الفصل الثاني

الشفرات الخطية
Linear Codes

(٢,١) الشفرات الخطية
Linear Codes

نقدم في هذا البند صنفاً عاماً من الشفرات حيث تنتمي جميع الشفرات التي سندرسها إلى هذا الصنف. وبدراستنا لهذا الصنف يكون بمقدورنا توظيف بعض المفاهيم الرياضية المهمة التي تساعدنا على حل بعض المسائل التي سبق وأن ناقشناها للشفرات التي تنتمي إلى هذا الصنف.

نقول إن الشفرة C **شفرة خطية على الحقل K (Linear Code)** إذا كانت $v + w \in C$ لكل $w, v \in C$. أي أن الشفرة الخطية هي الشفرة المغلقة تحت عملية جمع الكلمات. على سبيل المثال، الشفرة $C = \{000, 111\}$ شفرة خطية ؛ لأن جميع المجاميع الأربعة :

$$000 + 000 = 000$$
$$000 + 111 = 111$$
$$111 + 000 = 111$$
$$111 + 111 = 000$$

تنتمي إلى الشفرة C. ولكن الشفرة $C_1 = \{000, 001, 101\}$ ليست خطية ؛ لأن $001, 101 \in C_1$ ولكن $001 + 101 = 100 \notin C_1$.

لاحظ أنه إذا كانت C شفرة خطية وكانت $v \in C$ فإن $v + v = 0 \in C$. وبهذا نرى أن أي شفرة خطية يجب أن تحتوي الكلمة الصفرية. ولكن العكس، غير صحيح، فالشفرة C_1 المقدمة في الفقرة السابقة تحتوي على الكلمة الصفرية ولكنها ليست شفرة خطية.

تمارين

(**٢,١,١**) بيّن أي من الشفرات التالية هي شفرة خطية:

(أ) $C = \{101, 111, 011\}$

(ب) $C = \{000, 001, 010, 011\}$

(ج) $C = \{0000, 0001, 1110\}$

(د) $C = \{0000, 1001, 0110, 1111\}$

(هـ) $C = \{00000, 11111\}$

(و) $C = \{00000, 11100, 00111, 11011\}$

(ز) $C = \{00000, 11110, 01111, 10001\}$

(ح) $C = \{000000, 101010, 010101, 111111\}$

إحدى خصائص الشفرة الخطية التي تميزها عن الشفرات غير الخطية هي سهولة حساب مسافتها. فمسافة الشفرة الخطية هي أصغر أوزان كلماتها غير الصفرية. برهان هذه الحقيقة السهلة هو فحوى التمرين (**٢,١,٤**).

تمارين

(**٢,١,٢**) أثبت أن الشفرة $C = \{0000,1100,0011,1111\}$ خطية وأن مسافتها هي $d = 2$.

(**٢,١,٣**) جد مسافة كل من الشفرات الخطية المقدمة في التمرين (**٢,١,١**) ثم تحقق من أن ذلك يتفق مع ما وجدته في التمرين (**١,١١,١٢**).

(**٢,١,٤**) أثبت أن مسافة الشفرة الخطية تساوي أصغر أوزان كلماتها غير الصفرية.

سنرى في البنود القادمة أن سهولة حساب مسافة الشفرة الخطية ليست الميزة الوحيدة التي تجعلها أفضل من الشفرات غير الخطية، بل توجد عديد من الميزات الأخرى لهذه الشفرات حيث إن عديداً من المسائل التي يصعب معالجتها للشفرات العامة تكون معالجتها سهلة للشفرات الخطية وإليك بعض الأمثلة على ذلك:

(١) توجد خوارزمية أسهل وأسرع للتنفيذ لإيجاد MLD للشفرات الخطية من الخوارزمية المقدمة سابقاً (في الحقيقة، للشفرات الخطية التي تتمتع بخواص إضافية تكون خوارزمية فك التشفير سهلة جداً).

(٢) تشفير الشفرة الخطية أسرع ويحتاج إلى سعة تخزين أقل من الشفرات غير الخطية.

(٣) حساب الاحتمالات $\theta_p(C,v)$ مباشر للشفرات الخطية.

(٤) من السهل وصف أنماط الأخطاء التي تكتشفها الشفرة الخطية.

(٥) من السهل وصف أنماط الأخطاء التي تصوّبها الشفرة الخطية.

يُعد الجبر الخطي من أهم الموضوعات التي نحتاجها لدراسة الشفرات الخطية. ففي هذا البند وبعض البنود القادمة سنراجع بعض الحقائق الأساسية من الجبر الخطي ونحاول أن نبين أهمية ذلك لنظرية التشفير. معظم البراهين التي لا تعتمد على الضرب بعدد قياسي في K^n هي نسخة مطابقة تماماً للبراهين في $\mathbb{R}^n$ ومن ثم سنسقطها.

تذكر أن فضاء المتجهات K^n على K (يُسمى K حقل الأعداد القياسية) يتكون من مجموعة من متجهات (أو كلمات) K^n معرفاً عليها عملية الضرب بعدد قياسي وعملية جمع متجهات ويحقق الشروط العشرة التي قدمناها في البند (**١,٧**). نقول إن مجموعة جزئية غير خالية U من فضاء متجهات V، **فضاءً جزئياً من V (Subspace of V)** إذا كانت U مغلقة تحت عمليتي جمع المتجهات والضرب بعدد قياسي. أي أنه إذا كان $v,w \in U$ وكان a عدداً قياسياً فإن $v+w \in U$ وإن $av \in U$.

وعلى وجه الخصوص، بما أن أعداد K القياسية هي 0 و 1 فقط فتكون U فضاءً جزئياً من K^n إذا وفقط إذا كانت المجموعة الجزئية U مغلقة تحت عملية الجمع. وبهذا نرى أن الشفرة C خطية إذا وفقط إذا كانت فضاءً جزئياً من K^n. في البنود القليلة القادمة، نستخدم مفهوم الفضاءات الجزئية لتسهيل عمليتي التشفير وفك التشفير.

(٢,٢) فضاءان جزئيان مهمان
Two Important Subspaces

نقدم الآن فضائين جزئيين من فضاء المتجهات K^n وهما مثالان مهمان على الشفرات الخطية حيث سيؤديان دوراً مهماً في دراستنا المستقبلية. سنقدم التعاريف والنتائج على فضاء متجهات عام ثم نوظفها لفضاء المتجهات K^n.

نقول إن المتجه w **تركيب خطي (Linear Combination)** للمتجهات $v_1, v_2, \cdots, v_k$ إذا وجدت أعداد قياسية $a_1, a_2, \cdots, a_k$ بحيث يكون:

$$w = a_1v_1 + a_2v_2 + \cdots + a_kv_k$$

تُسمى جميع التركيبات الخطية لمتجهات المجموعة $S = \{v_1, v_2, \cdots, v_k\}$، **الفضاء الخطي المولّد بالمجموعة S (Linear Span of S)** ويُرمز له بالرمز $\langle S \rangle$. إذا كانت $S = \emptyset$ فنعرّف $\langle S \rangle = \{0\}$.

من المعلوم في الجبر الخطي أنه لأي مجموعة جزئية S من فضاء متجهات V يكون الفضاء الخطي المولّد الخطي $\langle S \rangle$ فضاءاً جزئياً من V ويُسمى **الفضاء الجزئي المولّد بالمجموعة S (Subspace Spanned or Generated by S)**. في حالة فضاء المتجهات K^n يوجد وصف سهل للفضاء الجزئي $\langle S \rangle$ وهو فحوى المبرهنة التالية. وبما أن $\langle S \rangle$ فضاء جزئي من K^n فنسمي $\langle S \rangle$ من الآن فصاعداً، **الشفرة الخطية المولّدة بالمجموعة S (Linear Code Generated by S)**.

مبرهنة (٢,٢,١)

لتكن $S \subseteq K^n$. تتكون الشفرة $C = \langle S \rangle$ من الكلمات التالية :

الكلمة الصفرية، جميع كلمات S، جميع مجاميع كلمتين أو أكثر من كلمات S. ■

مثال (٢,٢,٢)

إذا كانت $S = \{0100\,,0011\,,1100\}$ فإن كلمات الشفرة $C = \langle S \rangle$ هي :

$$0000\,,0100\,,1100\,,0011$$
$$0100 + 0011 = 0111$$
$$0100 + 1100 = 1000$$
$$0011 + 1100 = 1111$$
$$0100 + 0011 + 1100 = 1011$$

وبهذا يكون :

$$C = \langle S \rangle = \{0000\,,0100\,,0011\,,1100\,,0111\,,1000\,,1111\,,1011\}$$ ▲

تمرين

(٢,٢,٣) جد عناصر الشفرة الخطية $\langle S \rangle$ لكل من المجموعات S التالية :

(أ) $S = \{010\,,011\,,111\}$

(ب) $S = \{1010\,,0101\,,1111\}$

(ج) $S = \{0101\,,1010\,,1100\}$

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

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

(و) $S = \{10101\,,01010\,,11111\,,00011\,,10110\}$.

إذا كان $v = (a_1, a_2, \cdots, a_n), w = (b_1, b_2, \cdots, b_n) \in K^n$ فنُعرّف **الضرب القياسي أو الضرب النقطي (Scalar or Dot Product)** $v \cdot w$ للمتجهين v و w على النحو التالي :

$$v \cdot w = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

لاحظ أن $v \cdot w$ عدد قياسي. على سبيل المثال، في الفضاء K^5 لدينا:

$$\begin{aligned} 11001 \cdot 01101 &= 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 \\ &= 0 + 1 + 0 + 0 + 1 \\ &= 0 \end{aligned}$$

تمارين

(**٢,٢,٤**) جد أمثلة في الفضاء K^5 للقاعدتين التاليتين:

(أ) $u \cdot (v + w) = u \cdot v + u \cdot w$

(ب) $a(v \cdot w) = (av) \cdot w = v \cdot (aw)$

(**٢,٢,٥**) أثبت صواب القاعدتين المقدمتين في التمرين (**٢,٢,٤**) في الفضاء K^n.

نقول إن المتجهين v و w **متعامدان (Orthogonal)** إذا كان $v \cdot w = 0$. المثال المقدم في الفقرة أعلى الصفحة يُبين أن المتجهين $v = 11001$ و $w = 01101$ متعامدان في الفضاء K^5. إذا كانت S مجموعة جزئية من K^n وكان $v \in K^n$ فنقول إن v **عمودي على المجموعة S (Orthogonal to the Set S)** إذا كان $v \cdot w = 0$ لكل $w \in S$. أي أن v عمودي على جميع متجهات S. يُرمز لمجموعة جميع المتجهات العمودية على S بالرمز $S^{\perp}$ وتُسمى **المتمم العمودي على S (Orthogonal Complement of S)**.

نعلم من الجبر الخطي أنه إذا كانت S مجموعة جزئية من فضاء متجهات V فإن المتمم العمودي $S^{\perp}$ فضاء جزئي من V[1]. إذا كانت $C = \langle S \rangle$ في الفضاء K^n فنكتب $C^{\perp} = S^{\perp}$ ونقول إن $C^{\perp}$ هي **الشفرة الثنوية للشفرة C (The Dual Code of C)**.

---

(١) المترجمان: بما أن $\mathbf{0} \cdot w = 0$ لكل $w \epsilon S$ فنجد أن $\mathbf{0} \epsilon S$.

وإذا كان $w, u \epsilon S^{\perp}$ و $\alpha \epsilon K$ فعندئذ لكل $v \epsilon S$ لدينا:

$$v \cdot (w + u) = v \cdot w + v \cdot u = 0 + 0$$
$$(kv) \cdot w = k(v \cdot w) = k \cdot 0 = 0$$

وبهذا يكون $S^{\perp}$ فضاءاً جزئياً من V.

مثال (٢,٢,٦)

إذا كانت $S = \{0100\,, 0101\}$ فاحسب الشفرة الثنوية $C^{\perp} = S^{\perp}$.

الحل

المطلوب إيجاد جميع الكلمات $v = (x, y, z, w)$ في K^4 التي تحقق المعادلتين:

$$v \cdot 0100 = 0$$
$$v \cdot 0101 = 0$$

وبحساب الضرب القياسي نجد أن:

$$y = 0$$
$$y + w = 0$$

وبهذا نرى أن $y = w = 0$. وأما كل من x و z فتأخذ أياً من القيمتين 0 أو 1 (أي عنصر من عناصر K). وبإيجاد جميع الخيارات الممكنة للمتجه v نحصل على $C^{\perp} = S^{\perp} = \{0000\,, 0010\,, 1000\,, 1010\}$. ▲

تمارين

(٢,٢,٧) عيّن الشفرة الثنوية $C^{\perp}$ لكل من الشفرات $C = \langle S \rangle$ المبينة في التمرين **(٢,٢,٣)**.

(٢,٢,٨) جد مثالاً لكلمة غير صفرية v بحيث يكون $v \cdot v = 0$. ماذا يمكن القول عن أوزان مثل هذه الكلمات ؟

(٢,٢,٩) إذا كانت S مجموعة جزئية من فضاء المتجهات V فأثبت أن $\langle S \rangle = (S^{\perp})^{\perp}$.
استخدم المثال **(٢,٢,٦)** لإعطاء مثال لهذه الحقيقة في الفضاء K^4.

(٢,٢,١٠) أثبت أن $\langle S \rangle \subseteq (S^{\perp})^{\perp}$ (في الحقيقة، $\langle S \rangle = (S^{\perp})^{\perp}$) وللشفرات الخطية C هذا يعني أن $C = (C^{\perp})^{\perp}$.

(٢,٣) الاستقلال والأساس والبُعد

Independence, Basis, Dimension

نُقدم مراجعة عامة لعدة مفاهيم من الجبر الخطي ثم نوضح كيفية توظيف هذه المفاهيم للشفرات الخطية. الهدف الرئيس هو إيجاد طريقة فعّالة لوصف الشفرة الخطية

دون اللجوء إلى سرد جميع كلماتها. نقول إن مجموعة من المتجهات $S = \{v_1, v_2, \cdots, v_k\}$ **مرتبطة خطياً (Linearly Dependent)** إذا وجدت أعداد قياسية $a_1, a_2, \cdots, a_k$ ليست كلها أصفاراً بحيث يتحقق:

$$a_1v_1 + a_2v_2 + \cdots + a_kv_k = 0$$

وإذا لم تكن S مرتبطة خطياً فنقول إنها **مُستقلة خطياً (Linearly Independent)**.

