r بالخواص التالية:

(١) طولها هو $n = 2^m$.

(٢) مسافتها هي $d = 2^{m-r}$.

(٣) بُعدها هو $k = \sum_{i=0}^{r} \binom{m}{i}$.

(٤) $RM(r-1,m)$ شفرة جزئية من $RM(r,m)$ لكل $r > 0$.

(٥) الشفرة الثنوية هي $RM(m-1-r,m)$ حيث $r < m$.

البرهان

نستخدم الاستقراء الرياضي لبرهان جميع الفقرات. من الواضح أن جميع الفقرات صائبة عندما يكون $r = 0$ و $r = m$. سنترك إثبات صواب الفقرات لجميع الشفرات $RM(r,m)$ حيث $m = 1,2,3,4$ للتمارين.

سنبرهن أولاً الفقرة (٤). أي سنبرهن أن $RM(r-1,m) \subseteq RM(r,m)$. لاحظ أولاً أن:

$$G(1,m) = \begin{bmatrix} G(1,m-1) & G(1,m-1) \\ 0 & G(0,m-1) \end{bmatrix}$$

بما أن 1 هو الصف الأعلى للمصفوفة $G(1,m-1)$ فيكون المتجه $(1,1)$ هو الصف الأعلى في المصفوفة $[G(1,m-1) \quad G(1,m-1)]$. ومن ذلك نرى أن $RM(0,m) = \{0,1\}$ مجموعة جزئية من $RM(1,m)$. وفي العموم بما أن $G(r-1,m-1)$ مصفوفة جزئية من $G(r,m-1)$ وأن $G(r-2,m-1)$ مصفوفة جزئية من $G(r-1,m-1)$ فنجد أن:

$$G(r-1,m) = \begin{bmatrix} G(r-1,m-1) & G(r-1,m-1) \\ 0 & G(r-2,m-1) \end{bmatrix}$$

مصفوفة جزئية من $G(r,m)$. وهذا يبرهن أن $RM(r-1,m)$ شفرة جزئية من $RM(r,m)$.

سنبرهن الآن الفقرة (٢) بالاستقراء الرياضي على r. بما أن:

$$RM(r,m) = \{(x, x+y) : x \in RM(r,m-1) \text{ و } y \in RM(r-1,m-1)\}$$

وأن $RM(r-1,m-1) \subseteq RM(r,m-1)$ فنرى أن $x+y \in RM(r,m-1)$. إذا كـان $x \neq y$ فنجـد باسـتخدام الاسـتقراء الرياضـي أن $wt(x+y) \geq 2^{m-1-r}$ وأن $w(x) \geq 2^{m-1-r}$ ومن هذا نجد أن:

$$wt(x,x+y) = wt(x+y) + wt(x) \geq 2 + 2^{m-1-r} = 2^{m-r}.$$

وإذا كان $x = y$ فيكون $(x,x+y) = (0,y)$. ولأن $y \in RM(r-1,m-1)$ نجد أن:

$$wt(0,y) = wt(y) \geq 2^{m-1-(r-1)} = 2^{m-r}$$

وبهذا تنتهي خطوة الاستقراء ونخلص إلى أن $d = 2^{m-r}$.

ولبرهان الفقرة (٣) لاحظ أنه من تعريف $G(r,m)$ والاستقراء الرياضي يكون:

$$\begin{aligned} dimRM(r,m) &= dimRM(r,m-1) + dimRM(r-1,m-1) \\ &= \sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} \\ &= \sum_{i=0}^{r} \left(\binom{m-1}{i} + \binom{m-1}{i-1} \right) + \binom{m-1}{0} \end{aligned}$$

وبما أن $\binom{m-1}{0} = 1 = \binom{m}{0}$ وأن $\binom{m-1}{i} + \binom{m-1}{i-1} = \binom{m}{i}$ فيكون:

$$dimRM(r,m) = \sum_{i=0}^{r} \binom{m}{i} .$$

ولبرهان الفقرة (٥) افرض أن:

$$RM(r,m) = \{(x,x+y) : x \in RM(r,m-1), y \in RM(r-1,m-1)\}$$

وأن:

$$\begin{aligned} RM(m-r-1,m) = \{(x', x'+y') : x' \in RM(m-r-1,m-1), \\ y' \in RM(m-r-2,m-1)\} \end{aligned}$$

وباستخدام فرضية الاستقراء فإن الشفرة الثنوية للشفرة $RM(r,m-1)$ هي $RM(m-r-2,m-1)$ وأن الشفرة الثنوية للشفرة $RM(r-1,m-1)$ هي $RM(m-r-1,m-1)$. وبهذا نجد أن $x\cdot y'=0$ وأن $x'\cdot y=0$.

