الفصل السادس

شفرات ريد وسولومن
Reed-Solomon Codes

شفرات على $GF(2^r)$ $(٦,١)$
Codes Over $GF(2^r)$

شفرات ريد وسولومن هي بلا شك أكثر الشفرات استخداماً في التطبيقات العملية، فهي التي تستخدم حالياً من قبل وكالة الفضاء الأمريكية (NASA) ووكالة الفضاء الأوروبية. كما أن الشفرات التي يتم اختيارها لاستخدامها على الأقراص الممغنطة تنتمي إلى عائلة شفرات ريد وسولومن.

درسنا في البند السابق بالتفصيل شفرات BCH الثنائية التي تصوّب خطأين. في الحقيقة شفرات ريد وسولومن هي شفرات BCH ولكنها ليست ثنائية. قد يبدو هذا غريباً للوهلة الأولى حيث عمليات الإرسال تتم عبر قنوات اتصال ثنائية. سنُبيّن في وقت لاحق أن لهذه الشفرات تمثيلاً ثنائياً.

لنفرض أن $GF(2^r)[x]$ هي مجموعة جميع كثيرات الحدود التي معاملاتها تنتمي إلى الحقل $GF(2^r)$. لاحظ أن هذه المجموعة تحتوي مجموعة كثيرات الحدود ذات المعاملات الثنائية $K[x]$ حيث $K = GF(2) = \{0,1\}$. إذا كانت C شفرة خطية على

$GF(2^r)$ من الطول n وكانت $c\epsilon C$ فسوف نطابق c مع كثيرة حدود $c(x)\epsilon GF(2^r)[x]$ حيث $deg(c(x)) < n$.

لقد سبق وعرفنا الشفرات الدورية من الطول n بدلالة جذور كثيرات الحدود المقابلة. على سبيل المثال، عرفنا شفرة BCH من الطول $n = 2^r - 1$ التي تصوّب خطأين على النحو التالي: $c(x)\epsilon C_K$ إذا وفقط إذا كانت $\beta^1, \beta^2, \beta^3, \beta^4$ هي جميع جذور كثيرة الحدود $c(x)$ حيث $c(x)\epsilon K[x]$ و $deg(c(x)) < n$ و β عنصر بدائي في الحقل $GF(2^r)$. وفي هذه الحالة تكون $g_K(x) = m_1(x)m_3(x)$ هي كثيرة الحدود المولّدة لهذه الشفرة الدورية وتكون $c(x)\epsilon C_K$ إذا وفقط إذا كان $c(x) = a(x)g_K(x)$.

من الممكن تعميم هذه الشفرة إلى شفرة على الحقل $GF(2^r)$ بأخذ $c(x)\epsilon GF(2^r)[x]$ عوضاً عن $c(x)\epsilon K[x]$. وبهذا يكون $c(x)\epsilon C$ إذا وفقط إذا كانت $\{\beta^1, \beta^2, \beta^3, \beta^4\}$ هي جميع جذور $c(x)$. ولكون $x + \beta$ ، $x + \beta^2$ ، $x + \beta^3$ ، $x + \beta^4$ هي كثيرات حدود تنتمي إلى $GF(2^r)[x]$ نرى أن $c(x)\epsilon C$ إذا وفقط إذا كانت كثيرة الحدود $c(x)$ تقسم كثيرة الحدود $g(x) = (x + \beta)(x + \beta^2)(x + \beta^3)(x + \beta^4)$.

الشفرة الثنائية C_K المعرّفة في الفقرة الثانية من هذه الصفحة هي شفرة BCH وأما الشفرة C على الحقل $GF(2^r)$ فهي إحدى شفرات ريد وسولومن. لاحظ أن C_K شفرة جزئية من C. بصورة عامة، الشفرة C_K هي شفرة على **حقل جزئي وشفرة جزئية (Subfield Subcode)** من C ؛ لأن $C_K \subseteq C$ وجميع إحداثيات كلمات الشفرة C_K تنتمي إلى الحقل الجزئي K من $GF(2^r)$. أي أن $C_K = C \cap K^n$.

كل من الشفرتين C_K و C دورية ؛ لأنه إذا كانت $c(x)\epsilon C$ فنجد أن $c(x) \equiv xc(x)(mod 1 + x^n)\epsilon C$، وذلك باستخدام خوارزمية القسمة وكون β^i جذراً لكل من $1 + x^n$ و $xc(x)$. في الحقيقة، ليس بالأمر الصعب إثبات أنه إذا كانت $g(x)$

كثيرة حدود مولّدة لشفرة خطية دورية من الطول $2^r - 1$ على الحقل $GF(2^r)$ فنرى أن كثيرة الحدود $g_K(x)$ المولِّدة للشفرة الجزئية الثنائية التي هي شفرة على الحقل الجزئي، هي كثيرة الحدود التي مجموع جذورها هي أصغر مجموعة R تحقق:

(أ) $g(\alpha) = 0 \Rightarrow \alpha \epsilon R$ (ب) $\alpha \epsilon R \Rightarrow \alpha^2 \epsilon R$.

مما سبق نحصل على المبرهنة التالية:

مبرهنة (٦,١,١)

إذا كانت $\alpha_1, \alpha_2, \cdots, \alpha_t$ عناصر غير صفرية مختلفة في الحقل $GF(2^r)$ فإن $g(x) = (\alpha_1 + x)(\alpha_2 + x) \cdots (\alpha_t + x)$ تولّد شفرة خطية دورية من الطول $2^r - 1$ على الحقل $GF(2^r)$.

مثال (٦,١,٢)

لنفرض أن $F = GF(2^4)$ الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (٥,١)). عندئذ، $g(x) = (\beta + x)(\beta^2 + x) = \beta^3 + \beta^5 x + x^2$ تولّد شفرة خطية دورية C من الطول 15 على الحقل F. كلمة الشفرة المقابلة لكثيرة الحدود $g(x)$ هي $\beta^3\beta^5 1000000000000$. أيضاً، $g_K(x) = 1 + x + x^4 \leftrightarrow 110010000000000$ تولّد الشفرة الدورية الثنائية التي هي شفرة على الحقل الجزئي وشفرة جزئية من الشفرة C. ولإثبات ذلك نجد مجموعة جذور R فنرى أن $\beta, \beta^2 \epsilon R$ (استناداً إلى (أ))، واستناداً إلى الفقرة (ب) نرى أن $(\beta^2)^2 = \beta^4 \epsilon R$ وأن $(\beta^4)^2 = \beta^8 \epsilon R$. إذن، $R = \{\beta, \beta^2, \beta^4, \beta^8\}$ وبهذا تكون $g_K(x) = (\beta^4 + x)(\beta^8 + x)g(x)$. ▲

نقدم فيما يلي بعض الخصائص الأساسية للشفرات الدورية على الحقل $GF(2^r)$.

مبرهنة (٦,١,٣)

لتكن C شفرة خطية دورية من الطول n على الحقل $GF(2^r)$. عندئذ، يمكن كتابة أي كلمة شفرة $c(x)$ بطريقة وحيدة كحاصل ضرب $m(x)g(x)$ حيث $m(x) \epsilon GF(2^r)[x]$

درجتها أصغر من $n - deg(g(x))$. أيضاً، $g(x)$ تقسم $f(x)$ إذا وفقط إذا كانت $f(x)$ كلمة شفرة و $g(x)$ تقسم $1 + x^n$.

نتيجة (٦,١,٤)

لتكن $g(x)$ كثيرة حدود درجتها $n - k$. إذا ولّدت $g(x)$ شفرة خطية دورية C على الحقل $GF(2^r)$ من الطول $n = 2^r - 1$ والبُعد k فإن:

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

مصفوفة مولّدة للشفرة C وعدد كلمات الشفرة C يساوي $(2^r)^k$.

ملحوظة

نحصل على $|C| = 2^{rk}$ من المبرهنة (٦,١,٣)؛ وذلك لأن جميع كثيرات الحدود $m(x)g(x)$ التي درجة كل منها أصغر من k تقابل كلمات شفرة مختلفة $m(x)\epsilon GF(2^r)[x]$. ولكن عدد كثيرات الحدود $m(x)$ يساوي 2^{rk}؛ لأن كلاً من معاملات $m(x)$ وعددها k هو أحد عناصر الحقل والتي عددها 2^r.

مثال (٦,١,٥)

لنفرض أن $GF(2^3)$ الحقل المنشأ باستخدام $1 + x + x^3$ وأن العنصر البدائي المستخدم هو β. ولنفرض أن $g(x) = (\beta + x)(\beta^2 + x) = \beta^3 + \beta^4 x + x^2$. حينئذ، $g(x)$ تولّد شفرة خطية دورية C على الحقل $GF(2^3)$ من الطول 7. مصفوفة مولّدة للشفرة C هي:

$$G = \begin{bmatrix} \beta^3 & \beta^4 & 1 & 0 & 0 & 0 & 0 \\ 0 & \beta^3 & \beta^4 & 1 & 0 & 0 & 0 \\ 0 & 0 & \beta^3 & \beta^4 & 1 & 0 & 0 \\ 0 & 0 & 0 & \beta^3 & \beta^4 & 1 & 0 \\ 0 & 0 & 0 & 0 & \beta^3 & \beta^4 & 1 \end{bmatrix}$$

عـدد كلمـات الشـفرة C يسـاوي 8^5. وكلمـة الشـفرة المقابلـة لكـثيرة الحـدود $m(x) = 1 + \beta x + \beta^3 x^4$ هي $m = 1\beta 00\beta^3$. فمثلاً،

$$m(x)g(x) \leftrightarrow mG = \beta^3 0 \beta^4 \beta \beta^6 1 \beta^3 .$$ ▲

تمارين

(**٦,١,٦**) ليكن $GF(2^3)$ الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. ولنفرض أن $g(x) = (1 + x)(\beta + x)$ تولّد الشفرة C من الطول 7 على الحقل $GF(2^3)$.

(أ) ما هو عدد كلمات الشفرة C ؟

(ب) استخدم النتيجة (**٦,١,٤**) لإنشاء مصفوفة مولّدة G للشفرة C.

(ج) استخدم G لتشفير كل من الرسائل التالية:

(i) $m(x) = 1 + \beta^6 x$.

(ii) $m(x) = \beta^4 x^4$.

(iii) $m(x) = 1 + x + x^2$.

(د) جد كثيرة حدود مولّدة $g_K(x)$ للشفرة الدورية الثنائية التي هي شفرة على حقل جزئي وشفرة جزئية.

(**٦,١,٧**) ليكن $GF(2^4)$ الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$. ولتكن $g(x) = (\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)$ كثيرة الحدود المولّدة للشفرة الخطية الدورية C على الحقل المنشأ $GF(2^4)$ من الطول 15.

(أ) ما هو عدد كلمات الشفرة C ؟

(ب) استخدم النتيجة (**٦,١,٤**) لإنشاء مصفوفة مولّدة G للشفرة C.

(ج) استخدم G لتشفير كل من الرسائل التالية:

(i) $m(x) = 1 + \beta^7 x^{10}$.

(ii) $m(x) = \beta^2 x + x^2$.

(iii) $m(x) = 1 + x + x^2$.

(د) جد كثيرة الحدود $g_K(x)$ المولّدة للشفرة الدورية الثنائية التي هي شفرة على حقل جزئي وشفرة جزئية. جد $m(x)$ التي تحقق $g_K(x) = m(x)g(x)$.

(٦,٢) شفرات ريد وسولومن
Reed-Solomon Codes

وجدنا في البند (٦,١) مولّدات للشفرة الخطية الدورية على الحقل $GF(2^r)$ ولكننا لم نتطرق إلى كفاءة هذه الشفرات لتصويب الأخطاء والتي ندرسها في هذا البند. كما أننا سنعرف شفرات ريد وسولومن وننوّه أن معظم النتائج التي نحصل عليها لهذه الشفرات يمكن استخدامها مباشرة لشفرات BCH ؛ لأن الأخيرة هي شفرة على حقل جزئي وشفرة جزئية. نبدأ بالتمهيدية التالية :

تمهيدية (٦,٢,١)

لنفرض أن $\alpha_1, \alpha_2, \cdots, \alpha_t$ عناصر غير صفرية في الحقل $GF(2^r)$. عندئذ ،

$$det\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{t-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_t & \alpha_t^2 & \cdots & \alpha_t^{t-1} \end{bmatrix} = \prod_{1 \le j < i \le t} (\alpha_i + \alpha_j)$$

البرهان

إذا وجد عنصران $\alpha_i = \alpha_j$ حيث $i \neq j$ فتحتوي المصفوفة على صفين متساويين وتكون قيمة المحدد تساوي صفراً. إذن، لكل $t \ge i > j \ge 1$ يكون $(\alpha_i + \alpha_j)$ قاسماً لقيمة المحدد وبهذا نرى أن $\prod_{1 \le j < i \le t}(\alpha_i + \alpha_j)$ يقسم قيمة المحدد.

ولكون كل من طرفي المعادلة هو كثيرة حدود في $\alpha_1, \cdots, \alpha_t$ ولهما الدرجة نفسها نجد أنهما يختلفان بقاسم مشترك واحد على الأكثر. هذا القاسم المشترك هو 1 حيث نرى ذلك بمقارنة معاملات $\prod_{i=1}^{t} \alpha_i^{i-1}$ في الطرفين. ■

مثال (٦,٢,٢)

باستخدام التمهيدية (٦,٢,١) والحقل $GF(2^r)$ المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (٥,١)) نجد أن:

$$det\begin{bmatrix} 1 & \beta^2 & \beta^4 \\ 1 & \beta^7 & \beta^{14} \\ 1 & \beta^{10} & \beta^5 \end{bmatrix} = (\beta^7 + \beta^2)(\beta^{10} + \beta^2)(\beta^{10} + \beta^7)$$
$$= \beta^{12} \cdot \beta^4 \cdot \beta^6$$
$$= \beta^7 \quad \blacktriangle$$

تمرين

(٦,٢,٣) استخدم التمهيدية (٦,٢,١) لإيجاد قيمة المحدد المُبيّن بافتراض أن β عنصر بدائي في الحقل $GF(2^4)$ المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (٥,١)).

(أ) $$.det\begin{bmatrix} 1 & \beta^2 & \beta^2 \\ 1 & \beta^4 & \beta^8 \\ 1 & \beta^7 & \beta^{14} \end{bmatrix}$$

(ب) $$.det\begin{bmatrix} 1 & \beta^2 & \beta^4 & \beta^6 \\ 1 & \beta^3 & \beta^6 & \beta^9 \\ 1 & \beta^5 & \beta^{10} & 1 \\ 1 & \beta^8 & \beta^1 & \beta^9 \end{bmatrix}$$

(ج) $$.det\begin{bmatrix} 1 & \beta^3 \\ 1 & \beta^7 \end{bmatrix}$$

المبرهنة التالية هي المبرهنة الرئيسة لشفرات BCH العامة ومع أن الصيغة المقدمة ليست الصيغة العامة إلا أنها تفي بالغرض عند تطبيقها على شفرات ريد وسولومن.

مبرهنة (٦,٢,٤)

لتكن $g(x) = (\beta^{m+1} + x)(\beta^{m+2} + x) \cdots (\beta^{m+\delta-1} + x)$ كثيرة الحدود المولّدة للشفرة الخطية الدورية C على الحقل $GF(2^r)$ من الطول $n = 2^r - 1$ حيث β عنصر بدائي في الحقل $GF(2^r)$ وحيث m عدد صحيح موجب. حينئذ، $d(C) \geq \delta$.

