المعلومات والترميز

السنة : الخامسة

القسم : هندسة الالكترونيات والاتصالات

منشورات جامعة دمشق

كلية الهندسة الميكانيكية والكهربائية

المعلومات والترميز

Information and coding

تأليف

الدكتور المهندس
سمير كرمان
أستاذ مساعد في قسم هندسة الحواسيب والأتمتة

الدكتور المهندس
عادل خضور
مدرس في قسم هندسة الالكترونيات والاتصالات

جامعة دمشق

1437 – 1438
2016–2017

وقل رب زدني علما
جامعة دمشق
Damascus University

المحتويات

مقدمة

تعتمد نظرية المعلومات كغيرها من العلوم على المعادلات و النماذج الرياضيات لوضع قواعد قوية وراسخة، وهذا مما رسخ أسسها بين جميع العلوم في مجال علوم الحواسيب والاتصالات، وهي تصنف كفرع من علوم (Theoretical Computer Science) و كفرع في الرياضيات التطبيقية.

في سنة 1883 كان اكتشاف شفرة مورس من قبل العالم صامويل مورس مظهرا من مظاهر التطور في عملية الاتصال، ومدخلا غير مباشر لعلم ضغط البيانات كوسيلة لتسريع عملية الإرسال، إن القيود الطبيعية التي تشوب عملية الإرسال أو الاتصال من بطء وقابلية للضياع يستدعي الحاجة إلى تغيير الترميز وذلك بترميز آخر أقل حجما ويحمل المعلومات نفسها، مما سيسرع من عملية الإرسال ويقلل من احتمال الضياع و ورود الأخطاء.

في سنة 1948 نشر شانون بحثا هاما بعنوان النظرية الرياضية للاتصالات (A Mathematical Theory of Communication) وكان الأساس في بناء نظرية المعلومات، ومما يجب أن نشير إليه أن شانون لم يكن وحده الرقم الصعب في نظرية المعلومات بل كان هنالك من العلماء الذين نشروا أبحاثا أسهمت في تطوير هذه النظرية من بينهم نكويست في بحثه الذي تحدث فيه عن العوامل المؤثرة في سرعة التيليغراف (Certain factors affecting telegraph speed) وبحثه الثاني (Certain Topics in Telegraph Transmission Theory)

في سنة 1951 وذلك بعد اكتشاف ترميز شانون- فانو (Shannon–Fano coding) قام دافيد هوفمن (David A. Huffman) بطرح (Huffman Encoding) وهي طريقة لإيجاد أقصر تمثيل بحيث يكون (Optimal prefix–

(code وهو تمثيل يكون فيه(Code-words) أو المخرجات المضغوطة Compressor ليس لها علاقة ببعض اي لا تكون (prefix of each other) وبالتالي هذا سيضمن عملية (Decoding) بطريقة غير ملتبسة، وقد اعتمد هوفمن على البنية الشجرية (Trees Data Structure) كبنية تساعد في هذه العملية، بالإضافة إلى التوزيع الإحصائي للحروف أو ما يسمى بـ (Frequency of Occurrence) ليحديد إلمن يسند الترميز الأقصر وكان بعده وقبله ممن اسسوا لهذا العلم ومنهم (Leon G. Kraft) المعروف بـ (Kraft's inequality) والتي تحدد إمكانية وجود (uniquely decodable code) لأطوال Code-Words محددة، وهي تحدد بطريقة أخرى إمكانية وجود(Prefix-Code)لأطوال محددة.

إن الاعتماد على مفهوم التكرار و الاحتمالية و الإحصاء أنشأ ما يسمى بـ (Statistical Data Compression Approaches) لكن هذا النوع من ضغط البيانات يحتاج إلى موارد كبيرة وإلى وقت معين لإجراء عمليات الحساب و الضغط، وبالتالي بقي هذا العلم بعيدا عن البداهة و التلقائية في استثمار (Redundancy) أو التكرار وكيفية التغلب عليه.

لكن في سنة 1977 جاء (JACOB ZIV) و (ABRAHAM LEMPEL) واقترحوا نموذجا بسيطا جدا والذي سمي بعدها بـ (Dictionary-Based Compression Approaches) القاموس القائم على ضغط المناهج وكان من البداهة بمكان، مما جعله ينتشر بكثرة ويستعمل في أنظمة الفاكس و المودمات.

مما احتوته نظرية المعلومات وأدخله شانون إلى قاموس الاتصالات مفهوم القنوات ذات الضجيج (Noisy channels) و الذي أسست لـ Coding Theory الذي ساهم في تطور Error Correcting Codes و الذي كان من أشهرها Hamming code .

في حين أنه أُدخل مفهوم عجيب جدا وقوي في الوقت نفسه يستعمل في قياس (متوسط كمية المعلومات الموجودة في رسالة ما) وهذا ما سمي بأنتروبيا شانون أو (Shanon Entropy) و الذي كان له تأثير كبير في مجال ضغط البيانات خاصة ضغط البيانات دون ضياع (Lossless Compression) حيث تعبر الأنتروبيا عن القيمية الحقيقية أو الدنيا الذي يمكن أن تسند لترميز ما. لقد كان ومازال ضغط البيانات من أهم الفروع في علوم الكمبيوتر الذي أنتجته نظرية المعلومات، والذي كان له دور فاعل في تسريع عملية الاتصال، وحتى عملية أرشفة الملفات وتخزينها، فالحاجة الطبيعية التي كانت تفرضها الآلة في ذلك الوقت من قلة في السرعة ونقص في وسائط التخزين استدعى اكتشاف تقنيات تساعد في الوصول إلى هذا الهدف.

باختصار فإن ضغط البينات هو:

"The art of representing Data in Compact Form"

قد يصحب عملية الضغط ضياع في البيانات وذلك ما نسميه بـ (Pressure loss of data) وهذا لا يؤثر بشكل كبير في البيانات، مثال: ضغط الصور، ضغط الصوت، او الفيديو، فالتغيير في بيكسل واحد من الآلاف من البكسلات لن يؤثر في الصورة أو استبدال مجموعة من البكسلات بالمتوسط الحسابي لهم لن يؤثر، فغالبا ما يستثمر هذا النوع من الضغط ضعف الحس البصري أو السمعي لدى الإنسان في تمييز الفروق الضئيلة. قد يصحبها عدم ضياع في البيانات والذي نسميه (Lossless data compression) وهذا غالبا يكون في ضغط النصوص فلا يمكن أن تضغط كلمة "Printf" و بعد فك الضغط تصبح كلمة أخرى وبالتالي تضغط شفرة مصدرية وتنتج شفرة مصدرية أخرى، وهذا التقسيم أدى إلى توسع أكثر وإنتاج

غزير في علم ضغط البيانات.

تـم إعـداد كتـاب نظريـة المعلومـات والترميـز وفـق مفـردات مقـرر نظريـة المعلومـات والترميـز لطـلاب السـنة الخامسـة فـي قسـم هندسـة الالكترونيـات والاتصالات، وهي تشمل:

المعلومات المنفصلة

ترميز المنبع

منبع المعلومات المتقطع مع الذاكرة

ترميز القنوات ذات الضجيج

الترميز الدوري

الترميز الانطوائي

راعينا عند إعداد الكتاب التغطية " المضغوطة" للأسس التي تعتمد عليها نظريـة المعلومـات والتوضـيح الـوافي نسـبياً للمفـاهيم والأسـس التـي تعتمـد عليهـا النظريـات الحديثـة لنظريـة المعلومـات والترميـز، ويفضـل الاسـتفادة مـن المراجـع المذكورة في نهاية الكتاب وغيرها من مراجع نظرية المعلومات والترميز من أجل المزيد من التعمق والتوسع.

نطمح أن يكون هذا الكتاب عوناً للطلاب الأعزاء، ومرجعاً غنياً لزملائنا المهتمين في الاتصالات والحواسيب ، كما نأمل أن يكون خير رافد لمكتبتنا العربية في هذا الموضوع، وقد بذلنا فيه من الجهد ما يجعله سهل التناول ومحكم التبويب ولائقاً بالمكانة العلمية لجامعة دمشق العريقة.

وأخيراً لا بدّ من تقديم الشكر الجزيل إلى المقومين العلميين: الأستاذ الدكتور المهندس نديم شاهين، والأستاذ المساعد الدكتور المهندس خالد شاهين، والدكتور المهندس محمد ميهوب، والشكر موصول إلى المدقِّق اللُّغويّ: الدكتور حمود يونس والى كل من ساهم في طباعة ونشر هذا الكتاب .

نأمل أن نكون قد وُفقنا في بعض ما سعينا إليه، وكلنا أمل أن يحقق هذا الكتاب الفائدة المرجوة، والله ولي التوفيق.

وقل رب زدني علما
جامعة دمشق
Damascus University

الفصل الأول

المعلومات المتقطعة

The discrete information

وقل رب زدني علما
جامعة دمشق
Damascus University

الفصل الأول

المعلومات المتقطعة

The discrete information

1-1 أصل نظرية المعلومات:

يستخدم مفهوم المعلومات في حياتنا العملية بشكل متكرر وفي الكثير من المواقف بحيث من الصعب إعطاء المعنى الدقيق والمبسط لهذا المفهوم ، لكن بشكل عام يمكن أن نقول أن المعلومات هي مجموعة من الخصائص أو المظاهر المرافقة لأي خبر ، ظاهرة أو كائن بينما نظرية المعلومات هي العلم الذي يتعامل مع مفهوم "المعلومات " ، قياسها وتطبيقاتها.

من الناحية العامة هناك ثلاثة أنواع من المعلومات :

- المعلومات النحوية Syntactic information:وهي تتعلق بالرموز التي تتشكل منها الرسائل والعلاقات المتبادلة فيما بينها.

-المعلومات اللفظية Symantec information:وهي تتعلق بمعنى الرسائل وشكلها المرجعي.

- المعلومات الواقعية Pragmatic information:وهي تتعلق باستخدام وأثر هذه الرسائل.

ومن هنا فإن المعلومات النحوية تعتمد على شكل المعلومات ،بينما تتعلق المعلومات اللفظية والواقعية بمحتوى المعلومات نفسها. وقد حاول العالم كلود شانون في مقالته " النظرية الرياضية للاتصالات" المنشورة في عام 1948 استناداً إلى الجوانب النحوية للمعلومات استنتاج المعادلة الناظمة للاستغلال الفعال لأنظمة الاتصالات. وقد كان قبله العالم نايكويست 1924 يتساءل عن كيفية إرسال

الحروف (الرسائل، الرموز ، الكلمات)عبر قنوات الاتصال بأكبر سرعة ممكنة من دون حصول فقد في المعلومات. بينما يعد العالم هارتلي أول من وضع تعريفاً كمياً للمعلومات 1928 استناداً إلى مفاهيم بديهية.

1 – 2 القياس الكمي للمعلومات:Measure of Information

1 – 2 – 1 مقياس كمية المعلومات بالفطرة:

Common-Sense Measure of Information

لتوضيح هذا المفهوم نفرض ظهور عناوين إحدى الصحف الرئيسية على الشكل التالي:

1. غداً سوف تشرق الشمس من الشرق
2. الولايات المتحدة تغزو كوبا
3. كوبا تغزو الولايات المتحدة

سينظر القارئ إلى الخبر الأول على انه بديهي ومن دون أي قيمة. بينما سيشده الخبر الثاني أو الثالث ،وقد يكون الخبر الثالث الأكثر غرابة وغير متوقع.لذلك نعرف بالفطرة أن الخبر الأول لا يحمل أي كمية من المعلومات لأنه لن يزيد من مخزون المعرفة لدينابينما يقدم الثاني كمية كبيرة من المعلومات ، والخبر الثالث يقدم على الأغلب أكبر كمية من المعلومات. فإذا نظرنا إلى احتمال حدوث هذه الأحداث نجد أن احتمال الحدث الأول هو الواحد والحدث الثاني أقل بكثير بينما احتمال الحدث الثالث قريب من الصفر. إن ظهور الحدث ذي الاحتمال الصغير جداً سيسبب الكثير من الدهشة وبالتالي سيحمل في طياته كمية من المعلومات أكبر من الحدث ذي الاحتمال الأكبر.نلاحظ هنا أن المعلومات تترابط مع مقدار الاستغراب أو المفاجأة والتي بدورها تكون ناتجة عن عدم التوقع أوالغموض.أي أنه كلما زاد عدم توقع الحدث كانت المفاجأة أكبر وبالتالي كمية معلومات أكبر. نستطيع أن نقول إن احتمال ظهور الحدث هو مقياس لعدم التوقع

وبالتالي هو متعلق بالمحتوى المعلوماتي للحدث. عندها واعتمادنا على الفطرة السليمة لاحساسنا نقول أن كمية المعلومات المستلمة من رسالة تتعلق مباشرة بغموضها ،أو تتعلق عكسياً مع احتمال ظهورها.

إذا كانت P هي احتمال ظهور الرسالة و I هي كمية المعلومات المستلمة من هذه الرسالة ، فمن الواضح من النقاش السابق أنه عندما $P \to 1, \Rightarrow \mathrm{I} \to 0$ وأيضاً عندما $P \to 0, \Rightarrow \mathrm{I} \to \infty$ وبشكل عام P الصغيرة ستعطي كمية كبيرة من I وهذا يقودنا إلى النموذج التالي:

$$\mathrm{I} \sim \log \frac{1}{P} \qquad (1-1)$$

1 – 2 – 2 المقياس الهندسي لكمية المعلومات:

Engineering Measure of Information

محتوى الرسالة من المعلومات من وجهة نظر هندسية مشابهة لما هو في النموذج (1—1).لكن ما هو المقصود بوجهة النظر الهندسية لكمية المعلومات . إن مهمة أي مهندس اتصالات هو الإرسال الفعال للرسائل، ومقابل هذه الخدمة سيطلب المهندس من المستخدم مبلغاً يتناسب مع المعلومات التي تم إرسالها . لكن في الواقع نجد أن المهندس يطلب من المشترك ما يتناسب مع الزمن المطلوب لإرسال الرسالة ، وبالمختصر ومن وجهة نظر هندسية فإن المعلومات في أي رسالة تتناسب طرداً مع الزمن الأصغري اللازم لإرسالها. هذا يعني أن الرسالة ذات الاحتمال الكبير تستغرق زمناً أقل في الإرسال من الرسالة ذات الاحتمال الصغير. هذه الحقيقة يمكن التأكد منها عن طريق مثال لإرسال الأحرف الأبجدية للغة الانكليزية باستخدام ترميز إشارات مورس. هذا الترميز يتكون من تراكيب مختلفة من رمزين اثنين (العلامة والفراغ Mark & space)، أو باستخدام نبضات بارتفاع A أو $A-$ فولت. يمثل كل حرف بتسلسل محدد من هذه الرموز نسميه بكلمة الترميز وذات طول محدد. من الواضح أنه من أجل الإرسال الفعال تمثل الحروف

مثل e,t,a, o والتي نصادفها بكثرة في اللغة بكلمات ترميز قصيرة ، بينما تمثل الحروف والتي نصادفها بدرجة أقل مثل x,k,q, z بكلمات ترميز أطول. يمكن اعتبار كل حرف كرسالة .وهنا من الواضح أن الحروف التي تتكرر بشكل كبير(باحتمال حدوث كبير) ستتطلب زمناً قصيراً للإرسال (كلمة ترميز قصيرة) وذلك بالمقارنة مع الحروف ذات الاحتمال الصغير. وسنرى الآن أن بالمتوسط أن الزمن المطلوب لإرسال الرمز (أو الرسالة) باحتمال ظهور P في الواقع يتناسب مع $\log \frac{1}{P}$.

