

Information theory and coding

نظرية المعلومات و الترميز

مدرسة المقرر

د.بشرى علي معلا

مفردات المحاضرة

- كشف الأخطاء والأعراض المتزامنة
- علاقة الأعراض المتزامنة بشعاع الخطأ
- القدرة على كشف الأخطاء
- مسافة هامينغ
- ترميز هامينغ
- ترميز Cyclic Redundancy Check (CRC)

كشف الأخطاء والأعراض المتزامنة (3/1)

➤ بفرض لدينا ترميز خطي على شكل بلوكات $C_b(n, K)$ ، وكانت له مصفوفة توليد G و مصفوفة فحص الإنجابية H .

$$C = (c_0, c_1, \dots, c_{n-1})$$

$$r = (r_0, r_1, \dots, r_{n-1})$$

➤ و كانت كلمة الترميز المرسله عبر قناة ذات ضجيج هي:

➤ و كان الشعاع المستقبل على خرج هذه القناة (أي كلمة الترميز المستقبلة):

➤ فإن (r) سيكون مختلفاً عن (C) أي أن :

الشعاع المستقبل (r) هو شعاع الجمع لكلمة الترميز المرسله و شعاع الخطأ:

$$e = (e_0, e_1, \dots, e_{n-1}) \quad \text{حيث شعاع الخطأ هو:}$$

$$e_i = 1 \Rightarrow r_i \neq c_i \quad , \quad e_i = 0 \Rightarrow r_i = c_i \quad \text{و منه:}$$

كشف الأخطاء والأعراض المتزامنة (3/2)

❖ نعرف الأعراض المتزامنة (Syndrome) بأنها:

نتيجة فحص الإنجابية الذي يجرى على الشعاع المستقبل (r) لتحديد فيما إذا كان (r) هو أحد كلمات الترميز أم لا.

$$\begin{aligned} S &= r \circ H^T \\ &= (s_0, s_1, \dots, s_{n-k-1}) \end{aligned}$$

و تعرف بالعلاقة:

(1)

و هذا يدعى بالأعراض المتزامنة لـ r (Syndrome)

كشف الأخطاء والأعراض المتزامنة (3/3)

➤ انطلاقاً من العلاقة السابقة نلاحظ أن :

إذا و فقط إذا كان الشعاع المستقبل هو كلمة الترميز المرسله $S = r \circ H^T = 0$

إذا و فقط إذا كان الشعاع المستقبل r مختلف عن كلمة الترميز المرسله $S = r \circ H^T \neq 0$

✓ **ملاحظة:** من الممكن أن تكون الأخطاء في بعض أشعة الخطأ غير قابلة للكشف أي أنها تحتوي أخطاء بحيث ينتج:

$$S = r \circ H^T = 0$$

يدعى هذا النوع من الأخطاء بـ **الأخطاء غير القابلة للكشف**.

✓ بما أنه يوجد هناك $(2^k - 1)$ كلمة ترميز غير صفرية ، فإنه يوجد $(2^k - 1)$ شعاع خطأ غير قابل للكشف.

علاقة الأعراض المتزامنة بشعاع الخطأ

يمكن كتابة علاقة الأعراض المتزامنة كما يلي:

$$S = r \circ H^T = (C_i \oplus e_j) \circ H^T = C_i \circ H^T \oplus e_j \circ H^T$$

بما أن C_i هي كلمة الترميز الحقيقية المرسله (دون أخطاء) فإن:

$$C_i \circ H^T = 0$$

$$\Rightarrow S = r \circ H^T = e_j \circ H^T$$

أي يمكن تشكيل فحص الأعراض المتزامنة إما بكلمة ترميز خاطئة (r) أو شعاع الخطأ المسبب لذلك (e)

مثال

إذا كانت الترميز الخطي على شكل بلوكات $C_b(6,3)$ الذي يملك مصفوفة فحص الإنجابية الآتية:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

حدد قيم الأعراض المتزامنة المقابلة لأشعة الخطأ
الحل:

$$S = e_j \circ H^T$$

اعتماداً على العلاقة:

مثلاً من أجل شعاع الخطأ $e_0 = [1 \ 0 \ 0 \ 0 \ 0 \ 0]$ يكون:

$$\Rightarrow S = e_j \circ H^T = [1 \ 0 \ 0 \ 0 \ 0 \ 0] \circ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = 100$$

