الفصل التاسع

شفرات ريد ومولر وشفرات بريبرانا
Reed-Muller & Preparata Codes

(٩,١) شفرات ريد ومولر
Reed-Muller Codes

قدّمنا في الفصل الثالث طريقة لإنشاء شفرات ريد ومولر $RM(r,m)$ ودرسنا عديداً من خواصها الأساسية. من هذه الخواص، أنها شفرات خطيّة من النوع (n,k,d) حيث $n=2^m$ ، $k=\sum_{i=1}^{r}\binom{m}{i}$ ، $d=2^{m-r}$. نقوم في هذا البند بإنشاء هذه الشفرات بطريقة أنسب لعملية فك التشفير.

وكما هو الحال مع شفرات ريد وسولومن والشفرات الأخرى، نقوم بتعليم مواقع إحداثيات الكلمات من الطول $n=2^m$ ونستخدم هنا متجهات K^m. لغرض الاتّساق والسهولة نقوم بتعليم موقع الإحداثي i بالمتجه $u_i \epsilon K^m$ حيث u_i هو التمثيل الثنائي للعدد الصحيح i ونكتب الإحداثيات بترتيب معكوس (نكتب الإحداثي ذا الترتيب الأصغر أولاً). ونُسمي ذلك، **الترتيب المعتاد (Standard Ordering)** لمتجهات K^m.

مثال (٩,١,١)

الترتيب المعتاد لمتجهات K^2 هو $(11\ ,\ 01\ ,\ 10\ ,\ 00)$ والترتيب المعتاد لمتجهات K^3 هو :

$(111\ ,\ 011\ ,\ 101\ ,\ 001\ ,\ 110\ ,\ 010\ ,\ 100\ ,\ 000)$. ▲

لكل دالة f من K^m إلى $\{0,1\}$ يوجد تمثيل وحيد (شكل متجهي وحيد) $v = (f(u_0), f(u_1), \cdots, f(u_{2^m-1}))\epsilon K^m$ حيث $u_i \epsilon K^m$ ، $n = 2^m$ ، $u_0, u_1, \cdots, u_{2^m-1}$ بالترتيب المعتاد لمتجهات K^m كما هو موصوف في بداية البند.

ينصب اهتمامنا على صنف خاص من الدوال الأساسية. فإذا كانت I مجموعة جزئية من $\{0,1,\cdots,m-1\}$، نعرّف الدالة:

$$f_I(x_0, x_1, \cdots, x_{m-1}) = \begin{cases} \prod_{i\epsilon I}(x_i + 1) & , I \neq \phi \\ 1 & , I = \phi \end{cases}$$

(f_I دالة من K^m إلى $\{0,1\}$). نفرض أن v_I هو الشكل المتجهي المقابل للدالة f_I.

مثال (٩,١,٢)

لنفرض أن $m = 3$ ومن ثم فإن $n = 2^3$.

(أ) إذا كانت $I = \{1,2\}$ فنرى أن $f_I(x_0, x_1, x_2) = (x_1 + 1)(x_2 + 1)$. والمتجه المقابل للدالة $f_{\{1,2\}}(x_0, x_1, x_2)$ يمكن إيجاده بأخذ كل عنصر $x_0x_1x_2\epsilon K^3$ من عناصر K^3 (بالترتيب المعتاد) وإيجاد القيمة $f_{\{1,2\}}(x_0, x_1, x_2)$. وبهذا نرى أن:

$$f_{\{1,2\}}(0,0,0) = 1, f_{\{1,2\}}(1,0,0) = 1, f_{\{1,2\}}(0,1,0) = 0, f_{\{1,2\}}(1,1,0) = 0,$$
$$f_{\{1,2\}}(0,0,1) = 0, f_{\{1,2\}}(1,0,1) = 0, f_{\{1,2\}}(0,1,1) = 0, f_{\{1,2\}}(1,1,1) = 0$$

إذن، $v_I = 11000000$.

(ب) إذا كانت $I = \{0\}$ فنرى أن $f_I(x_0, x_1, x_2) = (x_0 + 1)$ ويكون $v_I = 10101010$.

(ج) إذا كانت $I = \phi$ فنرى أن $f_\phi(x_0, x_1, x_2) = 1$ ويكون $v_I = 11111111$.

▲

سنستخدم لاحقاً الحقيقتين التاليتين عن الدالة f_I. الأولى هي أن $f_I(x_0, x_1, \cdots, x_{m-1}) = 1$ إذا وفقط إذا كان $x_i = 0$ لكل $i\epsilon I$.

ففي المثال (٩,١,٢) (أ)، $I = \{1,2\}$ ، $f_I(x_0, x_1, x_2) = (x_1 + 1)(x_2 + 1)$ ومن ثم يكون $f_I(x_0, 0, 0) = (0 + 1)(0 + 1) = 1$ لكل $x_0\epsilon\{0,1\}$.

أما الحقيقة الثانية فهي $f_I(u_i)f_J(u_i) = f_{I\cup J}(u_i)$ لكل $u_i \epsilon K^m$. وبهذا يكون:

$$\begin{aligned} v_I \cdot v_J &= \sum_{i=0}^{2^m-1} f_I(u_i)f_J(u_i) \\ &= \sum_{i=0}^{2^m-1} f_{I\cup J}(u_i) \\ &\equiv Wt(v_{I\cup J}) \ (mod\ 2) \end{aligned}$$

نستخدم الرمز $\mathbb{Z}_m$ للمجموعة $\{0,1,2,\cdots,m-1\}$.

تمارين

(٩,١,٣) ليكن $m = 4$ ومن ثم $n = 2^4$. لكل من المجموعات الجزئية $I \subseteq \mathbb{Z}_4$ ، جد f_I و v_I:

(أ) $I = \{0,3\}$ (ب) $I = \{0,1,3\}$

(ج) $I = \{1\}$ (د) $I = \{2,3\}$

(هـ) $I = \phi$ (و) $I = \mathbb{Z}_4$.

(٩,١,٤) ليكن $m = 5$ ومن ثم $n = 2^5$. لكل من المجموعات الجزئية $I \subseteq \mathbb{Z}_5$ ، جد f_I و v_I:

(أ) $I = \{0,2,4\}$ (ب) $I = \{0,1,3,4\}$

(ج) $I = \{1\}$ (د) $I = \{1,2,4\}$

(هـ) $I = \phi$ (و) $I = \mathbb{Z}_5$.

(٩,١,٥) لتكن $I \subseteq \mathbb{Z}_m$. استخدم الحقيقة الأولى المقدمة في الصفحة السابقة لإثبات أن $wt(v_I) = 2^{m-|I|}$.

(٩,١,٦) إذا كان v تركيباً خطياً لمتجهات على الصورة v_I فمتى يكون وزن v زوجياً؟

(٩,١,٧) ليكن $m = 4$ ومن ثم $n = 2^4$. إذا كان $I = \{0,1,3\}$ و $J = \{2,3\}$ فاحسب $v_I \cdot v_J$.

مـن الممكـن تعريـف شـفرة ريـد ومـولر $RM(r,m)$ علـى أنهـا الشـفرة الخطيّـة $\langle\{v_I: I \subseteq \mathbb{Z}_m, |I| \leq r\}\rangle$.

لاحـظ أن المجموعـة $S = \{v_I: I \subseteq \mathbb{Z}_m, |I| \leq r\}$ مُسـتقلة خطيـاً (انظـر التمـرين **(٩,١,١٠)**) ومن ثم فهي أساس للشفرة $RM(r,m)$. وبحساب عدد الكلمات v_I حيث $I \subseteq \mathbb{Z}_m$ و $|I| \leq r$ نجد الشفرة $RM(r,m)$ أن:

$$k = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}$$

ومن الواضح أن $n = 2^m$. ومن الواضح أيضاً أنه يمكن ترتيب الكلمات v_I بأي طريقة لتشكيل مصفوفة مولّدة للشفرة $RM(r,m)$. نقول إن مصفوفة مولّدة $G_{r,m}$ للشفرة $RM(r,m)$ على **شكل قانوني (Canonical Form)** إذا كانت صفوفها مرتبة بحيث تأتي v_I قبل v_J إذا كان $|J| > |I|$ أو كان $|I| = |J|$ ، $f_I(u_j) < f_J(u_j)$ و $f_I(u_i) = f_J(u_i)$ لكل $i > j$.

مثال (٩,١,٨)

الشكل **(٩,١)** يُبيّن مصفوفة مولّدة $G_{4,4}$ على شكل قانوني للشفرة $R(4,4)$. لسهولة الترميز كتبنا v_3 عوضاً عن $v_{\{3\}}$ (وهكذا لبقية المتجهات). نحصل على الترتيب السابق من التعريف كما تبيّن الأمثلة التالية. إذا كان $I = \{3\}$ و $J = \{2,3\}$ فإن $|I| < |J|$ ومن ثم $v_3 = v_I$ يقع ترتيبه قبل $v_{2,3} = v_J$. وإذا كان $I = \{2,3\}$ و $J = \{0,2\}$ فيكون $f_I(u_j) = f_J(u_j)$ لكل $i > 0$ ولكن $f_I(u_{10}) = 0 < 1 = f_J(u_{10})$ (لاحظ أن الترتيب المعتاد للمتجه $u_{10} \epsilon K^4$ هو 0101). إذن، $v_{2,3} = v_I$ يقع ترتيبه قبل $v_{0,2} = v_J$.

