Damascus University Journal for the Basic Sciences
Vol 42 No.2 (2026): 58 -75

مجلة جامعة دمشق للعلوم الأساسية
مجلد 42-عدد 2 (2026): 58- 75

دراسة مقارنة بين خوارزميات فك ترميز رموز الاختبار المتكافئ ذات الكثافة المنخفضة

أسامة أحمد العلي[1*]، أ.م.د. غصون أحمد عبد الكريم الجيرودي[2]

[1]طالب ماجستير، جامعة دمشق، كلية العلوم، قسم لرياضيات
osama22.ali@damascusuniversity.edu.sy،
[2]أستاذة مساعدة، جامعة دمشق، كلية العلوم، قسم الرياضيات.
ghussoun.aljeiroudi@damascusuniversity.edu.sy

الملخّص:

في عالم الاتصالات ونقل البيانات يلعب الترميز دوراً حيوياً في ضمان سلامة وفهم البيانات المرسلة. كما يتيح الترميز تحويل البيانات إلى شكل يمكن فهمه بطريقة أفضل والحفاظ على سلامتها أثناء الإرسال. وهناك أنواع مختلفة من الرموز تستخدم في سياقات متنوعة منها رموز الاختبار المتكافئ ذات الكثافة المنخفضة LDPC التي تشكل حلاً مبتكراً وفعالاً في تحسين جودة وأمان الاتصالات الرقمية مما يجعلها جزءاً أساسياً في علم تصحيح الأخطاء وتقنيات الاتصال الحديثة بحيث تستخدم في معايير الاتصال المتقدمة مثل Wi-Fi والجيل الخامس لتحسين سرعة واستقرار الاتصال. نقدم هذا البحث لتوضيح أهم معايير المقارنة بين خوارزميتي فك ترميز رموز الاختبار المتكافئ ذات الكثافة المنخفضة باستخدام طريقتي تقليب البتات (BF) ونشر المعتقد (BP) ومن هذه المعايير تصحيح الأخطاء وقناة الترميز والأداء والذاكرة.

الكلمات المفتاحية: الترميز، رموز الاختبار المتكافئ، بيان تانر، تقليب البتات(BF) ، نشر المعتقد(BP) ، الكثافة المنخفضة.

تاريخ الإيداع: 2024/02/12
تاريخ القبول: 2024/08/13

حقوق النشر: جامعة دمشق – سورية، يحتفظ المؤلفون بحقوق النشر بموجب الترخيص CC BY-NC-SA 04

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

Study comparing decoding algorithms for low-density parity-check codes

Osama Ahmed Al Ali [1*] Ghussoun Ahmed Abdul Alkarim Al-Jeiroudi [2]

[1] Master's student, Department of Mathematics, Faculty of Sciences,Damascus University, Syria.osama22.ali@damascusuniversity.edu.sy .

[2] Professor, Department of Mathematics, Faculty of Sciences, Damascus University, Syria. ghussoun.aljeiroudi@damascusuniversity.edu.sy

Abstract

In the world of telecommunications and data transmission, encoding plays a vital role in ensuring the safety and understanding of transmitted data. Encoding also allows data to be converted into a more understandable form and to be kept safe during transmission. There are different types of codes used in various contexts, including Low Density Parity Check (LDPC) codes, which provide an innovative and efficient solution for improving the quality and security of digital communications, making them an essential part of error correction and modern communication techniques. They are used in advanced communication standards such as Wi-Fi and 5G to improve the speed and stability of connections. This research aims to clarify the most important comparison criteria between two decoding algorithms for LDPC codes, using the Bit Flipping (BF) and Belief Propagation (BP) methods. These criteria include error correction, encoding channel, performance, and memory usage.

Received: 12/02/2024
Accepted: 13/08/2024

Copyright: Damascus University- Syria, The authors retain the copyright under a CC BY- NC-SA

Keywords: Coding, Low-density parity-check codes, Tannar Graph, Bit-Flipping Decoding(BF), Belief Propagation(BP).

1. المقدمة (Introduction): (Shannon,C., 1948)

قدم شانون [11] عام 1948 مقالة بعنوان "Mathematical Theory of Communication" وكانت هذه المقالة هي النواة لنظرية الترميز.

ولعل أكثر ما يثير الاهتمام هو إحدى النظريات التي تحدثت عن وجود مخططات ترميز تمكننا من إرسال واستقبال البيانات بدون أي أخطاء تقريباً عبر أي قناة وبأي حال من الأحوال لكن إثبات هذه النظرية يعتمد على رموز مبنية بشكل عشوائي ذات أطوال كتلة تتجه إلى اللانهاية وهي غير ممكنة عملياً بسبب تعقيدات الترميز وفك الترميز العالية جداً.

ولذلك منذ نشر تلك المقالة تكرست الجهود لبناء مخططات تحقق سعة القناة مع تعقيدات ترميز وفك ترميز منخفضة نسبياً.