أيضاً، بما أن $y\cdot y'=0$ وأن $RM(r-1,m-1)\subseteq RM(r,m-1)$ نجد أن :

$$(x,x+y)\cdot(x',x'+y')=(x+y)\cdot(x'+y')+x\cdot x'$$
$$=2(x\cdot x')+x\cdot y'+y\cdot x'+y\cdot y'=0$$

وبهذا تكون كل متجهات الشفرة $RM(r,m)$ عمودية على كل من متجهات الشفرة $RM(m-r-1,m)$. وبما أن :

$$dimRM(r,m)+dimRM(m-r-1,m)=\sum_{i=0}^{r}\binom{m}{i}+\sum_{i=0}^{m-r-1}\binom{m}{i}$$
$$=\sum_{i=0}^{r}\binom{m}{m-i}+\sum_{j=0}^{m-r-1}\binom{m}{j}$$
$$=\sum_{j=0}^{m}\binom{m}{j}=2^m$$

فنستنتج أن $RM(m-r-1,m)$ هي الشفرة الثنوية للشفرة $RM(r,m)$. ■

تمرين

(٣,٨,٨) أثبت صواب فقرات المبرهنة **(٣,٨,٧)** للشفرة $RM(r,m)$ حيث $1\le m\le 4$ مُستعيناً بالأمثلة **(٣,٨,١)**، **(٣,٨,٣)**، **(٣,٨,٤)** والتمرينين **(٣,٨,٥)** و **(٣,٨,٦)**.

نقوم الآن بفك تشفير شفرة ريد ومولر الخاصة $RM(1,m)$ التي هي من الدرجة 1. لاحظ أن بُعد $RM(m-2,m)$ هو 2^m-m-1 وأن مسافتها هي 4 وطولها هو 2^m. وبهذا تكون هذه الشفرة هي شفرة هامينغ الممتدة. واستناداً إلى المبرهنة **(٣,٨,٧)** تكون $RM(1,m)$ هي الشفرة الثنوية لشفرة هامينغ الممتدة $RM(m-2,m)$. نقدم الآن خوارزمية

فعّالة لفك تشفير هذه الشفرة ونؤجل فك تشفير الشفرة العامة $RM(r,m)$ إلى الفصل التاسع.

لاحظ أن $RM(1,m)$ شفرة صغيرة مسافتها كبيرة ومن الممكن إنجاز هذه الخوارزمية بفعالية جيدة، وخوارزمية فك تشفيرها هي الخوارزمية البدائية التالية:

لكل كلمة مستقبلة w جد كلمة شفرة من $RM(1,m)$ الأقرب إلى w.

مثال (٣,٨,٩)

لنأخذ الشفرة $RM(1,3)$ حيث $m=3$. طولها هو $2^3=8$ وعدد كلماتها $2^{3+1}=16$.

مسافتها تساوي 4 ومصفوفة مولّدة لها هي:

$$G(1,3)=\begin{bmatrix}1111 & 1111\\ 0101 & 0101\\ 0011 & 0011\\ 0000 & 1111\end{bmatrix}.$$

إذا استقبلنا w وكان $d(w,c)<2$ فيكون فك تشفير w هو c. أما إذا كان $d(w,c)>6$ فنرى أن $d(w,1+c)<2$ ومن ثم يكون فك تشفير w هو $1+c$ (تذكر أن 1 هي كلمة شفرة). فمثلاً إذا كانت $w=10001111$ هي الكلمة المستقبلة فتكون $c=00001111$ هي كلمة الشفرة الأقرب. أما إذا كانت $w=10101011$ هي الكلمة المستقبلة فنجد أن $c=01010101$ حيث $d(w,c)>6$ ومن ثم تكون $c+1=10101010$ هي كلمة الشفرة الأقرب. نرى مما سبق أننا نحتاج لاختبار نصف كلمات $RM(1,m)$ على الأكثر. في الحقيقة، توجد طرائق مصفوفية فعالة لحساب هذه المسافات وسنقدمها في البند التالي. ▲

تمارين

(٣,٨,١٠) لتكن $G(1,3)$ مصفوفة مولّدة للشفرة $RM(1,3)$. فك تشفير كل من الكلمات المستقبلة التالية:

(أ) 01011110 (ب) 01100111

(ج) 00010100 (د) 11001110.

(**٣,٨,١١**) لتكن $G(1,4)$ مصفوفة مولّدة للشفرة $RM(1,4)$. فُك تشفير كل من الكلمات المستقبلة التالية:

(أ) 1011011001101001 (ب) 1111000001011111.

(٣,٩) فك تشفير سريع للشفرة $RM(1,m)$

Fast Decoding for $RM(1,m)$

نقدم في هذا البند باختصار وبدون تبرير طريقة فعّالة جداً لفك تشفير الشفرات $RM(1,m)$. نوظف لهذه الطريقة **تحويل هادامار السريع (Fast Hadamard Transform)** لإيجاد أقرب كلمة شفرة. ونحتاج أولاً إلى **ضرب كرونكر (Kronecker Product)** للمصفوفات المعرف على النحو $A \times B = [a_{ij}B]$. أي، نقوم باستبدال العنصر a_{ij} من A بالمصفوفة $a_{ij}B$.

