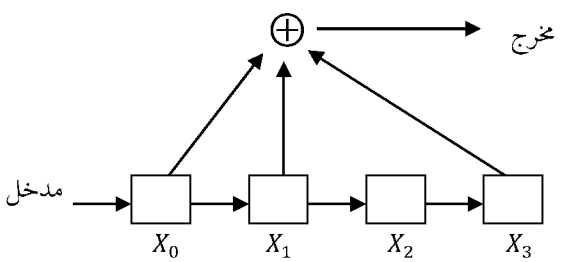
الفصل الثامن

شفرات التلاف
Convolutional Codes

(٨,١) مسجلات الإزاحة وكثيرات الحدود
Shift Registers & Polynomials

أحد الأسباب التي تجعل للشفرات الدورية أهمية خاصة هي وجود أدوات فعّالة لتنفيذ عمليتي تشفير وفك تشفير كثيرات الحدود، تُدعى **مسجلات الإزاحة (Shift Registers)**. يتكون مسجل الإزاحة من عدد n من المسجلات (أو عناصر تأخير) وساعة وظيفتها التحكم في حركة أو إزاحة البيانات الموجودة على المسجلات. بعد كل تكّة من تكّات الساعة تجري عملية جمع ثنائية على المحتويات الجديدة للمسجلات لنحصل على مخرج. ففي الشكل (٨,١)، المربعات تمثل المسجلات، المتجهات تمثل اتجاه تدفق البيانات وأخيراً ⊕ هي عملية الجمع الثنائي.



الشكل (٨,١). مسجل إزاحة.

مثال (٨,١,١)

يتكون مسجل الإزاحة في الشكل (٨,١) من أربعة مسجلات X_0, X_1, X_2, X_3 كل منها يحتوي على إحداثيات ثنائية. وكما هو مبين من الاتجاهات يتكون المخرج عند كل تكّة ساعة بجمع محتويات المسجلات الثلاثة X_0, X_1, X_3. لنفرض أن محتويات المسجلات X_0, X_1, X_2, X_3 هي 1,1,0,1 على التوالي. إذا كان المدخل التالي هو الإحداثي 0 فعند تكّة الساعة التالية، تتم إزاحة المدخل إلى المسجل X_0 وفي الوقت نفسه تتم إزاحة محتوى كل من المسجلات إلى المسجل الذي يليه. ولذا تكون المحتويات الجديدة للمسجلات X_0, X_1, X_2, X_3 هي 0,1,1,0 على التوالي ويكون المخرج هو $X_0 + X_1 + X_3 = 0 + 1 + 0 = 1$. ▲

لنفرض أن $a_0, a_1, a_2, \cdots$ هي متتالية مدخلات. عندئذ، يمكن استخدام جدول لمعرفة كل من المدخل، المخرج، محتويات المسجلات عند كل تكّة ساعة.

مثال (٨,١,٢)

لنفرض أن محتويات المسجلات الأربعة في مسجل إزاحة مراحل عددها 4 المبين في الشكل (٨,١) هي في البداية (0,0,0,0) وأن المدخلات $a_0, a_1, a_2, \cdots, a_6$ هي 1010000. الجدول التالي يلخص لنا محتويات المسجلات والمخرجات:

الزمن	المدخل	$X_0X_1X_2X_3$	المخرج $= X_0 + X_1 + X_3$
-1	—	0000	—
0	1	1000	1
1	0	0100	1
2	1	1010	1
3	0	0101	0
4	0	0010	0
5	0	0001	1
6	0	0000	0

ولهذا يكون مخرج مسجل الإزاحة هو 1110010 عندما يكون المدخل 1010000 ومحتويات المسجلات في البداية هي 0000. ▲

بصورة عامة، مسجل إزاحة مراحل عددها s هو مسجل إزاحة يحتوي على عدد s من المسجلات. مخرج مسجل إزاحة مراحل عددها s هو تركيب خطي لمحتويات المسجلات ويمكن وصفه باستخدام معاملات $g_0, g_1, \cdots, g_{s-1}$ حيث $g_i \epsilon K = \{0,1\}$. أي أن:

$$c_t = g_0 X_0(t) + g_1 X_1(t) + \cdots + g_{s-1} X_{s-1}(t)$$

حيث c_t هو المخرج عند الزمن t و $X_i(t)$ هو قيمة محتوى المسجل X_i عند الزمن t.

من الممكن استخدام كثيرات الحدود لوصف عمل هذه الأدوات، فإذا كانت $g_0, g_1, \cdots, g_{s-1}$ هي معاملات مسجل إزاحة مراحل عددها s فتكون كثيرة الحدود المقابلة لهذا المسجل هي:

$$g(x) = g_0 + g_1 x + \cdots + g_{s-1} x^{s-1}.$$

تُسمى كثيرة الحدود هذه بكثيرة الحدود المولّدة لمسجل الإزاحة. على سبيل المثال، $g(x) = 1 + x + x^3$ هي كثيرة حدود مولّدة لمسجل إزاحة مراحل عددها 4 المبين في الشكل (٨,١).

إذا كانت $a(x)$ كثيرة حدود المقابلة لمتتالية المدخل، $c(x)$ هي كثيرة الحدود المقابلة لمتتالية المخرج وكانت $g(x)$ هي كثيرة حدود مسجل الإزاحة فسنرى لاحقاً أن:

$$c(x) = a(x)g(x).$$

مثال (٨,١,٣)

كثيرة حدود مسجل الإزاحة المبين في الشكل (٨,١) هي $g(x) = 1 + x + x^3$. كثيرة الحدود المقابلة لمتتالية المدخل 1010000 هي $a(x) = 1 + x^2$. إذا افترضنا بداية أن محتويات المسجلات الأربعة هي 0000 فنرى استناداً إلى المثال (٨,١,٢) أن متتالية المخرج هي 1110010 وكثيرة حدودها المقابلة هي $c(x) = 1 + x + x^2 + x^5$. وبهذا نرى أن:

$$\begin{aligned} a(x)g(x) &= (1 + x^2)(1 + x + x^2) \\ &= 1 + x + x^2 + x^5 \\ &= c(x) \end{aligned}$$

▲

مثال (٨,١,٤)

لنفرض أن $g(x) = 1 + x + x^3$ هي كثيرة الحدود المقابلة لمسجل الإزاحة المقدم في الشكل (٨,١). الجدول التالي يُبيّن متتالية المخرجات عندما تكون متتالية المدخلات هي $a_0, a_1, a_2, a_3, 0,0,0$.

الزمن	المدخل	X_0	X_1	X_2	X_3	المخرج $= X_0 + X_1 + X_3$
-1	—	0	0	0	0	—
0	a_0	a_0	0	0	0	a_0
1	a_1	a_1	a_0	0	0	$a_1 + a_0$
2	a_2	a_2	a_1	a_0	0	$a_2 + a_1$
3	a_3	a_3	a_2	a_1	a_0	$a_3 + a_2 + a_0$
4	0	0	a_3	a_2	a_1	$a_3 + a_1$
5	0	0	0	a_3	a_2	a_2
6	0	0	0	0	a_3	a_3

من الواضح أن:

$$\begin{aligned} a(x)g(x) &= (a_0 + a_1x + a_2x^2 + a_3x^3)(1 + x + x^3) \\ &= a_0 + (a_1 + a_0)x + (a_2 + a_1)x^2 + (a_3 + a_2 + a_0)x^3 \\ &\quad + (a_3 + a_1)(x^4 + a_2x^5 + a_3x^6) \\ &= c(x) \end{aligned}$$

معاملات $c(x)$ تقابل متتالية المخرجات لهذا المسجل. ▲

لتكن $g(x)$ كثيرة حدود شفرة خطيّة دورية من الدرجة $n - k$. من الممكن تصميم مسجل إزاحة مراحل عددها $n - k + 1$ كثيرة حدوده المولّدة هي $g(x)$ لغرض تشفير كثيرات حدود المعلومات $a(x)$ باستخدام كثيرات الحدود.

تمارين

(٨,١,٥) ارسم مخططاً لمسجل الإزاحة المقابل لكثيرة الحدود المولّدة $g(x)$ حيث:

(أ) $g(x) = 1 + x$ (ب) $g(x) = 1 + x^2$

(ج) $g(x) = 1 + x^2 + x^3$ (د) $g(x) = 1 + x^3 + x^4$.

(٨,١,٦) استخدم مسجل الإزاحة المنشأ في التمرين **(٨,١,٥)** لحساب $c(x) = a(x)g(x)$.

احسب $a(x)g(x)$ مباشرة ثم قارن الإجابتين:

(أ) $a(x) = 1 + x$ ، $g(x) = 1 + x^2$.

(ب) $a(x) = 1 + x^3 + x^6$ ، $g(x) = 1 + x^3 + x^4$.

(ج) $a(x) = x + x^2$ ، $g(x) = 1 + x^2 + x^3$.

(د) $a(x) = x^2 + x^5 + x^6$ ، $g(x) = 1 + x^3 + x^4$.

(٨,١,٧) افرض أن $g(x) = 1 + x + x^3$ هي كثيرة الحدود المولّدة لمسجل الإزاحة المقدم في الشكل **(٨,١)**. احسب متتالية المخرجات $c_0, c_1, c_2, \cdots$ لكل من متتالية المدخلات $a_0, a_1, a_2, \cdots$ المبينة فيما يلي بافتراض أن محتويات جميع المسجلات هي في البداية 0:

(أ) $10101000\cdots$.

(ب) $0011000\cdots$.

(ج) $1010010000\cdots$.

مبرهنة (٨,١,٨)

لتكن $g(x) = g_0 + g_1x + \cdots + g_{l-1}x^{l-1}$ كثيرة حدود مولّدة لمسجل إزاحة ولتكن $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ كثيرة الحدود المقابلة لمتتالية المخرجات $c_0, c_1, \cdots$. عندئذ، $c(x) = a(x)g(x)$.

البرهان

لاحظ أولاً أنه إذا كان $c(x) = a(x)g(x)$ فإن:

$$c_t = \begin{cases} g_0a_t + g_1a_{t-1} + \cdots + a_0g_t & ,t \le l-1 \\ g_0a_t + g_1a_{t-1} + \cdots + a_{t-l+1}g_{l-1} & ,t > l-1 \end{cases}.$$

حيث افترضنا أن $a_t = 0$ عندما يكون $t > k - 1 = deg(a(x))$.

لنفرض الآن أن $g(x)$ هي كثيرة الحدود المولّدة لمسجل إزاحة. عندئذ، المخرج عند الزمن t هو تركيب خطي للمقادير $X_i(t)$:

$$c_t = g_0X_0(t) + g_1X_1(t) + \cdots + g_{l-1}X_{l-1}(t).$$

عند الزمن $t = 0$ يكون:

$$X_0(0) = a_0\,, X_1(0) = \cdots = X_{l-1}(0) = 0.$$

ومن ثم فإن $c_0 = g_0a_0$.

عند الزمن t حيث $t \le l - 1$ يكون:

$$X_0(t) = a_t\,, X_1(t) = a_{t-1}, \cdots, X_t(t) = a_0.$$

ومحتويات بقية المسجلات أصفار. إذن،

$$c_t = g_0a_t + g_1a_{t-1} + \cdots + g_ta_0.$$

وأخيراً عند الزمن t حيث $t > l - 1$ يكون:

$$X_0(t) = a_t\,, X_1(t) = a_{t-1}, \cdots, X_{l-1}(t) = a_{t-l+1}.$$

وبهذا نرى أن:

$$c_t = g_0a_t + g_1a_{t-1} + \cdots + g_{l-1}a_{t-l+1}.$$

فعليه نخلص إلى أن $c(x) = a(x)g(x)$. ■

من الممكن تنفيذ ضرب كثيرات الحدود (ومن ثم استخدام كثيرات الحدود في تشفير الشفرات الدورية) باستخدام مسجلات الإزاحة على النحو التالي: كثيرة الحدود $g(x)$ المولّدة لمسجل الإزاحة هي كثيرة الحدود المولّدة للشفرة الخطّية الدورية. من الممكن إجراء بعض التعديلات على مسجلات الإزاحة لنحصل على مسجلات إزاحة نستطيع استخدامها لتنفيذ قسمة كثيرات الحدود حيث تستخدم هذه في فك تشفير الشفرات الخطّية الدورية. تُسمى الأداة التي تستخدم لتنفيذ قسمة كثيرات الحدود (ومن ثم فك تشفير الشفرات الخطّية الدورية)، **مسجلات إزاحة ذات تغذية إرجاعية (Feedback Shift Registers)** أو اختصاراً FSR وهي عبارة عن مسجلات إزاحة تسمح

بإرجاع المخرجات إلى المسجلات. (يمكن للقارئ المهتم فقط بشفرات التلاف أن يتجاهل ما تبقى من هذا البند).

تذكّر أنه إذا كانت H مصفوفة اختبار نوعية لشفرة دورية كثيرة حدودها المولّدة هي $g(x)$ فإن الصف i من المصفوفة H هو $r_i \leftrightarrow r_i(x)$ حيث $r_i(x) \equiv x^i (mod\ g(x))$.

وعلى وجه الخصوص $r_i(x) \equiv x r_{i-1}(x) (mod\ g(x))$.

مثال (٨,١,٩)

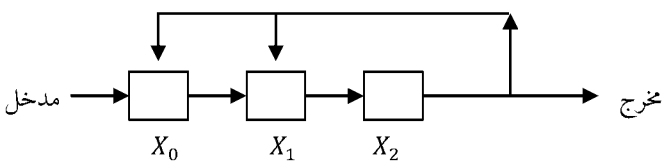
لتكن $g(x) = 1 + x + x^3$ كثيرة الحدود المولّدة. عندئذ، نرى في مصفوفة اختبار النوعية أن:

$$r_3 = 110 \leftrightarrow 1 + x \equiv x^3 (mod\ g(x)).$$

$$r_4 = 011 \leftrightarrow x + x^2 \equiv x^4 (mod\ g(x)).$$

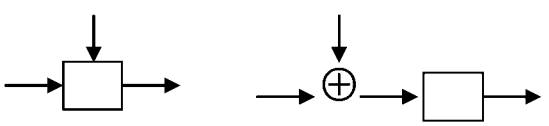
ولكن $r_5 \leftrightarrow x^2 + x^3 (mod\ g(x))$ أو $r_5 = 001 + 110$.

ينظر إلى المتجه 110 على أنه المتجه الارجاعي الذي يتم جمعه ارجاعياً إلى المسجلات عندما يكون المخرج هو الإحداثي 1. مسجل الإزاحة ذو التغذية الإرجاعية المبين في الشكل (٨,٢) يوضح كيفية تنفيذ هذه العملية.