وفي [6] عام 1996 تم إعادة اكتشاف رموز الاختبار المتكافئ ذات الكثافة المنخفضة LDPC التي قدمها جلاجر [3] عام 1963 والتي كانت من أفضل الرموز التي تقترب من سعة القناة بحيث استخدمت هذه الرموز خوارزميات فك ترميز بسيطة ومتكررة حيث أصبحت رموز LDPC هي الرموز المفضلة لتصحيح الأخطاء في الكثير من التطبيقات العملية مثل WiFi والتلفزيون الرقمي ولعل أبرز استخداماتها الفعالة في الوقت الحاضر هو استخدامها في تطوير شبكات الـ 5G نظراً لأدائها الاستثنائي في خوارزميات فك الترميز منخفضة التعقيد وهذا ما سوف نتناوله في هذه المقالة التي سنقدم فيها مقارنة حول بعض هذه الخوارزميات.

2. فكرة البحث وأهدافه (Idea and objectives):

تستخدم رموز الاختبار المتكافئ ذات الكثافة المنخفضة تقنيات فعالة للكشف عن الأخطاء في نقل البيانات وتصحيحها وذلك عن طريق تقليل عدد البتات الإضافية المستخدمة للتحقق من سلامة البيانات. ولعل أبرز هذه الطرق هي خوارزميات تقليب البتات ونشر المعتقد التي تعمل على تصحيح الأخطاء وفك الترميز. يدفعنا ذلك للعمل على توضيح هذه الطرائق وآلية عملها في تصحيح الأخطاء وفك الترميز بهدف معرفة أحسن طريقة واختيار أفضل الشروط حسب طبيعة التطبيقات المستخدمة.

3. مواد وطرائق البحث(Materials and Methods):

3-1 تعاريف أساسية (Basic Definitions):

3-1-1 الرمز الخطي (Linear Code): (Sudan et al., 2022,p.48)

ليكن لدينا العلاقة:

$$q = p^s$$

حيث p عدد أولي و $s \geq 1$ عدد صحيح.

$C \subseteq \mathbb{F}_q^n$ هي رمز خطي من الفضاء $\mathbb{F}_q^n$ من الطول n. إذا كانت C من البعد k والمسافة d فإننا نشير إليها $[n,k,d]_q$ أو بالشكل $[n,k]_q$.

2-1-3 **بوابة XOR (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

الشكل (1)

3-1-3 **المصفوفة المولدة ومصفوفة الاختبار المتكافئ (Generator and Parity Check Matrices):** (Sudan et al., 2022,p.49)

إذا كان C رمزاً خطياً $C = [n,k]_q$ فإنه يوجد مصفوفة G من البعد $k \times n$ تحقق: $C = \{x.G : x \in \mathbb{F}_q^k\}$

نسمي G المصفوفة المولدة لـ C.

إذا كان C رمزاً خطياً $[n,k]_q$ يوجد مصفوفة H من البعد $(n-k) \times n$ تحقق

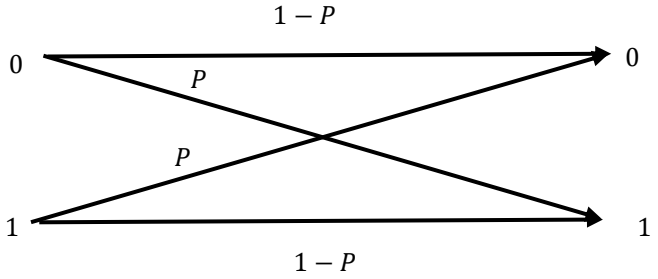
$$H.G^T = 0$$

نسمي H مصفوفة الاختبار المتكافئ لـ C.

4-1-3 **القناة الثنائية المتناظرة (Binary Symmetric Channel):** (Eleruja, 2021,p.61)

هي قناة ثنائية نشير إليها بـ (BSC) يتم فيها استكمال محارف الإدخال باحتمال p.

وهي أبسط نموذج للقناة التي تحتوي على أخطاء. عند حدوث خطأ يتم استلام 0 كـ 1 والعكس صحيح.

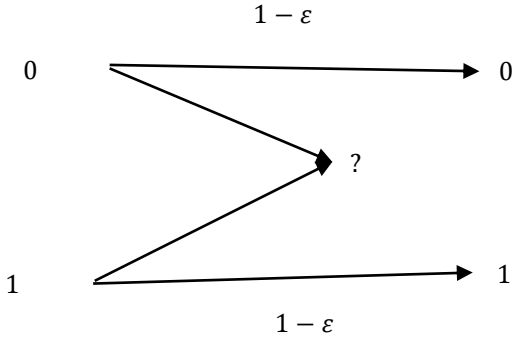


الشكل(2)

حيث P احتمال الخطأ وأن $(1 - P)$ احتمال الصح

3-1-5 **قناة المحو الثنائية (Binary Erasure Channel):** (Ivanov, 2022,p.2)

هي قناة محو ثنائية ذات احتمالية ε نشير اليها ب (BEC_ε)، ولها أبجدية مخراجات هي $y = x \cup \{?\}$ بحيث ان x هي الابجديه و ? هي عملية المحو التي حدثت اثناء الارسال بحيث ان احتمال $P(x|x) = 1 - \varepsilon$ هو انه اذا تم ارسال x واستلمنا x يكون $1 - \varepsilon$ اما الاحتمال $P(x|?) = \varepsilon$ فهو اذا أرسلنا x واستلمنا ? يكون الاحتمال هو ε .