من أجل التبسيط نبدأ بحالة الرسائل الثنائية m_1,m_2 باحتمالات متساوية .يمكن استخدام الخانات الثنائية لترميز هذه الرسائل ونمثل m_1 و m_2 بالأرقام 0 و 1 على الترتيب .من الواضح هنا أنه لترميز رسالتين مختلفتين متساويتي الاحتمال يلزمنا على الأقل خانة ثنائية واحدة. لكن لو فرضنا أن هناك أربع رسائل متساوية الاحتمال m_1,m_2,m_3,m_4 وأردنا ترميزها بالشكل الثنائي فسنحتاج على الأقل إلى خانتين ثنائيتين لكل رسالة .وبالتالي التركيبات الممكنة لخانتين ثنائيتين ستشكل أربع كلمات ترميز 00,01,10,11 والتي ستمثل أربع رسائل متساوية الاحتمالات m_1,m_2,m_3,m_4 على الترتيب ،من الواضح هنا أن أياً من هذه الرسائل سيأخذ ضعف زمن الإرسال المطلوب في حالة الرسالتين المتساويتين بالاحتمال وبالتالي ستحمل ضعف كمية المعلومات . وبشكل مشابه نستطيع ترميز أية رسالة من أصل ثماني رسائل متساوية الاحتمال بثلاث خانات ثنائية على الأقل ،كما نرى أننا نحتاج إلى $\log_2 n$ خانة ثنائية لترميز كل رسالة من أصل n رسالة متساوية الاحتمالات ، ولأن هذه الرسائل متساوية الاحتمال فإن احتمال أي رسالة P سيساوي إلى $\frac{1}{n}$ ،وبالتالي كل رسالة (باحتمال P) ستحتاج إلى $\log_2 \frac{1}{P}$ خانة

ثنائية لإنشاء الترميز ، ومن وجه نظر هندسية فإن المعلومات I الناتجة عن رسالة باحتمال حدوث P ستتناسب مع $\log_2 \frac{1}{P}$:

$$I = k \log_2 \frac{1}{P} \qquad (2-1)$$

حيث k ثابت سيتم تحديده ، ومن جديد نجد أن المعلومات الناتجة عن رسالة ومن وجه نظر هندسية تتناسب مع لوغاريتم مقلوب احتمال هذه الرسالة ، للتبسيط نأخذ قيمة الثابت k في المعادلة (2—1) مساوية للواحد عندها نأخذ واحدة كمية المعلومات بالوحدة الثنائية البت bit أي:

$$I = \log_2 \frac{1}{P} \ bits \qquad (3-1)$$

استناداً إلى ما سبق فإن كمية المعلومات في رسالة ما يمكن تعريفها بأنها عدد الخانات الثنائية الأصغري اللازم لترميز هذه الرسالة . لقد بينا ذلك من أجل رسائل متساوية الاحتمال وسنبين لاحقاً أن هذا أيضاً صحيح حتى في حالة عدم تساوي الاحتمالات.

نفرض أننا أردنا استخدام نظام عد r مختلف عن النظام الثنائي في عملية الترميز. سنجد أن أي خانة هنا ستأخذ واحداً من r قيمة مختلفة (0,1,2,…,r—1). فإذا كان لدينا n رسالة فإننا نحتاج إلى k خانة لتحقيق الترميز بحيث يكون لدينا rk كلمة ترميز مختلفة فإذا كانت الرسائل n متساوية الاحتمال فسنحتاج إلى $k = \log_r n$ خانة لإتمام عملية الترميز بنظام العد r ، لكن $n = 1/P$ حيث P احتمال حدوث أي رسالة .ومن الواضح أننا نحتاج على الأقل إلى $\log_r 1/P$ خانة. وبالتالي كمية المعلومات المتضمنة في هذه الرسالة :

$$\mathrm{I} = \log_r \frac{1}{P} \qquad (4-1)$$

من المعادلة (1—3) و (1—4) نجد :

$$\mathrm{I} = \log_2 \frac{1}{P} \ bits = \log_r \frac{1}{P} \quad r - ary \ units$$

وبالتالي:

$$1\ r - ary\ unit = \log_2 r \ \ bits \qquad (5-1)$$

كما نلاحظ أن اختيار أساس اللوغاريتم لن يغير من مفهوم المعلومات بل سيغير فقط واحدة الحساب، فإذا اخترنا اللوغاريتم الطبيعي على سبيل المثال فإن واحدة قياس المعلومات نسميها بـ "نات nat"، لكننا هنا ضمن هذا المقرر سنستخدم واحدة النظام الثنائي البت bit لقياس كمية المعلومات ، وسيكون أساس اللوغاريتم هو 2 حتى لو لم يظهر إلا إذا ذكر خلاف ذلك في السياق, مع الانتباه إلى أن هناك اختلافاً في المفهوم بينها وبين الخانة الثنائية الفيزيائية المستخدمة في نظم الاتصالات .

1- 3 مفهوم الاحتمالات:The Concept of probability

Yan نظرية الاحتمال هي المجال الذي يتعامل مع مفهوم الاحتمالات، وفي البداية هي مجموعة التجارب المنفذة لتعطي في النهاية نتائج محددة. نستطيع هنا أن نعمم ذلك على منبع معلومات يقوم بتوليد مجموعة من الرموز أو الأحرف أو الرسائل. يمكن اعتبار أي ظهور على خرج المنبع على أنه حدث ممكن من بين مجموعة من الأحداث المتوفرة للمنبع . نسمي مجموعة الأحداث الممكنة على خرج المنبع بفضاء العينات sample space، وهنا يمكن التحدث عن احتمال حدوث نتيجة معينة للتجربة أو احتمال أن يولد منبع المعلومات رمزاً أو رسالة محددة .نقوم عندئذ بإسناد رقم يتراوح بين 0 و 1 لكل حدث أو نتيجة بحيث يمثل هذا الرقم

احتمال ظهوره ، وللتبسيط نقتصر هنا على فضاء حالة محدد أي يحتوي على عدد محدد من الرموز أو النتائج أو الرسائل.

بفرض لدينا تجربة إحصائية X لها النتائج (الأحداث) الممكنة x_i بحيث $x_i \in X$ وتعرف X كفراغ احتمالي بالشكل:

$$X = \{x_1, ..., x_i, ..., .x_n\} \qquad (6-1)$$

فإذا كانت التجربة هي رمي حجر النرد فإن x_1 تمثل رمي النرد وأعطى الرقم 1 ،والحدث x_2 أعطى الرقم 2 وهكذا وهنا في هذه التجربة $n = 6$.ومهما كانت نتيجة أو حدثاً سيكون لها احتمال الحدوث المحدد . ونرمز $p(x_i)$ لاحتمال هذا الحدث x_i أو ببساطة P_i .وعندها نعرف مجموعة الاحتمالات المرتبطة بالحادثة X بالشكل التالي:

$$P = \{p_1, ..., p_i, ..., p_n\} \qquad (7-1)$$

والتي سنسميها توزع الاحتمالات probability distribution، والذي يفترض أن يحقق متطلبين أساسيين اثنين هما:

$$(i) \qquad p_i \geq 0, \; for \; all \; i$$

$$(ii) \qquad \sum_{i=1}^{n} p_i = 1,$$

حيث لا يوجد احتمال أقل من الصفر ، كما أن مجموع كافة الاحتمالات يجب أن يساوي الواحد.

في بعض الأحيان نهتم بنوعين اثنين من النتائج من التجربة نفسها كما لو كان لدينا دمج لتجربتين في تجربة واحدة ، عندها سنتعامل مع فراغين منفصلين للعينات ، مثل X و Y حيث فراغ العينات لـ Y المتعلق بالتجربة Yيكتب بالشكل التالي:

$$Y = \{y_1, ..., y_j, ..., y_m\} \qquad (8-1)$$

ويعطى توزع الاحتمالات لهذه التجربة بالشكل:

$$Q = \{q_1, ..., q_j, ..., q_m\} \qquad (9-1)$$

حيث $q(y_j) = q_j$ هي احتمال الحدث y_j . وإذا اعتبرنا أن (X,Y) هي تجربة إحصائية بزوج من النتائج (x_i, y_j) حيث $x_i \in X \ \& \ y_j \in Y$.

الاحتمال $r(x_i, y_j)$ يمثل بـ r_{ij} أو $p(x_i, y_j)$ وهو احتمال أن تعطي التجربة (X,Y) النتيجة (x_i, y_j) على خرجها وسنسميه بالاحتمال المشترك joint probability . يمكن استنتاج الاحتمالات p_i, q_j إذا كان الاحتمال المشترك معلوماً ، عندها نسمي هذه الاحتمالات بالهامشية وفي كل الأحوال من أجل جميع قيم i نجد :

$$p_i = \sum_{j=1}^{m} r_{ij} \qquad (10-1)$$

ومن أجل جميع قيم j نجد:

$$q_j = \sum_{i=1}^{n} r_{ij} \qquad (11-1)$$

وطالما أن مجموع الاحتمالات p_i أو الاحتمالات q_j يجب أن يساوي الواحد فإن مجموع الاحتمالات المشتركة يجب أن يساوي الواحد أي:

$$\sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} = 1$$

إلى جانب الاحتمالات المشتركة أو الاحتمالات المفردة يوجد نوع ثالث من الاحتمالات وهو الاحتمال المشروط conditional probability .يظهر هذا الاحتمال ضرورة تعلق التجربة الإحصائية Y شرطياً بالتجربة X .أي أن إحصائيات نتائج التجربة X ستؤثر في نتائج التجربة Y .أي أننا نهتم مثلاً باحتمال الحدث x_i وذلك عند التأكد ومعرفة حدوث نتيجة أخرى مثل y_j .

نعرف الاحتمال المشروط لـ x_i إذا تمت معرفة الحدث y_j بالشكل التالي:

$$p(x_i / y_j) = \frac{r(x_i, y_j)}{q(y_j)} \qquad ; q(y_j) > 0$$

أو بشكل مختصر

$$p_{ij} = \frac{r_{ij}}{q_j} \qquad ; q_j > 0 \qquad (12-1)$$

الاحتمال المشروط لـ y_j إذا تم معرفة الحدث x_i ويعرف بالطريقة نفسها بالشكل التالي:

$$q(y_j / x_i) = \frac{r(x_i, y_j)}{p(x_i)} \qquad ; p(x_i) > 0$$

أو بشكل مختصر :

$$q_{ji} = \frac{r_{ij}}{p_i} \qquad ; p_i > 0 \qquad (13-1)$$

من التعريفات السابقة يمكن أن نستنتج الاحتمال المشترك ونكتبه على شكل جداء بين الاحتمال المفرد والاحتمال المشروط:

$$r(x_i, y_j) = q(y_j)\, p(x_i / y_j) = p(x_i) q(y_j / x_i) \qquad (14-1)$$

إن مفهوم الاحتمال المشروط يمكن توسيعه ليشمل أكثر من حدثين ، فإذا أخذنا على سبيل المثال x_i, y_j & z_k :

$$p(x_i, y_j, z_k) = r(y_j, z_k)\, p(x_i / y_j, z_k) = p(z_k)\, p(y_j / z_k)\, p(x_i / y_j, z_k)$$

وبالتالي:

$$p(x_i / y_j, z_k) = p(x_i, y_j, z_k) / r(y_j, z_k)$$

وبالعودة للاحتمال المشروط فإن المجموع على قيم i عند معرفة y_j يعطي بالعلاقة :

$$\sum_{i=1}^{n} p(x_i / y_j) = 1 \qquad (15-1)$$

وبما أن الحدث y_j قد حصل فإن واحداً من فراغ العينات X يجب أن يحدث ، لذلك فإن المجموع يجب أن يساوي الواحد.لاحظ أن العكس غير صحيح إذ إن الصحيح هو :

$$\sum_{j=1}^{m} p(x_i / y_j) \neq 1 \qquad (16-1)$$

للسهولة يمكن استخدام نظرية بايس Bayes' theorem المبينة أدناه، غالباً ما يكون الاحتمال المشروط $q(y_j / x_i)$ معروفاً ونريد أن نحدد الاحتمال المشروط $p(x_i / y_j)$ ونستطيع حساب ذلك من المعادلة التالية:

$$r(x_i, y_j) = p(x_i)q(y_j / x_i) = q(y_j)p(x_i / y_j)$$

فإذا كان $q(y_j) > 0$ نجد أن :

$$p(x_i / y_j) = \frac{p(x_i)q(y_j / x_i)}{q(y_j)}$$

وأيضاً:

$$p(x_i / y_j) = \frac{p(x_i)q(y_j / x_i)}{\sum_{i=1}^{n} p(x_i)q(y_j / x_i)} \qquad (17-1)$$

نستطيع الآن معرفة $p(x_i / y_j)$ باستخدام $q(y_j / x_i)$.

أخيراً نلاحظ استقلالية الرمز x_i التي تظهر في حال $p(x_i / y_j) = p(x_i)$ ، تعني أن حدوث y_j لن يؤثر أبداً في x_i. لكن ذلك يتبعه بالضرورة:

$$r(x_i, y_j) = p(x_i)q(y_j)$$

وأيضاً:

$$q(y_j / x_i) = q(y_j)$$

في هذه الحالة نستنتج أن هذه الأحداث مستقلة بعضها عن بعض. والعكس صحيح ، فمن العلاقة $r(x_i, y_j) = p(x_i)q(y_j)$ ينتج كل من $q(y_j / x_i) = q(y_j)$ و $p(x_i / y_j) = p(x_i)$.

نقول عن تجربتين X, Y مستقلتين إحصائياً إذا كان من أجل كل قيم i, j :

$$r(x_i / y_j) = p(x_i)q(y_j) \qquad (18-1)$$

ونقول عن التجربة X متعلقة تماماً بأخرى مثل Y إذا كان من أجل كل قيم j هناك قيمة واحدة فريدة لـ i ولتكن k يتحقق فيها :

$$p(x_k / y_j) = 1 \qquad (19-1)$$

أو

$$r(x_k, y_j) = p(y_j) \qquad (20-1)$$

1 – 4 متوسط كمية المعلومات :إنتروبية المنبع:

Average Information per Message: Entropy of a source

بفرض وجود منبع من دون ذاكرة يولد مجموعة من الرسائل ضمن فراغ عينات X بتوزع احتمالات P (المقصود بالمنبع من دون ذاكرة أن أية رسالة يولدها هذا المنبع مستقلة تماماً عن الرسالة السابقة) ، من التعريفات السابقة تعطى كمية المعلومات للرسالة i بالعلاقة:

$$I_i = \log \frac{1}{p_i} \qquad (21-1)$$

ولتوصيف المنبع نأخذ متوسط كمية المعلومات لكافة رموزه وفق العلاقة:

$$H(X) = \sum_{i=1}^{n} p_i I_i = -\sum p(x_i) \log\, p(x_i) = -\sum_{i=1}^{n} p_i \log\, p_i \qquad (22-1)$$

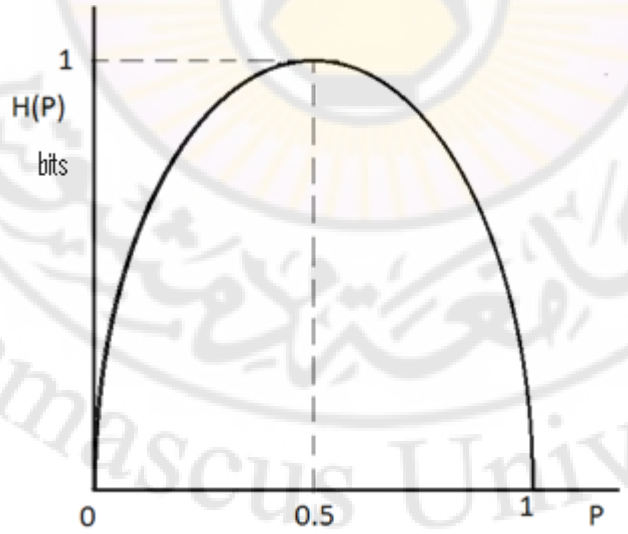
وهذا ما نسميه مقياس شانون للمعلومات ويمكن أن يرمز له أيضاً بـ H(P) أو $H(P_1,\ldots P_n)$.