الشكل (٨,٢). مسجل إزاحة ذو تغذية إرجاعية.

إذا تم إدخال أكثر من إحداثي واحد إلى المسجل سنفترض أن محتوى المسجل هو المجموع الثنائي لهذه القيم. أي أن الشكلين التاليين يمثلان الوضع نفسه:



عند كل تكّة ساعة يتم إزاحة المدخل ومحتويات المسجلات ويتم أيضاً إضافة المخرج c_t إلى مسجلات مختارة. أي أن يتم إضافة المتجه الجديد $c_t(1,1,0)$ إلى محتويات المسجلات.

الزمن	المدخل	$X_0 + c_t$	$X_1 + c_t$	X_2	المخرج $= c_t$
-1	—	0	0	0	—
0	1	1	0	0	0
1	0	0	1	0	0
2	0	0	0	1	0
3	0	$0+1$	$0+1$	0	1
4	0	0	1	1	0
5	0	$0+1$	$0+1$	1	1
6	0	$0+1$	$1+1$	1	1
.7 ▲	0	1	0	0	1

بصورة عامة، يوجد تقابل بين مسجل إزاحة مراحل عددها s ذي تغذية إرجاعية حيث $(g_0, g_1, \cdots, g_{s-1})$ هو متجه التغذية الإرجاعية وبين كثيرة الحدود من الدرجة s التالية:

$$g(x) = g_0 + g_1 x + \cdots + g_{s-1}x^{s-1} + x^s$$

محتويات المسجلات عند الزمن $t = deg(c(x))$ هي باقي خارج قسمة $c(x)$ على $g(x)$ ومتتالية المخرجات هي خارج القسمة $a(x)$. مع ملاحظة أن التغذية الإرجاعية لإحداثيات الكلمة المستقبلة تتم بترتيب عكسي للإحداثيات. لاحظ أن درجة كثيرة الحدود المقابلة لـ FSR تساوي s بينما درجة كثيرة الحدود المقابلة لمسجل إزاحة تساوي $s-1$ ومع ذلك فعدد المسجلات في كلتا الحالتين يساوي s.

مثال (٨,١,١٠)

لتكن $x + x^2 + x^4$ هي كثيرة الحدود المستقبلة وأنها تقابل الكلمة 0110100. إذا كانت $g(x) = 1 + x + x^3$ فإن FSR المقابل لها هو المبين في الشكل (٨,٢).

الزمن	المدخل	X_0	X_1	X_2	المخرج
-1	—	0	0	0	—
0	1	1	0	0	0
1	0	0	1	0	0
2	1	1	0	1	0
3	1	$1+1$	$1+1$	0	1
4	0	0	0	0	0

باقي القسمة هو 000 وخارج القسمة هو $x \leftrightarrow 0100000$ ويقابل متتالية المخرجات بترتيب عكسي للإحداثيات. ▲

بصورة عامة، محتويات المسجلات عند الزمن $t = n$ هو الباقي $c(x)(mod\ g(x))$ حيث $c(x)$ تقابل متتالية المدخلات.

مبرهنة (٨,١,١١)

تغذية $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ إلى مسجل FSR الذي يقابل $g(x) = g_0 + g_1x + \cdots + 1x^s$ بترتيب عكسي للإحداثيات (أي $c_{n-1}, c_{n-2}, \cdots, c_0$) تكافئ قسمة $c(x)$ على $g(x)$. المخرج بعد n تكّة ساعة هو خارج القسمة (بترتيب عكسي للمعاملات) ومحتويات المسجلات هي باقي القسمة (بترتيب عكسي للمعاملات).

البرهان

بما أن مخرج مجموع متتاليتي مدخلات هو مجموع متتاليتي المخرجات المقابلة فيكفي أن نتحقق من صواب المبرهنة للحالة $c(x) = x^l$. ولكن في هذه الحالة يكون من الواضح أن FSR يقابل الخوارزمية المقدمة سابقاً (انظر المثال (٤,٣,٧)) لحساب $(x^l(mod\ g(x))$. وبهذا فمحتويات المسجلات هي الباقي. كما أنه ليس بالأمر الصعب اثبات أن المخرج هو خارج قسمة $c(x)$ على $g(x)$. ■

تمارين

(٨,١,١٢) ليكن FSR هو المبيّن في الشكل **(٨,٢)** حيث تحتوي المسجلات بداية على أصفار. جد متتالية المخرجات لكل من الكلمات المستقبلة التالية. بيّن وضع المسجلات في النهاية وخارج القسمة إذا كان الباقي يساوي صفراً:

(أ) 0011010 (ب) 1010110 (ج) 0010001.

(٨,١,١٣) لتكن $g(x) = 1 + x + x^3$. احسب كثيرة حدود التناذر لكل من الكلمات المستقبلة في التمرين **(٨,١,١٢)**. قارن كثيرة حدود التناذر مع كثيرة الحدود المقابلة للوضع النهائي للمسجلات التي وجدت في التمرين **(٨,١,١٢)**.

(٨,١,١٤) لكل من كثيرات الحدود المولّدة أنشئ FSR. احسب متتالية المخرجات ثم جد الوضع النهائي للمسجلات لمتتالية المدخلات $c(x)$.

(أ) $g(x) = 1 + x^2 + x^3$ ، $c = 0010110$.

(ب) $g(x) = 1 + x + x^2$ ، $c = 111$.

(ج) $g(x) = 1 + x + x^4$ ، $c = 010000000100000$.

(٨,٢) تشفير شفرات التلاف
Encoding Convolutional Codes

شفرات التلاف هي شفرات عملية جداً وهي تستخدم إضافة إلى شفرات ريد وسولومن من قبل NASA و ESA للوثوق من صحة الاتصالات أثناء القيام بالرحلات الفضائية.

تُشفّر كل من الرسائل أولاً باستخدام شفرة ريد وسولومن ومن ثم تستخدم شفرة التلاف لتشفير الرسالة الناتجة عن ذلك. ندرس في البنود القادمة عملية تشفير وفك التشفير باستخدام شفرات التلاف ونناقش بعض المسائل التي تنشأ عن هذه الشفرات ونبدأ بالتعريف التالي:

شفرة التلاف (الثنائية) من النوع $(n, k = 1, m)$ وذات كثيرات الحدود المولّدة $g_1(x), \cdots, g_n(x)$ حيث $g_i(x) = g_{i,0} + g_{i,1}x + \cdots + g_{i,m}x^m$ ، $g_i \epsilon K[x]$ هي الشفرة المكوّنة من كلمات الشفرة $c(x) = (c_1(x), c_2(x), \cdots, c_n(x))$ حيث $c_i(x) = m(x)g_i(x)$ و $m(x) = m_0 + m_1x + m_2x^2 + \cdots \epsilon K[x]$. (سنكتب بالتفصيل عن العدد k لاحقاً حيث اعتبرنا لغرض السهولة أن قيمته تساوي 1 في هذا التعريف). لاحظ أن $m(x)$ هي الرسالة التي يتم تشفيرها إلى $c(x)$. لنفرض أن كلاً من $c(x)$ و $c'(x)$ كلمة شفرة. عندئذ،

$$\begin{aligned} c(x) + c'(x) &= \big(c_1(x), \cdots, c_n(x)\big) + (c_1'(x), \cdots, c_n'(x)) \\ &= \big(m(x)g_1(x), \cdots, m(x)g_n(x)\big) + (m'(x)g_1(x), \cdots, m'(x)g_n(x)\big) \\ &= (\big(m(x) + m'(x)\big)g_1(x), \cdots, \big(m(x) + m'(x)\big)g_n(x)) \end{aligned}$$

وهذا ما هو إلا كلمة الشفرة المقابلة للرسالة $m(x) + m'(x)$. إذن، شفرة التلاف هي شفرة خطيّة.

وجه الاختلاف بين شفرات التلاف والشفرات التي درسناها سابقاً هو أن طول الشفرات وطول الرسائل غير منته في شفرات التلاف.

مثال (٨,٢,١)

لتكن C_1 شفرة تلاف من النوع (2,1,3) حيث $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$. سنستخدم C_1 لتشفير الرسالتين التاليتين:

(أ) يتم تشفير الرسالة $m(x) = 1 + x^2$ إلى:

$$\begin{aligned} c(x) &= \big((1 + x^2)g_1(x), (1 + x^2)g_2(x)\big) \\ &= (1 + x + x^2 + x^5, 1 + x^3 + x^4 + x^5) \\ &\leftrightarrow (11100100\cdots, 10011100\cdots) \end{aligned}$$

(ب) يتم تشفير الرسالة $m(x) = 1 + x + x^2 + x^3 + \cdots = \sum_{i=0}^{\infty} x^i$ إلى:

$$c(x) = (1 + x^3 + x^4 + x^5 + \cdots, 1 + x + x^3 + x^4 + x^5 + \cdots)$$

$$= \left(1 + \sum_{i=3}^{\infty} x^i, 1 + x + \sum_{i=3}^{\infty} x^i\right)$$

$$\leftrightarrow (100111\cdots, 110111\cdots) \quad \blacktriangle$$

تمارين

(٨,٢,٢) شفّر الرسائل التالية باستخدام شفرة تلاف من النوع (3,1,3) حيث كثيرات الحدود المولّدة هي $g_1(x) = 1 + x + x^3$ ، $g_2(x) = 1 + x + x^2 + x^3$ ، $g_3(x) = 1 + x^2 + x^3$.

(أ) $m(x) = 1 + x^3$ (ب) $m(x) = 1 + x + x^3$

(ج) $m(x) = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$.

(٨,٢,٣) شفّر الرسائل التالية باستخدام شفرة تلاف من النوع (2,1,4) حيث كثيرتي الحدود المولّدة هي $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

(أ) $m(x) = 1 + x + x^2$ (ب) $m(x) = 1 + x + x^3$

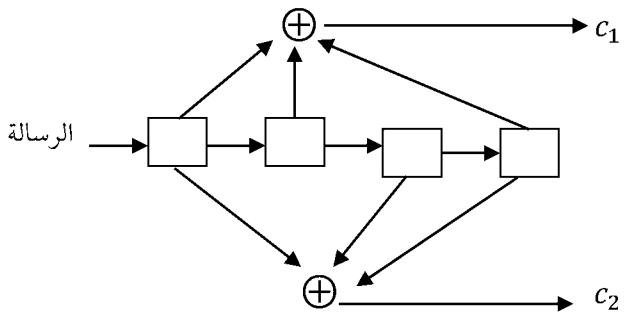
(ج) $m(x) = 1 + x^2 + x^4 + \cdots = \sum_{i=0}^{\infty} x^{2i}$.

استناداً إلى المبرهنة **(٨,١,٨)** نرى إمكانية وصف شفرات التلاف بدلالة مسجلات الإزاحة على النحو التالي:

$c_i(x)$ هي مخرج مسجل الإزاحة المولّد بكثيرة الحدود $g_i(x)$ عندما يكون المدخل هو $m(x)$.

مثال (٨,٢,٤)

يمكن وصف شفرة التلاف C_1 المقدمة في المثال **(٨,٢,١)** بدلالة مسجل إزاحة كثيرتي حدوده المولّدة وهما $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$ كما هو مبيّن في الشكل **(٨,٣)**.



الشكل (٨,٣). تشفير باستخدام شفرة تلاف C_1 من النوع $(2,1,3)$.

باستخدام هذا الوصف، إذا كانت الرسالة المراد تشفيرها هي $m(x) = 1 + x^2 \leftrightarrow 10100\cdots$ فإن $c_1 = 11100100\cdots$ وهذا يتفق مع الحسابات التي أُجريت في المثال **(٨,٢,١)**. وبالمثل يمكن رؤية أن c_2 هي $10011100\cdots$. ▲

من الممكن تحويل $c(x)$ إلى إحداثيات كلمة واحدة عوضاً عن إحداثيات n من الكلمات، وذلك بالتوريق البيني لكثيرات الحدود $c_1(x), c_2(x), \cdots, c_n(x)$. في ما تبقى من هذا الفصل سنعتبر أن $c(x)$ مورّقة بينياً وبهذا يتكون المخرج من معاملات x^0 في كثيرات الحدود $c_1(x), \cdots, c_n(x)$ متبوعة بمعاملات $x, x^2, \cdots$. وعند عرض $c \leftrightarrow c(x)$ بهذا الشكل للتوريق البيني نقوم بضم الإحداثيات التي عددها n والتي هي معاملات x^i ، $i \geq 0$ بعضها مع بعض.

مثال (٨,٢,٥)

التوريق البيني لتمثيل $c(x)$ المقدمة في المثال **(٨,٢,١)** (أ) هو:

$$c = 11\ 10\ 10\ 01\ 01\ 11\ 00\ 00\ \cdots$$

والتوريق البيني لتمثيل $c(x)$ المقدمة في المثال **(٨,٢,١)** (ب) هو:

$$c = 11\ 01\ 00\ 11\ 11\ 11\ \cdots.$$

▲

تمرين

(**٨,٢,٦**) أنشئ مسجل إزاحة مناسب للتشفير لكل من شفرتي التلاف المقدمتين في التمرينين (**٨,٢,٢**) و (**٨,٢,٣**). ثم استخدم مسجل الإزاحة لتشفير الرسائل المقدمة في التمرينين. جد التوريق البيني لكل من كلمات الشفرة.

إذا تم تشفير شفرة تلاف ثنائية من النوع $(n,1,m)$ باستخدام مسجلات الإزاحة فنرى أن إزاحة إحداثي واحد من إحداثيات الرسالة إلى مسجل الإزاحة ينتج عنه عدد n من إحداثيات الشفرة بواقع إحداثي واحد لكل من $c_1(x),\cdots,c_n(x)$. وبهذا يكون معدل المعلومات لمثل شفرة التلاف هذه هو $\frac{1}{n}$ (تذكر أن معدل معلومات شفرة يقيس جزء المعلومات التي يحملها كل إحداثي من إحداثيات كلمة الشفرة). ولذا، يكون من المناسب إنشاء شفرات تلاف معدل معلوماتها مختلف عن $\frac{1}{n}$، وعلى وجه الخصوص شفرات تلاف معدل معلوماتها أكبر من $\frac{1}{2}$.

