مجلة جامعة دمشق للعلوم الأساسية
مجلد 41-عدد 3 (2025): 67- 83

Damascus University Journal for the Basic Sciences
Vol 41 No.3 (2025): 83 - 67

دراسة مقارنة بين طرق فك ترميز ريد– ميلر من المرتبة الأولى

بكر محمد مشرف[1]، غصون أحمد عبد الكريم الجيرودي[2]

1 طالب ماجستير، جامعة دمشق، كلية العلوم، قسم الرياضيات، bakr.mushraf@damascusuniversity.edu.sy

2 أستاذة مساعدة، جامعة دمشق، كلية العلوم، قسم الرياضيات. ghussoun.aljeiroudi@damascusuniversity.edu.sy

الملخّص:

يُعد الترميز من العلوم الأساسية الرائدة في مجالات الاتصالات وحماية البيانات وخصوصاً مع التطور الحاصل في البيانات الرقمية، حيث أن الهدف من الترميز هو تقليل حجم البيانات وتحسين جودة الإرسال والاستقبال وتوفير السرية والأمان وزيادة الكفاءة والدقة، إن تقنية ترميز ريد–ميلر هي إحدى تقنيات الترميز المستخدمة بشكل كبير وفعال في العديد من التطبيقات الحديثة (اتصالات الأقمار الصناعية –تقنيات الأمان والحماية – أنظمة الذكاءالصناعي – أنظمة الاتصالات الكمية – البيانات الصحية والطب لرقمي–....).

الأمر الذي دفعنا إلى القيام بدراسة بحثية ضمن هذا المجال والتي تتضمن القيام بدراسة ترميز وفك ترميز ريد ميلر من المرتبة الأولى باستخدام طريقتي منطق الأغلبية ومصفوفات هادامارد والمقارنة بينهما من حيث الأداء والكفاءة والتعقيد الحسابي والسرعة والفعالية والقدرة على تصحيح الأخطاء.

الكلمات المفتاحية: الترميز، ترميز ريد– ميلر، الجبر الخطي، المصفوفات.

تاريخ الإيداع: 2023/11/13
تاريخ الموافقة: 2024/01/24

ISSN (online): 2789-6366
http://journal.damascusuniversity.edu.sy/index.php/index/index

A Comparative Study Between Decoding Methods for First-Order Reed-Muller Codes

Bakr Muhammad Mushrif[1*] Ghussoun Ahmed Abdul Al-karim Al-Jeiroudi[2]

[1] Master's student, Department of Mathematics, Faculty of Sciences, Damascus University, Syria. bakr.mushraf@damascusuniversity.edu.sy .
[2] Professor, Department of Mathematics, Faculty of Sciences,Damascus University, Syria. ghussoun.aljeiroudi@damascusuniversity.edu.sy

Abstract

Encoding is considered one of the fundamental sciences in the fields of communication and data protection, particularly with the advancement of digital data. The primary objective of encoding is to diminish the size of data, enhance the quality of transmission and reception, ensure confidentiality and security, and optimize efficiency and accuracy. Reed-Muller encoding technology stands out as a widely employed and effective technique in various modern applications, such as satellite communications, security and protection methods, artificial intelligence systems, quantum communications systems, health data, and digital medicine.

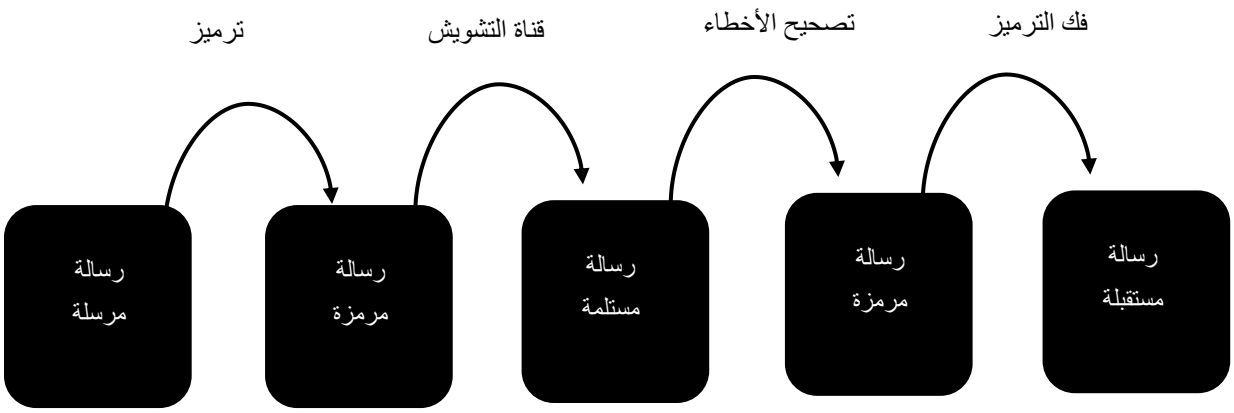
Motivated by the significance of Reed-Muller encoding, we embarked on a research study in this domain. The study encompasses an examination of the encoding and decoding processes of Reed-Muller at the first order, employing two distinct methods: majority logic and Hadamard matrices. The comparison between these methods is conducted with respect to performance, efficiency, computational complexity, speed, effectiveness, and error correction capability.