وطالما أننا نختار العدد 2 كواحدة لقياس المعلومات لذلك ستكون هذه الواحدة دوماً هي البت Bit ضمن هذا المقرر.

في حالة وجود حدثين فقط باحتمالات $P_1=P$ و $P_2=1-P$ نجد أن

$$H(P) = -P \log P - (1-P)\log(1-P) \qquad (23-1)$$

يبين الشكل (1—1) تغير H(P) كتابع للمتحول P، ومنه نستنتج أنه في حال كون الحدث مؤكداً فاحتماله هو الواحد ومقياس المعلومات (الانتروبية) يصبح مساوياً للصفر، وهذا يتطابق مع البديهيات السابقة ، وسنحصل على النتيجة نفسها من أجل P=0 لأن الاحتمال الآخر سيصبح مساوياً للواحد.



الشكل (1—1) تغيير الإنتروبية مع الاحتمال للمنبع الثنائي

تصل H(P) قيمتها العظمى عند P=0.5 والتي تساوي الواحد حيث يلاحظ تساوي الاحتمالين وبالتالي لا يوجد أي تأكيد لأي حدث منهما .

وبالرجوع إلى الحالة العامة نستطيع أن نثبت أن مقياس كمية المعلومات يحقق أربعة متطلبات بديهية:

1- H(P) تابع مستمر بالنسبة للمتحول P

2- H(P) تابع متناظر أي أن ترتيب الاحتمالات $P_1,\ldots,P_n$ لن يؤثر في قيمة H(P).

3- H(P) مقدار جمعي ،فإذا كانت X و Y فراغي عينات بحيث X مستقلة عن Y نجد أن المعلومات المرتبطة بالحدث المشترك (x_i,y_j)

$$H(p_1q_1,\ldots,p_1q_m,\ldots p_nq_1,\ldots,p_nq_m) = H(p_1,\ldots,p_n)+H(q_1,\ldots q_m) \qquad (24-1)$$

4- تأخذ H(P) قيمتها العظمى عند تساوي جميع الاحتمالات ، حيث يترافق هذا مع أقصى حالة من الغموض والشك ، وتأخذ قيمتها الدنيا عندما يكون احتمال أحد الحوادث قيمته الواحد

مثال 1—1: لنفرض أن لدينا التجربتين X,Y لهما فضاء العينات التالي:

X={لن تمطر غداً، سوف تمطر غداً}

بحيث: P={0.8, 0.2}

وأيضاً: {عمر محمد على الأقل30، عمر محمد أصغر من 30}=Y

بحيث: Q={0.2, 0.8}

كمية المعلومات المتعلقة بـ X هي :

$$H(X) = -0.8\log 0.8 - 0.2\log 0.2 = 0.72\ bits$$

ومن أجل Yنجد :

$$H(Y) = -0.2\log 0.2 - 0.8\log 0.8 = 0.72\ bits$$

أي أن : $H(X) = H(Y)$

نلاحظ من هذا المثال أن مقياس شانون للمعلومات لا يهتم أبداً بمحتواها بل يهتم فقط باحتمال حدوثها وليس بماهية هذه المعلومة .

كما أن هذا المقياس يحقق الخاصية الجمعية والتي تتوضح من خلال المثال التالي: لنفرض أن لدينا نردين وطالما أنهما مستقلان فلا يوجد أي فرق إذا تم رميهما في الوقت نفسه أو رمي أحدهما بعد الآخر ، فالمعلومات المتعلقة بالنرد لن تتغير إذا تم رميه مع الآخر أو رميه بالتتابع ،فإذا كانت H(X)هي كمية المعلومات المتعلقة برمي نرد واحد ، و H(Y) هي كمية المعلومات المتعلقة برمي النرد الآخر (مع ملاحظة أن H(X)=H(Y)في هذه الحالة) فإن H(X,Y) هي كمية المعلومات المتعلقة برمي النردين في الوقت نفسه، وسنحصل على النتيجة التالية:

$$H(X,Y) = H(X) + H(Y) \qquad (25-1)$$

وهذا هو بالضبط ما قصدناه بالخاصية الجمعية .

إذا كانت $X=(x_1,\ldots,x_n)$ فضاء العينات للتجربة X بحيث $P=(p_1,\ldots,p_n)$ قيم الاحتمالات الموافقة نستطيع أن نستنتج الخاصتين المهمتين التاليتين :

a- $H(P) \le \log n$ وتتحقق المساواة فقط عندما يكون $p_i = 1/n$ من أجل كل قيم i=1,…,n

b- $H(P) \ge 0$ وتتحقق المساواة فقط عند توفر عنصر k فيه $p_k=1$ بينما لباقي العناصر i≠k الاحتمال $p_i=0$

مثال1—2:

صورة تلفزيونية تتألف من 576 خطاً ،كل منها يتألف من 720عنصر صورة (بكسل)، عند ذلك صورة واحدة منها ستتألف من 414720 عنصر صورة ،فإذا كنا نتعامل مع صورة تدرجات رمادية تتألف من 10مستويات شدة فهناك 10414720 صورة مختلفة يمكن أن تظهر على الشاشة، فإذا كان لكل الصور احتمالات متساوية بالظهور، فإن كمية المعلومات المتعلقة بالصورة تساوي:

$$H(P) = \log n = \log(10^{414720}) \approx 1.4X10^{6}\ bits$$

لقد رأينا أيضاً أن كمية المعلومات لن تتغير إذا تغير ترتيب الاحتمالات، فإذا أخذنا توزعين للاحتمالات على الشكل التالي:

$$P = \{0.5,\ 0.25,\ 0.25\}$$

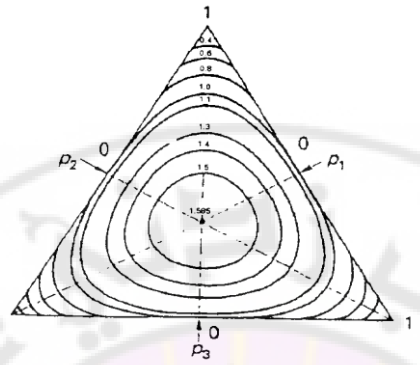
وأيضاً

$$Q = \{0.48,\ 0.32,\ 0.20\}$$

وعند حساب كمية المعلومات لكلا الحالتين نجد:

$$H(P) = H(Q) = 1.5 bits$$

ونلاحظ هنا أن توزيعين مختلفين للاحتمالات أعطيا كمية نفسها :هذا يعني أنه في بعض الحالات توزعات مختلفة للاحتمالات ستعطي كمية المعلومات نفسها . يظهر الشكل (1—2) توزعات الاحتمالات بيانياً والتي تعطي كمية المعلومات نفسها من أجل ثلاثة احتمالات (n=3)



الشكل (1—2) التوزيعات البيانية لثلاثة متحولات

تشير المنحنيات المغلقة إلى توزعات الاحتمالات التي ستعطي كمية المعلومات نفسها.يمكن إيجاد قيم الاحتمالات الموافقة عند كل نقطة من المنحني بالإسقاط المباشر على المحاور p_1,p_2, p_3.

من السهل التأكد أن كمية المعلومات العظمى من أجل n=3 ستساوي:

$$H(P) = \log 3 = 1.58 bits$$

وبما أن هناك توزعاً وحيداً للاحتمالات يحقق القيمة العظمى لكمية المعلومات وهي $P = \{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\}$وهذه تتحقق في الشكل 1—2 على شكل نقطة وحيدة بدلا من المنحني المغلق.

مثال 1—3:

لنفرض أن لدينا حقلاً بيانياً يتألف من 16 منطقة إحداها مظللة (الشكل 1—3)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

الشكل (1—3) الحقل البياني للمثال (1-3)

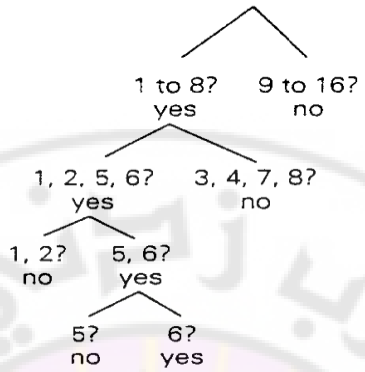
ونريد عن طريق طرح أسئلة أجوبتها "نعم" أو "لا" تحديد موقع هذه المنطقة، فما هي الإستراتيجية الأفضل لذلك ،قد يأتي أحدهم ويضطر لطرح 16 سؤالاً ليحدد المكان . كان من الأفضل العمل بشكل انتقائي وطرح الأسئلة على الشكل التالي (انظر الشكل 1—4 أيضاً) :

1- هل هذه المنطقة تقع ضمن المناطق الثماني السفلية؟ الجواب سيكون "لا" عندها سنستثني المناطق من 9 وحتى 16

2- هل هذه المنطقة تقع ضمن المناطق الأربع الواقعة على اليسار مما تبقى؟ الجواب سيكون "نعم" والمنطقة المعنية أصبحت هي 1،2،5، أو6

3- هل هذه المنطقة تقع ضمن المنطقتين السفليتين مما تبقى؟ الجواب سيكون "نعم" إذاً المنطقة المطلوبة هي 5، أو 6

4- هل هي المنطقة اليسارية؟ الجواب "لا" إذاً المنطقة المظللة هي 6.



الشكل (1—4) شجرة الوصول لحل المثال (1-3)

إذا تطلب الأمر أربعة أسئلة فقط لتحديد منطقة مظللة من أصل 16منطقة. فإذا أخذنا الآن كمية المعلومات المتعلقة بهذه المسألة بفرض أن المناطق لها نفس الاحتمال فسنجد:

$$H(P) = -\sum_{i=1}^{16} \frac{1}{16} \log \frac{1}{16} = \log(16) = 4 \; bits$$

تتطابق كمية المعلومات ظاهريا مع الحد الأدنى من الأسئلة المطلوبة لتحديد ما هو ناتج التجربة العشوائية ،وهذه النتيجة محققة حتى عند عدم تساوي الاحتمالات كما في المثال التالي:

مثال 1—4:

يعطى فضاء العينات X بالشكل $X=\{x_1,x_2,x_3\}$ والاحتمالات الموافقة بالشكل $P=\{1/2,\ 1/4,\ 1/4\}$ وبالعودة إلى لعبة الأسئلة والأجوبة بـ "نعم" أو "لا" نلاحظ بوضوح أنه من المفروض أن نبدأ بالسؤال عن x_1 في البداية طالما لديها الاحتمال الأكبر/ فإذا كان الجواب بـ "نعم" سنكون قد توصلنا للنتيجة ، وإذا كان الجواب بـ "لا" فالنتيجة هي إما x_2 أو x_3 ، ولتحديد أيهما نحتاج إلى سؤال آخر، وبالمجموع سنحتاج إلى سؤالين اثنين لتحديد النتيجة، أي سنضطر إلى طرح سؤال واحد أو سؤالين باحتمالين متساويين أي هناك 1.5 سؤال .

فإذا حسبنا كمية المعلومات حسب شانون لهذه التجربة فسنجد :

$$H(P) = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{4}\log\frac{1}{4} = 1.5\ bits$$

1—5 قياس كمية المعلومات المتبادلة ، المشتركة والمشروطة (الإنتروبية المتبادلة ،المشتركة والمشروطة):

Conditional, Joint and Mutual Information Measure

بالرجوع إلى التجربة الاحتمالية (X,Y) ونتائجها الممكنة (x_i,y_j) حيث $(x_i, y_j) \in (X, Y)$ استناداً إلى حجم فضاء العينات (X,Y) يمكن استنتاج أن التجربة (X,Y) لها nm مجموع خرج مشترك. فإذا أردنا تعريف كمية المعلومات المتعلقة بـ (X,Y) فإننا نلاحظ ما يلي :

هناك nm حوادث مشتركة (x_i,y_j) لها الاحتمالات $r(x_i,y_j)$ أو اختصاراً r_{ij} ، ولنفرض الآن أننا نريد كتابة nm حادثة مشتركة على شكل $z_1, z_2, \ldots, z_{nm}$ الموافقة للاحتمالات $p(z_1), p(z_2), \ldots p(z_{nm})$ ،أي أنه في الحقيقة هناك فراغ عينات ببعد وحيد ولإيجاد مقياس المعلومات له نكتب:

$$H(Z) = -\sum_{k=1}^{nm} p(z_k)\log p(z_k) \qquad (26-1)$$

لكن بسبب أن أي احتمال $p(z_k)$ سيساوي واحداً من الاحتمالات $r(x_i,y_j)$ فإن المجموع على k سيعطي المجموع نفسه على i و j وبكلمات أخرى :

$$H(Z) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i, y_j)\log[\, r(x_i, y_j)]$$

هذا يقودنا إلى تعريف مقياس كمية المعلومات المشتركة وفقاً لما يلي. بفرض لدينا التجربة الاحتمالية (X,Y) بفضاء عينات ذي بعدين بحيث r_{ij} أو

$r(x_i,y_j)$ هـي احتمـالات x_i و y_j مـع بعـض فإننـا نعـرف مقيـاس كميـة المعلومـات المشتركة بالشكل التالي:

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i,y_j)\log[\,r(x_i,y_j)] \qquad (27-1)$$

يمكـــن اســـتخدام تمثيـــل آخـــر $H(R)$ و $H(r_{11},\ldots.r_{nm})$ وأيضـــاً $H(X,Y)$للتعبير عن القيمة نفسها . وبالطريقة نفسها يمكن تعريف مقياس كمية المعلومات المشروطة وربطها بالاحتمالات المشروطة.