و منه و بنفس الطريقة نحصل على الجدول الذي يبين كل الأعراض المتزامنة و أشعة الخطأ المقابلة لها:

e	syndrome
0 0 0 0 0 0	000
1 0 0 0 0 0	100
0 1 0 0 0 0	010
0 0 1 0 0 0	001
0 0 0 1 0 0	110
0 0 0 0 1 0	011
0 0 0 0 0 1	101

إذا كانت الترميز الخطي على شكل بلوكات $C_b(6,3)$ إذا كانت كلمة الترميز C متعلقة بالرسالة 110 قد تم إرسالها و الشعاع المستقبل هو $r=001110$. هل كلمة الترميز المستقبلية هي نفسها كلمة الترميز المرسل؟
الحل:

نحسب الأعراس المتزامنة ل r كما يلي:

$$\Rightarrow S = r \circ H^T = [0 \ 0 \ 1 \ 1 \ 1 \ 0] \circ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = 100$$

قيمة S لا تساوي الصفر أي هناك خطأ في الاستقبال

$$e = 1000000$$

بمقارنة قيمة S مع الجدول نلاحظ أن الخطأ حدث في الخانة الأولى للشعاع المرسل

101110

و الكلمة الصحيحة هي

تفكيك تصحيح الخطأ

➤ من أجل شعاع مستقبل معطى r عند مدخل مفكك الترميز:

1. نحسب الأعراض المتزامنة لـ r باستخدام:

2. نحسب كلمة الترميز المخمئة:

$$S = r \circ H^T$$

$$\hat{C} = r \oplus \hat{e} = (C \oplus e) \oplus \hat{e} = C \oplus (e \oplus \hat{e})$$

$$e = \hat{e} \Rightarrow \hat{C} = C$$

✓ إذا كان الخطأ المخمن هو نفسه الخطأ الحقيقي فإن:

✓ إذا كان الخطأ المخمن غير صحيح، سيختار مفكك الترميز كلمة الترميز التي لم ترسل، مما ينتج عنه خطأ تفكيك الترميز.

مثال

2. بفرض أن كلمة الترميز المرسله $C=101110$ هل ستكون الرسالة المخمنه مطابقة للرسالة المرسله.

الحل: نحسب كلمة الترميز المخمنه:

من الجدول يكون شعاع الخطأ هو $e = 100000$

$$\hat{C} = r \oplus \hat{e} = 001110 \oplus 100000 = 101110$$

نلاحظ أن $\hat{C} = C$ هذا يعني أن الرسالة على الخرج هي مطابقة للرسالة الفعلية

المسافة الدنيا للترميز على شكل بلوكات

❖ إذا فرضنا أن لدينا كلمات الترميز: $C = (c_0, c_1, \dots, c_{n-1})$

$V = (v_0, v_1, \dots, v_{n-1})$

$X = (x_0, x_1, \dots, x_{n-1})$

❖ نعرف مايلي:

➤ **وزن هامنج (الوزن البسيط) لكلمة ترميز (C):** هو عدد الخانات غير الصفرية في هذه الكلمة. و يشار لها بـ $w(C)$

$$C = (1001011) \Rightarrow w(C) = 4 \quad \checkmark \text{مثال:}$$

المسافة الدنيا للترميز على شكل بلوكات

➤ مسافة هامنج (المسافة البسيطة) بين كلمتي ترميز (C, V) : هي عدد أماكن الاختلاف بين هاتين الكلمتين. و يشار لها بـ $d(C, V)$

$$\left. \begin{array}{l} C = (1001011) \\ V = (0100011) \end{array} \right\} \Rightarrow d(C, V) = 3$$

✓ مثال:

➤ من أجل ثلاث كلمات ترميز يكون :

$$d(C, V) + d(V, X) \geq d(C, X)$$

➤ مسافة هامنغ بين كلمتي ترميز (C, V) : يساوي وزن هامنغ لمجموع (C, V) باستخدام XOR

$$d(C, V) = w(C \oplus V)$$

$$\left. \begin{array}{l} C = (1001011) \\ V = (1110010) \end{array} \right\} \Rightarrow d(C, V) = 4$$

$$\left. \begin{array}{l} \\ \\ w(C \oplus V) = w(0111001) = 4 \end{array} \right\} \Rightarrow d(C, V) = w(C \oplus V)$$

✓ مثال:

➤ المسافة الدنيا من أجل الترميز على شكل بلوكات :