البرهان

بما أن β^{m+i} جذر لكثيرة الحدود $g(x)$ لكل $1 \le i \le \delta - 1$ نرى أن أعمدة المصفوفة:

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta^{m+1} & \beta^{m+2} & \cdots & \beta^{m+\delta-1} \\ (\beta^{m+1})^2 & (\beta^{m+2})^2 & \cdots & (\beta^{m+\delta-1})^2 \\ \vdots & \vdots & & \vdots \\ (\beta^{m+1})^{n-1} & (\beta^{m+2})^{n-1} & \cdots & (\beta^{m+\delta-1})^{n-1} \end{bmatrix}$$

تولّد $C^{\perp}$. لاحظ أن أي تركيب خطي لأي $\delta - 1$ من صفوف هذه المصفوفة لا يمكن أن يكون صفراً حيث يمكن التحقق من ذلك بايجاد قيمة محدد مصفوفة جزئية عدد صفوفها $\delta - 1$. على سبيل المثال:

$$det \begin{bmatrix} (\beta^{m+1})^{j_1} & \cdots & (\beta^{m+1})^{j_1} \\ (\beta^{m+1})^{j_2} & \cdots & (\beta^{m+1})^{j_2} \\ \vdots & & \vdots \\ (\beta^{m+1})^{j_{\delta-1}} & \cdots & (\beta^{m+1})^{j_{\delta-1}} \end{bmatrix}$$

$$= \beta^{(m+1)(j_1+j_1+\cdots+j_{\delta-1})} \begin{bmatrix} 1 & \beta^{j_1} & (\beta^{j_1})^{\delta-2} \\ 1 & \beta^{j_2} & (\beta^{j_2})^{\delta-2} \\ \vdots & & \\ 1 & \beta^{j_{\delta-1}} & (\beta^{j_{\delta-1}})^{\delta-2} \end{bmatrix}$$

$$= \beta^{(m+1)(j_1+j_1+\cdots+j_{\delta-1})} \prod_{1 \le y \le x \le \delta-1} (\beta^{j_x} + \beta^{j_y})$$

وقيمة هذا المحدد لا تساوي صفراً؛ لأن رتبة β تساوي $n = 2^r - 1$ وأن $1 \le j_1 < j_1 < \cdots < j_{\delta-1} \le n - 1$.

وبهذا نرى عدم وجود تركيب خطي من صفوف عددها أصغر من أو يساوي $\delta - 1$ قيمته تساوي صفراً. ومن ذلك نجد استناداً إلى المبرهنة (**٢,٩,١**) أن $d(c) \ge \delta$. وبملاحظة أن أعمدة H مُستقلة خطياً نخلص إلى أن H مصفوفة اختبار النوعية للشفرة C. ■

ملحوظة

تبقى المبرهنة صحيحة لأي شفرة ثنائية خطية دورية من الطول $2^r - 1$ بحيث تكون $\beta^{m+1}, \cdots, \beta^{m+\delta-1}$ من ضمن جذور كثيرة حدودها المولّدة. تُسمى هذه الشفرات الثنائية، **شفرات BCH البدائية (Primitive BCH Codes)** وتُسمى δ، **المسافة المعتمدة (Designed Distance)** لهذه الشفرة. وبملاحظة أن هذه الشفرات هي شفرات ثنائية على حقول جزئية وشفرات جزئية $C_K \subset C$ من شفرات ريد وسولومن C فنرى أن $d(C_K) \geq \delta$ مُحققة أيضاً لهذه الشفرات.

تُعرف شفرة ريد وسولومن الثنائية $RS(2^r, \delta)$ على أنها الشفرة الخطية الدورية على الحقل $GF(2^r)$ حيث كثيرة حدودها المولّدة هي:

$$g(x) = (\beta^{m+1} + x)(\beta^{m+1} + x) \cdots (\beta^{m+\delta-1} + x)$$

وحيث m عدد صحيح و β عنصر بدائي في الحقل $GF(2^r)$. على سبيل المثال، الشفرة المنشأة في المثال (**٦,١,٥**) هي الشفرة $RS(8,3)$ والشفرة المنشأة في المثال (**٦,١,٧**) هي الشفرة $RS(16,5)$.

مبرهنة (٦,٢,٥)

إذا كانت C هي الشفرة $RS(2^r, \delta)$ فإن:

(أ) $n = 2^r - 1$.

(ب) $k = 2^r - \delta$.

(ج) $d = \delta$.

(د) $|C| = 2^{rk}$.

البرهان

الفقرة (أ) نحصل عليها بتطبيق المبرهنة (**٦,١,١**) والفقرتان (ب) و (د) نحصل عليهما من النتيجة (**٦,١,٤**) (لاحظ أن بُعد الشفرة الخطية على الحقل $GF(2^r)$

يساوي k وعدد كلماتها يساوي 2^{rk} وهذا يتفق مع حقيقة أن الشفرة الثنائية الخطية، أي الشفرة الخطية على الحقل $GF(2)$ لها بُعد يساوي k وعدد كلماتها يساوي 2^k). وبرهان الفقرة (ج) نحصل عليه بتطبيق المبرهنة (**٦,٢,٤**) لنرى أن $d \geq \delta$ وتطبيق المبرهنة (**٣,١,٧**) لنرى أن $d \leq \delta$. ■

ملحوظة

بما أن $d = n - k + 1$ فنرى أن شفرات ريد وسولومن هي شفرات MDS (انظر المبرهنة (**٣,١,٨**)).

قبل تقديم مثال آخر ننوه إلى إمكانية النظر إلى أي شفرة C من النوع $RS(2^r, \delta)$ على أنها شفرة ثنائية؛ وذلك باستبدال كل إحداثي من إحداثيات كلمة الشفرة بكلمة ثنائية طولها r من جدول $GF(2^r)$. طول هذه الشفرة يساوي $r(2^r - 1)$ وأما طول الشفرة الثنائية التي هي شفرة على حقل جزئي وشفرة جزئية فهو $2^r - 1$. نستخدم الرمز $\hat{c}$ للتمثيل الثنائي لكلمة الشفرة $c \epsilon C$ والرمز $\hat{C}$ للشفرة الثنائية التي نحصل عليها من الشفرة C بالطريقة الموضحة في هذه الفقرة. سنرى لاحقاً (انظر المبرهنة (**٧,١,١٥**)) أهمية هذا التمثيل للشفرة $\hat{C}$ خاصة عند التصويب المفاجئ للأخطاء.

مثال (٦,٢,٦)

لنفرض أن $GF(2^2)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^2$ ولتكن C هي الشفرة $RS(4,2)$ حيث $g(x) = \beta + x$. استناداً إلى المبرهنة (**٦,٢,٥**) نرى أن طول C هو $n = 3$ وبُعدها هو $k = 2$ ومسافتها هي $d = 2$ وعدد كلماتها هو $|C| = 16$. واستناداً إلى النتيجة (**٦,١,٤**) نرى أن مصفوفة مولّدة للشفرة C هي:

$$G = \begin{bmatrix} \beta & 1 & 0 \\ 0 & \beta & 1 \end{bmatrix}$$

باستخدام جدول $GF(2^2)$ نرى أن $0,1,\beta,\beta^2$ تقابل المتجهات 00,10,01,11 على التوالي. الجدول التالي يُبيّن جميع الرسائل u (عددها 16) وتمثيلها الثنائي $\hat{u}$ وكلمات المقابلة $c = uG$ وتمثيلها الثنائي:

$\underline{\hat{u}}$	$\underline{u}$	$\underline{c = uG}$	$\underline{\hat{c}}$	$\underline{\hat{u}}$	$\underline{u}$	$c = uG$	$\underline{\hat{u}}$
0000	00	000	000000	0001	0β	$0\beta^2\beta$	001101
1000	10	$\beta 10$	011000	1001	1β	$\beta\beta\beta$	010101
0100	$\beta 0$	$\beta^2\beta 0$	110100	0101	$\beta\beta$	$\beta^2 1\beta$	111001
1100	$\beta^2 0$	$1\beta^2 0$	101100	1101	$\beta^2\beta$	10β	100001
0010	01	$0\beta 1$	000110	0011	$0\beta^2$	$01\beta^2$	001011
1010	11	$\beta\beta^2 1$	011110	1011	$1\beta^2$	$\beta 0\beta^2$	010011
0110	$\beta 1$	$\beta^2 01$	110010	0111	$\beta\beta^2$	$\beta^2\beta^2\beta^2$	111111
▲ 1110	$\beta^2 1$	111	101010	1111	$\beta^2\beta^2$	$1\beta\beta^2$	100111

تمارين

(**٦,٢,٧**) لتكن C هي الشفرة $RS(4,3)$ حيث كثيرة حدودها المولّدة هي $g(x) = (1+x)(\beta+x)$.

(أ) جد كلاً من n و k و d و $|C|$ لهذه الشفرة.

(ب) استخدم النتيجة (**٦,١,٤**) لإنشاء مصفوفة مولّدة G للشفرة C.

(ج) جد جميع كلمات الشفرة C والتمثيل الثنائي المقابل لهذه الكلمات في الشفرة $\hat{C}$ والرسائل المقابلة (شفّر هذه الرسائل مُستخدماً G التي وجدتها في الفقرة (ب)).

(**٦,٢,٨**) لنفرض أن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. ولتكن C هي الشفرة $RS(8,5)$ حيث $g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x)$ هي كثيرة حدودها المولّدة.

(أ) جد كلاً من n و k و d و $|C|$ لهذه الشفرة.

(ب) استخدم النتيجة (**٦,١,٤**) لإنشاء مصفوفة مولّدة G للشفرة C.

(ج) شفّر كلاً من الرسائل التالية مُستخدماً G إلى كلمة شفرة في الشفرة C ومن ثم إلى كلمة شفرة في الشفرة $\hat{C}$:

(i) $10\beta^2$ (ii) 111 (iii) $\beta^2\beta^4\beta^6$.

(**٦,٢,٩**) استخدم الحقول المنشأة في التمرين (**٥,١,١٥**) لإيجاد كثيرات حدود مولّدة للشفرات $RS(2^r,\delta)$ لكل من قيم r و δ و m التالية:

(أ) $m=2$ ، $\delta=3$ ، $r=2$

(ب) $m=2$ ، $\delta=3$ ، $r=3$

(ج) $m=0$ ، $\delta=5$ ، $r=3$

(د) $m=0$ ، $\delta=5$ ، $r=4$

(هـ) $m=0$ ، $\delta=7$ ، $r=5$.

(**٦,٢,١٠**) جد كل شفرة من شفرات التمرين (**٦,٢,٩**) مُبيّناً القيم n و k و d و $|C|$.

نرى استناداً إلى المبرهنة (**٦,٢,٥**) أن طول الشفرة C من النوع $RS(2^r,\delta)$ هو $n=2^r-1$. ولكننا أحياناً نحتاج إلى شفرات طولها مختلف عن 2^r-1 ويمكن إنشاء مثل هذه الشفرات بسهولة من الشفرة $RS(2^r,\delta)$ على النحو التالي:

لكل عدد صحيح s حيث $1\le s\le 2^r-\delta$ ولكل شفرة C من النوع $RS(2^r,\delta)$ تكوّن **الشفرة المقصورة (Shortened code)** بأخذ جميع كلمات الشفرة C التي تكون إحداثياتها الأخيرة (عددها يساوي s) أصفاراً ومن ثم نحذف هذه الأصفار من الكلمات.

مثال (٦,٢,١١)

إذا كانت C هي الشفرة $RS(4,2)$ المبينة في المثال (**٦,٢,٦**) فنرى أن الشفرة المقصورة $C(1)$ $(s=1)$ هي الشفرة المكوّنة من كلمات C التي إحداثيها الأخير 0، أي من كلمات الشفرة: $000,\beta 10,\beta^2\beta 0,1\beta^2 0$. وبهذا نرى أن:

$$C(1)=\{00,\beta 1,\beta^2\beta,1\beta^2\}.$$ ▲

ومن الممكن استخدام التمثيل بكثيرات الحدود للشفرة C من النوع $RS(2^r, \delta)$ لإنشاء الشفرة المقصورة $C(s)$ المكوّنة من كثيرات حدود C التي درجاتها أصغر من $n - s = 2^r - 1 - s$.

فإذا كانت $g(x)$ هي كثيرة الحدود المولّدة للشفرة C فنرى أن $C(s)$ هي مجموعة كثيرات الحدود $c(x) = a(x)g(x)$ حيث $deg(a(x)) < k - s = 2^r - \delta - s$ ؛ (لأن $deg(g(x)) = \delta$). وبهذا نجد أن مصفوفة مولّدة $G(s)$ للشفرة $C(s)$ هي :

$$G(s) = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-s-1}g(x) \end{bmatrix}.$$

وبمقارنة هذه المصفوفة مع المصفوفة المولّدة G للشفرة C المبينة في النتيجة (**٦,١,٤**) نجد أن $G(s)$ تتكون من أول $k - s$ صفاً من صفوف G بعد حذف الصفوف (عددها s) الأخيرة من G. وبهذا، إذا كانت الشفرة C من النوع $RS(2^r, \delta)$ لها طول n وبُعد k ومسافة d فمن الواضح أن طول الشفرة $C(s)$ يساوي $n(s) = n - s = 2^r - 1 - s$ وبُعدها $k(s) = k - s = 2^r - \delta - r$.

لإيجاد المسافة $d(s)$ للشفرة $C(s)$ لاحظ أولاً أنه إذا كانت $c_1, c_2 \epsilon C(s)$ فإن المسافة بينهما تساوي المسافة بين كلمتي الشفرة C المقابلتان لهما $c_1 00 \cdots 0$ و $c_2 00 \cdots 0$. ولذا فإن $d(C(s)) \geq d(C) = \delta$. أيضاً استناداً إلى المبرهنة (**٣,١,٧**) نعلم أن :

$$\begin{aligned} d(s) &\leq n(s) - k(s) + 1 \\ &= 2^r - 1 - s(2^r - \delta - s) + 1 \\ &= \delta \end{aligned}$$

إذن، $d(s) = \delta$. وأخيراً، استناداً إلى المبرهنة (**٣,١,٨**) نرى أن $C(s)$ شفرة MDS ونكون قد برهنا النتيجة التالية :

مبرهنة (٦,٢,١٢)

لتكن C شفرة من النوع $RS(2^r,\delta)$ ولتكن $C(s)$ هي الشفرة المقصورة للشفرة من النوع $RS(2^r,\delta)$ ومن الطول $n(s)$ والبُعد $k(s)$ ومسافتها $d(s)$. حينئذ:

$$n(s) = 2^r - 1 - s$$
$$k(s) = 2^r - \delta - s$$
$$d(s) = \delta$$

وكذلك، $C(s)$ شفرة MDS.

ملحوظة

من الممكن الحصول على شفرات مقصورة أخرى للشفرة $RS(2^r,\delta)$ بحذف أي s من إحداثيات كلمات الشفرة عوضاً عن حذف عدد s من الإحداثيات الأخيرة. وبما أن $RS(2^r,\delta)$ هي شفرة MDS فنرى أن أي شفرة مقصورة للشفرة $RS(2^r,\delta)$ تحقق الخصائص المبينة في المبرهنة (٦,٢,١٢).

مثال (٦,٢,١٣)

أنشأنا في المثال (٦,١,٥) الشفرة C من النوع $RS(2^3,3)$ حيث كثيرة حدودها المولّدة هي $g(x) = \beta^3 + \beta^4 x + x^2$. وبهذا نرى أن المصفوفة المولّدة للشفرة المقصورة $C(s)$ هي:

$$G(2) \leftrightarrow \begin{bmatrix} \beta^3 & \beta^4 & 1 & 0 & 0 \\ 0 & \beta^3 & \beta^4 & 1 & 0 \\ 0 & 0 & \beta^3 & \beta^4 & 1 \end{bmatrix}$$

وأن $n(2) = 5$ ، $k(2) = 3$ ، $d(2) = 3$. لاحظ أن $G(2)$ تم إنشاؤها بحذف آخر صفين ($s = 2$) من المصفوفة المولّدة G المبينة في المثال (٦,١,٥). ▲

(٦,٣) فك تشفير شفرات ريد وسولومن

Decoding Reed- Solomon Codes

بما أن إحداثيات كلمات الشفرة $RS(2^r,\delta)$ هي عناصر في الحقل $GF(2^r)$ فنرى أن تصويب الأخطاء في الكلمات المرسلة يحتاج علاوة على تحديد موقع الخطأ إلى معرفة

قيمة هذا الخطأ. ولهذا الغرض نُعرّف **مواقع الخطأ (Error Locations)** في الكلمة المستقبلة على أنها الإحداثيات التي يكون فيها نمط الخطأ لا يساوي صفراً. نقوم بتعيين عدد ليدل على موقع الخطأ فعند وقوع خطأ في الإحداثي j من الكلمة المستقبلة فيكون β^j هو **عدد موقع الخطأ (Error Location Number)**.