الشكل(3)

3-1-6 **رمز الاختبار المتكافئ منخفض الكثافة (Low-density parity-check code (LDPC)):** (Johnson, 2015,p.10)

هو رمز خطي مع مصفوفة الاختبار المتكافئ متناثرة (معظم عناصرها أصفار هذا يعني أن عدد الواحدات في المصفوفة صغير جداً مقارنة مع عدد الأصفار).

3-1-7 **رموز الاختبار المتكافئ منخفض الكثافة المنتظمة:** (Johnson, 2015,p.11)

إن رمز LDPC هو $[d_v, d_c]$ – منتظم حيث أن d_c تمثل عدد الواحدات في كل سطر و d_v تمثل عدد الواحدات في كل عمود أي أن كل سطر وكل عمود له عدد ثابت من الواحدات حسب كلاً من d_v, d_c.

3-1-8 **بناء مصفوفة الاختبار المتكافئ منخفض الكثافة:**

هناك العديد من الطرق لبناء مصفوفة الاختبار المتكافئ منها طريقتي Gallager و MacKay Neal ومصفوفات التلقيب.

3-1-9 **طريقة جلاجر:** (Johnson, 2015,p.11)

هي الطريقة التي أوجدها روبرت جلاجر وتقوم هذه الطريقة على تقسيم المصفوفة الى مجموعات وتتكون الطريقة من الخطوات الآتية:

1- يتم تقسيم المصفوفة $\boldsymbol{H}$ إلى عدة مجموعات عددها هو $\boldsymbol{d_c}$

2- كل مجموعة تحتوي على أسطر عددها هو $\frac{\boldsymbol{m}}{\boldsymbol{d_c}}$.

3- نرتب الـ 1 في المجموعة الأولى من اليسار الى اليمين وعددها هو $\boldsymbol{d_r}$.

4- بقية المجموعات نجري تحويلات عمودية على المجموعة الأولى لنحصل عليها.

مثال:

$$H = \left[\begin{array}{cccccccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

ليكن لدينا الرمز المنتظم **[3,4]** من الطول 12:

لدينا هنا $\boldsymbol{d_c = 3}$ و $\boldsymbol{d_r = 4}$

$$\boldsymbol{m = n \cdot \frac{d_c}{d_r} = 12 \cdot \frac{3}{4} = 9}$$

تقسم المصفوفة الى 3 مجموعات كون $\boldsymbol{d_c = 3}$ وكل مجموعة منها تحتوي على 3 اسطر لأنه $\frac{\boldsymbol{m}}{\boldsymbol{d_c}} = \frac{\boldsymbol{9}}{\boldsymbol{3}} = \boldsymbol{3}$

نقوم بإدخال واحدات المجموعة الأولى من اليسار الى اليمين وعددها $\boldsymbol{d_r = 4}$.

3-1-10 رموز الاختبار المتكافئ منخفض الكثافة غير المنتظمة(Johnson, 2015,p.10):

هي رموز LDPC بحيث أن عدد الواحدات غير ثابت في الأسطر والأعمدة.

ملاحظة: إن بناء هذا الرمز يتم بطريقة عشوائية لأنه لا يوجد شرط على عدد الواحدات في الأسطر والأعمدة.

مثال: مصفوفة الاختبار المتكافئ لرمز هامينغ (7,4)

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

هي مصفوفة الاختبار المتكافئ لرمز هامينغ (7,4) وهي ناتجة من المصفوفة المولدة لرمز هامينغ ذات الابعاد 7×4 وهي تشكل مثالاً على مصفوفة الاختبار المتكافئ منخفض الكثافة غير المنتظمة لأنه يكفي أن يكون لدينا سطر واحد أو عمود واحد لا يملك نفس عدد الـ 1 في الاسطر أو الأعمدة الأخرى.

3-2 رموز الاختبار المتكافئ منخفض الكثافة LDPC:

3-2-1- البيان ثنائي التجزئة (Bipartite Graph): (Marcus, 2020,p.25)

هو رسم بياني يمكننا فصل عُقده إلى مجموعتين x, y بحيث لا يوجد أضلاع تربط عقد المجموعة بنفسها.

3-2-2- بيان تانر: (Alfarano et al., 2021,p.2240)

إن بيان تانر للرمز C مع مصفوفة الاختبار المتكافئ H من البعد $(\mathrm{n}-\mathrm{k}) \times n$ هو البيان الثنائي التجزئة $G(V_1, V_2, E)$ حيث أن:

V_1 يمثل عقد المتغيرات $v_1, \dots, v_n$ وعددها n كل منها يتوافق مع بت في الكلمة المرمزة x_i.