أي أن S مُستقلة خطياً إذا تحقق ما يلي لكل أعداد قياسية $a_1, a_2, \cdots, a_k$

$$a_1v_1 + a_2v_2 + \cdots + a_kv_k = 0 \Rightarrow a_1 = a_2 = \cdots = a_k = 0$$

لاختبار فيما إذا كانت مجموعة S مُستقلة خطياً نقوم بكتابة المعادلة $a_1v_1 + a_2v_2 + \cdots + a_kv_k = 0$. فإذا كان حل هذه المعادلة هو الحل التافه (أي أن $a_i = 0$ لكل $i = 1,2,\cdots,k$) فتكون S مُستقلة خطياً. أما إذا وجد على الأقل حل a_i غير صفري فتكون S مرتبطة خطياً.

مثال (٢,٣,١)

أثبت أن $S = \{1001\ ,\ 1101\ ,\ 1011\}$ مجموعة جزئية مُستقلة خطياً في K^4.

الحل

لنفرض أن a ، b ، c أعداد قياسية (0 أو 1) حيث:

$$a(1001) + b(1101) + c(1011) = 0000$$

بمقارنة إحداثيات الطرفين نحصل على نظام المعادلات

$$a + b + c = 0$$
$$b = 0$$
$$c = 0$$

وبحل هذا النظام نجد أن $a = b = c = 0$. إذن، S مُستقلة خطياً. ▲

مثال (٢,٣,٢)

أثبت أن $S = \{110\ ,\ 011\ ,\ 101\ ,\ 111\}$ مرتبطة خطياً في K^3.

الحل

نفرض أن a، b، c، d أعداد قياسية حيث:

$$a(110) + b(011) + c(101) + d(111) = 000$$

بمقارنة إحداثيات الطرفين نحصل على نظام المعادلات:

$$a + c + d = 0$$
$$a + b + d = 0$$
$$b + c + d = 0$$

وبحل هذا النظام نجد أن $d = 0$ وأن $a = b = c$. وباختيار $a = b = c = 1$ نستنتج أن S مرتبطة خطياً. ▲

من حقائق الجبر الخطي أنه إذا كانت $S \neq \{0\}$ مجموعة من المتجهات فتوجد مجموعة جزئية S' من S مُستقلة خطياً حيث تحتوي S' أي مجموعة جزئية أخرى من S ومُستقلة خطياً (أي أن S' أكبر مجموعة جزئية من S مُستقلة خطياً). المثال التالي يبين كيفية إيجاد مثل هذه المجموعة S'.

مثال (٢,٣,٣)

بيّنا في المثال (**٢,٣,٢**) أن المجموعة $S = \{110, 011, 101, 111\}$ مرتبطة خطياً حيث وجدنا:

$$1(110) + 1(011) + 1(101) + 0(111) = 000$$

وبهذا نستطيع كتابة 101 كتركيب خطي لكلمات S الأخرى:

$$101 = 1(110) + 1(011) + 0(111)$$

إذا اعتبرنا أن ترتيب كلمات S هو الترتيب المعطى فنرى أن 101 هي أول كلمة يمكن كتابتها كتركيب خطي لكلمات S السابقة لها وهي 110، 011. بحذف هذه الكلمة من S نحصل على مجموعة جديدة $S' = \{110, 011, 111\}$. إذا كانت S' مُستقلة خطياً نتوقف وتكون S' هي المجموعة الجزئية المستقلة خطياً من S المنشودة. أما إذا كانت S'

مرتبطة خطياً فنقوم بحذف أول كلمة يمكن كتابتها كترتيب خطي للكلمات السابقة لها لنحصل على مجموعة جديدة S''. وهكذا إلى أن نحصل على مجموعة مُستقلة خطياً. وعند ذلك تكون هذه أكبر مجموعة جزئية من S مُستقلة خطياً. هذه المجموعة في مثالنا هذا هي S'. ▲

تمرين

(**٢,٣,٤**) بيّن أي من المجموعات التالية مُستقلة خطياً. وإذا كانت المجموعة مرتبطة خطياً فجد أكبر مجموعة جزئية من S مُستقلة خطياً.

(أ) $S = \{1101, 1110, 1011\}$

(ب) $S = \{101, 011, 110, 010\}$

(ج) $S = \{1101, 0111, 1100, 0011\}$

(د) $S = \{1000, 0100, 0010, 0001\}$

(هـ) $S = \{1000, 1100, 1110, 1111\}$

(و) $S = \{1100, 1010, 1001, 0101\}$

(ز) $S = \{0110, 1010, 1100, 0011, 1111\}$

(ح) $S = \{111000, 000111, 101010, 010101\}$

(ط) $S = \{00000000, 10101010, 01010101, 11111111\}$.

لاحظ أن المجموعة S في التمرين (**٢,٣,٤**) (ط) مرتبطة خطياً ولاحظ أيضاً أنها تحتوي الكلمة الصفرية. في الحقيقة أي مجموعة من المتجهات التي تحتوي المتجه الصفري هي مرتبطة خطياً.

نقول عن مجموعة جزئية غير خالية B من فضاء متجهات V إنها **أساس (Basis)** للفضاء V إذا حققت الشرطين التاليين:

(١) B تولّد V (أي أن $\langle B\rangle = V$).

(٢) B مُستقلة خطياً.

لاحظ أن أي مجموعة مُستقلة خطياً B هي أساس للفضاء $\langle B\rangle$. وبما أن أي مجموعة S من المتجهات المرتبطة خطياً وغير الصفرية تحتوي على أكبر مجموعة جزئية مُستقلة خطياً B، فنستطيع أن نحصل على أساس B كمجموعة جزئية من S للفضاء $\langle S\rangle$. إذا كانت $S = \{0\}$ فنقول في هذه الحالة أن أساس S هو المجموعة الخالية $\emptyset$.

مثال (٢,٣,٥)

وجدنا في المثال (**٢,٣,١**) أن المجموعة $S = \{1001, 1101, 1011\}$ مُستقلة خطياً. وبهذا تكون S أساساً للشفرة $C = \langle S\rangle = \{0000, 1001, 1101, 1011, 0100, 0010, 1111, 0110\}$ التي هي فضاء جزئي من K^4. ▲

مثال (٢,٣,٦)

وجدنا في المثال (**٢,٣,٢**) أن المجموعة $S = \{110, 011, 101, 111\}$ مُرتبطة خطياً. وفي المثال (**٢,٣,٣**) وجدنا أن $B = S' = \{110, 011, 111\}$ هي أكبر مجموعة جزئية مُستقلة خطياً من S. وبهذا تكون B أساساً للشفرة $C = \langle S\rangle$. ▲

في المثالين السابقين بيّنا كيفية إيجاد أساس للشفرة $C = \langle S\rangle$ المولدة بمجموعة جزئية غير خالية S من K^n. لإيجاد أساس للفضاء الثنوي $C^\perp$ نقوم بإيجاد أكبر مجموعة جزئية مُستقلة خطياً من $C^\perp$ بالطريقة المبينة في المثال (**٢,٣,٣**).

تمرين

(**٢,٣,٧**) جد أساساً B للشفرة $C = \langle S\rangle$ لكل مجموعة من المجموعات المبينة في التمرين (**٢,٢,٣**) ثم جد أساساً $B^\perp$ للشفرة الثنوية $C^\perp$.

وجدنا في المثال (**٢,٣,٦**) أن المجموعة الجزئية $B = \{110, 011, 111\}$ هي أكبر مجموعة جزئية مُستقلة خطياً من المجموعة $S = \{110, 011, 101, 111\}$. المجموعة B هذه ليست وحيدة فالمجموعة $B_1 = \{110, 101, 111\}$ هي أيضاً أكبر مجموعة جزئية مُستقلة خطياً من S ومن ثم فهي أيضاً أساس للشفرة $C = \langle S\rangle$.

في العموم يكون لفضاء متجهات V عدد كبير من الأساسات ولكن جميع هذه الأساسات تحتوي على العدد نفسه من العناصر. يُسمى هذا العدد **بُعد فضاء المتجهات (Dimension of the Vector Space)** ويُرمز له بالرمز $dimV$. بُعد الفضاء K^n يساوي n ؛ لأن جميع الكلمات ذوات الطول n والوزن 1 أساس للفضاء K^n. ومن جهة أخرى أساس الفضاء الصفري {0} هو ∅ ومن ثم فبُعده 0.

تمرين

(**٢,٣,٨**) جد بُعد كل من الشفرات $C = \langle S \rangle$ والشفرات الثنوية $C^{\perp}$ المقدمة في التمرين (**٢,٢,٣**) (انظر أيضاً التمرين (**٢,٢,٧**)).

يُزودنا أساس الشفرة الخطية بطريقة فعالة لوصف الشفرة؛ لأنه إذا كان $\{v_1, v_2, \cdots, v_k\}$ أساساً لأي فضاء متجهات V وكان $w \in V$ فيمكن كتابة w بطريقة وحيدة كتركيب خطي لعناصر الأساس $v_1, v_2, \cdots, v_k$. أي يمكن إيجاد أعداد قياسية وحيدة $a_1, a_2, \cdots, a_k$ بحيث يكون $w = a_1v_1 + a_2v_2 + \cdots + a_kv_k$.

مثال (٢,٣,٩)

أكتب $w = 011$ كتركيب خطي وحيد لكلمات الأساس $\{110, 001, 100\}$ للفضاء K^3.

الحل

سنجد أعداداً قياسياً a ، b ، c بحيث يكون:

$$a(110) + b(001) + c(100) = 011$$

وبمقارنة طرفي المعادلة نحصل على النظام:

$$a + c = 0$$
$$a = 1$$
$$b = 1$$

وبهذا نرى أن $a = b = c = 1$ ويكون:

$$011 = 1(110) + 1(001) + 1(100).$$ ▲

تمرين

(**٢,٣,١٠**) اكتب كلاً من كلمات K^4 التالية كتركيب خطي وحيد لكلمات الأساس $\{1000, 1100, 1110, 1111\}$.

(أ) 0011 (ب) 1010 (ج) 0111

(د) 0001 (هـ) 0000

وحقيقة أخرى مهمة عن فضاءات المتجهات هي أن أي مجموعة جزئية مُستقلة خطياً من فضاء متجهات تكون محتواة في أساس لهذا الفضاء. والمثال التالي يبيّن لنا كيفية إنجاز ذلك.

مثال (٢,٣,١١)

المجموعة الجزئية $S = \{110, 001\}$ مُستقلة خطياً في الفضاء K^3. سنقوم بتوسيع S إلى أساس للفضاء K^3 على النحو التالي: نضيف أولاً أساساً معلوماً للفضاء K^3 وليكن $\{100, 010, 001\}$ إلى المجموعة S وبهذا نحصل على مجموعة جديدة هي $S_1 = \{110, 001, 100, 010, 001\}$. الآن نستخدم الطريقة المتبعة في المثال (**٢,٣,٣**) لإيجاد أساس للفضاء K^3 كمجموعة جزئية من S_1. ويكون هو الأساس المنشود. ▲

تمرين

(**٢,٣,١٢**) (أ) عيّن أساساً للفضاء K^4 يحتوي المجموعة $\{1111, 1001\}$.

(ب) وسّع المجموعة $\{010101, 101010\}$ إلى أساس للفضاء K^6.

مبرهنة (٢,٣,١٣)

عدد كلمات شفرة خطية بُعدها k يساوي 2^k.

البرهان

إذا كانت C شفرة خطية بُعدها k وكان $\{v_1, v_2, \cdots, v_k\}$ أساساً للشفرة C فمن الممكن كتابة أي كلمة $w \in C$ على الصورة:

$$w = a_1v_1 + a_2v_2 + \cdots + a_kv_k$$

حيث $a_1, a_2, \cdots, a_k$ أعداد وحيدة في K. وبما أن $a_i = 0$ أو $a_i = 1$ لكل $i = 1,2, \cdots, k$ فيوجد 2^k من الخيارات المختلفة للأعداد $a_1, a_2, \cdots, a_k$ وبهذا نرى أن عدد كلمات C يساوي 2^k. ■

ويمكن برهان المبرهنة التالية باستخدام حقائق بدائية من نظرية أنظمة المعادلات الخطية.

مبرهنة (٢,٣,١٤)

لتكن $C = \langle S \rangle$ شفرة خطية مولّدة بالمجموعة الجزئية S من K^n. عندئذ:

$$dim C + dim C^{\perp} = n$$

تمارين

(٢,٣,١٥) تحقق من صواب المبرهنة **(٢,٣,١٤)** باستخدام إجابات التمرين **(٢,٣,٨)**.

(٢,٣,١٦) افرض أن S مجموعة جزئية من K^7 وأن $C = \langle S \rangle$ وافرض أن بُعد $C^{\perp}$ يساوي 3.

(أ) جد بُعد $C = \langle S \rangle$.

(ب) جد عدد كلمات C.

(٢,٣,١٧) افرض أن S مجموعة جزئية من K^8 وافرض أن $\{11110000, 00001111, 10000001\}$ أساس للشفرة الثنوية $C^{\perp}$. جد عدد كلمات $C = \langle S \rangle$.

(٢,٣,١٨) المبرهنة **(٢,٣,١٤)** صحيحة أيضاً للفضاء $\mathbb{R}^n$ حيث كل متجه ينتمي إلى $\mathbb{R}^n$ يكتب بطريقة وحيدة كمجموع متجهين أحدهما ينتمي إلى $\langle S \rangle$ والآخر ينتمي إلى $S^{\perp}$ حيث $\langle S \rangle \cap S^{\perp} = \{0\}$. (فمثلاً في $\mathbb{R}^3$، خذ $\langle S \rangle$ المستوى xy و $S^{\perp}$ محور z). استخدم $S = \{000, 101\}$ لإثبات عدم صواب ذلك في الفضاء K^n.

النتيجة الأخيرة في هذا البند تتعلق بعدد الأساسات المختلفة للشفرة الخطية حيث إن عدد أساسات أي فضاء جزئي من $\mathbb{R}^n$ هو عدد غير منته ولكن هذا العدد منته للفضاءات الجزئية من K^n وهذا ما تزودنا به المبرهنة التالية.

مبرهنة (٢,٣,١٩)

إذا كان بُعد الشفرة الخطية يساوي k فإن عدد أساساتها المختلفة يساوي:

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i) \quad .$$

مثال (٢,٣,٢٠)

بُعد الشفرة الخطية K^4 يساوي 4. وبهذا نجد أن عدد أساسات K^4 المختلفة يساوي:

$$\frac{1}{4!}\prod_{i=0}^{3}(2^4 - 2^i) = \frac{1}{4!}(2^4 - 1)(2^4 - 2)(2^4 - 2^2)(2^4 - 2^3) = 840$$

لاحظ أن أي فضاء جزئي من K^n حيث $n \geq 4$ وحيث بُعده يساوي 4 يكون عدد أساساته المختلفة يساوي 840. ▲

تمارين

(٢,٣,٢١) ليكن b_n عدد أساسات K^n المختلفة. تحقق من صواب أعداد الجدول التالي:

n	1	2	3	4	5	6
b_n	1	3	28	840	83328	27998208

(٢,٣,٢٢) جد جميع أساسات كل من K^2 و K^3.