هي أصغر مسافة هامنغ يمكن حسابها بين أية كلمتي ترميز مختلفتين في ترميز ما: ويشار لها بـ d_{\min}

$$d_{\min} = \min \{ d(W, V) ; W, V \in C_b(n, k) ; W \neq V \}$$

$$d_{\min} \stackrel{\Delta}{=} \min w_{\min}$$

المسافة الدنيا للترميز الخطي على شكل بلوكات = الوزن الأصغري لكلمات الترميز غير الصفريية لهذا الترميز

➤ إذا كانت المسافة الدنيا في الترميز على شكل بلوكات هي d_{\min} إن أي كلمتي ترميز مختلفتين من هذا الترميز تختلفان عن بعضهما بـ d_{\min} موضع.

➤ لا يمكن لأي شعاع خطأ مكون من $(d_{\min} - 1)$ أو أقل أن يحول كلمة الترميز إلى كلمة ترميز أخرى. لذا عندما سيكتشف المستقبل أن الشعاع المستقبل ليس كلمة ترميز من الترميز المستخدم , عندها يقرر أن هناك خطأ قد حدث.

مثال
من أجل ترميز خطي على شكل بلوكات معطى كالاتي:

ما هي المسافة الدنيا لهذا الترميز؟

الحل:

حسب التعريف يكون:

$$d_{\min}^{\Delta} = \min w_{\min} = 3$$

Codewords

0	0	0	0	0	0	0
1	0	1	0	0	0	1
1	1	1	0	0	1	0
0	1	0	0	0	1	1
0	1	1	0	1	0	0
1	1	0	0	1	0	1
1	0	0	0	1	1	0
0	0	1	0	1	1	1
1	1	0	1	0	0	0
0	1	1	1	0	0	1
0	0	1	1	0	1	0
1	0	0	1	0	1	1
1	0	1	1	1	0	0
0	0	0	1	1	0	1
0	1	0	1	1	1	0
1	1	1	1	1	1	1

المقدرة على تصحيح الأخطاء في الترميز الخطي على شكل بلوكات

$$t = \left(\frac{d_{\min} - 1}{2} \right)$$

➤ العدد الأعظمي للخانات القابلة للتصحيح هو:

✓ مثال

من أجل الترميز الخطي على شكل بلوكات فيه: $d_{\min} = 7$ يكون الترميز قادر
على كشف الأشعة الحاوية على $d_{\min} - 1 = 6$ خاتة خطأ أو أقل و تصحيح $t = 3$ خاتة



جامعة
المنارة

MANARA UNIVERSITY

ترميزات هامنج

(Hamming Codes)

➤ تعد ترميمات هامنج من أول أصناف الترميز الخطي المصمم من أجل تصحيح الأخطاء. تستخدم هذه الترميمات من أجل التحكم بالأخطاء في أنظمة الاتصالات الرقمية وتخزين المعلومات.

➤ من أجل أي عدد صحيح موجب $m \geq 3$ ، يوجد ترميز هامنج بالبارامترات الآتية:

$$n = 2^m - 1$$

طول كلمة الترميز:

$$k = 2^m - m - 1$$

عدد رموز المعلومات:

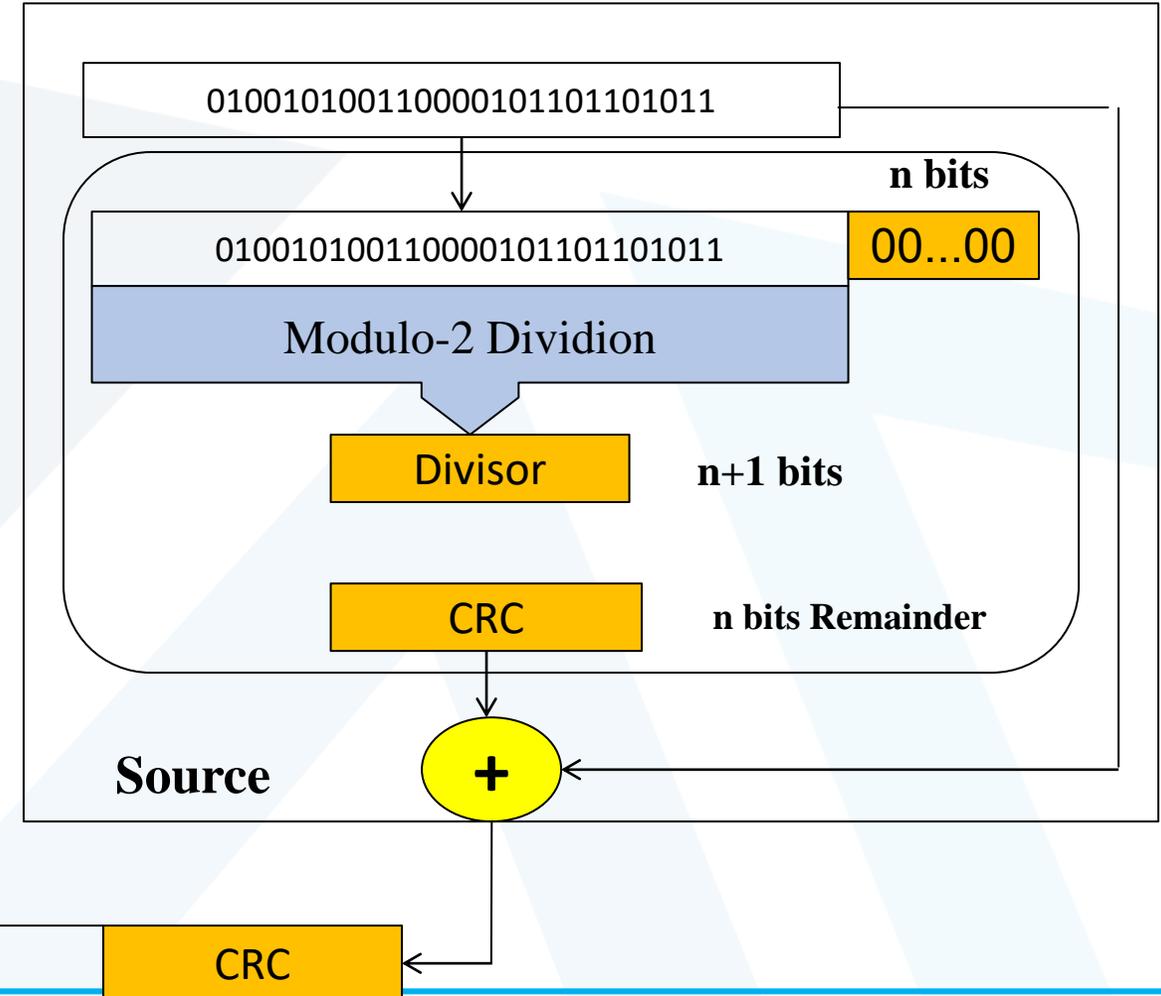
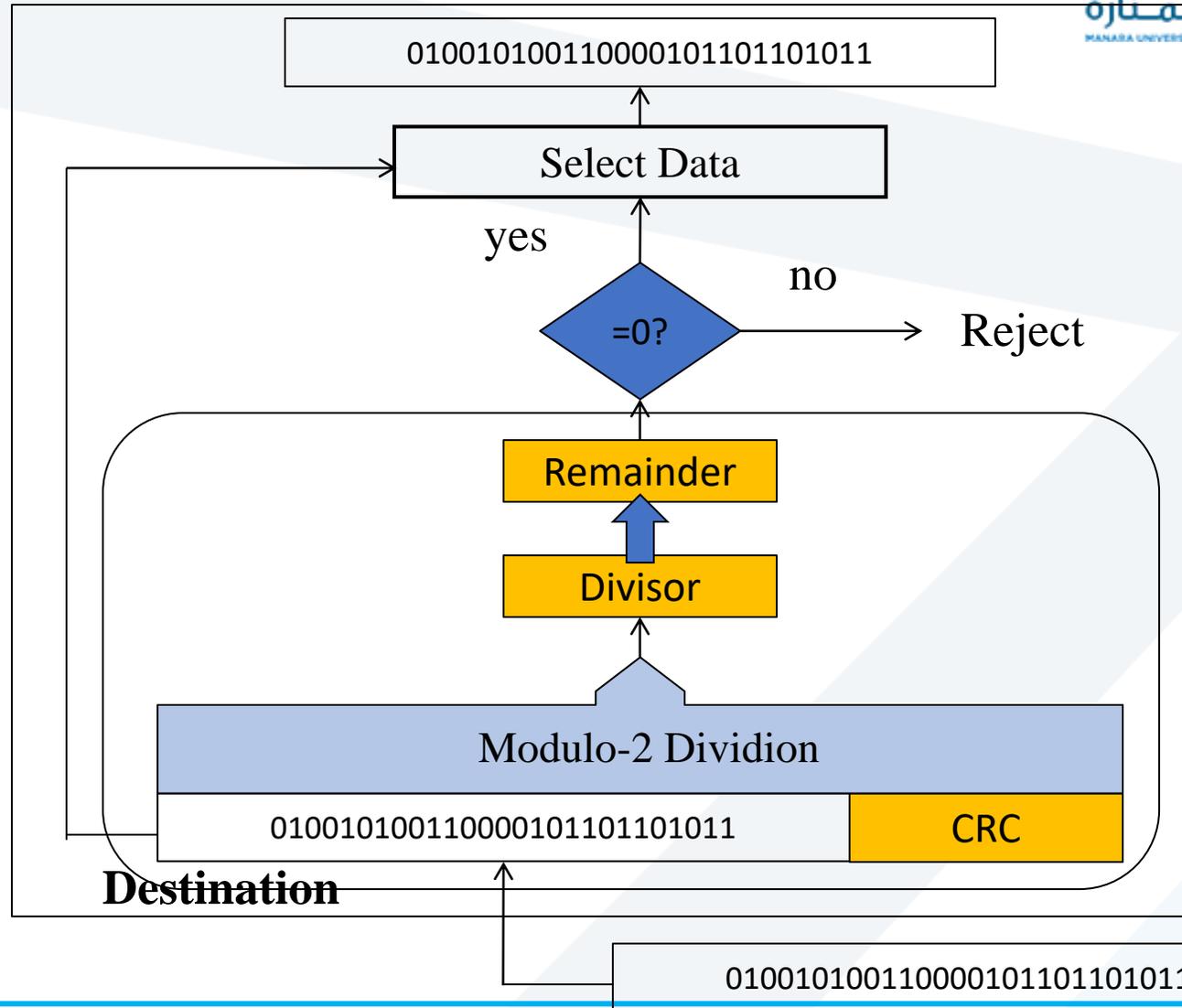
$$n - k = m$$