من السهل أن نرى أن $G_{0,4}$ ، $G_{1,4}$ ، $G_{2,4}$ ، $G_{3,4}$ هي المصفوفات الجزئية من $G_{4,4}$ المكوّنة من الصفوف الأولى وعددها $\binom{4}{0} = 1$، $\binom{4}{0} + \binom{4}{1} = 5$، $\binom{4}{0} + \binom{4}{1} + \binom{4}{2} = 11$، $\binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3} = 15$ من صفوف $G_{4,4}$ على التوالي. ▲

$$G_{4,4} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & v_{\emptyset} \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_3 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & v_2 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & v_1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & v_0 \\
 & & & & & & & & & & & & & & & & \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{2,3} \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{1,3} \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,3} \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & v_{1,2} \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & v_{0,2} \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & v_{0,1} \\
 & & & & & & & & & & & & & & & & \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{1,2,3} \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,2,3} \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,1,3} \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,1,2} \\
 & & & & & & & & & & & & & & & & \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,1,2,3}
\end{bmatrix}$$

الشكل (٩,١). المصفوفة المولّدة $G_{4,4}$.

تمارين

(٩,١,٩) جد كلاً من $G_{2,3}$ ، $G_{2,4}$ ، $G_{3,5}$ ، $G_{0,10}$.

(٩,١,١٠) أثبت أن المجموعة $\{v_I : |I| \leq r, I \subseteq \mathbb{Z}_m\}$ مُستقلة خطياً لكل $r \leq m$

[**إرشاد**: رتّب عناصر المجموعة بحيث يأتي v_I قبل v_J إذا وجد j بحيث يكون $f_I(u_j) = f_J(u_j)$ عندما $j + 1 \leq i \leq m$ ويكون $f_I(u_j) > f_J(u_j)$. أو استخدم الاستقراء على m و r].

تتم عملية التشفير مثل أي تشفير للشفرات الخطيّة حيث نقوم بضرب الرسالة بالمصفوفة $G_{r,m}$. وبهذا تكتب كل من كلمات الشفرة c على النحو التالي :

$$c = \sum_{I \subseteq \mathbb{Z}_m, |I| \leq r} m_I v_I$$

حيث قمنا بتعليم إحداثيات الرسالة m_I لتقابل الصف v_I من المصفوفة $G_{r,m}$.

مثال (٩,١,١١)

عند استخدام $G_{2,4}$ لتشفير الرسائل m نحصل على كلمة الشفرة c المقابلة.

(أ) إذا كانت : $m = 1\ 0000\ 001000$ $(m_{0,3} = 1, m_\phi = 1)$.

فإن : $c = v_\phi + v_{0,3} = 0101010111111111$.

(ب) : إذا كانت $m = 0\ 0101\ 001001$ $(m_2 = m_0 = m_{0,3} = m_{0,1} = 1)$.

فإن : $c = v_2 + v_0 + v_{0,3} + v_{0,1} = 0111100011010010$. ▲

تمرين

(**٩,١,١٢**) شفّر كلاً من الرسائل التالية باستخدام المصفوفة $G_{2,4}$:

(أ) $0\ 0101\ 000000$.

(ب) $0\ 0000\ 000001$.

(ج) $0\ 0100\ 001000$.

(٩,٢) فك تشفير شفرات ريد ومولر

Decoding Reed-Muller Codes

نستخدم طريقة سهلة التنفيذ لفك تشفير شفرات ريد ومولر تُدعى **فك التشفير المنطقي الغالب (Majority Logic Decoding)**. ولفهم هذه الطريقة يلزمنا بعض التحضير لذلك. إذا كانت $I \subseteq \mathbb{Z}_m$ فإن $I^c = \mathbb{Z}_m \backslash I$ هي متممة I في المجموعة $\mathbb{Z}_m$. لنفرض أن $H_I = \{u \epsilon K^m : f_I(u) = 1\}$. تذكر أن $f_I(x_0, \cdots, x_{m-1}) = \prod_{i \epsilon I}(x_i + 1) = 1$ إذا وفقط إذا كان $x_i = 0$ لكل $i \epsilon I$. إذا كان $x, y \epsilon H_I$ فمن الواضح أن $x_i = y_i = 0 = x_i + y_i$

لكل $i\epsilon I$ ، ومن ذلك نرى أن $x+y\epsilon H_I$. وبهذا يكون H_I فضاءً جزئياً من K^m. لكل $u=(x_0,\cdots,x_{m-1})\epsilon K^m$ ولكل $t=(t_0,t_1,\cdots,t_{m-1})\epsilon K^m$ نعرّف الدالة :

$$f_{I,t}(x_0,x_1\cdots,x_{m-1})=f_I(x_0+t_0\cdots,x_{m-1}+t_{m-1})=f_I(x+t)$$

ونعرّف $v_{I,t}$ على أنه الشكل المتجهي المقابل للدالة $f_{I,t}$.

سيكون اهتمامنا منصباً على إيجاد $v_{I,s}\cdot v_{J^c,t}$. ولهذا نحتاج إلى حساب عدد الكلمات $u\epsilon K^m$ التي تحقق $f_{I,s}(u)f_{J^c,t}(u)=1$. من تعريف H_I نرى أن $f_{I,t}(u)=f_I(u+t)=1$ إذا وفقط إذا كان $u+t=u'\epsilon H_I$ أو بصورة مكافئة $u=u'+t\epsilon H_I+t$ حيث H_I+t هي مجموعة H_I المشاركة التي يحددها t. كما أن القيمة $f_{I,s}(u)f_{J^c,t}(u)=\prod_{i\epsilon I}(x_i+s_i+1)\prod_{j\epsilon J^c}(x_j+t_j+1)$ لا تتغير لكل $x_k\epsilon\{0,1\}$ ، $k\epsilon\mathbb{Z}_m\backslash(I\cup J^c)$. وبما أنه يوجد $2^{m-|I\cup J^c|}$ خياراً للعناصر $u\epsilon K^m$ فنرى أن عدد المرات التي يكون فيها :

$$f_{I,s}(u)f_{J^c,t}(u)=1$$

هو مضاعف للعدد $2^{m-|I\cup J^c|}$ وهذا عدد زوجي ما عدا الحالة $|I\cup J^c|=m$. أي ما عدا الحالة $|I\cup J^c|=\mathbb{Z}_m$ وأما إذا فرضنا أن $|I|\leq|J|$ فنرى أن $|J^c|\leq|I^c|$ ومن ثم يكون $|I\cup J^c|=|I|+|J^c|-|I\cap J^c|<m$ إلاّ إذا كان $I=J$. وإذا كان $I=J$ فيوجد عنصر واحد $u\epsilon K^m$ يحقق $f_{I,s}(u)f_{I^c,t}(u)=1$ ، بالتحديد هذا العنصر u هو العنصر الذي يكون فيه $x_i=s_i$ لكل $i\epsilon I$ و $x_i=t_i$ لكل $i\epsilon I^c$. وبما أن إيجاد عدد المواقع التي يكون فيها $f_{I,s}(u)f_{J^c,t}(u)=1$ يُعطي مباشرة $v_{I,s}\cdot v_{J^c,t}$ فنكون قد برهنا التمهيدية التالية :

تمهيدية (٩,٢,١)

لتكن كل من I و J مجموعة جزئية من $\mathbb{Z}_m$ حيث $|J|\leq|I|$. لكل $s\epsilon H_{I^c}$ ولكل $t\epsilon H_J$ لدينا :

$$v_{I,s}\cdot v_{J^c,t}=1 \text{ إذا وفقط إذا كان } I=J.$$

نستطيع الآن وبسهولة الحصول على النتيجة التالية التي تعد الركيزة الأساسية لخطة فك التشفير التي سنستخدمها لاحقاً.

نتيجة (٩,٢,٢)

إذا كانت $c\epsilon RM(r,m)$ كلمة شفرة وكان $|J| = r$ فإن $m_J = c \cdot v_{J^c,t}$ لكل $t\epsilon H_J$.

البرهان

إذا كان $|J| = r$ فلكل $t\epsilon H_J$ نجد أن:

$$c \cdot v_{J^c,t} = \sum_{I\subseteq\mathbb{Z}_m,|I|\leq r} m_I v_I \cdot v_{J^c,t} = m_J v_J \cdot v_{J^c,t} = m_J$$

وذلك لأنه استناداً إلى التمهيدية (٩,٢,١) يكون الضرب القياسي الوحيد الذي لا يساوي صفراً في هذا المجموع هو الضرب الذي يحقق $I = J$. ■

تمهيدية (٩,٢,٣)

لتكن $J \subseteq \mathbb{Z}_m$. لكل كلمة e من الطول 2^m يكون $e \cdot v_{J^c,t} = 1$ لعلى الأكثر $wt(e)$ قيمة من القيم $t\epsilon H_J$.

البرهان

تذكر أنه لأي فضاء جزئي S من K^m تنتمي كلمتان إلى مجموعة مشاركة واحدة من المجموعات المشاركة لـ S إذا وفقط إذا كان مجموع الكلمتين كلمة تنتمي إلى S. كما أن H_J فضاء جزئي من K^m وأن $H_J \cap H_{J^c} = \{0\}$. من ذلك نرى عدم وجود كلمتين من كلمات H_J تنتميان إلى مجموعة مشاركة واحدة لـ H_{J^c}. وبهذا تكون $H_{J^c} + t$ هي جميع المجموعات المشاركة لـ H_{J^c} حيث t مأخوذة على جميع عناصر H_J. نحصل الآن على المطلوب بملاحظة أنه إذا كان $t_1, t_2\epsilon H_J$ حيث $t_1 \neq t_2$ فإن $(H_{J^c} + t_1) \cap (H_{J^c} + t_2) = \phi$ ومن ثم لا يوجد موقع مشترك بين v_{J^c,t_1} و v_{J^c,t_2} بحيث يكون الإحداثيان 1. إذن، كل

من الإحداثيات $wt(e)$ غير الصفرية في e تؤثر على قيمة واحدة على الأكثر من القيم $e \cdot v_{J^c,t}$ حيث t مأخوذة على جميع عناصر H_J. ■

نحصل الآن على خوارزمية فك تشفير على النحو التالي:

نفرض أن $w = c + e$ هي الكلمة المستقبلة حيث c كلمة شفرة تنتمي إلى $RM(r,m)$. عندئذ، $c = \sum_{I \subseteq \mathbb{Z}_m, |I| \le r} m_I v_I$ حيث $|I| \le r$. لنفرض أن $J \subseteq \mathbb{Z}_m$ حيث $|J| = r$. استناداً إلى التمهيدية (**٩,٢,٣**)، نرى أن $e \cdot v_{J^c,t} = 0$ لعلى الأقل $|H_J| - wt(e)$ قيمة من قيم $t \epsilon H_J$.