(٢,٣,٢٣) جد عدد الأساسات المختلفة لكل من الشفرات $C = \langle S \rangle$ حيث:

(أ) $S = \{001\,,011\,,111\}$

(ب) $S = \{1010\,,0101\,,1111\}$

(ج) $S = \{0101\,,1010\,,1100\}$

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

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

(و) $S = \{10101\,, 01010\,, 11111\,, 00011\,, 10110\}$.

(٢,٤) المصفوفات

Matrices

المصفوفة من الدرجة $m \times n$ هي مستطيل من الأعداد القياسية عدد **صفوفه (Rows)** يساوي m وعدد **أعمدته (Columns)** يساوي n. سنفترض أن القارئ على دراية بجبر المصفوفات على الأعداد الحقيقية. سنراجع في هذا البند المفاهيم البدائية من نظرية المصفوفات التي نحتاجها لدراسة نظرية التشفير.

إذا كانت A مصفوفة من الدرجة $m \times n$ وكانت B مصفوفة من الدرجة $n \times p$ فإن حاصل الضرب AB هو مصفوفة من الدرجة $m \times p$ حيث عنصرها في الموقع ij (أي في الصف i والعمود j) هو الضرب القياسي للصف i من المصفوفة A مع العمود j من المصفوفة B. على سبيل المثال:

$$\begin{bmatrix}1011\\0101\end{bmatrix}\begin{bmatrix}101\\011\\101\\100\end{bmatrix} = \begin{bmatrix}100\\111\end{bmatrix}$$

لاحظ أن عدد أعمدة المصفوفة الأولى (التي على اليسار) يجب أن يساوي عدد صفوف المصفوفة الثانية (التي على اليمين) لكي يكون الضرب معرفاً.

تمرين

(٢,٤,١) جد حاصل ضرب كل زوج من المصفوفات التالية كلما أمكن ذلك.

$$A = \begin{bmatrix}11011\\00101\\11011\end{bmatrix}, B = \begin{bmatrix}0101\\1001\\1100\end{bmatrix}, C = \begin{bmatrix}110110\\011011\\101101\\101011\end{bmatrix}, D = \begin{bmatrix}1111\\0101\\1010\\1101\end{bmatrix}$$

تبقى القواعد الجبرية المعتادة للمصفوفات على الأعداد الحقيقية صحيحة على المجموعة K. **المصفوفة الصفرية (Zero Matrix)** من الدرجة $m \times n$ هي مصفوفة من الدرجة $m \times n$ جميع عناصرها أصفار. المصفوفة المربعة I من الدرجة $n \times n$ التي تكون عناصر قطرها الرئيس $(i = j)$ تساوي 1 والعناصر الأخرى تساوي 0 هي **المصفوفة المحايدة (Identity Matrix)** من الدرجة $n \times n$ وتحقق $AI = A$ و $IA = A$.

التمارين الثلاثة التالية تتناول ثلاث قواعد جبرية غير محققة للمصفوفات على K.

تمارين

(**٢,٤,٢**) جد مصفوفتين A و B من الدرجة 2×2 على K بحيث يكون $AB \neq BA$.

(**٢,٤,٣**) جد مصفوفتين A و B غير صفريتين من الدرجة 2×2 على K بحيث يكون $AB = 0$.

(**٢,٤,٤**) جد ثلاث مصفوفات A و B و C من الدرجة 2×2 على K بحيث يكون $AB = AC$ ولكن $B \neq C$.

يوجد نوعان من **العمليات الصفية الأولية (Elementary Row Operations)** التي تُجرى على مصفوفات معرفة على K هما:

(١) تبديل صفين.

(٢) استبدال صف بحاصل جمعه مع صف آخر.

نقول إن مصفوفتين **متكافئتين صفياً (Row Equivalent)** إذا استطعنا الحصول على إحداهما من الأخرى بإجراء متتالية منتهية من العمليات الصفية الأولية. ونقول إن العدد 1 في مصفوفة M على K هو **عنصر متقدم (Leading Element)** إذا لم يكن هناك 1 على يساره في الصف الواقع فيه. كما يُسمى عمود من M **عموداً متقدماً (Leading Column)** إذا احتوى على 1 متقدم. ونقول إن مصفوفة M هي على **صيغة درجية صفية (Row Echelon Form)** أو اختصاراً على صيغة REF إذا كانت جميع

صفوف M الصفرية (إن وجدت) واقعة أسفل المصفوفة وكان كل عنصر 1 متقدم يقع على يمين العنصر 1 المتقدم في الصفوف الأعلى. وأخيراً نقول إن مصفوفة M على **صيغة درجية صفية مختزلة (Reduced Row Echelon Form)** أو اختصاراً على صيغة RREF إذا كانت على صيغة REF وكل من أعمدتها المتقدمة يحتوي على العدد 1 في صف واحد فقط وجميع الأعداد الأخرى في ذلك العمود أصفاراً.

من الممكن وضع أي مصفوفة معرفة على K على صيغة REF أو RREF بإجراء متتالية منتهية من العمليات الصفية الأولية. وبهذا نرى أن أي مصفوفة تكافئ صفياً مصفوفة على صيغة REF أو RREF. الصيغة RREF لمصفوفة ما وحيدة ولكن من الممكن أن يكون لها العديد من صيغ REF.

مثال (٢,٤,٥)

عيّن صيغة RREF للمصفوفة M المبينة بإجراء عمليات صفية أولية.

الحل

$$M=\begin{bmatrix}1011\\1010\\1101\end{bmatrix}\rightarrow\begin{bmatrix}1011\\0001\\0110\end{bmatrix}$$ (اضافة الصف ١ إلى الصفين ٢ و ٣)

$$\rightarrow\begin{bmatrix}1011\\0110\\0001\end{bmatrix}$$ (تبديل الصفين 2 و 3)

$$\rightarrow\begin{bmatrix}1010\\0110\\0001\end{bmatrix}$$ (إضافة الصف ٣ إلى الصف 1) ▲

تمرين

(٢,٤,٦) جد صيغة RREF لكل من المصفوفات الأربع المقدمة في التمرين (٢,٤,١).

منقول مصفوفة (Transpose of a Matrix) A من الدرجة $m \times n$ هي مصفوفة A^T من الدرجة $n \times m$ حيث العمود i من A هو الصف i من A^T. فمثلاً، منقول $A = \begin{bmatrix}1011\\0000\\0111\end{bmatrix}$ هو $A^T = \begin{bmatrix}100\\001\\101\\100\end{bmatrix}$. سنحتاج إلى الحقيقتين التاليتين عن منقول المصفوفات:

$$(A^T)^T = A \quad \text{و} \quad (AB)^T = B^T A^T.$$

(٢,٥) أساسات لكل من $C = \langle S \rangle$ و $C^\perp$

Bases for $C = \langle S \rangle$ & $C^\perp$

نقدم في هذا البند خوارزميات لإيجاد أساسات للشفرة الخطية وثنويتها وستساعدنا هذه الخوارزميات كثيراً في دراسة الشفرات الخطية.

لنفرض أن S مجموعة جزئية غير خالية من K^n. الخوارزميتان التاليتان تقدمان لنا أساساً للشفرة الخطية $C = \langle S \rangle$ المولّدة بالمجموعة S.

خوارزمية (٢,٥,١) [إيجاد أساس للشفرة C]

لتكن المصفوفة A هي المصفوفة التي صفوفها كلمات S. جد REF (أو RREF) للمصفوفة A بإجراء عمليات صفية أولية. عندئذ، الصفوف غير الصفرية في الصيغة REF هي أساس للشفرة $C = \langle S \rangle$.

لتبرير صواب الخوارزمية لاحظ أن صفوف A تولّد C وأن العمليات الصفية الأولية إما أنها تبدل كلمات أو تقوم باحلال كلمة (صف) مكان كلمة أخرى تنتمي إلى C ونتيجة لذلك نحصل على مجموعة جديدة من كلمات الشفرة التي لا زالت تولّد C. ومن الواضح أيضاً أن الصفوف غير الصفرية من صيغة REF مُستقلة خطياً.

مثال (٢,٥,٢)

عيّن أساساً للشفرة الخطية $C = \langle S \rangle$ حيث $S = \{11101, 10110, 01011, 11010\}$.

الحل

بوضع كلمات S كصفوف المصفوفة A وإيجاد صيغة REF نحصل على:

$$A=\begin{bmatrix}11101\\10110\\01011\\11010\end{bmatrix}\rightarrow\begin{bmatrix}11101\\01011\\01011\\00111\end{bmatrix}\rightarrow\begin{bmatrix}11101\\01011\\00111\\00000\end{bmatrix}$$

وبهذا نرى استناداً إلى الخوارزمية (**٢,٥,١**) أن $\{11101\,,01011\,,00111\}$ أساس للشفرة الخطية $C=\langle S\rangle$. وصيغة REF أخرى للمصفوفة A هي:

$$\begin{bmatrix}11101\\01101\\00111\\00000\end{bmatrix}$$

ويكون $\{11101\,,01101\,,00111\}$ أساساً آخر للشفرة الخطية $C=\langle S\rangle$. ▲

ملحوظة

لاحظ أن الأساس الذي نحصل عليه من الخوارزمية (**٢,٥,١**) ليس وحيداً كما هو موضح في المثال (**٢,٥,٢**). كما أن الأساس ليس بالضرورة أن يكون مجموعة جزئية من S.

تمرين

(**٢,٥,٣**) استخدم الخوارزمية (**٢,٥,١**) لإيجاد أساس للشفرة الخطية $C=\langle S\rangle$ لكل من المجموعات S التالية.

(أ) $S=\{010\,,011\,,111\}$

(ب) $S=\{1010\,,0101\,,1111\}$

(ج) $S=\{0101\,,1010\,,1100\}$

(د) $S=\{1000\,,0100\,,0010\,,0001\}$

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

(و) $S=\{10101\,,01010\,,11111\,,00011\,,10110\}$

(ز) $S = \{0110\,, 1010\,, 1100\,, 0011\,, 1111\}$

(ح) $S = \{111000\,, 000111\,, 101010\,, 010101\}$

(ط) $S = \{00000000\,, 10101010\,, 01010101, 11111111\}$.

خوارزمية (٢,٥,٤) [إيجاد أساس للشفرة C]

ضع كلمات S كأعمدة لمصفوفة A. استخدم العمليات الصفية الأولية على المصفوفة A لإيجاد صيغة REF (أو RREF). عيّن الأعمدة المتقدمة في صيغة REF. عندئذ، أعمدة المصفوفة A التي تقابل الأعمدة في صيغة REF هي أساس للشفرة الخطية $C = \langle S \rangle$.

من حقائق الجبر الخطي أنه إذا كانت أعمدة مصفوفة A مُستقلة خطياً فإن أعمدة المصفوفة التي نحصل عليها بعد إجراء عدد من العمليات الصفية الأولية على A، تكون أيضاً مُستقلة خطياً. ومن السهل إثبات أن الأعمدة المتقدمة لمصفوفة على صيغة REF مُستقلة خطياً.

مثال (٢,٥,٥)

استخدم الخوارزمية **(٢,٥,٤)** لإيجاد أساس للشفرة الخطية $C = \langle S \rangle$ حيث S هي كما في المثال **(٢,٥,٢)**.

الحل

بوضع كلمات S كأعمدة لمصفوفة A وإجراء عمليات صفية أولية لإيجاد صيغة REF نحصل على:

$$A = \begin{bmatrix} 1101 \\ 1011 \\ 1100 \\ 0111 \\ 1010 \end{bmatrix} \rightarrow \begin{bmatrix} 1101 \\ 0110 \\ 0001 \\ 0111 \\ 0111 \end{bmatrix} \rightarrow \begin{bmatrix} 1101 \\ 0110 \\ 0001 \\ 0000 \\ 0000 \end{bmatrix}$$

الأعمدة المتقدمة في صيغة REF هي 1، 2، 4 وبهذا تكون كلمات الأعمدة 1، 2، 4 من المصفوفة A وهي $\{11010\,, 10110\,, 11101\}$ أساساً للشفرة الخطية $C = \langle S \rangle$. ▲

ملحوظة

لاحظ أن الأساس الذي نحصل عليه من الخوارزمية (**٢,٥,٤**) للشفرة $C = \langle S \rangle$ هو مجموعة جزئية من المجموعة S.

تمرين

(**٢,٥,٦**) استخدم الخوارزمية (**٢,٥,٤**) لإيجاد أساس للشفرة $C = \langle S \rangle$ لكل مجموعة S من مجموعات التمرين (**٢,٥,٣**) ثم قارن إجاباتك.

الخوارزمية التالية تُزودنا بأساس للشفرة الثنوية $C^{\perp}$ والتي سنستخدمها في العديد من المواقع في هذا الكتاب. تقدم لنا هذه الخوارزمية أيضاً أساساً للشفرة C؛ لأن الخوارزمية (**٢,٥,١**) هي جزء منها.

خوارزمية (٢,٥,٧) [إيجاد أساس للشفرة $C^{\perp}$]

(١) ضع كلمات S كصفوف مصفوفة A.

(٢) استخدم العمليات الصفية الأولية لإيجاد صيغة RREF للمصفوفة A.

(٣) افرض أن G هي المصفوفة من الدرجة $k \times n$ المكوّنة من صفوف RREF غير الصفرية.

(٤) افرض أن X هي المصفوفة من الدرجة $k \times (n-k)$ التي نحصل عليها من G بحذف أعمدة G المتقدمة.

(٥) افرض أن H هي المصفوفة من الدرجة $n \times (n-k)$ التي نحصل عليها كالتالي:

(أ) صفوف H المقابلة لأعمدة G المتقدمة هي صفوف X (مع المحافظة على الترتيب نفسه). عدد هذه الصفوف يساوي k.

(ب) ضع في بقية صفوف H (وعددها $n-k$) المصفوفة المحايدة I من الدرجة $(n-k) \times (n-k)$ (مع المحافظة على الترتيب نفسه).

(٦) أعمدة H هي أساس للشفرة $C^{\perp}$.

لاحظ أن أعمدة H (عددها $n-k$) مُستقلة خطياً وأن:

$$dimC^{\perp} = n - dimC = n - k$$

كما أن $GH = X + X = 0$ (بعد القيام بالتبديل اللازم لأعمدة G وصفوف H). وهذا يبرر صحة الخوارزمية.

الوصف التالي للخوارزمية (**٢,٥,٧**) يساعد على تذكرها. لاحظ أن عدد أعمدة G المتقدمة يساوي k. بتبديل أعمدة G بحيث تصبح أعمدتها المتقدمة في البداية وبهذا تكون بقية أعمدتها هي المصفوفة X. نعيد الآن تسمية المصفوفة G ونسميها G'. أي أن $G' = [I_k|X]$.