إن الطريقة الواضحة لإنجاز ذلك تكون بتحريك أكثر من إحداثي واحد (وليكن عدد k من الإحداثيات) من إحداثيات الرسالة إلى مسجل الإزاحة قبل القيام بحساب الإحداثيات التالية لكلمات الشفرة، وبهذا نحصل على شفرة معدل معلوماتها يساوي $\frac{k}{n}$. وهذا في الحقيقة هو دور العدد k في تعريف شفرة التلاف من النوع (n,k,m). لاحظ أنه لو اتبعنا ذلك لوجدنا أن كل إحداثي من إحداثيات الرسالة سيظهر في المسجلات $X_i,X_{i+k},X_{i+2k},\cdots$ حيث i عدد يحقق $0\le i<k$. ولذا عوضاً عن تحريك k من إحداثيات الرسالة في الوقت نفسه إلى مسجل الإزاحة فمن الممكن اتباع اسلوب مكافئ وهو تقسيم مسجل الإزاحة إلى k من مسجلات الإزاحة:

$$X_0,X_k,X_{2k},\cdots,X_1,X_{k+1},X_{2k+1},\cdots,\cdots$$

وفي المقابل تكون الرسالة قد قسمت إلى k من الكلمات كل منها تدخل إلى واحد من مسجلات الإزاحة التي عددها k. المشكلة الوحيدة التي تنشأ عن ذلك هي أن محتويات

المسجلات في مسجلات إزاحة مختلفة يتم ضم بعضها مع بعض لتشكل مولّداً واحداً. وهذه هي الطريقة المتبعة عند التطبيق العملي لعملية التشفير، ونوضّح ذلك بالمثال التالي.

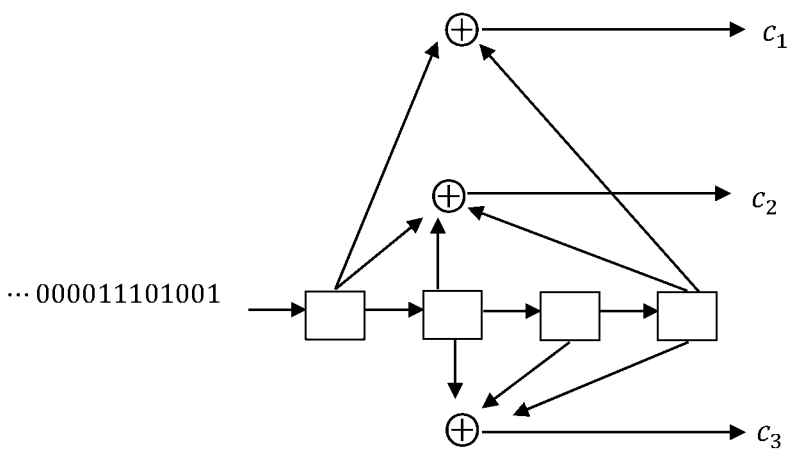
مثال (٨,٢,٧)

استخدم شفرة التلاف C من النوع (3,2,3) وذوات المولّدات $g_1(x) = 1 + x^3$ ، $g_2(x) = 1 + x + x^3$ ، $g_3(x) = x + x^2 + x^3$ لتشفير الرسالة:

$$m = 100101110000\cdots.$$

الحل

التفسير الأول للقيمة $k = 2$ هو تشفير الرسالة m باستخدام مسجل إزاحة واحد مبيّن في الشكل (٨,٤) ومن ثم إزاحة إحداثيين ($k = 2$) من إحداثيات الرسالة إلى مسجل الإزاحة مع كل تكّة ساعة. الجدول التالي يلخص لنا محتويات المسجلات والمخرجات:



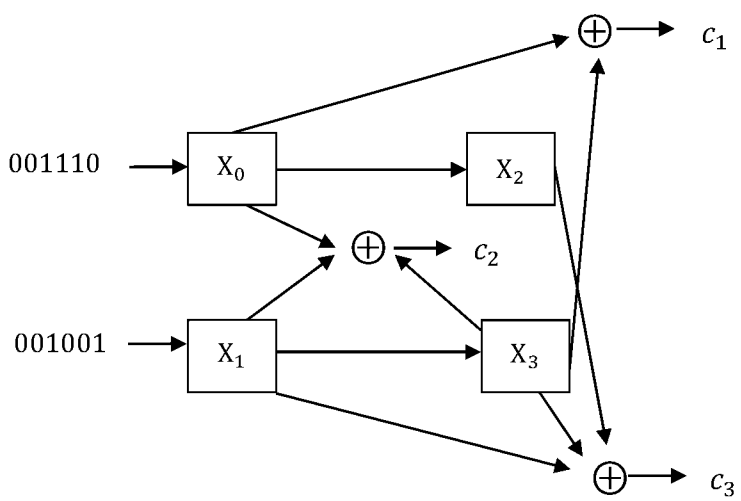
الشكل (٨,٤). تشفير باستخدام شفرة تلاف من النوع (3,2,3).

الزمن	المدخل	$X_0X_1X_2X_3$	المخرج $c_1\ c_2\ c_3$
-1	—	0000	—
0	01	0100	011
1	10	1001	001
2	10	1010	111
3	11	1110	100
4	00	0011	110
5	00	0000	000

وبهذا يكون تشفير الرسالة m (بعد التوريق البيني) هو :

$$c = 011\ 001\ 111\ 100\ 110\ 000\ \cdots.$$

أما التفسير الثاني للعدد $k = 2$ فهو ملاحظة أن الإحداثيات الأول، الثالث، الخامس، ... من الرسالة يتم إدخالها إلى مسجل الإزاحة فقط عند ظهورها في X_0 و X_2 وأن الإحداثيات الثاني، الرابع، السادس، ... من الرسالة يتم إدخالها إلى مسجل الإزاحة فقط عند ظهورها في X_1 و X_3. وبهذا نستطيع تقسيم الرسالة والمسجلات إلى جزأين $(k = 2)$ كما هو مبيّن في الشكل (٨,٥). ▲



الشكل (٨,٥). تشفير باستخدام شفرة تلاف من النوع (3,2,3).

تمرين

٨,٢,٨) شفّر الرسائل التالية باستخدام شفرة تلاف من النوع (3,2,4) حيث مولّداتها هي $g_1(x) = 1 + x^3$ ، $g_2(x) = x + x^4$ ، $g_3(x) = 1 + x + x^2 + x^3 + x^4$.

استخدم تقنيتي التشفير المبينتين في هذا البند.

(أ) $m(x) = 1 + x + x^3 + x^4 + x^5$.

(ب) $m(x) = 1 + x^3 + x^5 + x^7 + x^8$.

(ج) $m(x) = 1 + x + x^2 + x^3$.

نناقش في ما تبقى من هذا الفصل شفرات التلاف الثنائية من النوع $(2,1,m)$ ذات معدل المعلومات $r = \frac{1}{2}$. يمكن تعميم جميع النتائج والتقنية المستخدمة لشفرات التلاف من النوع (n,k,m) حيث الأفكار الرئيسة مشابهة للأفكار المقدمة في الشفرة الأسهل من النوع $(2,1,m)$. القارئ المهتم بدراسة شفرات التلاف عندما يكون $k > 1$ يستطيع الرجوع إلى التمارين لرؤية كيفية تعميم المادة المقدمة للشفرات في الحالة $k = 1$ إلى شفرات تلاف حيث $k > 1$.

من المناسب أن نذكر هنا أن **مسّاح المريخ الشامل (Mars Global Surveyor)** الذي أطلق من قبل NASA يستخدم شفرة تلاف حيث $r = \frac{1}{2}$ و $m = 7$ أثناء إرساله معلومات من المريخ إلى الأرض وأن **مستكشف المريخ (Mars Pathfinder)** يستطيع اختيار شفرة تلاف حيث $(r,m) = (\frac{1}{2}, 7)$ أو $(r,m) = (\frac{1}{6}, 15)$. تستطيع مشاهدة الصور التي التقطت من قبل بعثات NASA على الموقع http://www.msss.com.

أخيراً، توجد طريقة أخرى للتشفير باستخدام شفرات التلاف. تذكّر أنه من الممكن تشفير شفرة تلاف من النوع $(2,1,m)$ باستخدام مسجل إزاحة مكوّن من $m + 1$ مسجلاً. عند كل تكّة ساعة، تُسمى محتويات المسجلات الـ m الأولى، مرحلة **مسجل الإزاحة (State of the Shift Register)**. المرحلة صفر هي المرحلة التي تكون

فيها محتويات المسجلات الـ m الأولى أصفاراً. إذا كان مسجل الإزاحة في المرحلة $s_0, s_1, \cdots, s_{m-1}$ فعند تكّة الساعة التالية إما أن ينتقل مسجل الإزاحة إلى المرحلة $0, s_0, s_1, \cdots, s_{m-2}$ وإما إلى المرحلة $1, s_0, s_1, \cdots, s_{m-2}$ وهذا يعتمد على كون إحداثي الرسالة الذي تم إزاحته إلى المسجل X_0 هو 0 أو 1 على التوالي. أيضاً، إذا علمنا المرحلة الحالية $s_0, s_1, \cdots, s_{m-1}$ والمرحلة السابقة $s_1, \cdots, s_m$ فنستطيع معرفة المحتويات الحالية لجميع المسجلات ومن ثم نستطيع معرفة المخرج الحالي. تمثل هذه المعلومات في العادة بيانياً: مخطط المراحل لشفرة تلاف من النوع $(2,1,m)$ هو **رسم موجَّه (Directed Graph)** رؤوسه (أو مراحله) هي جميع الكلمات الثنائية ذات الطول m، ولكل مرحلة $s = s_1, s_2, \cdots, s_m$ يوجد ضلع موجّه من s إلى المرحلة $0, s_1, s_2, \cdots, s_{m-1}$ مُعلّماً بالمخرج عندما تحتوي المسجلات $X_0, X_1, \cdots, X_m$ على $1, s_1, \cdots, s_m$ على التوالي.

من الممكن أيضاً تمثيل مخطط المراحل لشفرة تلاف من النوع $(2,1,m)$ على شكل جدول: كل من صفوف الجدول يُبيّن المرحلة الحالية (أي محتويات $X_0, X_1, \cdots, X_{m-1}$) والمخرج المقابل لها وهذا بالطبع يعتمد على كون $X_m = 0$ أو $X_m = 1$.

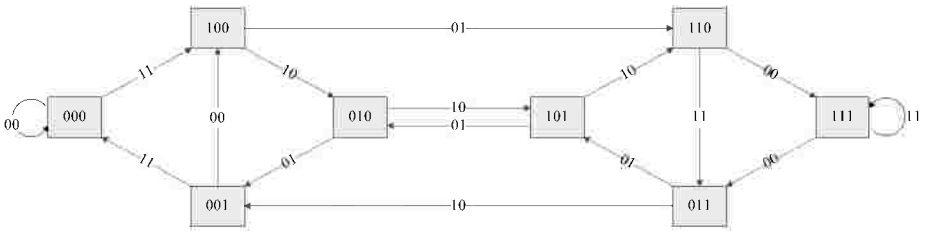
مثال (٨,٢,٩)

لنفرض أن C_1 شفرة تلاف من النوع $(2,1,3)$ مولداها $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$ (انظر المثالين (٨,٢,١) و (٨,٢,٤)). المراحل هي جميع الكلمات الثنائية ذات الطول $m = 3$:

$$.000,100,010,001,110,101,011,111$$

على سبيل المثال، يوجد ضلع موجّه من المرحلة $s = s_1s_2s_3 = 011$ إلى المرحلة $0s_1s_2 = 001$ وضلع موجّه من s إلى $1s_1s_2 = 101$. الضلع الموجّه من 011 إلى 001 يُعلَّم بالمخرج عندما يكون $X_0X_1X_2X_3 = 0011$، بالتحديد 10 والضلع الموجّه من 011

إلى 101 يُعلَّم بالمخرج عندما يكون $X_0X_1X_2X_3 = 1011$، بالتحديد 01. وباكمال ذلك لجميع المراحل نحصل على مخطط المراحل (الرسم الموجّه) المبيّن في الشكل (٨,٦).



الشكل (٨,٦). مخطط المراحل للشفرة C_1.

يمكن أيضاً تمثيل مخطط المراحل في الجدول التالي:

المرحلة	المخرج	
$X_0X_1X_2$	$X_3 = 0$	$X_3 = 1$
000	00	11
100	11	00
010	10	01
110	01	10
001	01	10
101	10	01
011	11	00
111	00	11

تذكر أن محتويات كل مسجلة بداية هي 0 ومن ثم فمرحلة البداية لمسجل الإزاحة هي $X_0X_1 \cdots X_{m-1} = 00 \cdots 0$. عند إدخال كل إحداثي من إحداثيات الرسالة إلى مسجل الإزاحة يتحرك مسجل الإزاحة إلى مرحلة أخرى وينتج عن كل مولّد إحداثي شفرة مخرجة. إن هذا يقابل في مخطط المراحل الحركة من مرحلة إلى المرحلة المجاورة (باتجاه الضلع الموجّه) والمخرجات هي علامات الأضلاع الموجّهة. وبهذا تقابل كلمة شفرة

مساراً موجّهاً في مخطط المراحل يبدأ عند المرحلة 0 ويتحرك باتجاه الأضلاع الموجّهة إلى المراحل المجاورة. لاحظ أنه عند كل تكّة ساعة، إحداثي الرسالة الذي يتحرك إلى مسجل الإزاحة هي الإحداثي الأول من المرحلة في مخطط المراحل. أيضاً، يكون من السهل معرفة الرسالة المقابلة لأي كلمة شفرة. ▲

مثال (٨,٢,١٠)

بالرجوع إلى المثالين (٨,٢,١) و (٨,٢,٩)، تُقابل الرسالة:

$$m(x) = 1 + x^2 \leftrightarrow 10100\cdots$$

المسار الذي يبدأ عند المرحلة 000 ومن ثم يتحرك إلى المراحل:

$$100,010,101,010,001,000,000,\cdots$$

على التوالي. علامات الأضلاع الموجّهة هذه هي:

$$11,10,10,01,01,01,11,00,\cdots$$

على التوالي، وهذه هي كلمة الشفرة التي تم تشفير الرسالة $m(x)$ لها (بعد التوريق البيني، انظر المثال (٨,٢,٥)). أيضاً، نستطيع وبسهولة الحصول على رسالة مقابلة لكلمة شفرة مُعطاة، فإذا كانت:

$$c = 00\ 11\ 01\ 11\ 01\ 01\ 01\ 11\ 00\ \cdots$$

فيكون المسار في مخطط المراحل الذي تنتج عنه الكلمة c هو المسار الذي يمر بالمراحل:

$$000,000,100,110,011,101,010,001,000,000,\cdots$$

(من المؤكد أن جميع كلمات الشفرة تبدأ عند المرحلة الصفرية 000). وبما أنه عند كل تكّة ساعة، يكون إحداثي الرسالة هي الإحداثي الأول في المرحلة التي يتحرك إليها المسجل، نرى أن الرسالة التي تقابل c هي التي نحصل عليها من الإحداثي الأول لكل مرحلة من مراحل المسار (عدا مرحلة البداية). أي أن:

$$.m = 0\,1\,1\,0\,1\,0\,0\,0\,0\,\cdots$$ ▲

تمارين

(٨,٢,١١) (أ) جد مخطط المراحل ومثله على شكل جدول لشفرة التلاف من النوع (2,1,2) التي لها المولّدان $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$.