لكل قيمة t من هذه القيم لدينا:

$$w \cdot v_{J^c,t} = c \cdot v_{J^c,t} + e \cdot v_{J^c,t}$$
$$= c \cdot v_{J^c,t}$$
$$= m_J \quad \text{(باستخدام النتيجة (٩,٢,٢)).}$$

وبهذا، إذا كان $2wt(e) < |H_J|$ حيث مجال t هو عناصر H_J فنرى أن أكثر من نصف القيم $w \cdot v_{J^c,t}$ يكون m_J. وبمجرد الانتهاء من حساب m_J بهذه الطريقة لكل $J \subseteq I_m$ حيث $|J| = r$، نضع $w(r-1) = w + \sum_{|J|=r} m_J v_J$. الآن، يمكن فك تشفير $w(r-1)$ على اعتبار أنها الكلمة المستقبلة التي تم تشفيرها باستخدام الشفرة $RM(r-1,m)$. ونستمر بهذا الأسلوب حتى ننتهي من إيجاد m_J لجميع $J \subseteq I_m$ حيث $|J| \le r$.

قبل تقديم وصف لهذه الخوارزمية، لاحظ أن هذه الخوارزمية تصوّب جميع أنماط الأخطاء التي وزنها أصغر من $|H_J|/2$ حيث $|J| \le r$. ولكن باستخدام التمرين (**٩,١,٥**)، نعلم أن $|H_J| = wt(v_J) = 2^{m-|J|}$. إذن، يتم تصويب جميع أنماط الأخطاء التي وزنها أصغر من 2^{m-r-1} وبهذا تكون مسافة الشفرة $RM(r,m)$ هي على الأقل 2^{m-r}.

ومن ناحية أخرى، إذا كانت $I \subseteq \mathbb{Z}_m$ و $|I| = r$ فنرى أن v_I كلمة من كلمات الشفرة $RM(r,m)$ وزنها يساوي 2^{m-r}.

وبهذا نكون قد قدّمنا برهاناً آخر للنتيجة التالية:

تمهيدية (٩,٢,٤)

مسافة الشفرة $RM(r,m)$ تساوي 2^{m-r}.

خوارزمية (٩,٢,٥) [فك التشفير المنطقي الغالب للشفرة $RM(r,m)$]

نفّذ الخطوات التالية لفك تشفير كلمة مستقبلة:

(١) ضع $i = r$ و $w(r) = w$.

(٢) لكل $J \subseteq \mathbb{Z}_m$ حيث $|J| = i$، احسب $w(i) \cdot v_{J^c,t}$ لكل $t \epsilon H_J$ حتى يظهر الإحداثي 0 أو الإحداثي 1 أكثر من 2^{m-i-1} مرة ومن ثم ضع $m_J = 0$ أو $m_J = 1$ على التوالي. إذا ظهر كل من الإحداثيين 0 و 1 أكثر من $e = 2^{m-r-1} - 1$ مرة فاطلب إعادة إرسال.

(٣) إذا كان $i > 0$ فضع $w(i-1) = w(i) + \sum_{J \subseteq \mathbb{Z}_m} m_J v_J$ حيث $|J| = i$. إذا كان وزن $w(i-1)$ على الأكثر $e = 2^{m-r-1} - 1$ فضع $m_J = 0$ لكل $J \subseteq \mathbb{Z}_m$ حيث $|J| \leq r$ وتوقف. وإذا لم يتحقق ذلك استبدل i بالعدد $i-1$ وارجع إلى الخطوة (٢). (إذا كان $i = 0$ فنكون قد حسبنا m_J لكل $J \subseteq \mathbb{Z}_m$ حيث $|J| \leq r$ ومن ثم نكون قد وجدنا الرسالة المرجحة).

مثال (٩,٢,٦)

استخدم الخوارزمية (٩,٢,٥) لفك تشفير الكلمة المستقبلة $w = 0101011110100000$ التي سبق وشُفّرت باستخدام $G_{4,4}$.

الحل

ابـدأ بوضـع $i = r = 2$ و $w = w(2)$. مـن حسـابات الشـكل (**٩,٢**) نـرى أن $m_{2,3} = 0$ ، $m_{1,3} = 0$ ، $m_{0,3} = 0$ ، $m_{1,2} = 0$ ، $m_{0,2} = 1$ ، $m_{0,1} = 0$. إذن $w(1) = w(2) + v_{0,2} = 1111\ 0111\ 0000\ 0000$ ويكون $i = 1$.

J	t	$v_{J^c,t}$	$w \cdot v_{J^c,t}$	m_J
{0,1}	0000	1111 0000 0000 0000	0	
	0010	0000 1111 0000 0000	1	0
	0001	0000 0000 1111 0000	0	
	0011	0000 0000 0000 1111	0	
{0,2}	0000	1100 1100 0000 0000	0	
	0100	0011 0011 0000 0000	1	1
	0001	0000 0000 1100 1100	1	
	0101	0000 0000 0011 0011	1	
{1,2}	0000	1010 1010 0000 0000	1	
	1000	0101 0101 0000 0000	0	0
	0001	0000 0000 1010 1010	0	
	1001	0000 0000 0101 0101	0	
{0,3}	0000	1100 0000 1100 0000	0	
	0100	0011 0000 0011 0000	0	0
	0010	0000 1100 0000 1100	1	
	0110	0000 0011 0000 0011	0	
{1,3}	0000	1010 0000 1010 0000	0	
	1000	0101 0000 0101 0000	0	0
	0010	0000 1010 0000 1010	1	
	1010	0000 0101 0000 0101	0	
{2,3}	0000	1000 1000 1000 1000	1	
	1000	0100 0100 0100 0100	0	0
	0100	0010 0010 0010 0010	0	
	1100	0001 0001 0001 0001	0	

الشكل (٩,٢). فك التشفير المنطقي للشفرة $RM(2,4)$ (الخطوة ١).

مرة أخرى، نرى من حسابات الشكل (**٩,٣**) أن $m_3 = 1$، $m_2 = 0$، $m_1 = 0$، $m_0 = 0$. ضع $w(0) = w(1) - v_3 = 0000\ 1000\ 0000\ 0000$ وضع $i = 0$. بما أن وزن $w(0)$

على الأكثر هو $e = 1$ فنضع $m_\phi = 0$ ونتوقف. إذن، الرسالة المرجحة هي 0 1000 000010 0 (شُفّرت الرسائل باستخدام $G_{2,4}$). ▲

J	t	$v_{J^c,t}$	$w_{(1)} \cdot v_{J^c,t}$	m_J
{0}	0000	1100 0000 0000 0000	0	
	0100	0011 0000 0000 0000	0	
	0010	0000 1100 0000 0000	1	0
	0110	0000 0011 0000 0000	0	
	0001	0000 0000 1100 0000	0	
	0101	0000 0000 0011 0000	0	
	0011	0000 0000 0000 1100		
	0111	0000 0000 0000 0011		
{1}	0000	1010 0000 0000 0000	0	
	1000	0101 0000 0000 0000	0	
	0010	0000 1010 0000 0000	1	0
	1010	0000 0101 0000 0000	0	
	0001	0000 0000 1010 0000	0	
	1001	0000 0000 0101 0000	0	
	0011	0000 0000 0000 1010		
	1011	0000 0000 0000 0101		
{2}	0000	1000 1000 0000 0000	1	
	1000	0100 0100 0000 0000	0	
	0100	0010 0010 0000 0000	0	0
	1100	0001 0001 0000 0000	0	
	0001	0000 0000 1000 1000	0	
	1001	0000 0000 0100 0100	0	
	0101	0000 0000 0010 0010		
	1101	0000 0000 0001 0001		
{3}	0000	1000 0000 1000 0000	1	
	1000	0100 0000 0100 0000	1	
	0100	0010 0000 0010 0000	1	1
	1100	0001 0000 0001 0000	1	
	0010	0000 1000 0000 1000	0	
	1010	0000 0100 0000 0100	1	
	0110	0000 0010 0000 0010		
	1110	0000 0001 0000 0001	1	

الشكل (٩,٣). فك التشفير المنطقي للشفرة $RM(2,4)$ (الخطوة ٢).

تمارين

(**٩,٢,٧**) إذا علمت أن الرسائل شُفّرت باستخدام المصفوفة $G_{2,4}$ ففك تشفير الكلمات المستقبلة التالية إن أمكن ذلك.