(نستخدم الأعداد $0,1,2,\cdots,n-1$ لترقيم الإحداثيات كما فعلنا لشفرات BCH التي تصوّب خطأين). على سبيل المثال، تجد لنا الخطوتان (٤) و (٦) من الخوارزمية (**٥,٥,٤**) عدد موقع الخطأ لنمط الخطأ عند استخدامنا شفرة BCH التي تصوّب خطأين. **قيمة الخطأ (Error Magnitude)** لموقع الخطأ i هي العنصر في الحقل $GF(2^r)$ الذي يظهر في الإحداثي i من نمط خطأ. بما أن الشفرة BCH المقدمة في الفصل الخامس هي شفرة على الحقل $GF(2)$، فنرى أن جميع قيم الخطأ تساوي 1 (العنصر غير الصفري الوحيد في الحقل $GF(2)$) وبهذا فهي تتحدد تماماً بمعرفة مواقع الأخطاء. ولكن الوضع مختلف في الشفرات المعرّفة على الحقل $GF(2^r)$ حيث $r \geq 2$ ومن ثم نحتاج لفك تشفير شفرات ريد وسولومن إلى إيجاد مواقع الأخطاء وقيم الأخطاء التي تقابل هذه المواقع.

مثال (٦,٣,١)

لنفرض أن $RS(8,3)$ هي الشفرة المبينة في المثال (**٦,١,٥**). إذا كانت $c = \beta^3\beta^4\beta^0000$ هي الكلمة المرسلة و $w = \beta^3\beta^4\beta^500$ هي الكلمة المستقبلة فنرى أن نمط الخطأ هو:

$$e = c + w = 00\beta^40000$$

بما أن β^4 هو العنصر غير الصفري في نمط الخطأ e وهو الإحداثي 2 فنجد أن عدد موقع الخطأ هو β^2 وأما قيمة الخطأ المقابلة فهي β^4. ▲

نقدم الآن خوارزمية لفك تشفير الشفرة $RS(2^r,\delta)$ (ومن ثم الشفرة المقابلة BCH والتي هي شفرة على حقل جزئي وشفرة جزئية). لهذا الغرض، نفرض أن:

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

هي كثيرة الحدود المولّدة حيث β عنصر بدائي في الحقل $GF(2^r)$. ولنفرض أن $t=\lfloor\delta-1/2\rfloor$ (كما في العادة) ولنفرض أن $a_1,\cdots,a_e$ هي أعداد مواقع الأخطاء وأن $b_1,\cdots,b_e$ هي قيم الأخطاء المقابلة لهذه الأعداد حيث $e\le t$ (في المثال **٦,٣,١**) لدينا $t=1$ وبما أنه وقع خطأ واحد في الموقع الثاني، نرى أن $a_1=\beta^2$ وأن $b_1=\beta^4$). إذا كان $e<t$ فيكون من المناسب جعل $a_i=0$ لكل $e+1\le i\le t$ على الرغم من عدم وجود مواقع لهذه الأخطاء. نقوم الآن بحساب التناذرات $s_{m+1},\cdots,s_{m+\delta-1}$ (عددها $\delta-1$) وهي معرّفة على النحو التالي: $s_j=w(\beta^j)$ حيث $m+1\le j\le m+\delta-1$. (لاحظ أن هذا هو التعريف نفسه للتناذرين s_1 و s_3 المستخدمين في الشفرة BCH). لكل $m+1\le j\le m+\delta-1$ نرى أن β^j جذر لكثيرة الحدود المولّدة $g(x)$ ومن ثم فهو جذر لجميع كلمات الشفرة ويكون:

$$s_j=w(\beta^j)=c(\beta^j)+e(\beta^j)=e(\beta^j)=\sum_{i=1}^{t}b_ia_i^j \qquad (٦,١)$$

لاحظ أن (**٦,١**) نظام معادلات عدد معادلاته يساوي $\delta-1$. إذن، مسألة فك التشفير تؤول إلى إيجاد طريقة فعّالة لحل نظام جزئي من نظام المعادلات (**٦,١**) عدد معادلاته $2e$ وعدد مجاهيله $2e$ وهي $a_1,\cdots,a_e,b_1,\cdots,b_e$. (لاحظ أن $2e\le 2t\le\delta-1$). المشكلة الأساسية تكمن في أن هذه المعادلات غير خطية ومع ذلك سنبيّن الآن كيفية إيجاد كثيرة حدود جذورها $a_1,\cdots,a_e$ بأسلوب مماثل للخطوة (٦) من الخوارزمية (**٥,٥,٤**) التي استخدمت لفك تشفير الشفرة BCH التي تصوّب خطأين.

لنفرض إذن أن $A = \{a_1, \cdots, a_e\}$. نُعرّف **كثيرة حدود موقع خطأ (Error Location (Polynomial** $\sigma_A(x)$ على أنها كثيرة الحدود ذات الجذور $a_1, \cdots, a_e$. أي أن:

$$\sigma_A(x) = (a_1 + x)(a_2 + x) \cdots (a_e + x) \tag{٦,٢}$$

لنفرض الآن أن σ_j هو معامل x^j في كثيرة الحدود $\sigma_A(x)$. حينئذ، بعد ضرب عوامل $\sigma_A(x)$ نرى أن:

$$\sigma_A(x) = \sigma_0 + \sigma_1 x + \cdots + \sigma_{e-1}x^{e-1} + x^e \tag{٦,٣}$$

الآن، بضرب طرفي المعادلة بالمقدار $b_i a_i^j$ لكل $1 \le i \le e$ وتعويض $x = a_i$ وأخذ المجموع من $i = 1$ إلى $i = t$ واستخدام المعادلة (**٦,٢**) نرى أن $\sigma_A(a_i) = 0$ ومن ثم نحصل على:

$$\begin{aligned} 0 &= \left(\sum_{i=1}^{t} b_i a_i^j\right)\sigma_0 + \left(\sum_{i=1}^{t} b_i a_i^j\right)\sigma_1 + \cdots + \left(\sum_{i=1}^{t} b_i a_i^{j+e}\right) \\ &= s_j\sigma_0 + s_{j+1}\sigma_1 + \cdots + s_{j+e} \end{aligned} \tag{٦,٤}$$

أي أن:

$$s_{j+e} = s_j\sigma_0 + s_{j+1}\sigma_1 + \cdots + \sigma_{e-1}s_{j+e-1} \tag{٦,٥}$$

وبما أن القيم $s_{m+1}, s_{m+2}, \cdots, s_{m+2e}$ معلومة فيكون باستطاعتنا تعويض القيم $j = m+1, \cdots, m+e$ لنحصل على e من المعادلات الخطية في المجاهيل $\sigma_0, \cdots, \sigma_{e-1}$ التي يمكن كتابتها على شكل المعادلة المصفوفية التالية (حيث الصف i يقابل المعادلة (**٦,٥**) عندما يكون $j = m + i$):

$$\begin{bmatrix} s_{m+1} & s_{m+2} & \cdots & s_{m+e} \\ s_{m+2} & s_{m+3} & \cdots & s_{m+e+1} \\ \vdots & \vdots & & \vdots \\ s_{m+e} & s_{m+e+1} & \cdots & s_{m+2e-1} \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \sigma_{e-1} \end{bmatrix} = \begin{bmatrix} s_{m+e+1} \\ s_{m+e+1} \\ \vdots \\ s_{m+2e} \end{bmatrix} \tag{٦,٦}$$

من المهم معرفة أنه يوجد دائماً حل غير تافه لهذا النظام الخطي.

لنفرض أن M هي مصفوفة المعاملات من الدرجة e في المعادلة (٦,٦). عندئذ، رتبة M تساوي e ولرؤية ذلك لاحظ أن

$$M=\begin{bmatrix}1 & \cdots & 1\\ a_1 & \cdots & a_e\\ \vdots & & \vdots\\ a_1^{e-1} & \cdots & a_e^{e-1}\end{bmatrix}\begin{bmatrix}b_1a_1^{m+1} & & 0\\ & \ddots & \\ 0 & & b_ea_e^{m+1}\end{bmatrix}\begin{bmatrix}1 & a_1 & \cdots & a_1^{e-1}\\ \vdots & \vdots & & \vdots\\ 1 & a_e & \cdots & a_e^{e-1}\end{bmatrix}$$

وبما أن $a_1,\cdots,a_e$ عناصر مختلفة وأن $a_1,\cdots,a_e,b_1,\cdots,b_e$ جميعها عناصر غير صفرية فنرى استناداً إلى التمهيدية (٦,٢,١) أن رتبة كل من المصفوفات الثلاث تساوي e وبهذا تكون رتبة M تساوي e. بناء على ما تقدم يكون بإمكاننا حل النظام (٦,٦) لإيجاد قيم $\sigma_0,\cdots,\sigma_{e-1}$. لاحظ أنه إذا افترض فاكك التشفير ابتداءً أن $e=t$ (بالطبع إن قيمة e لا تكون معروفة مسبقاً لفاكك التشفير) فتكون M مصفوفة من الدرجة $t\times(t+1)$ رتبتها e. ويمكن رؤية ذلك بكتابة M كحاصل ضرب ثلاث مصفوفات كما في السابق واستخدام الحقيقة $a_i=0$ لكل $e+1\le i\le t$. وبهذا تكون قيمة e معروفة الآن لدى فاكك التشفير. الآن، بما أن جذور $\sigma_A(x)=\sigma_0+\sigma_1x+\cdots+x^e$ هي $a_1,\cdots,a_e$ فنحصل عليها بتعويض عناصر الحقل في كثيرة الحدود $\sigma_A(x)$.

بعد إيجاد قيم $a_1,\cdots,a_e$ يتحوّل النظام (٦,١) إلى نظام معادلات خطية في المتغيرات $b_1,\cdots,b_e$ ومن ثم فباستطاعتنا حل هذا النظام بحل المعادلة المصفوفية المقابلة:

$$\begin{bmatrix}a_1^{m+1} & a_2^{m+1} & \cdots & a_e^{m+1}\\ a_1^{m+2} & a_2^{m+2} & \cdots & a_e^{m+2}\\ \vdots & \vdots & & \vdots\\ a_1^{m+e} & a_2^{m+e} & \cdots & a_e^{m+e}\end{bmatrix}\begin{bmatrix}b_1\\ b_2\\ \vdots\\ b_e\end{bmatrix}=\begin{bmatrix}s_{m+1}\\ s_{m+2}\\ \vdots\\ s_{m+e}\end{bmatrix} \qquad (٦,٧)$$

(مرة أخرى، نرى استناداً إلى التمهيدية (٦,٢,١) أن رتبة هذه المصفوفة تساوي e؛ وذلك لأن العناصر $a_1,\cdots,a_e$ غير صفرية وبهذا يمكن حل النظام الخطي لإيجاد $b_1,\cdots,b_e$).

مما تقدم يكون لدينا خوارزمية فك التشفير التالية لشفرات ريد وسولومن حيث نستخدم المصفوفة الموسّعة M' وهي المصفوفة M مُضافاً إليها عمود يمثل الطرف الأيمن للنظام (٦,٦). أي أن:

$$M' = \begin{bmatrix} s_{m+1} & s_{m+2} & \cdots & s_{m+e+1} \\ s_{m+2} & s_{m+3} & \cdots & s_{m+e+2} \\ \vdots & \vdots & & \vdots \\ s_{m+e} & s_{m+e+1} & \cdots & s_{m+2e} \end{bmatrix}.$$

خوارزمية (٦,٣,٢) [فك تشفير $RS(2^r, \delta)$]

لنفرض أنه تم إرسال إحدى كلمات الشفرة C من النوع $RS(2^r, \delta)$ حيث كثيرة حدودها المولّدة هي $g(x) = (\beta^{m+1} + x) \cdots (\beta^{m+\delta-1} + x)$ ولنفرض أن w هي الكلمة المستقبلة. ولنفرض أن $t = \lfloor (\delta - 1)/2 \rfloor$. عندئذ، لإيجاد أقرب كلمة شفرة تنتمي إلى C إلى الكلمة w نقوم بتنفيذ الخطوات التالية:

(١) حساب $s_j = w(\beta^j)$ لكل $m + 1 \le j \le m + 2t$.

(٢) نضع $e = t$ ثم نجد رتبة المصفوفة الموسّعة M'.

(٣) إذا كانت e هي رتبة المصفوفة الموسّعة M' فنقوم بحل النظام الخطي (٦,٦) لإيجاد $\sigma_0, \cdots, \sigma_{e-1}$.

(٤) نجد جذور كثيرة الحدود $\sigma_A(x) = \sigma_0 + \sigma_1 x + \cdots + x^e$ فتكون هذه الجذور هي أعداد مواقع الخطأ $a_1, \cdots, a_e$.

(٥) نقوم بحل النظام الخطي (٦,٧) لإيجاد القيم $b_1, \cdots, b_e$ وهي قيم الخطأ المقابلة للقيم $a_1, \cdots, a_e$. وبهذا يتم تحديد نمط الخطأ الأرجحي.

لاحظ أننا لسنا بحاجة لوضع المصفوفة في الخطوة (٣) من الخوارزمية (٦,٣,٢) على صيغة درجية صفية؛ لأنها مصفوفة جزئية من المصفوفة في الخطوة (٢) وهذا موضّح في المثال التالي:

مثال (٦,٣,٣)

لنفرض أن:

$$g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x) = \beta^6 + \beta^5 x + \beta^5 x^2 + \beta^2 x^3 + x^4$$

كثيرة حدود مولّدة للشفرة $RS(2^3,5)$ (لاحظ أن $m=-1$ وأن $t=2$) حيث استخدمنا كثيرة الحدود $1+x+x^3$ لإنشاء $GF(2^3)$. ولنفرض أن $w = \beta^6\beta\beta^5\beta^2 10\beta^2$ هي الكلمة المستقبلة. سنستخدم الخوارزمية (**٦,٣,٢**) لفك تشفير w.

(١) بما أن $m=-1$ و $\delta=5$ فنقوم بحساب التناذرات الأربعة s_0, s_1, s_2, s_3 (أي حساب s_i إذا كان β^i جذراً لكثيرة الحدود $g(x)$).

$$s_0 = w(\beta^0) = \beta^6 + \beta + \beta^5 + \beta^2 + 1 + 0 + \beta^2 = 1$$
$$s_1 = w(\beta) = \beta^6 + \beta^2 + \beta^7 + \beta^5 + \beta^4 + 0 + \beta^8 = \beta^3$$
$$s_2 = w(\beta^2) = \beta^6 + \beta^3 + \beta^9 + \beta^8 + \beta^8 + 0 + \beta^{14} = \beta^3$$
$$s_3 = w(\beta^3) = \beta^6 + \beta^4 + \beta^{11} + \beta^{11} + \beta^{12} + 0 + \beta^{20} = 1$$

(٢) بوضع $e=t=2$ نرى أن المصفوفة الموسّعة M' هي:

$$M' = \begin{bmatrix} 1 & \beta^3 & \beta^3 \\ \beta^3 & \beta^3 & 1 \end{bmatrix}$$

والصيغة الدرجية لها هي:

$$\begin{bmatrix} 1 & \beta^3 & \beta^3 \\ 0 & \beta^4 & \beta^2 \end{bmatrix}$$

وبهذا نرى أن رتبتها تساوي 2.