مثال (٣,٩,١)

إذا كانت $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ و $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ فيكون:

$$I_2 \times H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

و

$$H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}.$$

▲

نعرّف الآن متتالية من المصفوفات على النحو التالي:

$H_m^i = I_{2^{m-i}} \times H \times I_{2^{i-1}}$ حيث $i = 1,2,\cdots,m$ و H المصفوفة المقدمة في المثال (**٣,٩,١**).

مثال (٣,٩,٢)

إذا كان $m = 2$ فإن:

$$H_2^1 = I_2 \times H \times I_1 = I_2 \times H$$

$$H_2^2 = I_1 \times H \times I_2 = H \times I_2.$$ ▲

مثال (٣,٩,٣)

إذا كان $m = 3$ فإن:

$$H_3^1 = I_4 \times H \times I_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H_3^2 = I_2 \times H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

$$H_3^3 = H \times I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

تقترح الطريقة الاستقرائية التي استخدمت لإنشاء الشفرة $RM(1,m)$ وجود طريقة استقرائية لفك التشفير وهذه هي الفكرة الأساسية المبنية عليها خوارزمية فك تشفير $RM(1,m)$ التالية:

خوارزمية (٣,٩,٤) [فك تشفير الشفرة $RM(1,m)$]

لنفرض أن w كلمة مستقبلة وأن $G(1,m)$ مصفوفة مولّدة للشفرة $RM(1,m)$.

(١) كوّن الكلمة $\overline{w}$ من w باستبدال الإحداثيات 0 بإحداثيات -1.

(٢) احسب $w_1 = \overline{w}H_m^1$ و $w_i = w_{i-1}H_m^i$ لكل $i = 2,3,\cdots,m$.

(٣) جد الموقع j في الكلمة w_m للإحداثي الذي قيمته المطلقة أكبر ما يمكن.

لنفرض أن $v(j) \in K^m$ هو التمثيل الثنائي للعدد j (يبدأ من اليسار بالإحداثي ذي القوة الأصغر). عندئذ، إذا كان الإحداثي في الموقع j من w_m موجباً فتكون الرسالة المفترضة هي $(1, v(j))$ أما إذا كان سالباً فتكون الرسالة المفترضة هي $(0, v(j))$.

مثال (٣,٩,٥)

لنفرض أن $m = 3$ وأن $G(1,3)$ هي مصفوفة مولّدة للشفرة $RM(1,3)$ (انظر التمرين (٣,٩,٨)). إذا كانت $w = 10101011$ الكلمة المستقبلة فتكون $\overline{w} = (1,-1,1,-1,1,-1,1,1)$. نقوم الآن بحساب:

$$w_1 = \overline{w}H_3^1 = (0,2,0,2,0,2,2,0)$$
$$w_2 = w_1H_3^2 = (0,4,0,0,2,2,-2,2)$$
$$w_3 = w_2H_3^3 = (2,6,-2,2,-2,2,2,-2)$$

(انظر المثال (٣,٩,٢) لقيم H_3^1 ، H_3^2 ، H_3^3). أكبر قيمة في w_3 هي القيمة 6 في الموقع الأول. وبما أن $v(1) = 100$ و $6 > 0$ فتكون الرسالة المفترضة هي $m = (1101)$.

لنفرض الآن أن $w = (10001111)$. عندئذ، تكون $\overline{w} = (1,-1,-1,-1,1,1,1,1)$ ويكون:

$$w_1 = \overline{w}H_3^1 = (0,2,-2,0,2,0,2,0)$$

$$w_2 = w_1 H_3^2 = (-2,2,2,2,4,0,0,0)$$
$$w_3 = w_2 H_3^2 = (2,2,2,2,-6,2,2,2)$$

الإحداثي الأكبر في w_3 هو -6 وهو في الموقع 4. وبما أن $v(4) = 001$ وأن $-6 < 0$ فتكون الرسالة المفترضة هي (0001). ▲

تمارين

(**٣,٩,٦**) فُك تشفير الكلمات المستقبلة المقدمة في التمرين (**٣,٨,١٠**) باستخدام الخوارزمية (**٣,٩,٤**) والمثال (**٣,٩,٢**).

(**٣,٩,٧**) احسب H_4^i لكل من $i = 1,2,3,4$.

(**٣,٩,٨**) فُك تشفير الكلمات المستقبلة المقدمة في التمرين (**٣,٨,١١**) باستخدام الخوارزمية (**٣,٩,٤**) والتمرين (**٣,٩,٦**).