عدد رموز فحص الانجابية:

$$t = 1 (d_{\min} = 3)$$

المقدرة على تصحيح الأخطاء:

ترميز Cyclic Redundancy Check (CRC)



Cyclic Redundancy Check (CRC)

- إذا كانت PDU(Packet Data Unite) معروفة
- إذا كان المولد G معروف
- G : عملياً سلسلة من البتات ، إنه جزء من بروتوكول نقل المعطيات و يكون معلوماً في الإرسال و الاستقبال
- إذا كان G مكوناً من $r+1$ بت فتكون $r=G-1$
- نضيف r بت صفري إلى ال PDU و نسميه PDU'
- نقسم PDU' على G و هذا يعطي باقي قسمة R
- يكون لدينا الرسالة التي سترسل T :

$$T = PDU' + R$$

بعد التحويل إلى كثيرات الحدود، تتم القسمة:

$$X^3 + X^2 + X \quad \left. \vphantom{X^3 + X^2 + X} \right\} Q = \begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 0 \\ \hline \end{array}$$

$$\begin{array}{r} X^2 + 1 \\ \hline X^5 + X^4 + X^2 + 1 \\ X^5 + X^3 \\ \hline X^4 + X^3 + X^2 + 1 \\ X^4 + X^2 \\ \hline X^3 + 1 \\ X^3 + X \\ \hline X \end{array}$$

$\Rightarrow T = PDU' + R$

$$X \quad \left. \vphantom{X} \right\} R = \begin{array}{|c|c|} \hline 1 & 0 \\ \hline \end{array}$$

$$T = X^5 + X^4 + X^2 + X + 1 \quad \Rightarrow T = 110110$$

مولد ترميز CRC

- الهدف من مولد الترميز أن يمتلك الخواص الأكثر أهمية:
 - اكتشاف كل الأخطاء الأحادية و الثنائية
 - اكتشاف كل الأخطاء المفاجئة بطول 16 خانة أو أقل

- أمثلة عن عدة المولد:

100000111	CRC-8: •
11000110011	CRC-10: •
1100000000101	CRC-12: •
11000000000000101	CRC-16: •
10001000000100001	CRC-CCITT (ITU-T): •
100000100110000010001110110110111	CRC-32: •

نهاية المحاضرة الثامنة