الفصل الخامس

شفرات BCH
BCH Codes

(٥,١) الحقول المنتهية
Finite Fields

نقدم في هذا الفصل صنفاً خاصاً من الشفرات الدورية ونوظّف حقول جالوا $GF(2^r)$ لإيجاد طريقة أخرى لفك تشفيرها.

تذكر أن كثيرة الحدود $d(x)$ تكون قاسماً أو عاملاً لكثيرة الحدود $f(x)$ إذا كان $f(x) = g(x)d(x)$. من الواضح أن 1 و $f(x)$ قاسمان (تافهان) لأي كثيرة حدود $f(x)$. يُسمى أي قاسم آخر **قاسماً غير تافه أو قاسماً فعلياً (Nontrivial or Proper Divisor)** لكثيرة الحدود $f(x)$.

نقول إن كثيرة الحدود $f(x) \epsilon K[x]$ **غير قابلة للتحليل على K (Irreducible Over K)** إذا لم يكن لها قواسم فعلية في $K[x]$. وإذا وجد لها قواسم فعلية فتكون **قابلة للتحليل على K (Reducible or Factorable Over K)**.

مثال (٥,١,١)

من الواضح أن كلاً من x و $x+1$ غير قابلة للتحليل (هذه هي كثيرات الحدود من الدرجة الأولى على K). كما أن $1+x+x^2$ غير قابلة للتحليل ؛ لأن x و $x+1$

لا تقسمانها. ولكن x قاسم لكثيرتي الحدود x^2 و $x+x^2$ وأن $1+x$ قاسم لكثيرة الحدود $1+x^2$. وبهذا نرى أن كثيرات الحدود x^2 ، $1+x^2$ ، $x+x^2$ قابلة للتحليل. ▲

لاحظ أن $1+x$ قاسم لكثيرة الحدود $f(x)$ إذا وفقط إذا كان $f(1)=0$ وأن x قاسم لكثيرة الحدود $g(x)$ إذا وفقط إذا كان $g(0)=0$. فمثلاً $1+x$ قاسم لكثيرة الحدود $f(x)=1+x^2$ لأن $f(1)=1+1=0$. نُلفت نظر القارئ إلى أن عملية إيجاد قواسم غير قابلة للتحليل لكثيرة حدود ليست بالأمر البسيط ونقصر بحثنا عن هذه القواسم في الوقت الحالي على التجريب.

مثال (٥,١,٢)

إذا كانت $f(x)=1+x+x^2+x^3$ فنرى أن $f(1)=1+1+1+1=0$ ومن ثم تكون $1+x$ قاسماً لكثيرة الحدود $f(x)$. وبالقسمة المطوّلة نجد أن $f(x)=(1+x)(1+x^2)=(1+x)^3$. أما إذا كانت $g(x)=1+x+x^3$ فنرى أن $g(0)=1\neq 0$ وأن $g(1)=1\neq 0$. وبهذا لا يوجد قواسم خطية لكثيرة الحدود $g(x)$. إذن، $g(x)$ غير قابلة للتحليل على K؛ لأنه لو كانت كثيرة الحدود من الدرجة الثالثة قابلة للتحليل لكان لها قاسم خطي. ▲

مثال (٥,١,٣)

إذا كانت $f(x)=1+x+x^4$ فنرى أن $f(0)\neq 0$ و $f(1)\neq 0$ ومن ثم ليس لها قاسم خطي. وعليه، إذا كانت $f(x)$ قابلة للتحليل فيجب أن يكون لها قاسم من الدرجة الثانية. ولكن كثيرة الحدود الوحيدة غير القابلة للتحليل من الدرجة الثانية على K هي $g(x)=1+x+x^2$. وبقسمة $f(x)$ على $g(x)$ نحصل على باق غير صفري. وبهذا نرى أن $1+x+x^2$ ليس قاسماً لكثيرة الحدود $f(x)$. إذن، $f(x)$ غير قابلة للتحليل على K. ▲

تمارين

(**٥,١,٤**) بيّن ما إذا كانت كثيرة الحدود غير قابلة للتحليل على K:

(أ) $f(x) = 1 + x^2 + x^4$ (ب) $f(x) = 1 + x^8$

(ج) $f(x) = 1 + x^2 + x^3 + x^5$ (د) $f(x) = 1 + x^2 + x^6$

(هـ) $f(x) = 1 + x^4 + x^5$ (و) $f(x) = 1 + x + x^3 + x^7$.

(**٥,١,٥**) جد جميع كثيرات الحدود غير القابلة للتحليل على K من الدرجة 3 والدرجة 4.

(**٥,١,٦**) جد جميع كثيرات الحدود غير القابلة للتحليل على K من الدرجة 5.

نقول إن كثيرة الحدود غير القابلة للتحليل على K من الدرجة $n > 1$ هي **كثيرة حدود بدائية (Primitive Polynomial)** إذا لم تكن قاسماً لكثيرة الحدود $1 + x^m$ لكل $m < 2^n - 1$. سنبيّن أن أي كثيرة حدود غير قابلة للتحليل من الدرجة n يجب أن تكون قاسماً لكثيرة الحدود $1 + x^m$ عندما يكون $m = 2^n - 1$.

مثال (٥,١,٧)

كثيرة الحدود $1 + x + x^2$ غير قابلة للتحليل ولا تقسم $1 + x^m$ لكل $m < 3 = 2^2 - 1$ وبهذا فهي بدائية. كذلك، كثيرة الحدود $1 + x + x^3$ غير قابلة للتحليل وليست قاسماً لكثيرة الحدود $1 + x^m$ لكل $m < 7 = 2^3 - 1$ وبهذا فهي بدائية. أما كثيرة الحدود $f(x) = 1 + x + x^2 + x^3 + x^4$ فهي غير قابلة للتحليل (انظر التمرين (**٥,١,٥**)) ولكن:

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

و $5 < 15 = 2^4 - 1$. إذن، $f(x) = 1 + x + x^2 + x^3 + x^4$ ليست بدائية. ▲

تذكر أن بإمكاننا تعريف الجمع والضرب لكثيرات الحدود قياس كثيرة حدود $h(x)$ من الدرجة n. لنفرض أن $K^n[x]$ هي مجموعة جميع كثيرات حدود $K[x]$ التي درجاتها أصغر من n. وبما أن كل كلمة من كلمات K^n تقابل كثيرة حدود تنتمي إلى $K^n[x]$ فبالإمكان تعريف الجمع والضرب لكلمات K^n.

نقدم في هذا الفصل بعض خصائص الحقول المنتهية التي تساعدنا على إنشاء وفك تشفير بعض الشفرات. لقد سبق وعرفنا عمليتي الجمع والضرب على K^n ولكن لكي يكون هذا النظام حقلاً يجب توخي الحذر عند اختيارنا لكثيرة الحدود $h(x)$. فمثلاً، في الحقل يجب أن تتحقق خاصية الاختصار التالية: إذا كان $ab = 0$ فإن $a = 0$ أو $b = 0$.