لنأخذ أيضاً التجارب الاحتمالية X و Y ونفرض أننا نهتم بكمية المعلومات المتعلقة بـ Y بشرط أن العنصر x_i قد حدث .أي أن لدينا احتمالات من الشكل $q(y_j/x_i)$, حيث $j=1,\ldots,m$ بدلاً من الاحتمالات $q(y_j)$; $j=1,\ldots.m$ لكن المجموع سيبقى مساوياً للواحد. كمية المعلومات المتعلقة بـ Y بشرط حدوث x_i يمكن استنتاجها بالتشابه مع التعريف السابق بهذا الشكل:

$$H(Y/x_i) = -\sum_{j=1}^{m} q(y_j/x_i)\log[\,q(y_j/x_i)] \qquad (28-1)$$

ونأخذ المتوسط على كل قيم x_i فهو متوسط كمية المعلومات لـY مشروطة بمعرفة تامة بـ X:

$$\sum_{i=1}^{n} p(x_i)H(Y/x_i) = \sum_{i=1}^{n} p(x_i)\left\{-\sum_{j=1}^{m} q(y_j/x_i)\log[\,q(y_j/x_i)]\right\}$$

$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i)q(y_j/x_i)\log[\,q(y_j/x_i)]$$

$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i,y_j)\log[\,q(y_j/x_i)]$$

هذا المقدار يعرف بـ كمية المعلومات المشروطة H(Y/X) ، وهذا يقود إلى التعريف التالي:

مقياس كمية المعلومات المتعلقة بالتجربة Y إذا علمت التجربة X يساوي:

$$H(Y/X) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i, y_j)\log[\, q(y_j / x_i)] \qquad (29-1)$$

وبشكل مشابه نستطيع أن نعرف كمية المعلومات التي نحصل عليها من التجربة X إذا كانت التجربة Y معروفة :

$$H(X/Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i, y_j)\log[\, p(x_i / y_j)] \qquad (30-1)$$

خصائص كمية المعلومات المشروطة H(Y/X):

أ- $H(Y/X) \geq 0$ (31-1)

ب- $H(Y/X) \leq H(Y)$ (32-1)

والمساواة ستحصل عندما تكونX و Y مستقلتين إحصائياً تماماً.

نستنتج من هذه الخاصية أن كمية المعلومات الشرطية عادة أقل من كمية المعلومات الهامشية الحدسية أو تساويها. وبطريقة أخرى فإن المعلومات الخاصة بـ X ستقودنا بالضرورة إلى إنقاص الغموض، وهذا يتوافق مع الأفكار البديهية السابقة حول المعرفة المسبقة.

يجب أن تكون هنالك علاقة بين كميات المعلومات الهامشية ، الشرطية والمشتركة من أجل التجربتين X و Y تتحقق المعادلة التالية:

$$H(X,Y) = H(X) + H(Y/X) = H(Y) + H(X/Y) \qquad (33=1)$$

لإثبات ذلك لدينا :

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i, y_j)\log[\, p(x_i) q(y_j / x_i)]$$

$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i, y_j)\log p(x_i) - \sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i, y_j)\log[\, q(y_j / x_i)]$$

$$= H(X) + H(Y / X)$$

ونستطيع إثبات العلاقة $H(X,Y) = H(Y) + H(X / Y)$ بالطريقة نفسها.

بالاستناد إلى الخصائص الأخيرة يمكن أن نستنتج أن:

$$H(X,Y) = H(X) + H(Y / X) \le H(X) + H(Y) \qquad (34-1)$$

وتحصل المساواة عندما تكون X و Y مستقلتين تماما.

نستطيع أن نقول إن كمية المعلومات المشتركة تأخذ القيمة العظمى إذا كانت كلتا التجربتين الاحتماليتين مستقلتين ونبدأ بالانخفاض كلما زادت العلاقة بينهما ، وعند الترابط التام بينهما فإن نتائج التجربة Y ستكون محددة تماماً عند معرفة نتائج التجربة X وعندها تصبح $H(Y / X) = 0$ وفي هذه الحالة $H(X,Y) = H(X)$.

يتبقى حتى الآن تعريف نهائي وهو كمية المعلومات المتبادلة ، حيث يلعب هذا التعريف دوراً مهما في تحديد سعة قناة الاتصال والتي ستناقش فيما بعد.

تعرف كمية المعلومات المتبادلة بين تجربتين X و Y بالعلاقة التالية:

$$I(X;Y) = H(Y) - H(Y / X)$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{m} r(x_i, y_j)\log\left[\frac{r(x_i, y_j)}{p(x_i)q(y_j)}\right] \qquad (35-1)$$

نستطيع أن نفهم $I(X;Y)$ هي قياس معلوماتي للعلاقة التي تربط التجربة Y و التجربة X، وعندما تكون التجربتان مستقلتان يجب أن تكون $I(X;Y)$ بقيمة أصغريه أي: $I(X;Y) = 0$

إذا كانت Y متعلقة بشكل كامل بـ X عندها $H(Y / X) = 0$ وأيضا تتجه القيمة $I(X;Y)$ لتأخذ قيمتها العظمى والتي تساوي:

$$I(X;Y) = H(Y)$$

نترك للطالب من أجل التجربتين X و Y استنتاج العلاقة:

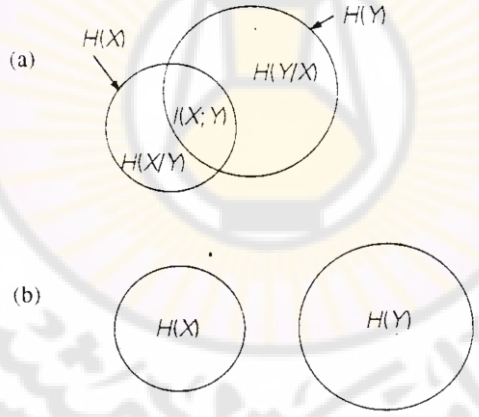
$$I(X;Y) = H(X) - H(X/Y)$$
$$= H(X) + H(Y) - H(X,Y) \qquad (36-1)$$

واستنتاج أن $I(X;Y)$ هي كمية متناظرة مهما تكن X و Y أي:

$$I(X;Y) = I(Y;X) \qquad (37-1)$$

بعد تعريف هذه القيم الثلاثة من المفيد استخدام مخططات فن (Venn) لتوضيح الترابط فيما بينهم كما في الشكل 1—5 حيث لدينا :

$$I(X;Y) = H(X) \cap H(Y)$$
$$H(X,Y) = H(X) \cup H(Y)$$



الشكل 1—5مخطط فين يمثل العلاقات بين جميع أنواع الانتروبية

ومن الشكل 1—5a ومن أجل الحالة العامة نستنتج:

- $H(X/Y) \le H(X)$ *and* $H(Y/X) \le H(Y)$
- $I(X;Y) \le H(Y)$ *and* $I(X;Y) \le H(X)$

- $I(X;Y) = H(X) - H(X/Y) = H(Y) - H(Y/X);$
- $H(X,Y) = H(X/Y) + I(X;Y) + H(Y/X)$
  $= H(Y) + H(X/Y) = H(X) + H(Y/X);$
- $H(X,Y) \le H(X) + H(Y).$

ومن الشكل 1—b5 عند استقلالية X عن Y نلاحظ:

- $I(X;Y) = 0;$
- $H(X,Y) = H(X) + H(Y);$
- $H(X) \le H(X/Y)\ and\ H(Y) = H(Y/X),$

لقد رأينا في هذه الفقرة أنه يمكن استنتاج كل العلاقات التي تربط بين مختلف تعاريف كميات المعلومات باستخدام مخططات فن (Venn) .

1- 6 أساسيات بديهية:

تم سابقاً استنتاج قياس شانون للمعلومات بالإضافة إلى بعض خصائص قياس المعلومات ، التي تتطابق مع الخصائص البديهية التي سيتوقعها المرء لقياس كمية المعلومات ، في حالة التوزع المنتظم ينطبق قياس شانون للمعلومات مع قياس هارتلي للمعلومات ويساوي لوغاريتم العدد الكلي للرسائل ، يمكن استنتاج قياس شانون للمعلومات الذي يعتمد على المعلومات بشكل مباشر من حالة التوزع المنتظم وقياس هارتلي للمعلومات.

بفرض أن قياس المعلومات يحقق المتطلبات التالية:

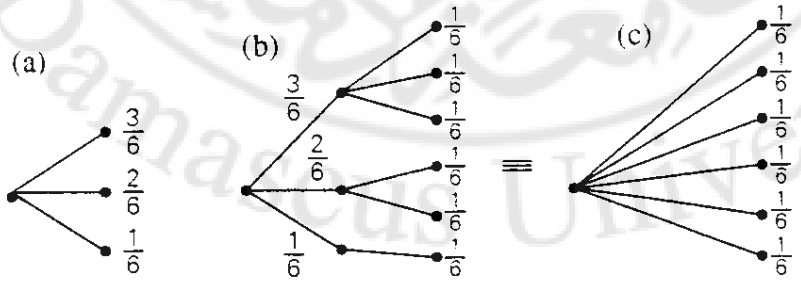
I. إذا قسمنا جميع نتائج الاحتمالية إلى مجموعات فإن جميع قيم H للمجموعات المختلفة مضروبة بوزنها الإحصائي يجب أن تعطي قيمة H الكلية.

II. يجب أن تكون قيمة H تابعاً مستمراً للاحتمالات p_i.

III. إذا كانت جميع قيم p_i متساوية أي أنه مهما تكن i فإن $p_i = \frac{1}{n}$ ، وعندها ستزداد قيمة H كتابع لقيمة n .وهذا يعني أن الغموض سيزداد مع زيادة عدد العناصر ذات الاحتمالات المتساوية.

من أجل n رسالة متساوية الاحتمالات تحقق H العلاقة $H = \log n$ وفقاً لعلاقة هارتلي والمتطلب (III). وعند عدم تساوي الاحتمالات ننظر إلى الحالة التالية: بفرض أن الاحتمالات هي $\frac{3}{6}, \frac{2}{6} and \frac{1}{6}$ ، يعطي الشكل (1—a6) شجرة القرار المطلوب استخدامها لحساب H .

قيمة H حسب شبكة القرار في الشكل (1—c6) يجب أن تساوي $H^C = \log 6$. وبما أن شجرتي القرار في الشكلين (1—b6) و(1—c6) متطابقتان في جوهرهما فإن القيمة المحسوبة وفق شجرة القرار الشكل (1–b6) يجب أن تساوي أيضاً $H^b = \log 6$; $\log 6$ واستناداً إلى المتطلب (I) يجب أن تساوي هذه القيمة الغموض المتعلق بالاختيار بين الأفرع المشار إليها بـ $\frac{3}{6}, \frac{2}{6} and \frac{1}{6}$ في الشكل (1—b6) (أي H^a) يضاف إليه الغموض المتعلق بالمسارات الفرعية كل منها مضروبة بوزنها أي أن :



الشكل (1—6) شجرة القرار

$$H^a + \frac{3}{6}\log 3 + \frac{2}{6}\log 2 + \frac{1}{6}\log 1 = \log 6$$

وأيضاً

$$H^a = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{3}\log\frac{1}{3} - \frac{1}{6}\log\frac{1}{6}$$

وبشكل عام :

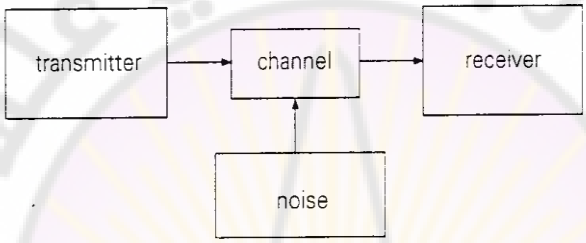
$$H(X) = -\sum_{i=1}^{n} p_i \log p_i$$

1 – 7: نموذج الاتصال:The communication Model

إن معلومات أي منبع لا تستخدم مباشرة في نظام الاتصالات . ومن الناحية العملية يجب التكلم عن الأسلوب الذي يتم فيه استخدام هذه المعلومات للإرسال وهو ما يسمى بنموذج الاتصالات . وفي هذا النموذج يتم التركيز على نقل المعلومات المولدة من المنبع إلى الجهة .أما تخزين المعلومات في الذواكر وعلى أهميته فهو لا يدخل في مسألة النقل ،والتي يمكن وصفها من خلال المصطلحات التالية:

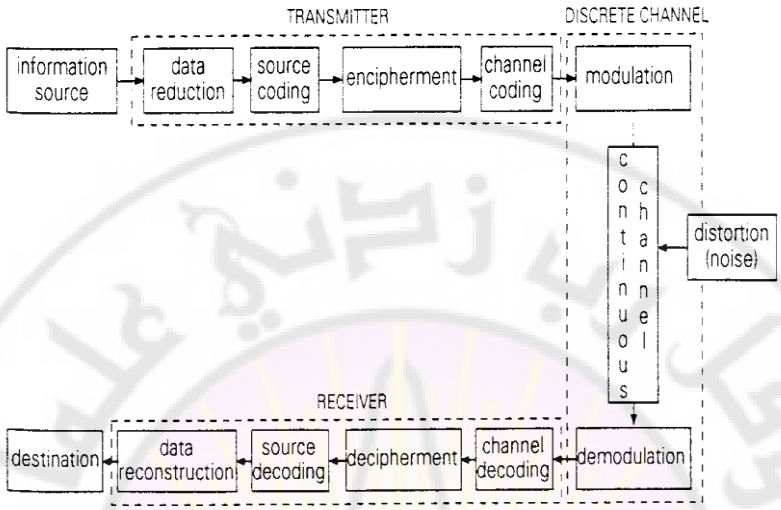
أثناء نقل المعلومات يتم الاتصال بين المنبع ، والذي يولد المعلومات ،والمسمى عادة بالمرسل من جهة و المستقبل من الجهة الأخرى. يظهر الشكل (1—7) النموذج الأساسي للاتصالات. والمشكلة الأساسية التي تظهر أثناء الاتصال بين المرسل والمستقبل هي ظهور الأخطاء أو التشويه كنتيجة للضجيج الذي يؤثر في القناة . يجب أن يكون نقل المعلومات من دون أخطاء إلى درجة محددة تعتمد على متطلبات يضعها المستقبل، أي أنه يجب أن يتوفر إمكانية لتصحيح الأخطاء ، أو أن النقل يتم بشكل جيد وكاف لتكون الأخطاء أقل من الحد المسموح به.

لا يمكن أن يكون هناك نقل مثالي من دون أخطاء وخاصة عند نقل إشارات مثل الكلام، الموسيقى أو الإشارة المرئية ، حيث يستطيع المرء وضع متطلبات إلى أي حد يسمح أن تختلف الإشارة المستقبلة عن الإشارة المرسلة. إن الجودة المطلوبة تقودنا إلى اختيار الوسط المناسب للنقل وبشكل خاص فرض الشروط الحدية لمواءمة القناة مع المرسل والمستقبل.



الشكل (1—7) نموذج الاتصالات

يظهر الشكل (1—8) وصفاً أكثر دقة لنموذج الاتصالات. حيث يجب على نظام الاتصالات إرسال المعلومات المولدة من المنبع إلى الجهة بدقة عالية قدر الإمكان. إذ يفترض أن منبع المعلومات والجهة والقناة ومنبع الضجيج (الذي يؤثر في القناة) محددين بشكل مسبق. نفرض أن القناة المستمرة ترسل الإشارات ذات الطبيعة التي تعتمد على وسط النقل الفيزيائي المتوفر ،وعلى طريقة التعديل المختارة .وتحدد أيضاً الخصائص الفيزيائية للقناة المستمرة مثل عرض المجال ونسبة الإشارة للضجيج .



الشكل(1—8) النموذج الدقيق للاتصالات

إن هدف المرسل هو جعل المعلومات القادمة من المنبع مناسبة للنقل في قناة الاتصال، بينما يحاول المستقبل تصحيح التشويه والأخطاء التي ظهرت في القناة وبالتالي تحويل المعلومات إلى شكل مناسب لاستخدامات الجهة المستقبلة. تقسم وظائف المرسل إلى أربعة مواضيع: الأول يتناول جزء المعلومات المولدة من المنبع والتي لا تهم المستقبل . ومن أجل اعتبارات الكفاءة من الأفضل الاستغناء عن هذه المعلومات، وهذا ما نسميه بإنقاص البيانات (data reduction). وتسمى المعلومات المتبقية بالمعلومات الفعالة(effective information) .