(٣) بما أن رتبة M' تساوي 2 فتستطيع حل النظام:

$$M \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_2 \\ S_3 \end{bmatrix}$$

والصيغة الدرجية الصفية للمصفوفة M هي التي حصلنا عليها في الخطوة (٢) ولذا نقوم بحل النظام:

$$\begin{bmatrix} 1 & \beta^3 \\ 0 & \beta^4 \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \beta^3 \\ \beta^4 \end{bmatrix}$$

وهذا يكافئ النظام:

$$\sigma_0 + \beta^3\sigma_1 = \beta^3$$
$$\beta^4\sigma_1 = \beta^2$$

من المعادلة الثانية نجد أن $\sigma_1 = \beta^5$. وبالتعويض في المعادلة الأولى نرى أن $\sigma_0 = 1$.

(٤) الآن كثيرة حدود مواقع الخطأ هي:

$$\sigma_A(x) = \sigma_0 + \sigma_1 x + x^2 = 1 + \beta^5 x + x^2$$

وبتجريب عناصر الحقل لإيجاد جذور $\sigma_A(x)$ نرى أن $\sigma_A(\beta) = 0$ و $\sigma_A(\beta^6) = 0$.

إذن، $\sigma_A(x) = 1 + \beta^5 x + x^2 = (\beta + x)(\beta^6 + x)$ ونرى أن قيمتي موقعي الخطأين هما $a_1 = \beta$ و $a_2 = \beta^6$.

(٥) نقوم الآن بحل النظام الخطي:

$$\begin{bmatrix} 1 & 1 \\ \beta & \beta^6 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} 1 \\ \beta^3 \end{bmatrix}$$

أي النظام:

$$\begin{bmatrix} 1 & 1 \\ 0 & \beta^5 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

ومنه نرى أن $\beta^5 b_2 = 1$ و $b_1 + b_2 = 1$. وعليه فإن $b_1 = \beta^6$ و $b_2 = \beta^2$. وبهذا يكون نمط الخطأ هو $e = 0\beta^6 0000\beta^2$. وكلمة الشفرة هي:

$$c = w + e = \beta^6\beta^5\beta^5\beta^2 100.$$ ▲

مثال (٦,٣,٤)

لتكن:
$$g(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)(\beta^5 + x)$$
$$= 1 + \beta^4 x + \beta^2 x^2 + \beta x^3 + \beta^{12} x^4 + \beta^9 x^5 + x^6$$

هي كثيرة الحدود المولّدة للشفرة $RS(2^4, 7)$ $(m = -1\ ،\ t = 3)$ حيث $GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (الجدول (٥,١)). ولنفرض أن الكلمة المستقبلة هي:

$$w(x) = 1 + \beta^4 x + \beta x^3 + \beta^9 x^5 + x^6.$$

عندئذ،

(١)

$$s_0 = w(\beta^0) = 1 + \beta^4 + \beta + \beta^9 + 1 = \beta^7$$
$$s_1 = w(\beta) = 1 + \beta^5 + \beta^4 + \beta^{14} + \beta^6 = 1$$
$$s_2 = w(\beta^2) = 1 + \beta^6 + \beta^7 + \beta^{19} + \beta^{12} = \beta^9$$
$$s_3 = w(\beta^3) = 1 + \beta^7 + \beta^{10} + \beta^{24} + \beta^{18} = \beta^{12}$$
$$s_4 = w(\beta^4) = 1 + \beta^8 + \beta^{13} + \beta^{29} + \beta^{24} = \beta^9$$
$$s_5 = w(\beta^5) = 1 + \beta^9 + \beta^{16} + \beta^{34} + \beta^{30} = \beta^7$$

(٢)

$$M' = \begin{bmatrix} \beta^7 & 1 & \beta^9 & \beta^{12} \\ 1 & \beta^9 & \beta^{12} & \beta^9 \\ \beta^9 & \beta^{12} & \beta^9 & \beta^7 \end{bmatrix} \leftrightarrow \begin{bmatrix} \beta^7 & 1 & \beta^9 & \beta^{12} \\ 0 & \beta^{12} & \beta^7 & \beta^6 \\ 0 & \beta^7 & \beta^2 & \beta \end{bmatrix}$$
$$\leftrightarrow \begin{bmatrix} \beta^7 & 1 & \beta^9 & \beta^{12} \\ 0 & \beta^{12} & \beta^7 & \beta^6 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

ونرى أن رتبة M هي 2 وعليه يكون وزن نمط الخطأ هو $e = 2$.

(٣) بما أن $e = 2$ فنرى أن النظام الخطي (٦,٧) هو:

$$\begin{bmatrix} \beta^7 & 1 \\ 1 & \beta^9 \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \beta^9 \\ \beta^{12} \end{bmatrix}$$

والنظام المختزل المقابل له هو:

$$\begin{bmatrix} \beta^7 & 1 \\ 0 & \beta^{12} \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \beta^9 \\ \beta^7 \end{bmatrix}$$

عندئذ، نحصل على النظام:

$$\beta^{12}\sigma_1 + \beta^7 = 0$$
$$\beta^7\sigma_0 + \sigma_1 + \beta^9 = 0$$

وبحل هذا النظام نجد أن $\sigma_1 = \beta^{10}$ و $\sigma_0 = \beta^6$.

(٤) $\sigma_A(x) = \beta^6 + \beta^{10}x + x^2 = (\beta^2 + x)(\beta^4 + x)$. ونرى أن $a_1 = \beta^2$ و $a_2 = \beta^4$.

$$\begin{bmatrix} 1 & 1 \\ \beta^2 & \beta^4 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} \beta^7 \\ 1 \end{bmatrix} \quad (٥)$$

وباختزال هذا النظام نجد أن:

$$\begin{bmatrix} 1 & 1 \\ 0 & \beta^{10} \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} \beta^7 \\ \beta^7 \end{bmatrix}$$

وبحل هذا النظام نجد أن $b_1 = \beta^2$ و $b_2 = \beta^{12}$. وبهذا يكون نمط الخطأ المرجح هو:

$$e = 00\beta^2 0\beta^{12}0\cdots 0$$

وكلمة الشفرة المرجحة هي:

$$c = w + e = 1\beta^4\beta^2\beta\beta^{12}\beta^9 100\cdots 0. \quad \blacktriangle$$

لاحظ أن خوارزمية فك التشفير (**٦,٣,٢**) لا تعتمد على البنية الدورية للشفرة ولهذا فيمكن استخدامها لشفرة $RS(2^r, \delta)$ المقصورة من الطول n.

تمارين

(**٦,٣,٥**) لتكن C هي الشفرة $RS(2^4, \delta)$ وكثيرة حدودها المولّدة هي:

$$g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x)(\beta^4+x)(\beta^5+x)$$

حيث $GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (**٥,١**)). فُك تشفير الكلمات المستقبلة التالية التي تم تشفيرها بواسطة الشفرة C:

(أ) $0\beta^3\beta\beta^5\beta^3\beta^2\beta^6\beta^{10}\beta 000000$.

(ب) $0\beta^4\beta^2\beta 0010\beta\beta^5\beta^3\beta^2 0\beta^{10}\beta$.

(ج) $\beta 0\beta^7 0\beta^{12}\beta^3\beta^3 10000000$.

(**٦,٣,٦**) لتكن C هي الشفرة $RS(2^4, \delta)$ وكثيرة حدودها المولّدة هي:

$$g(x) = (\beta+x)(\beta^2+x)(\beta^3+x)(\beta^4+x)$$

حيث $GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (**٥,١**) ولاحظ أن $m = 0$ في هذه الحالة). فُك تشفير الكلمات المستقبلة التالية إذا علمت أنها شُفّرت بواسطة الشفرة C:

(أ) $.001\beta^8 00\beta^5 00000000$

(ب) $.0\beta^{10}0\beta^6\beta^{13}0\beta^8\beta^{11}\beta^3\beta^5 00000$

(ج) $.\beta^4 0100\beta^2\beta^5\beta^{12}\beta^{14}000000$

(**٦,٣,٧**) لتكن C هي الشفرة $RS(2^4,5)$ المقدمة في التمرين (**٦,٣,٦**) ولتكن $C(4)$ هي الشفرة المقصورة من الطول $n = 11$ والبُعد $k = 7$. فُك تشفير كل من الكلمات المستقبلة التالية المشفّرة باستخدام C:

(أ) $.001\beta^8 00\beta^5 0000$

(ب) $.0\beta^{10}0\beta^6\beta^{13}0\beta^8\beta^{11}\beta^3\beta^5 0$

(ج) $.\beta^4 0100\beta^2\beta^5\beta^{12}\beta^{14}00$

(**٦,٣,٨**) لتكن C هي الشفرة $RS(2^4,9)$ وكثيرة حدودها المولّدة هي:

$$g(x) = (1+x)(\beta+x)\cdots(\beta^7+x)$$

حيث $GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (**٥,١**)). جد نمط الخطأ الأرجح للكلمات المستقبلة التي شُفّرت بواسطة الشفرة C والتي لها التناذرات التالية:

(أ) $.s_0 = \beta^2, s_1 = \beta^3, s_2 = \beta^4, s_3 = \beta^5, s_4 = \beta^6, s_5 = \beta^7, s_6 = \beta^8, s_7 = \beta^9$

(ب) $.s_0 = \beta^9, s_1 = \beta^{13}, s_2 = \beta^7, s_3 = \beta^4, s_4 = \beta^{12}, s_5 = \beta^4, s_6 = \beta^8, s_7 = \beta^2$

(ج) $.s_0 = 1, s_1 = 1, s_2 = 1, s_3 = 1, s_4 = 1, s_5 = 1, s_6 = 1, s_7 = 1$

(د) $.s_0 = \beta^{10}, s_1 = \beta^3, s_2 = \beta^{13}, s_3 = \beta^3, s_4 = \beta^{12}, s_5 = \beta^5, s_6 = \beta^{13}, s_7 = \beta^3$

(هـ) $.s_0 = \beta^{12}, s_1 = \beta^8, s_2 = 0, s_3 = \beta^7, s_4 = \beta^{13}, s_5 = \beta^4, s_6 = \beta^{13}, s_7 = 1$

(و) $.s_0 = \beta^2, s_1 = 0, s_2 = 0, s_3 = \beta^2, s_4 = 0, s_5 = 0, s_6 = \beta^2, s_7 = 0$

(٦,٤) طريقة التحويل لإنشاء شفرات ريد وسولومن
Transform Approach to Reed-Solomon Codes

تعتمد طريقة التحويل لإنشاء وفك تشفير شفرات ريد وسولومن على إمكانية تمثيل متجهات K^n كدوال من مجموعة S إلى الحقل $F = GF(2^r)$ عوضاً عن تمثيلها كمعاملات كثيرات حدود. ندرس الآن تفاصيل هذه الطريقة ونثبت أنها تُزودنا بمصفوفة مولّدة مختلفة لشفرات ريد وسولومن.

مثال (٦,٤,١)

لنفرض أن $S = GF(2^3)$ هو الحقل المنشأ باستخدام $1 + x + x^3$ والعنصر البدائي β.

ولنفرض أن $f: S \to \{0,1\}$ هي الدالة المعرّفة على النحو التالي:

$$f(0) = 0, f(1) = 0, f(\beta) = f(\beta^2) = f(\beta^4) = 1, f(\beta^6) = f(\beta^3) = f(\beta^5) = 0$$

عندئذ، يمكن تمثيل $f(x)$ بالمتجه:

$$v_f = \big(f(0), f(1), f(\beta), \cdots, f(\beta^6)\big) = (0,0,1,1,0,1,0,0).$$ ▲

مثال (٦,٤,٢)

لنفرض أن $S = GF(2^3)$ ولنفرض أن الدالة $g: S \to S$ معرّفة على النحو التالي:

$$v_g = \big(g(0), g(1), g(\beta), \cdots, g(\beta^6)\big) = (\beta^4, 0, 1, \beta^2, 1, \beta, 0, 0)$$

لاحظ أنه من الممكن تمثيل $g(x)$ بكثيرة الحدود:

$$g(x) = \beta^4 + \beta^2 x + \beta^3 x^2 + x^3.$$ ▲

تُمثل كثيرتا الحدود $p(x)$ و $q(x)$ الدالة نفسها من S إلى $GF(2^r)$ حيث $S \subseteq GF(2^r)$ إذا وفقط إذا كان $p(\alpha) = q(\alpha)$ لكل $\epsilon\alpha S$.

لنفرض أن V مجموعة جميع كثيرات الحدود من الدرجة التي لا تزيد عن $k - 1$ والتي معاملاتها عناصر من الحقل $GF(2^r)$ (أو مجموعة المتجهات التي تمثل كثيرات الحدود هذه كدوال من $S \subseteq GF(2^r)$ إلى $GF(2^r)$). المبرهنة التالية تُبيّن لنا أن V فضاء

متجهات ومجموعة كثيرات الحدود $\{1, x, x^2, \cdots, x^{k-1}\}$ أساس لهذا الفضاء. يُدعى فضاء المتجهات هذا **بالفضاء الدالي على S (Function Space on S)** S.

مبرهنة (٦,٤,٣)

مجموعة جميع الدوال من S إلى $F = GF(2^r)$ الممثلة بكثيرات حدود من درجات لا تزيد عن $k-1$ هي فضاء دالي بُعده k وأساسه $\{1, x, x^2, \cdots, x^{k-1}\}$.

البرهان

من الواضح أن أي كثيرة حدود درجتها لا تزيد عن $k-1$ تنتمي إلى $\langle\{1, x, x^2, \cdots, x^{k-1}\}\rangle$.

ولذا نحتاج فقط إلى إثبات وحدانية التمثيل لكل دالة. ولهذا الغرض نفرض أن $p(x)$ و $q(x)$ متساويتان كدالتين على S. حينئذ، نرى أن $p(\alpha) - q(\alpha)$ لكل $\epsilon\alpha S$. وعليه فإن $p(\alpha) - q(\alpha) = 0$ وتكون $p(x) - q(x)$ كثيرة حدود درجتها أصغر من k وعدد جذورها n وهذا مستحيل ؛ لأن $n \geq k$. إذن، $p(x) - q(x) = 0$. أي أن $p(x) = q(x)$. ■

مثال (٦,٤,٤)

لنفرض أن $F = GF(2^r)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$ وليكن V هو الفضاء الدالي المكوّن من كثيرات الحدود التي درجتها لا تزيد عن 2. عندئذ، $\{1, x, x^2\}$ أساس للفضاء الدالي والمتجهات المقابلة لهذا الأساس هي :

$$1 \leftrightarrow (1,1,1,1,1,1,1,1)$$
$$x \leftrightarrow (0,1,\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6)$$
$$x^2 \leftrightarrow (0,1,\beta^2,\beta^4,\beta^6,\beta,\beta^3,\beta^5)$$

المتجه المقابل لكثيرة الحدود $p(x) = a_0 + a_1 x + a_2 x^2$ (باعتبارها دالة) هو :

$$v_p = [a_0, a_1, a_2]\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 0 & 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5 \end{bmatrix}.$$ ▲

تذكر أن شفرة MDS هي شفرة خطية من النوع (n,k,d) حيث $d=n-k+1$.

مبرهنة (٦,٤,٥)

الفضاء الدالي على المجموعة $S\subseteq GF(2^r)$ المكوّن من كثيرات الحدود التي درجاتها لا تزيد عن $k-1$ ومعاملاتها تنتمي إلى $GF(2^r)$ هو شفرة MDS من النوع $(n,k,n-k+1)$ حيث $n=|S|\leq 2^r$.