مثال (٥,١,٨)

إذا استخدمنا عملية ضرب كثيرات الحدود قياس $1 + x^4$ لتعريف عملية ضرب كلمات K^4 فحينئذ، نرى أن:

$$\begin{aligned}(0101)(0101) &\leftrightarrow (x + x^3)(x + x^3)\\ &= x^2 + x^6\\ &\equiv (x^2 + x^2)(mod 1 + x^4)\\ &= 0\\ &\leftrightarrow 0000\end{aligned}$$

وبهذا يكون $(0101)(0101) = 0000$. ولكن $0101 \neq 0000$ في K^4. إذن، K^4 ليس حقلاً بهذا الاختيار لكثيرة الحدود. ▲

تكمن المشكلة الأساسية في المثال السابق في أن $1 + x^4$ قابلة للتحليل على K. ولكي يكون K^n حقلاً تحت عملية الضرب المبيّنة، يجب أن تكون كثيرة حدود القياس كثيرة حدود من الدرجة n غير قابلة للتحليل. في هذه الحالة يكون هذا الحقل هو حقل جالوا $GF(2^n)$ ونترك اثبات ذلك لمقرر في الجبر المجرد.

مثال (٥,١,٩)

إذا استخدمنا كثيرة الحدود غير القابلة للتحليل $h(x) = 1 + x + x^4$ لتعريف عملية الضرب في K^4 فنجد أن:

$$\begin{aligned}(1101)(0101) &\leftrightarrow (1 + x + x^3)(x + x^3)\\ &= x + x^2 + x^3 + x^6\\ &\equiv x(mod 1 + x + x^4)\end{aligned}$$

وبهذا نرى أن $x \leftrightarrow 0100 = (1101)(0101)$. ▲

تمارين

(٥,١,١٠) باستخدام $h(x) = 1 + x + x^4$ لتعريف عملية الضرب في K^4. احسب حواصل الضرب التالية:

(أ) $(0011)(1011)$ (ب) $(1110)(1001)$

(ج) $(1010)(0110)$ (د) $(0100)(0010)$

(هـ) $(1110)(0111)$ (و) $(1111)(0001)$.

(٥,١,١١) جد حواصل ضرب جميع عناصر K^2 مُستخدماً $1 + x + x^2$ لتعريف عملية الضرب (أي أنشئ جدول الضرب).

مثال (٥,١,١٢)

في هـذا المثال، نقوم بإنشاء $GF(2^3)$ باستخدام كثيرة الحدود البدائية $h(x) = 1 + x + x^3$ لتعريف عملية الضرب. لإنجاز ذلك نحسب $x^i (mod\ h(x))$:

الكلمة	$\leftrightarrow$	$x^i (mod\ h(x))$
100		1
010		x
001		x^2
110		$x^3 \equiv 1 + x$
011		$x^4 \equiv x + x^2$
111		$x^5 \equiv 1 + x + x^2$
101		$x^6 \equiv 1 + x^2$

لحساب $(1 + x)x^2 \leftrightarrow (110)(001)$ لاحظ أولاً أن $1 + x \equiv x^3 (mod\ h(x))$ (من الجدول المقدم سابقاً). وبهذا يكون:

$$\begin{aligned} x^2(1 + x) &\equiv x^2 \cdot x^3 \\ &\equiv x^5 \\ &\equiv 1 + x + x^2 (mod\ h(x)) \end{aligned}$$

إذن، $(110)(001) = 111$. ▲

إن استخدام كثيرة حدود بدائية لإنشاء $GF(2^r)$ أفضل من استخدام كثيرة حدود غير قابلة للتحليل وليست بدائية ويرجع السبب في ذلك إلى سهولة إجراء العمليات الحسابية في حالة استخدام كثيرة الحدود البدائية، فإذا كانت $\beta \in K^n$ تقابل كثيرة الحدود $x(mod\ h(x))$ حيث $h(x)$ بدائية من الدرجة n فيكون $\beta^i \leftrightarrow x^i(mod\ h(x))$. وبملاحظة أن $1 \equiv x^m(mod\ h(x))$ نرى أن $h(x)$ تقسم $1 + x^m$ ولكن $h(x)$ لا تقسم $1 + x^m$ لكل $m < 2^n - 1$ لكونها بدائية. إذن، $\beta^m \neq 1$ لكل $m < 2^n - 1$. وبما أن $\beta^j = \beta^i$ حيث $j \neq i$ إذا وفقط إذا كان $\beta^i = \beta^{j-i}\beta^i$ فنرى أن $\beta^{j-i} = 1$. إذن،

$$K^n\backslash\{0\} = \{\beta^i : i = 0,1,\cdots,2^n - 2\}$$

وبهذا نستطيع كتابة الكلمات غير الصفرية في K^n كقوى للعنصر β وبهذا تكون عملية الضرب في الحقل سهلة جداً.

نقول إن العنصر $\alpha \in GF(2^r)$ **بدائي (Primitive)** إذا كان $\alpha^m \neq 1$ لكل $1 \leq m < 2^r - 1$. أي أن α عنصر بدائي إذا وفقط إذا كانت جميع كلمات $GF(2^r)$ غير الصفرية قوى للعنصر α.

من النقاش المُبيّن في الفقرة السابقة نجد أن الكلمة $\beta \leftrightarrow x(mod\ h(x))$ عنصر بدائي في الحقل $GF(2^r)$ المنشأ باستخدام كثيرة الحدود البدائية $h(x)$.

مثال (٥,١,١٣)

الجدول (٥,١) يُبيّن إنشاء الحقل $GF(2^4)$ باستخدام كثيرة الحدود البدائية $h(x) = 1 + x + x^4$ حيث العناصر ممثلة كقوى للعنصر $\beta \leftrightarrow x(mod\ h(x))$. لاحظ أن $\beta^{15} = 1$.

الجدول (٥,١). إنشاء $GF(2^4)$ باستخدام $h(x) = 1 + x + x^4$.

قوى β	كثيرة الحدود في x قياس $h(x)$	الكلمة
–	0	0000
$\beta^0 = 1$	1	1000
β	x	0100
β^2	x^2	0010
β^3	x^3	0001
β^4	$1 + x \equiv x^4$	1100
β^5	$x + x^2 \equiv x^5$	0110
β^6	$x^2 + x^3 \equiv x^6$	0011
β^7	$1 + x + x^3 \equiv x^7$	1101
β^8	$1 + x^2 \equiv x^8$	1010
β^9	$x + x^3 \equiv x^9$	0101
β^{10}	$1 + x + x^2 \equiv x^{10}$	1110
β^{11}	$x + x^2 + x^3 \equiv x^{11}$	0111
β^{12}	$1 + x + x^2 + x^3 \equiv x^{12}$	1111
β^{13}	$1 + x^2 + x^3 \equiv x^{13}$	1011
β^{14}	$1 + x^3 \equiv x^{14}$	1001

يتم حساب (1101)(0110) على النحو التالي:

$$(0110)(1101) = \beta^5 \cdot \beta^7 = \beta^{12} = 1111$$

لأن $(x + x^2)(1 + x + x^3) \equiv x^5 \cdot x^7 = x^{12} (mod\ h(x))$. ▲

تمارين

(٥,١,١٤) استخدم الجدول **(٥,١)** لحساب حواصل الضرب في K^4 للعناصر المقدمة في التمرين **(٥,١,١٠)**.