(أ) $w = 0111\ 0101\ 1000\ 1000$

(ب) $w = 0110\ 0110\ 0001\ 0000$

(ج) $w = 0101\ 1010\ 0100\ 0101$

(د) $w = 1110\ 1000\ 1001\ 0001$

(هـ) $w = 0011\ 0000\ 0011\ 0100$

(و) $w = 1001\ 0110\ 0101\ 1010$

(ز) $w = 1010\ 1000\ 1010\ 0000$

(ح) $w = 0011\ 1100\ 0001\ 1100$

(ط) $w = 1001\ 1101\ 0001\ 1101$

(**٩,٢,٨**) إذا علمت أن الرسائل شُفّرت باستخدام المصفوفة $G_{2,4}$ ففك تشفير الكلمات المستقبلة التالية إن أمكن ذلك.

(أ) $w = 1100\ 1000\ 1110\ 0000\ 1100\ 0000\ 1100\ 0100.$

(ب) $w = 0101\ 0111\ 0101\ 1000\ 1000\ 1000\ 0111\ 1010.$

(ج) $w = 0011\ 0011\ 1111\ 0011\ 0011\ 0011\ 1111\ 1111.$

(د) $w = 0100\ 0000\ 1111\ 1111\ 0000\ 1100\ 0000\ 1111.$

(هـ) $w = 1001\ 0101\ 0110\ 1001\ 1001\ 0111\ 0110\ 1010.$

(و) $w = 0011\ 1111\ 0011\ 0011\ 1100\ 1100\ 1100\ 0100.$

(ز) $w = 0100\ 0100\ 1111\ 1111\ 0000\ 1100\ 0000\ 1111.$

(٩,٣) شفرات بريبراتا الممتدة
Extended Preparata Codes

في هذا البند نقوم بتعليم إحداثيات مواقع الكلمات من الطول 2^r باستخدام عناصر الحقل $GF(2^r)$. لقد سبق وأن استخدمنا طريقة التعليم هذه عند دراستنا لشفرات BCH حيث استخدمنا جميع كلمات الحقل غير الصفرية للتعليم. فإذا كانت U مجموعة جزئية من الحقل $GF(2^r)$ فنعرّف الكلمة $\chi(U)$ من الطول 2^r على النحو التالي:

نضع 1 في الموقع i إذا كان $\beta^i \epsilon U$ لكل $0 \le i \le 2^r - 2$.

نضع 1 في الموقع $2^r - 1$ إذا كان $0 \epsilon U$.

نضع 0 في ما تبقى من المواقع. (β عنصر بدائي في الحقل $GF(2^r)$).

مثال (٩,٣,١)

إذا كان β عنصراً بدائياً في الحقل $GF(2^3)$ فيكون:

$$\chi(\{0\}) = 00000001$$
$$\chi(\{\beta^2, \beta^5, \beta^6\}) = 00100110$$
$$\chi(\phi) = 00000000.$$ ▲

لنفرض أن $\alpha \in GF(2^r)$ وأن $U \subseteq GF(2^r)$. نعرّف المجموعتين $U + \alpha$ و αU على أنهما:

$$U + \alpha = \{u + \alpha : u \epsilon U\}$$
$$\alpha U = \{\alpha u : u \epsilon U\}.$$

كما نعرّف **الفرق التناظري (Symmetric Difference)** لمجموعتين جزئيتين U و V من الحقل $GF(2^r)$ ونرمز لذلك بالرمز $U \Delta V$ على النحو التالي:

$$U \Delta V = \{x : x \epsilon U \cup V, x \notin U \cap V\} = (U \cup V) - (U \cap V).$$

من السهل أن نرى أن:

$$\chi(U) + \chi(V) = \chi(U \Delta V).$$

مثال (٩,٣,٢)

ليكن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. ولتكن $U = \{\beta^2, \beta^5, \beta^6\}$ و $V = \{\beta^2, 0\}$. عندئذ، يكون:

$$U + \beta^2 = \{\beta^2 + \beta^2, \beta^5 + \beta^2, \beta^6 + \beta^2\} = \{0, \beta^3, \beta^0\}$$
$$\beta^2 U = \{\beta^2\beta^2, \beta^2\beta^5, \beta^2\beta^6\} = \{\beta^4, \beta^0, \beta\}$$
$$\begin{aligned}(U) + \chi(V) &= 00100110 + 00000101\\ &= 00100011\\ &= \chi(\{\beta^2, \beta^6, 0\})\\ &= \chi(U \Delta V)\end{aligned}$$

▲

تعريف (٩,٣,٣)

تُعرف شفرة **بريبراتا الممتدة (Extended Preparata Code)** $P(r)$ على أنها مجموعة كلمات شفرة على الشكل $\chi(U)$ متبوعة بكلمات شفرة على الشكل $\chi(V)$ حيث U و V مجموعتان جزئيتان من الحقل $GF(2^r)$ بحيث يتحقق ما يلي:

(i) كل من $|U|$ و $|V|$ عدد زوجي.

(ii) $\sum_{u\epsilon U} u = \sum_{v\epsilon V} v$.

(iii) $\sum_{u\epsilon U} u^3 + (\sum_{u\epsilon U} u)^3 = \sum_{v\epsilon V} v^3$.

(iv) r عدد فردي.

نكتب كلمات الشفرة على الصورة $[\chi(U), \chi(V)]$. وبما أن طول كل من $\chi(U)$ و $\chi(V)$ هو 2^r فنرى أن $P(r)$ شفرة طولها 2^{r+1}.

مثال (٩,٣,٤)

ليكن $GF(2^3)$ الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. ولنفرض أن $U = \{\beta, \beta^2, \beta^5, 0\}$ و $V = \{\beta^0, \beta, \beta^2, \beta^3, \beta^6, 0\}$. من الواضح أن الشرطين (i) و (iv) من التعريف **(٩,٣,٣)** محققان. أيضاً:

. $\sum_{u\epsilon U} u = \beta + \beta^2 + \beta^5 + 0 = 010 + 001 + 111 + 000 = \beta^0$

. $\sum_{v\epsilon V} v = \beta^0 + \beta + \beta^2 + \beta^3 + \beta^6 + 0 = 100 + 010 + 001 + 110 + 101 + 000 = \beta^0$

ومن ثم فالشرط (ii) محقق. كما أن :

. $\sum_{u\epsilon U} u^3 = \beta^3 + \beta^6 + \beta + 0 = 110 + 101 + 010 + 000 = \beta^2$

$\sum_{u\epsilon V} v^3 = \beta^0 + \beta^3 + \beta^6 + \beta^2 + \beta^4 + 0 = 100 + 110 + 101 + 001 + 000 = \beta^6$

ومن ثم فالشرط (iii) محقق ؛ لأن $\beta^2 + (\beta^0)^3 = \beta^6$. إذن ،

$[\chi(U), \chi(V)] = 0110010111110011$ كلمة من كلمات الشفرة $P(3)$. ▲

لاحظ أن وجود (أو عدم وجود) العنصر 0 في المجموعة U أو المجموعة V لا يؤثر في حسابات الشروط (ii) ، (iii) ، (iv) من التعريف (**٩,٣,٣**). ولهذا فالاستخدام الوحيد للعنصر 0 في V هو جعل $|U|$ أو $|V|$ زوجياً. وبهذا نرى أن الإحداثي الذي في الموقع 2^{r-1} من $\chi(U)$ هو إحداثي اختبار نوعية $\chi(U)$ ، وبالمثل ، الإحداثي الذي في الموقع 2^{r-1} من $\chi(V)$ هو إحداثي اختبار نوعية $\chi(V)$.

سنبيّن في المبرهنة (**٩,٣,١٨**) أن $P(r)$ ليست شفرة خطيّة وبهذا لا يوجد لها بُعد.

تمهيدية (٩,٣,٥)

لتكن كل من $[\chi(U), \chi(V)]$ و $[\chi(A), \chi(B)]$ كلمة شفرة تنتمي للشفرة $P(r)$. ولنفرض أن $\alpha = \sum_{u\epsilon U} u$. عندئذ ، $[\chi(U\Delta A + \alpha), \chi(V\Delta B)]$ كلمة شفرة تنتمي إلى $P(r)$.

البرهان

سنثبت أن $[\chi(U\Delta A + \alpha), \chi(V\Delta B)]$ تحقق الشروط (i) ، (ii) ، (iii) من التعريف (**٩,٣,٣**).

(i) بما أن كل من $|U|$ ، $|V|$ ، $|A|$ ، $|B|$ عدد زوجي فنرى أن :

$$|V\Delta B| = |V| + |B| - 2|V \cap B|$$

وهذا عدد زوجي. كما أن :

$$|U\Delta A + \alpha| = |U\Delta A| = |U| + |A| - 2|U \cap A|$$

وهذا أيضاً عدد زوجي (استخدمنا المثال **٩,٣,٢**) في المساواة الأولى).

(ii) لاحظ أولاً أن $\sum_{x\epsilon I\Delta J} x = \sum_{x\epsilon I} x + \sum_{x\epsilon J} x$ لكل $I,J \subseteq GF(2^r)$ ؛ وذلك لأن أي $\beta^i \epsilon I \cap J$ يُحسب مرتين في الطرف الأيمن ولا يُحسب في الطرف الأيسر وأن $2\beta^i = 0$.

