الفصل الرابع

الشفرات الخطية الدورية
Cyclic Linear Codes

(٤,١) كثيرات الحدود والكلمات
Polynomials & Words

سيكون من الملائم تمثيل الشفرات الدورية بدلالة كثيرات الحدود. ولهذا الغرض نبدأ بمراجعة الحقائق التي نحتاجها عن كثيرات الحدود بمتغير واحد.

كثيرة الحدود من الدرجة n على K هي $a_0 + a_1x + \cdots + a_nx^n$ حيث المعاملات $a_0, a_1, \cdots, a_n$ عناصر تنتمي إلى K. يُرمز لمجموعة كثيرات الحدود على K بالرمز $K[x]$. كما يرمز لكثيرات الحدود (عناصر $K[x]$) بالرموز $f(x)$ ، $g(x)$ ، $p(x)$ وهكذا ويُرمز لدرجة كثيرة الحدود $f(x)$ بالرمز $deg(f(x))$.

عمليتا جمع وضرب كثيرات الحدود على K هما كالمعتاد مع ملاحظة أن $1 + 1 = 0$. أي أن $x^k + x^k = 0$ ومن ثم ليس بالضرورة أن تتحقق المساواة:

$$deg\big(f(x) + g(x)\big) = max\{deg\big(f(x)\big), deg(g(x))\}.$$

مثال (٤,١,١)

إذا كان $f(x) = 1 + x + x^3 + x^4$ ، $g(x) = x + x^2 + x^3$ ، $h(x) = 1 + x^2 + x^4$ فنجد أن:

(أ) $f(x) + g(x) = 1 + x^2 + x^4$.

(ب) $f(x)+h(x)=x+x^2+x^3$.

(ج) $f(x)g(x)=(x+x^2+x^3)+x(x+x^2+x^3)+$
$x^3(x+x^2+x^3)\ +x^4(x+x^2+x^3)=x+x^7$

▲

تمارين

(**٤,١,٢**) جد مجموع وحاصل ضرب كل زوج من أزواج كثيرات الحدود التالية على K:

(أ) $h(x)=1+x^2+x^3+x^4\ ,f(x)=x^5+x^6+x^7$.

(ب) $h(x)=1+x^3+x^9\ ,f(x)=1+x^2+x^3+x^8+x^{13}$.

(ج) $h(x)=1+x+x^2+x^3+x^4\ ,f(x)=1+x$.

(**٤,١,٣**) إذا كانت $f(x)=1+x$ فجد:

(أ) $(f(x))^2$ (ب) $(f(x))^3$ (ج) $(f(x))^4$.

(**٤,١,٤**) أعد التمرين (**٤,١,٣**) لكثيرة الحدود $f(x)=1+x+x^2$.

(**٤,١,٥**) جد جميع كثيرات الحدود على K من الدرجة n حيث $n=0,2,3,4$.

(**٤,١,٦**) جد عدد كثيرات الحدود على K ذات الدرجات التي لا تزيد عن 10.

(**٤,١,٧**) لقد لاحظت في التمرينين (**٤,١,٣**) (أ) و (**٤,١,٤**) (أ) أن $(f(x)+g(x))^2=(f(x))^2+(g(x))^2$ لأي كثيرتي حدود $f(x)$ و $g(x)$ على K؛ وذلك لأن $x^k+x^k=0$. هل تستطيع إيجاد صيغة خاصة لحساب كل من:

(أ) $(f(x)+g(x))^4$ (ب) $(f(x)+g(x))^3$

(ج) $(f(x)+g(x))^n$ حيث n عدد صحيح موجب.

عملية القسمة المطوّلة لكثيرات الحدود على K مشابهة تماماً لعملية القسمة المطوّلة لكثيرات الحدود على الأعداد الكسرية.

خوارزمية (٤,١,٨) [خوارزمية القسمة Division Algorithm]

لتكن $f(x), h(x)\epsilon K[x]$ حيث $h(x) \neq 0$. عندئذ، توجد كثيرتا حدود وحيدتان $q(x), r(x)\epsilon K[x]$ تحققان:

$$f(x) = q(x)h(x) + r(x)$$

حيث $r(x) = 0$ أو $deg(r(x)) < deg(h(x))$.

تُدعى كثيرة الحدود $q(x)$ **خارج القسمة (quotient)** وتُدعى كثيرة الحدود $r(x)$ **باقي القسمة (remainder)**. تجرى قسمة $f(x)$ على $h(x)$ بعملية القسمة المطوّلة المعتادة مع ملاحظة أن المعاملات تنتمي إلى K.

مثال (٤,١,٩)

إذا كانت $f(x) = x + x^2 + x^6 + x^7 + x^8$ وكانت $h(x) = 1 + x + x^2 + x^4$ فيكون:

$$\begin{array}{r|l} & x^4 + x^3 \\ \hline x^8 + x^7 + x^6 + x^2 + x & \\ x^8 + x^6 + x^5 + x^4 & \\ \hline x^7 + x^5 + x^4 + x^2 + x & \\ x^7 + x^5 + x^4 + x^3 & \\ \hline x^3 + x^2 + x & \end{array} \qquad x^4 + x^2 + x + 1$$

وبهذا نرى أن خارج القسمة هو $q(x) = x^3 + x^4$ وباقي القسمة هو $r(x) = x + x^2 + x^3$. لاحظ أنه من الممكن التعبير عن ذلك بكتابة:

$$f(x) = h(x)(x^3 + x^4) + (x + x^2 + x^3)$$

لاحظ أيضاً أن $deg(r(x)) < deg(h(x))$. ▲

تمارين

(٤,١,١٠) جد خارج القسمة والباقي عند قسمة $f(x)$ على $h(x)$ لكثيرات الحدود على K المقدمة في التمرين **(٤,١,٢)**.

(٤,١,١١) جد خارج القسمة والباقي عند قسمة $f(x)$ على $h(x)$ لكثيرات الحدود التالية :

(أ) $f(x) = x^2 + x^3 + x^4 + x^8 , h(x) = 1 + x^5$.

(ب) $f(x) = 1 + x^{10} , h(x) = 1 + x^5$.

(ج) $f(x) = 1 + x^7 , h(x) = 1 + x + x^3$.

(د) $f(x) = 1 + x^{15} , h(x) = 1 + x^4 + x^6 + x^7 + x^8$.

يمكن تمثيل كثيرة الحدود $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ التي درجتها لا تزيد عن $n - 1$ على K ككلمة $v = a_0a_1a_2 \cdots a_{n-1}$ من الطول n في K^n. على سبيل المثال إذا كان $n = 7$ فإن :

الكلمة	كثيرة الحدود
1110100	$1 + x + x^2 + x^4$
1000111	$1 + x^4 + x^5 + x^6$
1101000	$1 + x + x^3$

وعليه يمكن تمثيل شفرة C طولها n كمجموعة كثيرات حدود على K درجاتها لا تزيد عن $n - 1$. أي أنه يوجد تقابل بين كثيرات الحدود على K التي لا تزيد درجاتها عن $n - 1$ والكلمات من الطول n في K^n.

عند تمثيل الكلمات بكثيرات الحدود يكون من المناسب ترقيم إحداثيات الكلمة التي طولها n من 0 إلى $n - 1$ عوضاً عن الترقيم من 1 إلى n. فالكلمة $a_0a_1a_2a_3$ ذات الطول 4 تمثل بكثيرة الحدود $a_0 + a_1x + a_2x^2 + a_3x^3$ من الدرجة الثالثة.

مثال (٤,١,١٢)

العمود الأيسر من الجدول التالي يُبيّن كلمات شفرة C والعمود الأيمن يُبيّن كثيرات الحدود المقابلة لهذه الكلمات.

كثيرة الحدود $c(x)$	كلمة الشفرة
0	0000
$1+x^2$	1010
$x+x^3$	0101
$1+x+x^2+x^3$	1111

▲

تمارين

(**٤,١,١٣**) مثّل كلاً من الشفرات C التالية بمجموعة كثيرات حدود:

(أ) $C=\{000,001,010,011\}$.

(ب) $C=\{00000,11111\}$.

(ج) $C=\{0000,0001,1110\}$.

(د) $C=\{0000,1001,0110,1111\}$.

(هـ) $C=\{00000,11100,00111,11011\}$.

(**٤,١,١٤**) اكتب كلمات شفرة هامينغ من الطول 7 ذات المصفوفة المولّدة G المعطاة، ثم مثّل هذه الكلمات بكثيرات حدود:

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

وجدنا في التمرين (**٤,١,١١**) (أ) أن باقي قسمة $f(x)=x^2+x^3+x^4+x^8$ على $h(x)=1+x^5$ هو $r(x)=x^2+x^4$. لاحظ أن هذا الباقي وحيد ودرجته أصغر من درجة $h(x)$.