بهذا نرى أن خطوات الخوارزمية (**٢,٥,٧**) تأخذ المسار التالي: $(I_k|X)$

(١) $A \to \begin{bmatrix} G \\ 0 \end{bmatrix}$ (RREF).

(٢) $G' = [I_k|X]$ (بعد تبديل أعمدة G).

(٣) $H' = \begin{bmatrix} X \\ I_{n-k} \end{bmatrix}$.

(٤) H هي المصفوفة التي نحصل عليها من H' بتبديل صفوف H' (هذا التبديل هو عكس التبديل الذي استخدمناه لتبديل أعمدة G).

مثال (٢,٥,٨)

استخدم الخوارزمية (**٢,٥,٧**) لإيجاد أساس للشفرة الثنوية $C^{\perp}$ حيث S هي كما في المثال (**٢,٥,٢**).

الحل

$$A = \begin{bmatrix} 11101 \\ 10110 \\ 01011 \\ 11010 \end{bmatrix} \to \begin{bmatrix} 11101 \\ 01011 \\ 00111 \\ 00000 \end{bmatrix} \to \begin{bmatrix} 11010 \\ 01011 \\ 00111 \\ 00000 \end{bmatrix} \to \begin{bmatrix} 10001 \\ 01011 \\ 00111 \\ 00000 \end{bmatrix}$$

وهذه هي صيغة RREF للمصفوفة A. عندئذ:

$$k = 3 \text{ ، } X = \begin{bmatrix} 01 \\ 11 \\ 11 \end{bmatrix} \text{ ، } G = \left[\begin{array}{c|c} 100 & 01 \\ 010 & 11 \\ 001 & 11 \end{array}\right].$$

أعمدة G المتقدمة هي 1، 2، 3 ومن ثم تكون X هي الصفوف 1، 2، 3 على التوالي من المصفوفة H ذات الدرجة $(3-5)\times 5$. أما بقية صفوف H فهي المصفوفة المحايدة من الدرجة 2×2. وبهذا نحصل على:

$$H=\begin{bmatrix}01\\11\\11\\10\\01\end{bmatrix}$$

وتكون أعمدة H هي الأساس المنشود للشفرة $C^{\perp}$. لاحظ أيضاً أن صفوف G هي أساس للشفرة $C=\langle S\rangle$، وذلك استناداً إلى الخوارزمية (**٢,٥,١**). ▲

مثال (٢,٥,٩)

لنفرض أن $n=10$ وأن S مجموعة جزئية من K^{10} وأن صيغة RREF للمصفوفة A التي نحصل عليها من الخوارزمية (**٢,٥,٧**) تحتوي على الصفوف غير الصفرية التالية (صفوف G):

$$G=\begin{bmatrix}1010010101\\0001010001\\0000100100\\0000001001\\0000000011\end{bmatrix}$$

أعمدة G المتقدمة هي الأعمدة 1، 4، 5، 7، 9، وبعد تبديل أعمدة G لتصبح الأعمدة المتقدمة في البداية نحصل على الترتيب 10، 8، 6، 3، 2، 9، 7، 5، 4، 1. وبهذا نرى أن:

$$.G'=\left[\begin{array}{c|c}10000&01111\\01000&00101\\00100&00010\\00010&00001\\00001&00001\end{array}\right]$$

نكوّن الآن المصفوفة H' ونقوم بتبديل صفوفها لنحصل على المصفوفة H:

$$H=\begin{bmatrix}01111\\10000\\01000\\00101\\00010\\00100\\00001\\00010\\00001\\00001\end{bmatrix}\begin{matrix}1\\2\\3\\4\\5\\6\\7\\8\\9\\10\end{matrix}\quad,\quad H'=\begin{bmatrix}X\\I\end{bmatrix}=\begin{bmatrix}01111\\00101\\00010\\00001\\00001\\10000\\01000\\00100\\00010\\00001\end{bmatrix}\begin{matrix}1\\4\\5\\7\\9\\2\\3\\6\\8\\10\end{matrix}$$

وأخيراً تكون أعمدة H أساساً للشفرة $C^{\perp}$ وذلك استناداً إلى الخوارزمية (**٢,٥,٧**). ▲

تمارين

(**٢,٥,١٠**) استخدم الخوارزمية (**٢,٥,٧**) لإيجاد أساس للشفرة $C^{\perp}$ لكل من الشفرات $C=\langle S\rangle$ للمجموعات S التالية:

(أ) $S=\{010\,,011\,,111\}$

(ب) $S=\{1010\,,0101\,,1111\}$

(ج) $S=\{0101\,,1010\,,1100\}$

(د) $S=\{1000\,,0100\,,0010\,,0001\}$

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

(و) $S=\{10101\,,01010\,,11111\,,00011\,,10110\}$

(ز) $S=\{0110\,,1010\,,1100\,,0011\,,1111\}$

(ح) $S=\{111000\,,000111\,,101010\,,010101\}$

(ط) $S=\{00000000\,,10101010\,,01010101\,,11111111\}$.

(**٢,٥,١١**) استخدم ترميز الخوارزمية (**٢,٥,٧**) لتفسير صواب المعادلة $GH=0$.

(**٢,٥,١٢**) لكل من المجموعات S التالية، عيّن أساساً B للشفرة $G=\langle S\rangle$ وأساساً $B^{\perp}$ للشفرة الثنوية $C^{\perp}$ مستخدماً الخوارزمية (**٢,٥,٧**):

(أ) $S = \{000000, 111000, 000111, 111111\}$

(ب) $S = \{1101000, 0110100, 0011010, 0001101, 1000110, 0100011, 1010001\}$

(ج) $S = \{1111000, 0111100, 0011110, 0001111, 1000111, 1100011, 1110001\}$

(د) $S = \{101101110, 011011101, 110110010, 011011110, 111111101\}$

(هـ) $S = \{100100100, 010010010, 111111111, 000000000\}$

(و) $S = \{001101, 001000, 001111, 000101, 000001\}$

(٢,٦) المصفوفات المولّدة والتشفير
Generating Matrices & Encoding

نوظّف الآن المفاهيم التي درسناها في البنود القليلة السابقة لإيجاد مصفوفة مهمة للشفرات الخطية ونبين كيفية استخدام هذه المصفوفة لإرسال الرسائل.

نحتاج أولاً إلى بعض المفاهيم الأولية. تُعرف **رتبة مصفوفة A (Rank of a Matrix A)** على K ونرمز لها بالرمز $\boldsymbol{rank\, A}$ على أنها عدد الصفوف غير الصفرية في صيغة REF للمصفوفة. **بُعد الشفرة (Dimension of the Code)** C هو بُعد C كفضاء جزئي من K^n. إذا كان طول الشفرة C يساوي n وبُعدها يساوي k ومسافتها تساوي d فنقول **إنها شفرة خطية من النوع (n,k,d) ((n,k,d)-Linear Code)**. هذه الأعداد الثلاثة، الطول والبُعد والمسافة هي المعلومات الأهم التي يجب معرفتها عن الشفرة C. إذا كانت C شفرة خطية طولها n وبُعدها k فنعني **بمصفوفة مولّدة (Generation Matrix)** للشفرة C، أي مصفوفة G، صفوفها أساس للشفرة C. لاحظ أن درجة مصفوفة مولّدة G للشفرة C هي $k \times n$ وأن رتبتها تساوي k. وبهذا نحصل على المبرهنة التالية:

مبرهنة (٢,٦,١)

تكون مصفوفة G مصفوفة مولّدة لشفرة خطية C إذا وفقط إذا كانت صفوف G مُستقلة خطياً. أي أن رتبة G تساوي عدد صفوف G. ■

وبما أن للمصفوفات المتكافئة صفياً الرتبة نفسها فإننا نحصل على المبرهنة التالية:

مبرهنة (٢,٦,٢)

إذا كانت G مصفوفة مولّدة للشفرة الخطية C فإن أي مصفوفة مكافئة صفياً للمصفوفة G هي أيضاً مصفوفة مولّدة للشفرة C. على وجه الخصوص، لأي شفرة خطية C يكون لها مصفوفة مولّدة على صيغة RREF. ■

لإيجاد مصفوفة مولّدة لشفرة خطية C نضع كلماتها كصفوف لمصفوفة A. وبما أن $C = \langle C \rangle$، نستخدم الخوارزمية (٢,٥,١) أو الخوارزمية (٢,٥,٧) لإيجاد أساس للشفرة C. عندئذ، تكون المصفوفة التي صفوفها كلمات الأساس هي مصفوفة مولّدة للشفرة C.

مثال (٢,٦,٣)

عيّن مصفوفة مولّدة للشفرة الخطية $C = \{0000, 1110, 0111, 1001\}$.

الحل

بإنشاء المصفوفة A التي صفوفها كلمات C واستخدام الخوارزمية (٢,٥,١) نحصل على:

$$A = \begin{bmatrix} 0000 \\ 1110 \\ 0111 \\ 1001 \end{bmatrix} \rightarrow \begin{bmatrix} 1110 \\ 0111 \\ 1001 \\ 0000 \end{bmatrix} \rightarrow \begin{bmatrix} 1110 \\ 0111 \\ 0111 \\ 0000 \end{bmatrix} \rightarrow \begin{bmatrix} 1110 \\ 0111 \\ 0000 \\ 0000 \end{bmatrix}$$

وبهذا نرى أن $G = \begin{bmatrix} 1110 \\ 0111 \end{bmatrix}$ مصفوفة مولّدة للشفرة C. أما إذا استخدمنا الخوارزمية (٢,٥,٧) فنجد أن صيغة RREF للمصفوفة A هي $\begin{bmatrix} 1001 \\ 0111 \\ 0000 \\ 0000 \end{bmatrix}$ وتكون $G_1 = \begin{bmatrix} 1001 \\ 0111 \end{bmatrix}$ مصفوفة مولّدة أخرى للشفرة C.

تمارين

(**٢,٦,٤**) بيّن أي من المصفوفتين التاليتين هي مصفوفة مولّدة لشفرة خطية.

$$A = \begin{bmatrix} 010011101 \\ 100101101 \\ 101100110 \\ 101101101 \end{bmatrix} \quad ، \quad B = \begin{bmatrix} 1001101001 \\ 1101000101 \\ 1000010111 \\ 1010001110 \end{bmatrix}.$$

(**٢,٦,٥**) عيّن مصفوفة مولّدة على صيغة RREF لكل من الشفرات التالية:

(أ) $C = \{000\,, 001\,, 010\,, 011\}$

(ب) $C = \{0000\,, 1001\,, 0110\,, 1111\}$

(ج) $C = \{00000\,, 11111\}$

(د) $C = \{00000\,, 11100\,, 11100\,, 00111\,, 11011\}$

(هـ) $C = \{00000\,, 11110\,, 01111\,, 10001\}$

(و) $C = \{00000\,, 101010\,, 010101\,, 111111\}$

(**٢,٦,٦**) عيّن مصفوفة مولّدة لكل من الشفرات التالية ثم جد بُعد الشفرة:

(أ) $C = \{000000\,, 001011\,, 010101\,, 011110\,, 100110\,, 101101\,, 110011\,, 111000\}$

(ب) $C = \{00000000\,, 01101111\,, 11011000\,, 11111101\,, 10010010\,, 0100101\,, 01001010\,, 101101111\}$

(ج) $C = \{0000000000\,, 1111100000\,, 0000011111, 1111111111\}$

(**٢,٦,٧**) عيّن مصفوفة مولّدة لكل من الشفرات الخطية المولّدة بالمجموعة المبينة. جد (n, k, d) لكل من هذه الشفرات:

(أ) $S = \{11111111\,, 11110000\,, 11001100\,, 10101010\}$

(ب) $S = \{11111100\,, 11110011\,, 11001111\,, 00111111\}$

(ج) $S = \{100100100\,, 010010010\,, 001001001\,, 11111111\}$

(د) $S = \{10101\,, 01010\,, 11111\,, 00011\,, 10110\}$

(هـ) $S = \{1010\,, 0101\,, 1111\}$

(و) $S = \{101101\,, 011010\,, 110111\,, 000111\,, 110000\}$

(ز) $S = \{1001011\,, 0101010\,, 1001100\,, 0011001\,, 0000111\}$.

المبرهنة التالية تبين لنا كيفية استخدام المصفوفة المولّدة للشفرة الخطية في تشفير الرسائل.

مبرهنة (٢,٦,٨)

لنفرض أن G مصفوفة مولّدة للشفرة الخطية C ذات الطول n والبعد k. عندئذ، C هي مجموعة جميع الكلمات التي على الصورة uG حيث $u \in K^k$. أي أن $C = \{uG : u \in K^k\}$. إضافة إلى ذلك لكل $u_1, u_2 \in K^k$ نجد أن $u_1G = u_2G$ إذا وفقط إذا كان $u_1 = u_2$.

البرهان

لنفرض أن $G = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix}$ حيث $g_1, g_2, \cdots, g_k$ هي صفوف المصفوفة المولّدة G. ولنفرض أن $v \in C$. بما أن $g_1, g_2, \cdots, g_k$ أساس للشفرة الخطية C فتوجد أعداد $a_1, a_2, \cdots, a_k \in K$ بحيث يكون:

$$v = a_1g_1 + a_2g_2 + \cdots + a_kg_k.$$

وبوضع $u = (a_1, a_2, \cdots, a_k)$ نرى أن $uG = a_1g_1 + a_2g_2 + \cdots + a_kg_k$.

إذن، $v = uG$ حيث $u \in K^k$ ومن ناحية أخرى، إذا كان $u = (a_1, a_2, \cdots, a_k) \in K^k$ فنرى أن $uG = a_1g_1 + a_2g_2 + \cdots + a_kg_k \in C$. إذن، $C = \{uG: u \in K^k\}$.

وأخيراً، إذا كان $u_1, u_2 \in K^k$ حيث $u_1 = u_2$ فمن الواضح أن $u_1G = u_2G$. وبالعكس، لنفرض أن $u_1 = (a_1, a_2, \cdots, a_k)$ وأن $u_2 = (b_1, b_2, \cdots, b_k)$ كلمتان في K^k حيث $u_1G = u_2G$. حينئذ يكون:

$$u_1G = u_2G \Rightarrow a_1g_1 + a_2g_2 + \cdots + a_kg_k = b_1g_1 + b_2g_2 + \cdots + b_kg_k$$

$$\Rightarrow (a_1 - b_1)g_1 + (a_2 - b_2)g_2 + \cdots + (a_k - b_k)g_k = 0$$

وبما أن $g_1, g_2, \cdots, g_k$ مُستقلة خطياً فنرى أن $a_i - b_i = 0$ لكل $i = 1,2,\cdots,k$. وبهذا يكون $u_1 = u_2$. ■

ملحوظة

لاحظ أن المبرهنة (**٢,٦,٨**) تنص على أن الرسائل التي يتم تشفيرها باستخدام شفرة خطية من النوع (n,k,d) هي بالضبط الرسائل $u \in K^k$ حيث يتم تشفير الرسالة u على أنها $v = uG$. وبهذا يستخدم فقط عدد k من إحداثيات أي كلمة شفرة لتشفير الرسالة. لاحظ أيضاً أن معدل المعلومات لشفرة خطية من النوع (n,k,d) هو $log_2(2^k)/n = k/n$.