V_2 يمثل عقد التحقق $c_1, \dots, c_{n-k}$ وعددها n−k وكل منها يتوافق مع مجموعة التحقق من التكافؤ.

E يمثل الأضلاع التي تصل بين عقد المتغيرات v_i و عقد التحقق c_j إذا وفقط إذا كان $h_{ji} = 1$.

غالباً ما نمثل عقد المتغيرات في الرسم البياني لبيان تانر بالدوائر وعقد التحقق بالمربعات.

4. خوارزميات الاختبار المتكافئ منخفض الكثافة:

إن فهم خوارزميات تصحيح الأخطاء لرموز الاختبار المتكافئ ذات الكثافة المنخفضة تشمل دراسة العديد من الأساسيات الرياضية والتقنيات الحاسوبية ويعتمد ذلك على مفاهيم عديدة مثل تحليل الأداء وطرق تصحيح الأخطاء ولدينا العديد من خوارزميات تصحيح الأخطاء منها: تقليب البتات، ونشر المعتقد، تقليل المتغيرات وغيرها من الطرق الأخرى. سنتناول في دراستنا طريقتي تقليب البتات ونشر المعتقد.

4-1- خوارزمية تقليب البتات (Bit-Flipping Decoding): (Ntuli, 2013,p.51)

لدينا العديد من طرق فك الترميز لرموز LDPC وقد اقترح جلاجر هذه الخوارزمية التي تنطبق على فك ترميز الرموز الثنائية كما اقترح استخدام هذه الخوارزمية في القناة الثنائية المتناظرة (BSC) بمعدلات خطأ منخفضة جداً.

خطوات الخوارزمية:

1. نوجد جميع مجموعات الاختبار المتكافئ للمصفوفة H (التي هي عبارة عن عملية XOR لجميع الـ 1 في كل سطر على حدا من أسطر المصفوفة).
2. بعد تلقي الكلمة المرسلة نقوم بحساب مجموعات الاختبار المتكافئ لهذه الكلمة.
3. إذا كانت جميع مجموعات الاختبار المتكافئ محققة فإنه لا يوجد أخطاء، أما إذا كانت إحدى هذه المجموعات غير محققة يكون لدينا خطأ.
4. لتحديد مكان الخطأ نقوم بأخذ البت الأكثر تكراراً في المجموعات غير المحققة ثم نقوم بقلب هذا البت.

إذا كان لدينا أكثر من خطأ والبتات المحتملة لها نفس التكرار ونفس عدد المجموعات غير المحققة نقوم بقلب أحد البتين إذا تم التصحيح تم المطلوب والإ نقوم بقلب البت الثاني أي بطريقة عشوائية تجريبية للحصول على التصحيح.

5. نعيد حساب مجموعات الاختبار إذا كانت محققة فقد تم تصحيح الخطأ أما إذا لم يكن كذلك نعيد تكرار الخطوة 4 حتى يتم تصحيح جميع الأخطاء.

مثال:

بفرض لدينا الكلمة المرسلة الآتية:

$$x = \{00000011111110101100\}$$

والكلمة المستلمة هي

$$y = \{10000011111110101100\}$$

وفق مصفوفة الاختبار المتكافئ ذات الكثافة منخفضة الآتية:

$$n = 20, d_c = 4, d_v = 3$$

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

باستخدام خوارزمية تقليب البتات سوف نحاول تصحيح الخطأ.

1. من خلال المصفوفة H نوجد مجموعات الاختبار المتكافئ

#	مجموعات التكافؤ
c_1	{1,2,3,4}
c_2	{5,6,7,8}
c_3	{9,10,11,12}
c_4	{13,14,15,16}
c_5	{17,18,19,20}
c_6	{1,5,9,13}
c_7	{2,6,10,17}
c_8	{3,7,14,18}
c_9	{4,11,15,19}
c_{10}	{8,12,16,20}
c_{11}	{1,6,12,18}
c_{12}	{2,7,11,16}
c_{13}	{3,8,13,19}
c_{14}	{4,9,14,17}
c_{15}	{5,10,15,20}

2. نتحقق من مجموعات الاختبار المتكافئ للكلمة المستلمة إذا كانت جميعها محققة أم لا.

ملاحظة: تتم عمليات التحقق باستخدام XOR.

c_i	العمليات	النتيجة
c_1	$1+0+0+0=1$	غير محققة
c_2	$0+0+1+1=0$	محققة
c_3	$1+1+1+1=0$	محققة
c_4	$1+0+1+0=0$	محققة
c_5	$1+1+0+0=0$	محققة
c_6	$1+0+1+1=1$	غير محققة
c_7	$0+0+1+1=0$	محققة
c_8	$0+1+0+1=0$	محققة
c_9	$0+1+1+0=0$	محققة
c_{10}	$1+1+0+0=0$	محققة
c_{11}	$1+0+1+1=1$	غير محققة
c_{12}	$0+1+1+0=0$	محققة
c_{13}	$0+1+1+0=0$	محققة
c_{14}	$0+1+0+1=0$	محققة
c_{15}	$0+1+1+0=0$	محققة

إن c_1, c_6, c_{11} غير محققة وبما أن البت 1 مشترك بين المجموعات الثلاثة فهناك احتمال قوي أنه هو الخطأ.