نقول إن $\boldsymbol{f(x)}$ **قياس** $\boldsymbol{h(x)}$ **(**$\boldsymbol{f(x)}$ **modulo** $\boldsymbol{h(x)}$**)** هي $\boldsymbol{r(x)}$ إذا كانت $\boldsymbol{r(x)}$ هي **باقي قسمة** $\boldsymbol{f(x)}$ **على** $\boldsymbol{h(x)}$ ونكتب $\boldsymbol{r(x)\equiv f(x)(mod\ h(x))}$. كما نقول إن $f(x)$ و $p(x)$ متكافئتان قياس $h(x)$ إذا وفقط إذا كان لهما الباقي نفسه عند قسمتهما على $h(x)$. أي أن:

$$f(x)\big(mod\ h(x)\big)\equiv r(x)\equiv p(x)(mod\ h(x)).$$

وفي هذه الحالة نكتب $f(x) \equiv p(x)(mod\ h(x))$[1].

مثال (٤,١,١٥)

افرض أن $h(x) = 1 + x^5$ وأن $f(x) = 1 + x^4 + x^9 + x^{11}$. بقسمة $f(x)$ على $h(x)$ نحصل على الباقي $r(x) = 1 + x$. وبالمثل إذا كانت $p(x) = 1 + x^6$ فنجد أن $1 + x^6 \equiv 1 + x(mod\ h(x))$ ويكون $p(x) \equiv f(x)(mod\ h(x))$. ▲

مثال (٤,١,١٦)

لتكن $h(x) = 1 + x^2 + x^5$. بحساب $f(x)(mod\ h(x))$ حيث $f(x) = 1 + x^2 + x^6 + x^9 + x^{11}$ نجد أن الباقي هو $r(x) = x + x^4$. وبهذا نرى أن $x + x^4 \equiv f(x)(mod\ h(x))$. وإذا كانت $p(x) = x^2 + x^8$ فنجد أن $p(x) \equiv 1 + x^3 \big(mod\ h(x)\big)$. وعليه فإن $p(x)$ و $f(x)$ غير متكافئتين قياس $h(x)$. ▲

تُحافظ عمليتا جمع وضرب كثيرات الحدود على تكافؤ كثيرات الحدود. أي أن:

تمهيدية (٤,١,١٧)

إذا كانت $f(x) \equiv g(x)(mod\ h(x))$ وكانت $p(x)$ كثيرة حدود على K فإن:

$$f(x) + p(x) \equiv g(x) + p(x)(mod\ h(x))$$
$$f(x)p(x) \equiv g(x)p(x)(mod\ h(x))$$

البرهان

لنفرض أن $r(x) \equiv f(x)\big(mod\ h(x)\big) \equiv g(x)(mod\ h(x))$

وأن $s(x) \equiv p(x)(mod\ h(x))$. حينئذ،

$$f(x) + p(x) = q_1(x)h(x) + r(x) + q_2(x)h(x) + s(x)$$
$$= \big(q_1(x) + q_2(x)\big)h(x) + r(x) + s(x)$$

---

(١) المترجمان: استخدم المؤلفون الرمز $r(x) = f(x)\ (mod\ h(x))$ للدلالة على باقي قسمة $f(x)$ على $h(x)$ كما استخدموا الرمز $f(x) \equiv p(x)\ (mod\ h(x))$ للدلالة على أن باقي قسمة $f(x)$ على $h(x)$ يساوي باقي قسمة $p(x)$ على $h(x)$. وسنستخدم في الترجمة الرمز $\equiv$ ليدل على الحالتين حيث يكون من الواضح المقصود من السياق وحيث أن هو الترميز الشائع الاستخدام.

وبما أن $deg\big(r(x)+s(x)\big) < deg(h(x))$ فنجد أن $r(x)+s(x) \equiv f(x)+ p(x)(mod\ h(x))$. وبصورة مشابهة نجد أيضاً أن:

$$r(x)+s(x) \equiv g(x)+p(x)(mod\ h(x)).$$

الفقرة الثانية من البرهان نتركها للتمرين (**٤,١,٢٢**). ■

مثال (٤,١,١٨)

لتكن $h(x)=1+x^5$ و $f(x)=1+x+x^7$ و $g(x)=1+x+x^2$ و $p(x)=1+x^6$. لاحظ أن $f(x) \equiv g(x)(mod\ h(x))$. الآن:

$$f(x)+p(x)=x+x^6+x^7$$
$$g(x)+p(x)=x+x^2+x^6$$

ولكن $x+x^6+x^7\big(mod\ h(x)\big) \equiv x^2 \equiv (x+x^2+x^6)(mod\ h(x))$. وبالمثل

$$(1+x+x^7)(1+x^6)\big(mod\ h(x)\big) \equiv 1+x^3 \equiv (1+x+x^2)(1+x^6)(mod\ h(x))$$

ولكن $1+x \equiv 1+x^6(mod\ h(x))$. من ذلك نجد أن:

$$\begin{aligned}(1+x+x^7)(1+x^6) &\equiv (1+x+x^2)(1+x^6)\\ &\equiv (1+x+x^2)(1+x)\\ &\equiv 1+x^3\big(mod\ h(x)\big)\end{aligned}$$

▲

تمارين

(**٤,١,١٩**) لتكن $h(x)=1+x^3+x^5$. احسب $f(x)(mod\ h(x))$ والكلمة المقابلة لها لكل مما يلي:

(أ) $f(x)=1+x+x^6$.

(ب) $f(x)=x+x^4+x^7+x^8$.

(ج) $f(x)=1+x^{10}$.

(**٤,١,٢٠**) افرض أن $h(x)=1+x^7$ احسب كلاً من $f(x)(mod\ h(x))$ و $p(x)(mod\ h(x))$ وبيّن ما إذا كان $f(x) \equiv p(x)(mod\ h(x))$:

(أ) $f(x)=1+x^3+x^8$ و $p(x)=x+x^3+x^7$.

(ب) $f(x) = x + x^5 + x^9$ و $p(x) = x + x^5 + x^6 + x^{13}$.

(ج) $f(x) = 1 + x$ و $p(x) = x + x^7$.

(٤,١,٢١) إذا كانت $h(x) = 1 + x^7$ فاحسب $f(x) + g(x)(mod\ h(x))$ و $f(x)g(x)(mod\ h(x))$ لما يلي:

(أ) $f(x) = 1 + x^6 + x^8$ و $g(x) = 1 + x$.

(ب) $f(x) = x + x^5 + x^9$ و $g(x) = x + x^2 + x^7$.

(ج) $f(x) = 1 + x^4 + x^5$ و $g(x) = 1 + x + x^2$.

(٤,١,٢٢) إذا كان $f(x) \equiv g(x)(mod\ h(x))$ فأثبت أن:

$$f(x)p(x) \equiv g(x)p(x)(mod\ h(x)).$$

(٤,٢) مقدمة للشفرات الدورية
Introduction to Cyclic Codes

نبدأ الآن بدراسة صنف من الشفرات تُدعى الشفرات الدورية ونستخدم لاحقاً خواص هذه الشفرات لإنشاء مصفوفة مولّدة لشفرة BCH التي تصوّب خطأين إضافة إلى بعض الشفرات الأخرى. في الحقيقة سنرى أن كلاً من شفرة هامينغ وشفرة جولاي دورية أو تكافئ شفرة دورية.

لتكن v كلمة طولها n. **الإزاحة الدورية (Cyclic Shift)** $\pi(v)$ للكلمة v هي الكلمة من الطول n التي نحصل عليها من الكلمة v بنقل الإحداثي الأخير من v إلى بداية الكلمة ثم إزاحة الإحداثيات الأخرى إلى اليمين موقعاً واحداً. على سبيل المثال:

v	10110	111000	0000	1011
$\pi(v)$	01011	011100	0000	1101

نقول إن الشفرة C هي **شفرة دورية (Cyclic Code)** إذا كانت الإزاحة الدورية لكل كلمة شفرة هي أيضاً كلمة شفرة. أي أن C مغلقة تحت تأثير الإزاحة الدورية.

مثال (٤,٢,١)

لتكن $C = \{000, 110, 101, 011\}$. عندئذ الشفرة C خطية (لماذا ؟). بحساب $\pi(v)$ لكل $v\epsilon C$ نجد أن $\pi(000) = 000, \pi(110) = 011, \pi(101) = 110, \pi(011) = 101$. وبهذا نرى أن $\pi(v)\epsilon C$ لكل $v\epsilon C$. وعليه فإن C شفرة دورية وتكون C شفرة خطية دورية. ▲

مثال (٤,٢,٢)

الشفرة $C = \{000,100,011,111\}$ ليست دورية ؛ لأن $\pi(100) = 010 \notin C$. ▲

لاحظ أن الإزاحة الدورية π هي تحويل خطي. أي أن :

تمهيدية (٤,٢,٣)

$\pi(v + w) = \pi(v) + \pi(w)$ و $\pi(av) = a\pi(v)$ لكل $a\epsilon K = \{0,1\}$. وعليه، إذا كانت C شفرة خطية فلإثبات أن C شفرة دورية يكفي أن نثبت أن $\pi(v)\ \epsilon C$ لكل كلمة v من كلمات أساس للشفرة C.