(٥,١,١٥) أنشئ الحقول التالية بأسلوب المثال **(٥,١,١٣)**:

(أ) $GF(2^2)$.

(ب) $GF(2^3)$ باستخدام $h(x) = 1 + x^2 + x^3$.

(ج) $GF(2^4)$ باستخدام $h(x) = 1 + x^3 + x^4$.

(د) $GF(2^5)$ باستخدام $h(x) = 1 + x^2 + x^5$.

(٥,١,١٦) إذا كانت $h(x)\epsilon K[x]$ كثيرة حدود غير قابلة للتحليل من الدرجة n فأثبت وجود $m \leq 2^n - 1$ بحيث تقبل كثيرة الحدود $1 + x^m$ القسمة على $h(x)$.

(٥,١,١٧) جد جميع العناصر البدائية في الحقل $GF(2^4)$ (انظر الجدول **(٥,١)**).

(٥,١,١٨) أثبت أن $\beta^i \epsilon GF(2^r)$ عنصر بدائي إذا وفقط إذا كان $gcd(i, 2^r - 1) = 1$.

(٥,٢) كثيرات الحدود الأصغرية

Minimal Polynomials

نعلم أنه إذا كان $GF(2^r) = F\epsilon\alpha$ فإن α جذر لكثيرة الحدود $p(x)\epsilon F[x]$ إذا وفقط إذا كان $p(\alpha) = 0$. أي أنه إذا كانت $p(x) = a_0 + a_1 x + \cdots + a_k x^k = 0$ فإن $p(\alpha) = a_0 + a_1\alpha + \cdots + a_k\alpha^k = 0$.

مثال (٥,٢,١)

لنفرض أن $p(x) = 1 + x^3 + x^4$ وأن β هو العنصر البدائي في الحقل $GF(2^4)$ المنشأ باستخدام كثيرة الحدود $h(x) = 1 + x + x^4$ (انظر الجدول **(٥,١)**). عندئذ،

$$\begin{aligned} p(\beta) = 1 + \beta^3 + \beta^4 &= 1000 + 0001 + 1100 \\ &= 0101 \\ &= \beta^9 \end{aligned}$$

ولذا فإن β ليس جذراً لكثيرة الحدود $p(x)$. ولكن:

$$\begin{aligned} p(\beta^7) &= 1 + (\beta^7)^3 + (\beta^7)^4 \\ &= 1 + \beta^{21} + \beta^{28} \\ &= 1 + \beta^6 + \beta^{13} \qquad (\text{لأن } \beta^{15} = 1) \\ &= 1000 + 0011 + 1011 + 0000 = 0 \end{aligned}$$

وعليه يكون β^7 جذراً لكثيرة الحدود $p(x)$. لاحظ أننا استخدمنا $1 \leftrightarrow 1000$ و $0 \leftrightarrow 0000$ و $\beta^{15} = 1$. فمثلاً، لدينا $\beta^{21} = \beta^{15}\beta^6 = 1 \cdot \beta^6 = \beta^6$. أيضاً، $\beta^{28} = \beta^{15}\beta^{13} = 1 \cdot \beta^{13} = \beta^{13}$. ▲

ليكن $\alpha \epsilon GF(2^r) \neq 0$. تُعرف **رتبة العنصر α (Order of α)** غير الصفري على أنها أصغر عدد صحيح موجب m يحقق $\alpha^m = 1$. إذا كان m هو رتبة العنصر غير الصفري $\alpha \epsilon GF(2^r)$ فنرى أن $m \leq 2^r - 1$. وعلى وجه الخصوص يكون α عنصراً بدائياً إذا كان $m = 2^r - 1$.

تُعرف **كثيرة حدود الأصغرية $\alpha \epsilon GF(2^r)$ (Minimal Polynomial of α)** على أنها كثيرة الحدود في $K[x]$ ذات الدرجة الصغرى التي يكون α جذراً لها، ويُرمز لها بالرمز $m_\alpha(x)$. لاحظ أنه إذا كانت رتبة α تساوي m (أي، $\alpha^m = 1$) فإن α جذر لكثيرة الحدود $1 + x^m$. عليه، فكل عنصر من عناصر $GF(2^r)$ هو جذر لكثيرة حدود ما في $K[x]$.

تُساعدنا الحقائق التالية في إيجاد كثيرات الحدود الأصغرية لعناصر الحقل $GF(2^r)$.

مبرهنة (٥,٢,٢)

ليكن $\alpha \neq 0$ عنصراً في الحقل $GF(2^r)$ ولتكن $m_\alpha(x)$ كثيرة حدود α الأصغرية. عندئذ:

(أ) $m_\alpha(x)$ غير قابلة للتحليل على K.

(ب) إذا كانت $f(x) \epsilon K[x]$ حيث $f(\alpha) = 0$ فإن $m_\alpha(x)$ تقسم $f(x)$.

(ج) $m_\alpha(x)$ وحيدة.

(د) $m_\alpha(x)$ تقسم $1 + x^{2^r - 1}$.

البرهان

(أ) لنفرض أن $m_\alpha(x) = g(x)h(x)$. عندئذ، $m_\alpha(\alpha) = g(\alpha)h(\alpha) = 0$ ونرى أن $g(\alpha) = 0$ أو $h(\alpha) = 0$. بما أن $m_\alpha(x)$ أصغرية حيث $m_\alpha(\alpha) = 0$ فنجد أن $g(x) = 1$ أو $h(x) = 1$. وبهذا تكون $m_\alpha(x)$ غير قابلة للتحليل.

(ب) باستخدام خوارزمية القسمة نجد أن:

$$f(x) = m_\alpha(x)g(x) + r(x)$$

حيث $r(x) = 0$ أو $deg\, r(x) < deg\, m_\alpha(x)$. الآن

$$\begin{aligned} 0 = f(\alpha) &= m_\alpha(x)g(\alpha) + r(\alpha) \\ &= 0 \cdot g(\alpha) + r(\alpha) = r(\alpha) \end{aligned}$$

وباستخدام أصغرية درجة $m_\alpha(x)$ نرى أن $r(x) = 0$. وبهذا نرى أن $m_\alpha(x)$ تقسم $f(x)$.

(ج) لنفرض أن $m'(x)$ كثيرة حدود أصغرية أخرى للعنصر α. عندئذ، باستخدام الفقرة (ب) نرى أن $m'(x)$ تقسم $m_\alpha(x)$ وأن $m_\alpha(x)$ تقسم $m'(x)$. وبهذا يكون $m_\alpha(x) = m'(x)$. ونخلص إلى أن $m_\alpha(x)$ وحيدة.