وبهذا نرى أن :

$$\sum_{x\epsilon U\Delta A+\alpha} x = \sum_{y\epsilon U\Delta A} (y+\alpha) = \sum_{y\epsilon U\Delta A} y + \alpha|U\Delta A|$$

$$= \sum_{y\epsilon U} y + \sum_{y\epsilon A} y + 0 \qquad (\text{لأن } |U\Delta A| \text{ زوجي})$$

$$= \sum_{y\epsilon V} y + \sum_{y\epsilon B} y$$

$$= \sum_{y\epsilon V\Delta \mathrm{B}} y$$

(iii)

$$\sum_{u\epsilon U} x^3 + \left(\sum_{x\epsilon \mathrm{U}\Delta\mathrm{A}+\alpha} x\right)^3 = \sum_{y\epsilon U\Delta A} (y+\alpha)^3 + \left(\sum_{y\epsilon V\Delta \mathrm{B}} y\right)^3$$

$$= \sum_{y\epsilon U} (y+\alpha)^3 + \sum_{y\epsilon A} (y+\alpha)^3 + \left(\sum_{y\epsilon V} y + \sum_{y\epsilon B} y\right)^3$$

$$= \sum_{y\epsilon U} y^3 + \alpha \sum_{y\epsilon U} y^2 + \alpha^2 \sum_{y\epsilon U} y + \alpha^3|U| + \sum_{y\epsilon A} y^3 + \alpha \sum_{y\epsilon A} y^2 + \alpha^2 \sum_{y\epsilon A} y + \alpha^3|A|$$
$$+ \left(\sum_{y\epsilon V} y\right)^3 + \left(\sum_{y\epsilon V} y\right)^2 \left(\sum_{y\epsilon B} y\right) + \left(\sum_{y\epsilon V} y\right)\left(\sum_{y\epsilon B} y\right)^2$$
$$+ \left(\sum_{y\epsilon B} y\right)^3$$

ولكن $\alpha = \sum_{y\epsilon U} y$ ومن ثم $\sum_{y\epsilon V} y = \sum_{y\epsilon U} y = \alpha$. أيضاً، $\left(\sum_{y\epsilon V} y\right)^2 = \sum_{y\epsilon V} y^2$ حيث استخدمنا مرة أخرى حقيقة كون كل من $|U|$ و $|A|$ عدداً زوجياً. وبهذا يختصر المقدار السابق إلى:

$$\sum_{y\epsilon V} y^3 + \sum_{y\epsilon B} y^3 = \sum_{y\epsilon V\Delta B} y^3$$ ■

على الرغم من أن الشفرة $P(r)$ ليست خطيّة، إلاّ أنها تشترك مع الشفرات الخطيّة ببعض الخصائص.

تعريف (٩,٣,٦)

نقول عن شفرة C إنها **لا متغيرة المسافة (Distance Invariant)** إذا حققت ما يلي:

لكل $c_1, c_2 \epsilon C$، عدد كلمات الشفرة التي تبعد مسافة i ، $1 \le i \le n$، عن c_1 يساوي عدد كلمات الشفرة التي تبعد مسافة i، عن c_2.

من التعريف (٩,٣,٦)، نرى أن مسافة شفرة لا متغيرة المسافة وتحتوي الكلمة الصفرية هي أصغر أوزان كلمات الشفرة غير الصفرية. أي أن:

$$d(C) = min\{wt(c): 0 \neq c\epsilon C\}.$$

نتيجة (٩,٣,٧)

$P(r)$ شفرة لا متغيرة المسافة.

البرهان

لنفرض أن $[\chi(U), \chi(V)]$ و $[\chi(A), \chi(B)]$ كلمتا شفرة تنتميان إلى $P(r)$ حيث المسافة بينهما تساوي i. استناداً إلى التمهيدية (٩,٣,٥) نرى أن كلاً من $[\chi(U\Delta U + \alpha), \chi(V\Delta V)]$ و $[\chi(U\Delta A + \alpha), \chi(V\Delta B)]$ كلمة شفرة وأنه ليس صعباً أن نرى أن المسافة بينهما تساوي i. بما أن $U\Delta U = \phi$ فنجد أن $[\chi(U\Delta U + \alpha), \chi(V\Delta V)]$ هي الكلمة الصفرية. وبهذا يكون وزن الكلمة $[\chi(U\Delta A + \alpha), \chi(V\Delta B)]$ يساوي i. ■

تقدم التمهيدية التالية بعض خصائص الشفرة $P(r)$ وبرهان هذه الخصائص يشبه البرهان المقدم في التمهيدية (**٩,٣,٥**)، ولذا نتركه للقارئ.

تمهيدية (٩,٣,٨)

لنفرض أن $[\chi(U),\chi(V)]\epsilon P(r)$. عندئذ، جميع كلمات الشفرة التالية تنتمي إلى $P(r)$:

(i) $[\chi(V),\chi(U)]$.

(ii) $[\chi(U+\alpha),\chi(V+\alpha)]$ لكل $\alpha\epsilon GF(2^r)$.

(iii) $[\chi(\alpha U),\chi(\alpha V)]$ لكل $\alpha\epsilon GF(2^r) \neq 0$.

مثال (٩,٣,٩)

إذا كانت $U=\{\beta,\beta^2,\beta^5,0\}$ و $V=\{\beta^0,\beta,\beta^2,\beta^3,\beta^6,0\}$ فقد وجدنا في المثال (**٩,٣,٤**) أن $[\chi(U),\chi(V)]\epsilon P(3)$. وباستخدام التمهيدية (**٩,٣,٨**) حيث $\alpha=\beta^3$ نرى أن الكلمات التالية هي كلمات شفرة:

(i) $[\chi(V),\chi(U)] = 11110011\ \ 01100101$

(ii) $[\chi(U+\alpha),\chi(V+\alpha)] = [\chi(\{\beta^0,\beta^5,\beta^2,\beta^3\}),\chi(\{\beta,\beta^0,\beta^5,0,\beta^4,\beta^3\})]$
$= 10110100\ \ 11011101$

(iii) $[\chi(\alpha U),X(\alpha V)] = [\chi(\{\beta^4,\beta^5,\beta,0\}),\chi(\{\beta^3,\beta^4,\beta^5,\beta^6,\beta^2,0\})]$
$= 01001101\ \ 00111111$ ▲

تمارين

(**٩,٣,١٠**) طبّق التمهيدية (**٩,٣,٨**) على كلمة الشفرة $[\chi(U),\chi(V)]$ المعرّفة في المثال (**٩,٣,٩**) في الحالات التالية:

(أ) $\alpha=\beta^0$ (ب) $\alpha=\beta$ (ج) $\alpha=\beta^6$.

(**٩,٣,١١**) إذا كان $\alpha=0$ فبيّن أن الكلمة $[\chi(\alpha U),\chi(\alpha V)]$ ليست كلمة شفرة (استُثنيت هذه الحالة في التمهيدية (**٩,٣,٨**)).

(**٩,٣,١٢**) أثبت أن الكلمات التي كوّناها في المثال (**٩,٣,٩**) تحقق التعريف (**٩,٣,٦**).

من الممكن استخدام التمهيدية (**٩,٣,٨**) لتبسيط مسألة إيجاد مسافة الشفرة $P(r)$ ولكن قبل ذلك نقدم التمهيدية التالية التي توضح السبب وراء كون العدد r فردياً.

تمهيدية (٩,٣,١٣)

إذا كان $\beta \epsilon GF(2^r)$ عنصراً بدائياً فإن β^3 عنصر بدائي عندما يكون r فردياً ولكنه ليس عنصراً بدائياً عندما يكون r زوجياً.

البرهان

لاحظ أن β^i عنصر بدائي إذا وفقط إذا كان $gcd(i, 2^r - 1) = 1$ (انظر التمرين (**٥,١,١٨**)).

من السهل أن نبرهن بالاستقراء الرياضي أن:

$$2^r - 1 \equiv \begin{cases} 1(mod\ 3) & ,r \text{ فردي} \\ 0(mod\ 3) & ,r \text{ زوجي} \end{cases}.$$

أي أن:

$$2^r - 1 \equiv \begin{cases} 3x + 1 & ,r \text{ فردي} \\ 3x & ,r \text{ زوجي} \end{cases}.$$

وبهذا نرى أن β^3 عنصر بدائي عندما يكون r فردياً ولكنه ليس عنصراً بدائياً عندما يكون r زوجياً. ■

نتيجة (٩,٣,١٤)

إذا كان r عدداً فردياً فلكل عنصر $x \epsilon GF(2^r) \neq 0$ يوجد عنصر وحيد y (الجذر التكعيبي للعنصر x) يحقق $y^3 = x$.

مبرهنة (٩,٣,١٥)

مسافة الشفرة $P(r)$ تساوي 6.

البرهان

بما أن $P(r)$ شفرة لا متغيرة المسافة فنرى أنها تحتوي على كلمة شفرة وزنها d ولتكن كلمة الشفرة هذه هي $[\chi(U),\chi(V)]$. عندئذ،

$$.d = wt\left(\chi(U)\right) + wt\left(\chi(V)\right) = |U| + |V|$$

واستناداً إلى الفقرة (i) من التعريف (**٩,٣,٣**) نرى أن d عدد زوجي. وبهذا يكفي أن نبرهن أن $d \neq 2$ ، $d \neq 4$ وأن $P(r)$ تحتوي على كلمة وزنها 6.

لنفرض أن $d = 2$. عندئذ، استناداً إلى التمهيدية (**٩,٣,٨**) (i)، من الممكن افتراض أن $|U| = 2$ وأن $|V| = 0$. واستناداً إلى التمهيدية (**٩,٣,٨**) (ii)، من الممكن افتراض أن $U = \{0, x\}$ حيث $x \epsilon K^r \neq 0$. وبهذا نرى أن $\sum_{u \epsilon U} u = 0 + x = x$ وهذا يناقض الشرط (ii) من التعريف (**٩,٣,٣**) لأن $V = \phi$.

لنفرض الآن أن $d = 4$. مرة أخرى باستخدام الفقرة (i) من التمهيدية (**٩,٣,٨**) نستطيع افتراض أن ($|U| = 4$ و $|V| = 0$) أو ($|U| = |V| = 2$).