البرهان

لنفرض أن $v = (v_0, v_1, \cdots, v_{n-1})$ وأن $w = (w_0, w_1, \cdots, w_{n-1})$. حينئذ،

ويكون $v + w = (v_0 + w_0, v_1 + w_1, \cdots, v_{n-1} + w_{n-1})$

$$\pi(v + w) = (v_{n-1} + w_{n-1}, v_0 + w_0, \cdots, v_{n-2} + w_{n-2})$$
$$= (v_{n-1}, v_0, \cdots, v_{n-2}) + (w_{n-1}, w_0, \cdots, w_{n-2})$$
$$= \pi(v) + \pi(w)$$

أيضاً $av = (av_0, av_1, \cdots, av_{n-1})$ ويكون :

$\pi(av) = (av_{n-1}, av_0, \cdots, av_{n-2}) = a(v_{n-1}, v_0, \cdots, v_{n-2}) = a\pi(v)$.[٢] ■

(٢) المترجمان: أضفنا برهان الفقرة الأخيرة من التمهيدية (٤,٢,٣) نعتقد أنه سقط سهواً من الأصل الإنجليزي.

مثال (٤,٢,٤)

لاحظ أن $\{110, 101\}$ أساس للشفرة C المقدمة في المثال (**٤,٢,١**). بما أن $\pi(110) = 011 \epsilon C$ وأن $\pi(101) = 110 \epsilon C$ فتكون C شفرة خطية دورية. ▲

لإنشاء شفرة خطية دورية نقوم باختيار كلمة v ثم نجد المجموعة S المكوّنة من v وجميع إزاحاتها الدورية. أي نجد $S = \{v, \pi(v), \pi^2(v), \cdots, \pi^{n-1}(v)\}$[٣]. حينئذ. نأخذ $C = \langle S \rangle$ الشفرة المولّدة بالمجموعة S. بما أن S تحتوي على أساس للشفرة C فاستناداً إلى التمهيدية (**٤,٢,٣**) تكون C دورية. ومن ثم فهي الشفرة الخطية الدورية المنشودة.

مثال (٤,٢,٥)

لنفرض أن $n = 3$ وأن $v = 100$. عندئذ،

$$S = \{v, \pi(v), \pi^2(v)\} = \{100, 010, 001\}.$$

ومن ثم فإن $\langle S \rangle = K^3$. لاحظ أنه إذا كان $w = a_0 v + a_1 \pi(v) + a_2 \pi^3(v)$ فنرى أن:

$$\pi(w) = a_0 \pi(v) + a_1 \pi^2(v) + a_2 \pi^3(v) = a_2 v + a_0 \pi(v) + a_1 \pi^2(v).$$

▲

مثال (٤,٢,٦)

لنفرض أن $n = 4$ وأن $v = 0101$. حينئذ، $\pi(v) = 1010$ ، $\pi^2(v) = 0101$.

ونرى أن $S = \{1010, 0101\}$. وبهذا تكون الشفرة الدورية $C = \langle S \rangle$ هي:

$$C = \{0000, 0101, 1010, 1111\}.$$ ▲

لتكن v كلمة ولتكن $S = \{v, \pi(v), \cdots, \pi^{n-1}(v)\}$ مجموعة الازاحات الدورية للكلمة v ولتكن $C = \langle S \rangle$ الشفرة المولّدة بالمجموعة S. حينئذ، نقول إن الكلمة v **مولّدة (generator)** للشفرة الخطية الدورية C. وبما أن أي شفرة خطية دورية تحتوي v يجب أن

---

(٣) لاحظ أن $\pi^2(v) = \pi(\pi(v))$ وأن $\pi^3(v) = \pi(\pi(\pi(v)))$ وهكذا.

تحتوي S فتكون C هي أصغر شفرة خطية دورية تحتوي v. لاحظ إمكانية وجود أكثر من مولّدة للشفرة الخطية الدورية.

تمارين

(٤,٢,٧) جد أساساً لأصغر شفرة خطية دورية من الطول n تحتوي v لكل من:

(أ) $v = 1101000$ ، $n = 7$.

(ب) $v = 010101$ ، $n = 6$.

(ج) $v = 11011000$ ، $n = 8$.

(٤,٢,٨) جد جميع الكلمات v من الطول n التي تحقق $\pi(v) = v$.

(٤,٢,٩) جد جميع الكلمات v من الطول 6 التي تحقق:

(أ) $\pi^2(v) = v$ (ب) $\pi^3(v) = v$.

من الممكن استخدام كثيرات الحدود للحصول على تمثيل ملائم للشفرات الدورية، وذلك بملاحظة أنه إذا كانت $v(x)$ هي كثيرة الحدود المقابلة للكلمة v فإن كثيرة الحدود $xv(x)(mod 1 + x^n)$ هي كثيرة الحدود التي تقابل الإزاحة الدورية $\pi(v)$. لاحظ أن $1 \equiv x^n (mod\ 1 + x^n)$.

مثال (٤,٢,١٠)

لنفرض أن $v = 100$. عندئذ، $v(x) = 1$ وبهذا نرى أن $\pi(v) = 010$ تقابل $xv(x) = x$. وإذا كانت $v = 1101$ فإن $v(x) = 1 + x + x^3$ وإن $\pi(v) = 1110$ تقابل $xv(x)(mod 1 + x^4) = 1 + x + x^2$. ▲

مما سبق يكون من المناسب أيضاً النظر إلى كلمات الشفرة الدورية على أنها كثيرات حدود. ولهذا، إذا كانت v كلمة طولها n وكانت $v(x)$ كثيرة الحدود المقابلة لها فإن الإزاحات الدورية للكلمة v تقابل كثيرات الحدود $x^i v(x)(mod 1 + x^n)$ حيث $i = 0,1,\cdots,n-1$.

مثال (٤,٢,١١)

لنفرض أن $v = 1101000$ وأن $n = 7$. حينئذ، $v(x) = 1 + x + x^3$ والجدول (٤,١) يُبيّن $x^i v(x)$ حيث $1 \le i \le 6$.

الجدول (٤,١). كثيرات الحدود المقابلة للإزاحات الدورية.

$x^i v(x)\ (mod\ 1 + x^7)$	الكلمة
$xv(x) = x + x^2 + x^4$	0110100
$x^2v(x) = x^2 + x^3 + x^5$	0011010
$x^3v(x) = x^3 + x^4 + x^6$	0001101
$x^4v(x) = x^4 + x^5 + x^7 \equiv 1 + x^4 + x^5 (mod 1 + x^7)$	1000110
$x^5v(x) = x^5 + x^6 + x^8 \equiv x + x^5 + x^6 (mod 1 + x^7)$	0100011
$x^6v(x) = x^6 + x^7 + x^9 \equiv 1 + x^2 + x^6 (mod 1 + x^7)$	1010001

▲

تمهيدية (٤,٢,١٢)

لتكن C شفرة دورية ولتكن $v \epsilon C$، ولتكن $c(x) \epsilon \langle \{v(x), xv(x), \cdots, x^{n-1}v(x)\} \rangle$. عندئذ، توجد كثيرة حدود $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ بحيث يكون:

$$c(x) \equiv a(x)v(x)(mod 1 + x^n).$$

البرهان

بما أن $c(x) \epsilon \langle \{v(x), xv(x), \cdots, x^{n-1}v(x)\} \rangle$ فيوجد $a_0, a_1, \cdots, a_{n-1} \epsilon K$ بحيث يكون:

$$\begin{aligned} c(x) &\equiv \big(a_0v(x) + a_1xv(x) + \cdots + a_{n-1}x^{n-1}v(x)\big)(mod 1 + x^n) \\ &\equiv (a_0 + a_1x + \cdots + a_{n-1}x^{n-1})v(x)(mod 1 + x^n) \\ &\equiv a(x)v(x)(mod 1 + x^n) \end{aligned}$$

وهذا ينهي البرهان. ■

لتكن C شفرة خطية دورية. من الواضح أن C تحتوي كلمة غير صفرية g بحيث تكون درجة $g(x)$ أصغر ما يمكن ولتكن k. سنبرهن الآن أن g وحيدة. لنفرض أن $g'\epsilon C$ غير صفرية حيث $g'(x)$ درجتها k أيضاً. عندئذ، $g(x)+g'(x)=c(x)\epsilon C$ ؛ وذلك لأن C خطية. وبما أن $x^k+x^k=0$ فإن $deg\, c(x)<k$. وبهذا تكون $c(x)=0$ ونخلص إلى أن $g(x)=g'(x)$.