Received :2023/11/13
Accepted:2024/01/24

Keywords: Coding, Reed-Muller codes, Linear Algebra ,Matrices.

1. المقدمة (Introduction):

في عصر المعلومات الرقمية والتكنولوجيا الحديثة، تصبح عمليات نقل وتخزين البيانات أمراً حيوياً وحساساً، هنا تَكمُن أهمية الترميز. الترميز هو عملية تحويل البيانات من شكلها الأصلي إلى شكل آخر يمكن تمييزها واستعادتها بسهولة، والهدف الرئيسي من الترميز زيادة موثوقية نقل البيانات والحفاظ على دقتها من خلال النقل أو التخزين، آلية الترميز تتم بالشكل:



واحدة من التقنيات المهمة المستخدمة لضمان ذلك هي ترميز ريد ميلر (Reed-Muller Code).

ترميز ريد ميلر هو تقنية ترميز وفك ترميز تعتمد على تحويل البيانات إلى شكل يمكن نقله وتخزينه بأمان، تأتي هذه التقنية مع القدرة على كشف تصحيح الأخطاء في البيانات مما يجعلها مثالية للتطبيقات التي تتطلب دقة عالية مثل الاتصالات السلكية واللاسلكية وتخزين البيانات. تهدف هذه الدراسة البحثية إلى تقييم ومقارنة الأداء والكفاءة والتعقيد الحسابي لفك ترميز ريد ميلر باستخدام طريقتي منطق الأغلبية ومصفوفات هادامارد.

2. فكرة البحث وأهدفه (Idea and objectives):

تُعد تقنيات ترميز ريد ميلر في عالم اتصالات النقل الرقمي للبيانات من أهم الأدوات لضمان سلامة البيانات والمعلومات، الأمر الذي يتطلب فهم عملية الترميز والأساليب والأفكار المتبعة في هذه العملية.

بالمقابل هناك العديد من الطرق التي تقوم بفك هذا الترميز الأمر الذي يدفع إلى المقارنة بين تلك الطرق واختيار الأفضل لتحسين وتسريع هذه العملية، والهدف الأساسي من هذا البحث هو المقارنة بين طريقتي منطق الأغلبية ومصفوفات هادامارد من حيث الأداء والكفاءة وغيرها من المعايير.

3. مواد وطرق البحث(Materials and Methods):

3-1 تعاريف أساسية (Basic Definitions): (Sudan et al., 2023,p.5)

3-1-1 **الرموز (Symbols):** هي كائنات مجردة مثل ...,A,B,7,*.

3-1-2 **الأبجدية(The Alphabet): هي مجموعة منتهية وغير خالية من الرموز نشير إليها بـ** .

3-1-3 **مثل:** $= \{0, 1\}$ ، $= \{x, y, z\}$.

3-1-4 **كلمات من الأبجدية (Words from The Alphabet): هي مجموعة العناصر من** ^{n} **بحيث كل عنصر يُكتب بالشكل** $(a_1, a_2, \dots, a_n)$ **وهو عبارة عن متجه بـ** n **رمز من الابجدية** .

3-1-5 **بوابةXOR (XOR Gate): هي بوابة لها عدد من المداخل والمخارج فقط، وتُعطي خرج "1" إذا كانت المداخل مختلفة، وتُعطي خرج "0" إذا كانت المداخل متشابهة.**

A	B	C
0	0	0
1	0	1
0	1	1
1	1	0

3-2 تعاريف أساسية في

3-3 الجبر(Basic Definitions in Algebra):

3-2-1- **الحقل(Field):(** الراشد، 2014،30) لتكن F مجموعة غير خالية مزودة بقانوني تشكيل داخليين نرمز لهما بـ $(*_1,*_2)$ نقول عن الثلاثية $(F,*_1,*_2)$ إنها حقل إذا تحقق:

1) $(F,*_1)$ زمرة تبديلية.

2) $(F^*,*_2)$ زمرة تبديلية حيث $F^* = F\backslash\{0\}$.

3) $*_2$ توزيعي على $*_1$ من اليمين واليسار.

مثال: مجموعة الأعداد العادية مع الجمع والضرب تشكل حقلاً.