(ب) استخدم مخطط المراحل لتشفير كل من الرسالتين:

(i) $m(x) = 1 + x^2$

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

(ج) استخدم مخطط المراحل لإيجاد الرسالة التي تقابل كلاً من كلمتي الشفرة:

(i) ... 11 01 00 01 11 00.

(ii) ... 00 11 10 01 01 10 00.

(٨,٢,١٢) (أ) جد مخطط المراحل ومثله على شكل جدول لشفرة التلاف من النوع (2,1,3) التي لها المولّدان $g_1(x) = 1 + x + +x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$.

(ب) استخدم مخطط المراحل لتشفير الرسائل التالية:

(i) $m(x) = 1 + x^3$

(ii) $m(x) = 1 + x + x^3$

(iii) $m(x) = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$.

(ج) استخدم مخطط المراحل لإيجاد الرسالة التي تقابل كلاً من كلمتي الشفرة:

(i) ... 11 10 00 01 00 10 10.

(ii) ... 00 11 01 10 01 10 00.

(٨,٢,١٣) (أ) جد مخطط المراحل ومثله على شكل جدول لشفرة التلاف من النوع (2,1,4) التي لها المولّدان $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

(ب) استخدم مخطط المراحل لتشفير الرسائل التالية:

(i) $m(x) = 1 + x + x^2$

(ii) $m(x) = 1 + x + x^3$

(iii) $m(x) = 1 + x^2 + x^4 + \cdots = \sum_{i=0}^{\infty} x^{2i}$.

قارن إجاباتك مع إجابات التمرين **(٨,٢,٣)**.

(٨,٢,١٤) إذا كان $1 \le k \le \frac{m}{2}$ فمن الممكن تعريف مخطط المراحل لشفرة تلاف من النوع (n,k,m) بصورة مشابهة للتعريف المقدم على النحو التالي:

المراحل هي جميع الكلمات الثنائية ذات الطول $m+1-k$ ولكل مرحلة $s = s_k, s_{k+1}, \cdots, s_m$ وكل كلمة ثنائية u من الطول k يوجد ضلع موجّه من المرحلة s إلى المرحلة $u, s_{k+1}, \cdots, s_{m-k}$ مُعَلَّم بالمخرج عندما تحتوي المسجلات $X_0, X_1 \cdots, X_m$ على $u, s_{k+1}, \cdots, s_{m-k}$. (عندما يكون $k > 1$ استخدمنا توصيف التشفير بإزاحة k إحداثياً من إحداثيات الرسالة إلى مسجل واحد من مسجلات الإزاحة عند كل تكّة ساعة). جد مخطط المراحل لشفرة التلاف من النوع (n,k,m) عندما تكون مولّداتها هي:

(أ) $g_1(x) = 1 + x + x^3$ ، $g_2(x) = 1 + x + x^2 + x^3$ ، $g_3(x) = 1 + x^2 + x^3$ حيث $k = 1$.

(ب) $g_1(x) = 1 + x^3$ ، $g_2(x) = 1 + x + x^3$ ، $g_3(x) = x + x^2 + x^3$ حيث $k = 2$.

(ج) $g_1(x) = 1 + x^3$ ، $g_2(x) = x + x^4$ ، $g_3(x) = 1 + x + x^2 + x^3 + x^4$ حيث $k = 2$.

(٨,٣) فك تشفير شفرات التلاف
Decoding Convolutional Codes

كلمات شفرات التلاف ذات طول غير منته، ولذا يكون من الطبيعي توقع اختلاف فك تشفيرها عن فك تشفير الشفرات الأخرى. ولتجنب مشكلات التخزين فعملية فك التشفير تبدأ قبل الانتهاء من استقبال جميع إحداثيات كلمة الشفرة ومن ثم فعلينا تحديد زمن الانتظار اللازم قبل البدء بفك التشفير. على سبيل المثال، لتكن C_1 هي شفرة التلاف من النوع (2,1,3) حيث مولّداها هما $g_1(x) = 1 + x + x^3$

و $g_2(x) = 1 + x^2 + x^3$ (مخطط المراحل لهذه الشفرة هو المخطط المبيّن في الشكل (٨,٦)). لنفرض أن الكلمة المستقبلة هي :

$$w(x) = 1 + x \leftrightarrow 11\ 00\ 00\ 00\ \cdots = w.$$

تذكر أن كلمات الشفرة تقابل مسارات موجّهة في مخطط المراحل تبدأ بالمرحلة 000 ، ولكن من الواضح عدم وجود مسار موجّه مخرجه w. ولهذا يتوجب علينا إيجاد أقرب كلمة شفرة للكلمة w. أي ايجاد مسار موجّه في مخطط المراحل يكون مخرجه قريباً من w. عند معرفتنا جميع إحداثيات w نرى أن المسار الموجّه الذي لا يغادر المرحلة 000 يقابل كلمة الشفرة $c_1 = 00\ 00\ 00\ \cdots$ التي تبعد مسافة مقدارها 2 عن الكلمة w. ومن السهل التحقق من أن أي مسار موجّه آخر يكون مخرجه كلمة تختلف عن الكلمة w بأكثر من إحداثيين. إذن ، c_1 هي كلمة الشفرة الأقرب ويكون فك تشفير w هو الرسالة $m = 000\cdots$.

لنفترض الآن أن سعة التخزين محدودة جداً بحيث يتوجب علينا فك تشفير إحداثي من إحداثيات الرسالة عند كل تكّة ساعة. عند التكّة الأولى نبدأ عند المرحلة 000 ونرى أن 11 إحداثيان من إحداثيات w. وبما أن الضلع الموجّه من 000 إلى 100 مُعَلَّم بالإحداثيين 11 فالخيار الأفضل لنا هو التحرك إلى المرحلة 100 وهو الخيار الذي مخرجه يتفق مع إحداثيات الكلمة المستقبلة w. إذن ، نقوم بفك تشفير الإحداثي الأول من الرسالة على أنه الإحداثي 1. عند التكّة الثانية نكون في المرحلة 100 ولدينا الإحداثيان 00 من الكلمة w ومن ثم نقع في المأزق التالي :

إما التحرك إلى المرحلة المجاورة 010 وإما المرحلة المجاورة 110 لنحصل على المخرج 10 أو 01 على التوالي وكلاهما يبعد مسافة 1 عن الإحداثيات المستقبلة. وبهذا يتوجب علينا أخذ قرار اعتباطي حيث اكتشفنا وقوع خطأ أثناء الإرسال لا نستطيع تصويبه. وإما أن يكون فك تشفير w هو $c_2 = 11\ 10\ \cdots$ أو $c_2' = 11\ 01\ \cdots$ حيث

الرسالة الأقرب هي $m = 1 * \cdots *$ (العلامة * تعني أننا قمنا باتخاذ قرار اعتباطي عند اختيار فك تشفير الإحداثي ليكون 0 أو 1). لاحظ أن فك التشفير * يتوجب عليه أن يكون اختيار المرحلة التالية اعتباطياً أيضاً من بين المرحلتين المجاورتين للمرحلة الحالية.

ندرس الآن خياراً آخر وهو إمكانية تخزين معلومات تكتين قبل البدء بعملية فك التشفير. في هذه الحالة نبدأ بأخذ جميع المسارات من المرحلة الصفرية التي طول كل منها يساوي 2 ونقارن علامات أضلاعها مع أول تكّتين للكلمة w، بالتحديد مع 00 11 لنحصل على معلومات الشكل (٨,٧).

المسار	المخرج	المسافة من 00 11
000,000,000	00 00	2
000,000,100	00 11	4
000,100,010	11 10	1
000,100,110	11 01	1

الشكل (٨,٧). معلومات قرار فك التشفير الأول.

من هذه المعلومات نرى وجود مسارين هما الأقرب إلى 00 11 وهو الجزء المعروف من الكلمة w لحد الآن. وهذا لا يسبب أي مشكلة ؛ لأن المسارين يتفقان في أن الحركة الأولى يجب أن تكون إلى المرحلة 100. وهذان المساران يختلفان فقط في القرار الذي يجب علينا اتخاذه للتحرك من المرحلة 100 وهو قرار ليس علينا اتخاذه إلا بعد استقبال إحداثيات أخرى من w. إذن، يكون قرار فك التشفير في هذه الحالة هو التحرك إلى المرحلة 100 ويتم فك تشفير الإحداثي الأول من الرسالة على أنه الإحداثي 1. نستخدم الآن التكّتان الثانية والثالثة من معلومات w (أي 00 00) لاتخاذ قرار فك التشفير التالي. نقوم بايجاد المسافة بين 00 00 ومخرجات جميع المسارات من الطول 2 التي تبدأ عند المرحلة الحالية 100 كما هو مبين في الشكل (٨,٨).

المسافة من 00 00	المخرج	المسار
2	10 01	100,010,001
2	10 10	100,010,101
3	01 11	100,110,111
1	01 00	100,110,111

الشكل (٨,٨). معلومات قرار فك التشفير الثاني.

في هذه الحالة نرى وجود مسار هو وحيد هو الأقرب إلى الجزء المختار من w. هذا المسار هو 100,110,111. إذن، يكون قرار فك التشفير هو التحرك إلى المرحلة 110 ويكون فك تشفير الإحداثي الثاني من الرسالة هو الإحداثي 1.

تمرين

(٨,٣,١) لتكن C شفرة تلاف من النوع (2,1,3) حيث مولّداها هما $g_1(x) = 1 + x + x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$ (تم إنشاء مخطط مراحل C في التمرين **(١٢ ، ٢ ، ٨)**). فُك تشفير أول 4 إحداثيات من إحداثيات الكلمة المستقبلة $w = 11\ 00\ 00\ 00\ \cdots \leftrightarrow 1 + x = w(x)$ وذلك باستخدام جداول مماثلة للجدولين المقدمين في الشكلين **(٨,٧)** و **(٨,٨)** عندما يكون زمن الانتظار قبل البدء بفك التشفير هو :

(أ) تكّتان (ب) ثلاث تكّات (ج) أربع تكّات.

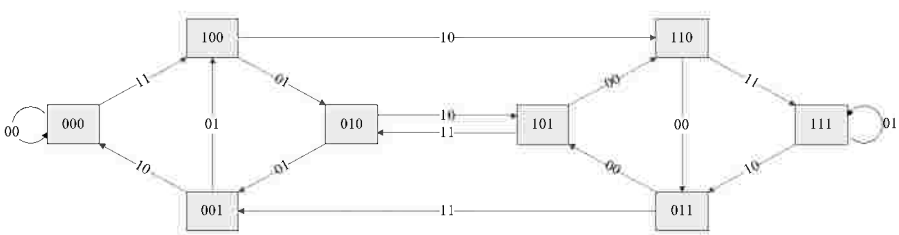
في حالة وجود مسارين هما الأقرب بحيث يكون التحرك إلى المرحلة التالية غير واضح فضع * في مكان فك تشفير إحداثي الرسالة ومن ثم افترض أن إحداثي الرسالة في هذه الحالة هو 0 لكي تتمكن من معرفة المرحلة التالية.

إذا قرّرنا الانتظار τ خطوة قبل بدء عملية فك التشفير فيكون قرار فك التشفير هو دراسة جميع المسارات ذات الطول τ التي تبدأ من المرحلة الحالية ومقارنة كل من هذه المسارات مع معلومات τ تكّة التي بحوزتنا من الكلمة المستقبلة. بعد ذلك نقوم بالتحرك

إلى المرحلة التالية في جميع المسارات الأكثر قُرباً إلى w. ومن ثم نستقبل تكّة أخرى من w قبل الانتقال إلى الخطوة التالية. أيضاً، وكما هو الحال عند التكّة الثانية عندما $\tau = 1$، إذا وجد مساران إلى w تكّة مستقبلة من الكلمة w يختلفان في القرار الذي يجب اتخاذه فنقوم باتخاذ قرار اعتباطي للتحرك إلى إحدى المراحل التالية. تُسمى خوارزمية فك التشفير هذه، **خوارزمية الاستنفاد لفك تشفير (Exhaustive Decoding Algorithm)** شفرات التلاف (لأنه قد تم دراسة جميع المسارات من الطول τ التي تبدأ من المرحلة الحالية قبل فك تشفير كل من إحداثيات الرسالة). كما يُسمى العدد τ، **سعة النافذة (Window Size)**؛ لأن τ هو كمية المعلومات التي لدينا من الكلمة w عند الشروع في اتخاذ قرار فك التشفير.

من الواضح أن مقدار زمن الانتظار قبل بدء عملية فك التشفير له تأثير على اختيارنا للكلمة الأقرب إلى كلمة الشفرة. والمسألة الآن تتلخص فيما إذا كان بإلامكان إيجاد وسط مناسب بين اتخاذ قرار فك التشفير عند كل تكّة ساعة وبين فك التشفير بعد معرفة جميع إحداثيات الكلمة المستقبلة بحيث يكون باستطاعتنا تصويب بعض أنماط الأخطاء. ولكن ذلك يطرح السؤال التالي: ما هي الأخطاء الممكن تصويبها؟ سنحصل على عدد من الإجابات لهذا السؤال ونناقش الفترة الزمنية اللازمة قبل بدء فك التشفير لكل من هذه الاجابات.

نحتاج أولاً لدراسة مسألة أخرى. لنفرض أن C شفرة تلاف من النوع (2,1,3) لها المولّدان $g_1(x) = 1 + x^3$ و $g_2(x) = 1 + x + x^2$. الشكل (٨,٩) يُبيّن مخطط المراحل لهذه الشفرة.



الشكل (٨,٩). مخطط المراحل لشفرة تلاف إخفاقية.