3. نقلب البت المستقبل الأول فتصبح الكلمة بعد قلب البت $y = \{00000011111110101100\}$

4. نقوم بالتحقق من مجموعات الاختبار المتكافئ للكلمة المستلمة بعد قلب البت فتكون كالآتي:

c_i	العمليات	النتيجة
c_1	$0+0+0+0=0$	محققة
c_2	$0+0+1+1=0$	محققة
c_3	$1+1+1+1=0$	محققة
c_4	$1+0+1+0=0$	محققة
c_5	$1+1+0+0=0$	محققة
c_6	$0+0+1+1=0$	محققة
c_7	$0+0+1+1=0$	محققة
c_8	$0+1+0+1=0$	محققة
c_9	$0+1+1+0=0$	محققة
c_{10}	$1+1+0+0=0$	محققة
c_{11}	$0+0+1+1=0$	محققة
c_{12}	$0+1+1+0=0$	محققة
c_{13}	$0+1+1+0=0$	محققة
c_{14}	$0+1+0+1=0$	محققة
c_{15}	$0+1+1+0=0$	محققة

نلاحظ بأن جميع مجموعات الاختبار المتكافئ محققة أي تم تصحيح الخطأ.

5. يتم فك ترميز الرسالة المستلمة بعد تصحيح الخطأ.

مثال (رسالة تحتوي على خطأين):

بفرض لدينا الكلمة المرسلة الآتية:

$$x = \{00000011111110101100\}$$

والكلمة المستلمة هي

$$y = \{11000011111110101100\}$$

وفق مصفوفة الاختبار المتكافئ ذات الكثافة منخفضة الآتية:

$$n = 20, d_c = 4, d_v = 3$$

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

باستخدام خوارزمية تقليب البتات سوف نحاول تصحيح الأخطاء في الرسالة المستلمة.

1. نوجد مجموعات الاختبار المتكافئ

#	مجموعات التكافؤ
c_1	{1,2,3,4}
c_2	{5,6,7,8}
c_3	{9,10,11,12}
c_4	{13,14,15,16}
c_5	{17,18,19,20}
c_6	{1,5,9,13}
c_7	{2,6,10,17}
c_8	{3,7,14,18}
c_9	{4,11,15,19}
c_{10}	{8,12,16,20}
c_{11}	{1,6,12,18}
c_{12}	{2,7,11,16}
c_{13}	{3,8,13,19}
c_{14}	{4,9,14,17}
c_{15}	{5,10,15,20}

2. نتحقق من مجموعات الاختبار المتكافئ للكلمة المستلمة إذا كانت جميعها محققة أم لا.

c_i	العمليات	النتيجة
c_1	$1+1+0+0=0$	محققة
c_2	$0+0+1+1=0$	محققة
c_3	$1+1+1+1=0$	محققة
c_4	$1+0+1+0=0$	محققة
c_5	$1+1+0+0=0$	محققة
c_6	$1+0+1+1=1$	غير محققة
c_7	$1+0+1+1=1$	غير محققة
c_8	$0+1+0+1=0$	محققة
c_9	$0+1+1+0=0$	محققة
c_{10}	$1+1+0+0=0$	محققة
c_{11}	$1+0+1+1=1$	غير محققة
c_{12}	$1+1+1+0=1$	غير محققة
c_{13}	$0+1+1+0=0$	محققة
c_{14}	$0+1+0+1=0$	محققة
c_{15}	$0+1+1+0=0$	محققة

إن c_6, c_7, c_{11}, c_{12} غير محققة أي يوجد بها أخطاء مشتركة نلاحظ بأن البتات المشتركة بين المجموعات هي البت الأول والثاني والسادس لتحديد البتات الخطأ نقوم بمقارنة المجموعات التي تحوي على بتات الخطأ ونأخذ الغالبية بينها فنلاحظ بأن البت الأول موجود في المجموعات {1,6,11} والبت الثاني موجود في {1,7,12} والبت السادس موجود في {2,7,11} فنلاحظ بأن المجموعة الأولى مشتركة بين البت الأول والثاني وهي محققة فهناك احتمال قوي بأن الخطأ موجود في البت الأول والثاني.