مثال (٢,٦,٩)

لتكن C الشفرة الخطية من النوع $(5,3,d)$ حيث المصفوفة المولّدة لها هي $G = \begin{bmatrix}10110\\01011\\00101\end{bmatrix}$. عندئذ، معدل المعلومات للشفرة C هو $\frac{k}{n} = \frac{3}{5}$. وبهذا نرى أنه يمكن تشفير جميع الرسائل $u \in K^3$. فمثلاً، يتم تشفير الرسالة $u = 101$ على النحو $v = uG = [101]\begin{bmatrix}10110\\01011\\00101\end{bmatrix} = 10011$. ▲

تمارين

(**٢,٦,١٠**) لكل من المصفوفات المولّدة المعطاة شفِّر الرسائل المبينة:

(أ) $G = \begin{bmatrix}10011\\01010\\00101\end{bmatrix}$

(i) $u = 100$ (ii) $u = 010$ (iii) $u = 111$

(ب) $G = \begin{bmatrix} 1000111 \\ 0100101 \\ 0010011 \end{bmatrix}$

(i) $u = 100$ (ii) $u = 010$ (iii) $u = 111$

(ج) $G = \begin{bmatrix} 1101001 \\ 0010111 \\ 0101010 \\ 1111111 \end{bmatrix}$

(i) $u = 1000$ (ii) $u = 1010$ (iii) $u = 0011$

(iv) $u = 1011$.

(**٢,٦,١١**) لنفرض أن:

000	100	010	001	110	101	011	111
A	B	E	H	M	R	T	W

هو تقابل بين حروف الرسائل وكلمات K^3. استخدم المصفوفة المولّدة المبينة في المثال (**٢,٦,٩**) لتشفير الرسالة BE THERE (تجاهل الفراغ).

(**٢,٦,١٢**) لتكن C شفرة مصفوفتها المولّدة هي:

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

وليكن

0000	1000	0100	0010	0001	1100	1010	1001
A	B	C	D	E	F	G	H
0110	0101	0011	1110	1101	1011	0111	1111
I	J	K	L	M	N	O	P

تقابلاً بين حروف الرسائل وكلمات K^4.

(أ) شفّر الرسالة HELP.

(ب) شفّر الرسالة HELP بافتراض وقوع الأخطاء التالية أثناء عملية الإرسال: خطأ في الإحداثي الأول من الكلمة الأولى، عدم وقوع أخطاء في الكلمة الثانية، خطأ

في الإحداثي السابع من الكلمة الثالثة، خطأ في الإحداثيين الخامس والسادس من الكلمة الرابعة.

(ج) شفّر الرسالة CALL HOME BAMA (تجاهل الفراغات).

(٢,٦,١٣) جد عدد الرسائل التي يمكن إرسالها ومعدل المعلومات r لكل من الشفرات الخطية في التمرينين **(٢,٦,٦)** و **(٢,٦,٧)**.

(٢,٧) مصفوفات اختبار النوعية

Parity-Check Matrices

نقدم الآن مصفوفة أخرى مرتبطة مع المصفوفة المولّدة للشفرات الخطية وسنوظفها في تصميم خطط فك التشفير. نقول إن مصفوفة H هي **مصفوفة اختبار (أو تحديد) النوعية (Parity-Check Matrix)** للشفرة الخطية C إذا كانت أعمدة H أساساً للشفرة الثنوية $C^{\perp}$.

إذا كانت C من الطول n والبعد k فنرى أن H من الدرجة $n \times (n-k)$ ورتبتها هي $n-k$ وذلك لأن $dimC + dimC^{\perp} = n$.

المبرهنة التالية هي رديف المبرهنة **(٢,٦,١)**.

مبرهنة (٢,٧,١)

تكون H مصفوفة اختبار النوعية لشفرة خطية C إذا وفقط إذا كانت أعمدة H مُستقلة خطياً.

البرهان[٢]

نحصل على البرهان بملاحظة أن درجة مصفوفة اختبار النوعية H لشفرة خطية من الطول n والبعد k هي $n \times (n-k)$ وأن رتبة H هي $n-k$. ■

---

(٢) المترجمان

المبرهنة التالية تصف لنا الشفرة الخطية بدلالة مصفوفة اختبار النوعية.

مبرهنة (٢,٧,٢)

إذا كانت H مصفوفة اختبار النوعية لشفرة خطية من الطول n فإن:

$$C = \{v \in K^n : vH = 0\}.$$

إذا كان لدينا مصفوفة مولّدة لشفرة خطية C فبإمكاننا إيجاد مصفوفة اختبار النوعية للشفرة C باستخدام الخوارزمية (**٢,٥,٧**) حيث إن هذه المصفوفة هي المصفوفة H المنشأة باستخدام الخوارزمية (**٢,٥,٧**)؛ لأن أعمدة H هي أساس للشفرة الثنوية $C^{\perp}$.

مثال (٢,٧,٣)

وجدنا في المثال (**٢,٦,٣**) أن $G_1 = \begin{bmatrix} 10 & 01 \\ 01 & 11 \end{bmatrix} = [I \ X]$ هي مصفوفة مولّدة على صيغة RREF للشفرة $C = \{0000, 1110, 0111, 1001\}$ ولذا نجد استناداً إلى الخوارزمية (**٢,٥,٧**) أن:

$$H = \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} 01 \\ 11 \\ 10 \\ 01 \end{bmatrix}$$

هي مصفوفة اختبار النوعية للشفرة C. لاحظ أن $vH = 00$ لكل $v \in C$. ▲

تمارين

(**٢,٧,٤**) جد مصفوفة اختبار النوعية لكل من الشفرات التالية:

(أ) $C = \{000, 001, 010, 011\}$

(ب) $C = \{0000, 1001, 0110, 1111\}$

(ج) $C = \{00000, 11111\}$

(د) $C = \{00000, 11100, 11100, 00111, 11011\}$

(هـ) $C = \{00000, 11110, 01111, 10001\}$

(و) $C = \{00000, 101010, 010101, 111111\}$.

(**٢,٧,٥**) جد مصفوفة اختبار النوعية لكل من الشفرات التالية (المصفوفة المولّدة تم إيجادها في التمرينين (**٢,٦,٦**) و (**٢,٦,٧**)):

(أ) $C = \{000000, 001011, 010101, 011110, 100110, 101101, 110011, 111000\}$

(ب) $C = \{00000000, 01101111, 11011000, 11111101, 010010, 00100101, 01001010, 10110111\}$

(ج) $C = \{0000000000, 1111100000, 0000011111, 1111111111\}$

(د) $C = \langle S \rangle, S = \{11111111, 11110000, 11001100, 10101010\}$

(هـ) $C = \langle S \rangle, S = \{11111100, 11110011, 11001111, 00111111\}$

(و) $C = \langle S \rangle, S = \{100100100, 010010010, 001001001, 1111111111\}$

(ز) $C = \langle S \rangle, S = \{10101, 01010, 11111, 00011, 10110\}$

(ح) $C = \langle S \rangle, S = \{1010, 0101, 1111\}$

(ط) $C = \langle S \rangle, S = \{101101, 011010, 110111, 000111, 110000\}$

(ي) $C = \langle S \rangle, S = 1001011, 0101010, 1001100, 0011001, 0000111\}$

نقدم الآن العلاقة بين المصفوفة المولّدة ومصفوفة اختبار النوعية للشفرات الخطية ونقدم أيضاً العلاقة بين هذه المصفوفات لشفرة خطية وثنويتها.

مبرهنة (٢,٧,٦)

تكون G مصفوفة مولّدة و H مصفوفة اختبار النوعية لشفرة خطية C إذا وفقط إذا تحقق ما يلي:

(١) صفوف G مُستقلة خطياً.

(٢) أعمدة H مُستقلة خطياً.

(٣) عدد صفوف G مضافاً إليه عدد أعمدة H يساوي عدد أعمدة G وهذا بدوره يساوي عدد صفوف H.

(٤) $GH = 0$.

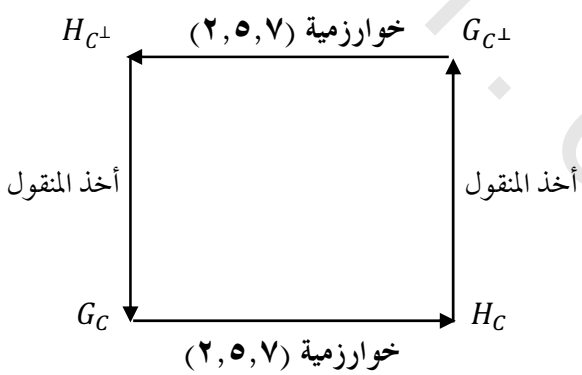
مبرهنة (٢,٧,٧)

تكون H مصفوفة اختبار النوعية لشفرة خطية C إذا وفقط إذا كانت H^T مصفوفة مولّدة للشفرة الثنوية $C^{\perp}$.

البرهان

نحصل على البرهان بتوظيف المبرهنة (**٢,٧,٦**) والحقيقة $H^T G^T = (GH)^T = 0$. ■

إذا كان لدينا مصفوفة مولّدة أو مصفوفة اختبار نوعية لشفرة C أو ثنويتها $C^{\perp}$ فيكون بإمكاننا توظيف الخوارزمية (**٢,٥,٧**) للحصول على الثلاث مصفوفات الأخرى، والمخطط التالي يوضح كيفية إنجاز ذلك



مثال (٢,٧,٨)

لتكن H مصفوفة اختبار النوعية للشفرة C حيث:

$$H = \begin{bmatrix} 11 \\ 11 \\ 01 \\ 10 \\ 01 \end{bmatrix} = \begin{bmatrix} X \\ I \end{bmatrix}$$

عندئذ،

(أ) $H^T = \begin{bmatrix} 11010 \\ 11101 \end{bmatrix}$ مصفوفة مولّدة للشفرة الثنوية $C^\perp$.

(ب) $\begin{bmatrix} 11010 \\ 00111 \end{bmatrix}$ صيغة RREF للمصفوفة H^T.

ونرى استناداً إلى الخوارزمية (٢,٥,٧) أن مصفوفة اختبار النوعية للشفرة $C^\perp$ هي:

$$\cdot \begin{bmatrix} 110 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

(ج) باستخدام H نجد مصفوفة مولّدة للشفرة C وهي:

$$G = \begin{bmatrix} 100 & 11 \\ 010 & 11 \\ 001 & 01 \end{bmatrix} = [I \quad X]$$

وذلك باستخدام خطوات عكسية للخوارزمية (٢,٥,٧). وبهذا تكون:

$$G^\top = \begin{bmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 111 \end{bmatrix}$$

مصفوفة اختبار النوعية للشفرة الثنوية $C^\perp$، وذلك استناداً للمبرهنة (٢,٧,٧). ▲

تمارين

(٢,٧,٩) مصفوفة اختبار النوعية H لشفرة خطية C معطاة في كل فرع من فروع التمرين. جد:

(١) مصفوفة مولّدة للشفرة الثنوية $C^\perp$.

(٢) مصفوفة مولّدة للشفرة C.

$$H=\begin{bmatrix}100\\100\\010\\001\\010\\001\end{bmatrix}$$ (أ) $$H=\begin{bmatrix}01\\10\\01\\10\\01\end{bmatrix}$$ (ب) $$H=\begin{bmatrix}111\\110\\101\\011\\100\\010\\001\end{bmatrix}$$ (ج).

٢,٧,١٠) جد جميع كلمات الشفرة الثنوية $C^{\perp}$ للشفرة $C=\{00000\,,11111\}$ ومن ثم عيّن مصفوفة مولّدة ومصفوفة اختبار النوعية للشفرة $C^{\perp}$.

٢,٧,١١) لكل من الشفرات C المبينة أدناه، جد بُعد C، بُعد $C^{\perp}$، درجة مصفوفة مولّدة ومصفوفة اختبار النوعية لكل من C و$C^{\perp}$، عدد كلمات كل من C و$C^{\perp}$، معدل المعلومات r لكل من C و$C^{\perp}$.

(أ) C من الطول $n=2^t-1$ وبُعد t.

(ب) C من الطول $n=23$ والبعد 11.

(ج) C من الطول $n=15$ والبعد 8.

(٢,٨) الشفرات المتكافئة
Equivalent Codes

لتكن $G=[I_k\ \ X]$ هي المصفوفة من الدرجة $k\times n$ ، $k<n$ حيث I_k المصفوفة المحايدة من الدرجة $k\times k$. من الواضح أن G على صيغة RREF وأن صفوفها مُستقلة خطياً. إذن، G مصفوفة مولّدة لشفرة خطية طولها n وبُعدها k. نقول إن G **مصفوفة مولّدة قياسية (Standard Generating Matrix).** كما تُسمى الشفرة الخطية C المولّدة بالمصفوفة G، **شفرة نظامية (Systematic Code).**

ليس بالضرورة أن يكون لجميع الشفرات الخطية مصفوفة مولّدة قياسية. على سبيل المثال، الشفرة الخطية المولّدة بالمصفوفة G في التمرين **(٢,٨,١)** التالي لها إضافة إلى G خمس مصفوفات مولّدة أخرى وجميعها ليست مصفوفات مولّدة قياسية.

تمرين

(**٢,٨,١**) جد المصفوفات المولّدة الخمس الأخرى للشفرة الخطية المولّدة بالمصفوفة:

$$.G = \begin{bmatrix} 100 \\ 001 \end{bmatrix}$$

تتمتع الشفرة الخطية C التي يكون لها مصفوفة مولّدة قياسية $G = [I \;\; X]$ بميزات خاصة. إحدى هذه الميزات هي استخدام الخوارزمية (**٢,٥,٧**) للحصول مباشرة على مصفوفة اختبار النوعية H للشفرة C حيث إن H في هذه الحالة هي:

$$.H = \begin{bmatrix} X \\ I \end{bmatrix}$$

ونعلم أيضاً استناداً إلى المبرهنة (**٢,٦,٨**) أنه يمكن كتابة أي كلمة v من كلمات الشفرة الخطية C ذات الطول n والبعد k على الصورة uG حيث u كلمة وحيدة من كلمات K^k و G مصفوفة مولّدة للشفرة C. يمكن التفكير في الكلمة u ذات الطول k على أنها الرسالة المرسلة ولكننا بدلاً من إرسال u فإننا بالطبع نقوم بإرسال كلمة الشفرة $v = uG$. وإذا استطاعت طريقة MLD الاستنتاج صواباً أن $v = uG$ هي الكلمة التي تم إرسالها فعندئذ، يكون من المهم على المستقبل استخدام uG للحصول على الرسالة الأصلية u. فإذا كانت G مصفوفة مولّدة قياسية فهذا يجعل الأمر بغاية السهولة وذلك لأن:

$$v = uG = u[I \;\; X] = [uI \;\; uX] = [u \;\; uX]$$

وتكون الرسالة الأصلية u هي أول k إحداثي من كلمة الشفرة $v = uG$ ونكون قد برهنا المبرهنة التالية التي تبين إحدى الميزات المهمة لوجود مصفوفة مولّدة قياسية.