(د) لنفرض أن β عنصر بدائي في الحقل $GF(2^r)$ وأن $\alpha = \beta^i$. عندئذ،

$$\alpha^{2^r-1} = (\beta^i)^{2^r-1} = (\beta^{2^r-1})^i = 1^i = 1$$

ونرى أن α جذر لكثيرة الحدود $1 + x^{2^r-1}$. واستناداً إلى الفقرة (ب) نجد أن $m_\alpha(x)$ قاسم لكثيرة الحدود $1 + x^{2^r-1}$. ■

لإيجاد كثيرة حدود α الأصغرية حيث $\alpha \epsilon GF(2^r)$ يكفي أن نجد تركيباً خطياً للمتجهات $\{1, \alpha, \alpha^2, \cdots, \alpha^r\}$ حيث $1 + \alpha + \alpha^2 + \cdots + \alpha^r = 0$. إن ضمان وجود مثل هذا التركيب الخطي يرجع إلى أن أي مجموعة جزئية من K^r عدد عناصرها $r + 1$ يجب أن تكون مرتبطة خطياً.

عند استخدام كثيرة حدود بدائية لإنشاء $GF(2^r)$ يكون من الطبيعي تمثيل $m_\alpha(x)$ بكثيرة الحدود $m_i(x)$ حيث $\alpha = \beta^i$. سنوضح ذلك في المثال التالي.

مثال (٥,٢,٣)

ليكن $\alpha = \beta^3 \epsilon GF(2^4)$ حيث استخدمنا $h(x) = 1 + x + x^4$ لإنشاء $GF(2^4)$ (انظر الجدول (٥,١)). كثيرة حدود α الأصغرية هي:

$$m_\alpha(x) = m_3(x) = a_0 + a_1 x + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4$$

ولإيجادها يتوجب علينا إيجاد القيم $a_0, a_1, \cdots, a_4 \epsilon \{0,1\}$. وبملاحظة أن:

$$\begin{aligned} m_\alpha(\alpha) = 0 &= a_0 1 + a_1 + a_2 + a_3 + a_4 \\ &= a_0\beta^0 + a_1\beta^3 + a_2\beta^6 + a_3\beta^9 + a_4\beta^{12} \end{aligned}$$

نرى أن:

$$a_0(1000) + a_1(0001) + a_2(0011) + a_3(0101) + a_4(1111) = 0000.$$

وبحل هذا النظام لإيجاد a_0, a_1, a_2, a_3, a_4 نحصل على $a_0 = a_1 = a_2 = a_3 = a_4 = 1$.

وبهذا تكون $m_\alpha(x) = 1 + x + x^2 + x^3 + x^4$. جذور $m_\alpha(x)$ هي:

$$\left\{\alpha, \alpha^2, \alpha^4, \alpha^8\right\} = \{\beta^3, \beta^6, \beta^{12}, \beta^9\}.$$

وعليه يكون:

$m_3(x) = m_6(x) = m_9(x) = m_{12}(x)$ حيث $m_i(x)$ هي كثيرة حدود β^i الأصغرية. ▲

إذا أردنا إيجاد كثيرات الحدود الأصغرية لجميع عناصر $GF(2^4)$ فنحتاج إلى الحقائق المهمة التالية: تذكر أن $f(x)^2 = f(x^2)$. عندئذ،

$$\left(\sum_{i=0}^{n} a_i x^i\right)^2 = \sum_{i=0}^{n} a_i^2 (x^i)^2 = \sum_{i=0}^{n} a_i (x^2)^i$$

حيث استخدمنا الحقيقة $(a+b)^2 = a^2 + b^2$ والحقيقة $a_i^2 = a_i$ ؛ لأن $a_i \epsilon \{0,1\}$.

عندئذ، إذا كان $f(\alpha) = 0$ فنرى أن $f(\alpha^2) = (f(\alpha))^2 = 0$ ويكون α^2 جذراً آخر لكثيرة الحدود $f(x)$. وبالمثل $f(\alpha^4) = (f(\alpha^2))^2 = 0$ وهكذا. وبهذا نرى أنه إذا كان α

جذراً لكثيرة الحدود $f(x)$ فإن $\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^i}$ جذور لها أيضاً. وبقليل من الجهد يمكن إثبات:

مبرهنة (٥,٢,٤)

إذا كانت $m_\alpha(x)$ كثيرة حدود $\alpha \epsilon GF(2^r)$ الأصغرية فإن $\left\{\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{r-1}}\right\}$ هي جميع جذور $m_\alpha(x)$. وعلى وجه الخصوص درجة $m_\alpha(x)$ تساوي $\left|\left\{\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{r-1}}\right\}\right|$.

مثال (٥,٢,٥)

لنفرض أن $m_5(x)$ كثيرة حدود $\alpha = \beta^5$ حيث α عنصر في الحقل $GF(2^4)$ المنشأ في الجدول (٥,١). استناداً إلى المبرهنة (٥,٢,٤) نجد أن $\left\{\alpha, \alpha^2, \alpha^4, \alpha^8\right\} = \{\beta^5, \beta^{10}\}$ هي جميع جذور $m_5(x)$ وبهذا نرى أن $deg(m_5(x)) = 2$ وذلك من المبرهنة (٥,٢,٤). إذن، $m_5(x) = a_0 + a_1 x + a_2 x^2$. ونرى أن:

$$\begin{aligned} 0 &= a_0 + a_1\beta^5 + a_2\beta^{10} \\ &= a_0(1000) + a_1(0110) + a_2(1110) \end{aligned}$$

وبحل هذا النظام نجد أن $a_0 = a_1 = a_2 = 1$. إذن، $m_5(x) = 1 + x + x^2$.

وبالأسلوب نفسه نستطيع إيجاد كثيرات الحدود الأصغرية لبقية عناصر الحقل $GF(2^4)$ المنشأ باستخدام $h(x) = 1 + x + x^4$ والجدول (٥,٢) يُبيّن ذلك.

الجدول (٥,٢). كثيرات الحدود الأصغرية لعناصر $GF(2^4)$.

عناصر $GF(2^4)$	كثيرات الحدود الأصغرية
0	x
1	$1 + x$
$\beta, \beta^2, \beta^4, \beta^8$	$1 + x + x^4$
$\beta^3, \beta^6, \beta^9, \beta^{12}$	$1 + x + x^2 + x^3 + x^4$
β^5, β^{10}	$1 + x + x^2$
$\beta^7, \beta^{11}, \beta^{13}, \beta^{14}$	$1 + x^3 + x^4$

▲

تمارين

(**٥,٢,٦**) تحقق من صواب الجدول (**٥,٢**) للحقل $GF(2^4)$.

(**٥,٢,٧**) جد كثيرة الحدود الأصغرية لكل من عناصر $GF(2^3)$ المنشأ باستخدام $p(x) = 1 + x + x^3$ (انظر التمرين (**٥,١,١٥**)).

(**٥,٢,٨**) جد كثيرة الحدود الأصغرية لكل من عناصر $GF(2^4)$ المنشأ باستخدام $p(x) = 1 + x^3 + x^4$ (انظر التمرين (**٥,١,١٥**)).

(**٥,٢,٩**) جد كثيرة الحدود الأصغرية لكل من عناصر $GF(2^5)$ المنشأ باستخدام $p(x) = 1 + x^2 + x^5$ (انظر التمرين (**٥,١,١٥**)).

(**٥,٢,١٠**) أثبت أن $1 + x + x^2 = (\beta^5 + x)(\beta^{10} + x)$ (استخدم الجدول (**٥,١**)).