الثاني: أثناء تطبيق ترميز المنبع تتم عادة معالجة المعلومات بطريقة رقمية باستخدام النظام الثنائي لجعلها ذات بنية داخلية مهمة. عادة يسمى هذا بضغط البيانات، حيث تمثل المعلومات الفعالة بشكل مضغوط قدر الإمكان.

الثالث: يبرهن في الكثير من الأحيان أنه من المفضل تأمين المعلومات الناتجة لمنع الاستخدام غير المناسب لها. والحل هو تشفير المعلومات بواسطة الرموز السرية.

عملية حماية المعلومات من الأخطاء التي تحصل في القناة هي الموضوع الرابع الخاص بالمرسل. لتحقيق ذلك تضاف معلومات زائدة ستستخدم فيما بعد لإعادة بناء المعلومات الأصلية إذا حصل أي خطأ فيها. نتكلم هنا عن ترميز القناة (channel coding) حيث نستخدم ترميزات تستطيع كشف و/أو تصحيح الأخطاء. تقدم المعلومات الناتجة من المرسل فيما بعد إلى القناة. يمكن اعتبار القناة قناة متقطعة إذا اقتصرت القناة على مستوى المعلومات القادمة بشكل منفصل من جهة المدخل وتعطي بعد النقل على خرجها رموزاً منفصلة مرة أخرى.

يتم النقل داخلياً عن طريق الإشارات التي يجب أن تمرر عبر الوسط الفيزيائي. تتم عملية التحويل من الرموز إلى الإشارات المناسبة بواسطة التعديل. تتشوه هذه الإشارات عبر نموذج الاتصالات تحت تأثير الضجيج.

وهكذا يظهر مزيج من الإشارة والضجيج يطلب تحويله فيما بعد إلى رموز مرة أخرى بواسطة عملية فك التعديل. أي ظهور عرضي للضجيج سيبدل الرمز الحالي بآخر ويكشف بشكل خاطئ عند المستقبل. تفحص المعلومات القادمة من خرج القناة والتأكد من خلوها من الأخطاء والبحث عن إمكانية تصحيح الأخطاء إن وجدت باستخدام كاشف ترميز القناة.

يفك تشفير وترميز المعلومات الناتجة بالتتابع ضمن كاشف الترميز .وتسلم المعلومات في النهاية إلى الجهة وفق الترتيب والشكل المطلوب عن طريق إعادة بناء البيانات التي تمثلها (data reconstruction) . يمكن النظر إلى خطوات المعالجة السابقة بشكل واسع على أنها تحويلات محددة انطلاقاً من أن التحويلات الأمامية والعكسية ستعطي النتائج نفسها مرة أخرى. الاستثناء من هذا هو ضغط

البيانات وإعادة بنائها حيث يظهر الضجيج الإحصائي المفترض. فيما بعد سيتم العمل على نموذج قناة الاتصال هذا من أجل تحقيق نقل فعال وخال من الضجيج للمعلومات المطلوبة.

الفصل الثاني

منبع المعلومات المتقطعة من دون ذاكرة

The discrete memoryless information source

وقل رب زدني علما
جامعة دمشق
Damascus University

الفصل الثاني

منبع المعلومات المتقطعة من دون ذاكرة

The discrete memoryless information source

2—1 منابع المعلومات المتقطعة:

يمكن فهم منبع المعلومات المتقطعة كمنبع يولد سلسلة من الرموز symbols(أحياناً نسميها الحروف)، بحيث ينتمي كل رمز إلى مجموعة الرموز الممكنة نفسها أو المسموح بها، هذه المجموعة من الرموز الممكنة نسميها أبجدية المنبع (source alphabet). نرمز لهذه الحروف بـ $u_1,u_2,\ldots,u_n$ والأبجدية بـ :

$$U = \{u_1,...,u_i,...,u_n\}$$

تولد هذه الرموز أو الحروف عند لحظات منفصلة (متقطعة) من الزمن ولهذا وبالإضافة إلى أن أبجدية المنبع محدودة نقول: إن المنبع هو منبع معلومات متقطعة. مجموعة من الرموز المتتابعة نسميها رسالة أو كلمة.

هناك تشابه كبير مع اللغة المكتوبة، حيث أن أبجدية المنبع U يمكن النظر إليها كأبجدية مؤلفة من 26 حرف، وفي اللغة المكتوبة تتألف الكلمات من مجموعات من الحروف المتباعدة عن بعضها بالفراغات .نمثل الكلمات أو الرسائل ذات الطول l بالرمز v. وطالما أن الأبجدية تحوي على n حرف فسيصل عدد الرسائل الممكنة إلى n^l .تشكل المجموعة $V = \{v_1,...,v_j,...v_{n^l}\}$ المجموعة الكلية للرسائل الممكنة.

للتفريق بين الأحرف(الرموز) والرسائل ننظر إلى منبع المعلومات بطريقتين: على مستوى الأحرف الرمزية أو على مستوى الرسائل. ولنفرض أن منبع المعلومات احتمالي، هذا يعني أن لكل رمز من الأبجدية U احتمال ظهور أو حدوث. لنرمز لهذه الاحتمالات بـ $p(u_1) = p_1, p(u_2) = p_2, etc...$ حيث نهتم الآن بتوزع الاحتمالات الخاص بـ U: $P = \{p_1,..., p_i,..., p_n\}$.

سنفترض في كل الحالات أن الاحتمالات لن تتغير مع مرور الزمن ، وهذه الحالة محققة دوماً في معظم التطبيقات. نستطيع القول إذاً: إن الرموز المولدة ستشكل تتابعاً احتمالياً مستقراً.

الأمر الثاني المهم هو العلاقة الداخلية بين الرموز المتعاقبة في الرسالة. وهنا الكلام يصبح عن ذاكرة المنبع .وسنفرض في هذا الفصل أن المنبع من دون ذاكرة، أي أن الرموز المولدة مستقلة إحصائياً.

عند النظر إلى منبع المعلومات على مستوى الرموز (الحروف) فإن كمية المعلومات المولدة من منبع من دون ذاكرة ستساوي:

$$H(U) = -\sum_{i=1}^{n} p_i \log p_i \ \ bits/symbol \qquad (1-2)$$

وكمية المعلومات العظمى الممكن توليدها من المنبع المتقطع من دون ذاكرة هي:

$$\max_u H(U) = \log n \ bits/symbol. \qquad (2-2)$$

لقد رأينا سابقاً أنه تتحقق القيمة العظمى إذا كان لجميع الرموز الاحتمال نفسه، وهذا يعني $p_i = \frac{1}{n}$ من أجل كل قيم i .بمقارنة كمية المعلومات $H(U)$ مع القيمة العظمى الممكنة سنحصل على مفهوم **الفائض للمنبع:**

تعريف (2-1):

يعرف الفائض (redundancy) لمنبع المعلومات المتقطعة من دون ذاكرة بالعلاقة:

$$red = 1 - \frac{H(U)}{\max\limits_{u} H(U)} = 1 - \frac{H(U)}{\log n} \qquad (3-2)$$

حيث أن $H(U)$ هي كمية المعلومات(المحتوى المعلوماتي) لمنبع معلومات له أبجدية منبع حجمها n .

عندما يولد المنبع الرموز باحتمالات متساوية فإن $H(U) = \max H(U)$ ويصبح الفائض red=0 .وعندما يولد المنبع رمزاً واحداً باحتمال يساوي الواحد فإن $H(U) = 0$ والفائض red=1 .أي أن قيمة الفائض تتراوح بين 0 و 1 .

يسمى المنبع الذي يولد رمزين فقط بالمنبع الثنائي (binary source) . هذا المنبع سينتج كمية معلومات أعظمية $\log 2 = 1 bits / symbol$ لكن في الحالة العامة عندما تكون الاحتمالات هي p و (1—p) على الترتيب فإن كمية المعلومات المولدة ستكون أقل أي:

$$H(U) = -p \log p - (1-p) \log(1-p) \; bits / symbol$$

والفائض أيضاً سيكون أكبر.

مثال 2—1:

يولد منبع ثنائي من دون ذاكرة الرموز 0 و 1 باحتمالات $\frac{1}{4} and \frac{3}{4}$، فالأبجدية هي $U\{0,1\}$ لذلك لدينا:

$$H(U) = -\frac{1}{4}\log\frac{1}{4} - \frac{3}{4}\log\frac{3}{4} = 0.81 bit / symbol$$

وأيضاً

$$\max_{u} H(U) = \log 2 = 1 bit / symbol$$

إذاً الفائض سيساوي :

$$red = 1 - \frac{H(U)}{\max_u H(U)} = 1 - \frac{0.81}{1} = 0.19$$

سنحدد فيما بعد كمية المعلومات للرسالة بدلاً من الرمز الواحد، وفي البداية لنأخذ التمرين التالي:

مثال 2—2:

لنأخذ المنبع الثنائي في المثال 2—1 ولنفرض أنه تم تشكيل رسائل بطول 3 ، وكما يظهر من الشكل (2—1) هناك 8 رسائل محتملة نرمز لها بـ $v_1,...,v_8$.

وبما أن المنبع من دون ذاكرة والرموز مستقلة احتمالياً فسنجد من أجل v_2 على سبيل المثال:

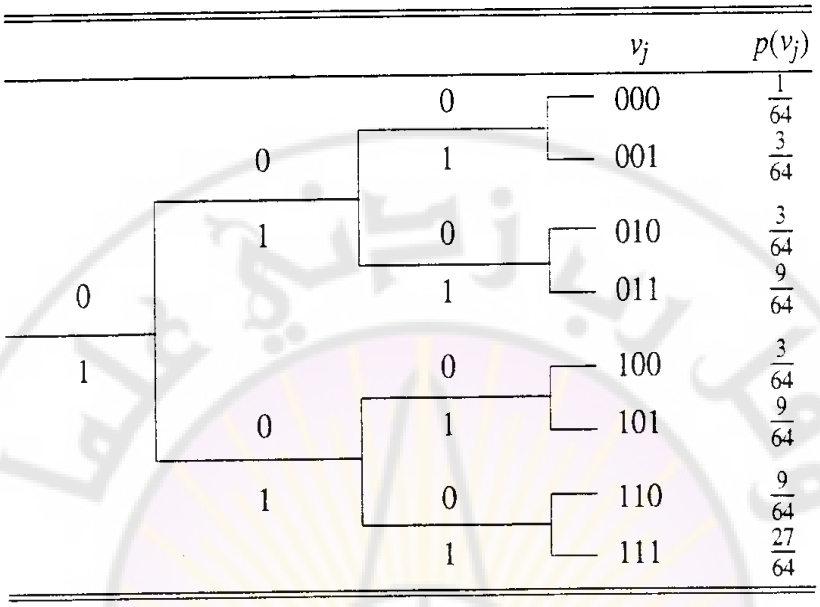
$$p(001) = p(0)\,p(0)\,p(1) = \frac{1}{4}\frac{1}{4}\frac{3}{4} = \frac{3}{64}$$

وبكلمات أخرى فإن احتمال الرسالة يساوي جداء الاحتمالات للرموز المفردة التي تدخل في الرسالة. يظهر الشكل (2—1) احتمالات جميع الرسائل . إذا حسبنا كمية المعلومات استناداً إلى الرسائل سنجد:

$$H(V) = -\frac{1}{64}\log\frac{1}{64} - 3X\,\frac{3}{64}\log\frac{3}{64} - 3X\,\frac{9}{64}\log\frac{9}{64} - \frac{27}{64}\log\frac{27}{64}$$
$$= 2.45\,bits/message$$

نلاحظ هنا أن :

$$H(V) = 3H(U)$$



الشكل (2—1) عدد حالات الرسائل الممكنة في حال كون طول الرسالة 3 بت

في الحالة العامة هناك n^l رسالة بطول l يمكن تشكيلها من منبع أبجديته U وحجمه n . بما أننا نتعامل مع منبع من دون ذاكرة فإن احتمال ظهور أي رسالة سيساوي جداء احتمالات l رمز مفرد من مكونات الرسالة. وكمية المعلومات على مستوى الرسائل ستعطى بالعلاقة :

$$H(V) = -\sum_{j=1}^{n^l} p(v_j) \log p(v_j) \qquad (4-2)$$

وعند كتابة الاحتمالات $p(v_j)$ بواسطة الاحتمالات $p(u_1),...,p(u_n)$ سنرى أنه من السهل برهان أن :

$$H(V) = lH(U) \qquad (5-2)$$

أي أن الرسالة ذات الطول l ستحوي على معلومات أكبر بـ l مرة من الرسائل ذات الطول 1، ونلاحظ أن الأمر كذلك طالما أن الرموز المتتابعة مستقلة. وسنعود فيما بعد إلى حالة قد يكون ذلك فيها غير صحيح.

يمكن تمثيل كمية معلومات المنبع بالبت في واحدة الزمن أي bits/second ، وهنا يجري الكلام عن إنتاجية المنبع ، فإذا كان لجميع الرموز الفترة الزمنية نفسها ولتكن t ثانية فإنتاجية المنبع $H_t(U)$ هي :

$$H_t(U) = \frac{1}{t} H(U)\, bits/\sec ond \qquad (6-2)$$

إذا لم يكن للرموز الفترة الزمنية نفسها (كما هو الحال في ترميز مورس على سبيل المثال فالشَرْطه تأخذ وقتاً أطول من النقطة) يمكن استخدام متوسط الزمن t.

2 – 2 ترميز المنبع *Source coding*:

لنأخذ منبع معلومات من دون ذاكرة يولد رسائل مؤلفة من رموز أبجدية المنبع $U = \{u_1,...,u_i,...,u_n\}$. واستناداً إلى نموذج الاتصالات حيث أنه في البداية يتم إنقاص البيانات (data reduction) بهدف إزالة المعلومات التي لا تهم الجهة المستفيدة من المعلومات . سنفرض هنا أن منبع المعلومات يولد رسائل لا يمكن إنقاصها أكثر من ذلك. من أجل زيادة الكفاءة يجب علينا أن نمثل الرسائل بشكل مضغوط قدر الإمكان، تعرف هذه العملية بترميز المنبع (source coding) .

سنقوم نحن بوضع بعض الأمثلة عن الترميز من خلالها نستطيع ترميز هذه الرسائل . بما أن منبع المعلومات من دون ذاكرة ، يكفي أن نعتمد ترميز حروف المنبع بدلاً من الرسائل. تعطى أبجدية الترميز بالشكل $S = \{s_1, s_2,..., s_r\}$ ، وسنحاول إيجاد تراميز تعطي تركيبة محددة من أجل كل رمز يولده المنبع ،أو ما نسميه كلمة الترميز.

فإذا كانت كلمات الترميز جميعها مختلفة عن بعضها ، نقول عن الترميز :إنه ترميز غير مفرد (non—singular). فإذا شكل تعاقب كلمات الترميز

أيضا ترميزاً غير مفرد، نستطيع القول إن هذا الترميز قابل للكشف بشكل وحيد (uniquely decodable) . وفي هذه الحالة يجب أن تترجم الرسالة المستقبلة بشكل فريد ووحيد . أيضاً في حالة الترميز القابل للكشف بشكل وحيد يجب على كل رمز من الرسالة أن يكشف مباشرة ومن دون النظر إلى الرموز التي تليه، عندها نقول عن الترميز :إنه ترميز لحظي آني (instantaneous code).