3-2-2- **حقل غالوا (Galois Field)**: لأجل p عدد طبيعي أولي عندئذ حقل غالوا يُعطى بالشكل:

$$\mathbb{F}_{p^n} = \{0,1,2,\dots,p^n-1\} = \mathbb{z}_{p^n}$$

حيث n عدد طبيعي.

مثال: $\mathbb{F}_2 = \{0,1\}$ حقل منتهي.

3-2-3- **المصفوفة (The Matrix)**: (الراشد، 2014،49) لأجل n,m عددين طبيعيين نعرف المصفوفة ذات n سطر و m عمود بالشكل:

$$M_{n\times m} = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}$$

في حال كان n=m نقول أن المصفوفة هي مصفوفة مربعة.

3-2-4- **جداء كرونيكر(Kronecker Product)**: (Wicker,1994,p.169) لأجل C,D مصفوفتين نعرف جداء كرونيكر بالشكل:

$$C\otimes D = \begin{bmatrix} c_{11}D & c_{12}D & \dots & c_{1n}D \\ c_{21}D & c_{22}D & \dots & c_{2n}D \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1}D & c_{m2}D & \dots & c_{mn}D \end{bmatrix}$$

جداء كرونيكر عملية غير تبديلية أي $C\otimes D \neq D\otimes C$

مثال: من أجل

$$D = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad C = [1 \quad 3]$$

$$C\otimes D = \begin{bmatrix} 1 & 2 & 3 & 6 \\ 3 & 4 & 9 & 12 \end{bmatrix}$$

$$D\otimes C = \begin{bmatrix} 1 & 3 & 2 & 6 \\ 3 & 9 & 4 & 12 \end{bmatrix}$$

3-2-5- **العمليات على المتجهات:** (Cooke, 1999,p. 21) نتعامل مع متجهات بطول n بعناصر من الحقل $\mathbb{F}_2$.

لأجل كل $x = (x_1, x_2, \dots, x_n)$ ، $y = (y_1, y_2, \dots, y_n)$ ، $a \in \mathbb{F}_2$ نعرف:

1) جمع متجهين:

$$x + y = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

2) جمع متجه مع عدد:

$$x + a = (x_1 + a, x_2 + a, \dots, x_n + a)$$

3) ضرب متجهين:

$$x * y = (x_1 * y_1, x_2 * y_2, \dots, x_n * y_n)$$

4) ضرب متجه بعدد:

$$x * a = (x_1 * a, x_2 * a, \dots, x_n * a)$$

5) الضرب النقطي لمتجهين:

$$x.y = x_1 * y_1 + x_2 * y_2 + \cdots + x_n * y_n$$

3-4 ترميز ريد ميلر(Reed-Muller Codes):

3-4-1 تعريف ريد ميلر:(Ayats et al., 2005,p.83)

لأجل أي عددين **r,m** طبيعيين بحيث $\mathbf{0} \leq \boldsymbol{r} \leq \boldsymbol{m}$ يوجد ترميز ريد ميلر من المرتبة r نشير إليه بـ RM(r,m).

3-4-2 مبرهنة: (Hoffman et al.,1991,p.219)

ترميز ريد ميلر RM(r,m) من مرتبة **r** له الخصائص الآتية:

1) طول الترميز $\boldsymbol{n} = \mathbf{2}^{\boldsymbol{m}}$

2) بُعد الترميز $\boldsymbol{k} = \sum_{\boldsymbol{i}=\mathbf{0}}^{\boldsymbol{r}} \binom{\boldsymbol{m}}{\boldsymbol{i}}$ حيث $\binom{\boldsymbol{m}}{\boldsymbol{i}} = \frac{\boldsymbol{m}!}{\boldsymbol{i}!(\boldsymbol{m}-\boldsymbol{i})!}$

3) مسافته الصغرى $\boldsymbol{d} = \mathbf{2}^{\boldsymbol{m}-\boldsymbol{r}}$

3-4-3 تعريف ترميز ريد ميلر من المرتبة الأولى:(Meyer,2021,p.13)

لأجل العدد الصحيح الموجب m ترميز ريد ميلر من المرتبة الأولى نشير إليه بـ RM(1,m) له الخصائص الآتية:

طول الترميز	بُعده	مسافته الصغرى
$\boldsymbol{n} = \mathbf{2}^{\boldsymbol{m}}$	$k = m + 1$	$d = 2^{m-1}$

3-4-4 تمهيدية: (Sudan et al., 2023,p.13)

لدينا ترميز RM(r,m) من المرتبة r عندئذ يمكن الكشف عن $d - 1$ خطأ حيث $d = 2^{m-1}$.

3-4-5 المصفوفة المولدة لترميز ريد ميلر من المرتبة الأولى وعناصرها: (Blahut, 2003,p. 419)

تُعد المصفوفة المولدة مكون أساسي لترميز الرسائل وأن أسطر هذه المصفوفة عبارة عن متجهات نشير إليها بـ v_i.