سنبرهن الآن أن كثيرة الحدود غير الصفرية التي درجتها أصغر ما يمكن تولّد الشفرة الخطية الدورية. ولهذا الغرض نفرض أن $c(x)\epsilon C$. بما أن $deg(c(x)) \geq deg(g(x))$ فنجد استناداً إلى خوارزمية القسمة أن:

$$c(x)=q(x)g(x)+r(x) \text{ أو } r(x)=q(x)g(x)+c(x).$$

ولكن استناداً إلى التمهيدية (**٤,٢,١٢**) نرى أن كلاً من $c(x)$ و $q(x)g(x)$ كلمة شفرة وبهذا تكون $r(x)$ كلمة شفرة. وبما أن $deg(r(x)) \geq deg(g(x))$ فنرى أن $r(x)=0$. ومن ثم يكون $c(x)=q(x)g(x)$ وبهذا نرى أن $g(x)$ تولّد الشفرة C.

سنسمي كثيرة الحدود غير الصفرية ذات الدرجة الصغرى والتي تولّد الشفرة الخطية الدورية C، **كثيرة الحدود المولّدة (Generator Polynomial)** للشفرة C.

مبرهنة (٤,٢,١٣)

لتكن C شفرة دورية طولها n ولتكن $g(x)$ كثيرة الحدود المولّدة للشفرة C. إذا كان $deg(g(x))=n-k$ فإن:

(١) بُعد C يساوي k.

(٢) كلمات الشفرة المقابلة لكثيرات الحدود $g(x), xg(x), \cdots, x^{k-1}g(x)$ أساس للشفرة C.

(٣) $c(x)\epsilon C$ إذا وفقط إذا كان $c(x)=a(x)g(x)$ حيث $a(x)$ كثيرة حدود تُحقق $deg(a(x))<k$ (أي أن $g(x)$ قاسم لجميع كلمات الشفرة $c(x)$).

البرهان

إثبات الفقرة (٣) نحصل عليه من النقاش السابق للمبرهنة (**٤,٢,١٣**).

ولبرهان الفقرتين (١) و (٢) نفرض أن $deg(g(x)) = n - k$. عندئذ، $g(x), xg(x), \cdots, x^{k-1}g(x)$ مُستقلة خطياً (لماذا ؟). وبما أن $g(x)$ تقسم جميع كلمات الشفرة فنجد كثيرة حدود وحيدة $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ تُحقق :

$$c(x) = a(x)g(x) = a_0g(x) + a_1xg(x) + \cdots + a_{k-1}x^{k-1}g(x).$$

وبهذا يكون $c(x)\epsilon(\{g(x), xg(x), \cdots, x^{k-1}g(x)\})$. ونخلص إلى أن :

$\{g(x), xg(x), \cdots, x^{k-1}g(x)\}$ أساس للشفرة C. ■

مثال (٤,٢,١٤)

لنفرض أن $n = 7$ وأن $g(x) = 1 + x + x^3$ مولّد للشفرة الدورية C. أحد أساسات C هو :

$$g(x) = 1 + x + x^3 \leftrightarrow 1101000$$
$$xg(x) = x + x^2 + x^4 \leftrightarrow 0110100$$
$$x^2g(x) = x^2 + x^3 + x^5 \leftrightarrow 0011010$$
$$x^3g(x) = x^3 + x^4 + x^6 \leftrightarrow 0001101$$

لاحظ أن $x^4g(x)(mod1 + x^7) \equiv 1 + x^4 + x^5$ هي كلمة شفرة ؛ لأن :

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

مثال (٤,٢,١٥)

لتكن C الشفرة الدورية $C = \{0000, 1010, 0101, 1111\}$. مجموعة كثيرات الحدود المقابلة هي $\{0, 1 + x^2, x + x^3, 1 + x + x^2 + x^3\}$. لاحظ أن $1 + x^2 \leftrightarrow 1010$ هي كثيرة الحدود المولّدة للشفرة C ؛ وذلك لأن C تحتوي على كثيرة حدود واحدة فقط

من الدرجة الثانية ولا تحتوي كثيرات حدود من الدرجة الأولى. أيضاً كل من كلمات الشفرة (كثيرات الحدود) هي مضاعف لكثيرة الحدود المولّدة:

$$0 = 0(1 + x^2)$$
$$x + x^3 = x(1 + x^2)$$
$$1 + x^2 = 1(1 + x^2)$$
$$1 + x + x^2 + x^3 = (1 + x)(1 + x^2).$$ ▲

مثال (٤,٢,١٦)

من السهل التحقق من أن الشفرة:

$$C = \{000000, 100100, 010010, 001001, 110110, 101101, 011011, 111111$$

هي أصغر شفرة خطية طولها 6 وتحتوي على $100100 \leftrightarrow g(x) = 1 + x^3$. كثيرة الحدود الأصغرية التي تقابل كلمة شفرة هي $g(x) = 1 + x^3$ ولا تحتوي C على كثيرات حدود أخرى من الدرجة 3. وبهذا نرى أن $g(x) = 1 + x^3$ تولّد الشفرة C. الجدول (٤,٢) يُبيّن كلمات C كمضاعفات لكثيرة الحدود $g(x)$:

الجدول (٤,٢). كلمات الشفرة كمضاعفات لكثيرة الحدود المولّدة.

الكلمة	كثيرة الحدود $f(x)$	$f(x) = h(x)g(x)$
000000	0	$0(1 + x^3)$
100100	$1 + x^3$	$1(1 + x^3)$
010010	$x + x^4$	$x(1 + x^3)$
001001	$x^2 + x^5$	$x^2(1 + x^3)$
110110	$1 + x + x^3 + x^4$	$(1 + x)(1 + x^3)$
101101	$1 + x^2 + x^3 + x^5$	$(1 + x^2)(1 + x^3)$
011011	$x + x^2 + x^4 + x^5$	$(x + x^2)(1 + x^3)$
111111	$1 + x + x^2 + x^3 + x^4 + x^5$	$(1 + x + x^2)(1 + x^3)$

▲

من السهل توليد شفرة دورية وذلك باختيار كلمة v وحساب:

$$C = \langle \{v(x), xv(x), \cdots, x^{n-1}v(x)\} \rangle (mod 1 + x^n).$$

ولكننا بحاجة إلى إيجاد مولّد لهذه الشفرة وكتابة جميع كلمات C وهذه ليست الطريقة الملائمة لذلك. ولكن كثيرة الحدود المولّدة للشفرة الدورية تتمتع بالخاصية المهمة التالية:

مبرهنة (٤,٢,١٧)

$g(x)$ كثيرة حدود مولّدة للشفرة الخطية الدورية من الطول n إذا وفقط إذا كانت $g(x)$ تقسم $1+x^n$. أي أن $1+x^n=h(x)g(x)$.

البرهان

استناداً إلى التمهيدية (٤,٢,١٢) نجد أن:

$$c(x)=h(x)g(x)(mod1+x^n)=h(x)g(x)+q(x)(1+x^n)$$

كلمة شفرة لكل $h(x)$. واستناداً إلى خوارزمية القسمة نرى أن $g(x)$ تقسم أي كلمة شفرة $c(x)$ إذا وفقط إذا كانت $g(x)$ تقسم $1+x^n$. وبهذا نجد استناداً إلى المبرهنة (٤,٢,١٣) أن $g(x)$ تولّد الشفرة الدورية من الطول n إذا وفقط إذا كانت $g(x)$ تقسم $1+x^n$. ■

نتيجة (٤,٢,١٨)

لتكن $g(x)$ كثيرة الحدود المولّدة لأصغر شفرة دورية من الطول n تحتوي على الكلمة v (كثيرة الحدود $v(x)$). عندئذ، $g(x)=gcd(v(x),1+x^n)$.