بقلب البت الأول والثاني من ال1 إلى 0 ،نقلب البت المستقبل الأول والثاني فتصبح الكلمة بعد قلب البت

$$y = \{00000011111110101100\}$$

نقوم بالتحقق من مجموعات الاختبار المتكافئ للكلمة المستلمة بعد قلب البت فتكون كالآتي:

c_i	العمليات	النتيجة
c_1	$0+0+0+0=0$	محققة
c_2	$0+0+1+1=0$	محققة
c_3	$1+1+1+1=0$	محققة
c_4	$1+0+1+0=0$	محققة
c_5	$1+1+0+0=0$	محققة
c_6	$0+0+1+1=0$	محققة
c_7	$0+0+1+1=0$	محققة
c_8	$0+1+0+1=0$	محققة
c_9	$0+1+1+0=0$	محققة
c_{10}	$1+1+0+0=0$	محققة
c_{11}	$0+0+1+1=0$	محققة
c_{12}	$0+1+1+0=0$	محققة

محققة	$0+1+1+0=0$	c_{13}
محققة	$0+1+0+1=0$	c_{14}
محققة	$0+1+1+0=0$	c_{15}

نلاحظ بأن جميع مجموعات الاختبار المتكافئ محققة أي تم تصحيح الخطأ، يتم فك ترميز الرسالة المستلمة بعد تصحيح الخطأ.

4-2- **خوارزمية نشر المعتقد (Belief Propagation):** (Onverwagt, 2023,p.27)

هناك طريقة أخرى لفك ترميز رموز LDPC، هذه الخوارزمية تعتمد على قناة المحو الثنائية (BEC).

خطوات الخوارزمية:

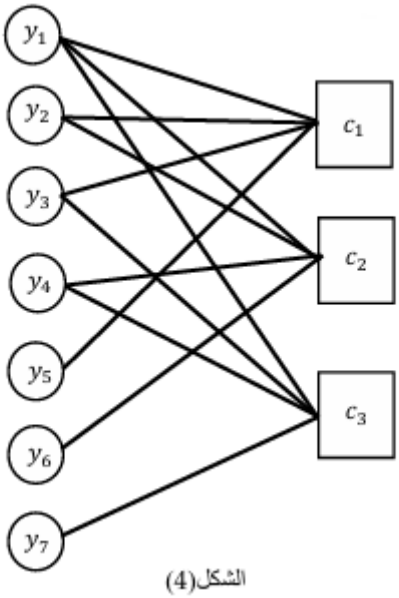
1. التهيئة:(Initialization)
   - يتم تهيئة جميع عقد المتغيرات بالقيم المستلمة y_i من القناة.
   - ترسل كل عقدة المتغير قيمتها عبر جميع الاضلاع المرتبطة بها إلى عقد التحقق.
2. تحديث عقد التحقق:(Check Nodes Updates)
   - تقوم كل عقدة تحقق بحساب الرسائل المرسلة إلى عقد المتغيرات بناءً على الرسائل المستلمة من عقد المتغيرات الأخرى.
   - إذا كانت جميع الرسائل المستلمة غير محذوفة (0 أو 1)، تقوم عقدة التحقق بحساب الرسالة الصادرة كمجموع XOR لجميع الرسائل المستلمة الأخرى.
   - إذا كانت أي رسالة مستلمة محذوفة (؟)، تقوم عقدة التحقق بإرسال رمز المحو (؟).
3. تحديث عقد المتغيرات:(Variable Nodes Updates)
   - تقوم كل عقدة المتغير بحساب الرسائل المرسلة إلى عقد التحقق بناءً على الرسائل المستلمة من عقد التحقق الأخرى.
   - إذا كانت جميع الرسائل المستلمة من الاضلاع الأخرى محذوفة (؟)، تقوم عقدة المتغير بإرسال رمز المحو (؟).
   - إذا كانت هناك أي رسالة غير محذوفة، تقوم عقدة المتغير بإرسال تلك الرسالة.
4. الإنهاء:(Termination)
   - إذا تم استعادة جميع عقد المتغيرات (أي لا توجد أي عقدة المتغير تحتوي على رمز المحو)، يتم إيقاف الخوارزمية.
   - إذا كانت هناك عقد المتغيرات لا تزال تحتوي على رمز المحو (؟)، يتم العودة إلى خطوة 3 لمواصلة عملية التحديث.

مثال: ليكن لدينا $x=[0,1,1,1,0,0,0]$ هي الكلمة المرسلة المرمزة باستخدام رمز هامينغ $(7,4)$

ولتكن لدينا $y=[0\ ?\ ?\ 1\ 0\ ?\ 0]$ هي الكلمة المستلمة عبر القناة ***BEC*** ولتكن لدينا مصفوفة الاختبار المتكافئ الموافقة لهذا الرمز

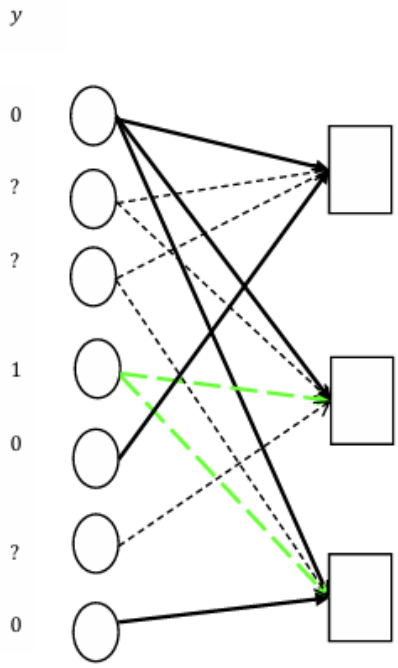
$$H=\begin{bmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\1&0&1&1&0&0&1\end{bmatrix}$$