لنفرض أن كلمة الشفرة المرسلة هي كلمة الشفرة الصفرية وأن الرسالة المقابلة لها هي $m = 000\cdots$ وأن الكلمة المستقبلة هي :

$$w = 11\ 10\ 00\ 00\ \cdots \leftrightarrow 1 + x + x^2 = w(x).$$

فك تشفير w عملية سهلة ؛ لأن w هي كلمة شفرة في هذه الحالة وهذا ما يؤكده مخطط المراحل باتباع المسار الذي يمر بالمراحل :

$$.000,100,110,011,101,110,\cdots$$

حيث افترضنا مسبقاً في هذه الحالة عدم وقوع أخطاء أثناء عملية الإرسال ومن ثم سنفترض أن الرسالة الأقرب هي $m = 110110\cdots \leftrightarrow \sum_{i=0}^{\infty}(x^{3i} + x^{3i+1})$ وهذا وضع خطير جداً ؛ لأنه قد وقع خطأ في إرسال أول ثلاث إحداثيات افترضنا أن $c = 00\ 00\ \cdots$ هي الكلمة المرسلة) وهذا يقودنا إلى الوقوع في عدد غير منته من الأخطاء أثناء فك التشفير ؛ (لأننا قمنا بفك تشفير $m = 110110\cdots$ عوضاً عن فك تشفير $m = 000000\cdots$). ومع ذلك فمن السهل أن نرى أن المشكلة هنا تكمن في وجود دورة في مخطط المراحل (مختلفة عن العروة التي عند المرحلة الصفرية) حيث إن مخرجات الأضلاع الموجّهة لهذه الدورة مُعلّمة بالأصفار. وهذا هو السبب ؛ لأن وقوع عدد منته من الأخطاء أثناء عملية الإرسال ينتج عنه عدد غير منته من أخطاء فك التشفير. إذا عرفنا وزن مسار (أو دورة) في مخطط المراحل على أنه وزن مخرجات الأضلاع الموجّهة لهذا المسار، فإننا نعرّف **شفرة التلاف الإخفاقية (Catastrophic Convolutional Code)** على أنها شفرة التلاف التي يحتوي مخطط مراحلها على دورة وزنها صفر مختلفة عن العروة التي عند المرحلة الصفرية. من الممكن اثبات أن شفرة التلاف من النوع $(2,1,m)$ هي شفرة إخفاقية إذا كان $gcd(g_1(x), g_2(x)) \neq 1$. في شفرة التلاف هذه لدينا $g_1(x) = 1 + x^3 = (1 + x)(1 + x + x^2)$ ومن ثم نرى أن $gcd(g_1(x), g_2(x)) = 1 + x + x^2 \neq 1$.

تمرين

(**٨,٣,٢**) لكل من شفرات التلاف من النوع $(2,1,m)$، احسب $gcd(g_1(x), g_2(x))$ لتقرر فيما إذا كانت الشفرة اخفاقية. في حالة الشفرة الإخفاقية جد الدورة التي وزنها صفر (ومختلفة عن العروة التي عند المرحلة الصفرية) في مخطط مراحل الشفرة.

(أ) $g_1(x) = 1 + x$ و $g_2(x) = 1 + x + x^2 + x^3$.

(ب) $g_1(x) = 1 + x + x^4$ و $g_2(x) = 1 + x^2 + x^4$.

(ج) $g_1(x) = 1 + x + x^2$ و $g_2(x) = 1 + x + x^3 + x^4$.

فيما تبقى من هذا الفصل سنفرض أن الشفرات هي شفرات غير إخفاقية.

نرجع الآن إلى دراسة زمن الانتظار قبل البدء بعملية فك التشفير ومعرفة أنماط الأخطاء التي يمكن تصويبها. البداية الطبيعية لهذا الغرض هي إيجاد المسافة d لشفرة التلاف (تُسمى هنا المسافة الحرة الصغرى). لاحظنا سابقاً أن شفرة التلاف هي شفرة خطيّة وبهذا تكون مسافتها d هي أصغر أوزان كلمات الشفرة غير الصفرية. وبما أن دراستنا تقتصر على شفرات التلاف غير الإخفاقية فإن كلمة الشفرة غير الصفرية ذات الوزن المنتهي تقابل مساراً يخرج بداية من المرحلة الصفرية (لضمان وزن غير صفري لكلمة الشفرة) ومن ثم يعود بعد فترة معينة إلى المرحلة الصفرية ولا يخرج مرة أخرى (لضمان أن يكون وزن كلمة الشفرة منتهياً). لاحظ أن وزن أي مسار يخرج من المرحلة الصفرية في الشفرات غير الإخفاقية يجب أن يكون موجباً؛ لعدم وجود دورات وزنها صفر عدا العروة التي عند المرحلة الصفرية. على سبيل المثال، وزن المسار $\cdots$,000,100,010,001,000,000 في الشكل (**٨,٦**) يساوي 6؛ لأنه يقابل كلمة الشفرة $\cdots$ 00 00 11 01 10 11 التي وزنها يساوي 6. كما أن المسار $\cdots$,000,100,110,111,011,001,000,000 يقابل كلمة الشفرة

… 00 00 11 10 00 00 01 00 11 ومن ثم فوزنه هو أيضاً يساوي 6. وبهذا تكون مسافة الشفرة C_1 هي $d(C_1) = 6$ (سنقدم في البند القادم خوارزمية لحساب $d(C)$).

تمرين

(٨,٣,٣) جد مسافة شفرات التلاف التي لها المولّدات التالية (مخططات المراحل لهذه الشفرات مقدمة في التمارين **(٨,٢,١١)**، **(٨,٢,١٢)**، **(٨,٢,١٣)**).

(أ) $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$.

(ب) $g_1(x) = 1 + x + x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$.

(ج) $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

بعد قيامنا بحساب مسافة الشفرة سنحاول تصويب جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن $\lfloor (d-1)/2 \rfloor$. ولكن علينا الاجابة الآن عن السؤال التالي: ما هو زمن الانتظار اللازم قبل البدء بفك التشفير؟ مسافة C_1 هي $d(C_1) = 6$ ومع ذلك عند استخدامنا خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau = 1$ وجدنا أن فك تشفير الكلمة المستقبلة $w = 11\ 00$ … 00 00 00 هي الكلمة … 00 00 00. ولهذا لم يتم تصويب نمط الخطأ w الذي وزنه يساوي 2 حيث $\lfloor (d(C_1)-1)/2 \rfloor = 3 < 2$. ولكننا لو انتظرنا زمناً غير محدود لاستطعنا تصويب w إلى … 00 00.

يُعرف طول المسار على أنه عدد الأضلاع الموجهة في المسار (يُساهم الضلع الموجّه بعدد مرات وقوعه في المسار). إذا أردنا تصويب جميع أنماط الأخطاء ذات الأوزان التي لا تزيد عن e فيجب أن يكون زمن الانتظار $\tau(e)$ اللازم من المرحلة الصفرية أكبر من $2e$. ولرؤية ذلك، نفرض أنه قد تم إرسال كلمة الشفرة الصفرية وأن عدد الأخطاء التي وقعت أثناء عملية الإرسال لا يزيد عن e (لاحظ أن شفرات التلاف هي شفرات خطيّة، ولذا يمكننا افتراض أن الكلمة الصفرية هي الكلمة التي تم

إرسالها دون المساس بالعمومية). باستخدام خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau(e)$ نقوم بعد $\tau(e)$ تكّة ساعة بمقارنة العلامات لجميع المسارات من المرحلة الصفرية التي طولها $\tau(e)$ مع أول $\tau(e)$ تكّة من الكلمة المستقبلة w ومن ثم نختار أقرب المسارات لتحديد المرحلة التي يجب التحرك إليها. ولإجراء عملية فك تشفير صائبة يجب علينا اتخاذ قرار البقاء عند المرحلة الصفرية؛ لأننا قد فرضنا أن كلمة الشفرة المرسلة هي الكلمة الصفرية. ومن اختيار $\tau(e)$ نرى أن وزن جميع المسارات التي تغادر مباشرة المرحلة الصفرية لا يزيد عن $2e$ بعد عدد $\tau(e)$ من المراحل، وبهذا فهو يختلف عن أول $\tau(e)$ تكّة من w بأكثر من عدد e من المواقع.

من ناحية أخرى، وزن المسار الذي لا يغادر المرحلة الصفرية على الإطلاق يساوي صفراً ومن ثم فهو يبعد مسافة $wt(w) \leq e$ عن أول $\tau(e)$ تكّة من w.

إذن، لا يوجد أي مسار من المسارات التي تغادر مباشرة المرحلة الصفرية بحيث يكون هو الأقرب، ولذا فجميع المسارات الأقرب إلى w تتفق على البقاء عند المرحلة الصفرية بعد أول $\tau(e)$ تكّة. وكما لاحظنا عند دراستنا للشكلين (٨,٧) و (٨,٨) فإن عملية فك التشفير تتوقف إلى أن نستقبل تكّة أخرى من w. ولكن بعد استقبالنا لتكّة جديدة يكون بالإمكان تكرار النقاش السابق ونخلص إلى أن فك تشفير w صائب. في الحقيقة، من النقاش المقدّم سابقاً نكون قد برهنا أنه باستطاعتنا إجراء فك تشفير صائب للكلمة w إذا وقع عدد من الأخطاء لا يزيد عن e في أي $\tau(e)$ تكّة متتالية من الكلمة المستقبلة. بهذا نستطيع تصويب عدد غير منته من الأخطاء إذا كان عدد أخطاء $\tau(e)$ من التكّات المتتالية لا يزيد عن e (إن ذلك شبيه بوضع الشفرات القالبية ذات الطول المنتهي؛ لأنه يتم تصويب الأخطاء في مثل هذه الشفرات إذا كان عدد الأخطاء في أي من كلمات الشفرة لا يزيد عن e). وبهذا نكون قد عرفنا الزمن اللازم للانتظار.

لتكن C شفرة تلاف غير اخفاقية. لكل $1 \le e \le \lfloor (d-1)/2 \rfloor$ يُعرف $\tau(e)$ على أنه أصغر عدد صحيح x يحقق: جميع المسارات ذات الطول x في مخطط المراحل التي تغادر مباشرة المرحلة الصفرية لها وزن لا يزيد عن $2e$.

لاحظ أن تنفيذ خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau(e)$ يحتاج إلى جميع المسارات من الطول $\tau(e)$ من المرحلة الحالية إلى كل من إحداثيات الرسالة المراد فك تشفيرها. ولكن إنشاء جميع هذه المسارات التي عددها $2^{\tau(e)}$ عند كل تكّة يستغرق فترة زمنية كبيرة، ولهذا سنقدم خوارزمية أسرع في البند (٨,٤). ولكن في الوقت الحالي لدينا المبرهنة التالية:

مبرهنة (٨,٣,٤)

لتكن C شفرة تلاف غير إخفاقية. لكل e حيث $1 \le e \le \lfloor (d-1)/2 \rfloor$، إذا وقع عدد من الأخطاء لا يزيد عن e في أي من أنماط الأخطاء ولكل $\tau(e)$ من الخطوات المتتالية أثناء عملية الإرسال فيكون باستطاعة خوارزمية الاستنفاد بنافذة سعتها $\tau(e)$ فك تشفير الكلمة المستقبلة بصورة صائبة. ■

مثال (٨,٣,٥)

لتكن C_1 شفرة التلاف التي لها المولّدان $g_1(x) = 1 + x + x^3$ و $g_2(x) = 1 + x^2 + x^3$ (الشكل (٨,٦) هو مخطط المراحل للشفرة C_1). بما أن $d(C_1) = 6$ فإننا ندرس الحالتين $e = 1$ و $e = 2$.

في الحالة $e = 1$ نرى أن جميع المسارات ذات الطول 2 التي تغادر مباشرة المرحلة الصفرية لها وزن أكبر من $2e = 2$. ويوجد على الأقل مسار واحد من الطول 1 يغادر مباشرة المرحلة الصفرية وزنه لا يزيد عن $2e$. إذن، $\tau(1) = 2$.

أما في الحالة $e = 2$ فنرى أن جميع المسارات ذات الطول 7 التي تغادر مباشرة المرحلة الصفرية لها وزن أكبر من $2e = 4$ (تحقق من ذلك!). ويوجد على الأقل مسار واحد طوله 6 يغادر مباشرة المرحلة الصفرية ووزنه لا يزيد عن $2e$. أحد هذه المسارات هو:

$$000,100,110,111,011,001,100$$

إذن، $\tau(2) = 7$ (الخوارزمية الأسرع التي سنقدمها في البند (٨,٤) تستطيع أيضاً حساب $\tau(e)$ بسرعة).

إذا استخدمنا خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau(1)$ فإستناداً إلى المبرهنة (٨,٣,٤) نستطيع تصويب جميع أنماط الأخطاء التي تحتوي على عدد من الأخطاء لا يزيد عن $e = 1$ لأي $\tau(1) = 2$ تكّة متتالية. على سبيل المثال، نستطيع تصويب نمط الخطأ:

$$e_1 = 10\ 00\ 01\ 00\ 01\ 00\ 10\ \cdots.$$

وإذا استخدمنا خوارزمية الاستنفاد لفك التشفير بنافذة سعتها $\tau(2)$ فمن الممكن تصويب جميع أنماط الأخطاء التي تحتوي على عدد من الأخطاء لا يزيد عن $e = 2$ لأي $\tau(2) = 7$ تكّة متتالية. على سبيل المثال، نستطيع تصويب نمط الخطأ:

$$e_2 = 11\ 00\ 00\ 00\ 00\ 00\ 00\ \cdots.$$

لاحظ أن المبرهنة (٨,٣,٤) لا تضمن لنا تصويب نمط الخطأ e_2 إذا اخترنا $e = 1$ (يوجد عدد $e < 2$ من الأخطاء عند التكّة الأولى لنمط الخطأ e_2).

كذلك، لا يمكن تصويب e_1 إذا اخترنا $e = 2$ (يوجد عدد $e < 4$ من الأخطاء عند أول $\tau(2) = 7$ تكّة متتالية لنمط الخطأ e_1). عند دراستنا للشفرات القالبية (ذات الطول المنتهي) لم نجد سبباً لكي يكون $e < \lfloor (d-1)/2 \rfloor$ ولكن يتحتم علينا عمل ذلك عند فك تشفير شفرات التلاف حيث نقوم باختيار e لنتمكن من تصويب نمط الخطأ المرجح وقوعه. ▲

تمارين

(**٨,٣,٦**) لكل من الشفرات C التالية ولكل e حيث $1 \le e \le \lfloor (d(C)-1)/2 \rfloor$ جد $\tau(e)$ (وجدنا $d(C)$ في التمرين (**٨,٣,٣**) ووجدنا مخططات المراحل في التمارين (**٨,٢,١١**)، (**٨,٢,١٢**)، (**٨,٢,١٣**)).

(أ) $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$.

(ب) $g_1(x) = 1 + x + x^2 + x^3$ و $g_2(x) = 1 + x^2 + x^3$.