مبرهنة (٢,٨,٢)

لتكن C شفرة خطية طولها n وبُعدها k ولتكن G مصفوفة مولّدة قياسية للشفرة C. عندئذ، أول k إحداثي من كلمة الشفرة $v = uG$ هي إحداثيات الكلمة $u \in K^k$. ■

مثال (٢,٨,٣)

إذا كانت:

$$G = \left[\begin{array}{c|c} 1000 & 101 \\ 0100 & 100 \\ 0010 & 110 \\ 0001 & 011 \end{array}\right] = [I_4 \;\; X]$$

وكانت الرسالة هي $u = 0111$ فإن $uG = 0111001 = [u001]$. وأما إذا كانت $u = 1011$ فنرى أن $uG = 1011000 = [u000]$. ▲

تمارين

(٢,٨,٤) لتكن G هي المصفوفة المولّدة المبينة في المثال **(٢,٨,٣)**. شفّر كلاً من الرسائل u التالية ثم تحقق من أن الإحداثيات الأربعة الأولى من كلمة الشفرة الناتجة هي الرسالة u.

(أ) $u = 1111$ (ب) $u = 1011$ (ج) $u = 0000$

(٢,٨,٥) بيّن كيفية استرداد u من uG إذا لم تكن G مصفوفة مولّدة قياسية.

(٢,٨,٦) إذا كانت المصفوفة المولّدة للشفرة C هي:

$$G = \begin{bmatrix} 1100101 \\ 0110101 \\ 1011011 \\ 1100110 \\ 0110000 \end{bmatrix}$$

فبيّن كيف يمكنك استرداد u من $v = uG = 0000101$.

عند توفر شروط المبرهنة **(٢,٨,٢)**، تسمى الإحداثيات k الأولى من كلمة الشفرة $v = uG$، **إحداثيات المعلومات (Information Digits)**؛ لأنها بالفعل هي الرسالة u، أما الإحداثيات $n - k$ الباقية فتسمى **الإحداثيات الزائدة أو إحداثيات اختبار النوعية (Redundancy or Parity-Check Digits)**.

مع كل هذه الميزات التي تتمتع بها شفرة خطية ذات مصفوفة مولّدة قياسية فما الذي يمكن عمله لو واجهنا شفرة خطية C ليس لها أي مصفوفة مولّدة قياسية؟ للإجابة عن هذا السؤال، دعنا نعتبر الشفرة C ذات المصفوفة المولّدة $G = \begin{bmatrix}100\\001\end{bmatrix}$ المبينة في التمرين (**٢,٨,١**). من السهل أن نرى أن C هي:

$$.C = \{000\,,100\,,001\,,101\}$$

وهذه شفرة خطية ليس لها مصفوفة مولّدة قياسية كما هو مبين في التمرين (**٢,٨,١**). لنفرض الآن أننا قمنا بإعادة ترتيب إحداثيات كل من كلمات C على النحو "الأول، الثالث، الثاني" عوضاً عن الترتيب الأصلي "الأول، الثاني، الثالث". عندئذ، نحصل على شفرة جديدة C' وهي:

$$.C' = \{000\,,100\,,010\,,110\}$$

على الرغم من أن الشفرتين C وC' مختلفتان، إلا أنهما تتشاركان في عديد من الخصائص، فمثلاً، كل منهما خطية وكل منهما من الطول 3 وبُعد كل منهما 2 ومسافة كل منهما 1. ولكن تتميز الشفرة C' عن الشفرة C بأن لها مصفوفة مولّدة قياسية G' نحصل عليها من المصفوفة G بتبديل العمودين الثاني والثالث (بالضبط كما حصلنا على C' من C). أي أن:

$$.G' = \begin{bmatrix}100\\101\end{bmatrix}$$

لتكن C شفرة قالبية من الطول n. إذا حصلنا على شفرة قالبية C' من الطول n من C بتبديل ما لإحداثيات كلمات C فعندئذ نقول إن الشفرة C' **تكافئ (Equivalent)** الشفرة C.

مثال (٢,٨,٧)

ليكن $n = 5$ ولتكن C هي الشفرة:

$$.C = \{11111\,,01111\,,00111\,,00011\,,00001\}$$

إذا استخدمنا الترتيب 3، 5، 4، 1، 2 لإحداثيات كلمات الشفرة C فنحصل على الشفرة C' المكافئة للشفرة C

$$C' = \{11111, 10111, 00111, 00110, 00010\}.$$

لاحظ أن الشفرتين غير خطيتين. ▲

مبرهنة (٢,٨,٨)

أي شفرة خطية C تكافئ شفرة خطية C' لها مصفوفة مولّدة قياسية.

البرهان

لنفرض أن G مصفوفة مولّدة للشفرة C. ضع G على صيغة RREF. أعد ترتيب أعمدة RREF بحيث تكون الأعمدة المتقدمة في البداية. عندئذ، المصفوفة الناتجة عن ذلك G' هي مصفوفة مولّدة قياسية لشفرة خطية C' تكافئ C. ■

مثال (٢,٨,٩)

المصفوفة:

$$G = \begin{bmatrix} 011000010 \\ 000100110 \\ 000010010 \\ 000001100 \\ 000000001 \end{bmatrix}$$

هي مصفوفة مولّدة على صيغة RREF وأعمدتها المتقدمة هي 9، 6، 5، 4، 2. وبإعادة ترتيب هذه الأعمدة لتأخذ الترتيب الجديد 8، 7، 3، 1، 9، 6، 5، 4، 2 نحصل على المصفوفة:

$$G' = \begin{bmatrix} 10000 & 0101 \\ 01000 & 0011 \\ 00100 & 0001 \\ 00010 & 0010 \\ 00001 & 0000 \end{bmatrix}$$

وهي مصفوفة مولّدة قياسية لشفرة خطية مكافئة للشفرة المولّدة بالمصفوفة G. ▲

تمارين

(**٢,٨,١٠**) جد شفرة نظامية C' مكافئة للشفرة C المعطاة. وتحقق من أن C وC' لهما الطول والبُعد نفسه والمسافة نفسها.

(أ) $C = \{00000, 10110, 10101, 00011\}$

(ب) $C = \{00000, 11100, 00111, 11011\}$.

(**٢,٨,١١**) جد مصفوفة مولّدة قياسية G' لشفرة مكافئة للشفرة التي لها المصفوفة المولّدة G المعطاة.

(أ) $$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(ب) $$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

(**٢,٨,١٢**) عيّن مصفوفة مولّدة قياسية G' لشفرة مكافئة للشفرة C التي لها مصفوفة اختبار النوعية المعطاة.

(أ) $$H = \begin{bmatrix} 110 \\ 100 \\ 010 \\ 110 \\ 101 \\ 001 \\ 011 \end{bmatrix}$$

(ب) $$H = \begin{bmatrix} 110 \\ 100 \\ 011 \\ 010 \\ 001 \end{bmatrix}.$$

(**٢,٨,١٣**) أثبت أن الشفرات المتكافئة لها الطول والبُعد نفسه والمسافة نفسها.

(**٢,٨,١٤**) بيّن فيما إذا كان كل زوج من المصفوفات G_1 و G_2 المعطاة يولّد شفرتين متكافئتين.

(أ) $$G_1 = \begin{bmatrix} 1100 \\ 0110 \\ 0011 \end{bmatrix} \quad \text{و} \quad G_2 = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}$$

(ب) $$G_1 = \begin{bmatrix} 110000 \\ 001100 \\ 000011 \end{bmatrix} \quad \text{و} \quad G_2 = \begin{bmatrix} 111111 \\ 011011 \\ 001001 \end{bmatrix}$$

(ج) $G_1 = \begin{bmatrix}1011000\\0101100\\0010110\\0001011\end{bmatrix}$ و $G_2 = \begin{bmatrix}1000111\\0100110\\0010101\\0001011\end{bmatrix}$.

(٢,٩) مسافة شفرة خطية
Distance of a Linear Code

بيَّنا سابقاً أن مسافة شفرة خطية هي أصغر أوزان كلمات الشفرة غير الصفرية. سنُبين في هذا البند كيفية توظيف مصفوفة اختبار النوعية لإيجاد مسافة شفرة خطية.

مبرهنة (٢,٩,١)

لنفرض أن H مصفوفة اختبار النوعية لشفرة خطية C. عندئذ، مسافة C تساوي d إذا وفقط إذا كانت كل مجموعة عدد كلماتها $d-1$ من صفوف H مُستقلة خطياً ويوجد على الأقل مجموعة واحدة تحتوي على d من صفوف H مرتبطة خطياً.

فكرة البرهان

الفكرة وراء تبرير صواب المبرهنة (٢,٩,١) هي أنه إذا كانت v كلمة فإن vH تركيب خطي لصفوف من H عددها بالضبط يساوي $wt(v)$. وعليه، إذا كانت $v \in C$ حيث $wt(v) = d$ فلا بُد من وجود عدد d من صفوف H المرتبطة خطياً؛ وذلك لأن $vH = 0$. كما أن $vH = 0$ يُبين أن وزن كلمة الشفرة v يحقق المتباينة $wt(v) \geq d$. ■

مثال (٢,٩,٢)

لتكن H مصفوفة اختبار النوعية للشفرة الخطية C:

$$H = \begin{bmatrix}110\\011\\100\\010\\001\end{bmatrix}.$$

بالتجريب نرى عدم وجود صفين من صفوف H مجموعهما يساوي 000 وبهذا يكون كل صفين من صفوف H مستقلين خطياً. ولكن مجموع الصفوف 4، 3، 1 يساوي 000 وبهذا فهي مرتبطة خطياً. إذن مسافة الشفرة C هي $d = 3$. ▲

تمارين

(**٢,٩,٣**) عيّن كلمات الشفرة C المقدمة في المثال (**٢,٩,٢**). احسب وزن كل من هذه الكلمات وتحقق من أن مسافة C هي $d = 3$.

(**٢,٩,٤**) احسب مسافة كل من الشفرات الخطية C التي لها مصفوفة اختبار النوعية المعطاة باستخدام المبرهنة (**٢,٩,١**) ثم تحقق من صواب إجابتك بإيجاد أوزان $wt(v)$ لكل $v \in C$.

(أ) $H = \begin{bmatrix} 0111 \\ 1110 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$ (ب) $H = \begin{bmatrix} 1110 \\ 1101 \\ 1011 \\ 0111 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$ (ج) $H = \begin{bmatrix} 0111 \\ 1110 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$.

(**٢,٩,٥**) استخدم المبرهنة (**٢,٩,١**) لإيجاد مسافة الشفرة الخطية ذات المصفوفة المولّدة التالية:

(أ) $G = \begin{bmatrix} 111000000 \\ 000111000 \\ 111111111 \end{bmatrix}$ (ب) $G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}$.

(٢,١٠) المجموعات المشاركة

Cosets

نقدم في هذا البند مفهوماً سنوظفه في البند القادم لفك تشفير الشفرات الخطية. لتكن C شفرة خطية من الطول n ولتكن u كلمة طولها n (أي $u \in K^n$). نعرّف **المجموعة المشاركة (Coset)** للشفرة C التي تعينها الكلمة u على أنها مجموعة جميع الكلمات $v + u$ حيث $v \in C$. أي أن:

$$C + u = \{v + u : v \in C\}.$$

مثال (٢,١٠,١)

إذا كانت $C = \{000\,,111\}$ وكانت $u_1 = 101$ ، $u_2 = 111$ ، $u_3 = 010$ فنجد أن:

$$C + u_1 = C + 101 = \{000 + 101\,,111 + 101\} = \{101\,,010\}$$

$$C + u_2 = C + 111 = \{000 + 111\,,111 + 111\} = \{111\,,000\}$$

$$C + u_3 = C + 010 = \{000 + 010\,,111 + 010\}$$

$$= \{010\,,101\} = C + u_1$$

▲

تمرين

(٢,١٠,٢) جد المجموعات المشاركة الأخرى للشفرة $C = \{000\,,111\}$. لاحظ أن عدد المجموعات المشاركة الممكنة للشفرة C يساوي ثمانية (مجموعة مشاركة لكل كلمة من كلمات K^3) ولكن عدد المجموعات المشاركة المختلفة يساوي أربعة فقط.

لتكن C شفرة خطية من الطول n. قد يتبادر إلى ذهن القارئ أن عدد المجموعات المشاركة المختلفة $C + u$ يساوي 2^n. أي مجموعة مشاركة لكل $u \in K^n$. ولكن كما هو مبين في المثال (٢,١٠,١) والتمرين (٢,١٠,٢) فهذا ليس صحيحاً. إذ إنه من الممكن أن تكون $u_1, u_2 \in K^n$ حيث $u_1 \neq u_2$ ولكن $C + u_1 = C + u_2$.

المبرهنة التالية تقدم عديداً من الحقائق المهمة عن المجموعات المشاركة ودراسة الأمثلة التي تلي نص المبرهنة تساعد القارئ على فهم هذه الحقائق. يحتاج برهان هذه الحقائق إلى معرفة بعض تقنيات نظرية المجموعات ولذا نتركها كتمارين للقارئ.

مبرهنة (٢,١٠,٣)

لتكن C شفرة خطية من الطول n ولتكن $u, v \in K^n$. عندئذ:

(١) إذا كانت $u \in C + v$ فإن $C + u = C + v$. أي أن كل كلمة من كلمات المجموعة المشاركة تحدد تماماً المجموعة المشاركة.

(٢) $u \in C + u$.

(٣) إذا كان $u + v \in C$ فإن $C + u = C + v$.

(٤) إذا كان $u + v \notin C$ فإن $C + u \neq C + v$.

(٥) كل كلمة من كلمات K^n محتواة في مجموعة مشاركة وحيدة للشفرة C.

أي أن:

$$C + u = C + v \text{ أو } (C + u) \cap (C + v) = \emptyset.$$

(٦) $|C + u| = |C|$ لكل $u \in K^n$. أي أن عدد كلمات أي مجموعة مشاركة للشفرة C يساوي عدد كلمات الشفرة C نفسها.