فيكون بيان تانر الموافق لهذه المصفوفة بالشكل:



الشكل(4)

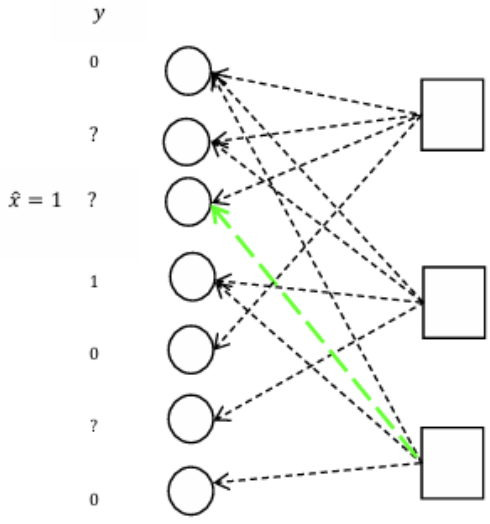
ملاحظة: سوف نشير لـ 0 بخط أسود وَ ? بخط متقطع وَ 1 بخط أخضر متقطع عريض.



الشكل(5)

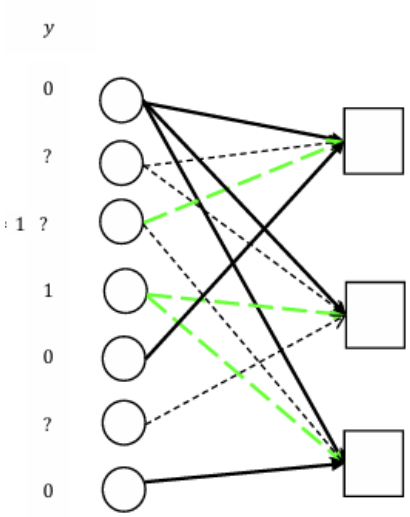
الخطوة الأولى: تهيئة جميع عقد المتغيرات بالقيمة المستلمة.

ترسل كل عقدة المتغير قيمتها.



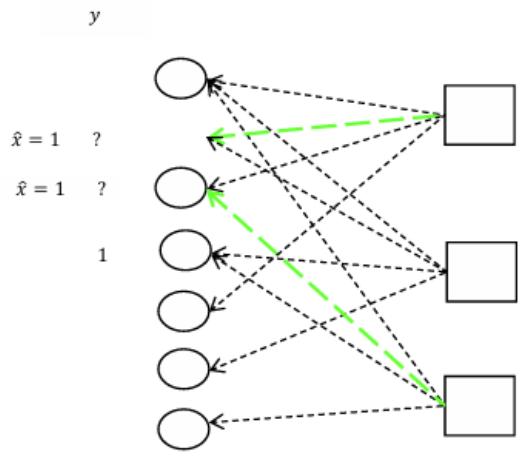
الشكل(6)

الخطوة الثانية: تحديث عقد التحقق بعد أن تلقت عقد التحقق الرسائل من عقد المتغيرات نلاحظ أنه قد وصل إلى c_1, c_2 محوين ووصل إلى c_3 محو واحد فهنا لا يمكننا تصحيح المحوين في c_1, c_2 لكن يمكننا تصحيح المحو في c_3 كما يلي:



الشكل(7)

الخطوة الثالثة: تحديث عقد المتغيرات نقوم بإرسال القيم من عقد المتغيرات ونقوم بإعادة توجيه القيمة المرسلة من c_3 إلى y_3 لتصبح من y_3 إلى c_2.



الشكل(8)

الخطوة الرابعة: نلاحظ أنه لم يتم تصحيح جميع الأخطاء فنقوم بتكرار الخطوة 2 مرة ثانية.

نلاحظ بعد تحديث عقد المتغيرات أصبح بإمكاننا تصحيح المحو في c_1 كما يلي:

وأصبحت الكلمة المستلمة بالشكل:

$$\hat{x} = (y_1, \hat{x}_2, \hat{x}_3, y_4, y_5, \hat{x}_6, y_7) = (0,1,1,1,0,0,0)$$

ويمكننا التأكد من صحتها بالشكل:

$$H.\hat{x}^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} . \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

5. النتائج والمناقشة:(Results and Discussion)

بعد التحليل والمقارنة لطريقتي فك ترميز LDPC باستخدام طريقة نشر المعتقد وطريقة تقليب البتات، نبين نتائج المقارنة بينهما.

معايير مقارنة بين طريقتي فك الترميز:

1. قناة الترميز:

إن طريقة تقليب البتات تستخدم قناة (BSC) وطريقة نشر المعتقد تستخدم قناة (BEC).

2. الأداء:

طريقة نشر المعتقد تقدم أداء أفضل من طريقة تقليب البتات لتصحيح الأخطاء وخاصة لطول الكتلة الأكبر، كما أنه يقترب من الأداء الأمثل وفقاً لحد شانون، بينما طريقة تقليب البتات فهي بسيطة وسريعة ولكنها قد لا تكون دقيقة دائماً.