مثال (2—3):

منبع معلومات له أبجدية مؤلفة من أربعة حروف u1, u2, u3, u4 .أبجدية الترميز تتألف من رمزين فقط 0, 1 .تشكل كلمات الترميز باستخدام أربعة نظم ترميز مختلفة حسب الجدول التالي:

	A	B	C	D
u_1	0	00	0	0
u_2	11	01	10	01
u_3	00	10	110	011
u_4	01	11	1110	0111

جميع هذه التراميز غير مفردة. الترميز A لا يمكن كشفه بشكل وحيد، لأن التسلسل 0011على سبيل المثال يمكن أن تكون $u_1u_1u_2$ أو أن تكون u_3u_2 .بينما يمكن كشف الترميزات B, C, D بشكل وحيد ومن دون التباس ،جميع كلمات الترميز B متساوية الطول ولكشفها يكفي أن نقسم تتابع كلمات الترميز إلى مجموعات من حرفين فقط، في الترميز C كل كلمة ترميز تنتهي بـ 0 والتي ستلعب دور الفاصلة، بينما في الترميز D كل كلمة ترميز تبدأ بـ 0 لذلك فإن هذا الترميز لا يكشف بشكل آني، ويجب الانتظار حتى بداية الحرف الأول من كلمة الترميز التالية قبل أن نستطيع كشف الكلمة الحالية.

هناك متطلب ضروري وكافٍ للترميز الفوري الآني وهو عدم جعل أية كلمة ترميز بداية لكلمة ترميز أخرى.

نلاحظ من المحددات السابقة وجود علاقة واحد إلى واحد بين رموز المنبع ذي الأبجدية $U = \{u_1,...,u_i,...,u_n\}$ وكلمات الترميز، وللتبسيط سوف نشير إلى كلمات الترميز بالشكل $u_1,u_2,...,u_n$، وسنشير إلى أطوال كلمات الترميز بالشكل $l_1,l_2,...,l_n$، حيث يتحدد هذا الطول بعدد حروف الترميز التي تشكل كلمة الترميز. سنقوم في النظرية التالية بفحص المتطلبات التي يجب أن يحققها الترميز ليصبح ترميزاً قابلاً للكشف بشكل آني (فوري)

2 – 2 – 1 نظرية (متراجحة كرافت Kraft's inequality**):**

هناك متطلب كافٍ وضروري لوجود الترميز الآني وهو:

$$\sum_{i=1}^{n} r^{-l_i} \le 1 \qquad (7-2)$$

حيث r هي حجم أبجدية الترميز وأيضاً $l_i, i = 1,...,n$ طول كلمة الترميز u_i .

البرهان:

لنفرض أن عدد كلمات الترميز ذات الطول 1 يساوي w1.هذا العدد سيكون على الأكثر مساوياً لـ r أي $(w_1 \le r)$.إن كلمات الترميز المستخدمة لا يمكن أن تكون بداية لكلمة ترميز أخرى ، أي أنه سيبقى $r—w_1$ حروف ترميز للبداية . ومن أجل عدد كلمات الترميز ذات الطول 2 نجد:

$$w_2 \le (r - w_1)r = r^2 - w_1 r$$

وبشكل مشابه:

$$w_3 \le \{(r - w_1)r - w_2\}r = r^3 - w_1 r^2 - w_2 r.$$

فإذا كانت m الطول الأعظمي لكلمات الترميز نجد:

$$w_m \le r^m - w_1 r^{m-1} - w_2 r^{m-2} - .... - w_{m-1} r.$$

وبالتقسيم على r^m نجد:

$$0 \le 1 - w_1 r^{-1} - w_2 r^{-2} - .... - w_{m-1} r^{-m+1} - w_m r^{-m}.$$

$$\sum_{j=1}^{m} w_j r^{-j} \le 1 \qquad \text{أو}$$

وهذا يعني:

$$\underbrace{\frac{1}{r}+\frac{1}{r}+...+\frac{1}{r}}_{w_1}+\underbrace{\frac{1}{r^2}+\frac{1}{r^2}+...+\frac{1}{r^2}}_{w_2}+...+\underbrace{\frac{1}{r^m}+\frac{1}{r^m}+...+\frac{1}{r^m}}_{w_m} \le 1$$

لكن $w_1 + w_2 + ...w_m = n$ أي تساوي العدد الكلي لكلمات الترميز وهذه المتراجحة مطابقة لـ:

$$\sum_{i=1}^{n} r^{-l_i} \le 1$$

لاحظ أن متراجحة كرافت تشير إلى الترميز الآني الموجود له كلمات ترميز بطول l_i. هذا لا يعني أن كل ترميز يحقق هذه المتراجحة هو آني.

تهتم الخطوة التالية بأسلوب الاختيار المناسب للطول l_i. يفضل البعض أن تكون أطوال كلمات الترميز مرتبطة باحتمال ظهور الرسالة لتحقيق الاستخدام المثالي للقناة. أي أن البعض يفضل أن يعطي للرسالة ذات الاحتمال الأكبر كلمة ترميز أقصر من بقية الرسائل ذات احتمال الحدوث الأصغر.

مثال (2—4):

لنأخذ ترميز مورس ، حيث تبدل الأحرف من الأبجدية إلى كلمات ترميز مؤلفة من نقاط وشرطات، كلمات الترميز الموافقة للأحرف التي تظهر بكثرة (مثل

حرف e) اختيرت بحيث تحتوي على القليل من النقاط أو الشرطات قدر الإمكان ،هذا من جهة، وتتألف من النقاط وهي المفضلة من جهة أخرى لأنها تأخذ وقتاً أقصر من الشرطة. تحتاج النقطة 2 وحدة زمنية ، بينما تحتاج الشرطة إلى 4 وحدات زمنية ، ويحتاج الفراغ بين الأحرف 3 وحدات زمنية . يظهر الشكل (2—2) ترميز مورس للأحرف .

تعطي النظرية التالية العلاقة بين متوسط طول كلمة الترميز L وكمية المعلومات الخاصة بالمنبع.

2 – 2 – 2 نظرية (نظرية ترميز المنبع):

لنفرض أن لدينا مجموعة من n كلمة ترميز u_i باحتمالات $P = (p_1,..., p_n), p_i > 0$ من أجل كل قيم i ،حيث تتألف جميع كلمات الترميز من أحرف تتبع للأبجدية $S = (s_1, s_2,..., s_r)$ ، فإذا تحققت متراجحة كرافت فهذا يعني:

$$\frac{H(U)}{\log r} \le L \qquad (8-2)$$

حيث L متوسط طول كلمة الترميز وهي معرفة بالشكل:

$$L = \sum_{i=1}^{n} p_i l_i \qquad (9-2)$$

و l_i هي طول كلمة الترميز ui .

تتحقق المساواة فقط إذا كان $p_i = r^{-l_i}$ من أجل $i = 1,...n$

البرهان:

لدينا :

$$H(U) - L\log r = -\sum_{i=1}^{n}[p_i \log p_i + p_i l_i \log r]$$

$$= \sum_{i=1}^{n} p_i \log\left\{\frac{1}{p_i r^{l_i}}\right\} = \sum_{i=1}^{n} p_i \frac{\ln\left\{\frac{1}{p_i r^{l_i}}\right\}}{\ln 2} \qquad (10-2)$$

وطالما $a > 0$ فأن $\ln a \le a - 1$ وتحصل المساواة عندما $a = 1$ ومن المعادلة (10−2) نجد:

$$\sum_{i=1}^{n} p_i \ln\left\{\frac{1}{p_i r^{l_i}}\right\} \le \sum_{i=1}^{n} p_i \left(\frac{1}{p_i r^{l_i}} - 1\right) = \sum_{i=1}^{n} r^{-l_i} - 1$$

وبما أن متراجحة كرافت قد تحققت فإننا نستنتج:

$$H(U) - L \log r \le 0$$

وهي تعطي بالضبط المعادلة (2−8) يمكن استنتاج متطلب المساواة بشكل مباشر فيما يلي:

Symbol	Probability	Morse code	Symbol	Probability	Morse code
A	0.0642	• —	N	0.0574	— •
B	0.0127	— • • •	O	0.0632	— — —
C	0.0218	— • — •	P	0.0152	• — — •
D	0.0317	— • •	Q	0.0008	— — • —
E	0.1031	•	R	0.0484	• — •
F	0.0208	• • — •	S	0.0515	• • •
G	0.0152	— — •	T	0.0796	—
H	0.0467	• • • •	U	0.0228	• • —
I	0.0575	• •	V	0.0083	• • • —
J	0.0008	• — — —	W	0.0175	• — —
K	0.0049	— • —	X	0.0014	— • • —
L	0.0321	• — • •	Y	0.0164	— • — —
M	0.0198	— —	Z	0.0005	— — • •
			SPACE	0.1859	

الشكل (2−2) جدول ترميز مورس

تشير النظرية (2-2)إلى أن الطول المتوسط لن يكون أصغر من كمية المعلومات (بواحدة الـ r) لمنبع المعلومات. يظهر أصغر طول متوسط لكلمات الترميز عندما نختار الأطوال بعناية حتى تتحقق المساواة للمعادلة (2-8) .

وهذا يحصل إذا كان من أجل كل قيم i يتحقق:

$$p_i = r^{-l_i} \quad or \quad l_i = -\log_r p_i \qquad (11-2)$$

يتحقق ذلك فقط إذا كان $-\log_r p_i$ هو العدد الكلي، لأن l_i هي طول كلمة الترميز المشكلة من العدد الكلي للأحرف ذات الطول يساوي الـ 1. وإذا لم تكن $-\log_r p_i$ هي العدد الكلي، فلن يكون هناك ترميز مثالي أبداً. يبدو واضحاً التوجه لاختيار العدد الصحيح الذي يصادف مباشرة بعد الطول l_i ، أي نختار l_i حسب الطريقة التي تحقق :

$$-\log_r p_i \le l_i <= \log p_i + 1 \qquad (12-2)$$

نلاحظ هنا في حالة الترميز المثالي أي $l_i = -\log_r p_i$ أنه لدينا $\sum_i r^{-l_i} = 1$ (بالمقارنة مع متراجحة كرافت) ، أما في الحالات الأخرى فسيكون $\sum_i r^{-l_i} < 1$.

نستطيع ببساطة استناداً للنظرية (2-2) وضع شرط المساواة للترميز. واقتراب القيمة $H(U)/(L\log r)$ من قيمة الواحد تجعل الترميز أكثر فعالية.

تعريف (2-2):

تعرف كفاءة (فعالية) الترميز η بالمعادلة التالية :

$$\eta = \frac{H(U)}{L\log r} \qquad (13-2)$$

حيث أن $H(U)$ هي كمية معلومات المنبع ، L هي متوسط طول كلمات الترميز، و r هي حجم أبجدية الترميز.

مثال (2-5):

منبع معلومات له أبجدية مؤلفة من أربعة رموز منبع u_1,u_2,u_3,u_4 . تتألف أبجدية الترميز من رمزين فقط 0 و 1.احتمالات رموز الرسالة كلها مساوية لـ 1/4. بفرض شكل الترميز هو :

symbol	Code (r=2)
u_1	00
u_2	01
u_3	10
u_4	11

لهذا الترميز $H(U)=\log 4 bits,\ r=2\quad ,L=2$ ، وبالتالي كفاءة هذا الترميز هي: $\eta=\frac{H(U)}{L\log r}=\frac{2}{2\times 1}=1=100\%$

مثال (2-6):

لنأخذ المنبع نفسه ونغير الاحتمالات ، ولتكن $\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{8}$ ،ونأخذ الترميز نفسه سنجد:

$$H(U)=-\frac{1}{2}\log\frac{1}{2}-\frac{1}{4}\log\frac{1}{4}-2\times\frac{1}{8}\log\frac{1}{8}=\frac{7}{4}\ bits,\ r=2\quad ,L=2$$

وستكون كفاءة الترميز:

$$\eta=\frac{7/4}{2\times 1}=\frac{7}{8}=87.5\%$$

مثال(2-7):

لنأخذ المنبع السابق نفسه ونجعل الترميز حسب الجدول التالي:

symbol	Code (r=2)
u_1	0
u_2	10
u_3	110
u_4	111

نجـــــــد أيضـــــــاً أن $H(U)=\frac{7}{4}\ bits,\ r=2$ لكـــــــن الآن

$$L=p_1\times 1+p_2\times 2+p_3\times 3+p_4\times 3=\frac{1}{2}\times 1+\frac{1}{4}\times 2+\frac{1}{8}\times 3+\frac{1}{8}\times 3=\frac{7}{4}$$

وتصبح الكفاءة هنا:

$$\eta=\frac{7/4}{7/4\times 1}=1=100\%$$

نلاحظ هنا أن شرط الترميز المثالي قد تحقق وهو $p_i=r^{-l_i}$ من كل قيم i.

2 – 3 استراتيجيات الترميز *Coding strategies*:

لقد تم في الفقرات السابقة مناقشة متطلبات الحصول على الترميز المثالية أي تلك الترميز ذات الكفاءة العالية، هناك الكثير من الاستراتيجيات المعروفة والتي تساعدنا للوصول إلى ترميز يقترب من المثالية . من المفروض من أجل الترميز الثلاثة الأولى التالية ترتيب رموز المنبع حسب تناقص الاحتمالات.

2 – 3 – 1 ترميز فانو Fano code

بعد ترتيب رموز أو رسائل خرج المنبع حسب تناقص احتمالاتها ، نقوم بتقسيم الرموز إلى r مجموعة متساوية الاحتمالات قدر الإمكان. تأخذ كل مجموعة واحد من r حروف الترميز كأول خانة . يكرر هذا التقسيم لكل مجموعة لأكثر من مرة طالما هناك إمكانية للتقسيم.

مثال (2–8):

نجد في هذا المثال أن $H(U) = L = 2.88$ وبالتالي كفاءة هذا الترميز ستساوي $\eta = 1$ ، بالطبع ليس ممكناً على الدوام تقسيم الاحتمالات إلى مجموعات متساوية الاحتمال بدقة ، في هذه الحالة يجب أن يكون التقسيم جيداً قدر الإمكان ، وفي النتيجة قد نحصل على عدة خيارات .

Symbol	Probability	Binary code(r=2)
u_1	1/4	00
u_2	1/4	01
u_3	1/8	100
u_4	1/8	101
u_5	1/16	1100
u_6	1/16	1101
u_7	1/32	11100
u_8	1/32	11101
u_9	1/32	11110
u_{10}	1/32	11111

مثال (2-9):

في هذا المثال أطوال كلمات الترميز المتوسطة هي نفسها (L=2.22). إذا لم نحصل على هذه الحالة فإنه يفضل اختيار الترميز ذي الكفاءة الأعلى .يمكن تطبيق فانو أيضاً في حالة r>2.