البرهان

نفرض أن $S\subseteq GF(2^r)$ حيث $|S|=n$ ولنفرض أن الفضاء الدالي هو الفضاء المكوّن من جميع كثيرات الحدود $p:S\to GF(2^r)$ حيث $deg(p(x))\leq k-1$.

من الواضح أن طول كل من المتجهات (ومن ثم طول الشفرة) هو n وأن بعد الفضاء يساوي k حيث $k\leq n$ (استناداً إلى المبرهنة (٦,٤,٣)). ولحساب المسافة لاحظ أولاً أن عدد الجذور المختلفة لكثيرة حدود $p(x)$ حيث $deg(p(x))\leq k-1$ هو على الأكثر $k-1$. وبهذا نرى أن المتجه المقابل لكثيرة الحدود $p(x)$ يحتوي على الأكثر $k-1$ صفراً ويكون وزنه على الأقل $n-k+1$. واستناداً إلى المبرهنة (٣,١,٧) نعلم أن $d\leq n-k+1$ لأي شفرة خطية. إذن، $d=n-k+1$. ■

تُسمى المجموعة الجزئية $S=\{\alpha\epsilon F:\alpha^n=1\}$ من الحقل $F=GF(2^r)$ **جذور الوحدة من النوع n (nth Roots Of Unity)**. لاحظ أن n يقسم 2^r-1 (ولكن ليس من الضروري أن يكون $n=2^r-1$). وبهذا نرى أن n عدد فردي. لاحظ أيضاً أن S هي مجموعة جذور كثيرة الحدود $1+x^n$ في الحقل F. نقول إن $\epsilon\beta S$ هو **جذر وحدة بدائي من النوع n (Primitive nth Root Of Unity)** في الحقل $GF(2^r)$ إذا كانت $S=\{1,\beta,\beta^2,\cdots,\beta^{n-1}\}$. هذا المفهوم هو تعميم لمفهوم العنصر البدائي في الحقل وبهذا يتيح لنا فرصة إنشاء شفرات ريد وسولومن دورية من الطول n الذي يقسم 2^r-1 (ليس بالضرورة أن يكون $n=2^r-1$). إن جلّ ما درسناه سابقاً في هذا الفصل للشفرات من الطول

$n = 2^r - 1$ حيث β عنصر بدائي يبقى صحيحاً في الحالة التي يكون فيها β جذر وحدة بدائياً من النوع n.

مثال (٦,٤,٦)

لنفرض أن $F = GF(2^4)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^4$ والعنصر البدائي β. جذور الوحدة من النوع 5 هي $\{1, \beta^3, \beta^6, \beta^9, \beta^{12}\}$ وجذور الوحدة من النوع 3 هي $\{1, \beta^5, \beta^{10}\}$. إذن، β^3 جذر وحدة بدائي من النوع 5 و β^5 جذر وحدة بدائي من النوع 3. ▲

قبل الشروع في إنشاء شفرات ريد وسولومن الدورية سنثبت أن كثيرتي حدود تقابلان الدالة نفسها على S إذا وفقط إذا كانتا متطابقتين قياس $1 + x^n$.

مبرهنة (٦,٤,٧)

لتكن $p(x), q(x) \epsilon GF(2^r)$ ولتكن $S \subseteq GF(2^r)$ مجموعة جميع جذور الوحدة من النوع n. عندئذ، $p(x)$ و $q(x)$ تمثلان الدالة نفسها $f: S \to GF(2^r)$ (أي $p(\beta^i) = q(\beta^i)$ لكل $\beta^i \epsilon S$) إذا وفقط إذا كان $p(x) \equiv q(x) (mod 1 + x^n)$.

البرهان

لنفرض أن $q(x) = h(x)(1 + x^n) + p(x)$ حيث $deg(p(x)) < n$. عندئذ، $q(\beta^i) = h(\beta^i)(1 + \beta^{in}) + p(\beta^i) = p(\beta^i)$؛ لأن β^i جذر لكثيرة الحدود $1 + x^n$.

ولبرهان العكس، نفرض أن $p(\beta^i) = q(\beta^i)$ لكل $\beta^i \epsilon S$. حينئذ يكون β^i جذراً لكثيرة الحدود $p(x) - q(x)$ ونرى أن:

$$p(x) - q(x) = h(x) \prod_{i=0}^{n-1} (x + \beta^i) = h(x)(1 + x^n).$$ ■

مبرهنة (٦,٤,٨)

لتكن S مجموعة جذور الوحدة من النوع n في الحقل $GF(2^r)$. عندئذ، الفضاء الدالي على S المكوّن من جميع كثيرات الحدود التي تنتمي إلى $GF(2^r)[x]$ ودرجاتها لا تزيد عن $k - 1$ هو شفرة دورية من النوع $(n, k, n - k + 1)$ على الحقل $GF(2^r)$.

البرهان

لنفرض أن $v_p(p(1), p(\beta), \cdots, p(\beta^{n-1}))\epsilon C$. لإثبات أن C شفرة دورية يكفي أن نثبت أن $(p(\beta), p(\beta^2), \cdots, p(\beta^{n-1}))\epsilon C$. وبملاحظة أن $p(\beta x)$ كثيرة حدود درجتها لا تزيد عن $k-1$ نرى أن $p'(x) = p(\beta x)\epsilon C$. ولكن:

$$(p'(1), p'(\beta), \cdots, p'(\beta^{n-1}) = (p(\beta), p(\beta^2), \cdots, p(\beta^{n-1}), p(1)).$$ ■

مثال (٦,٤,٩)

لنفرض أن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. ولتقابل $p(x) = \beta^4 + \beta^2 x + \beta^3 x^2 + x^3$ المتجه $(0,1,\beta^2,1,\beta,0,0)$. عندئذ، المتجه $(1,\beta^2,1,\beta,0,0,0)$ هو إزاحة لهذا المتجه ويقابل الدالة:

$$p(\beta x) = \beta^4 + \beta^3 x + \beta^5 x^2 + \beta^3 x^3 = (\beta^4 + x)(\beta^5 + x)(\beta^6 + x)\beta^3.$$ ▲

لتكن $V(x) = V_0 + V_1 x + \cdots + V_{n-1}x^{n-1}$. نقول إن كثيرة الحدود $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$ هي **تحويل (Transform)** كثيرة الحدود $V(x)$ إذا كان $V(\beta^j) = \sum V_i \beta^{ji} = v_j$ لكل $j = 0,1,\cdots,n-1$. وهذا يكافئ المعادلة المصفوفية $(V_0, V_1, \cdots, V_{n-1})A = (v_0, v_1, \cdots, v_{n-1})$ حيث $A = [a_{ij}]$ و $a_{ij} = \beta^{ij}$ و β جذر وحدة بدائي من النوع n في الحقل $GF(2^r)$. تُسمى المصفوفة A، **تحويل فورييه المنتهي (Finite Fourier Transform)** أو **تحويل الحقل المنته (Finite Field Transform)**. A مصفوفة قابلة للعكس ونرى أن:

$$(V_0, V_1, \cdots, V_{n-1}) = (v_0, v_1, \cdots, v_{n-1})A^{-1}$$

أو $V_i = \sum_{j=0}^{n-1} v_j \beta^{-ij} = v(\beta^{-i})$.

بيّنا في التمهيدية (٦,٢,١) أن A قابلة للعكس ولكننا نُقدم الآن برهاناً آخر لذلك بإثبات أن A^{-1} تحوّل v إلى V.

مبرهنة (٦,٤,١٠)

لنفرض أن β جذر وحدة بدائي من النوع n. إذا كان $v_i = V(\beta^i)$ حيث $V(x) = V_0 + V_1x + \cdots + V_{n-1}x^{n-1}$ فإن $V_i = v(\beta^{-i})$ حيث :

$$v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1}.$$

البرهان

$$v(\beta^{-i}) = \sum_j v_j\beta^{-ij} = \sum_j (\sum_k V_k(\beta^{kj})\,\beta^{-ij} = \sum_k V_k \sum_j \beta^{(k-i)j} = V_i$$

لأن

$$\sum_{j=0}^{n-1} \beta^{(k-i)j} = \begin{cases} n\ mod 2, & k-i=0 \\ 0 \quad\quad , & k-i \neq 0 \end{cases}$$

وبملاحظة أن $(1+x^n) = (1+x)(1+x+\cdots+n^{n-2}+x^{n-1})$ نرى أن $\beta^{k-i} \neq 1$ جذر لكثيرة الحدود $1+x+\cdots+x^{n-2}+x^{n-1}$. أيضاً n فردي ؛ لأن n يقسم 2^r-1. ■

إذا كان $(v_0, v_1, \cdots, v_{n-1})$ متجهاً فقد بيّنا كيفية استخدام هذا المتجه للحصول على معاملات كثيرة الحدود $V(x) = V_0 + V_1x + \cdots + V_{n-1}x^{n-1}$. وهذا هو بالفعل ما تنجزه خوارزمية فك التشفير المقدمة في البند (٦,٣).

مبرهنة (٦,٤,١١)

لتكن S مجموعة جذور الوحدة من النوع n في الحقل $GF(2^r)$. عندئذ، الفضاء الدالي المكوّن من كثيرات الحدود التي درجاتها أصغر من $n-\delta+1$ على S هو شفرة MDS دورية حيث $g(x) = (\beta+x)(\beta^2+x)\cdots(\beta^{\delta-1}+x)$ كثيرة حدوده المولّدة و β جذر وحدة بدائي من النوع n.

البرهان

كثيرة الحدود $C(x)$ التي متجهها يقابل $c(x) = a(x)g(x)$ هي :

$$C(x) = \sum_{i=0}^{n=i} c(\beta^{n-i})x$$

وبما أن $c(\beta^{n-i}) = 0$ لكل $i = n-\delta+1, n-\delta+2, \cdots, n-1$ فنرى أن معامل x^i في $C(x)$ يساوي صفراً وبهذا تكون $deg(C(x)) < n-\delta+1$. ■

نستطيع القول الآن إن الطريقة البديلة التي قدّمناها لإنشاء شفرة $RS(2^r, \delta)$ حيث $n = 2^r - 1$ تُزودنا بمصفوفة مولّدة مختلفة عن تلك التي حصلنا عليها في السابق (إضافة إلى نظرة مختلفة لإحداثيات المعلومات).

مثال (٦,٤,١٢)

ليكن $\epsilon\beta GF(2^3)$ عنصراً بدائياً حيث $GF(2^3)$ هو الحقل المنشأ باستخدام $1 + x + x^3$. ولنفرض أن $RS(2^3, 5)$ هي الشفرة المبينة في المثال (**٦,٢,٨**) حيث كثيرة حدودها المولّدة هي:

$$g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x) = \beta^6 + \beta^5 x + \beta^5 x^2 + \beta^2 x^3 + x^4.$$

المتجه المقابل لكثيرة الحدود $g(x)$ هو $(\beta^6, \beta^5, \beta^5, \beta^2, 1, 0, 0)$. أما تحويل $g(x)$ فهو كثيرة الحدود $G(x) = \sum_{k=0}^{6} g(\beta^{7-k}) x^k$.

بما أن $(g(\beta^0), g(\beta^1), \cdots, g(\beta^6) = (0,0,0,0,1,\beta,\beta^4))$ فنرى أن:

$$\begin{aligned} G(x) &= g(\beta^{7-1})x + g(\beta^{7-2})x + g(\beta^{7-3})x \\ &= \beta^4 x + \beta x^2 + x^3 \\ &= x(\beta^4 + \beta x + x^2) \end{aligned}$$

ومن السهل التحقق من أن $G(x)$ تمثل دالة متجهها:

$$(G(\beta^0), G(\beta^1), \cdots, G(\beta^6)) = (\beta^6, \beta^5, \beta^5, \beta^2, 1, 0, 0).$$

ننظر هنا إلى الشفرة $RS(2^3, 5)$ على أنها الفضاء الدالي لمجموعة كثيرات الحدود التي درجاتها بين 1 و 3. ومن الواضح أن $\{x, x^2, x^3\}$ أساس لهذا الفضاء الدالي وأن المصفوفة المولّدة له هي:

$$\begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^1 & \beta^3 & \beta^5 \\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta^1 & \beta^4 \end{bmatrix}$$

إذن، $G(x) = \beta^4 x + \beta x^2 + x^3$ إذا وفقط إذا كان المتجه المقابل لها هو:

$$(\beta^4, \beta, 1)\begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^1 & \beta^3 & \beta^5 \\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta^1 & \beta^4 \end{bmatrix} = (\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0). \quad \blacktriangle$$

نُبيّن الآن كيفية استخدام هذه الطريقة لفك تشفير شفرات ريد وسولومن. تذكر أنه إذا كانت $g(x)$ كثيرة الحدود المولّدة لشفرة ريد وسولومن وكانت $w(x)$ هي الكلمة المستقبلة فإن $w(x) = c(x) + e(x)$ حيث $c(x) = a(x)g(x)$ و $e(x)$ هي كثيرة حدود الخطأ.

لنفرض أن $W(x)$، $C(x)$، $E(x)$ هي تحويلات $w(x)$، $c(x)$، $e(x)$ على التوالي. بما أن التحويل هو تطبيق خطي نجد أن:

$$W(x) = \sum_k w(\beta^{n-k})x^k = \sum_k c(\beta^{n-k})x^k + \sum_k e(\beta^{n-k})x^k$$
$$= C(x) + E(x)$$

وبما أن لكثيرة الحدود $g(x)$ عدد $\delta - 1$ من الجذور المتتالية β^k حيث $k = m+1, m+2, \cdots, m+\delta-1$ نرى أن $c(\beta^k) = 0$ وأن التناذرات s_{n-k} هي $w(\beta^{n-k}) = e(\beta^{n-k}) = E_k$ لقيم k المبينة. وهذا يعني أن التناذرات تُزودنا بعدد $\delta - 1$ من معاملات تحويل $e(x)$. ويبقى علينا إيجاد المعاملات المتبقية. ولإنجاز ذلك نحتاج كثيرة حدود مواقع الخطأ.

من تعريف $\sigma(x)$ نعلم أن $\sigma(\beta^k) = 0$ إذا وفقط إذا كان $e_k \neq 0$ (تذكر أن $\sigma(\beta^k) = 0$ إذا وفقط إذا كان β^k عدد موقع خطأ وهذه بدوره يعني أن الإحداثي k من $e(x)$ لا يساوي صفراً). وبما أن $E(\beta^k) = e_k$ فنرى أن $\sigma(\beta^k)E(\beta^k) = 0$ لكل k ويكون:

$$\sigma(x)E(x) \equiv 0 (mod 1 + x^n)$$

و $\sigma(x)E(x) \equiv \sum_{i=0}^{t} \sigma_i x^i \sum_{\ell} E_\ell x^\ell \ (mod 1 + x^n)$ (لأن درجة $\sigma(x)$ هي على الأكثر $t = \lfloor (\delta - 1)/2 \rfloor$).بمقارنة معاملات x^{t+k} نرى أن:

$$\sigma_t E_k + \sigma_{t-1} E_{k+1} + \sigma_{t-2} E_{k+2} + \cdots + \sigma_0 E_{k+t} = 0.$$

نستطيع الآن استخدام معرفتنا المسبقة لعدد $\delta - 1$ من قيم E_k المتتالية (أي، التناذرات s_{n-k}) لحساب المعاملات σ_i ومن ثم استخدام ذلك لإيجاد جميع قيم E_k.