لأجل $1 \leq i \leq m$ نأخذ v_i من البُعد 2^m بعناصر من $\mathbb{F}_2$ بالشكل الآتي:

$$v_i = (\underbrace{\underbrace{00\dots0}_{2^{i-1}}\ \underbrace{11\dots1}_{2^{i-1}}\ \underbrace{00\dots0}_{2^{i-1}}\dots\underbrace{11\dots1}_{2^{i-1}}}_{2^m})$$

وَ v_0 بالشكل:

$$v_0 = (\underbrace{11\dots1}_{2^m})$$

ترميز $RM(1,m)$ من المرتبة الأولى بطول 2^m عناصر مصفوفته المولدة متجهات مستقلة:

$$\{v_0, v_1, \dots, v_m\}$$

إذا تم ترتيب هذه المتجهات كأسطر في مصفوفة فإن المصفوفة هي المصفوفة المولدة لـ $RM(1,m)$ نشير إليها بـ $G_{RM(1,m)}$ وتُعطى بالشكل:

$$G_{RM(1,m)} = \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_m \end{bmatrix}$$

والمصفوفة المولدة $G_{RM(1,m)}$من المرتبة $k \times n$ حيث:

$n = 2^m$ عدد أعمدة المصفوفة المولدة.

$k = m + 1$ عدد أسطر المصفوفة المولدة.

مثال(1): المصفوفة المولدة لـ $RM(1,2)$ تُعطى بالشكل:

$$G_{RM(1,2)} = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

مثال(2): المصفوفة المولدة لـ $RM(1,3)$ تُعطى بالشكل:

$$G_{RM(1,3)} = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

3-4-6 آلية ترميز ريد ميلر من المرتبة الأولى: (Blahut, 2003,p. 421)

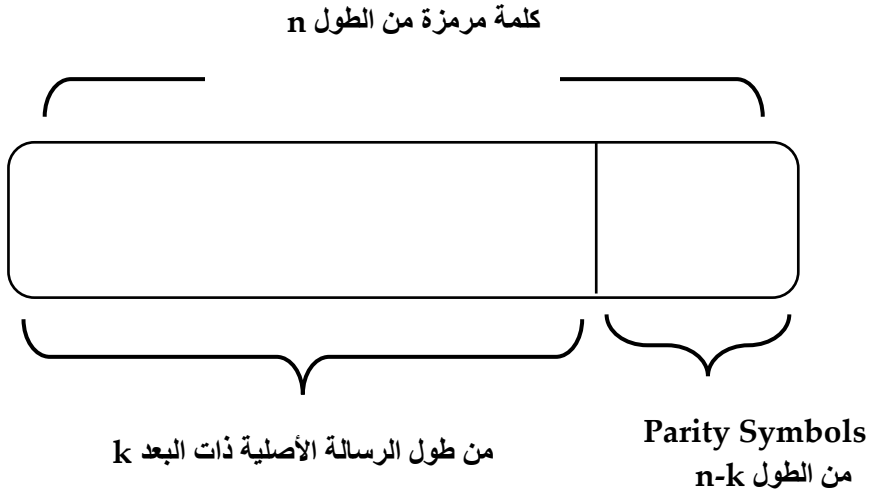
آلية ترميز ريد ميلر من المرتبة الأولى:

1) نقوم بتقسيم الرسائل إلى كتل بطول k.

2) نقوم بتشكيل المصفوفة المولدة المقابلة لترميز ريد ميلر من المرتبة الأولى، يتم تشكيل المصفوفة بمراعاة إن بُعد الترميز k أي يساوي طول الكتلة في تقسيم الرسائل.

3) نقوم بضرب كل كتلة بالمصفوفة المولدة لترميز ريد ميلر من المرتبة الأولى، نحصل على ترميز هذه الكتلة.

4) بتجميع جميع الكتل المُرمزة نحصل على مجموعة جميع الكتل المُرمزة التي هي $Codewordes$.



مثال: نأخذ الرسالة (1010) لأجل$RM(1,3)$ نقوم بترميز الرسالة وذلك بضرب الرسالة بالمصفوفة المولدة للترميز $RM(1,3)$

$$(1010).G_{RM(1,3)} = (1010).\begin{bmatrix}1&1&1&1&1&1&1&1\\0&1&0&1&0&1&0&1\\0&0&1&1&0&0&1&1\\0&0&0&0&1&1&1&1\end{bmatrix}$$
$$= (11001100)$$

4. فك ترميز ريد ميلر من المرتبة الأولى (Reed Muller's First-Order Decoder):

عملية فك ترميز الرسائل باستخدام ريد ميلر يُعد أكثر تعقيدا من ترميزها. هنالك العديد من طرق فك ترميز ريد ميلر من المرتبة الأولى منها طريقة منطق الأغلبية (Majority Logic) - طريقة مصفوفات هادامارد (Hadamard Matrices) وتم أختيار طريقتي فك الترميز هاتين وذلك بسبب استخدامها في مجموعة متنوعة من التطبيقات الحديثة منها:

تكنولوجيا الاتصالات: استخدمت طريقة منطق الأغلبية لفك ترميز ريد ميلر لتحسين أداء الاتصالات عبر شبكات الجيل الخامس(5G).