في الحالة العامة طول كلمات الترميز الوسطي سينقص عند زيادة حجم أبجدية الترميز r. (انظر المثال(2-10))

Symbole	Probability	Code1 (r=2)	Code2 (r=2)
u_1	1/3	00	0
u_2	1/3	01	10
u_3	1/9	10	110
u_4	1/9	110	1110
u_5	1/9	111	1111

مثال (2−10):

Symbol	Probability	Code1 (r=2)	Code2 (r=3)	Code3 (r=4)
u_1	0.30	00	0	0
u_2	0.25	01	10	1
u_3	0.12	100	11	20
u_4	0.10	101	20	21
u_5	0.10	110	21	30
u_6	0.05	1110	220	31
u_7	0.04	11110	221	32
u_8	0.04	11111	222	33
H(U)=2.64bits/symbol		L_1=2.66	L_2=1.83	L_3=1.45
		$\eta_1 = 0.99$	$\eta_2 = 0.91$	$\eta_3 = 0.91$

2− 3 − 1 ترميز شانون Shannon code:

يقوم شانون بحساب سلسلة من الاحتمالات التراكمية $p_k = \sum_{i=1}^{k-1} p(u_i)$ من أجل $k = 1,2,...,n$ ، وسيتم كتابة هذه الاحتمالات فيما بعد (في الترميز الثنائي) بالنظام الثنائي. عدد الرموز لكل كلمة ترميز تحسب من المتراجحة التالية:

$$\log \frac{1}{p_k} \le l_k < \log \frac{1}{p_k} + 1 \qquad (14-2)$$

في المثال التالي تم تمثيل رمز المنبع u6 بالرمز 1101 لأن p6=13/16 حيث يكتب بالشكل $1\times 2^{-1}+1\times 2^{-2}+0\times 2^{-3}+1\times 2^{-4}$. يجب أن يكون عدد حروف الترميز على الأقل $\log(1/p_k)=\log 16=4$ لذلك لن نحتاج إلى أصفار نضيفها لهذا الرمز .

مثال (2-11):

Symbol	probability	p_k	Length l_i	Code(r=2)
u_1	1/4	p_1=0	$l_1=2$	=00
u_2	1/4	p_2=1/4	$l_2=2$	=01
u_3	1/8	p_3=1/2	$l_3=3$	=100
u_4	1/8	p_4=5/8	$l_4=3$	=101
u_5	1/16	p_5=3/4	$l_5=4$	=1100
u_6	1/16	p_6=13/16	$l_6=4$	=1101
u_7	1/32	p_7=7/8	$l_7=5$	=11100
u_8	1/32	p_8=29/32	$l_8=5$	=11101
u_9	1/32	p_9=15/16	$l_9=5$	=11110
u_{10}	1/32	p_{10}=31/32	$l_{10}=5$	=11111

نستخلص من المثال (2-11) أن طريقة شانون في هذه الحالة تعطي الترميز نفسه الذي تعطيه طريقة فانو (قارن مع المثال (2-8)). لكن هذه الحالة ليست دائمة وهذا ما سنراه في حالة المثال التالي.

مثال(2-12):

Symbol	probability	p_k	l_i	Shannon code (r=2)	Fano code (r=2)
u_1	0.4	0	2	00	0
u_2	0.3	0.4	2	01	10
u_3	0.2	0.7	3	101	110
u_4	0.1	0.9	4	1110	111

تسمى النتيجة الخاصة لترميز فانو في هذا المثال بترميز الفاصلة، لأن الخانة الثنائية 0 تشير هنا إلى نهاية كلمة الترميز بالإضافة إلى حقيقة أنه لا توجد كلمة ترميز طولها أكبر من 3.

2 - 3 - 2 ترميز هوفمان Huffman code

في ترميز هوفمان وفي حالة الترميز الثنائي ندمج آخر رسالتين (حرفين) لخرج المنبع والأقل احتمالاً مع بعضهما لتشكيل أبجدية رسائل جديدة حجمها أقل بمقدار عنصر واحد، يعاد الترتيب من جديد ومن ثم مرة أخرى يتم دمج عنصرين بالطريقة نفسها ، تكرر هذه العملية حتى يتبقى لدينا عنصران فقط. يعطى لهذين العنصرين الرموز 0 و 1 من النظام الثنائي ،وبالعودة للخلف يضاف 0 أو 1 إلى كلمة الترميز عند كل مكان تم فيه دمج العنصرين مع بعضهما

مثال (2-13)

symbol	probability					code(r=2)
u_1	0.4	0.4	0.4	0.4	0.6(0)	1
u_2	0.3	0.3	0.3	0.3(0)	0.4(1)	00
u_3	0.1	0.1	0.2(0)	0.3(1)		011
u_4	0.1	0.1(0)	0.1(1)			0100
u_5	0.06(0)	0.1(1)				01010
u_6	0.04(1)					01011

يعطي هذا المثال نتيجة قابلة للمقارنة مع نتيجة طريقة فانو حيث تعطي طريقة شانون ترميزاً أقل كفاءة ، بينما تؤدي طريقة هوفمان في الحالة العامة إلى ترميز أكثر كفاءةً .

إذا كان عدد أبجدية الترميز هو r فإن ترميز هوفمان المثالي يتحقق عندما يكون عدد رموز منبع هو $r+k(r-1)$ ،حيث k عدد صحيح. فإذا كان عدد رموز المنبع أقل من ذلك ، فإنه يجب إضافة هذه الرموز وإعطاؤها احتمالاً يساوي الصفر وإهمالها في النهاية .لنأخذ المثال التالي:

مثال (2-14):

symbol	probability			code(r=3)
u_1	1/3	1/3	4/9(0)	1
u_2	1/6	2/9	1/3(1)	00
u_3	1/6	1/6(0)	2/9(2)	01
u_4	1/9	1/6(1)		02
u_5	1/9(0)	1/9(2)		20
u_6	1/9(1)			21
u_7	0(2)			22

نلاحظ هنا أن طول كلمة الترميز الوسطي L=1.67 ، بينما لو أننا لم نضف الرمز u_7 واستخدمنا ترميز هوفمان لكان الطول الوسطي هو L=2

2 – 3 – 3 ترميز جيلبرت– مور (الترميز الأبجدي)

Gilbert-Moore code(alphabetic code)

تختلف طريقة جيلبرت– مور بشكل كلي عما سبق. في هذه الطريقة توضع رموز خرج المنبع بأي ترتيب مرغوب (الهجائي مثلاً). فإذا كان طول كلمة الترميز u_i هو l_i فهو يحدد حسب العلاقة التالية :

$$2^{1-l_i} \le p(u_i) < 2^{2-l_i}, \quad i = 1,2,...,n \qquad (15-2)$$

ونوجد السلسلة المتزايدة $(\alpha_1, \alpha_2, ...)$ حسب الشكل التالي:

$$\left.\begin{aligned} &\alpha_1 = \frac{1}{2} p(u_1), \\ &\alpha_2 = p(u_1) + \frac{1}{2} p(u_2), \\ &\vdots \\ &\alpha_i = p(u_1) + p(u_2) + ... + p(u_{i-1}) + \frac{1}{2} p(u_i). \end{aligned}\right\} \qquad (16-2)$$

لدينا هنا $0 \le \alpha_1 \le \alpha_2 ... \le 1$. ونحصل على الرمز الخاص بـ u_i بتحويل العدد α_i إلى النظام الثنائي ونقتصر على الطول l_i.

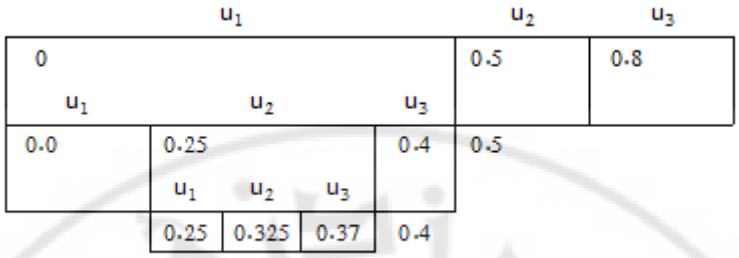
مثال (2–15):

لنأخذ أول ثلاثة أحرف من الأبجدية a, b, c مع احتمالات ظهورها في اللغة الانكليزية وسنجد:

symbol	probability	l_i	α_i	code(r=2)
u_1	0.064	5	0.032	00001
u_2	0.013	8	0.071	00010010
u_3	0.022	7	0.088	00010111

2 – 3 – 4 الترميز الحسابية The arithmetic code:

باستخدام هذا الترميز ننظر إلى الاحتمالات $p(u_1), p(u_2),..., p(u_n)$ الخاصة برموز خرج المنبع على أنها مسافات جزئية من المجال الواحدي $[0,1]$ (مجموع الاحتمالات يساوي الواحد) . سوف نطبق جوهر هذه الطريقة على ثلاثة رموز n=3 حيث $p(u_1) = 0.5, p(u_2) = 0.3, p(u_3) = 0.2$. تحسب الاحتمالات التراكمية $P_1 = 0, P_2 = 0.5, P_3 = 0.8$ ، يظهر هذا في الشكل (2–3). حيث كل نقطة ستمثل الاحتمال التراكمي P_i الخاص بالرموز $u_1, u_2,..., u_{i-1}$. فإذا حصل رمز المنبع u_1 (باحتمال 0.5) فهذا يوافق المجال $[0.0, 0.5]$. وبعد ذلك لنفرض أن الرمز الثاني قد تولد من المنبع. لذلك نقسم المجال الحالي أي $[0.0, 0.5]$ مرة أخرى إلى مجالات جزئية حسب توزع الاحتمالات التراكمية للمنبع أي $0.0, 0.5, 0.8, 1.0$ لينتج لدينا ثلاثة مجالات جزئية $[0.0, 0.25]$ و $[0.25, 0.4]$ و $[0.40, 0.50]$. إذا تولد الرمز u_2 سنجد أنفسنا بعد رمزي منبع ضمن المجال $[0.25, 0.4]$. وعند تكرار العملية نشكل النتيجة كما لو أن تتابع رموز المنبع ضمن مجال جزئي $[0, 1]$ ومرتبطة به.



الشكل (2−3) طريقة الترميز الحسابي

نأخذ الآن التمثيل الثنائي للنقطة في أقصى اليسار من المجال لتشكيل كلمة الترميز الخاصة بتتابع رموز المنبع $u_1,u_2,.....etc$. يقابل عرض المجال هنا بالاحتمال الذي يحصل فيه التتابع الموافق لرموز المنبع.

نستطيع الآن اعتبار الترميز عملية عودية تعمل بالشكل التالي:

من أجل كل خطوة وعندما يظهر رمز منبع جديد مرة أخرى، سنفترض النقطة أقصى اليسار C للمجال الحالي والعرض الحالي A للمجال نفسه. النقطة أقصى اليسار الجديدة هي النقطة القديمة إضافة إلى جزء من عرض المجال الحالي، استناداً إلى:

$$C_{new} = C_{old} + A_{old} p_i \qquad (17-2)$$

حيث P_i هي الاحتمال التراكمي للعنصر u_i. يحسب عرض المجال الجديد عن طريق ضرب العرض القديم بالاحتمال P_i، أي:

$$A_{new} = A_{old} P_i \qquad (18-2)$$

في المثال للشكل(2−3) لدينا في البداية:

$$C_{start} = 0.0$$
$$A_{start} = 1.0$$

بعد الرمز u_1 نحصل على النتائج التالية:

$$C_{new} = 0.0 + 1.0 \times 0.0 = 0.0$$
$$A_{new} = 1.0 \times 0.5 = 0.5$$

وبعد الرمز الثاني u_2 سنحصل بالتتابع على :

$$C_{new} = 0.0 + 0.5 \times 0.5 = 0.25$$
$$A_{new} = 0.5 \times 0.3 = 0.15$$

فإذا قمنا بترميز مجموعة من l رمز أو حرف مع بعضها وفقاً لهذا المسار العودي، فإننا سنستطيع إيجاد النقطة اليسارية C والعرض A للمجال الناتج. وللوصول إلى كلمة الترميز النهائية سنختار النقطة اليسارية C ونكتبها بالشكل الثنائي باستخدام عدد من الخانات الثنائية بطريقة تمكننا من التفريق بينها وبين النقاط اليسارية للمجالات الأخرى، في هذا المثال يمكن ترميز زوج من رموز المنبع u_1, u_2 عن طريق إيجاد التمثيل الثنائي للرقم العشري 0.25 وهو 0.01 .

إن كاشف الترميز في الواقع يتبع العملية المعاكسة ، ويحدد، خطوة خطوة، أي الرموز قد ظهر ضمن المجال الحالي، ومنه يحدد أيضاً المجال السابق.

2 – 3 – 5 الترميز استناداً إلى توسيع الأبجدية:

افترضنا في هذا الفصل أن المنبع من دون ذاكرة وبالتالي رموز المنبع المتتالية مستقلة ، لكن وبالرغم من ذلك فإن ترميز مجموعة من الرموز ستؤدي إلى ترميز فعال . لهذا نقوم بتجميع l من رموز المنبع على شكل رسالة، وحساب احتمال هذه الرسائل وبعدها استخدام أيٍ من استراتيجيات الترميز (مثل هوفمان) للحصول على الترميز النهائي. سنناقش هذه الطريقة، المسماة بتوسع الأبجدية، بمساعدة المثال التالي.

مثال 2–16:

لدينا منبع يولد على خرجه الرمزين u_1, u_2 باحتمالات على الترتيب $\frac{3}{4}, \frac{1}{4}$.

استخدمت طريقة فانو لإيجاد هذا الترميز:

symbol	probability	code(r=2)
u_1	3/4	0
u_2	1/4	1

ونحسب $H(U) = 0.811\ bit,\ L = 1,\ r = 2,\ \eta = 0.81$

بعد هذا سنقوم بدمج عنصرين لتشكيل رسائل جديدة $v_1,\ldots,v_4$ ويصبح لدينا الآن:

$$H(V) = 1.622\ bit,\ \ L = 27/16,\ \ r = 2,\ \eta = 0.961$$

symbol	probability	code(r=2)
$v_1 = u_1u_1$	$p(v_1) = p(u_1, u_1) = \frac{9}{16}$	$\underline{0}$
$v_2 = u_1u_2$	$p(v_2) = p(u_1, u_2) = \frac{3}{16}$	$1\underline{0}$
$v_3 = u_2u_1$	$p(v_3) = p(u_2, u_1) = \frac{3}{16}$	$11\underline{0}$
$v_4 = u_2u_2$	$p(v_4) = p(u_2, u_2) = \frac{1}{16}$	111

نلاحظ زيادة ملحوظة بالكفاءة عند دمج عنصرين من المنبع، فعند ترميز l عنصر منبع مع بعضهم سيتشكل لدينا منبع جديد بأبجدية موسعة ، بالضبط n^l رسالة (بدلاً من المنبع الأصلي بـ nعنصر)، حيث يصبح احتمال الرسالة الجديدة عبارة عن جداء احتمالات الرموز التي تشكلها.

الفصل الثالث

منبع المعلومات المتقطعة مع الذاكرة

The discrete information source with memory

وقل رب زدني علما
جامعة دمشق
Damascus University

الفصل الثالث

منبع المعلومات المتقطعة مع الذاكرة

The discrete information source with memory

3-1 عمليات ماركوف *Markov process*

لقد فرضنا في الفصل الثاني أن منابع المعلومات لا تملك ذاكرة، وهذا يعني أن الرموز المتتابعة في الرسالة المولدة من المنبع مستقلة احتمالياً. لكن في الكثير من التطبيقات العملية نجد أن ذلك غير محقق، واحتمال ظهور الرمز في الرسالة سوف يعتمد على عدد محدد من الرموز التي سبقته. وفي هذه الحالة نتكل على ما يسمى بالمنبع مع الذاكرة. يعد التتابع المولد من منبع كهذا المنبع مشابهاً لما يسمى بسلسلة ماركوف Markov chain .وقبل أن نناقش المنبع المتقطع مع الذاكرة ، سنورد بعضاً من خصائص سلاسل ماركوف بشيء من التفصيل.