3. التعقيد:

تكون تقليب البتات أقل تعقيداً حسابياً مقارنة بـ نشر المعتقد. حيث نشر المعتقد يحوي عمليات أكثر تعقيداً لنقل الرسائل وتحديثها ولكنها تكون أكثر دقة.

4. تصحيح الأخطاء:

تقليب البتات تصحيح أكثر من خطأ في نفس مجموعة التكافؤ. بينما نشر المعتقد لا يصحح أكثر من خطأ في نفس مجموعة التكافؤ.

5. الذاكرة:

تقليب البتات تتطلب ذاكرة أقل مقارنة بـ نشر المعتقد مما يجعلها مناسبة للتطبيقات ذات الموارد المحدودة، بينما نشر المعتقد تتطلب ذاكرة إضافية نظراً لتبادل الرسائل وحسابات الاحتمالات.

إن الاختيار بين طريقتي تقليب البتات ونشر المعتقد تعتمد على متطلبات النظام بما في ذلك سرعة الترميز وقيود الأجهزة والمستوى المرغوب من أداء تصحيح الأخطاء والتكلفة. في المجالات العملية نلاحظ تميز كل من الخوارزميتين حسب بيئة العمل ونرى ان نشر المعتقد أفضل من تقليب للبتات لكن ليس بشكل مطلق بسبب تفوق خوارزمية تقليب البتات من ناحية الذاكرة المطلوبة والتعقيد الحسابي.

الجدول (1) مقارنة بين طريقتي فك ترميز LDPC

المعايير	تقليب البتات	نشر المعتقد
قناة الترميز	BSC	BEC
السرعة	سريع	بطيء
الأداء	أقل أداء	أفضل أداء
الدقة	أقل دقة	أكثر دقة
التعقيد الحسابي	أقل	أكثر
تصحيح الأخطاء	تصحيح أكثر من خطأ	تصحيح خطأ واحد
الذاكرة	تتطلب ذاكرة أقل	تتطلب ذاكرة إضافية

الاستنتاجات والتوصيات (Discussion and Further Work):

في الختام، تظهر رموز الاختبار المتكافئ ذات الكثافة المنخفضة LDPC أنها تقنية متطورة وحيوية في ميدان تصحيح الأخطاء وتحسين جودة الاتصالات الرقمية من خلال تصميمها الفريد وفعاليتها العالية في عمليات الترميز وفك الترميز كما تعزز الاستقرار والأداء العالي في نقل البيانات.

لقد قمنا في هذا البحث بتقديم مقارنة بين خوارزميتي نشر المعتقد وتقليب البتات لفك ترميز رموز الاختبار المتكافئ ذات الكثافة المنخفضة LDPC . وبينا أن طريقة نشر المعتقد هي الأفضل بحسب معايير المقارنة.

لذلك نحاول انطلاقاً من هذا البحث تطبيق هذه الخوارزميات على أنواع رسوم بيانية جديدة، كما يمكننا العمل على تطوير هذه الخوارزميات لجعلها تتناسب مع بيئة عمل محددة لتكون أكثر جودة وسرعة في الأداء.

المراجع(References):

1. Alfarano,G. , Lieb,J. And Rosenthal,J. (2021). Construction of LDPC Convolutional Codes Via Difference Traingle Sets. Institute of Mathematics, University of Zurich.
2. Eleruja,S. (2021). Binary LDPC Design for Slepian-Wolf Coding of Correlated Information Sources. (Doctoral dissertation, University of Plymouth).
3. Gallager,R,G.(1963). Low-Density Parity-Check Codes. IEEE Transactions on Information Theory.
4. Ivanov, K. (2022). Symmetry in Design and Decoding of Polar-Like Codes. (Doctoral dissertation, EPFL).
5. Johnson,S. (2015).Introducing Low-Density Parity-Check Codes. The University of New Castle Australia.
6. MacKay,D. and Neal,R.(1996). Near shannon Limit Performance of Low-Density Parity check codes. Electronics Letters.
7. Marcus, D. (2020). Graph Theory A Problem Oriented Approach. The Mathematical Association of America.205.
8. Mathews,R. (2020).Decoding LDPC codes with Probabilistic Local Maximum Likelihood Bit Filpping. (Master's Thesis, Utah State University).
9. Ntuli,S. (2013). Bit Flipping Decoding for Binary Product Codes.(Master's Thesis, University of The Wit-Watersrand).
10. Onverwagt, H. .(2023). Irregular LDPC Code Design using Large Girth Tanner Graphs. (Master's Thesis, Universiteit Utrecht).
11. Shannon,C. (1948).A Mathematical Theory of Communication. The Bell System Technical Journal, 27,379-423.
12. Sudan,M. Guruswami,V.and Rudra,A. (2022). *Essential Coding Theory*. University at Buffalo.473.
13. Zemor,G. And Leverrier,A. (2022).Decoding quantum Tanner codes. IEEE Transactions on Information Theory.