(٧) إذا كان بُعد الشفرة C يساوي k فإن عدد المجموعات المشاركة المختلفة للشفرة C يساوي 2^{n-k} وعدد كلمات أي مجموعة مشاركة يساوي 2^k.

(٨) الشفرة C هي إحدى مجموعاتها المشاركة. في الحقيقة، $C = C + 0$.

مثال (٢,١٠,٤)

في هذا المثال نجد المجموعات المشاركة للشفرة:

$$C = \{0000\,, 1011\,, 0101\,, 1110\}.$$

بداية، C نفسها مجموعة مشاركة (**خاصية ٨**) وكل كلمة من كلمات C تحدد المجموعة المشاركة C (**الخاصتان ١ و ٥**)، ولذا نختار $u \in K^4$ حيث $u \notin C$ (ولغرض فك التشفير لاحقاً نختار u بحيث يكون وزنها أصغر ما يمكن) ولتكن $u = 1000$. عندئذ، نحصل على المجموعة المشاركة التالية بجمع u إلى كل من كلمات C:

$$C + 1000 = \{1000\,, 0011\,, 1101\,, 0110\}.$$

لاحظ أن $u = 1000 \in C + u = C + 1000$.

الآن، نقوم باختيار كلمة أخرى من كلمات K^4 وزنها أصغر ما يمكن ولا تنتمي إلى C أو إلى $C + 1000$ ولتكن 0100. وبهذا نجد مجموعة مشاركة جديدة:

$$C + 0100 = \{0100, 1111, 0001, 1010\}.$$

وباختيار 0010 نجد المجموعة المشاركة:

$$C + 0010 = \{0010, 1001, 0111, 1100\}.$$

نتوقف الآن؛ لأننا نكون قد وجدنا جميع المجموعات المشاركة المختلفة؛ وذلك لأن بُعد C هو $k = 2$. ومن ثم عدد المجموعات المشاركة المختلفة يساوي $2^{n-k} = 2^{4-2} = 2^2 = 4$ و اتحادها يساوي K^4.

لاحظ أيضاً أن $0001 + 1010 = 1011 \in C$. ونرى أن 0001 و 1010 تنتميان للمجموعة المشاركة نفسها، بالتحديد المجموعة المشاركة $C + 0100$ (**خاصية ٣**). ومن جهة أخرى، $0100 + 0010 = 0110 \notin C$ وبهذا فكل من الكلمتين 0100 و 0010 تنتمي إلى مجموعة مشاركة مختلفة (**خاصية ٤**). ▲

مثال (٢,١٠,٥)

جد جميع المجموعات المشاركة للشفرة الخطية C التي لها المصفوفة المولّدة:

$$G = \begin{bmatrix} 100110 \\ 010011 \\ 001111 \end{bmatrix}.$$

الحل

بإيجاد جميع المجاميع المختلفة لصفوف G نجد أن:

$$C = \{000000, 100110, 010011, 001111, 110101, 101001, 011100, 111010\}$$

المجموعات المشاركة المختلفة هي:

000000	100000	010000	001000
100110	000110	110110	101110
010011	110011	000011	011011
001111	101111	011111	000111
110101	010101	100101	111101
101001	001001	111001	100001
011100	111100	001100	010100
111010	011010	101010	110010

000100	000010	000001	000101
100010	100100	100111	100011
010111	010001	010011	010110
001011	001101	001110	001010
110001	110111	110100	110000
101101	101011	101000	101100
011000	011110	011101	011001
111110	111000	111000	111111

لاحظ أن عدد المجموعات المشاركة المختلفة يساوي 8 وأن المجموعة الأول هي C. الكلمة u التي استخدمت لإيجاد المجموعة المشاركة $C+u$ هي الكلمة العليا في كل من المجموعات المشاركة. ▲

تمارين

(**٢,١٠,٦**) جد جميع المجموعات المشاركة لكل من الشفرات الخطية التالية:

(أ) $C = \{0000, 1001, 0101, 1100\}$

(ب) $C = \{0000, 1010, 1101, 0111\}$

(ج) $C = \{00000, 10100, 01011, 11111\}$

(د) $C = \{0000\}$.

(**٢,١٠,٧**) جد جميع المجموعات المشاركة لكل من الشفرات الخطية التالية التي لها المصفوفة المولّدة المعطاة.

(أ) $G = \begin{bmatrix} 111000 \\ 001110 \\ 100011 \end{bmatrix}$ (ب) $G = \begin{bmatrix} 101010 \\ 010101 \end{bmatrix}$

(ج) $G = \begin{bmatrix} 1000111 \\ 0100110 \\ 0010101 \\ 0001011 \end{bmatrix}$ (د) $G = \begin{bmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{bmatrix}$

(هـ) $G = \begin{bmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$ (و) $G = [1111]$.

(٢,١٠,٨) جد جميع المجموعات المشاركة لكل من الشفرات الخطية التالية التي لها مصفوفة اختبار النوعية المعطاة.

(أ) $H = \begin{bmatrix} 10 \\ 11 \\ 10 \\ 01 \end{bmatrix}$ (ب) $H = \begin{bmatrix} 111 \\ 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$ (ج) $H = \begin{bmatrix} 100 \\ 010 \\ 010 \\ 001 \\ 001 \\ 001 \end{bmatrix}$.

(٢,١٠,٩) برهن جميع فقرات المبرهنة **(٢,١٠,٣)**.

(٢,١١) MLD للشفرات الخطية

MLD for Linear Codes

أحد أهدافنا هو تصميم شفرات تتميز بسهولة وسرعة فك تشفير الكلمات المستقبلة. والشفرات الخطية تقدم لنا طريقة أكثر فاعلية لتنفيذ MLD من استخدام جدول IMLD. ولهذا الغرض، نقدم هنا طريقة لتنفيذ CMLD أو IMLD للشفرات الخطية حيث تؤدي المجموعات المشاركة ومصفوفة اختبار النوعية دوراً أساسياً في عملية فك التشفير.

لتكن C شفرة خطية ولنفرض أن كلمة الشفرة $v \in C$ قد تم إرسالها واستقبلت الكلمة w. ولنفرض أنه قد تم وقوع نمط الخطأ $u = v + w$ أثناء عملية الإرسال والاستقبال. عندئذ، يكون $w + u = v \in C$. وبهذا نرى أن نمط الخطأ u والكلمة

المستقبلة w ينتميان إلى المجموعة المشاركة نفسها للشفرة C (انظر **الخاصية ٣** من المبرهنة **(٢,١٠,٣)**).

بما أن أنماط الأخطاء المرجح وقوعها هي ذات أوزان صغيرة فإليك طريقة تنفيذ MLD لشفرة خطية C:

عند استقبالنا للكلمة w نقوم باختيار كلمة u وزنها أصغر ما يمكن في المجموعة المشاركة $C + w$ ونستنتج أن $v = w + u$ هي الكلمة المرسلة.

مثال (٢,١١,١)

لتكن $C = \{0000, 1011, 0101, 1110\}$. وجدنا في المثال **(٢,١٠,٤)** مجموعات C المشاركة وهي:

0000	1000	0100	0010
1011	0011	1111	1000
0101	1101	0001	0111
1110	0110	1010	1100

لنفرض الآن أننا استقبلنا الكلمة $w = 1101$. المجموعة المشاركة $C + w = C + 1101$ التي تحتوي w هي المجموعة الثانية في القائمة السابقة. والكلمة u ذات الوزن الأصغر في المجموعة المشاركة هذه هي $u = 1000$ (هي الكلمة التي نختارها كنمط خطأ). عندئذ، نستنتج أن $v = w + u = 1101 + 1000 = 0101$ هي على الأرجح كلمة الشفرة التي أرسلت. لنفرض الآن أن $w = 1111$ هي الكلمة المستقبلة. عندئذ، توجد في المجموعة المشاركة $C + w$ التي تحتوي 1111 كلمتان وزنهما أصغر ما يمكن هما 0101 و 0001. فإذا كانت طريقة فك التشفير هي CMLD، نقوم باختيار أي من هاتين الكلمتين ولتكن $u = 0100$ كنمط خطأ وبهذا نستنتج أن $v = w + u = 1111 + 0100 = 1011$ هي على الأرجح كلمة الشفرة التي قد تم إرسالها. ▲

تمرين

(**٢,١١,٢**) لتكن C الشفرة المبينة في المثال (**٢,١٠,٥**). استخدم طريقة CMLD لفك التشفير كل من الكلمات المستقبلة التالية:

(أ) 000011 (ب) 001001 (ج) 001101

(د) 010110 (هـ) 110101 (و) 001010

الجزء الأصعب في الطريقة الموصوفة أعلاه هو البحث عن المجموعة المشاركة التي تحتوي الكلمة المستقبلة w ومن ثم إيجاد الكلمة ذات الوزن الأصغر في المجموعة المشاركة هذه. ومن الممكن توظيف مصفوفة اختبار النوعية لإيجاد طريقة تسهل علينا هذه المهمة.

لتكن C شفرة خطية من الطول n والبعد k. ولتكن H مصفوفة اختبار النوعية للشفرة C. لكل $w \in K^n$ نعرّف **تناذر w (Syndrome of w)** على أنه الكلمة $wH \in K^{n-k}$.

مثال (٢,١١,٣)

المصفوفة H التالية هي مصفوفة اختبار النوعية للشفرة C المقدمة في المثال (**٢,١١,١**). فإذا كانت $w = 1101$ فنرى أن تناذر w هو:

$$wH = 1101\begin{bmatrix}11\\01\\10\\01\end{bmatrix} = 11.$$

لاحظ أن الكلمة ذات الوزن الأصغر في المجموعة المشاركة $C + w$ هي $u = 1000$ (انظر المثال (**٢,١١,١**)) وبهذا نرى أن تناذر u هو:

$$uH = 1000\begin{bmatrix}11\\01\\10\\01\end{bmatrix} = 11 = wH.$$

إضافة إلى ذلك، إذا كانت $w = 1101$ هي الكلمة المستقبلة فتستنتج طريقة CMLD أن:

$$v = w + u = 1101 + 1000 = 0101$$

هي كلمة الشفرة المرسلة ومن ثم نرى وقوع خطأ في الإحداثي الأول. لاحظ أيضاً أن لنمط الخطأ u يكون التناذر uH هو صف H (الصف الأول في هذه الحالة) المقابل لموقع الإحداثي الذي على الأرجح قد يكون وقع خطأ فيه. ▲

المبرهنة التالية تحتوي على بعض الحقائق الأساسية المهمة للتناذر. ويمكن برهان هذه الحقائق باستخدام تعريف المفاهيم المبينة وخصائص المجموعات المشاركة المقدمة في المبرهنة (**٢,١٠,٣**).

مبرهنة (٢,١١,٤)

لتكن C شفرة خطية من الطول n ولتكن H مصفوفة اختبار النوعية للشفرة C. إذا كانت $w, u \in K^n$ فإن:

(١) $wH = 0$ إذا وفقط إذا كانت $w \in C$.

(٢) $wH = uH$ إذا وفقط إذا كانت u وw تنتميان إلى المجموعة المشاركة نفسها للشفرة C.

(٣) إذا كان u نمط خطأ في الكلمة المستقبلة w فإن uH هو مجموع صفوف H المقابلة لمواقع وقوع الأخطاء أثناء الإرسال. ■

لاحظ أنه في حالة عدم وقوع أخطاء أثناء عملية الإرسال وإذا كانت w هي الكلمة المستقبلة فإن $wH = 0$. ولكن العكس ليس بالضرورة صحيحاً، أي من الممكن أن يكون $wH = 0$ على الرغم من وقوع أخطاء وذلك لأن كلمة الشفرة w ليس بالضرورة أن تكون هي كلمة الشفرة المرسلة.

بما أن الكلمات التي تنتمي للمجموعة المشاركة نفسها يكون لها التناذر نفسه وأن الكلمات التي تنتمي إلى مجموعات مشاركة مختلفة يكون تناذرها مختلفاً فنستطيع تحديد مجموعة مشاركة بمعرفة تناذرها حيث نعرِّف **تناذر المجموعة المشاركة (Syndrome of a Coset)** على أنه تناذر أي كلمة من كلماتها. وبهذا نرى أنه إذا كان طول الشفرة يساوي n وبُعدها يساوي k فكل كلمة طولها $n-k$ من الكلمات التي عددها 2^{n-k} يجب أن تكون تناذراً لمجموعة مشاركة واحدة فقط من المجموعات المشاركة جميعاً والتي عددها 2^{n-k}.

مثال (٢,١١,٥)

طول الشفرة C المقدمة في المثال (**٢,١١,١**) هو $n=4$ وبُعدها هو $k=2$. مجموعات C المشاركة (مبينة في المثال (**٢,١١,١**)) تحتوي على جميع الكلمات من الطول $n=4$ وعددها $2^n=2^4=16$. وعدد الكلمات ذات الطول $n-k=2$ يساوي $2^{n-k}=2^{4-2}=2^2=4$. وكل من هذه الكلمات هي تناذر لمجموعة مشاركة واحدة فقط من المجموعات المشاركة للشفرة C وعددها $2^{n-k}=4$. ▲

لحساب تناذُر مجموعة مُشاركة نقوم باختيار كلمة w في المجموعة المشاركة وعندئذ يكون تناذُرها هو wH. ولتنفيذ طريقة MLD نحتاج إلى كلمة في المجموعة المشاركة وزنها أصغر ما يمكن لاستخدامها كنمط خطأ. في الأمثلة التي تناولناها في البند السابق حرصنا على ترتيب عناصر المجموعات المشاركة لكي تكون الكلمة ذات الوزن الأصغر في الأعلى (أول كلمة من كلمات المجموعة المشاركة). تسمى أي كلمة ذات وزن أصغر في مجموعة مشاركة، **طليعة المجموعة المشاركة (Coset Leader)**. وإذا كان هناك أكثر من طليعة واحدة في مجموعة مشاركة فنختار أي واحدة منها عند تنفيذ CMLD.

مثال (٢,١١,٦)

لنفرض أن C هي الشفرة المقدمة في المثال (**٢,١١,١**). لحساب تناذر المجموعات المشاركة نقوم باختيار طليعة كل من المجموعات المشاركة ومن ثم نقوم بحساب التناذر كما هو مبين في الجدول التالي:

طليعة المجموعة المشاركة u	التناذر uH
0000	00
1000	11
0100	01
0010	10

لاحظ مرة أخرى أن كل كلمة من الطول 2 ظهرت مرة واحدة فقط كتناذر. ▲

يُسمى الجدول المبين في المثال (**٢,١١,٦**) الذي يقابل بين طلائع المجموعات المشاركة وتناذراتها، **صفيف فك التشفير القياسي (Standard Decoding Array)** أو اختصاراً SDA. لإنشاء الجدول SDA نقوم أولاً بإيجاد المجموعات المشاركة للشفرة ومن ثم نختار طليعة u لكل منها (وهي كلمة ذات وزن أصغر في المجموعة المشاركة). بعد ذلك نجد مصفوفة اختبار النوعية H للشفرة ومن ثم نقوم بحساب uH لكل طليعة u. وطريقة أسرع لإنشاء SDA تكون باستخدام مصفوفة اختبار النوعية H لحساب المسافة d للشفرة C وتوليد جميع أنماط الأخطاء e التي تحقق $wt(e) \leq \lfloor (d-1)/2 \rfloor$ ومن ثم حساب التناذر $s = eH$ لكل منها.