(**٥,٢,١١**) أثبت أن $m_\alpha(x)$ كثيرة حدود بدائية إذا وفقط إذا كان α عنصراً بدائياً.

(٥,٣) شفرات هامينغ الدورية
Cyclic Hamming Codes

رأينا سابقاً أن شفرات هامينغ تتمتع بخصائص مهمة فهي شفرات تامة وتستطيع تصويب خطأ واحد وعملية فك التشفير سهلة. في هذا البند سنثبت وجود شفرة هامينغ دورية من الطول $n = 2^r - 1$ لكل $r \geq 2$ مما يؤدي إلى سهولة التشفير لهذه الشفرات (كشفرات دورية).

تتكون مصفوفة اختبار النوعية لشفرة هامينغ من الطول $n = 2^r - 1$ من عدد $2^r - 1$ صفاً من الكلمات غير الصفرية من الطول r. إذا كان β عنصراً بدائياً في الحقل $GF(2^r)$ فنجد من التعريف أن جميع قوى β مختلفة ولذلك يكون بمقدورنا إنشاء شفرة هامينغ من الطول $n = 2^r - 1$ بحيث تكون مصفوفة اختبار النوعية لها هي المصفوفة:

$$\begin{bmatrix} 1 \\ \beta \\ \beta^2 \\ \vdots \\ \beta^{2^r-2} \end{bmatrix}$$

لاحظ أن درجة H تساوي $(2^r-1)\times r$. لاحظ أيضاً أنه إذا كانت $w = w_0 w_1 \cdots w_{n-1}$ كلمة مستقبلة فإن $wH = w_0\beta^0 + w_1\beta^1 + \cdots + w_{n-1}\beta^{n-1}$. وبهذا تكون w كلمة شفرة إذا وفقط إذا كانت β جذراً لكثيرة الحدود $w(x)$. إذن، استناداً إلى المبرهنة **(٥,٢,٢)** (ب) نجد أن $m_\beta(x)$ تقسم جميع كلمات الشفرة وهي كلمة شفرة بحد ذاتها. وبهذا تكون شفرة هامينغ دورية مولّدة بكثيرة الحدود $m_\beta(x)$ ونكون قد أثبتنا المبرهنة التالية:

مبرهنة (٥,٣,١)

أي كثيرة حدود بدائية من الدرجة r هي كثيرة حدود مولّدة لشفرة هامينغ الدورية من الطول $2^r - 1$. ■

مثال (٥,٣,٢)

لنفرض أن $r = 3$. عندئذ، $n = 2^3 - 1 = 7$. باستخدام $p(x) = 1 + x + x^3$ لإنشاء $GF(2^3)$ و $\beta \leftrightarrow 010$ كعنصر بدائي $(\beta^i \longleftrightarrow x^i (mod\ p(x))$ نجد أن مصفوفة اختبار النوعية لشفرة هامينغ من الطول 7 هي:

$$\begin{bmatrix} 1 \\ \beta \\ \beta^2 \\ \beta^3 \\ \beta^4 \\ \beta^5 \\ \beta^6 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 111 \\ 101 \end{bmatrix}$$

وهي مصفوفة اختبار النوعية نفسها للشفرة الدورية المولّدة بكثيرة الحدود $p(x) = m_\beta(x)$. ▲

فك تشفير شفرة هامينغ الدورية أمر يسير، فإذا كانت كثيرة الحدود المولّدة هي كثيرة الحدود البدائية $m_\alpha(x)$ وكانت $w(x)$ هي الكلمة المستقبلة فنرى أن $w(x) = c(x) + e(x)$ حيث $c(x)$ كلمة شفرة و $w(\alpha) = e(\alpha)$. وبما أن وزن e يساوي 1 فنرى أن $e(\alpha) = \alpha^j$ حيث j هو موقع الإحداثي 1 في الكلمة e، وذلك باستخدام الترقيم $0,1,\cdots,n$ لمواقع إحداثيات e. إذن، كثيرة حدود الخطأ هي على الأرجح $e(x) = x^j$. وبهذا يكون $c(x) = w(x) + x^j$.

مثال (٥,٣,٣)

لنفرض أن الحقل $GF(2^3)$ أنشئ باستخدام $1 + x + x^3$. عندئذ، $m_1(x) = 1 + x + x^3$ هي كثيرة حدود مولّدة لشفرة هامينغ الدورية من الطول 7. لنفرض أن الكلمة المستقبلة هي $w(x) = 1 + x + x^3 + x^6$. حينئذ،

$$\begin{aligned} w(\beta) &= 1 + \beta^2 + \beta^3 + \beta^6 \\ &= 100 + 001 + 110 + 101 \\ &= 110 \\ &= \beta^3 \end{aligned}$$

إذن، $e(x) = x^3$ ويكون $c(x) = w(x) + x^3 = 1 + x^2 + x^6$. ▲

تمارين

(٥,٣,٤) جد مصفوفة اختبار النوعية لشفرة هامينغ الدورية من الطول 7 باستخدام $GF(2^3)$ المنشأ بكثيرة الحدود $1 + x + x^3$ حيث كثيرة الحدود المولّدة هي $m_3(x)$. وإذا كانت $w(x) = x + x^2 + x^4$ هي الكلمة المستقبلة فجد كلمة الشفرة $c(x)$ التي تكون على الأرجح قد أُرسلت.

(٥,٣,٥) أعد التمرين **(٥,٣,٤)** إذا استخدمت $p(x) = 1 + x^2 + x^3$ لإنشاء $GF(2^3)$ وكانت $m_1(x)$ هي كثيرة الحدود المولّدة.

(٥,٣,٦) أعد التمرين (٥,٣,٤) إذا استخدمت $p(x) = 1 + x^2 + x^3$ لإنشاء $GF(2^3)$ وكانت $m_3(x)$ هي كثيرة الحدود المولّدة.

(٥,٣,٧) أنشئ مصفوفة اختبار النوعية لشفرة هامينغ الدورية من الطول 15.

(٥,٣,٨) جد كثيرة حدود مولّدة لشفرة هامينغ الدورية من الطول 15 التي جذورها $1, \beta^7, \beta^5 \epsilon GF(2^4)$ (استخدمت $1 + x + x^4$ لإنشائه). أنشئ مصفوفة اختبار النوعية لهذه الشفرة. أثبت أن $c(x) \epsilon C$ إذا وفقط إذا كان $wt(c)$ زوجياً.

(٥,٣,٩) أثبت أن وزن كلمة شفرة من شفرة دورية يكون زوجياً إذا وفقط إذا كان $1 + x$ قاسماً لكثيرة الحدود المولّدة.