إذا كان $|U| = 4$ و $|V| = 0$ فنرى استناداً إلى الفقرة (ii) من التمهيدية (**٩,٣,٨**) أن $U = \{0, x, y, z\}$ حيث x ، y ، z عناصر غير صفرية مختلفة تنتمي إلى K^4. عندئذ، نجد باستخدام الشرط (iii) من التعريف (**٩,٣,٣**) أن:

$$0^3 + x^3 + y^3 + z^3 + (0 + x + y + z)^3 = 0$$

ومن ذلك يكون $(x + y)(x + z)(y + z) = 0$ وهذا مستحيل لأن x ، y ، z عناصر غير صفرية مختلفة.

وإذا كان $|U| = |V| = 2$ فنستطيع أن نفرض أن $U = \{0, x\}$ ، $V = \{y, z\}$ حيث $y \neq z$. وبتطبيق الشرط (iii) من التعريف (**٩,٣,٣**) نحصل على:

$$0^3 + x^3 + (0 + x)^3 = y^3 + z^3$$

ولكن إذا كان $y^3 = z^3$ فنرى باستخدام النتيجة (**٩,٣,١٤**) أن $y = z$ وهذا تناقض. نجد الآن كلمة شفرة طولها 6. لتكن x ، y ، z عناصر غير صفرية مختلفة من K^r، نفرض أن $w \epsilon K^r$ هو العنصر الوحيد الذي يحقق $w^3 = x^3 + y^3 + z^3$ (استخدمنا النتيجة (**٩,٣,١٤**)). بوضع $u = w + x + y + z$ نرى أن w لا يساوي أياً من x أو y أو z (إذا كان $w = x$ على سبيل المثال، فيكون $w^3 = x^3$ ومن ثم $y^3 + z^3 = 0$ وبهذا نحصل على التناقض $y = z$) وأن $u \neq 0$ (لأن $w^3 + (x + y + z) = (x + y)(x + z)(y + z) \neq 0$ ومن ثم فإن $w \neq x + y + z$). الآن نفرض أن $U = \{0, u\}$ وأن $V = \{w, x, y, z\}$. بما أن $u \neq 0$ وأن $w \neq x \neq y \neq z$ فنرى أن $[\chi(U), \chi(V)]$ كلمة وزنها 6 ومن السهل أن نرى أنها كلمة من كلمات الشفرة $P(r)$. ■

مثال (٩,٣,١٦)

لنفرض أن K^3 هو الحقل المقدم في المثال (**٩,٣,٤**). باستخدام ترميز المبرهنة (**٩,٣,١٥**)، نفرض أن x ، y ، z عناصر غير صفرية مختلفة في الحقل، ولتكن $x = \beta$ ، $y = \beta^3$ ، $z = \beta^5$.

عندئذ،

$$\begin{aligned} w^3 = x^3 + y^3 + z^3 &= \beta^3 + \beta^9 + \beta^{15} \\ &= 100 + 001 + 100 \\ &= \beta^4 \\ &= \beta^{18} \qquad (\text{لأن } \beta^7 = 1) \\ &= (\beta^6)^3 \end{aligned}$$

إذن، $w = \beta^6$. الآن، بوضع :

$$u = w + x + y + z = \beta^6 + \beta + \beta^4 + \beta^5 = \beta^4$$

وفرض أن $U = \{0, u\} = \{0, \beta^4\}$ وأن $V = \{w, x, y, z\} = \{\beta^6, \beta, \beta^3, \beta^5\}$ نجد أن $[\chi(U), \chi(V)] = 00001001\ 01010110$ كلمة شفرة تنتمي إلى $P(3)$ وزنها 6. ▲

تمرين

(**٩,٣,١٧**) إذا كان K^3 هو الحقل المنشأ باستخدام $1 + \beta + \beta^3 = 0$ وإذا كانت $x, y, z \epsilon K^3$ هي العناصر المبيّنة في الفقرات التالية فعرِّف w و u كما في المبرهنة (**٩,٣,١٥**) لإنشاء كلمة شفرة وزنها 6 تنتمي إلى $P(3)$.

(أ) $x = \beta$ ، $y = \beta^2$ ، $z = \beta^3$.

(ب) $x = \beta$ ، $y = \beta^4$ ، $z = \beta^6$.

(ج) $x = \beta^0$ ، $y = \beta^3$ ، $z = \beta^6$.

مبرهنة (٩,٣,١٨)

$P(r)$ ليست شفرة خطيّة.

البرهان

لاحظنا في بداية هذا البند أن:

$$[\chi(U), \chi(V)] + [\chi(A), \chi(B)] = [\chi(U \Delta A), \chi(V \Delta B)]$$

وباستخدام المبرهنة (**٩,٣,١٥**) نستطيع انشاء كلمتي شفرة:

$$[\chi(U), \chi(V)], [\chi(A), \chi(B)] \epsilon P(r)$$

حيث $U = \{0, u_1\}$ ، $V = \{x_1, y_1, z_1, w_1\}$ ، $A = \{0, u_2\}$ ، $B = \{x_2, y_2, z_2, w_2\}$. عندئذ، نرى استناداً إلى التمهيدية (**٩,٣,٥**) أن $c = [\chi(U \Delta A + u_1), \chi(V \Delta B)]$ كلمة شفرة تنتمي إلى $P(r)$. بما أن $|U \Delta A + u_1| \leq 2$ وبما أن المسافة بين c و $[\chi(U \Delta A + u_1), \chi(V \Delta B)]$ هي على الأكثر $2|U \Delta B + u_1| \leq 4$ وأن مسافة الشفرة $P(r)$ تساوي 6 نخلص إلى أن الكلمة $[\chi(U), \chi(V)] + [\chi(A), \chi(B)]$ ليست كلمة شفرة من كلمات $P(r)$. إذن، $P(r)$ شفرة غير خطيّة. ■

الآن، $P(r)$ غير خطيّة، ولذا لا يوجد لها بُعد. كما أننا لا نعرف لحد الآن عدد كلمات الشفرة $P(r)$ ولكننا سنحصل على هذا العدد كنتيجة لعملية التشفير.

(٩,٤) تشفير شفرات بريبراتا الممتدة

Encoding Extended Preparata Codes

رأينا في البند (٥,٤) أن $g(x) = m_\beta(x)m_{\beta^3}(x)$ مولّد لشفرة BCH التي تُصوّب خطأين حيث مصفوفة اختبار النوعية هي:

$$H = \begin{bmatrix} \beta^0 & \beta^0 \\ \beta^1 & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \\ \beta^{2^m-2} & \beta^{3(2^m-2)} \end{bmatrix} \qquad (٩,١)$$

وحيث β عنصر بدائي في الحقل $GF(2^r)$. تذكر أيضاً أن $deg(g(x)) = 2r$. وبما أن $g(x)$ كلمة شفرة غير صفرية وزنها أصغري فنرى عدم وجود تركيب خطي من أول $2r$ من صفوف المصفوفة (٩,١) بحيث يساوي صفراً. في الحقيقة، بما أن $g(x)$ تولّد شفرة دورية فإن أي مصفوفة جزئية مكوّنة من $2r$ من الصفوف المتتالية من المصفوفة H تكون صفوفها مُستقلة خطياً ومن ثم يوجد لها معكوس. لنفرض أن A هي المصفوفة الجزئية من H المكوّنة من الصفوف $2r$ الأخيرة (السفلى) ولنفرض أن H' هي المصفوفة الجزئية من H التي نحصل عليها بحذف الصفوف $2r$ الأخيرة.

مثال (٩,٤,١)

ليكن K^3 هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. عندئذ، يكون:

$$A = \begin{bmatrix} 010 & 110 \\ 001 & 101 \\ 110 & 001 \\ 011 & 111 \\ 111 & 010 \\ 101 & 011 \end{bmatrix} \leftrightarrow \begin{bmatrix} \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^2 \\ \beta^6 & \beta^5 \\ \beta^5 & \beta^1 \\ \beta^6 & \beta^4 \end{bmatrix} \text{ و } A^{-1} = \begin{bmatrix} 001 & 011 \\ 111 & 010 \\ 011 & 101 \\ 110 & 100 \\ 101 & 110 \\ 111 & 001 \end{bmatrix}.$$

وإذا استخدمنا $1 + x^2 + x^5$ لإنشاء K^5 (انظر المثال (**٥,١,١٥**)) نرى أن:

$$A = \begin{bmatrix} 00111 & 00010 \\ 00011 & 10001 \\ 10011 & 00011 \\ 11011 & 01010 \\ 01101 & 10101 \\ 10101 & 11001 \\ 00110 & 11111 \\ 11001 & 01110 \\ 11000 & 00111 \\ 10001 & 10100 \end{bmatrix} \text{ و } A^{-1} = \begin{bmatrix} 00011 & 01000 \\ 10101 & 00001 \\ 11110 & 00101 \\ 01111 & 10001 \\ 10011 & 00111 \\ 11101 & 11011 \\ 11010 & 01100 \\ 01101 & 10101 \\ 10010 & 10011 \\ 01001 & 01101 \end{bmatrix} \leftrightarrow \begin{bmatrix} \beta^{21} & \beta^{63} \\ \beta^{22} & \beta^{66} \\ \vdots & \vdots \\ \beta^{30} & \beta^{90} \end{bmatrix}$$

▲

لنفرض أن $m = m_L, m_R$ أي كلمة ثنائية من الطول $2^{r+1} - 2r - 2$ حيث m_L كلمة ثنائية طولها $2^r - 2r - 1$ و m_R كلمة ثنائية طولها $2^r - 2r - 1$. عندئذ، بتمثيل m_L و m_R باستخدام كثيرات الحدود نرى أن:

$$[m_L(\beta), m_L(\beta^3)] \leftrightarrow m_L H$$
$$[m_R(\beta), m_R(\beta^3)] \leftrightarrow m_R H$$

نعرّف الآن:

$$v_R = [m_L(\beta) + m_R(\beta), m_L(\beta^3) + \big(m_L(\beta)\big)^3 + m_R(\beta^3)]A^{-1}.$$

مبرهنة (٩,٤,٢)

لنفرض أن r عدد فردي ولنفرض أن m أي كلمة ثنائية من الطول $2^{r+1} - 2r - 2$. إذا كان $\chi(U) = [m_L, p_L]$ و $\chi(V) = [m_R, v_R, p_R]$ حيث p_L و p_R إحداثي اختبار نوعية لكل من m_L و $[m_R, v_R]$ على التوالي فإن $[\chi(U), \chi(V)] \epsilon P(r)$.