البرهان

بما أن $g(x)$ كثيرة الحدود المولّدة للشفرة فنرى أن $g(x)$ تقسم كلاً من $v(x)$ و $1+x^n$. وبما أن $g(x)\epsilon\langle\{v(x),xv(x),\cdots,x^{n-1}v(x)\}$ فنجد أن $g(x)\equiv a(x)v(x)(mod1+x^n)$. أي أن:

$$g(x)=a(x)v(x)+b(x)(1+x^n).$$

الآن، إذا كانت $h(x)$ تقسم $v(x)$ و $1+x^n$ فنرى أن $h(x)$ تقسم $a(x)v(x)+b(x)(1+x^n)$. ومن ثم نجد أن $h(x)$ تقسم $g(x)$. إذن،

$$g(x)=gcd(v(x),1+x^n).$$ ■

مثال (٤,٢,١٩)

لنفرض أن $n=8$ وأن $v=11011000$. أي أن $v(x)=1+x+x^3+x^4$. بما أن:

$$gcd(v(x),1+x^8)=1+x^2$$

فنجد أن $g(x)=1+x^2$ كثيرة الحدود المولّدة لأصغر شفرة دورية تحتوي على $v(x)$ وبُعد هذه الشفرة يساوي $8-2=6$. ▲

من الممكن استخدام خوارزمية إقليدس لحساب القاسم المشترك الأعظم لكثيرتي حدود وهذه الطريقة موضّحة في الملحق A. من الممكن أيضاً استخدام العمليات الصفية الأولية لإيجاد كثيرة الحدود المولّدة لشفرة دورية طولها n وبُعدها $n-k$ ويتم ذلك على النحو التالي:

نقوم باختيار أساس (مصفوفة مولّدة) للشفرة ثم نستخدم العمليات الصفية الأولية للحصول على RREF حيث الأعمدة المتقدمة (عددها k) هي الأعمدة الأخيرة. عندئذ، يكون الصف (كلمة الشفرة) ذو الدرجة الصغرى هو كثيرة الحدود المولّدة.

تمارين

(٤,٢,٢٠) جد كثيرة الحدود المولّدة لأصغر شفرة خطية دورية تحتوي على الكلمة المبينة:

(أ) 010101 (ب) 010010

(ج) 01100110 (د) 0101100

(هـ) 001000101110000 (و) 000010010000000

(ز) 010111010000000.

(**٤,٢,٢١**) أعد التمرين (**٤,٢,٢٠**) لكل من الكلمات التالية:

(أ) 101010 (ب) 1100

(ج) 10001000 (د) 011011

(هـ) 10101 (و) 111111.

(**٤,٢,٢٢**) لكل من الشفرات $C = \langle S \rangle$ حيث S هي المجموعة المعطاة فيما يلي، جد كثيرة الحدود $g(x)$ المولّدة ومن ثم اكتب كلمات الشفرة كمضاعفات لكثيرة الحدود $g(x)$:

(أ) $S = \{010\,, 011\,, 111\}$.

(ب) $S = \{1010\,, 0101\,, 1111\}$.

(ج) $S = \{0101\,, 1010\,, 1100\}$.

(د) $S = \{1000\,, 0100\,, 0010\,, 0001\}$.

(هـ) $S = \{11000\,, 01111\,, 11110\,, 01010\}$.

(٤,٣) المصفوفات المولّدة ومصفوفات اختبار النوعية للشفرات الدورية

Generating & Parity Check Matrices for Cyclic Codes

يوجد عديد من المصفوفات المولّدة للشفرات الخطية الدورية، وأبسط هذه المصفوفات هي المصفوفة التي تتكون صفوفها من كلمات الشفرة المقابلة لكثيرة الحدود المولّدة وأول $k-1$ من ازاحاتها الدورية (انظر المبرهنة (**٤,٢,١٣**)):

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

مثال (٤,٣,١)

لتكن $C = \{0000,1010,0101,1111\}$ شفرة خطية دورية. كثيرة الحدود المولّدة للشفرة C هي $g(x) = 1 + x^2$. عندئذ، $n = 4$ و $k = 2$ ونرى أن أساساً للشفرة C هو:

$$g(x) = 1 + x^2 \leftrightarrow 1010$$
$$xg(x) = x + x^3 \leftrightarrow 0101$$

وبهذا تكون مصفوفة مولّدة للشفرة C هي $G = \begin{bmatrix} g(x) \\ xg(x) \end{bmatrix} = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix}$. ▲

مثال (٤,٣,٢)

لتكن C شفرة خطية دورية من الطول $n = 7$ وكثيرة حدود مولّدة $g(x) = 1 + x + x^3$ من الدرجة $n - k = 3$. عندئذ، $k = 4$ وأساس للشفرة C هو:

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

ومصفوفة مولّدة للشفرة C هي:

$$G = \begin{bmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{bmatrix}.$$ ▲

لتكن C شفرة خطية دورية من الطول n والبُعد k (ومن ثم كثيرة الحدود المولّدة $g(x)$ من الدرجة $n - k$). عندئذ، إحداثيات المعلومات $(a_0, a_1, \cdots, a_{k-1})$ المراد تشفيرها (عددها k) تقابل كثيرة الحدود $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ وتُسمى **كثيرة حدود المعلومات أو كثيرة حدود الرسالة (Information or Message Polynomial)**. عملية التشفير تتم بواسطة ضرب كثيرات حدود. أي أن $a(x)g(x) = c(x)$ هي عملية تشفير $a(x)$. وعليه نرى أنه يتم تخزين كثيرة الحدود المولّدة عوضاً عن تخزين المصفوفة المولّدة من الدرجة $k \times n$ وهذا تحسن ملحوظ عند حساب تعقد عملية التشفير.

إن العملية العكسية لضرب كثيرات الحدود هي قسمتها. ولهذا، نحصل على الرسالة المقابلة لأقرب كلمة شفرة $c(x)$ للكلمة المستقبلة بقسمة $c(x)$ على $g(x)$ ويكون خارج القسمة هو كثيرة حدود الرسالة $a(x)$.

مثال (٤,٣,٣)

لنفرض أن $g(x) = 1 + x + x^3$ و $n = 7$. عندئذ، $k = 7 - 3 = 4$. لنفرض أن $a(x) = 1 + x^2$ هي كثيرة حدود الرسالة والتي تقابل الكلمة $a = 1010$. يتم تشفير $a(x)$ على النحو التالي:

$$c(x) = a(x)g(x) = (1 + x^2)(1 + x + x^3) = 1 + x + x^2 + x^5$$

وبهذا تكون $c = 1110010$ هي كلمة الشفرة المقابلة. وإذا كانت $c(x) = 1 + x + x^4 + x^6$ فنجد أن كثيرة حدود الرسالة هي:

$$a(x) = c(x)/g(x) = 1 + x^3.$$

وتقابل الرسالة $a = 1001$. ▲

تمارين

(٤,٣,٤) لتكن $g(x) = 1 + x^2 + x^3$ كثيرة الحدود المولّدة للشفرة الخطية الدورية من الطول 7.

(أ) شفّر كثيرات حدود الرسائل التالية: $1 + x^3$ ، x ، $x + x^2 + x^3$.

(ب) جد كثيرة حدود الرسالة المقابلة لكل من كلمات الشفرة $c(x)$ التالية:

$$x^4 + x^5 \text{ ، } 1 + x + x^2 + x^4 \text{ ، } x^2 + x^3 + x^4 + x^6.$$

(٤,٣,٥) جد أساساً ومصفوفة مولّدة للشفرة الخطية الدورية من الطول n حيث كثيرة الحدود المولّدة المعطاة $g(x)$:

(أ) $g(x) = 1 + x^2 + x^3$ ، $n = 7$.

(ب) $g(x) = 1 + x^3 + x^6$ ، $n = 9$.

(ج) $g(x) = 1 + x + x^4$ ، $n = 15$.

(د) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ ، $n = 15$.

(هـ) $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$ ، $n = 15$.

(٤,٣,٦) أثبت أن الشفرة الخطية ذات المصفوفة المولّدة المعطاة G هي شفرة دورية وجد كثيرة حدودها المولّدة:

(أ) $G = \begin{bmatrix} 110110 \\ 001001 \\ 101101 \end{bmatrix}$ (ب) $G = \begin{bmatrix} 010101 \\ 111111 \end{bmatrix}$.

بعد أن وجدنا طريقة فعّالة للحصول على مصفوفة مولّدة للشفرة الخطية الدورية بدلالة كثيرة حدودها المولّدة، ننتقل إلى دراسة كيفية الحصول على مصفوفة اختبار النوعية لهذه الشفرات. ولهذا الغرض نحتاج إلى إيجاد مصفوفة H تحقق:

$wH = 0$ إذا وفقط إذا كانت w كلمة شفرة.

ولإنجاز ذلك نكتب بداية $w(x) = c(x) + e(x)$ حيث $c(x)$ هي كلمة شفرة و $e(x)$ كثيرة حدود الخطأ.

تُعرف **كثيرة حدود التناذر (Syndrome Polynomial)** $s(x)$ على أنها:

$$s(x) \equiv w(x) (mod\ g(x)).$$

إذا فرضنا أن درجة $g(x)$ تساوي $n-k$ فتكون درجة $s(x)$ أصغر من $n-k$ وتقابل كلمة ثنائية s من الطول $n-k$. وبما أن $w(x) = c(x) + e(x)$ و $c(x) = a(x)g(x)$ حيث $a(x)$ كثيرة حدود تنتمي إلى $K[x]$ فنرى أن $s(x) \equiv e(x) (mod\ g(x))$. أي أن كثيرة حدود التناذر تعتمد فقط على الخطأ.