أنظمة الذكاء الاصطناعي: تستخدم هذه الطرق لتحسين نقل البيانات والاتصالات لتطبيقات الذكاء الاصطناعي.

4-1- **طريقة منطق الأغلبية (Majority Logic):** (Blahut, 2003,p. 430) تعتمد هذه الطريقة مفهوم الأغلبية لتصحيح الأخطاء من خلال مقارنة قيم غالبية مواقع البتات، حيث إذا كان عدد الأصفار أكثر من عدد الوحدات يكون عنصر الأغلبية هو صفر أما إذا كان عدد الوحدات أكثر من عدد الأصفار يكون عنصر الأغلبية هو واحد، وتستخدم هذه الطريقة على نطاق واسع في أنظمة الاتصالات المختلفة وأنظمة تصحيح الأخطاء نظراً لفعاليتها وبساطتها.

خوارزمية منطق الأغلبية:

الخطوة الأولى: المدخلات

الرسالة المستلمة من الطول 2^m وهي $r = (x_0\ x_1\ \dots\ x_{2^m-1})$.

الخطوة الثانية:

- حساب طول الرسالة m واستنتاج k .
- تشكيل مصفوفة ترميز ريد ميلر.

الخطوة الثالثة: تشكيل المتجهات c_k لكُل سطر v_i من المصفوفة المولدة بحيث $1 \le i \le m$

$$c_1 = x_0 + x_{2^{i-1}}$$
$$\vdots$$
$$c_{m+1} = x_{2^m-2^{i-1}-1} + x_{2^m-1}$$

الخطوة الرابعة: يُختار معامل المتجهات c_k لأجل كل متجه v_i بحيث $1 \le i \le m$ وفق منطق الأغلبية ونرمز لهذا المعامل بـ a_i بحيث $1 \le i \le m$.

الخطوة الخامسة:

- نشكل المتجه $\sum_{i=1}^{m} a_i v_i$.
- يُختار معامل المتجه v_0 وفق منطق الأغلبية للمتجه $r + \sum_{i=1}^{m} a_i v_i$ ونرمز له بـ a_0 .
- المركبات المخالفة لعنصر الأغلبية هي المركبات التي تحوي خطأ في الكلمة المستلمة وعدد هذه الأخطاء لا يتجاوز $d-1$ خطأ وذلك حسب تمهيدية (3-3-4).

الخطوة السادسة: المخرجات (الرسالة الأصلية$((a_0 a_1 \dots a_m)$).

مثال: نُرمز الرسالة (0110) باستخدام $RM(1,3)$:

$$(0110).G_{RM(1,3)} = (0110).\begin{bmatrix}1&1&1&1&1&1&1&1\\0&1&0&1&0&1&0&1\\0&0&1&1&0&0&1&1\\0&0&0&0&1&1&1&1\end{bmatrix}$$

$$= (01100110)$$

الكلمة المرمزة (01100110) عند دخولها قناة التشويش وخروجها لنفترض أننا حصلنا على الرسالة المستلمة الآتية:

$r = (01000110)$ لنكتب r بالشكل $r = (x_0\ x_1\ \dots\ x_7)$.

- فك الترميز باستخدام منطق الأغلبية:

نختار المتجه v_1 ، ونقوم بأخذ:

$$c_1 = x_0 + x_1 = 1$$
$$c_2 = x_2 + x_3 = 0$$
$$c_3 = x_4 + x_5 = 1$$
$$c_4 = x_6 + x_7 = 1$$

عنصر الأغلبية 1 وبالتالي $a_1 = 1$

نختار المتجه v_2 ، ونقوم بأخذ:

$$c_1 = x_0 + x_2 = 0$$
$$c_2 = x_1 + x_3 = 1$$
$$c_3 = x_4 + x_6 = 1$$
$$c_4 = x_5 + x_7 = 1$$

عنصر الأغلبية $a_2 = 1$

نختار المتجه v_3 ، ونقوم بأخذ:

$$c_1 = x_0 + x_4 = 0$$
$$c_2 = x_1 + x_5 = 0$$
$$c_3 = x_2 + x_6 = 1$$
$$c_4 = x_3 + x_7 = 0$$