البرهان

$$\begin{aligned} [m_R, v_R]H &= [m_R]H' + [v_R]A \\ &= [m_R(\beta), m_R(\beta^3)] + [m_L(\beta) + m_R(\beta), m_L(\beta^3) + \big(m_L(\beta)\big)^3 + m_R(\beta^3)] \\ &= [m_L(\beta), m_L(\beta^3) + \big(m_L(\beta)\big)^3]. \end{aligned}$$

ولكن $[m_R, v_R]H = [\sum_{v \epsilon V} v, \sum_{v \epsilon V} v^3]$. وبالمثل، نرى أن $m_L(\beta) = \sum_{u \epsilon U} u$ وأن:

$$m_L(\beta^3) + \big(m_L(\beta)\big)^3 = \sum_{u \epsilon U} u^3 + \left(\sum_{u \epsilon U} u\right)^3$$

وبهذا يتحقق الشرطان (ii) و (iii) من التعريف (**٩,٣,٣**). ومن الواضح أن الشرطين (i) و (iv) محققان. إذن، $[\chi(U),\chi(V)]\epsilon P(r)$. ■

نتيجة (٩,٤,٣)

عدد كلمات الشفرة $P(r)$ يساوي $2^{2^{r+1}-2r-2}$.

البرهان

استناداً إلى المبرهنة (**٩,٤,٢**)، يوجد عدد $2^{2^{r+1}-2r-2}$ خياراً للكلمة m وكل منها يؤدي إلى كلمة شفرة مختلفة. بقية إحداثيات كلمة الشفرة التي تحتوي m تتحدد تماماً بالشروط (i) ، (ii) ، (iii) من التعريف (**٩,٣,٣**). ■

خوارزمية (٩,٤,٤) [تشفير $P(r)$]

لتكن m_L و m_R كلمتين من الطول 2^{r-1} و $2^r - r - 1$ على التوالي. ولتكن v_R معرفة كما في المبرهنة (**٩,٤,٢**). عندئذ، $[m_L, p_L, m_R, v_R, p_R]$ كلمة شفرة تقابل الرسالة $m = [m_L, m_R]$.

مثال (٩,٤,٥)

لنفرض أن $r = 3$ ، $m_L = 0110010$ ، $m_R = 1$. عندئذ،

$$m_L(\beta) = \beta + \beta^2 + \beta^5 = \beta^0, m_R(\beta) = \beta^0$$
$$m_L(\beta^3) = \beta^0 , m_L(\beta^3) = \beta^3 + \beta^6 + \beta^{15} = \beta^2$$
$$v_R = [\beta^0 + \beta^0, \beta^2 + \beta^2 + \beta^0 + \beta^0]A^{-1}$$
$$= [000,001]A^{-1} = 111001$$

حيث A^{-1} هي المصفوفة المقدمة في المثال (**٩,٤,١**). إذن، تُشفّر الرسالة $m = [0110010\ ,1]$ إلى كلمة الشفرة $c = [m_L, p_L, m_R, v_R, p_R] = [0110010\ ,1\ ,1\ ,111001\ ,1]$. وباستخدام ترميز البند (**٩,١**) تكون $\left[\chi(U),\chi(V)\right]$ = c حيث $\chi(U) = 01100101$ و $\chi(V) = 11110011$. هذه هي كلمة الشفرة من $P(3)$ المبيّنة في المثال (**٩,٣,٤**). ▲

تمارين

(**٩,٤,٦**) إذا كان K^3 هو الحقل المنشأ باستخدام $1 + x + x^3$ وكانت A^{-1} هي المصفوفة المبيّنة في المثال (**٩,٤,١**) فاستخدم $P(3)$ لتشفير كل من الرسائل التالية:

(أ) $m_L = 1010100$ و $m_R = 1$.

(ب) $m_L = 1010100$ و $m_R = 0$.

(ج) $m_L = 1111111$ و $m_R = 1$.

(د) $m_L = 1111111$ و $m_R = 0$.

(هـ) $m_L = 0000000$ و $m_R = 1$.

(**٩,٤,٧**) إذا كان K^5 هو الحقل المنشأ باستخدام $1 + x^2 + x^5$ وكانت A^{-1} هي المصفوفة المبيّنة في المثال (**٩,٤,١**) فاستخدم $P(5)$ لتشفير كل من الرسائل التالية:

(أ) $m_L = 10100 \cdots 0$ و $m_R = 000001000100 \cdots 0$.

(ب) $m_L = 10100 \cdots 0$ و $m_R = 00 \cdots 0$.

(ج) $m_L = 10100 \cdots 0$ و $m_R = 11110 \cdots 0$.

(د) $m_L = 00 \cdots 0$ و $m_R = 100 \cdots 0$.

(**٩,٤,٨**) جد طول كل من (أ) m_L و (ب) m_R المعطاة في التمرين (**٩,٤,٧**).

(**٩,٥**) فك تشفير شفرات بريبراتا الممتدة

Decoding Extended Preparata Codes

وجدنا أن مسافة الشفرة $P(r)$ تساوي 6 (مبرهنة (**٩,٣,١٥**))، وبهذا نحتاج إلى خوارزمية تُصوّب خطأين على الأكثر. لنفرض أن w هي الكلمة المستقبلة ولنفرض أن $w = [m_L, p_L, w_R, p_R]$ حيث كل من w_L و w_R كلمة من الطول $2^r - 1$ وأن كلاً من p_L و p_R إحداثي اختبار النوعية. عندئذ، نقوم بحساب $w_L H = [w_L(\beta), w_L(\beta^3)]$ و $w_R H = [w_R(\beta), w_R(\beta^3)]$.

ندرس الحالات التالية اعتماداً على أماكن وقوع الأخطاء:

(١) إذا اقتصر وقوع الأخطاء على إحداثيي اختبار النوعية فنرى استناداً إلى الشرطين (ii) و (iii) من التعريف (**٩,٣,٣**) أن:

$$w_L(\beta) = w_R(\beta)$$

$$w_L(\beta^3) + \big(w_L(\beta)\big)^3 = w_R(\beta^3).$$

(٢) إذا كانت w_L خالية من الأخطاء ووجد خطأ واحد في الموقع i من w_R وعلى الأكثر خطأ واحد في إحداثيي اختبار النوعية فنرى أن:

$$w_L(\beta) = w_R(\beta) + \beta^i$$

$$w_L(\beta^3) + \big(w_L(\beta)\big)^3 = w_R(\beta^3) + \beta^{3i}$$

$$\text{إذن، } \big(w_L(\beta) + w_R(\beta)\big)^3 = w_L(\beta^3) + \big(w_L(\beta)\big)^3 + w_R(\beta^3)$$

(استناداً إلى الشرطين (ii) و (iii) من التعريف (**٩,٣,٣**)). إذا تحققت المساواة الأخيرة فنكتب $\beta^i = w_L(\beta) + w_R(\beta)$ ونقوم بتغيير الإحداثي i من w_R وعلى الأكثر إحداثي اختبار نوعية واحد.

(٣) إذا كانت w_R خالية من الأخطاء ووجد خطأ واحد في الموقع i من w_L وعلى الأكثر خطأ واحد في مرتبتي اختبار النوعية فنرى اعتماداً على الفقرة (i) من التمهيدية (**٩,٣,٨**) أن بإمكاننا تكرار الخطوة (٢) لنجد:

$$\big(w_R(\beta) + w_L(\beta)\big)^3 = \big(w_R(\beta^3) + w_R(\beta)\big)^3 + w_L(\beta^3).$$

وفي هذه الحالة نضع $\beta^i = w_R(\beta) + w_L(\beta)$ ونقوم بتغيير الإحداثي i من w_L وعلى الأكثر إحداثي اختبار نوعية واحد.

(٤) إذا وقع خطآن في w_R، في الموقعين i و j فنجد باستخدام التعريف (**٩,٣,٣**) أن:

$$w_L(\beta) = w_R(\beta) + \beta^i + \beta^j$$

$$w_L(\beta^3) + \big(w_L(\beta)\big)^3 = w_R(\beta^3) + \beta^{3i} + \beta^{3j}.$$

وبهذا نستطيع معرفة $\beta^i + \beta^j$ و $\beta^{3i} + \beta^{3j}$. أما i و j فنستطيع ايجادهما الآن بالاسلوب المستخدم في الشفرة BCH التي تُصوّب أنماط أخطاء من النوع 2 (انظر البند **٩,٣,٨**).

(٥) إذا وقع خطآن في w_L فمن الممكن استخدام التمهيدية **٥,٥** (i) (كما في الحالة (٣)) ونقاش الخطوة (٤) لإيجاد مواقع الخطأين.