(ج) $g_1(x) = 1 + x^3 + x^4$ و $g_2(x) = 1 + x + x^2 + x^4$.

(**٨,٣,٧**) ماذا يحدث لو حاولنا حساب $\tau(e)$ عندما يكون $e > \lfloor (d-1)/2 \rfloor$ ؟

(٨,٤) فك تشفير ڤيتربي المبتور
Truncated Viterbi Decoding

نقدم في هذا البند خوارزمية فك تشفير ڤيتربي المبتور لشفرات تلاف ثنائية من النوع $(2,1,m)$. نحتاج لتنفيذ هذه الخوارزمية إلى 2^m عملية حسابية وتخزين 2^m مساراً من الطول τ عند كل تكّة مقارنة مع 2^τ عملية حسابية وتخزين 2^τ مساراً من الطول τ عند تنفيذ خوارزمية الاستنفاد لفك التشفير. من الملائم هنا أنه عند التطبيق العملي للخوارزمية يتم اختيار سعة النافذة τ لتكون بين القيمتين $4m$ و $6m$ (هذا العدد غالباً ما يكون أكبر بكثير من $\tau(e)$). بُني هذا الاختيار على برهان احتمالي يُبيّن أن بهذا الاختيار لسعة النافذة يكون عدد أنماط الأخطاء التي لا يتم تصويبها قليل جداً. لهذا فإن تخزين 2^m مساراً عوضاً عن 2^τ مساراً يؤدي إلى توفير مناسب سواء في الزمن أو التخزين.

يعود السبب لتفضيل فك تشفير ڤيتربي المبتور على خوارزمية الاستنفاد لفك التشفير إلى أنه لكل مرحلة s يتم تخزين مسار واحد على الأكثر من الطول τ من المرحلة

الحالية إلى المرحلة s. نقوم أولاً بوصف مختصر لهذه الخوارزمية ثم نقدم بعد ذلك خطواتها بالتفصيل.

لنفرض أن $w = w_0, w_1, \cdots$ هي الكلمة المستقبلة. تذكّر أن w_i لكل $i \geq 0$ هي عديد من النوع n؛ لأننا استخدمنا التوريق البيني لتمثيل كلمات الشفرة والكلمات المستقبلة. وبما أننا نستخدم $n = 2$ فتتكون w_i من إحداثيين (يتم استقبال الإحداثيين عند الزمن i).

جميع المسارات من المرحلة الصفرية لا تزال مخزّنة عند أول m تكّة. ولكن عند الزمن m يوجد 2^m مساراً كل منها ينتهي عند مرحلة مختلفة، ولهذا فإن $t = m$ هي المرة الأولى التي ينتهي بها مسار واحد فقط عند كل مرحلة. وأثناء إنشاء 2^m من المسارات تقوم الخوارزمية بحساب المسافة بين مخرج المسار والكلمة المستقبلة وتخزن هذه المسافة مع المسار. عند $t > m$ يوجد لكل مرحلة $s = s_0, s_1, \cdots, s_{m-1}$ مرحلتان ينطلق من كل منهما ضلع موجّه إلى s وهاتان المرحلتان هما:

$$S_0 = s_1, s_2, \cdots, s_{m-1}, 0 \text{ و } S_1 = s_1, s_2, \cdots, s_{m-1}, 1.$$

عند $t = m$ تقوم الخوارزمية بتخزين المسارين W_0 و W_1 من المرحلة الحالية إلى المرحلتين S_0 و S_1 على التوالي مع المسافتين $d(S_0, t)$ و $d(S_1, t)$ من المسارين W_0 و W_1 على التوالي إلى الكلمة المستقبلة. عند $t > m$ وعند التكّة t تقوم الخوارزمية بجمع المسافتين بين w_{t-1} ومخرجات الضلعين الموجهين من S_0 وS_1 إلى s مع المسافتين $d(S_0, t-1)$ و $d(S_1, t-1)$ على التوالي وتأخذ المجموع الأصغر ليكون المسافة $d(s, t)$ بين امتداد المسار W_0 أو W_1 (أيهما يُعطي مسافة أصغر) والمرحلة s.

يتم تخزين المسارات كمتتالية من الإحداثيات المستقبلة وليس على صورة متتالية من المراحل أو متتالية من مخرجات الأضلاع الموجّهة. في اللحظة التي يكون فيها $t \geq \tau$ يتم فك تشفير إحداثي رسالة عند كل تكّة. ويتم التعامل مع المراحل ذات المسافات

$d(s,t)$ الصغرى: إذا اتفقت المسارات المخزّنة في كل مرحلة من هذه المراحل على المرحلة التالية للحركة (أي أن تحتوي المسارات على نفس إحداثي الرسالة السابقة) فعند ذلك يتم فك تشفير إحداثي الرسالة هذه. وإذا لم تتفق جميع المسارات فنقوم بتعليم إحداثي الرسالة المراد فك تشفيرها بالعلامة * (من الممكن فك تشفير هذا الإحداثي إلى 0 ولكن من المناسب توضيح أن أياً من الإحداثيين ليس هو المفضل). بعد اتخاذ قرار بشأن إحداثي الرسالة يتم حذفها من جميع المسارات المخزنة. ومن ثم ينقص طول المسارات المخزنة إلى $\tau - 1$ ولكن يتم زيادة هذا الطول ليصبح τ عند تمديد هذه المسارات عند التكّة $\tau + 1$.

خوارزمية (٨,٤,١) [خوارزمية ڤيتربي المبتورة لفك تشفير شفرات تلاف من النوع $(n, 1, m)$ بنافذة سعتها τ]

لتكن $w_0 w_1 \cdots$ هي الكلمة المستقبلة. يتم تنفيذ الخطوات التالية:

(١) (خطوة البداية) إذا كان $t = 0$ فنعرّف $W(s;t)$ و $d(s;t)$ على النحو التالي:

$$W(s;t) = s{*}{*}\cdots{*} \qquad \text{(طولها } \tau\text{)}$$

$$d(s;t) = \begin{cases} 0 & \text{إذا كانت } s \text{ هي المرحلة الصفرية} \\ \infty & \text{خلاف ذلك} \end{cases}$$

(٢) (حساب المسافة) لكل $t > 0$ ولكل مرحلة $s = s_0, s_1, \cdots, s_{m-1}$ نعرف:

$$d(s;t) = min\{d(s_1, s_2, \cdots, s_{m-1}, 0; t-1) + d(s_1, s_2, \cdots, s_{m-1}, 1; t-1) + d_1(s)\}$$

حيث $d_i(s)$ هي المسافة بين w_{t-1} ومخرج الضلع الموجّه من $s_1, s_2, \cdots, s_{m-1}, i$ إلى s.

(٣) (حساب المسارات)

(أ) إذا كان:

$$d(s_1, \cdots, s_{m-1}, i; t-1) + d_i(s) < d(s_1, \cdots, s_{m-1}, j; t-1) + d_j(s)$$

حيث $\{i,j\} = \{0,1\}$ فنكوّن $W(s;t)$ من $W(s_1,\cdots,s_{m-1},0;t-1)$ وذلك باضافة الإحداثي الواقع أقصى يسار s إلى يسار $W(s_1,\cdots,s_{m-1},0;t-1)$ ثم نحذف الإحداثي الواقع في أقصى اليمين.

(ب) إذا كان:

$$d(s_1,\cdots,s_{m-1},0;t-1)+d_0(s)=d(s_1,\cdots,s_m;t-1)+d_1(s)$$

فنكوّن $W(s;t)$ من $W(s_1,\cdots,s_{m-1},0;t-1)$ وذلك بإضافة الإحداثي الواقع أقصى يسار s إلى يسار $W(s_1,\cdots,s_{m-1},0;t-1)$.

(٤) (فك التشفير) لكل $t \geq \tau$، ضع {لكل مرحلة s $S(t)=\{s: d(s;t) \leq$ $d(s';t)$، s'. إذا كان إحداثي أقصى اليمين في المسار $W(s;t)$ وليكن i هو نفسه لجميع $s \epsilon S(t)$ فنقوم بفك تشفير إحداثي الرسالة على أنه i وخلاف ذلك يكون فك إحداثي الرسالة على أنه *.

ملحوظة

لاحظ أن الإحداثيات التي عددها m في أقصى يسار $W(s;t)$ يجب أن تساوي s ومن ثم لا توجد حاجة إلى تخزينها.

يقدم التمرين (**٨,٤,٦**) تعميماً للخوارزمية (**٨,٤,١**) لفك تشفير شفرات تلاف من النوع (n,k,m).

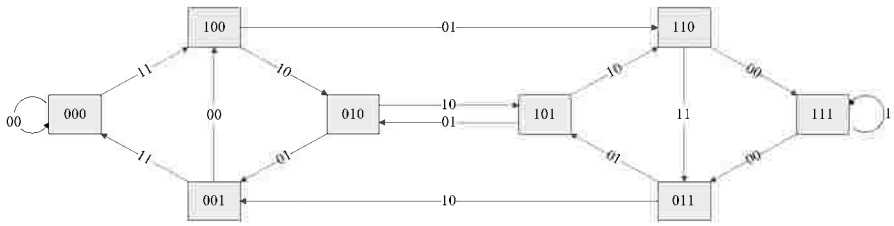
مثال (٨,٤,٢)

لتكن C_1 الشفرة التي لها المولّدان $g_1(x)=1+x+x^3$ و $g_2(x)=1+x^2+x^3$.

ولتكن:

$$w = w_0w_1w_2\cdots = 11\ \ 00\ \ 00\ \ \cdots \leftrightarrow 1+x$$

هي الكلمة المستقبلة (سبق وأن درسنا هذا المثال بشيء من التفصيل في البند (**٨,٣**)). ولنفرض أن سعة النافذة هي $\tau = \tau(2) = 7$ (انظر المثال (**٨,٣,٥**)). مخطط المراحل للشفرة C_1 هو المبين في الشكل (**٨,١٠**).



الشكل (٨,١٠). مخطط مراحل الشفرة C_1.

عنـــد $t = 0$: نضـــع $W(s;0) = s$ **** لكـــل مرحلـــة s ونعـــرف $d(000;0)$ و $d(s';0) = \infty$ لكل مرحلة s' مختلفة عن المرحلة الصفرية.

عند $t = 1$: $w_{t-1} = w_0 = 11$. استناداً إلى الخطوة (٢) من الخوارزمية (**٨,٤,١**) نقوم بدراسة جميع المراحل، مرحلة مرحلة.

$: s = 000$

$$\begin{aligned} d(000;1) &= min\{d(000;0) + 2, d(001;0) + 0\} \\ &= min\{2, \infty\} \\ &= 2 \end{aligned}$$

(نحصل على $d_0(000) = 2$ بملاحظة أن مخرج الضلع الموجّه من المرحلة 000 إلى المرحلة 000 هو 00 وهذا يختلف عن $w_0 = 11$ بموقعين. وبالمثل، $d_1(000) = 0$ ؛ لأن مخرج الضلع الموجّه من المرحلة 001 إلى المرحلة 000 هو 11 وهذا لا يختلف عن w_0).

باستخدام الترميز المستخدم في الخطوة (٣أ) من الخوارزمية (**٨,٤,١**) نجد أننا نحصل على القيمة الصغرى عند $i = 0$، وبهذا نحصل على $W(000;1)$ من $W(000;0)$ بإضافة الإحداثي الذي يقع أقصى يسار المرحلة 000 إلى $W(000;0) = 000$ **** وبعد ذلك نقوم بحذف الإحداثي الواقع في أقصى اليمين. إذن، $W(000;1) = 0000$ ***.

$: s = 100$

$$\begin{aligned} d(100;1) &= min\{d(000;0) + d_0(100), d(001;0) + d_1(100)\} \\ &= min\{0 + 0, \infty + 2\} = 0 \end{aligned}$$

وفي هذه الحالة أيضاً نحصل على القيمة الصغرى عند $i = 0$، وبهذا نحصل على $W(100;1)$ من $W(000;0)$ باضافة الإحداثي الواقع في أقصى يسار المرحلة $s = 100$ إلى $W(000;0)$ ومن حذف الإحداثي الواقع في أقصى اليمين فيكون $W(100;1) = 1000$ ***.

$s = 010$:

$$\begin{aligned} d(010;1) &= min\{d(100;0) + d_0(010), d(101;0) + d_1(010)\} \\ &= min\{\infty + 1, \infty + 1\} \\ &= \infty \end{aligned}$$

في هذه الحالة نستخدم الخطوة (٣ب)؛ لأننا نحصل على قيمة صغرى في كلا الحدّين. لدينا:

$$W(100;0) = 100\ ****$$
$$W(101;0) = 101\ ****$$

ومن ثم فإن $W(010;1) = 010$ **** .

الإحداثي الرابع في المسار $W(010;1)$ هو * لأن $W(100;0)$ و $W(101;0)$ يختلفان في هذا الموقع.

بالمثل، من الممكن حساب $W(s;t)$ و $d(s;t)$ لبقية المراحل. الجدول التالي يلخص لنا الحسابات التي أجريناها:

المرحلة s	$t = 0$	$t = 1$
000	0,000 ****	2,0000 ***
100	∞, 100 ****	0,1000 ***
010	∞, 010 ****	∞, 010 ****
110	∞, 110 ****	∞, 110 ****
001	∞, 001 ****	∞, 001 ****
101	∞, 101 ****	∞, 101 ****
011	∞, 011 ****	∞, 011 ****
111	∞, 111 ****	∞, 111 ****

(كل مدخل في الجدول السابق هو $d(s;t), W(s;t)$).

لاحظ أن تمثيل مخطط المراحل في الجدول السابق يُبيّن إلى جانب المرحلة s مخرج الأضلاع الموجّهة إلى s في مخطط المراحل. وهذه هي بالضبط المخرجات التي نحتاج إليها لحساب $d_0(s)$ و $d_1(s)$، وبهذا نرى أهمية هذه الجدولة للمعلومات وسنظهرها في الجداول التي تلي.

باستمرار فك التشفير عند $t = 2$ و $t = 3$ نحصل على الجدول التالي (لاحظ هنا أن $w_1 = 00$ و $w_2 = 00$).