لتكن H هي المصفوفة التي صفوفها الكلمات r_i من الطول $n-k$ المقابلة لكثيرات الحدود $r_i(x) \equiv x^i (mod\ g(x))$. عندئذ، H هي مصفوفة اختبار النوعية للشفرة. ولإثبات ذلك، نفرض أن w كلمة مستقبلة. عندئذ، $w(x) = c(x) + e(x)$ ويكون:

$$wH = (c+e)H = \sum_{i=0}^{n-1}(c_i + e_i)r_i$$

$$\Leftrightarrow \sum_{i=0}^{n-1}(c_i + e_i)\, r_i(x) \equiv (\sum_{i=0}^{n-1} c_i x^i)\, mod\ g(x) + (\sum_{i=0}^{n-1} e_i x^i)\, mod\ g(x)$$

$$\equiv c(x) mod\ g(x) + e(x) mod\ g(x)$$

$$\equiv 0 + e(x) mod\ g(x)$$

$$\equiv s(x)$$

وبهذا نجد أن $s(x) = 0$ إذا وفقط إذا كانت $w(x)$ كلمة شفرة. إذن، H مصفوفة اختبار النوعية. أيضاً، إذا كان $wH = s$ فنرى أن $s(x) \equiv w(x)(mod\ g(x))$. وبهذا يتضح السبب وراء تسمية $s(x)$ كثيرة حدود التناذر. سنستخدم هذا التمثيل للتناذر في الفصل السابع عند تصويب متتالية من الأخطاء.

مثال (٤,٣,٧)

لنفرض أن $n = 7$ وأن $g(x) = 1 + x + x^3$. عندئذ، $n - k = 3$ ونجد H كالتالي:

$$r_0(x) \equiv 1 mod\ g(x) = 1 \leftrightarrow 100$$
$$r_1(x) \equiv x mod\ g(x) = x \leftrightarrow 010$$
$$r_2(x) \equiv x^2 mod\ g(x) = x^2 \leftrightarrow 001$$
$$r_3(x) \equiv x^3 mod\ g(x) = 1 + x \leftrightarrow 110$$
$$r_4(x) \equiv x^4 mod\ g(x) = x + x^2 \leftrightarrow 011$$
$$r_5(x) \equiv x^5 mod\ g(x) = 1 + x + x^2 \leftrightarrow 111$$
$$r_6(x) \equiv x^6 mod\ g(x) = 1 + x^2 \leftrightarrow 101$$

وبهذا تكون $H = \begin{bmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 111 \\ 101 \end{bmatrix}$. إذا استقبلنا كثيرة الحدود $w(x) = 1 + x^5 + x^6$. أي الكلمة $w = 1000011$ فنرى أن $wH = s = 110$ وأن:

$$s(x) = 1 + x \equiv 1 + x^5 + x^6 mod(1 + x + x^3) \equiv w(x)(mod\ g(x)).$$ ▲

تمارين

(**٤,٣,٨**) جد مصفوفة اختبار النوعية للشفرة الخطية الدورية من الطول 7 حيث كثيرة حدودها المولّدة هي $g(x) = 1 + x + x^2 + x^4$.

(**٤,٣,٩**) جد مصفوفة اختبار النوعية للشفرة الدورية من الطول n حيث كثيرة حدودها المولّدة هي $g(x)$:

(أ) $g(x) = 1 + x^2$، $n = 6$.

(ب) $g(x) = 1 + x^3$، $n = 6$.

(ج) $g(x) = 1 + x^2$، $n = 8$.

(د) $g(x) = 1 + x^3 + x^6$، $n = 9$.

(هـ) $g(x) = 1 + x + x^4$، $n = 15$ (هذه تولّد شفرة هامينغ).

(و) $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$، $n = 23$ (هذه تولّد شفرة جولاي).

(ز) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$، $n = 15$ (هذه تولّد شفرة BCH التي تصوّب خطأين وسنناقشها في الفصل الخامس).

(٤,٤) إيجاد الشفرات الدورية
Finding Cyclic Codes

يلزمنا لإنشاء شفرة خطية دورية من الطول n والبُعد k إيجاد قاسم لكثيرة الحدود $1 + x^n$ من الدرجة $n - k$. في بعض الأحيان يوجد أكثر من قاسم واحد وفي أحيان أخرى لا يوجد مثل هذا القاسم. ومسألة مهمة أخرى هي مسألة إيجاد شفرة خطية مسافتها صغرى وهذه مسألة لا يوجد لها حل عام حتى الآن وسنؤجل نقاشها إلى وقت لاحق.

بما أن أي مولّد للشفرة الدورية من الطول n يقسم كثيرة الحدود $1+x^n$ فلإيجاد جميع هذه الشفرات يتعيّن علينا إيجاد جميع قواسم $1+x^n$ ويمكن إنجاز ذلك بإيجاد جميع القواسم **غير القابلة للتحليل (Irreducible)**.

نقول إن كثيرة الحدود $f(x)\epsilon K[x]$ التي درجتها أكبر من أو تساوي 1، **غير قابلة للتحليل (Irreducible)** إذا لم نستطع كتابتها كحاصل ضرب كثيرتي حدود في $K[x]$ درجة كل منهما على الأقل 1. إنه ليس بالأمر اليسير إيجاد القواسم غير القابلة للتحليل (ومن ثم جميع القواسم) لكثيرة الحدود $1+x^n$. يُزوّدنا الملحق B بتحليل $1+x^n$ لكل $n \leq 31$ إلى عوامل غير قابلة للتحليل، كما نقدم في المثال (٤,٤,١٤) طريقة لتحليل $1+x^n$.

الشفرة الخطية الدورية المولّدة بالقاسم 1 لكثيرة الحدود $1+x^n$ هي الشفرة التي بُعدها n (لأن درجة 1 تساوي 0) ومن ثم فهي الشفرة K^n. أيضاً الشفرة $C=\{0\}$ حيث 0 الكلمة الصفرية من الطول n هي شفرة دورية مولّدة بكثيرة الحدود $g(x)=0\equiv 1+x^n(mod 1+x^n)$. تُسمى كل من K^n و $\{0\}$ **شفرة دورية غير فعلية (Improper Cyclic Code)** وتُسمى جميع الشفرات الدورية الأخرى، **شفرات دورية فعلية (Proper Cyclic Codes)**.

مثال (٤,٤,١)

إذا كان $n=3$ فنرى أن:

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

هو تحليل $1+x^3$ إلى عوامل غير قابلة للتحليل. وعليه توجد شفرتان فعليتان دوريتان من الطول 3. الأولى منهما مولّدة بكثيرة الحدود $g(x)=1+x$ ولها مصفوفة مولّدة $G=\begin{bmatrix}110\\011\end{bmatrix}$، وهذه الشفرة هي $C=\{000,110,011,101\}$. أما الشفرة الأخرى فهي مولّدة بكثيرة الحدود $g(x)=1+x+x^2$ ومصفوفتها المولّدة هي $G=[111]$. وبهذا تكون $C=\{000,111\}$. ▲

مثال (٤,٤,٢)

إذا كان $n = 6$ فإن تحليل $1 + x^6$ إلى عوامل غير قابلة للتحليل هو:

$$1 + x^6 = (1 + x^3)^2 = (1 + x)^2(1 + x + x^2)^2.$$

وعليه، لإيجاد مولّدات الشفرات الخطية الدورية الفعلية من الطول 6، نقوم بإيجاد جميع حواصل الضرب الممكنة لهذه العوامل (عدا 1 و $1 + x^6$). كل من حواصل الضرب هذه تولّد شفرة خطية دورية فعلية من الطول 6. الجدول التالي يُبيّن كلاً من هذه المولّدات وبُعد الشفرة التي يُولّدها.

البُعد	المولّد
5	$1 + x$
4	$(1 + x)^2 = 1 + x^2$
4	$1 + x + x^2$
2	$(1 + x + x^2)^2 = 1 + x^2 + x^4$
3	$(1 + x)(1 + x + x^2) = 1 + x^3$
2	$(1 + x)^2(1 + x + x^2) = 1 + x + x^3 + x^4$
1	$(1 + x)(1 + x + x^2)^2 = 1 + x + x^2 + x^3 + x^4 + x^5$. ▲

مبرهنة (٤,٤,٣)

إذا كان $n = 2^r s$ فإن $1 + x^n = (1 + x^s)^{2^r}$.