من المناسب التنويه هنا عن إمكانية استخلاص نتائج أعم مما حصلنا عليه في هذا البند. لتكن C شفرة دورية طولها n ولتكن $g(x)$ كثيرة حدودها المولّدة. لنفرض أن $\epsilon \alpha GF(2^r)$ جذر لكثيرة الحدود $g(x)$. عندئذ، $c(\alpha) = 0$ لكل $c(x) \epsilon C$. واستناداً إلى المبرهنة (٥,٢,٢) (ب) نرى أن $m_\alpha(x)$ تقسم $c(x)$. وبما أنه من الممكن دائماً كتابة $g(x)$ كحاصل ضرب كثيرات حدود أصغرية لعناصر من $GF(2^r)$ فنرى إمكانية استخدام ذلك لإنشاء مصفوفة اختبار النوعية وإيجاد خوارزمية لفك الشفرة C. سنناقش الحالة $g(x) = m_\beta(x) m_{\beta^3}(x)$ في البند (٥,٤).

(٥,٤) شفرات BCH

BCH Codes

شفرات **بوسيه وتشودري وهوكنـــهام (Bose-Chaudhuri-Hocquengham)** أو اختصاراً شفرات BCH هي صنف مهم من الشفرات التي تصوّب عديدًا من الأخطاء. سنبدأ بإنشاء وفك تشفير شفرات خاصة من هذا الصنف تصوّب خطأين ونرجئ دراسة شفرات BCH العامة إلى وقت لاحق.

هناك سببان يجعلان شفرات BCH في غاية الأهمية، أولهما وجود خوارزمية سهلة نسبياً لفك تشفيرها والسبب الآخر هو الانتشار الواسع لهذه الشفرات. في واقع الأمر، لكل عددين صحيحين موجبين r و t حيث $t \leq 2^{r-1} - 1$ توجد شفرة BCH من الطول $n = 2^r - 1$ والبُعد $k \geq n - rt$ التي تصوّب أخطاء من النوع t.

شفرة BCH من الطول $2^r - 1$ التي تصوّب خطأين هي الشفرة الخطية الدورية المولّدة بكثيرة الحدود $g(x) = m_\beta(x)m_{\beta^3}(x)$ حيث β عنصر بدائي في الحقل $GF(2^r)$ ، $r \geq 4$. لاحظ أن $g(x)$ كثيرة حدود مولّدة لشفرة دورية ؛ لأن $n = 2^r - 1$ و $g(x)$ تقسم $1 + x^n$ (انظر المبرهنة (٥,٢,٢) (ج)).

مثال (٥,٤,١)

لنفرض أن $GF(2^4)$ هو الحقل المنشأ باستخدام $p(x) = 1 + x + x^4$ (انظر الجدول (٥,١)).

حينئذ، β عنصر بدائي و $m_1(x) = 1 + x + x^4$ و $m_3(x) = 1 + x + x^2 + x^3 + x^4$.

إذن،

$$g(x) = m_1(x)m_3(x) = 1 + x^4 + x^6 + x^7 + x^8$$

هي كثيرة حدود مولّدة لشفرة BCH من الطول 15 التي تصوّب خطأين. ▲

تمارين

(٥,٤,٢) شفرات BCH التي تصوّب خطأين معرّفة عندما يكون $r \geq 4$. ما هي الشفرة التي تولّدها $g(x) = m_1(x)m_3(x)$ في الحالة $r = 3$.

(٥,٤,٣) ليكن β عنصراً بدائياً في الحقل $GF(2^4)$ المنشأ باستخدام كثيرة الحدود غير القابلة للتحليل $p(x) = 1 + x^3 + x^4$. جد كثيرة حدود مولّدة $g(x)$ لشفرة BCH من الطول 15 التي تصوّب خطأين مُستخدماً هذا التمثيل للحقل $GF(2^4)$. أي جد $g(x) = m_1(x)m_3(x)$ (انظر التمرين (٥,١,١٥)).

(٥,٤,٤) استخدم كثيرة الحدود غير القابلة للتحليل $1 + x^2 + x^5$ لإنشاء $GF(2^5)$ ثم جد كثيرة حدود مولّدة لشفرة BCH من الطول 31 التي تصوّب خطأين (انظر التمرين **(٥,١,١٥)**).

تمهيدية (٥,٤,٥)

المصفوفة التالية H هي مصفوفة اختبار النوعية لشفرة BCH من الطول $2^r - 1$ التي تصوّب خطأين حيث β عنصر بدائي في الحقل $GF(2^r)$ و $g(x) = m_1(x)m_3(x)$ كثيرة الحدود المولّدة.

$$H = \begin{bmatrix} \beta^0 & \beta^0 \\ \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \vdots \\ \beta^i & \beta^{3i} \\ \vdots & \vdots \\ \beta^{2^r-2} & \beta^{3(2^r-2)} \end{bmatrix}$$

البرهان

بما أن $\beta^i \epsilon GF(2^r)$ فهي تمثل كلمة طولها r ونرى أن H مصفوفة من الدرجة $(2^r - 2) \times (2r)$. وبما أن $deg(m_1(x)) = r = deg(m_3(x))$ فنجد أن درجة $g(x) = m_1(x)m_3(x)$ تساوي $2r$. وبهذا يكون بُعد الشفرة هو $n - 2r = 2^r - 1 - 2r$.

سنترك إثبات أن درجة $m_3(x)$ تساوي r للتمرين **(٥,٤,٩)**. ■

على سبيل المثال، إذا استخدمنا الحقل $GF(2^4)$ المنشأ في الجدول **(٥,١)** باستخدام كثيرة الحدود البدائية $p(x) = 1 + x + x^4$ لإنشاء شفرة BCH لتصويب خطأين C_{15} نجد أن C_{15} هي الشفرة الخطية التي لها مصفوفة اختبار النوعية H من الدرجة 8×15 وكثيرة الحدود المولّدة $m_1(x)m_3(x)$ (انظر الجدول **(٥,٣)**).

الجدول (٥,٣). مصفوفة اختبار النوعية للشفرة C_{15}.

$$\begin{bmatrix} 1 & 1 \\ \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \beta^3 & \beta^9 \\ \beta^4 & \beta^{12} \\ \beta^5 & 1 \\ \beta^6 & \beta^3 \\ \beta^7 & \beta^6 \\ \beta^8 & \beta^9 \\ \beta^9 & \beta^{12} \\ \beta^{10} & 1 \\ \beta^{11} & \beta^3 \\ \beta^{12} & \beta^6 \\ \beta^{13} & \beta^9 \\ \beta^{14} & \beta^{12} \end{bmatrix} \longleftrightarrow \begin{bmatrix} 1000 & 1000 \\ 0100 & 0001 \\ 0010 & 0011 \\ 0001 & 0101 \\ 1100 & 1111 \\ 0110 & 1000 \\ 0011 & 0001 \\ 1101 & 0011 \\ 1010 & 0101 \\ 0101 & 1111 \\ 1110 & 1000 \\ 0111 & 0001 \\ 1111 & 0011 \\ 1011 & 0101 \\ 1001 & 1111 \end{bmatrix} = H$$

مبرهنة (٥,٤,٦)

لكل عدد صحيح $r \geq 4$ توجد شفرة BCH من الطول $n = 2^r - 1$ والبُعد $k = 2^r - 2r - 1$ التي تصوّب خطأين ومسافتها تساوي 5 وكثيرة حدودها المولّدة هي $m_1(x)m_3(x)$.