المرحلة	المخرج			
$s = X_0X_1X_2$	$X_3 = 0$	$X_3 = 1$	$t = 2$	$t = 3$
000	00	11	2,00000 **	2,000000 *
100	11	00	4,10000 **	4,100000 *
010	10	01	1,01000 **	5,010000 *
110	01	10	1,11000 **	5,110000 *
001	01	10	∞, 001 ****	2,001000 *
101	10	01	∞, 101 ****	2,101000 *
011	11	00	∞, 011 ****	3,011000 *
111	00	11	∞, 111 ****	1,111000 *

لاحظ أننا وصلنا الآن إلى $t = 3 = m$. وفي هذه الحالة لدينا $d(s;t) < \infty$ لجميع المراحل s. وهذا يعني وجود مسار طوله m من المرحلة الصفرية إلى كل من المراحل الأخرى. لحد الآن، وجدنا عند حسابنا للقيمة الصغرى باستخدام الخطوة (٢) من الخوارزمية (**٨,٤,١**) أن إحدى القيمتين هي ∞. وهذا ليس صحيحاً عندما يكون $t > m$.

عند $t = 4$: $w_3 = 00$ وبدراسة المراحل نجد أن:

$: s = 000$

$$\begin{aligned} d(000;4) &= min\{d(000;3) + d_0, d(001;3) + d_1\} \\ &= min\{2 + 0,2 + 2\} \\ &= 2 \end{aligned}$$

ونحصل على القيمة الصغرى عند $i = 0$ ومن ثم نحصل على $W(000;4)$ من $W(000;3)$. إذن:

$$W(000;4) = 0000000.$$

$s = 100$:

$$\begin{aligned} d(100;4) &= min\{d(000;3) + d_0, d(001;3) + d_1\} \\ &= min\{2 + 2,2 + 0\} \\ &= 2 \end{aligned}$$

حيث نحصل على القيمة الصغرى عند $i = 1$ ومن ثم نحصل على $W(100;4)$ من $W(001;3)$ ويكون $W(100;4) = 1001000$.

$s = 010$:

$$\begin{aligned} d(010;4) &= min\{d(100;3) + d_0, d(101;3) + d_1\} \\ &= min\{4 + 1,2 + 1\} \\ &= 3 \end{aligned}$$

(حيث المسافة d_0 هي المسافة بين w_3 ومخرج الضلع الموجّه من المرحلة 100 إلى المرحلة 010 ومن ثم فإن $d_0 = 1$. أيضاً، d_1 هي المسافة بين w_3 ومخرج الضلع الموجّه من المرحلة 101 إلى المرحلة 100 ومن ثم فإن $d_1 = 1$.). إذن، نحصل على $W(010;4)$ من $W(101;3)$ ويكون $W(010;4) = 0101000$.

وبحساب مماثل لكل من المراحل الأخرى نحصل على:

المرحلة	المخرج		
s	$X_3 = 0$	$X_3 = 1$	$t = 4$
000	00	11	2,0000000
100	11	00	2,1001000
010	10	01	3,0101000
110	01	10	3,1101000
001	01	10	4,0011000
101	10	01	4,1011000
011	11	00	1,0111000
111	00	11	3,1111000

عند $t = 5$: $w_4 = 00$ وندرس كل مرحلة من المراحل.

$:s = 000$

$$\begin{aligned} d(000;5) &= min\{d(000;4) + d_0, d(001;4) + d_1\} \\ &= min\{2 + 0{,}4 + 2\} \\ &= 2 \end{aligned}$$

ويكون $W(000;5) = 0000000$.

$:s = 100$

$$\begin{aligned} d(100;5) &= min\{d(000;4) + d_0, d(001;4) + d_1\} \\ &= min\{2 + 2{,}4 + 0\} \\ &= 4 \end{aligned}$$

في هذه الحالة، لدينا $d(000;4) + d_0 = d(001;4) + d_1$. ومن ذلك نرى استناداً إلى الخطوة (٣ب) أننا نحصل على $W(100;5)$ من كل من $W(000;4)$ و $W(001;4)$ بوضع * عندما يختلفان وإضافة الإحداثي أقصى يسار 100 وحذف الإحداثي الواقع في أقصى اليمين. وبما أن $W(000;4) = 0000000$ وأن $W(001;4) = 0011000$ فيكون:

$$W(100;5) = 100 ** 00.$$

وبالاستمرار على هذه الشاكلة لبقية المراحل ومن الحالتين $t = 6$ و $t = 7$ نحصل على الجدول التالي:

المرحلة	المخرج				
s	$X_3 = 0$	$X_3 = 1$	$t = 5$	$t = 6$	$t = 7$
000	00	11	2,0000000	2,0000000	2,0000000
100	11	00	4,100 ** 00	2,1001110	4,100 ****
010	10	01	3,0100100	3,0101110	3,0100111
110	01	10	3,1100100	3,1101110	3,1100111
001	01	10	2,0011100	4,001 ** 10	4,001 * 1 * 1
101	10	01	2,1011100	4,101 ** 10	4,101 * 1 * 1
011	11	00	3,0111100	3,0111010	3,0111001
111	00	11	3,1110100	3,1110010	3,1110111

أخيراً وصلنا إلى الحالة $t = \tau$. نستطيع الآن فك تشفير إحداثي الرسالة الأول باستخدام الخطوة (٤) من الخوارزمية (**٨,٤,١**). في هذه الحالة لدينا $S(7) = \{000\}$؛ لأن $d(000;7) = 2 < d(s;7)$ لجميع المراحل $s \neq 000$. وبهذا يكون أول إحداثي يفك تشفيره هو الإحداثي الواقع في أقصى اليمين للمسار $W(000;7)$، أي الإحداثي 0. الآن، نقوم بحذف الإحداثي الواقعة في أقصى اليمين للمسار $W(s;7)$ عند $t = 8$ وذلك أثناء انشاء $W(s;8)$ (الخطوة (٣) من الخوارزمية (**٨,٤,١**)).

الجدول التالي يُبيّن فك التشفير لبعض التكّات الأخرى:

المرحلة s	$t = 8$	$t = 9$	$t = 10$	$t = 11$	$t = 12$
000	2,0000000	2,0000000	2,0000000	2,0000000	2,0000000
100	4,100 ****	4,100 *** 0	4,100 ****	4,100 *** 0	4,1000000
010	5,010 ****	5,010 ****	5,010 ****	5,010 ****	5,0100 ***
110	5,110 ****	5,110 ****	5,110 ****	5,110 ****	5,1100 ***
001	4,001 ****	4,0011101	4,0011100	6,001 ****	6,001 ****
101	4,101 ****	4,1011101	4,1011100	6,101 ****	6,101 ****
011	3,0111011	3,0111001	5,0111 ***	5,01110 **	5,01110 **
111	3,1110011	5,111 ****	5,1110 ***	5,1110 ***	5,1110 ***
: فك التشفير إلى. ▲	0	0	0	0	0

مثال (٨,٤,٣)

مرة أخرى نأخذ الشفرة C_1 المقدمة في المثال (**٨,٤,٢**). لنفرض أن:

$$w = 11\ 00\ 00\ 00\ 10\ 00\ \cdots \leftrightarrow 1 + x + x^8$$

هي الكلمة المستقبلة. ومرة أخرى نستخدم الخوارزمية (**٨,٤,١**) بنافذة سعتها $\tau(2) = 7$ (انظر المثال (**٨,٣,٥**)). الحسابات هي تكرار للحسابات التي أجريناها في المثال (**٨,٤,٢**) إلى أن تصل الحالة $t = 5$ حيث يبدأ تأثير الحد x^8 في الكلمة $w(x)$.

المرحلة	المخرج					
s	$X_3=0$	$X_3=1$	$t=4$	$t=5$	$t=6$	$t=7$
000	00	11	2,0000000	3,0000000	3,000 *** 0	3,0000 ***
100	11	00	2,1001000	3,1000000	1,1001110	3,1001001
010	10	01	3,0101000	2,0100100	4,010 *** 0	2,0100111
110	01	10	3,1101000	4,110 * 100	4,110 *** 0	2,1100111
001	01	10	4,0011000	1,0011100	3,0010010	5,001 ****
101	10	01	4,1011000	3,101 * 100	3,1010010	5,101 ****
011	11	00	1,0111000	4,011 * 100	4,0111 * 10	4,01110 * 1
111	00	11	3,1111000	4,111 * 100	4,1110 * 10	4,1110 ***
فك التشفير إلى :						1

في هذه الحالة، عند $t=7$ نقوم بفك تشفير الإحداثي 1 من الرسالة. إذا فرضنا أن الكلمة الصفرية هي الكلمة التي تم إرسالها فيكون الخطأ الثالث في الكلمة $w(x)$ هو الذي تسبب في فك تشفير خاطئ. ▲

تمارين

(٨,٤,٤) استمر في فك تشفير $w(x)$ المقدمة في المثال **(٨,٤,٣)** عند $t=8,9,10,11,12$. هل من الممكن أن يكون إحداثي الرسالة التي تم فك تشفيرها هو 0 عندما يكون $t\geq 12$ ؟

(٨,٤,٥) مرة أخرى، استخدم شفرة التلاف C_1 حيث $g_1=1+x+x^3$ و $g_2=1+x^2+x^3$ واستخدم الخوارزمية **(٨,٤,١)** بنافذة سعتها $\tau(2)=7$ لفك تشفير كل من الكلمات المستقبلة التالية. استمر في عملية فك التشفير حتى $t=9$.

(أ) $w(x)=1+x^3\leftrightarrow 10\ 01\ 00\ 00\ \cdots$.

(ب) $w(x)=1+x+x^2\leftrightarrow 11\ 10\ 00\ 00\ \cdots$.

(ج) $w(x)=x^3+x^8+x^{12}\leftrightarrow 00\ 01\ 00\ 00\ 10\ 00\ 10\ 00\ \cdots$.

(٨,٤,٦) يمكن تعميم الخوارزمية (٨,٤,١) لفك تشفير شفرات تلاف من النوع (n,k,m) على النحو التالي (مخططات المراحل لهذه الشفرات هي المقدمة في التمرين (٨,٢,١٤)).

(١) نفس خطوة الخوارزمية (٨,٤,١).

(٢) لكل $t>0$ ولكل مرحلة $s_0,s_1,\cdots,s_{m-k}$ نعرف:

$$d(s;t)=\min_u\{d(s_k,\cdots,s_{m-k},u;t-1)+d_u\}$$

حيث مجال u هو جميع الكلمات الثنائية من الطول k وحيث d_u هي المسافة بين w_{t-1} ومخرج الضلع الموجّه من المرحلة $s_k,\cdots,s_{m-k},u$ إلى المرحلة s في مخطط المراحل.

(٣) (أ) إذا كان لكل $v\neq u$

$$d(s_k,\cdots,s_{m-k},u;t-1)+d_u<d(s_k,\cdots,s_{m-k},v;t-1)+d_v$$

فنقوم بإنشاء $W(s;t)$ من $W(s_k,\cdots,s_{m-k},u;t-1)$ بحذف الإحداثيات التي عددها k في أقصى اليمين وإضافة الإحداثيات التي عددها k في أقصى يسار s إليه.

(ب) إذا لم تكن $d(s_k,\cdots,s_{m-k},u;t-1)$ هي القيمة الصغرى لخيار وحيد u فنقوم بإنشاء $W(s;t)$ باختيار أي من القيم u ومن ثم نستمر كما في الخطوة (٣أ). من الممكن أيضاً أن نأخذ تركيباً لجميع المسارات $W(s_k,\cdots,s_{m-k},u;t-1)$ التي تكون فيها المسافة $d(s_k,\cdots,s_{m-k},u;t-1)$ مسافة صغرى (كما هو الحال في الخوارزمية (٨,٤,١))، ومن ثم نضع العلامة * في المواقع التي يختلف فيها مساران.

(٤) لكل $t\geq\tau$، ضع $S(t)=\{s:d(s;t)\leq d(s';t)$ ، لجميع المراحل $s'\}$.

فك تشفير إحداثيات الرسالة $m_{1,t},m_{2,t},\cdots,m_{k,t}$ حيث $m_{i,t}$ هو الإحداثي i من الإحداثيات k الواقعة في أقصى يمين $W(s;t)$ لكل $s\epsilon S(t)$. وإذا اختلف مساران في الموقع i يكون فك التشفير هو $m_{i,t}=*$.

برهن أن هذه الخوارزمية هي بالفعل تعميم للخوارزمية (٨,٤,١).

نناقش بعض الملاحظات على الخوارزمية (٨,٤,١). أولى هذه الملاحظات هي إمكانية وجود طرق أخرى لتعريف خطوة فك التشفير (الخطوة (٤) من الخوارزمية). على سبيل المثال، من الممكن عدم البدء بعملية فك التشفير حتى تتفق جميع المسارات إلى كل من المراحل في الإحداثي الواقع في أقصى اليمين (أي الإحداثي المستخدمة في فك التشفير). ولكن في مثل هذه الحالة يجب علينا انتظار عدد كبير من التكّات قبل تنفيذ فك التشفير وهذا يحتاج إلى سعة تخزين أكبر. من الممكن أيضاً إجراء تعديل آخر على الخطوة (٤) وهو حذف كل من المسارات التي تختلف فيها الإحداثي الواقع في أقصى اليمين عن إحداثي الرسالة الجاري فك تشفيره؛ (لأن مثل هذه المسارات تتحرك إلى مراحل مختلفة). ولكن مثل هذه الإجراء سيطرح بعض الأسئلة النظرية عن الخوارزمية حيث من الممكن أن يؤدي فك التشفير في هذه الحالة إلى عدد غير منته من الأخطاء في أنماط أخطاء اندفاعية منتهية أثناء عملية الإرسال.

أما ثاني هذه الملاحظات فهي السؤال: هل من الممكن إثبات نتيجة مماثلة للمبرهنة (٨,٣,٤) لخوارزمية ڤيتربي المبتورة لفك التشفير (خوارزمية (٨,٤,١))؟ الاجابة عن هذا السؤال هي لا؛ لأن هذه الخوارزمية تحتاج إلى بعض الوقت لكي تتخلص من الأخطاء التي يمكن وقوعها في كلمة الشفرة أثناء عملية الإرسال. ولرؤية لماذا يوجد فرق بين الخوارزميتين، افرض أن $t = 2$ في المثال (٨,٤,٢). عند استخدام خوارزمية ڤيتربي المبتورة لفك التشفير فإن المسار الذي ينتظر في المرحلة 000 سيتذكر الخطأين اللذين سبق وقوعهما في w عند التكّة $t = 1$ عندما كانت $w_{t-1} = 11$ والسبب في ذلك يعود إلى أن $d(000; 2) = 2$. سنرى في المثال (٨,٤,٧) أن تأثير هذين الخطأين سيبقى حتى التكّة $t = 12$. ولكن من ناحية أخرى، عند استخدام خوارزمية الاستنفاد لفك التشفير نرى أن الخطأين اللذين كان لهما تأثير في قرار فك التشفير عند التكّة

$t = 1$ ينتهي تأثيرهما بعد ذلك (أي عند $t \geq 2$). تذكر أنه عند $t \geq 2$ يتم مقارنة المسارات ذات الطول τ من المرحلة 000 مع $w_{t-1}, w_t, \cdots, w_{t+\tau-2} = 00\cdots0$ وهذا جزء من الكلمة المستقبلة يتفق فقط مع المسارات التي لا تزال عند المرحلة الصفرية.