عنصر الأغلبية $a_3 = 0$

نشكل المتجه:

$$\sum_{i=1}^{3} a_i v_i = 1(01010101) + 1(00110011) + 0(00001111) = (01100110)$$

عندئذ:

$$r + \sum_{i=1}^{3} a_i v_i = (01000110) + (01100110) = (00100000)$$

بتصحيح المركبة x_2 في الكلمة المستلمة نحصل على الكلمة المرمزة، ونلاحظ أن عنصر الأغلبية 0 في المتجه $r + \sum_{i=1}^{3} a_i v_i$

وبالتالي معامل المتجه v_0 هو $a_0 = 0$

الكلمة المرسلة الأصلية:

$$(a_0 a_1 a_2 a_3) = (0110)$$

4-2- **طريقة مصفوفات هادامارد (Hadamard Matrices):** (Lint, 1991,p. 95) تعتمد هذه الطريقة على استخدام مصفوفات هادامارد وهي مصفوفات مربعة ذات أسطر متعامدة، والفكرة الرئيسية من هذه الطريقة هي تنفيذ سلسلة من عمليات المصفوفات لفك الترميز.

تعريف مصفوفات هادامارد: (Wicker,1994,p.131)

مصفوفة هادامارد H من المرتبة n هي مصفوفة ابعادها $n \times n$ عناصرها $1, -1$ بحيث يكون

$$HH^T = nI .$$

حيث $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

إن الخوارزمية تتطلب المصفوفات:

$$H_m^j = I_{2^{m-j}} \otimes H_2 \otimes I_{2^{j-1}} \qquad ; j = 1, \dots, m \qquad \dots (\star)$$

خوارزمية مصفوفات هادامارد:

الخطوة الأولى: المدخلات

الرسالة المستلمة من الطول 2^m وهي $r = (x_0\ x_1\ \dots\ x_{2^m-1})$.

الخطوة الثانية:

- حساب طول الرسالة m واستنتاج k .
- تشكيل مصفوفة ترميز ريد ميلر.

الخطوة الثالثة:

- المتجه r_0 يُعطى:

$$r_0 = 2r - e \qquad ; e = (\underbrace{11 \dots 1}_{2^m})$$

- وفق مصفوفة هادامارد H_2 والعلاقة (★) نُعرف:

$$r_j = r_{j-1}.H_m^j \qquad ; \ j = 1, \dots, m$$

الخطوة الرابعة:

- نختار العنصر الأكبر بالقيمة المطلقة في r_m وليكن دليله i_0 نُشير إليه بـ $(r_m)_{i_0}$
- نأخذ $v_{i_0} \in \mathbb{K}^m$ التمثيل الثنائي لـ i_0 مضاف إليه أصفار لليمين بحيث يكون طول v_{i_0} هو n.

v_0	$000 \dots 0$
v_1	$100 \dots 0$
v_2	$010 \dots 0$
v_3	$110 \dots 0$
$\vdots$	$\vdots$
v_{2^m-1}	$111 \dots 1$

الخطوة الخامسة: المخرجات(الرسالة الأصلية):

$$\begin{cases} (1 \quad v_{i_0}) & ; ((r_m)_{i_0}) > 0 \\ (0 \quad v_{i_0}) & ; ((r_m)_{i_0}) < 0 \end{cases}$$

مثال: نُرمز الرسالة (0110) باستخدام $RM(1,3)$:

$$(0110).G_{RM(1,3)} = (0110).\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$= (01100110)$$

الكلمة المرمزة (01100110) عند دخولها قناة التشويش وخروجها لنفترض أننا حصلنا على الرسالة المستلمة الآتية:

$r = (01000110)$ لنكتب r بالشكل $r = (x_0 \ x_1 \ \dots \ x_7)$.

- فك الترميز باستخدام مصفوفات هادامارد:

نوجد المتجه r_0:

$$r_0 = 2r - e = 2(01000110) - (11111111) = (-1 \quad 1 \quad -1 \quad -1 \quad -1 \quad 1 \quad 1 \quad -1)$$

نوجد $r_j \;;\; 1 \le j \le 3$

$$r_1 = r_0.H_3^1 = r_0.[I_{2^2} \otimes H_2 \otimes I_{2^0}] = r_0.[I_4 \otimes H_2 \otimes I_1] = r_0 \left[\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right]$$

$$r_1 = r_0 \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} = (0 \; -2 \; -2 \; 0 \quad 0 \; -2 \; 0 \quad 2)$$

$$r_2 = r_1.H_3^2 = r_1.[I_{2^1} \otimes H_2 \otimes I_{2^1}] = r_1.[I_2 \otimes H_2 \otimes I_2] = r_1 \left[\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right]$$

$$r_2 = (-2 \quad -2 \quad 2 \quad -2 \quad 0 \quad 0 \quad 0 \quad -4)$$

$$r_3 = r_2.H_3^3 = r_2.[I_{2^0} \otimes H_2 \otimes I_{2^2}] = r_2.[I_1 \otimes H_2 \otimes I_4] = r_2 \left[\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \right] =$$

$$r_3 = (-2 \quad -2 \quad 2 \quad -6 \quad -2 \quad -2 \quad 2 \quad 2)$$

المركبة $(r_3)_3 = -6$ الأكبر بالقيمة المطلقة في r_3، وإن $v_3 = 110 \in \mathbb{K}^3$.