مثال (٦,٤,١٣)

لنفرض أن $\sigma(x) = \sigma_0 + \sigma_1 x + x^2$ وأن $E(x) = E_0 + E_1 x + \cdots + E_6 x^6$. عندئذ، $\sigma(x)E(x) \equiv 0 (mod 1 + x^7)$ إذا وفقط إذا كان $E_k = \sigma_1 E_{k+1} + \sigma_0 E_{k+2}$ حيث $k = 0,1,\cdots,6$ ▲

مثال (٦,٤,١٤)

بالرجوع إلى المثال (٦,٣,٣) نفرض أن $w = (\beta^6, \beta, \beta^5, \beta^2, 1, 0, \beta^2)$. بما أن $d = 5$ فنرى أن $t \leq 2$ وأن:

$$E_0 = w(\beta^0) = 1, E_6 = w(\beta) = \beta^3, E_5 = w(\beta^2) = \beta^3, E_4 = w(\beta^3) = 1$$

وأن $\sigma(x) = x^2 + \sigma_1 x + \sigma_0$. وباستخدام المثال (٦,٣,٣) لإيجاد القيم σ_0 و σ_1 نرى أن $\sigma_0 = 1$ و $\sigma_1 = \beta^5$. وبهذا يكون $E_k = \beta^5 E_{k+1} + E_{k+2}$. وبما أن $(E_0, E_6, E_5, E_4) = (1, \beta^3, \beta^3, 1)$ فنجد أن:

$$E_3 = \beta^5 E_4 + E_5 = \beta^5 + \beta^3 = \beta^2$$
$$E_2 = \beta^5 E_3 + E_4 = \beta^5 + \beta^2 + 1 = 0$$
$$E_1 = \beta^5 E_2 + E_3 = 0 + \beta^2 = \beta^2$$

ومن ذلك يكون تحويل $e(x)$ هو $E(x) = \sum E_k x^k$ حيث:

$$(E_0, E_1, \cdots, E_6) = (1, \beta^2, 0, \beta^2, 1, \beta^3, \beta^3).$$

الآن، $E(x) = 1 + \beta^2 x + \beta^2 x^3 + x^4 + \beta^3 x^5 + \beta^3 x^6$. إذن، يكون متجه نمط الخطأ الأرجح وقوعه هو $e = \big(E(\beta^0), E(\beta^1), \cdots, E(\beta^6)\big) = (0, \beta^6, 0,0,0,0, \beta^2)$. ونخلص إلى أن كلمة الشفرة هي: $c = w + e = (\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0)$.

ومن جهة أخرى، لو استخدمنا المصفوفة المولّدة المبينة في المثال (**٦,٤,١٢**) فلا نحتاج إلى إيجاد متجه الخطأ وعوضاً عن ذلك نقوم بحساب القيم $w(\beta^k)$ لكل $k = 0,1,\cdots,6$ ومن ثم جمع هذه القيم مع تحويل $e(x)$ لنجد أن:

$$\begin{aligned}(w_0, w_1, \cdots, w_6) &= (w(\beta^0), w(\beta^6), w(\beta^5), \cdots, w(\beta^1)) \\ &= (1, \beta, \beta, \beta^6, 1, \beta^3, \beta^3) \\ (E_0, E_1, \cdots, E_6) &= (1, \beta^2, 0, \beta^2, 1, \beta^3, \beta^3)\end{aligned}$$

وبهذا يكون:

$$\begin{aligned}(C_0, C_1, \cdots, C_6) &= (W_0, W_1, \cdots, W_6) + (E_0, E_1, \cdots, E_6) \\ &= (0, \beta^4, \beta, 1,0,0,0)\end{aligned}$$

إذن، $C(x) = \beta^4 x + \beta x^2 + x^3$ وتكون إحداثيات المعلومات هي $(\beta^4, \beta, 1)$. سنترك للقارئ التحقق من أن $c = (\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0)$ هو متجه $C(x)$. ▲

تمارين

(**٦,٤,١٥**) أثبت أن $(\beta^6, \beta^5, \beta^5, \beta^2, 1,0,0)$ هو متجه $C(x) = \beta^4 x + \beta x^2 + x^3$ حيث β عنصر بدائي في الحقل $GF(2^3)$ المنشأ باستخدام $1 + x + x^3$.

(**٦,٤,١٦**) ليكن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. جد المصفوفة المولّدة لشفرة MDS من الطول 7 للفضاء الدالي المكوّن من جميع كثيرات الحدود على $S = GF(2^3)\backslash\{0\}$ حيث أساسه هو:

(أ) $\{x, x^2, x^3\}$.

(ب) $\{1, x, x^2, x^3, x^4\}$.

(ج) $\{x, x^3, x^6\}$.

(**٦,٤,١٧**) أثبت أن جميع الشفرات المبينة في التمرين السابق هي شفرات دورية وجد كثيرة الحدود المولّدة لكل منها.

(**٦,٤,١٨**) ليكن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. لكل من $G(x)$ المبينة فيما يلي، جد المتجه المقابل v_g في الفضاء الدالي.

(أ) $G(x) = x + \beta x^3$.

(ب) $G(x) = 1 + x^2 + x^4$.

(**٦,٤,١٩**) لنفرض أن $GF(2^3)$ هو الحقل المنشأ باستخدام كثيرة الحدود $1 + x + x^3$. ولنفرض أن β عنصر بدائي. جد معاملات كثيرة الحدود $G(x)$ إذا علمت أن:

(أ) $v_g = (\beta^3, \beta, \beta^4, 0, \beta^6, \beta^5, \beta^2)$.

(ب) $v_g = (\beta^4, \beta^2, \beta, \beta^3, 0, \beta^6, 1)$.

(**٦,٤,٢٠**) لكل من التمارين (**٦,٣,٥**)، (**٦,٣,٦**)، (**٦,٣,٨**)، استخدم طريقة التحويل لحساب نمط الخطأ ومن ثم فك التشفير.

(٦,٥) خوارزمية بيرلكامب ومايسي
Berlekamp-Massy Algorithm

نقدم في هذا البند خوارزمية بيرلكامب ومايسي لحساب كثيرة حدود موقع الخطأ $\sigma(x)$ بمعرفة التناذرات $s_j = w(\beta^j)$ حيث $m + 1 \le j \le m + 2t$. هذه الخوارزمية أسرع من الخوارزمية التي قدّمناها في البند السابق والتي تعتمد على حل النظام الخطي (**٦,٦**).

لنفرض أن $\sigma_R(x) = 1 + \sigma_{t-1}x + \sigma_{t-2}x^2 + \cdots + \sigma_0 x^t$. أي أن $\sigma_R(x)$ هي عكس (**reverse**) كثيرة حدود موقع الخطأ $\sigma(x)$. ولنفرض أن $s(x) = 1 + s_{m+1}x + s_{m+2}x^2 + \cdots + s_{m+2t}x^{2t}$ هي كثيرة حدود التناذرات. باستخدام خوارزمية القسمة نجد أن:

$$\sigma_R(x)s(x) = q(x)x^{2t+1} + r(x)$$

حيث $deg(r(x)) \leq 2t$. ولكن معاملات $x^{t+1}, \cdots, x^{2t}$ في كثيرة الحدود $\sigma_R(x)s(x)$ جميعها أصفار ومن ثم فإن $deg(r(x)) \leq t$.

تُزودنا النسخة **(version)** التي نُقدمها من خوارزمية بيرلكامب ومايسي بكثيرة حدود $P_{2t}(x)$ تحقق:

$$P_{2t}(x)s(x) = q_{2t}(x)x^{2t+1} + r_{2t}(x)$$

حيث $deg(P_{2t}(x)) \leq t$ و $deg(r_{2t}(x)) \leq t$ و $P_{2t}(0) = 1$ (إن وجد). وهذا كافٍ لكي يكون $P_{2t}(x) = \sigma_R(x)$. في واقع الأمر مخرج الخوارزمية هو متتالية من كثيرات الحدود $P_i(x)$ وأعداد صحيحة D_i تحقق ما يلي:

إذا كان $P_i(x)s(x) = q_i(x)x^{i+1} + r_i(x)$ حيث $deg(r_i(x)) \leq i$ فإن $deg(P_i(x)) \leq i - \lfloor D_i/2 \rfloor$ وإن $deg(r_i(x)) \leq i - \lfloor (1 + D_i)/2 \rfloor$. إضافة إلى ذلك تكون $P_i(x)$ تركيباً خطياً لكثيرة الحدود $P_{i-1}(x)$ وكثيرة حدود سابقة $P_{z_i-1}(x)$.

لنفرض أن:

$$q_i(x) = q_{i,0} + q_{i,1}x + \cdots + q_{i,2t-1-i}x^{2t-1-i}$$

وأن:

$$P_i(x) = x^{2t-1-i}P_i(x) = P_{i,0} + P_{i,1}x + \cdots + P_{i,\ell}x^{\ell}.$$

الخطوة i من الخوارزمية هي حساب $q_i(x)$ ، $P_i(x)$، الأعداد الصحيحة D_i، الدلائل z_i (التي تستخدم لتحديد كثيرة الحدود $P_{z_i}(x)$ التي نحتاج إليها إضافة إلى $P_i(x)$ لتنفيذ الخطوة التالية). إن إثبات صواب الخوارزمية أمر يسير وسنطلب من القارئ إنجاز ذلك في التمرين (**٦,٥,٥**).

خوارزمية (٦,٥,١) [خوارزمية بيرلكامب ومايسي لإيجاد كثيرة حدود موقع الخطأ]

لنفرض أن w كلمة مستقبلة تم تشفيرها باستخدام كثيرة الحدود المولّدة $g(x)$ التي جذورها القوى المتتالية $\beta^{m+1},\cdots,\beta^{m+2t}$ لعنصر β. يتم فك تشفير w بتنفيذ الخطوات التالية:

(١) احسب $s_i \coloneqq w(\beta^j)$ حيث $m+1 \le j \le m+2t$.

(٢) افرض أن:

$$q_{-1}(x) \coloneqq 1 + s_{m+1}x + s_{m+2}x^2 + \cdots + s_{m+2t}x^{2t}$$
$$q_0(x) \coloneqq s_{m+1} + s_{m+2}x + \cdots + s_{m+2t}x^{2t-1}$$
$$P_{-1}(x) \coloneqq x^{2t+1}$$
$$P_0(x) \coloneqq x^{2t}$$

افرض أن $D_{-1} \coloneqq -1$ و $D_0 \coloneqq 0$ و $z_0 \coloneqq -1$.

(٣) لكل $1 \le i \le 2t$ نقوم ارتجاعياً بتعريف $q_i(x)$ ، $P_i(x)$ ، D_i ، z_i على النحو التالي:

(أ) إذا كان $q_{i-1,0} = 0$ فنضع:

$$q_i(x) \coloneqq q_{i-1}(x)/x$$
$$P_i(x) \coloneqq P_{i-1}(x)/x$$
$$D_i \coloneqq 2 + D_{i-1}$$
$$z_i \coloneqq z_{i-1}$$

(ب) إذا كان $q_{i,0} \neq 0$ فنضع:

$$q_i(x) \coloneqq (q_{i-1}(x) - \frac{q_{i-1,0}}{q_{z_i-1,0}} q_{z_i-1}(x))/x$$

وهذه يمكن قصرها لتكون درجتها على الأكثر $2t-1-i$ ومن ثم نفرض أن:

$$P_i(x) \coloneqq (P_{i-1}(x) - \frac{q_{i-1,0}}{q_{z_i-1,0}} P_{z_i-1}(x))/x$$

$$D_i \coloneqq 2 + min\{D_{i-1}, D_{z_i-1}\}$$

$$z_i \coloneqq \begin{cases} i-1, & D_i \geq D_{z_i-1} \\ z_i - 1, & \text{خلاف ذلك} \end{cases}$$

إذا وقع عدد $e \leq t$ من الأخطاء أثناء عملية الإرسال فنجد أن درجة $P_{2t}(x) = \sigma_R(x)$ تساوي e وأن كثيرة حدود موقع الخطأ هي :

$$\sigma(x) = P_{2t,e} + P_{2t,e-1}x + \cdots + P_{2t,1}x^{e-1} + x^e$$

ولها عدد e من الجذور المختلفة.

لاحظ أن خطوات الخوارزمية لا تقوم بحساب كثيرات حدود الباقي $r_i(x)$ ومع هذا يكون لكثيرات الحدود $r_{2t}(x) \coloneqq P_{2t}(x)q_{-1}(x)(mod x^{2t+1})$ استخدامات أخرى في عملية فك التشفير. تُسمى $r(x) \coloneqq r_{2t}(x)$ أو $\rho(x) \coloneqq r_{2t}(x) - P_{2t}(x)$ **كثيرة حدود حساب الخطأ (Error Evaluator Polynomial)** وذلك لإمكانية استخدامها مع $\sigma'_R(x)$ لحساب قيم الخطأ b_j إذا علمت مواقع الخطأ a_j. فيما يلي نُبيّن كيفية إيجاد صيغة لحساب b_j بدلالة ($\rho(x)$ و $\sigma'_K(n)$) أو ($r(x)$ و $\sigma'_R(x)$). نفرض أن :

$$S(x) \coloneqq \sum_{i=0}^{\infty} s_{i+m+1}x^i$$

عندئذ، نرى أن :

$$S(x) = \sum_{i=0}^{\infty}\left(\sum_{j=1}^{t} b_j a_j^{i+m+1}\right)x^i = \sum_{j=1}^{t} b_j a_j^{m+1}\sum_{i=0}^{\infty} a_j^i x^i = \sum_{j=1}^{t}\frac{b_j a_j^{m+1}}{1-a_j x}$$

وبما أن $\sigma_R(x) \coloneqq \prod_{k=1}^{t}(1-a_k x)$ فنفرض أن $\sigma_i(x) \coloneqq \sigma_R(x)/(1-a_j x)$ لنحصل على كثيرة الحدود $\rho(x)$ التي درجتها أصغر من درجة $\sigma(x)$

$$\rho(x) \coloneqq \sigma_R(x)S(x) = \sum_{j=1}^{t} b_j a_j^{m+1}\,\sigma_j(x)$$

وبهذا يكون :

$$\rho(a_k^{-1}) = \sigma_R(a_k^{-1})S(a_k^{-1}) = \sum_{j=1}^{t} b_j a_j^{m+1}\,\sigma_j(a_k^{-1})$$

ولكن $\sigma_j(a_k^{-1}) = 0$ ما لم يكن $j = k$ ومن ذلك نرى أن $\rho(a_k^{-1}) = b_k a_k^{m+1}\sigma_k(a_k^{-1})$.