نقدم الآن بعض التفصيلات عن الزمن الذي يستمر فيه تأثير الأخطاء أثناء عملية الإرسال على فك التشفير عند استخدام خوارزمية ڤيتربي المبتورة لفك التشفير بنافذة سعتها $\tau(e)$ المعرفة في الخوارزمية (**٨,٤,١**). نبدأ بتقديم بعض التعريفات. نفرض أن $w(s,s')$ هو الوزن الأصغر لممر من s إلى s' في مخطط المراحل. لنفرض أن $s(t)$ هي المرحلة الصحيحة عند التكّة t (أي أن $s(t)$ هي مرحلة وصول كلمة الشفرة المرسلة عند التكّة t). سنقول إن فك التشفير جاهز من **النوع *e*** **(*e*-ready)** عند التكّة t إذا تحقق الشرطان التاليان:

(١) $d(s';t) \geq d(s(t);t) + min\{1+e, w(s(t),s')\}$ لكل $s' \neq s(t)$.

(٢) إذا كان $w(s(t),s') < 1+e$ فإن $W(s';t) = s'v$ (من الطول τ)حيث v يحقق $W(s(t);t) = s(t)v$.

مثال (٨,٤,٧)

في المثال (**٨,٤,٢**)، نرى أن المرحلة الصحيحة لكل $t \geq 1$ هي $s(t) = 000$؛ لأننا افترضنا أن كلمة الشفرة التي تم إرسالها هي الكلمة الصفرية. وبما أن $m = 3$ عدد صغير فيمكن حساب $w(s(t),s') = w(000,s')$ لكل $s' \neq 000$ من مخطط المراحل بسهولة:

$$w(000,100) = 2, w(000,010) = 3, w(000,001) = 4,$$
$$w(000,110) = 3, w(000,101) = 4, w(000,011) = 3,$$
$$w(000,111) = 3$$

المرة الأولى التي يكون عندها فك التشفير جاهزاً من النوع 2 في المثال (**٨,٤,٢**) هي عند التكّة $t = 12$. ولرؤية ذلك لاحظ ما يلي:

عند $t = 10$، لدينا:

$$d(001; 10) = 4 < 5 = d(000; 10) + min\{1 + e, w(000,001)\}$$

ولذا فالشرط (١) من تعريف جاهزية فك التشفير غير محقق.

عند $t = 11$ نرى أن جميع المراحل تحقق الشرط (١) من تعريف جاهزية فك التشفير ولكن $w(000,100) = 2 < 3 = 1 + e$ وأن $W(100; 11) = 100 \text{****} \neq 100v$ (لأن $W(000; 11) = 0000000 = s(1)v$ وبهذا يكون $v = 0000$).

عند $t = 12$ نرى أن جميع المراحل تحقق الشرط (١) وأن $s' = 100$ هي المرحلة الوحيدة حيث $\mathrm{w}(000, s') < 1 + e$ و $W(100; 12) = 1000000 = s'0000 = s'v$. ▲

المبرهنة التالية تُبيّن أهمية أن يكون فك التشفير جاهزاً من النوع e.

مبرهنة (٨,٤,٨)

لتكن C شفرة تلاف غير إخفاقية تستخدم خوارزمية ڤيتربي المبتورة لفك التشفير (خوارزمية (٨,٤,١)). عند التكّة t، إذا كان فك التشفير جاهزاً من النوع e فسنحصل على فك تشفير صائب إذا وقعت أخطاء لا يزيد عددها عن e أثناء عملية الإرسال.

توضح لنا المبرهنة خلفية تسمية الجاهزية من النوع e. ومن الواضح أن هذه المبرهنة أضعف بكثير من المبرهنة (٨,٣,٤). يُعرف **فضاء الحماية (Guard Space)** على أنه الفترة الزمنية الخالية من أخطاء الإرسال التي تلي أخطاء اندفاعية. للحصول على نتيجة مشابهة للمبرهنة (٨,٣,٤) نحتاج لمعرفة فضاء الحماية اللازم قبل أن يكون فك التشفير جاهزاً من النوع e. عند استخدام فك التشفير الاستنفادي، نرى أن المبرهنة (٨,٣,٤) تضمن لنا فضاء حماية يساوي 0 (إذا اعتبرنا أن الجاهزية من النوع e تعني أن أي نمط خطأ لاحق وزنه لا يزيد عن e يؤدي إلى فك تشفير صائب للكلمة المستقبلة). في الحقيقة، يمكن إثبات أن فضاء الحماية اللازم ليكون فك تشفير ڤيتربي المبتور جاهزاً من النوع e بعد أخطاء اندفاعية هو زمن منته وأنه من الممكن معرفة طول

فضاء الحماية لبعض شفرات التلاف التي يكون فيها العدد m صغيراً. إن أقرب صيغة للمبرهنة (٨,٣,٤) يمكن الحصول عليها هي :

مبرهنة (٨,٤,٩)

لتكن C شفرة تلاف غير اخفاقية تستخدم خوارزمية ڤيتربي المبتورة لفك التشفير بنافذة سعتها $\tau(e)$ (الخوارزمية (٨,٤,١)). إذا أمكن تجزئة أنماط الأخطاء إلى أخطاء اندفاعية وزن كل منها لا يزيد عن e حيث يتبع كل منها فضاء حماية طوله كافٍ (منته) فإن فك التشفير يكون صائباً.

تمارين

(٨,٤,١٠) (أ) استخدم الخوارزمية (٨,٤,١) بنافذة سعتها $\tau(2) = 6$ لفك تشفير الكلمة المستقبلة $w = 11\ 00\ 00\ \cdots \leftrightarrow 1 + x = w(x)$ المشفرة باستخدام شفرة تلاف من النوع (2,1,2) بمولّدين $g_1(x) = 1 + x^2$ و $g_2(x) = 1 + x + x^2$. استمر في عملية فك التشفير لإثبات أن فك التشفير جاهز من النوع 2 عند $t = 10$ بفرض أن كلمة الشفرة التي تم إرسالها هي الكلمة الصفرية (ومن ثم فالمرحلة الصحيحة $s(t)$ هي المرحلة الصفرية لكل t).

(ب) أثبت أن فك التشفير ليس جاهزاً من النوع 2 عند $t = 9$ ومن ثم لا تضمن لنا المبرهنة (٨,٤,٨) تصويب أي نمط خطأ لاحق وزنه لا يزيد عن $e = 2$. إذا كان $t = 10$ و $t = 11$ فأثبت أن إحداثيات الكلمة المستقبلة يتغير كل منها إلى 10 (أي أن الكلمة المستقبلة هي $w(x) = 1 + x + x^{18} + x^{20}$) ومن ثم يكون فك التشفير * عند $t = 12$.

(٨,٤,١١) لكل كلمة مستقبلة في التمرين (٨,٤,٥)، جد أصغر t بحيث يكون فك التشفير جاهزاً من النوع 2 عند التكّة t.

أخيراً نقوم بحساب كل من $d(C)$ و $\tau(e)$. ولانجاز ذلك علينا إيجاد أوزان المسارات التي غادرت للتو المرحلة الصفرية. لحساب $d(C)$ نحتاج إلى إيجاد المسار ذي الوزن الأصغر ولحساب $\tau(e)$ نحتاج إلى إيجاد الطول x بحيث يكون وزن أي مسار طوله على الأقل x لا يزيد عن $2e$. من الممكن تعديل خوارزمية ڤيتربي المبتورة لفك التشفير (الخوارزمية (٨,٤,١)) لانجاز المهمتين. لنفرض أولاً أن الكلمة الصفرية هي الكلمة المرسلة. عندئذ، دالة المسافة تحسب لنا أوزان المسارات. ثانياً، لإرغام المسارات على مغادرة مباشرة للمرحلة الصفرية نضع $d(00\cdots 0;1)=\infty$. ولهذا نسقط من حساباتنا المسارات التي تبقى عند المرحلة الصفرية؛ لأن المسار المتبقي حيث $d(s;1)$ منته، هو المسار إلى $s=100\cdots 0$ (أي المسار المغادر مباشرة المرحلة الصفرية). ثالثاً، لا نحتاج إلى تخزين المسارات $W(s;t)$؛ لأنها لا تؤثر في هذه الحسابات. رابعاً، يجب علينا معرفة الاجابة! لكل شفرة غير اخفاقية، نرى أن كل مسار من المسارات ذات الوزن المنتهي الذي يعود إلى المرحلة الصفرية يبقى في هذه المرحلة ولا يغادرها أبداً. عند كل تكّة t، تكون $d(s;t)$ هي وزن مسار أصغري من الطول t الذي يغادر مباشرة المرحلة الصفرية وينتهي عند المرحلة s. أيضاً إذا كان $d(s;t)\geq d(00\cdots 0;t)$ عند التكّة t لكل المراحل s فنجد أن $d(00\cdots 0;t')=d(00\cdots 0;t)$ لكل $t'\geq t$ (استناداً إلى الخطوة (٢) من الخوارزمية (٨,٤,١)) يكون من الواضح أن $d(s';t')\geq min_s\{d(s;t'-1)\}$ لكل مرحلة s'). إذن، $d(C)=d(00\cdots 0;t)$. وبالمثل، بمجرد أن يكون $d(s;t)>2e$ لكل مرحلة s، نرى أن وزن جميع المسارات من الطول t التي تغادر مباشرة المرحلة الصفرية أكبر من $2e$. وبهذا نجد أن $\tau(e)$ هو أول تكّة t تحقق $d(s;t)>2e$ لكل مرحلة s. وعليه يكون لدينا التعديل التالي للخوارزمية (٨,٤,١) لحساب $d(C)$ و $\tau(e)$.

خوارزمية (٨,٤,١٢) [إيجاد $d(C)$ و $\tau(e)$ لشفرات تلاف غير إخفاقية]

نفرض أن $wt(s;s')$ وزن الضلع الموجّه من s إلى s' في مخطط المراحل. يتم تنفيذ الخطوات التالية:

(١) إذا كان $t=1$ فنعرّف:

$$d(s;t)=\begin{cases} wt(00\cdots0;100\cdots0) & ,s=100\cdots0 \\ \infty & \text{خلاف ذلك}, \end{cases}$$

(٢) لكل $t>1$ ولكل مرحلة $s=s_0,\cdots,s_{m-1}$ نعرّف:

$$\begin{aligned} d(s;t)=min\{&d(s_0,\cdots,s_{m-1},0;t-1)\\ &+wt(s_0,\cdots,s_{m-1},0;s),d(s_0,\cdots,s_{m-1},1;t-1)\\ &+wt(s_0,\cdots,s_{m-1},1;s)\} \end{aligned}$$

(٣) إذا كان $d(00\cdots0;t)\geq d(s;t)$ لكل مرحلة s فإن $d(C)=d(00\cdots0;t)$.

(٤) إذا كان $d(s;t)>2e$ لكل مرحلة s وتوجد مرحلة s' حيث $d(s';t-1)\leq 2e$ فإن $\tau(e)=t$.

ملحوظة

إذا فرضنا أن الكلمة المستقبلة هي $w=000\cdots$ فتكون الخوارزمية (٨,٤,١٢) هي الخوارزمية (٨,٤,١) مع الفرق الوحيد وهو تعريفنا $d(00\cdots0;1)=\infty$ وعدم حساب $W(s;t)$.

مثال (٨,٤,١٣)

نحسب $d(C)$ و $\tau(e)$ حيث $1\leq e\leq\lfloor(d(C)-1)/2\rfloor$ للشفرة C_1 التي لها المولّدان $g_1(x)=1+x+x^3$ و $g_2(x)=1+x^2+x^3$ (قمنا سابقاً بهذه الحسابات في المثال (٨,٣,٦) والفقرة المقدمة قبل المثال (٨,٣,٥)). سنستخدم المثال (٨,٤,٢) عند تنفيذ الخوارزمية (٨,٤,١).

المرحلة	المخرج										
s	$X_3=0$	$X_3=1$	$t=1$	2	3	4	5	6	7	8	9	10
000	00	11	∞	∞	∞	6	6	6	6	6	6	6
100	11	00	2	∞	∞	4	6	4	6	6	6	6
010	10	01	∞	3	∞	5	5	5	5	7	7	7
110	01	10	∞	3	∞	5	5	5	5	7	7	7
001	01	10	∞	∞	4	6	4	6	6	6	6	6
101	10	01	∞	∞	4	6	4	6	6	6	6	6
011	11	00	∞	∞	5	3	5	5	5	5	5	7
111	00	11	∞	∞	3	5	5	5	5	5	7	7

عند $t=10$: $d(000;10) \geq d(s;10)$ لكل مرحلة s، وبهذا يكون $d(C)=d(000;10)=6$ (من الخطوة (٣) في الخوارزمية (٨,٤,١١)). بما أن $1 \leq e \leq \lfloor (d(C)-1)/2 \rfloor$ فنرى أن $e=1$ و $e=2$.

عند $e=1$: $d(s;2)>2e$ لكل مرحلة s وإن $d(000;1)=2 \leq 2e$. إذن، باستخدام الخطوة (٤) من الخوارزمية (٨,٤,١٢) يكون $\tau(1)=2$.

عند $e=2$: $d(s;7)>2e$ لكل مرحلة s وإن $d(100;6)=4 \leq 2e$. إذن، باستخدام الخطوة (٤) من الخوارزمية (٨,٤,١٢) نجد أن $\tau(1)=2$. ▲

تمرين

(٨,٤,١٤) لكل من شفرات التلاف C ذات المولّدات المبيّنة، استخدم الخوارزمية (٨,٤,١٢) لحساب $d(C)$ و $\tau(e)$ حيث $1 \leq e \leq \lfloor (d(C)-1)/2 \rfloor$. قارن إجابتك مع إجابات التمرينين (٨,٣,٣) و (٨,٣,٦).

(أ) $g_1(x)=1+x^2$ و $g_2(x)=1+x+x^2$.

(ب) $g_1(x)=1+x+x^2+x^3$ و $g_2(x)=1+x^2+x^3$.

(ج) $g_1(x)=1+x^3+x^4$ و $g_2(x)=1+x+x^2+x^4$.