بما أن $(r_3)_3 < 0$ تكون الكلمة المرسلة الأصلية هي (0110).

ملاحظة:

إن طريقة البناء المصفوفي باستخدام طريقة مصفوفات هادامارد لفك ترميز رید ميلر من المرتبة الأولى تؤدي إلى عدم تكرار العناصر بالقيمة المطلقة في المتجه r_m.

5. النتائج والمناقشة (Results and Discussion):

بعد التحليل والمقارنة لطرق فك ترميز رید ميلر من المرتبة الأولى باستخدام طريقة منطق الأغلبية وطريقة مصفوفات هادامارد، نبين ايجابيات وسلبيات كل من هاتين الطريقتين ونتائج المقارنة بينهما.

إيجابيات وسلبيات فك ترميز رید ميلر من المرتبة الأولى باستخدام منطق الأغلبية:

الإيجابيات: (Yang,2020)

توفر طريقة منطق الأغلبية قدرة محدودة على تصحيح الأخطاء أي هذه الطريقة فعالة في تحليل وتصحيح الأخطاء في البيانات المستلمة مما يؤدي إلى زيادة في موثوقية ودقة المعلومات التي تم فك ترميزها.

كما أنها توفر كفاءة وسرعة أعلى في عملية فك الترميز مما يقلل الوقت ويسمح بمعالجة المعلومات بشكل أسرع.

علاوة على ذلك إن لهذه الطريقة تعقيد حسابي أقل أي تتطلب موارد حسابية أقل مما يؤدي إلى انخفاض متطلبات وتكاليف التطبيق.

السلبيات: (Suresh,2020)

مع هذه الإيجابيات هنالك بعض السلبيات لهذه الطريقة هي ازدياد طول الخوارزمية مما يؤدي إلى زيادة تعقيد التنفيذ والأمر الذي يتطلب موارد إضافية، وأنها حساسة للقنوات المشوشة مما يجعلها أقل فعالية في البيئات التي تمتلك مستويات عالية من التشويش، وإمكانية تصحيح الأخطاء يمكن أن تتأثر في القنوات المشوشة.

إيجابيات وسلبيات فك ترميز ريد ميلر من المرتبة الأولى باستخدام مصفوفات هادامارد:

الإيجابيات: (Doan, 2022)

توفر طريقة هادامارد قدرة عالية على تصحيح الأخطاء الذي يؤدي إلى نقل أكثر موثوقية للبيانات مما يقلل من فرص فقدان البيانات أو تلفها مما يجعلها خيار موثوق لأنظمة الاتصالات التي تتعرض للأخطاء.

كما أنه يتوافق مع أنظمة الاتصالات الحالية مما يسهل اندماجه دون الحاجة إلى تعديلات كبيرة.

السلبيات: (Li,2022)

على الرغم من كفائتها وقدرتها العالية على تصحيح الأخطاء إلا أن التنفيذ يكون معقداً مما يتطلب المزيد من الموارد الحسابية أي ذاكرة وتخزين أكبر مما يجعلها غير مناسبة للتطبيقات ذات الموارد المحدودة، وزيادة العمليات الحسابية يؤدي إلى تباطُئ في عملية فك الترميز.

التعقيد الحسابي: (Yatribi,2020) ; (Doan,2022)

طريقة فك الترميز باستخدام منطق الأغلبية: تتميز هذه الطريقة بتعقيد حسابي منخفض لأنها تتطلب عمليات أساسية ومنطقية وبالتالي يكون تعقيدها الحسابي $\boldsymbol{O(n)}$ حيث يمثل $\boldsymbol{n}$ طول كلمة الترميز أو عدد البتات في الرسالة المستلمة.

طريقة فك الترميز باستخدام مصفوفات هادامارد: إن لهذه الطريقة تعقيد حسابي مرتفع نسبياً بسبب استخدام عمليات المصفوفات وبالتالي يكون تعقيدها الحسابي $O(n^2)$ حيث يمثل n طول كلمة الترميز أو عدد البتات في الرسالة المستلمة.