وبملاحظة أن:

$$\sigma'_R(a_k^{-1}) = -a_k \prod_{j=1, j\neq k}^{t} (1 - a_j a_k^{-1}) = -a_k \sigma_k(a_k^{-1})$$

نجد أن:

$$b_k = -\frac{\rho(a_k^{-1})}{a_k^m \sigma'_R(a_k^{-1})}$$

وبما أن $\sigma_R(a_k^{-1}) = 0$ فمن الممكن اعتبار البسط $a_k r(a_k^{-1})$ عوضاً عن $\rho(a_k^{-1})$ لنحصل على:

$$b_k = -\frac{r(a_k^{-1})}{a_k^{m-1}\sigma'_R(a_k^{-1})}.$$

مثال (٦,٥,٢)

لنأخذ المثال (٦,٣,٤) والتناذرات $s_0 = \beta^7, s_1 = \beta^0, s_2 = \beta^9, s_3 = \beta^{12}, s_4 = \beta^9, s_5 = \beta^7$. بتنفيذ خطوات الخوارزمية (٦,٥,١) نحصل على:

$$q_{-1}(x) = 1 + \beta^7 x + x^2 + \beta^9 x^3 + \beta^{12} x^4 + \beta^9 x^5 + \beta^7 x^6$$
$$q_0(x) = \beta^7 + x + \beta^9 x^2 + \beta^{12} x^3 + \beta^9 x^4 + \beta^7 x^5$$
$$P_{-1}(x) = x^7$$
$$P_0(x) = x^6$$
$$D_{-1} = -1\,, D_0 = 0\,, z_0 = -1$$

نفرض الآن أن $i = 1$. وبما أن $q_{0,0} = \beta^7 \neq 0$ فنحصل من الخطوة (٣ب) على:

$$q_0(x) + \beta^7 q_{-1}(x))/x = \beta^3 + x + \beta^{13} x^2 + \beta^{14} x^3 + \beta^{14} x^4 + \beta^{14} x^5$$

وبقصرها إلى الدرجة $2t - i - 1 = 4$ نحصل على:

$$q_1(x) = \beta^3 + x + \beta^{13} x^2 + \beta^{14} x^3 + \beta^{14} x^4$$
$$P_1(x) = 1 + \beta^7 x$$
$$D_1 = 2 + min\{D_{-1}, D_0\} = 0$$

ولكون $D_0 \geq D_{-1}$ نجد أن $z_i = i - 1 = 0$. وبتبني ترميز مختصر لتمثيل كثيرات الحدود بكلماتها المقابلة نحصل على الجدول التالي :

i	q_i								p_i		D_i	z_i
	-1	β^0	β^7	β^0	β^9	β^{12}	β^9	β^7	—	β^0	-1	
	0	β^7	β^0	β^9	β^{12}	β^9	β^7	—	β^0		0	-1
	1	β^3	β^0	β^{13}	β^{14}	β^{14}	—	β^0	β^7		1	0

وبتكملة الجدول من $i = 2$ إلى $i = 2t = 6$ نحصل على الجدول :

i	q_i						—	p_i		D_i	z_i
-1	β^0	β^7	β^0	β^9	β^{12}	β^9	β^7	—	β^0	-1	
0	β^7	β^0	β^9	β^{12}	β^9	β^7	—	β^0		0	-1
1	β^3	β^0	β^{13}	β^{14}	β^{14}	—	β^0	β^7		1	0
2	β^{12}	β^7	β^6	β^{12}	—	β^0	β^8			2	1
3	β^0	β^{10}	β^9	—	β^0	β^{12}	β^1			3	2
4	0	0	—	β^0	β^{10}	β^6				4	3
5	0	—	β^0	β^{10}	β^6					6	3
6	—	β^0	β^{10}	β^6						8	3

وأخيراً نحصل على $\sigma(x)$ بقراءة $P_{2t}(x) = P_6(x)$ عكسياً لنجد :

$$\sigma(x) = \beta^6 + \beta^{10}x + x^2 .$$ ▲

مثال (٦,٥,٣)

لتكن C هي الشفرة $RS(2^4, 9)$ حيث كثيرة حدودها المولّدة هي $g(x) = (1 + x)(\beta + x) \cdots (\beta^7 + x)$ والحقل $GF(2^4)$ منشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (٥,١)). لنفرض أن w هي الكلمة المستقبلة وأن تناذرات w هي :

$$s_0 = \beta^{12}, s_1 = \beta^9, s_2 = \beta^6, s_3 = \beta^3, s_4 = \beta^5, s_5 = \beta^{12}, s_6 = \beta^6, s_7 = \beta^6$$

باستخدام الخوارزمية (**٦,٥,١**) والترميز المستخدم في المثال (**٦,٥,٢**) نحصل على كثيرة حدود موقع الخطأ على النحو التالي:

i	q_i									—	p_i	D_i	z_i
-1	β^0	β^{12}	β^9	β^6	β^3	β^5	β^{12}	β^6	β^6	—	β^0	-1	
0	β^{12}	β^9	β^6	β^3	β^5	β^{12}	β^6	β^6	—	β^0		0	-1
1	0	0	0	β^{10}	β^7	β^5	β^2	—	β^0	β^{12}		1	0
2	0	0	β^{10}	β^7	β^5	β^2	—	β^0	β^{12}			3	0
3	0	β^{10}	β^7	β^5	β^2	—	β^0	β^{12}				5	0
4	β^{10}	β^7	β^5	β^2	—	β^0	β^{12}					7	0
5	0	β^8	β^5	—	β^0	β^{12}	0	0	β^{13}			2	4
6	β^8	β^5	—	β^0	β^{12}	0	0	β^{13}				4	4
7	0	—	β^0	β^{12}	β^{13}	β^{10}	β^{13}					6	4
8	—	β^0	β^{12}	β^{13}	β^{10}	β^{13}						8	4

إذن، كثيرة حدود موقع الخطأ هي:

$$\sigma(x) = \beta^{13} + \beta^{10}x + \beta^{13}x^2 + \beta^{13}x^3 + x^4.$$ ▲

ملحوظة

لاحظ أن قيمة z_i في كل من خطوات الخوارزمية (**٦,٥,١**) هي $i-1$ أو z_{i-1}. وعليه نحتاج فقط إلى تخزين q_{i-1} ، p_{i-1} ، D_{i-1} ، z_{i-1} ، $q_{z_{i-1}}$ ، $p_{z_{i-1}}$ ولا نحتاج إلى تخزين جميع القيم الأخرى التي تم حسابها سابقاً كما هو موضح في جدولي المثالين (**٦,٥,٢**) و (**٦,٥,٣**). ومن الواضح أن ذلك يوفر الكثير من الوقت عند التطبيق العملي للخوارزمية ولكن لغرض توضيح الخوارزمية يكون من المناسب وضع جميع الحسابات في جدول واحد.

تمارين

(**٦,٥,٤**) لتكن C هي الشفرة $RS(2^4, 9)$ حيث $g(x) = (1+x)(\beta+x)\cdots(\beta^7+x)$ هي كثيرة حدودها المولّدة وحيث $GF(2^4)$ منشأ باستخدام كثيرة الحدود $1 + x + x^4$ (انظر الجدول (**٥,١**)). استخدم الخوارزمية (**٦,٥,١**) لإيجاد كثيرة حدود موقع الخطأ للكلمات المستقبلة التي تم تشفيرها بواسطة C والتي لها التناذرات التالية:

(أ) $s_0 = \beta^2, s_1 = \beta^3, s_2 = \beta^4, s_3 = \beta^5, s_4 = \beta^6, s_5 = \beta^7, s_6 = \beta^8, s_7 = \beta^9$.

(ب) $s_0 = \beta^9, s_1 = \beta^{13}, s_2 = \beta^7, s_3 = \beta^4, s_4 = \beta^{12}, s_5 = \beta^4, s_6 = \beta^8, s_7 = \beta^2$.

(ج) $s_0 = 1, s_1 = 1, s_2 = 1, s_3 = 1, s_4 = 1, s_5 = 1, s_6 = 1, s_7 = 1$.

(د) $s_0 = \beta^{10}, s_1 = \beta^3, s_2 = \beta^{13}, s_3 = \beta^3, s_4 = \beta^{12}, s_5 = \beta^5, s_6 = \beta^{13}, s_7 = \beta^3$.

(هـ) $s_0 = \beta^{12}, s_1 = \beta^8, s_2 = 0, s_3 = \beta^7, s_4 = \beta^{13}, s_5 = \beta^4, s_6 = \beta^{13}, s_7 = 1$.

(و) $s_0 = \beta^2, s_1 = 0, s_2 = 0, s_3 = \beta^2, s_4 = 0, s_5 = 0, s_6 = \beta^2, s_7 = 0$.

(**٦,٥,٥**) **[اثبات صواب خوارزمية بيرلكامب ومايسي]**

(أ) أثبت إرجاعياً أن $deg(P_i(x)) \le i - \lfloor D_i/2 \rfloor$ (لاحظ $P_i(0) = 1$).

(ب) أثبت إرجاعياً أن $deg(R_i(x)) \le i - \lfloor (1+D_i)/2 \rfloor$ وذلك بعد إثبات أن اختيار $q_i(0)$ يجعل معامل x^i في كثيرة الحدود $P_i(x)q_{-1}(x)$ يساوي صفراً.

(ج) أثبت أن كون جميع قيم D_j مختلفة يؤدي إلى أن تكون قيمة على الأقل من قيم $j \le i, D_j$ تساوي على الأقل i واستنتج أن $D_j \ge i$ أو $D_{z_i} \ge i$.

(د) إذا كان $D_{2t} \ge 2t$ فأثبت أن $deg(P_{2t}(x)) \le t$ وأن عدد t على الأقل من معاملات $P_{2t}(x)q_{-1}(x)$ المتتالية تساوي صفراً؛ (لأن $deg(R_{2t}(x)) \le t$. وهذا يعني أن على الأقل t من متطابقات نيوتن المتتالية يجب أن تكون متحققة.

(٦,٦) الكلمات المحوّة

Erasures

الكلمة المحوة هي خطأ حيث عدد موقع الخطأ معلوم ولكن قيمة الخطأ غير معلومة. يمكن معرفة عدد موقع الخطأ من قراءة الإشارة المستقبلة (الإحداثي المستقبل لا يشبه الصفر أو الواحد) أو من بنية الشفرة. على سبيل المثال، لنفرض أن C شفرة من النوع $RS(2^r, \delta)$ وأن $\hat{C}$ التمثيل الثنائي للشفرة C. ولتكن $\widehat{C'}$ هي الشفرة الثنائية التي نحصل عليها من C بإضافة إحداثي اختبار النوعية للتمثيل الثنائي لكل إحداثي في كل كلمة من كلمات الشفرة C.

مثال (٦,٦,١)

لنفرض أن C هي الشفرة $RS(4,2)$ المقدمة في المثال (٦,٢,٦). لإنشاء $\widehat{C'}$ نقوم باستبدال الإحداثيات 0، 1، β، β^2 في كلمات الشفرة C بالكلمات 000، 101، 011، 110 على التوالي (الإحداثي الثالث في هذه الكلمات هو إحداثي اختبار النوعية). إذن، كلمة الشفرة التي تنتمي إلى $\widehat{C'}$ المقابلة لكلمة الشفرة $\beta 10 \epsilon C$ هي 011101000. ▲

تمرين

(٦,٦,٢) لتكن C هي الشفرة $RS(4,3)$ حيث $g(x) = (1+x)(\beta + x)$ هي كثيرة حدودها المولّدة (انظر التمرين (٦,٢,٧)). جد جميع كلمات الشفرة $\widehat{C'}$.

لاحظ أن كلاً من إحداثيات كلمة شفرة $c \epsilon C$ حيث C هي الشفرة $RS(2^r, \delta)$ يتم تمثيلها بكلمة ثنائية من الطول $r+1$ في كلمة الشفرة المقابلة $\hat{c'} \epsilon \widehat{C'}$ ذات الطول $(r+1)(2^r - 1)$. وبما أن أي إحداثي غير صفري من إحداثيات كلمة الشفرة c يتم استبداله بكلمة ذات وزن زوجي في الشفرة $\widehat{C'}$ فنرى أن الشفرة $\widehat{C'}$ تحتوي على $2^r - 1$ كلمة طول كل منها $r+1$ ووزن كل منها عدد زوجي. وبهذا نرى أنه إذا كان وزن إحدى المجموعات $2^r - 1$ فردياً في الكلمة المستقبلة $\widehat{w'}$ فيكون قد وقع خطأ في أحد الإحداثيات $r+1$. عندئذ، يكون باستطاعتنا فك تشفير $\widehat{w'}$ على أنها الكلمة w. أي

الكلمة التي إحداثياتها في الحقل $GF(2^r)$ التي تقابل $\widehat{w^r}$ إحداثياً كلمة شفرة في الشفرة C. وعليه فمعرفتنا بوقوع أخطاء في مجموعة مكوّنة من $r+1$ إحداثياً تقابل معرفتنا بعدد موقع الخطأ واحد من w وبهذا يكون هذا الخطأ كلمة ممحوّة.

مثال (٦,٦,٣)

لتكن $\widehat{C^r}$ الشفرة المقدمة في المثال (٦,٢,٦). ولنفرض أن 000 100 011 هي الكلمة المستقبلة. عندئذ، يكون قد وقع خطأ في المجموعة الثانية المكوّنة من ثلاث إحداثيات ؛ (لأن وزن هذه المجموعة فردي) وبهذا يكون β^1 عدد موقع كلمة ممحوة. وبما أن هذا الموقع في w هو كلمة ممحوّة فنستطيع استبداله بالإحداثي 0 (لكي يسهل عملية ايجاد التناذرات) وبهذا نقوم بفك تشفير $w = \beta 00$ إلى أقرب كلمة شفرة من كلمات الشفرة C على اعتبار أن $a_1 = \beta$ هو عدد موقع الخطأ. ▲

مبرهنة (٦,٦,٤)

لتكن C هي الشفرة $RS(2^r, \delta)$ المستخدمة في إرسال رسائل. ولنفرض أن w كلمة مستقبلة تحتوي على عدد ε من الكلمات الممحوّة وعدد e من الأخطاء التي ليست كلمات ممحوّة. إذا كان $2e + \varepsilon \leq \delta - 1$ فعندئذ، نستطيع فك تشفير w بشكل صائب.

البرهان

لنفرض أن B مجموعة مواقع الكلمات الممحوّة ولنفرض أن A مجموعة مواقع الأخطاء. حينئذ، تكون $A - B$ مجموعة مواقع الأخطاء التي ليست مواقع كلمات ممحوّة. وإذا كانت :

$$\sigma_B(x) = \prod_{i \epsilon B} (\beta^i + x)$$

كثيرة حدود مواقع الكلمات الممحوّة، فنجد أن :

$$\sigma_A(x) = \sigma_B(x)\sigma_{A-B}(x).$$

لإيجاد مواقع الخطأ نحتاج إلى معرفة جذور كثيرة الحدود $\sigma_{A-B}(x)$. وإذا كان بإمكاننا إزالة تأثير الكلمات الممحوّة على التناذرات فحينئذ، نستطيع توظيف الخوارزمية (**٦,٣,٢**) أو الخوارزمية (**٦,٥,١**) لإيجاد جذور $\sigma_{A-B}(x)$ (بعد تعديل التناذرات).

لمعرفة التناذرات المعدّلة نجري تعديلاً بسيطاً على الخوارزمية (**٦,٣,٢**) فنفرض أن $\sigma_B(x) = B_0 + B_1x + \cdots + B_{\varepsilon-1}x^{\varepsilon-1} + x^{\varepsilon}$ وأن:

$$\sigma_{A-B}(x) = A_0 + A_1x + \cdots + A_{e-1}x^{e-1} + x^e.$$

وبالطريقة نفسها التي استخدمناها للحصول على (**٦,٤**)، نقوم بضرب طرفي المعادلة $\sigma_A(x) = \sigma_B(x)\sigma_{A-B}(x)$ بالمقدار $b_i a_i^j$ حيث $m+1 \le j \le m+\delta-1$ وحيث $a_1, \cdots, a_{e+\varepsilon}$ هي أعداد مواقع الأخطاء، ثم تعويض $x = a_i$ وجمع الطرفين من $i = 1$ إلى $e+\varepsilon$ لنحصل على:

$$\begin{aligned}&\left(B_0 s_j + B_1 s_{j+1} + \cdots + B_{\varepsilon-1} s_{j+\varepsilon-1} + s_{j+\varepsilon}\right)A_0 \\ &\quad + \left(B_0 s_{j+1} + B_1 s_{j+2} + \cdots + B_{\varepsilon-1} s_{j+\varepsilon} + s_{j+\varepsilon+1}\right)A_1 + \cdots \\ &\quad + \left(B_0 s_{j+e} + B_1 s_{j+e+1} + \cdots + s_{j+e+\varepsilon}\right) = 0\end{aligned} \tag{٦,٨}$$

وبهذا نجد التناذرات المعدّلة بوضع:

$$s_j^* = B_0 s_j + B_1 s_{j+1} + \cdots + B_{\varepsilon-1} s_{j+\varepsilon-1} + s_{j+\varepsilon}.$$

لاحظ أن s_j^* مقادير معلومة لكل $m+1 \le j \le \delta-1-\varepsilon$؛ لأن s_j مقادير معلومة لكل $m+1 \le j \le m+\delta-1$ وأن $B_0 + \cdots + B_{\varepsilon-1}$ مقادير معلومة. وبما أن $2e+\varepsilon \le \delta-1$ (أي $2e \le \delta-1-\varepsilon$) فيكون بامكاننا حل نظام المعادلات الخطية (**٦,٩**) الذي نحصل عليه من (**٦,٨**) بصورة مشابهة تماماً لحل نظام المعادلات الخطية الذي حصلنا عليه من (**٦,٦**) وبذلك نحصل على المجاهيل $A_0, A_1, \cdots, A_{e-1}$.

$$\begin{bmatrix} s_{m+1}^* & s_{m+2}^* & \cdots & s_{m+e}^* \\ \vdots & \vdots & & \vdots \\ s_{m+e}^* & s_{m+e+1}^* & \cdots & s_{m+2e-1}^* \end{bmatrix} \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{e-1} \end{bmatrix} = \begin{bmatrix} s_{m+e+1}^* \\ \vdots \\ s_{m+2e}^* \end{bmatrix} \tag{٦,٩}$$

■

نقوم الآن بتعديل الخوارزمية (٦,٣,٢) كما هو مبيّن في المبرهنة (٦,٦,٤) لنحصل على خوارزمية لفك تشفير شفرة ريد وسولومن التي تحتوي على كلمات ممحوّة.