(٦) إذا وقع خطأ في w_L وخطأ في w_R في الموقعين i و j على التوالي فنجد استناداً إلى التعريف **٩,٣,٣** أن:

$$w_L(\beta) + \beta^i = w_R(\beta) + \beta^j$$
$$w_L(\beta^3) + \beta^{3i} + (w_L(\beta) + \beta^i)^3 = w_R(\beta^3) + \beta^{3j}$$

وبحل هاتين المعادلتين لإيجاد β^i و β^j نجد من المعادلة الأولى:

$$\beta^j = w_L(\beta) + \beta^i + w_R(\beta)$$

وبالتعويض في المعادلة الثانية نرى أن:

$$w_L(\beta^3) + \beta^{3i} + (w_L(\beta) + \beta^i)^3 = w_R(\beta^3) + (w_L(\beta) + \beta^i)^3 + (w_L(\beta) + \beta^i)^2 w_R(\beta) + (w_L(\beta) + \beta^i) w_R(\beta)^2 + w_R(\beta)^3$$

بالتبسيط نحصل على:

$$\beta^{3i} + \beta^{2i} w_R(\beta) + \beta^i \big(w_R(\beta)\big)^2 + \big(w_R(\beta)\big)^3 = w_L(\beta^3) + w_R(\beta^3) + w_L(\beta)^2 w_R(\beta) + w_L(\beta) w_R(\beta)^2$$

وبهذا نرى أن:

$$\big(\beta^i + w_R(\beta)\big)^3 = \big(w_L(\beta^3) + w_R(\beta^3)\big) + \big(w_L(\beta) + w_R(\beta)\big)^3 + w_L(\beta)^3 + w_R(\beta)^3 = \Delta$$

إذن:

$$\beta^i = w_R(\beta) + \Delta^{1/3}$$
$$.\beta^j = w_L(\beta) + \Delta^{1/3}$$

وبهذا نرى أن بالإمكان ايجاد جميع مواقع الأخطاء. تُسهّل علينا شروط اختبار النوعية على كل من نصفي w في اختيار الحالة التي تطبق على w. وبهذا نحصل على خوارزمية فك التشفير التالية حيث خطواتها تقابل الحالات التي درسناها في هذا البند.

خوارزمية (٩,٥,١) [فك تشفير $P(r)$]

لتكن $w = [m_L, p_L, w_R, p_R]$ كلمة مستقبلة.

(٠) احسب $L_1 = w_L(\beta)$ ، $L_3 = w_L(\beta^3)$ ، $R_1 = w_R(\beta)$ ، $R_3 = w_R(\beta^3)$.

(١) إذا كان $L_1 + R_1 = 0$ و $L_3 + L_1^3 + R_3 = 0$ فتقع الأخطاء فقط في إحداثيي اختبار النوعية.

(٢) إذا كان $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = 0$ فضع $\beta^i = L_1 + R_1$. صوّب الموقع i من w_R وإحداثي اختبار نوعية واحدة على الأكثر. اطلب إعادة ارسال إذا احتجت إلى تغيير إحداثيي اختبار النوعية.

(٣) إذا كان $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = 0$ فضع $\beta^i = L_1 + R_1$. صوّب الموقع i من w_L وإحداثي اختبار نوعية واحد على الأكثر. اطلب إعادة ارسال إذا احتجت إلى تغيير إحداثيي اختبار النوعية.

(٤) إذا كانت نوعية كل من نصفي w زوجية ووجد i و j بحيث يكون:

$$x^2 + (L_1 + R_1)x + \frac{L_3 + L_1^3 + R_3 + (L_1 + R_1)^3}{L_1 + R_1} = (x + \beta^i)(x + \beta^j)$$

فصوّب الموقعين i و j من w_L.

(٥) إذا كانت نوعية كل من نصفي w زوجية ووجد i و j بحيث يكون:

$$x^2 + (L_1 + R_1)x + \frac{R_3 + R_1^3 + L_3 + (L_1 + R_1)^3}{L_1 + R_1} = (x + \beta^i)(x + \beta^j)$$

فصوّب الموقعين i و j من w_R.

(٦) إذا كانت نوعية كل من نصفي w فردية فضع :

$$\beta^i = R_1 + (L_1^3 + R_1^3 + (L_1 + R_1)^3 + L_3 + R_3)^{1/3}$$

$$.\beta^j = L_1 + (L_1^3 + R_1^3 + (L_1 + R_1)^3 + L_3 + R_3)^{1/3}$$

صوّب الموقع i من w_L والموقع j من w_R.

(٧) إذا لم تحصل على كلمة شفرة هي الأقرب فاستنتج وقوع على الأقل ثلاثة أخطاء أثناء الإرسال واطلب إعادة إرسال.

مثال (٩,٥,٢)

فك تشفير كل من الكلمات المستقبلة التالية إذا علمت أنها شُفّرت باستخدام الشفرة $P(3)$، علماً بأنه قد تم إنشاء الحقل $GF(2^3)$ باستخدام $1 + x + x^3$.

(أ) 10010011 11100111.

(ب) 10100100 10001001.

(ج) 10001000 11101001.

الحل

فك تشفير (أ) :

(٠) $[L_1, L_3] = w_L H = [111,110]$ و $[R_1, R_3] = w_R H = [101,110]$.

(١) $L_1 + R_1 = 111 + 101 = \beta \neq 0$.

(٢) $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^3 + \beta^3 + \beta^{15} + \beta^3 = \beta^0 \neq 0$.

(٣) $(L_1 + R_1)^3 + R_3 + R_1^3 + L_1 = \beta^3 + \beta^3 + \beta^{18} + \beta^3 = \beta^6 \neq 0$.

(٤) $x^2 + \beta x + \frac{\beta^3 + \beta^{15} + \beta^3 + \beta^3 + \beta^3}{\beta} = x^2 + \beta x + \beta^6 = (x + \beta^2)(x + \beta^4)$

فك تشفير w إلى 10010011 11001111.

فك تشفير (ب) :

(٠) $[L_1, L_3] = w_L H = [010,011]$ و $[R_1, R_3] = w_R H = [111,011]$.

(١) $L_1 + R_1 = 010 + 111 = \beta^6 \neq 0$.

(٢) $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^{18} + \beta^4 + \beta^3 + \beta^4 = \beta^6 \neq 0$.

(٣) $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = \beta^{18} + \beta^4 + \beta^{15} + \beta^4 = \beta^2 \neq 0$.

(٤) و (٥) نوعية كل من نصفي w فردية.

(٦)
$$\begin{aligned}\beta^i &= \beta^5 + (\beta^3 + \beta^{15} + \beta^{18} + \beta^4 + \beta^4)^{1/3} \\ &= \beta^5 + (\beta^5)^{1/3} \\ &= \beta^5 + (\beta^{12})^{1/3} \\ &= \beta^5 + \beta^4 \\ &= \beta^0\end{aligned}$$

إذن، $i = 0$ ونضع مباشرة:

$$\beta^j = \beta + \beta^4 = \beta^2.$$

إذن، $j = 2$ ويكون فك تشفير w هو 10101001 00100100.

فك تشفير (ج):

(٠) $[L_1, L_3] = w_L H = [111,011]$ و $[R_1, R_3] = w_R H = [100,000]$.

(١) $L_1 + R_1 = 11 + 100 = \beta^4 \neq 0$.

(٢) $(L_1 + R_1)^3 + L_3 + L_1^3 + R_3 = \beta^{12} + \beta^4 + \beta^{15} + 0 = \beta^3 \neq 0$.

(٣) $(L_1 + R_1)^3 + R_3 + R_1^3 + L_3 = \beta^{12} + 0 + \beta^0 + \beta^4 = \beta^2 = 0$.

ضع $\beta^i = L_1 + R_1 = \beta^4$. ولذا $i = 4$. ولكن تغيير الموقع 4 من w_L يتطلب تغيير إحداثيي اختبار النوعية. وبهذا نطلب اعادة ارسال لأننا نستطيع إيجاد كلمة شفرة تبعد مسافة 3 عن الكلمة w. ▲

تمارين

(**٩,٥,٣**) فك تشفير كل من الكلمات المستقبلة التالية التي تم تشفيرها باستخدام $P(3)$ علماً بأنه استخدمت $1 + x + x^3$ لانشاء $GF(2^3)$.

(أ) 10000001, 11101000 (ب) 00011010, 01000010

(ج) 00100101, 10100100 (د) 01010110, 00011110

(هـ) 11101000, 10001001 (و) 10011001, 01010101

(ز) 01000111, 11001000 (ح) 10101101, 11010000

(ط) 11101110, 01010101 (ي) 10111011, 01101010

(ك) 01011101, 11101101 (ل) 10011100, 10100100

(م) 01101101, 10011000 (ن) 10101010, 10111011

(س) 10100101, 00010001

(**٩,٥,٤**) فك تشفير كل من الكلمات المستقبلة التالية التي تم تشفيرها باستخدام $P(5)$ علماً بأنه استخدمت $1 + x^2 + x^5$ لإنشاء الحقل $GF(2^5)$ (انظر التمرين (**٥,١,١٥**)).

(أ) 11000 11000 10000 00000 00000 10000 10, 00011 11000 00000 00000 00011 00100 00

(ب) 10100 00000 10000 00000 00000 00000 00, 00000 10001 00000 00100 01010 10111 00

(**٩,٥,٥**) لنفرض أن w هي كلمة مستقبلة بحيث إن نوعية نصفها الأيسر فردية ونوعية نصفها الأيمن زوجية. هل من الممكن استخدام الخطوة (٢) من الخوارزمية (**٩,٥,١**) لفك تشفير w إلى كلمة شفرة تبعد مسافة 2 عن w ؟