المقارنة بين طريقتي فك ترميز ريد ميلر من المرتبة الأولى باستخدام منطق الأغلبية ومصفوفات هادامارد:

على الرغم من أن طريقة منطق الأغلبية نجحت في تصحيح أخطاء محدودة في البيانات المرمزة، إلا أن طريقة مصفوفات هادامارد قادرة على تصحيح عدد أكبر من الأخطاء مما يجعلها أكثر دقة.

من جهة ثانية تعتبر طريقة منطق الأغلبية أسرع من طريقة مصفوفات هادامارد، وذلك لقلة العمليات الحسابية التي تتطلبها طريقة منطق الأغلبية، لأن التعقيد الحسابي لها أقل من التعقيد الحسابي لطريقة مصفوفات هادامارد.

ومنه نجد أن الاختيار بين الطريقتين يعتمد على الأداء والموارد المتاحة أي التطبيقات التي تتطلب موارد محدودة وسرعة أكبر ستخدم طريقة منطق الأغلبية بينما التطبيقات التي تمتلك موارد عالية لا بد من استخدام طريقة هادامارد.

تم تمثيل المقارنة بين طريقتي فك ترميز ريد ميلر من المرتبة الأولى في الجدول الآتي:

الجدول(1) مقارنة بين طريقتي فك ترميز ريد ميلر من المرتبة الأولى

المعايير	طريقة منطق الأغلبية	طريقة مصفوفات هادامارد
البساطة والتنفيذ	سهل التنفيذ	صعبة نسبياً
السرعة والفعالية	سريع	بطيء
التعقيد الحسابي	منخفض	مرتفع نسبياً
تصحيح الأخطاء	قدرة محدودة	قدرة عالية
الكفاءة	منخفضة	عالية
وقت التنفيذ	$O(n)$	$O(n^2)$

6. الاستنتاجات والتوصيات (Discussion and Further Work):

التزايد الكبير لاستخدام أجهزة التكنولوجيا وعمليات الترميز المترافقة معها لحماية البيانات، أمرا يقودنا إلى تطوير عملية الترميز وفك الترميز. قمنا في هذا البحث بمقارنة بين طريقتي فك ترميز ريد ميلر من المرتبة الأولى والحصول على بعض الخصائص المهمة

لاختيار الطريقة الأنسب لعملية فك الترميز بما يتناسب بين المعايير ومتطلبات التطبيق وتحقيق أقصى استفادة ممكنة. بعد الدراسة البحثية التي قُدمت يمكن التحسين والقيام بوضع خوارزميات فك ترميز بديلة يُمكنها التعامل بفعالية مع رسائل أكبر ومعدلات خطأ أعلى. ستساهم هذه الأتجاهات البحثية المستقبلية في تطوير مجال فك ترميز ريد ميلر من المرتبة الأولى وتوسيع تطبيقاتها في مختلف المجالات.

المراجع (References):

1. Ayats,J and Phelps,K . (2005).On Reed-Muller And Related Quatenary Codes.
2. Bernal, J. and Simón,J. (2023). New advances in permutation decoding of first-order Reed-Muller codes.
3. Bernal, J. and Simón,J. (2018). Information sets from defining sets for Reed-Muller codes of first and second order.
4. Blahut, R. (2003). Algebraic Codes for Data Transmission.
5. Cooke,B. (1999). Reed_Muller Error Correcting Codes.
6. Doan,N. , Hashemi,SA. And Gross,WJ. (2022). Successive-cancellation decoding of Reed-Muller codes with fast Hadamard transform.
7. Doan,N. , Hashemi,SA. And Mondelli,M. (2022). Decoding Reed-Muller codes with successive code-word permutations.
8. Hoffman,D.Leonard,D. Lindner,C. Phelps,K. Rodger,C.and Wall,J. (1991).Coding Theory The Essentials.
9. Li,J. and Gross,W. (2022). Optimization and Simplification of PCPA Decoder for Reed-Muller Codes.
10. Lint,J. (1991). Introduction to Coding Theory.
11. Meyer,L. (2021). Coding and Decoding of Reed-Muller Codes.
12. Muller, D. (1954). Application of Boolean Algebra to Switching Circuit Design and to Error Detection.
13. Reed, I. (1954). A class of multiple-error-correcting codes and the decoding scheme.
14. Sudan,M. Guruswami,V.and Rudra,A. (2023). Essential Coding Theory.
15. Suresh,V. Love,D.and Rudra,A. (2020) .A Novel Systematic Representation of Reed-Muller Codes with an Application to Linear Block Feedback Encoding.
16. Yang,TY., Chen,H. and Chuang,CH. (2020) .Modified Majority Logic Decoding of Reed-Muller Codes for Channel Coding.
17. Yatribi,A. , Belkasmi,M. and Ayoub,F. (2020). Gradient-descent decoding of one-step majority-logic decodable codes.
18. Wicker,S.(1994).Error Control Systems.
19. الراشد، شوقي .(2014).الجبر الخطي(1).