مثال (٢,١١,٧)

لإنشاء جدول SDA للشفرة C المقدمة في المثال (**٢,١٠,٥**) حيث المجموعات المشاركة مبينة في المثال المذكور. لاحظ أولاً أن لكل من المجموعات المشاركة السبع الأولى كلمة طليعية واحدة فقط وهي أول كلمة في المجموعة المشاركة، أما بالنسبة للمجموعات المشاركة الأخيرة فلها ثلاث كلمات طليعية هي 000101، 001010، 110000، وزن

كل منها يساوي 2. إذا أردنا استخدام طريقة CMLD فنختار أي منها ولتكن 000101 كطليعة (نمط الخطأ المفترض) للمجموعة المشاركة. أما إذا استخدمنا طريقة IMLD فنقوم بطلب إعادة إرسال ونضع علامة * في جدول SDA ليدل على ذلك. نجد الآن مصفوفة اختبار النوعية H للشفرة C:

$$.H = \begin{bmatrix} 110 \\ 011 \\ 111 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

وبافتراض استخدام طريقة CMLD يكون جدول SDA للشفرة C هو:

التناذر uH	نمط الخطأ
000	000000
110	100000
001	010000
111	001000
100	000100
010	000010
001	000001
101	000101

لاحظ أن التناذرات هي جميع كلمات K^3. طليعة المجموعة المشاركة C هي الكلمة الصفرية دائماً ويكون تنادُرها الكلمة الصفرية. تناذر الكلمة $u = 000101$ التي اخترناها كطليعة للمجموعة المشاركة الأخيرة هو $uH = 101$ وهذا مجموع الصفين 4 و 6 من المصفوفة H ويمثلان مواقع الإحداثي 1 في نمط الخطأ u. لو استخدمنا طريقة IMLD فنضع علامة * في هذا المكان. ▲

تمارين

(٢,١١,٨) أنشئ جدول SDA بافتراض استخدام IMLD لكل من شفرات التمرين **(٢,١٠,٦)**.

(**٢,١١,٩**) أنشئ جدول SDA بافتراض استخدام IMLD لكل من شفرات التمرين (**٢,١٠,٧**).

(**٢,١١,١٠**) أنشئ جدول SDA بافتراض استخدام IMLD لكل من شفرات التمرين (**٢,١٠,٨**).

(**٢,١١,١١**) برهن المبرهنة (**٢,١١,٤**).

بعد هذا الجهد المبذول لإنشاء جدول SDA نستطيع الآن استخدامه لفك التشفير بطريقة MLD ويتم ذلك على النحو التالي:

عند استقبالنا لكلمة w نقوم بحساب تناذُرها wH وبعد ذلك نبحث في جدول SDA لإيجاد طليعة المجموعة المشاركة u بحيث يكون $wH = uH$. وبهذا نستنتج أن كلمة الشفرة التي على الأرجح تكون قد أرسلت هي $v = w + u$.

مثال (٢,١١,١٢)

لتكن C الشفرة المبينة في المثال (**٢,١١,١**). جدول SDA أنشأناه في المثال (**٢,١١,٦**) ووجدنا مصفوفة اختبار النوعية H في المثال (**٢,١١,٣**). لنفرض أن $w = 1101$ كلمة مستقبلة. عندئذ، تناذر w هو $wH = 11$. وبالنظر إلى جدول SDA نجد أن الكلمة الطليعية u التي تحقق $wH = uH$ هي $u = 1000$ التي تقع في الصف الثاني من جدول SDA. وبهذا نستنتج أن $v = w + u = 0101$ هي كلمة الشفرة المرسلة. أما إذا كانت $w = 1111$ هي الكلمة المستقبلة فنرى أن $wH = 01 = uH$ حيث $u = 0100$ هي الكلمة الواقعة في الصف الثالث من جدول SDA. إذن، يكون فك تشفير w هو $v = w + u = 1011$. هذه النتائج تتفق مع ما وجدناه في المثال (**٢,١١,١**). ▲

لاحظ أن كلمة الشفرة $v = 0101$ هي فك تشفير الكلمة المستقبلة $w = 1101$ (في المثال السابق). وبحساب المسافات بين $w = 1101$ وكلمات الشفرة C نجد أن:

$$d(0000\,,1101) = 3 \quad , \quad d(0101\,,1101) = 1$$
$$d(1011\,,1101) = 2 \quad , \quad d(1110\,,1101) = 2$$

وبهذا نرى أن $v = 0101$ هي بالفعل أقرب كلمة شفرة إلى w.

أما في حالة الكلمة المستقبلة $w = 1111$ فكان فك تشفيرها هو $v = 1011$. وبحساب المسافات بين w وكلمات الشفرة C نجد أن:

$$d(0000, 1111) = 4 \quad , \quad d(0101, 1111) = 2$$
$$d(1011, 1111) = 1 \quad , \quad d(1110, 1111) = 1$$

من ذلك نرى وجود كلمتي شفرة هما الأقرب إلى $w = 1111$. وهذا ليس بالشيء المفاجئ؛ لأن الكلمة الطليعية في المجموعة المشاركة التي تحتوي w لم تكن وحيدة. وبما أننا نستخدم طريقة CMLD، فنختار كلمة طليعية للمجموعة المشاركة من بين كلماتها الطليعية المختلفة وهذا بدوره يؤدي إلى اختيار إحدى كلمات C الأقرب إلى w. ▲

مثال (٢,١١,١٣)

إذا كانت C هي الشفرة المقدمة في المثال (**٢,١٠,٥**) فإن جدول SDA هو المنشأ في المثال (**٢,١١,٧**). سنقوم بفك بعض التشفيرات باستخدام SDA.

لنفرض أن الكلمة المستقبلة هي $w = 110111$. عندئذ، $wH = 010$ وكلمة طليعية u تحقق $wH = uH$ هي الكلمة الواقعة في الصف السادس من جدول SDA ($u = 000010$). إذن تستنتج طريقة CMLD أن:

$$v = w + u = 110111 + 000010 = 110101$$

هي كلمة الشفرة التي تم إرسالها في هذه الحالة.

أما إذا كانت الكلمة المستقبلة هي $w = 110000$ فيكون $wH = 101 = uH$ حيث $u = 000101$ هي الكلمة الطليعية الواقعة في الصف الأخير من جدول SDA. إذن، يكون فك تشفير w هو:

$$v = w + u = 110000 + 000101 = 110101$$

لاحظ أنه لو اخترنا $u' = 001010$ ككلمة طليعية في المجموعة المشاركة الأخيرة لكان فك تشفير w هو:

$$v = w + u' = 110000 + 001010 = 111010.$$ ▲

تمارين

(**٢,١١,١٤**) إذا كانت الكلمة المستقبلة هي $w = 110000$ في المثال (**٢,١١,١٣**) وإذا اخترنا $u'' = 110000$ ككلمة طليعية للمجموعة المشاركة الأخيرة ففك تشفير w.

(**٢,١١,١٥**) لنفرض أن $w = 110111$ هي الكلمة المستقبلة في المثال (**٢,١١,١٣**). بيّن أن كلمة الشفرة $v = 110101$ هي بالفعل الأقرب إلى w.

(**٢,١١,١٦**) إذا كانت $w = 110000$ هي الكلمة المستقبلة في المثال (**٢,١١,١٣**) فجد جميع كلمات الشفرة C الأقرب إلى w.

(**٢,١١,١٧**) أعد فك التشفير للتمرين (**٢,١١,٢**) باستخدام جدول SDA المبين في المثال (**٢,١١,٧**).

(**٢,١١,١٨**) للشفرة المعطاة في المثال (**٢,١١,١٣**)، فك تشفير كل من الكلمات المرسلة w التالية:

(أ) 011101 (ب) 110101

(ج) 111111 (د) 000000.

(**٢,١١,١٩**) استخدم جدول SDA لكل من الشفرات التالية لفك تشفير الكلمات المرسلة المعطاة (جداول SDA لهذه الشفرة تم إنشاؤها في التمرينين (**٢,١١,٨**) و (**٢,١١,٩**))

(أ) $C = \{0000, 1001, 0101, 1100\}$

(i) $w = 1110$ (ii) $w = 1001$ (iii) $w = 0101$

(ب) $C = \{00000, 10100, 01011, 11111\}$

(i) $w = 10101$ (ii) $w = 01110$ (iii) $w = 10001$

(ج) $C = \{111000, 001110, 100011\}$

(i) $w = 101010$ (ii) $w = 011110$ (iii) $w = 011011$

(**٢,١١,٢٠**) لتكن H مصفوفة اختبار النوعية لشفرة C حيث:

$$H = \begin{bmatrix} 011 \\ 101 \\ 110 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

فك تشفير كل من الكلمات المستقبلة w التالية:

(أ) 110100 (ب) 111111

(ج) 101010 (د) 000110

(**٢,١١,٢١**) لتكن C شفرة من الطول 7 حيث مصفوفة اختبار النوعية H هي المصفوفة من الدرجة 3×7 التي جميع كلمات صفوفها غير صفرية ومن الطول 3.

(أ) أنشئ جدول SDA للشفرة C.

(ب) فك تشفير 1010101.

يتم إنشاء جدول SDA لغرض استخدامه في فك التشفير بطريقة IMLD على النحو التالي:

لنفرض أن w هي الكلمة المستقبلة. عندئذ يكون عدد كلمات الشفرة C الأقرب إلى w مساوياً لعدد أنماط الأخطاء في المجموعة المشاركة $C + w$ ذات الوزن الأصغر. ففي حالة وجود مجموعة مشاركة للشفرة C تحتوي على أكثر من كلمة وزنها أصغري نقوم بحذف هذه المجموعة المشاركة وتنادُرها من جدول SDA. علاوة على ذلك فإن وزن كلمة طليعية في مجموعة مشاركة يساوي عدد أنماط الأخطاء التي يتم تصويبها عند استخدام طريقة MLD عند استقبالنا لكلمة تنتمي إلى المجموعة المشاركة نفسها، فإذا كان هذا الوزن كبيراً فمن الممكن اتخاذ قرار حذف المجموعة المشاركة هذه مع تنادُرها من جدول SDA (في حالة استخدام IMLD) حتى لو كانت هذه الكلمة ذات الوزن الأصغر وحيدة في المجموعة المشاركة المشار إليها. بهذا نحصل على جدول SDA

مختصر لطريقة IMLD. وفي هذه الحالة عند استقبالنا لكلمة تناذرها ليس من ضمن التناذرات التي يتكون منها جدول SDA المختصر فإننا نطلب إعادة إرسال.

عند التطبيق العملي نتعامل عادة مع شفرات عدد كلماتها كبير جداً، على سبيل المثال، ليس مفاجئاً أن يكون عدد كلمات شفرة يساوي 2^{50} ومن ثم يكون عدد صفوف جدول SDA حوالي 1.126×10^{15} مما يتسبب في صعوبة تنفيذ جدول SDA لغرض فك تشفير شفرات خطية. وبهذا يمكن القول إنه لم يتم حل مسألة فك التشفير عند الاستخدام العملي لطريقة MLD. ومع ذلك سنرى لاحقاً أن طريقة MLD فعّالة حسابياً لشفرات خطية يتم إنشاؤها بمواصفات محددة. في الحقيقة، أحد أهداف نظرية التشفير هو إنشاء شفرات يكون فك تشفيرها سهلاً بواسطة طريقة MLD.

(٢,١٢) موثوقية IMLD للشفرات الخطية

Reliability of IMLD for Linear Codes

لتكن C شفرة خطية طولها n وبُعدها k. تذكر أنه إذا تم إرسال $v \in C$ عن طريق قناة BSC باحتمال p فإن $\theta_p(C, v)$ هو احتمال استنتاج طريقة IMLD بأن الكلمة v هي بالفعل الكلمة المرسلة.

لكل كلمة طليعية وحيدة u في مجموعة مشاركة ولكل كلمة v من كلمات شفرة C تكون $v+u$ أقرب إلى v منها إلى أي كلمة شفرة أخرى. أيضاً، إذا كانت $w \neq v+u$ لكلمة v من كلمات الشفرة ولكلمة طليعية وحيدة u في مجموعة مشاركة فإنه توجد كلمة شفرة أخرى بحيث يكون قرب w منها أقل من أو يساوي قرب w من v. عندئذ، للشفرات الخطية تكون مجموعة الكلمات $L(v)$ الأقرب إلى v من كلمات الشفرة الأخرى هي:

$$L(v) = \{w : w = v + u \text{ ، } u \text{ هي كلمة طليعية وحيدة لمجموعة مشاركة}\}$$

وبهذا نرى أنه إذا كانت $w = v + u$ فقيمة $\theta_p(v,w)$ تعتمد فقط على $wt(u)$. وبهذا لا تعتمد قيمة الاحتمال $\theta_p(C,v)$ على v للشفرات الخطية C. سنرمز لهذا الاحتمال المشترك بالرمز $\theta_p(C)$. عندئذ،

$$\theta_p(C) = \sum_{u \in L(0)} p^{n-wt(u)}(1-p)^{wt(u)}$$

بناء على ذلك، لإيجاد موثوقية شفرة خطية نحتاج فقط إلى معرفة الكلمات الطليعية الوحيدة للمجموعات المشاركة، حيث نقوم بحساب احتمال كل من كلمات الطليعة الوحيدة في المجموعات المشاركة باعتبارها نمط خطأ ومن ثم نأخذ مجموع هذه الاحتمالات للحصول على $\theta_p(C)$.

لاحظ أننا قد بيّنا أيضاً أن مجموعة أنماط الأخطاء التي تصوّبها الشفرات الخطية بطريقة IMLD تساوي مجموعة الكلمات الطليعية الوحيدة للمجموعات المشاركة.

مثال (٢,١٢,١)

لتكن C الشفرة المقدمة في المثال (**٢,١٠,٥**). توجد للمجموعات المشاركة كلمة طليعية واحدة وزنها 0 وست كلمات طليعية وزن كل منها يساوي 1. إذن، باستخدام IMLD نجد أن $\theta_p(C) = p^6 + 6p^5(1-p)$. ▲

تمرين

(**٢,١٢,٢**) احسب $\theta_p(C)$ لكل من شفرات التمارين (**٢,١٠,٦**)، (**٢,١٠,٧**)، (**٢,١٠,٨**).