البرهان

باستخدام الاستقراء الرياضي على r. إذا كان $r = 1$ فإن $n = 2s$ ونرى أن:

$$(1 + x^s)^2 = 1 + x^s + x^s + x^{2s} = 1 + x^{2s}$$

وعليه فالعبارة صائبة عندما $r = 1$. لنفرض الآن أن العبارة صحيحة عند $r - 1$[٤]. حينئذ،

$$(1 + x^s)^{2^r} = \left[(1 + x^s)^{2^{r-1}}\right]^2$$

(٤) المترجمان: قمنا بكتابة تفاصيل خطوة الاستقراء للمبرهنة (٤,٤,٣).

$$= (1 + x^{2^{r-1}s})^2 \qquad \text{(خطوة الاستقراء)}$$
$$= 1 + 2x^{2^{r-1}s} + x^{2^{rs}}$$
$$= 1 + x^{2^{rs}}$$

وبهذا تكون العبارة صحيحة عند r. ■

نتيجة (٤,٤,٤)

لنفرض أن $n = 2^r \cdot s$ حيث s عدد فردي ولنفرض أن $1 + x^s$ هي حاصل ضرب عدد z من كثيرات الحدود غير القابلة للتحليل. عندئذ، يوجد عدد $(2^r + 1)^z$ شفرة خطية دورية من الطول n ومن ثم يوجد عدد $(2^r + 1)^z - 2$ شفرة خطية دورية فعلية من الطول n. ■

مثال (٤,٤,٥)

بيّنا في المثال (٤,٤,١) أن $1 + x^3 = (1 + x)(1 + x + x^2)$ حيث كل من $1 + x$ و $1 + x + x^2$ غير قابلة للتحليل. باستخدام النتيجة (٤,٤,٤) حيث $r = 0$، $s = 3$، $z = 2$ نجد أن عدد الشفرات الخطية الدورية من الطول 3 هو $(2^0 + 1)^2 = 4$، منها شفرتان فعليتان كما هو مبيّن في المثال (٤,٤,١). أما لكثيرة الحدود $1 + x^6$ فلدينا $n = 6 = 2^1 \times 3$. عندئذ، $r = 1$، و $z = 2$ ويكون عدد الشفرات الخطية الدورية من الطول 6 هو $(2 + 1)^2 = 9$ حيث 7 منها فعلية وهذا ما وجدناه في المثال (٤,٤,١). ▲

تمارين

(٤,٤,٦) جد عدد الشفرات الخطية الدورية الفعلية من الطول n حيث:

(أ) $n = 4$ (ب) $n = 5$

(ج) $n = 7$ (د) $n = 14$

(هـ) $n = 56$ (و) $n = 15$

(ز) $n = 120$ (ح) $n = 1024$.

(**٤,٤,٧**) جد كثيرة الحدود المولّدة لجميع الشفرات الخطية الدورية من الطول n حيث:

(أ) $n = 4$ (ب) $n = 5$.

(**٤,٤,٨**) جد مولّدين من الدرجة 4 للشفرة الخطية الدورية من الطول 7.

(**٤,٤,٩**) جد مولّداً ومصفوفة مولّدة للشفرة الخطية الدورية من الطول n والبُعد k حيث:

(أ) $n = 12$ ، $k = 5$ (ب) $n = 12$ ، $k = 7$

(ج) $n = 14$ ، $k = 5$ (د) $n = 14$ ، $k = 6$

(هـ) $n = 14$ ، $k = 8$.

(**٤,٤,١٠**) أثبت أن شفرة جولاي C_{23} تكافئ شفرة خطية دورية.

نقدم الآن طريقة سهلة لإيجاد جميع الشفرات الدورية (أي عوامل $(1 + x^n)$) حيث n عدد فردي.

الخطوة الأولى من هذه الطريقة هي توليد جميع كثيرات الحدود $I(x)(mod 1 + x^n)$ التي تحقق $I(x) \equiv I(x)^2 (mod 1 + x^n)$. تُسمى كثيرات الحدود هذه **بكثيرات الحدود متساوية القوى (Idempotent Polynomials)**. إذا كانت كل من $u(x)$ و $v(x)$ كثيرة حدود متساوية القوى فمن السهل أن نرى أن كلاً من $u(x) + v(x)$ و $u(x)v(x)(mod\ 1 + x^n)$ كثيرة حدود متساوية القوى. نحتاج الآن لإنشاء مجموعة "أساسية" من كثيرات الحدود المتساوية القوى. ولهذا الغرض نجزئ المجموعة $\mathbb{Z}_n = \{0,1,2,\cdots,n-1\}$ إلى فصول تكافؤ. لنفرض أن:

$C_i = \{s \equiv 2^i \times i (mod\ n) : j = 0,1,\cdots,r\}$ حيث $1 \equiv 2^r (mod\ n)$.

مثال (٤,٤,١١)

إذا كان $n = 7$ فلدينا $C_0 = \{0\}$ ، $C_1 = \{1,2,4\} = C_2 = C_4$ ، $C_3 = \{3,5,6\} = C_5 = C_7$.

وإذا كان $n = 9$ فلدينا $C_0 = \{0\}$ ، $C_1 = \{1,2,4,8,7,5\}$ ، $C_3 = \{3,6\}$.

الآن، لكل فصل من فصول التكافؤ المختلفة C_i نجد كثيرة حدود مقابلة $c_i(x)$ حيث:

$$c_i(x) = \sum_{j\epsilon C_i} x^j$$

الآن، $c_i(x)$ كثيرة حدود متساوية القوى لأن:

$$c_i(x)^2 = c_i(x^2) = \sum_{j\epsilon C_i} x^{2j} \equiv \sum_{k\epsilon C_i} x^k \ (mod(1 + x^n))$$

وذلك لأنه إذا كان $j\epsilon C_i$ فإن $2j(mod\ n)\epsilon C_i$. لاحظ أيضاً، أنه إذا كانت $I(x)(mod(1 + x^n))$ كثيرة حدود متساوية القوى فإن:

$$I(x) = \sum_{i=0}^{k} a_i c_i(x) \quad \text{حيث } a_i\epsilon\{0,1\}.$$ ▲

مثال (٤,٤,١٢)

إذا كان $n = 7$ فلدينا:

$$c_0(x) = x^0 = 1 \quad ، \ C_0 = \{0\}$$

$$c_1(x) = x + x^2 + x^4 \quad ، \ C_1 = \{1,2,4\}$$

$$c_3(x) = x^3 + x^6 + x^5 \quad ، \ C_3 = \{3,5,7\}.$$

وبهذا، إذا كانت $I(x)(mod1 + x^7)$ كثيرة حدود متساوية القوى فنرى أن:

$$I(x) = a_0c_0(x) + a_1c_1(x) + a_3c_3(x)$$

حيث $a_i\epsilon\{0,1\}$. إذن، يوجد $2^3 - 1$ من كثيرات الحدود المتساوية القوى المختلفة قياس $1 + x^7$ (حيث تجاهلنا كثيرة الحدود المتساوية القوى التافهة $I(x) = 0$). ▲

المبرهنة التالية تقدم لنا العلاقة بين كثيرات الحدود المتساوية القوى والشفرات الدورية:

مبرهنة (٤,٤,١٣)

تحتوي أي شفرة دورية على كثيرة حدود متساوية القوى وحيدة وتولّد الشفرة.

البرهان

لتكن $g(x)$ كثيرة حدود مولّدة للشفرة الدورية من الطول n ولنفرض أن $g(x)h(x) = 1 + x^n$ حيث n فردي.حينئذ، $gcd(h(x), g(x)) = 1$. ونرى استناداً إلى خوارزمية إقليدس (ملحق A) وجود كثيرتي حدود $t(x)$ و $s(x)$ تحققان:

$$1 = t(x)g(x) + s(x)h(x)$$

وبهذا نجد أن:

$$\begin{aligned} t(x)g(x) &= (t(x)g(x))^2 + t(x)s(x)h(x)g(x) \\ &= (t(x)g(x))^2 + t(x)s(x)(1 + x^n) \\ &\equiv \big(t(x)g(x)\big)^2 (mod 1 + x^n) \end{aligned}$$

إذن، $t(x)g(x)$ كثيرة حدود متساوية القوى و $g(x) = \gcd(t(x)g(x), 1 + x^n)$. ■

مثال (٤,٤,١٤)

لإيجاد جميع الشفرات الدورية من الطول 9، يكفي أن نجد جميع كثيرات الحدود المتساوية القوى ومن ثم إيجاد كثيرات الحدود المولّدة المقابلة لها. بما أن:

$$C_0 = \{0\} \ ، \ C_1 = \{1,2,4,8,7,5\} \ ، \ C_3 = \{3,6\}$$

فنرى أن $c_0(x) = 1$ ، $c_1(x) = x + x^2 + x^4 + x^5 + x^7 + x^8$ ، $c_3(x) = x^3 + x^6$ وأن:

$$I(x) = a_0c_0(x) + a_1c_1(x) + a_3c_3(x).$$

والجدول التالي يُبيّن $I(x)$ وكثيرة الحدود المولّدة المقابلة لها:

كثيرة الحدود المولّدة $g(x) \equiv gcd(I(x), 1+x^9)$	كثيرة الحدود المتساوية القوى $I(x)$
1	1
$1+x+x^3+x^4+x^6+x^7$	$x+x^2+x^4+x^5+x^7+x^8$
$1+x^3$	x^3+x^6
$1+x+x^2$	$1+x+x^2+x^4+x^5+x^7+x^8$
$1+x^3+x^6$	$1+x^3+x^6$
$1+x$	$x+x^2+x^3+x^4+x^5+x^6+x^7+x^8$
$1+x+x^2+x^3+x^5+x^6+x^7+x^8$	$1+x+x^2+x^3+x^5+x^6+x^7+x^8$. ▲

تمرين

(**٤,٤,١٥**) جد جميع كثيرات الحدود المتساوية القوى قياس $1+x^n$ وكثيرات الحدود المولّدة المقابلة لها لقيم n التالية:

(أ) $n=5$ (ب) $n=7$ (ج) $n=11$

(د) $n=15$ (هـ) $n=31$.

(٤,٥) الشفرات الدورية الثنوية

Dual Cyclic Codes

إحدى الخواص المهمة للشفرات الدورية هي أن الشفرة الثنوية هي شفرة دورية أيضاً وسنقدم طريقة لإنشاء كثيرة حدود مولّدة للشفرة الثنوية.

سنبرهن الآن أن الشفرة الثنوية للشفرة الدورية هي دورية أيضاً. يعتمد هذا البرهان على الملاحظة التالية: إذا كان $a \cdot b = 0$ وكانت π الإزاحة الدورية فإن:

$$a \cdot b = a_0 b_0 + a_1 b_1 + \cdots + a_n b_n = 0$$
$$\Rightarrow \pi(a) \cdot \pi(b) = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n + a_0 b_0 = 0$$

لنفرض الآن أن C شفرة دورية مولّدة بالكلمة v. عندئذ،

$$C = \langle \{v, \pi(v), \cdots, \pi^{n-1}(v)\} \rangle.$$

إذا كانت $u \epsilon C^{\perp}$ فنجد أن $\pi^i(v) \cdot u = 0$ لكل $i = 0,1,\cdots,n-1$. وعليه فإن $\pi^{i+1}(v) \cdot \pi(u) = 0$ ويكون $\pi(u)$ متعامداً على $\langle \{\pi(v), \pi^2(v), \cdots, \pi^n(v)\} \rangle = C$؛ وذلك لأن $\pi^n(v) = v$. وبما أن $u \epsilon C^{\perp}$ يؤدي إلى أن $\pi(u) \epsilon C^{\perp}$ فنخلص إلى أن $C^{\perp}$ دورية.

لإيجاد مولِّد للشفرة الثنوية نحتاج إلى إيجاد علاقة بين ضرب كثيرات الحدود والضرب القياسي للمتجهات.

تمهيدية (٤,٥,١)

لنفرض أن $a \leftrightarrow a(x)$ ، $b \leftrightarrow b(x)$ ، $b' \leftrightarrow b'(x) \equiv x^n b(x^{-1}) (mod 1 + x^n)$. عندئذ، $a(x)b(x)(mod 1 + x^n) = 0$ إذا وفقط إذا كان $\pi^k(a) \cdot b' = 0$ لكل $k = 0,1,\cdots,n-1$.

البرهان

لنفرض أن $c(x) \equiv a(x)b(x)(mod 1 + x^n)$. بملاحظة أن $x^k \equiv x^{n+k}(mod 1 + x^n)$ فنجد أن معامل x^k في $c(x)$ هو:

$$c_k = a_k b_0 + a_{k+1} b_{n-1} + \cdots + a_{n-1} b_{k+1} + a_0 b_k + \cdots + a_{k-1} b.$$

الآن، إذا كان $a = (a_0, a_1, \cdots, a_{n-1})$ و $b = (b_0, b_1, \cdots, b_{n-1})$ فيكون:

$$b' = (b_0, b_{n-1}, b_{n-2}, \cdots, b_1)$$ و $$c_k = \pi^k(a) \cdot b'.$$

إذن، $c_k = 0$ لكل $k = 0,1,\cdots,n-1$. إذا وفقط إذا كان:

$$c(x) = 0 \equiv a(x)b(x)(mod 1 + x^n).$$ ■

لنفرض أن C شفرة خطية دورية من الطول n وأن $g(x)$ كثيرة حدود مولّدة للشفرة C. حينئذ، $g(x)$ تقسم $1 + x^n$ ومن ثم توجد كثيرة حدود وحيدة $h(x)$ تحقق $1 + x^n = g(x)h(x)$. واستناداً إلى التمهيدية (٤,٥,١) نعلم أن $x^n h(x^{-1}) \epsilon C^{\perp}$.

مبرهنة (٤,٥,٢)

لنفرض أن C شفرة خطية دورية من الطول n والبُعد k ولنفرض أن $g(x)$ كثيرة حدود مولّدة للشفرة C. إذا كان $1+x^n=g(x)h(x)$ فإن $C^{\perp}$ شفرة دورية من البُعد $n-k$ و $x^n h(x^{-1})$ كثيرة حدود مولّدة لها.

البرهان

بما أن بُعد C يساوي k ودرجة $g(x)$ تساوي $n-k$ فتكون درجة $h(x)$ تساوي k. وبما أن $g(x)h(x)=1+x^n$ فنرى أن $g(x^{-1})h(x^{-1})=1+(x^{-1})^n$ وأن:

$$x^n g(x^{-1})h(x^{-1})=x^n(1+x^{-n})$$

$$x^{n-k}g(x^{-1})x^k h(x^{-1})=1+x^n$$

إذن، $x^k h(x^{-1})$ قاسم لكثيرة الحدود $1+x^n$ درجتها تساوي k وبهذا تكون مولّدة للشفرة الخطية الدورية $C^{\perp}$ ذات البُعد $n-k$ التي تحتوي $x^n h(x^{-1})$. ■

مثال (٤,٥,٣)

كثيرة الحدود $g(x)=1+x+x^3$ تولّد شفرة خطية دورية من الطول 7 والبُعد $k=7-3=4$. وبما أن $g(x)$ قاسم لكثيرة الحدود $1+x^7$ فنستطيع إيجاد كثيرة حدود $h(x)$ تحقق $1+x^7=g(x)h(x)$. ونرى بالقسمة المطوّلة أن $h(x)=1+x+x^2+x^4$. إذن، كثيرة الحدود المولّدة للشفرة $C^{\perp}$ هي:

$$g^{\perp}(x)=x^4h(x^{-1})=x^4(1+x^{-1}+x^{-2}+x^{-4})=1+x^2+x^3+x^4$$

وتقابل الكلمة $w=1011100$. من الواضح أن $g\cdot w=(11010000)(1011100)$ وأن $\pi^k(g)\cdot w=0$. لاحظ أن $g^{\perp}(x)\neq h(x)$ في هذا المثال. ▲

مثال (٤,٥,٤)

كثيرة الحدود $g(x)=1+x+x^2$ تولّد شفرة خطية دورية من الطول 6 وكثيرة الحدود $h(x)$ التي تحقق $g(x)h(x)=1+x^6$ هي $h(x)=1+x+x^3+x^4$. إذن،

$g^{\perp}(x) = x^4 h(x^{-1}) = x^4(1 + x^{-1} + x^{-2} + x^{-4}) = x^4 + x^3 + x + 1$ هي كثيرة حدود مولّدة للشفرة الثنوية. لاحظ أن $g^{\perp}(x) = h(x)$ في هذا المثال. ▲

تمرين

(**٤,٥,٥**) جد كثيرة حدود مولّدة لشفرة ثنوية للشفرة الدورية من الطول n التي كثيرة حدودها المولّدة $g(x)$ هي :

(أ) $g(x) = 1 + x^2$ ، $n = 6$.

(ب) $g(x) = 1 + x^3$ ، $n = 6$.

(ج) $g(x) = 1 + x^2$ ، $n = 8$.

(د) $g(x) = 1 + x^3 + x^6$ ، $n = 9$.

(هـ) $g(x) = 1 + x + x^4$ ، $n = 15$.

(و) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ ، $n = 15$.

(ز) $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$ ، $n = 23$.

(ح) $g(x) = 1 + x + x^2 + x^4$ ، $n = 7$.