البرهان

إثبات أن المسافة تساوي 5 نحصل عليه من كون الشفرة تصوّب خطأين ومن ثم فإن مسافتها على الأقل 5. ومن تعريف مصفوفة اختبار النوعية نرى أن $n = 2^r - 1$. وبملاحظة أن درجة كل من $m_1(x)$ و $m_3(x)$ تساوي r نجد أن درجة $g(x)$ تساوي $n - k = 2r$ وبهذا يكون $k = 2^r - 2r - 1$. ■

تمارين

(٥,٤,٧) أثبت أن أعمدة مصفوفة اختبار النوعية للشفرة C_{15} المبينة في الجدول **(٥,٣)** مُستقلة خطياً ومن ثم بُعد C_{15} هو $k = 7$.

(٥,٤,٨) استخدم مصفوفة اختبار النوعية لإثبات أن مسافة C_{15} هي $d = 5$.

(٥,٤,٩) إذا كان β عنصراً بدائياً في الحقل $GF(2^r)$ حيث $r > 2$ فأثبت أن:

$$\left|\left\{\beta^{2^i}: 0 \le i \le r-1\right\}\right| = r$$

وأن

$$\left|\left\{(\beta^3)^{2^i}: 0 \le i \le r-1\right\}\right| = r$$

واستنتج أن درجة كل من $m_1(x)$ و $m_3(x)$ تساوي r.

(٥,٤,١٠) بيّن ما إذا كانت الكلمات التالية من الطول 15 هي كلمات تنتمي إلى الشفرة C_{15} حيث $g(x) = 1 + x^4 + x^6 + x^7 + x^8$.

(أ) 011001011000010 (ب) 000111010000110

(ج) 011100000010001 (د) 111111111111111.

(٥,٥) فك تشفير شفرة BCH التي تصوّب خطأين

Decoding 2 Error-Correcting BCH Code

نقدم خوارزمية لفك تشفير BCH التي تصوّب خطأين المقدمة في البند السابق.

في هذا البند نطابق الكلمة الثنائية من الطول r مع قوة β المقابلة لها. مصفوفة اختبار النوعية لشفرة BCH التي تصوّب خطأين من النوع $(2^r - 1, 2^r - 2r - 1, 5)$ والتي كثيرة حدودها المولّدة $g(x) = m_1(x)m_3(x)$ هي المصفوفة H المقدمة في التمهيدية (٥,٤,٥).

لنفرض أن w هي الكلمة المستقبلة وأن $w \leftrightarrow w(x)$. عندئذ، تناذر w هو:

$$wH = [w(\beta), w(\beta^3)] = [s_1, s_3]$$

حيث s_1 و s_3 كلمتان طول كل منهما يساوي r.

إذا لم يحدث خطأ في الإرسال فنرى أن التناذر $wH = 0$ ويكون $s_1 = s_3 = 0$.

إذا وقع خطأ واحد فقط أثناء عملية الإرسال فإن كثيرة حدود الخطأ هي $e(x) = x^i$ ونرى أن $wH = eH = [e(\beta), e(\beta^3)] = [\beta^i, \beta^{3i}] = [s_1, s_3]$.

وبهذا يكون $s_1^3 = s_3$. أما إذا وقع خطآن أثناء عملية الإرسال في الموقعين i و j حيث $i \neq j$ فنجد أن $e(x) = x^i + x^j$ وأن $wH = eH = [e(\beta), e(\beta^3)] = [s_1, s_3]$.

وبهذا نرى أن تناذر wH هو $wH = [s_1, s_3] = [\beta^i + \beta^j, \beta^{3i} + \beta^{3j}]$.

ونحصل على نظام المعادلات:

$$\beta^i + \beta^j = s_1$$
$$\beta^{3i} + \beta^{3j} = s_3$$

ولكن لدينا التحليل:

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

و

$$s_1^2 = (\beta^i + \beta^j)^2 = \beta^{2i} + \beta^{2j}$$

إذن،

$$\begin{aligned} s_3 &= \beta^{3i} + \beta^{3j} \\ &= (\beta^i + \beta^j)(\beta^{2i} + \beta^{2j} + \beta^{i+j}) \\ &= s_1(s_1^2 + \beta^{i+j}) \end{aligned}$$

وبهذا نرى أن:

$$\frac{s_3}{s_1} + s_1^2 = \beta^{i+j}.$$

ولكن β^i و β^j جذرا المعادلة التربيعية:

$$x^2 + (\beta^i + \beta^j)x + \beta^{i+j} = 0.$$

ومن ثم فهما جذرا المعادلة:

$$x^2 + s_1 x\left(\frac{s_3}{s_1} + s_1^2\right) = 0.$$

وعليه نستطيع إيجاد موقعي الخطأين بإيجاد جذري المعادلة. كثيرة الحدود في الطرف الأيسر للمعادلة تُسمى **كثيرة حدود تعيين الخطأ (Error Locator Polynomial)**.

مثال (٥,٥,١)

لنفـــرض أن $w \leftrightarrow w(x)$ كلمـــة مســـتقبلة بتنـــاذر $s_1 = 0111 = w(\beta)$ و $s_3 = 1010 = w(\beta^3)$ حيث تم تشفير w باستخدام C_{15}. باستخدام الجدول (٥,١) نجد أن $s_1 \leftrightarrow \beta^{11}$ و $s_3 \leftrightarrow \beta^8$. عندئذ،

$$\begin{aligned}\frac{s_3}{s_1} + s_1^2 &= \beta^8\beta^{-11} + \beta^{22} \\ &= \beta^{12} + \beta^7 \\ &= \beta^2\end{aligned}$$

وعليه نجد أن جذري كثيرة الحدود $x^2 + \beta^{11}x + \beta^2$ هما β^4 و β^{13}. وبهذا نستطيع تحديد موقعي الخطأ فيكونا الموقعين 4 و 13 (أي أن $e(x) = x^4 + x^{13}$). إذن، نمط الخطأ الأرجح هو:

.000010000000010 ▲

تمارين

(٥,٥,٢) أثبت أن β^4 و β^{13} هما بالفعل جذرا كثيرة الحدود $x^2 + \beta^{11}x + \beta^2 = 0$.

بيّن أيضاً أن مجموع الصفين 4 و 13 من المصفوفة H المبينة في الجدول (٥,٣) هو $[s_1, s_3]$.

(٥,٥,٣) جد جذور كثيرات الحدود التالية في الحقل $GF(2^4)$ إن أمكن ذلك (استخدم الجدول (٥,١)):

(أ) $x^2 + \beta^4x + \beta^{13}$ (ب) $x^2 + \beta^7x + \beta^2$

(ج) $x^2 + \beta^2x + \beta^5$ (د) $x^2 + \beta^6$

(هـ) $x^2 + \beta^2x$ (و) $x^2 + x + \beta^8$.

نقدم الآن خوارزمية لطريقة الاحتمالية القصوى غير التامة IMLD لفك تشفير شفرات BCH التي تصوّب خطأين. لنفرض أن w كلمة مستقبلة. الخوارزمية تتوقف في اللحظة التي يتم بها تحديد نمط الخطأ.

خوارزمية (٥,٥,٤) [فك تشفير شفرة BCH التي تصوّب خطأين]

لنفرض أن كثيرة الحدود المولّدة هي $m_1(x)m_3(x)$.