خوارزمية (٦,٦,٥) [فك تشفير الكلمات الممحوّة في الشفرة $RS(2^r,\delta)$]

لتكن C هي الشفرة $RS(2^r,\delta)$ ولتكن $c\epsilon C$ ولتكن:

$g(x)=(\beta^{m+1}+x)\cdots(\beta^{m+\delta-1}+x)$ كثيرة الحدود المولّدة التي تم ارسالها ولنفرض أن w هي الكلمة المستقبلة التي تحتوي على عدد ε من الكلمات الممحوّة حيث أعداد مواقع الكلمات الممحوّة هي عناصر المجموعة $B=\{a_1,\cdots,a_\varepsilon\}$. ولنفرض أن $\sigma_B(x)=(a_1+x)\cdots(a_\varepsilon+x)=B_0+B_1x+\cdots+B_{\varepsilon-1}x^{\varepsilon-1}+x^\varepsilon$ هي كثيرة حدود مواقع الكلمات الممحوّة. نحصل على كثيرة حدود مواقع الخطأ $\sigma_{A-B}(x)=A_0+A_1x+\cdots+A_{e-1}x^{e-1}+x^e$ بإيجاد $\sigma_A(x)=\sigma_B(x)\sigma_{A-B}(x)$ على النحو التالي:

(١) نقوم بحساب $s_j=w(\beta^j)$ لكل $m+1\le j\le m+\delta-1$.

(٢) نقوم بحساب $s_j^*=B_0s_j+B_1s_{j+1}+\cdots+B_{\varepsilon-1}s_{j+\varepsilon-1}+s_{j+\varepsilon}$ لكل $m+1\le j\le m+\delta-1-\varepsilon$.

(٣) نجد $A_0,A_1,\cdots,A_{e-1}$ بحل النظام الخطي (٦,٩).

(٤) نقوم بتنفيذ الخطوتين (٤) و (٥) من الخوارزمية (٦,٣,٢) لفك تشفير w.

بتوظيف التناذرات المعدّلة في الخوارزمية (٦,٦,٥) يكون بمقدورنا تعديل الخوارزمية (٦,٥,١) لإيجاد كثيرة حدود الخطأ في حالة وجود كلمات ممحوّة.

خوارزمية (٦,٦,٦) [فك تشفير بيرلكامب ومايسي بوجود كلمات ممحوّة]

لنفرض أن C هي الشفرة $RS(2^r,\delta)$ ولنفرض أن:

$g(x)=(\beta^{m+1}+x)\cdots(\beta^{m+\delta-1}+x)$ هي كثيرة الحدود المولّدة ولنفرض أن w هي الكلمة المستقبلة. ولتكن $\sigma_B(x)=B_0+B_1x+\cdots+x^\varepsilon$ كثيرة حدود موقع الخطأ

للكلمة w. يتم تعديل الخوارزمية (**٦,٥,١**) لإيجاد كثيرة حدود موقع الخطأ للكلمة w على النحو التالي:

(١) نقوم بحساب $s_j = w(\beta^j)$ لكل $m+1 \le j \le m+\delta-1$.

(٢) نقوم بحساب $s_j^* = B_0 s_j + B_1 s_{j+1} + \cdots + B_{\varepsilon-1} s_{j+\varepsilon-1} + s_{j+\varepsilon}$ لكل $m+1 \le j \le m+\delta-1-\varepsilon$.

(٣) نضع
$$q_{-1}(x) = 1 + s_{m+1}^* x + s_{m+1}^* x^2 + \cdots + s_{m+\delta-1-\varepsilon}^* x^{m+\delta-1-\varepsilon}$$
$$q_0(x) = s_{m+1}^* + s_{m+2}^* x + \cdots + s_{m+\delta-2-\varepsilon}^* x^{m+\delta-2-\varepsilon}$$

ونعرّف $P_{-1}(x)$ ، $P_0(x)$ ، D_{-1} ، P_0 ، z_0 كما في الخطوة (٢) من الخوارزمية (**٦,٥,١**).

(٤) نكرّر الخطوة (٣) من الخوارزمية (**٦,٥,١**) لنجد $\sigma_{A-B}(x)$ مع مراعاة أن i تقع في الفترة $1 \le i \le \delta-1$.

عندئذ، تكون كثيرة حدود موقع الخطأ هي $\sigma_A(x) = \sigma_B(x)\sigma_{A-B}(x)$.

ملحوظة

لإنهاء عملية فك التشفير نوظّف الخطوة (٥) من الخوارزمية (**٦,٣,٢**) ونستخدم التناذرات الأصلية لإيجاد $b_1, b_2, \cdots, b_{\varepsilon+e}$ (من الواضح أن (**٦,٧**) هو الآن نظام معادلات خطية عدد معادلاته يساوي $\varepsilon + e$).

نستخدم في الأمثلة التالية الشفرة $\widehat{C'}$ لإرسال الرسائل وبهذا يمكن التعرف على بعض الكلمات المحوّة من بنية (تركيب) الشفرة.

مثال (٦,٦,٧)

لتكن C هي الشفرة $RS(2^4, 6)$ ولتكن $g(x) = (1+x)(\beta+x)\cdots(\beta^4+x)$ هي كثيرة الحدود المولّدة حيث استخدمت كثيرة الحدود $1 + x + x^4$ لإنشاء $GF(2^4)$. ولنفرض أن الشفرة $\widehat{C'}$ هي الشفرة المستخدمة لتشفير الرسائل. فُك تشفير الكلمة المستقبلة:

$$\widehat{w'} = 11101 \quad 11001 \quad 00101 \quad 00000 \quad 00110 \quad 10010 \quad 0\cdots0$$

الحل

عدد موقع الكلمة الممحوّة الوحيدة هنا هو β^1. ولذا فإن $\sigma_B(x) = \beta + x$.

نوظّف الآن الخوارزمية (**٦,٦,٦**) لإيجاد كثيرة حدود موقع الخطأ للكلمة:

$$w = \beta^{10}0\beta^{2}0\beta^{6}\beta^{14}0\cdots 0$$

حيث وضعنا القيمة 0 للإحداثي المقابل للكلمة الممحوّة (إن ذلك يسهّل علينا حساب التناذرات).

بما أن:

$$w(x) = \beta^{10} + \beta^2 x^2 + \beta^6 x^4 + \beta^{14} x^5$$

فنرى أن $s_4 = \beta^3, s_3 = \beta^4, s_2 = \beta^3, s_1 = 0, s_0 = \beta^5$. وبما أن $B_0 = \beta$ وأن $\mathcal{E} = 1$ فنجد من الخطوة (٢) أن $s_0^* = \beta^6$ ، $s_1^* = \beta^3$ ، $s_2^* = 0$ ، $s_3^* = \beta^{11}$. وباستخدام الطريقة المستخدمة في الخوارزمية (**٦,٥,١**) مع استخدام التناذرات المعدّلة نحصل على:

i	p_i					q_i				D_i	z_i
-1	1	β^6	β^3	0	β^{11}				1	-1	
0	β^6	β^3	0	β^{11}				1		0	-1
1	β^{10}	β^9	β^{11}				1	β^6		1	0
2	β^0	β^{11}				1	β^{12}			2	1
3	β^{10}					1	β^{14}	β^{11}		3	2
4					1	β^{11}	β^8			4	3

ونرى أن $\sigma_{A-B}(x) = \beta^8 + \beta^{11}x + x^2$. إذن،

$$\begin{aligned}\sigma_A(x) &= \sigma_B(x)\sigma_{A-B}(x)\\ &= (\beta + x)(\beta^8 + \beta^{11}x + x^2)\\ &= (\beta + x)(\beta^3 + x)(\beta^5 + x)\end{aligned}$$

وبهذا تكون أعداد موقع الخطأ هي $a_1 = \beta$ ، $a_2 = \beta^2$ ، $a_3 = \beta^5$. لإكمال فك التشفير نجد الآن b_1 ، b_2 ، b_3 بتطبيق الخطوة (٥) من الخوارزمية (**٦,٣,٢**) والتناذرات الأصلية والصيغة (**٦,٧**) فنجد:

$$\begin{bmatrix} 1 & 1 & 1 \\ \beta & \beta^3 & \beta^5 \\ \beta^2 & \beta^6 & \beta^{10} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} \beta^5 \\ 0 \\ \beta^3 \end{bmatrix}$$

أو

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & \beta^9 & \beta^2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} \beta^5 \\ \beta^6 \\ \beta^3 \end{bmatrix}$$

وبحل هذا النظام نرى أن $b_3 = \beta^3$ ، $b_2 = 1$ ، $b_1 = \beta^{12}$ وبهذا يكون فك تشفير $w(x)$ هو:

$$c(x) = w(x) + e(x)$$
$$= (\beta^{10} + \beta^2 x^2 + \beta^6 x^4 + \beta^{14} x^5) + (\beta^{12} x + x^3 + \beta^3 x^5)$$
$$c(x) \leftrightarrow \beta^{10}\beta^{12}\beta^2 1 \beta^6 10 \cdots 0$$

وبالتالي ففك تشفير $\widehat{w'}$ هو:

$$0 \cdots 0 \quad 10001 \quad 00110 \quad 10001 \quad 00101 \quad 11110 \quad 11101. \qquad \blacktriangle$$

مثال (٦,٦,٨)

إذا استخدمت الشفرة $\widehat{C'}$ المبينة في المثال (**٦,٦,٧**) لتشفير الرسائل فَفُك تشفير $\overline{f}(w) = 11101 \quad 11001 \quad 00101 \quad 00100 \quad 00110 \quad 10010 \quad 0 \cdots 0$.

الحل

كثيرة حدود موقع الكلمة المحوّة هي:

$$\sigma_B(x) = (\beta + x)(\beta^3 + x) = \beta^4 + \beta^9 x + x^2.$$

ولهذا نقوم بفك تشفير:

$$w = \beta^{10} 0 \beta^2 0 \beta^6 \beta^{14} 0 \cdots 0$$

إلى كلمة شفرة من كلمات C (مرة أخرى وضعنا القيمة 0 للإحداثي المقابل للكلمة المحوّة). بما أن $w(x) = \beta^{10} + \beta^2 x^2 + \beta^6 x^4 + \beta^{14} x^5$ فنرى أن $s_4 = \beta^3, s_3 = \beta^4, s_2 = \beta^3, s_1 = 0, s_0 = \beta^5$. باستخدام الخطوة (٢) من الخوارزمية (٦,٦,٦) نجد أن $s_0^* = \beta$ ، $s_1^* = \beta^6$ ، $s_2^* = \beta^{11}$. وبهذا نحصل على:

i	p_i					q_i			D_i	z_i
-1	1	β^1	β^6	β^{11}				1	-1	
0	β^1	β^6	β^{11}				1		0	-1
1	β^3	β^8				1	β		1	1
2	0				1	β^5			2	2
3				1	β^5				4	3

إذن، $\sigma_{A-B}(x) = \beta^5 + x$. ويكون $\sigma_A(x) = (\beta + x)(\beta^3 + x)(\beta^5 + x)$. وبالتالي نستطيع حساب قيمة الخطأ كما في المثال (٦,٦,٧). ▲

إذا كانت C هي الشفرة $RS(2^r, \delta)$ فإن مسافة الشفرة $\widehat{C^r}$ هي على الأقل 2δ وبهذا فهي تصوّب جميع أنماط الخطأ الثنائية ذوات الأوزان التي لا تزيد عن $\delta - 1$. سنبيّن الآن أنه بتنفيذ الخوارزمية (٦,٦,٦) نستطيع إيجاد أقرب كلمة شفرة للكلمة المستقبلة إذا كان عدد الأخطاء الثنائية الواقعة أثناء عملية إرسال $\hat{c}^r$ لا يزيد عن $\delta - 1$. لرؤية ذلك، نفرض أن u نمط خطأ ثنائي حيث $wt(u) \le \delta - 1$ وحيث إن u يتسبب بوقوع عدد ε من الكلمات المحوّة وعدد e من الأخطاء التي ليست كلمات محوّة. وبما أنه يجب أن يقع على الأقل خطآن في الكلمة $\widehat{w^r}$ ليحدث خطأ في w وهذا الخطأ ليس كلمة محوّة فإن $2e + \varepsilon \le \delta - 1$. بتوظيف المبرهنة (٦,٦,٤) نرى فك تشفير w صحيح (ومن ثم فك تشفير $\widehat{w^r}$). أما إذا كانت نتيجة فك تشفير $\widehat{w^r}$ باستخدام الخوارزمية (٦,٦,٦) هي كلمة شفرة $\hat{c}$ تبعد بمسافة أكبر من $\delta - 1$ عن $\widehat{w^r}$ فإننا لا نستطيع ضمان أن $\widehat{c^r}$ هي بالفعل كلمة الشفرة الأقرب إلى $\widehat{w^r}$.

تمارين

(**٦,٦,٩**) لتكن C هي الشفرة $RS(2^3,5)$ ولتكن $g(x)=(1+x)(\beta+x)(\beta^2+x)(\beta^3+x)$ حيث استخدمت كثيرة الحدود $1+x+x^3$ لإنشاء $GF(2^3)$. فُك تشفير كل من الكلمات المستقبلة التالية التي تم تشفيرها باستخدام الشفرة $\widehat{C'}$ والخوارزمية (**٦,٦,٦**).

(أ) 0000 0000 1001 0011 1111 1010 1011.

(ب) 1001 0011 1010 0011 1000 0000 1011.

(ج) 0101 1100 1100 1100 0000 1000 0101.

(د) 0000 1001 0111 1101 1011 1010 0000.

(**٦,٦,١٠**) استخدم الشفرة $\widehat{C'}$ المقدمة في المثال (**٦,٦,٧**) والخوارزمية (**٦,٦,٦**) لفك تشفير الكلمات المستقبلة التالية:

(أ) $0\cdots0$ 10100 10100 10100 11110 00111 11010 11110 11101.

(ب) $0\cdots0$ 00101 10001 00000 11011 11111 01010 00000 11000.

(ج) $0\cdots0$ 10100 11101 10100 00101 10000 10000 10000 00000.

(**٦,٦,١١**) لتكن C هي الشفرة $RS(2^4,7)$ ولتكن $g(x)=(\beta+x)\cdots(\beta^6+x)$ كثيرة الحدود المولّدة حيث استخدمت كثيرة الحدود $1+x+x^4$ لإنشاء الحقل $GF(2^4)$. فُك تشفير الكلمة المستقبلة التالية إذا علمت أن الشفرة التي استخدمت في عملية التشفير $\widehat{C'}$ هي:

$0\cdots0$ 10000 11110 11101 01001 11011 10001 11011 01011.