(١) احسب التناذر $wH = [s_1, s_3] = [w(\beta), w(\beta^3)]$.

(٢) إذا كان $s_1 = s_3 = 0$ فنستنتج عدم وقوع أخطاء ونخلص إلى أن $c = w$ هي كلمة الشفرة المرسلة.

(٣) إذا كان $s_1 = 0$ و $s_3 \neq 0$ فنطلب إعادة الإرسال.

(٤) إذا كان $s_1^3 = s_3$ فيتم تصويب خطأ واحد فقط في الموقع i حيث $s_1 = \beta^i$.

(٥) كوّن المعادلة التربيعية $x^2 + s_1 x + \frac{s_3}{s_1} + s_1^2 = 0$. (*)

(٦) إذا كان للمعادلة (*) جذرين مختلفين β^i و β^j فنصوّب خطئين في الموقعين i و j.

(٧) إذا لم يكن للمعادلة (*) جذرين مختلفين في الحقل $GF(2^r)$ فنخلص إلى وقوع ثلاثة أخطاء على الأقل أثناء الارسال ونطلب إعادة الإرسال.

جميع الأمثلة والتمارين التي سنناقشها تستخدم الشفرة C_{15} حيث مصفوفة اختبار النوعية مبينة في الجدول (٥,٣) وكثيرة حدودها المولّدة $g(x)$ هي المقدمة في المثال (٥,٤,١).

مثال (٥,٥,٥)

لنفرض أن w كلمة مستقبلة وأن التناذر هو:

$$wH = 01111010 \leftrightarrow [\beta^{11}, \beta^8]$$

عندئذ، $s_1^3 = (\beta^{11})^3 = \beta^{33} = \beta^3 \neq \beta^8 = s_3$.

في هذه الحالة تكون المعادلة (*) هي $x^2 + \beta^{11}x + \beta^2 = 0$ وهي المعادلة المبينة في المثال (٥,٥,١). لهذه المعادلة جذران مختلفان هما β^4 و β^{13}. إذن، نستطيع تصويب خطأين في الموقعين $i = 4$ و $j = 13$. أي أن نمط الخطأ الأرجح هو:

$u = 000010000000010$ وأن $e(x) = x^4 + x^{13}$ هي كثيرة حدود الخطأ. ▲

مثال (٥,٥,٦)

لنفـــرض أن التنـــاذر هـــو $wH = [w(\beta), w(\beta^3)] = [\beta^3, \beta^9]$. عندئـــذ، $s_1^3 = (\beta^3)^3 = \beta^9 = s_3$. إذن، نستنتج وقوع خطأ واحد على الأرجح في الموقع $i = 3$. ويكون نمط الخطأ الأرجح $u = 000010000000000$ و $e(x) = x^3$ هي كثيرة حدود الخطأ. ▲

مثال (٥,٥,٧)

لنفرض أن $w = 110111101011000$ كلمة مُستقبلة. عندئذ، التناذر هو:

$$wH = 01110110 \leftrightarrow [\beta^{11}, \beta^5] = [s_1, s_3].$$

الآن، $s_1^3 = (\beta^{11})^3 = \beta^{33} = \beta^3 \neq s_3 = \beta^5$. لايجاد المعادلة التربيعية (*) يلزمنا حساب:

$$\begin{aligned} \frac{s_3}{s_1} + s_1^2 &= \beta^5\beta^{-11} + (\beta^{11})^2 \\ &= \beta^9 + \beta^7 \\ &\leftrightarrow 0101 + 1101 \\ &= 1000 \\ &\leftrightarrow \beta^0 \end{aligned}$$

ونرى أن المعادلة (*) في هذه الحالة هي $x^2 + \beta^{11}x + \beta^0 = 0$. وبتجريب عناصر $GF(2^4)$ لإيجاد الجذور المحتملة نجد أن $x = \beta^7$ يحقق:

$$\begin{aligned} (\beta^7)^2 + \beta^{11}\beta^7 + \beta^0 &= \beta^{14} + \beta^3 + \beta^0 \\ &\leftrightarrow 1001 + 0001 + 1000 \\ &= 0000 \end{aligned}$$

وبملاحظة أن $\beta^7\beta^i = 1 = \beta^{15}$ نجد أن $\beta^i = \beta^8$ هو الجذر الآخر. إذن، يمكن تصويب خطأين في الموقعين $i = 7$ و $j = 8$ ويكون نمط الخطأ هو $u = 000000011000000$ ونخلص إلى أن $v = w + u = 110111110011000$ هي الكلمة المرسلة. ▲

مثال (٥,٥,٨)

لنفرض أنه أثناء عملية إرسال كلمة من كلمات الشفرة C_{15} قد وقعت أخطاء في المواقع 2 و 6 و 12. عندئذ، يكون التناذر wH هو مجموع الصفوف 2 ، 6 ، 12 من المصفوفة H حيث w هي الكلمة المستقبلة. حينئذ،

$$wH = 00100011 + 00110001 + 11110011$$
$$= 11100001 \leftrightarrow [\beta^{10}, \beta^3] = [s_1, s_3]$$

الآن، $s_1^3 = (\beta^{10})^3 = \beta^{30} = 1 \neq \beta^3 = s_3$. وعليه فإن:

$$\frac{s_3}{s_1} + s_1^2 = \beta^3\beta^{-10} + \beta^{20} = \beta^8 + \beta^5$$
$$\leftrightarrow 1010 + 0110 = 1100 \leftrightarrow \beta^4$$

ومن ثم فالمعادلة التربيعية هي $x^2 + \beta^{10}x + \beta^4 = 0$.

وبتجريب جميع عناصر $GF(2^4)$ نخلص إلى عدم وجود جذور لهذه المعادلة في الحقل $GF(2^4)$. إذن، تستنتج طريقة IMLD لفك تشفير C_{15} إلى وقوع ثلاثة أخطاء على الأقل أثناء الإرسال ومن ثم نطلب إعادة الإرسال. ▲

تمارين

(٥,٥,٩) تم تشفير رسائل باستخدام C_{15}. إذا كانت w هي الكلمة المستقبلة وكان wH تناذرها فحدّد مواقع الأخطاء التي حدثت أثناء الارسال (إن أمكنك ذلك).

(أ) 0100 0101 (ب) 1110 1000

(ج) 1100 1101 (د) 0100 0000

(هـ) 0000 0100 (و) 1010 0100

(ز) 0011 1101 (ح) 0000 0000.

(٥,٥,١٠) الشفرة هي C_{15}. فُك تشفير كل من الكلمات المستقبلة w التالية إن أمكن ذلك.

(أ) 11000 00000 00000 (ب) 00001 00001 00001

(ج) 01000 10101 00000 (د) 11001 11001 11000

(هـ) 11001 11001 00000 (و) 11100 00000 00001

(ز) 10111 00000 00000 (ح) 10101 00101 10001

(ط) 01000 01000 00000 (ي) 01010 10010 11000

(ك) 11011 10111 01100 (ل) 10111 00000 01000

(م) 11100 10110 00000 (ن) 00011 10100 00110.