لنأخذ تتابع من المتحولات الإحصائية المنفصلة (المتقطعة) $u_1,u_2,..u_{n-1}$، يمكن أن تكون هذه رموز من منبع معلومات متقطع، أو عينات مكماة من إشارة عشوائية. العنصر الأول u_1 متعلق مع كل الرموز التي يمكن أن تأتي في المركز الأول، u_2متعلق بالرموز التي يمكن أن تأتي في المركز الثاني، ..وهكذا.

في حالة المنابع من دون ذاكرة كل رموز الرسالة المولدة يمكن أن تكون كل الرموز المتوفرة لأبجدية المنبع. لكن في حالة المنبع مع الذاكرة يمكن أن يقتصر الرمز الثاني مثلاً على مجموعة جزئية محددة من أبجدية المنبع بسبب ظهور الرمز الأول قبله، وهكذا.....، نهتم الآن بتوزع الاحتمالات الخاص بـ u_n ،الذي

حسب سلسلة ماركوف من الدرجة kيعتمد على قيم k متحول احتمالي يسبقها أي $\mathbf{u_{n-k}, u_{n-(k-1)}, \ldots, u_{n-1}}$حيث تختار k بالطريقة التي تحقق:

أ- قيم المتحولات الاحتمالية التي تسبق $\mathbf{u_{n-k}}$ لن يكون لها أية تأثير في التوزع الاحتمالي لـ $\mathbf{u_n}$,

ب-k هي القيمة الأصغرية الممكن تحقيقها.

الاحتمال الشرطي للقيمة u_n للمتحول الإحصائي $\mathbf{u_n}$ وعند معرفة كل القيم السابقة $u_{n-1}, u_{n-2}, \ldots\ldots$سيساوي $p(u_n / u_{n-k}, u_{n-k+1}, \ldots, u_{n-1})$ ، تشكل تركيبة القيم $S_i = (u_{n-k}, u_{n-k+1}, \ldots, u_{n-1})$ الجزء الشرطي من توزع الاحتمالات الشرطية لـ $\mathbf{u_n}$، ولذلك نسمي S_i بحالة سلسلة ماركوف state of Markov chain. فإذا حدثت القيمة u_n، فإن سلسلة ماركوف تتقدم إلى حالة جديدة S_j:

$$S_j = (u_{n-(k-1)}, u_{n-(k-2)}, \ldots, u_n)$$

نتكلم هنا عن الانتقال من الحالة S_i إلى الحالة S_j. بالإضافة إلى إيجاد التوزع الاحتمالي الشرطي لـ $\mathbf{u_n}$ نستطيع وصف سلسلة ماركوف بإيجاد مصفوفة الاحتمالات الانتقالية من أجل عدة حالات. سنرمز لاحتمال انتقال سلسلة ماركوف من الحالة S_i إلى الحالة S_j بـ $P(j/i)$.

لاحظنا في الفقرة (2-1) أنه عند توليد l رمز من منبع معلومات تم التعامل معها على أساس رسالة جديدة . لكن في الواقع نحن نتعامل مع منبع معلومات جديد له أبجدية أخرى V، الرمز فيه سيتألف من مجموعة رموز من الأبجدية الأصلية U. فإذا نظرنا إلى التركيبة S_i المؤلفة من k قيمة من المتحولات الاحتمالية بالطريقة نفسها كما لو أن S_i متحول احتمالي جديد، وعندها احتمال الحالة S_j سوف يعتمد فقط على الحالة S_i. عند ذلك تخفض سلسلة ماركوف من الدرجة القديمة k من حيث الرموز إلى سلسلة ماركوف من الدرجة 1 من حيث

الحالات. لقد استخدم عالم الرياضيات الروسي سلاسل من الدرجة k بقيم أكبر من الواحد، لكن هنا سنقتصر على السلاسل من الدرجة k=1 استثنائياً. على كل حال، في نظرية المعلومات لتوخي الدقة يجب الاهتمام بسلاسل ماركوف من الدرجات العالية لأن وصف منبع المعلومات من خلالها سيصبح في بعض الأحيان أبسط.

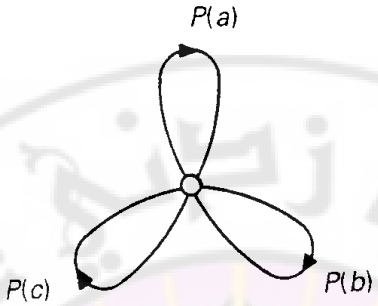
إذا فرضنا هنا أن كل متحول احتمالي u_i له m قيمة ممكنة ، عندها سلسلة ماركوف من الدرجة k ستقتصر على m^k حالة مختلفة، بحيث تتحدد كل حالة بتتابع من k رمز اختير أي منها من m إمكانية. بعد كل حالة نستطيع الاختيار بين m إمكانية ، ولذلك فهناك m^{k+1} انتقال يمكن تخيله وعدد احتمالات الانتقال لأي منها متساوٍ. من أجل أي مجموعة من m احتمال انتقال، هناك $m-1$ احتمال يمكن الاختيار فيما بينها بحرية. وتثبت بعدها باقي الاحتمالات، لأن مجموع احتمالات الانتقال يساوي الواحد. عندئذ تتحدد m^{k+1} احتمال انتقال عن طريق $m^{k+1}-m^k$ احتمال انتقال يمكن الاختيار بينها بحرية.

نستطيع الآن وصف الحالات المعرفة بواسطة احتمالاتها الانتقالية باستخدام مخطط الحالة state diagram. سنفرض في البداية أن تتابع الرموز المستقلة احتمالياً بأبسط حالاته، حيث k تساوي الصفر، عندها الحديث سيدور عن سلسلة ماركوف من الدرجة 0 . في مثل هذه السلسلة سيكون لدينا حالة وحيدة فقط S ، وبعد كل انتقال تعود السلسلة إلى الحالة نفسها . عدد الانتقالات الممكنة سيساوي عدد الرموز الممكن الاختيار فيما بينها، فمن أجل ثلاثة رموز (a, b, c) تشكل السلسلة المبينة بالشكل (3-1).

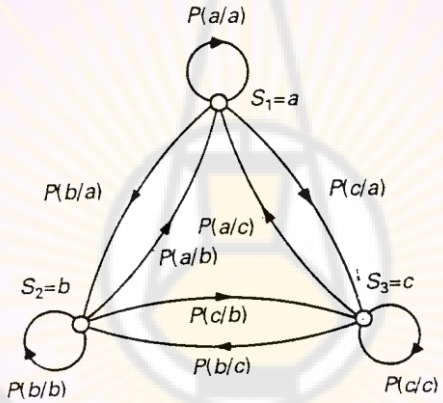
من أجل سلسلة ماركوف من الدرجة 1 ،عدد الحالات سيساوي عدد الرموز، وإذا كان عدد الرموز 3 و هي a, b, c فإن عدد الانتقالات هو $3^2=9$ وهي :

$$a \to a, a \to b, a \to c, b \to a, ...etc$$

تمثل سلسلة ماركوف هذه في الشكل (3−2)



الشكل(3−1)مخطط حالة لسلسلة ماركوف من الدرجة 0



الشكل (3−2) مخطط حالة لسلة ماركوف من الدرجة الأولى

نستطيع أن نشير للحالات S_1, S_2, S_3 في هذا المثال بـ a, b, c .وبشكل طبيعي من أجل كل حالة S_i, $i = 1, 2, and\ 3$ ، سنجد:

$$P(S_1 / S_i) + P(S_2 / S_i) + P(S_3 / S_i) = 1 \qquad (1-3)$$

تتحدد قيم احتمالات الحالات الثلاث من احتمالات الانتقال:

$$P(S_i) = P(S_1) \cdot P(S_i / S_1) + P(S_2) \cdot P(S_i / S_2) + P(S_3) \cdot P(S_i / S_3) \qquad (2-3)$$

من أجل $i = 1, 2, 3$.

تظهر نظرية بايس كيف يمكن حساب الاحتمالات الشرطية $p(x_i / y_j)$ استناداً إلى الاحتمالات المشروطة $q(y_j / x_i)$. لكن هذه النظرية يمكن ألا تستخدم من أجل احتمالات الانتقال في سلاسل ماركوف . والسبب في ذلك أن هذه النظرية صحيحة إذا كان من أجل كل قيم i, j تتحقق العلاقة التالية:

$$p(x_i, y_j) = p(y_j, x_i)$$

على كل حال، هذه ليست المسألة نفسها من أجل سلاسل ماركوف. حيث لدينا بالمقابل :

$$P(S_i, S_j) \neq P(S_j, S_i) \qquad (3-3)$$

السبب في ذلك هو أن عامل الزمن يلعب دوراً مهماً في سلاسل ماركوف حتى إنه يتدخل في ترتيب الرموز. فإذا نظرنا إلى اللغة المكتوبة (التي تعد من عمليات ماركوف، حيث أن ظهور أي حرف محكوم بالحروف التي سبقته) يصبح واضحاً أن احتمال زوج الحروف (q,u) لن يساوي احتمال زوج الحروف (u,q).

تعود أهمية سلاسل ماركوف إلى حقيقة أن k ،عدد المتحولات الاحتمالية والتي ستحدد قيمها احتمال الانتقال إلى المتحول الاحتمالي التالي $\mathbf{u_n}$ ، هي رقم محدد ولذلك لن ننظر إلى الماضي حتى اللانهاية.

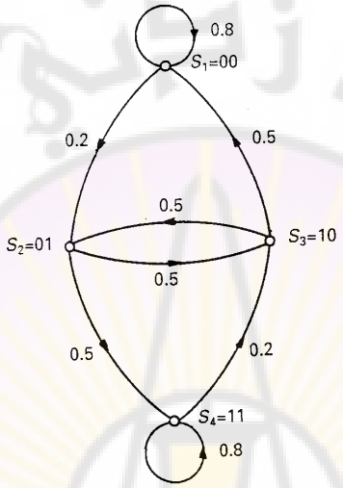
مثال (3-1):

لنأخذ مولد معلومات يولد سلسلة ماركوف . أبجدية المنبع هي $U = \{0,1\}$. وبفرض الاحتمالات الانتقالية هي :

$$P(0/00) = P(1/11) = 0.8,$$
$$P(1/00) = P(0/11) = 0.2,$$
$$P(0/01) = P(0/10) = P(1/01) = P(1/10) = 0.5.$$

نستطيع القول في البداية أننا هنا نتعامل مع سلسلة ماركوف من الدرجة الثانية. يرتبط ظهور أي رمز بظهور رمزين قبله. أي هناك أربع

حالات:00,01,10,11، مخطط الحالة يمثل في الشكل (3-3).ونستنتج من هذا الشكل أننا لا نستطيع الوصول مباشرة من أية حالة إلى أية حالة أخرى، إننا نستطيع الانتقال إلى S_2من الحالة S_1، لكننا لا نستطيع الانتقال من S_3 أو S_4.



الشكل (3-3) مخطط الحالة للمثال (3-1)

وفي بعض الأحيان نستطيع التحرك من حالة إلى حالة أخرى لكن لا نستطيع العودة بالطريق نفسه: نستطيع الذهاب إلى S_2من S_1، لكن لا نستطيع الذهاب من S_2إلى S_1 مباشرة. يمكن حساب الاحتمالات الفردية للحالات S_1وحتى S_4 انطلاقاً من المعادلة (3-2).

$$P(S_1) = P(S_1)\cdot P(S_1/S_1) + P(S_2)\cdot P(S_1/S_2) + P(S_3)\cdot P(S_1/S_3) + P(S_4)\cdot P(S_1/S_4)$$
$$= P(S_1)\cdot 0.8 + P(S_2)\cdot 0 + P(S_3)\cdot 0.5 + P(S_4)\cdot 0$$
$$= 0.8P(S_1) + 0.5P(S_3)$$

وبالطريقة نفسها نحصل على:

$$P(S_2) = P(S_1)\cdot 0.2 + P(S_2)\cdot 0 + P(S_3)\cdot 0.5 + P(S_4)\cdot 0$$
$$= 0.2P(S_1) + 0.5P(S_3)$$

$$P(S_3) = P(S_1)\cdot 0 + P(S_2)\cdot 0.5 + P(S_3)\cdot 0 + P(S_4)\cdot 0.2$$
$$= 0.5P(S_2) + 0.2P(S_4)$$
$$P(S_4) = P(S_1)\cdot 0 + P(S_2)\cdot 0.5 + P(S_3)\cdot 0 + P(S_4)\cdot 0.8$$
$$= 0.5P(S_2) + 0.8P(S_4)$$

بحل هذه المعادلات الأربع لحساب المجاهيل الأربعة نجد:

$$P(S_1) = P(S_4) = 5/14$$
$$P(S_2) = 0.8P(S_3) = 2/14$$

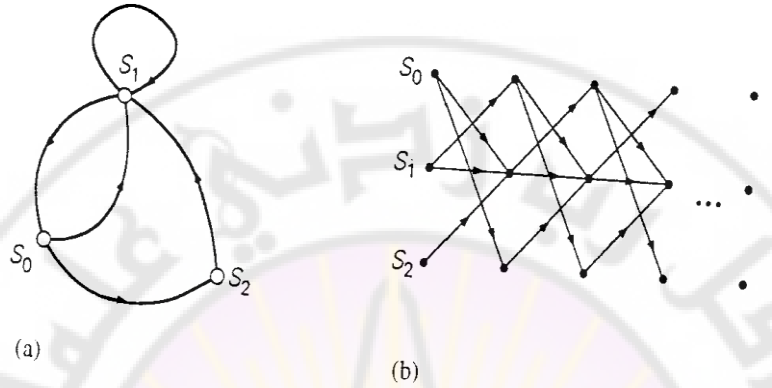
في بعض الأحيان ومن أجل الإتقان والتوضيح نبدل مخطط الحالة بالمخطط الشبكي trellis diagram. إن المخطط الشبكي في الواقع هو نفسه مخطط الحالة لكنه مفرود على محور الزمن، عندها نستطيع رؤية تغير الحالة كتابع للزمن، قارن بين الشكل (3-4)a و b . عندئذ تقابل أي سلسلة من سلاسل ماركوف بمسار خاص في المخطط الشبكي.

سنذكر هنا بعضاً من خصائص سلاسل ماركوف. وجدت اثنتان من هذه الخصائص تطبيقاتها في نظرية المعلومات وسنذكرها هنا من دون اشتقاق.

a- جزء من سلسلة ماركوف يشكل هو نفسه سلسلة ماركوف

b- سلسلة ماركوف والتي تمر بالاتجاه المعاكس هي أيضاً سلسلة ماركوف

سوف نفرض بعض الحدود على سلاسل ماركوف فيما يلي. في البداية نحن نحتاج إلى أن تكون مصفوفة احتمالات الانتقالات هي نفسها عند كل انتقال. عندها نسمي احتمالات الانتقالات بالمستقرة stationary، وسلسلة ماركوف بالمتجانسة homogeneous. سنحتاج أيضاً إلى أن تكون سلسلة ماركوف نفسها مستقرة، أي أن احتمالات الحالات في السلسلة لن تتغير. أخيراً سنحدد اهتمامنا بسلاسل ماركوف الأرغدية ergodic، وذلك يعني أنه لا يهم في أي حالة نبدأ أو نكون، فإننا نستطيع منها الوصول إلى أي حالة أخرى.

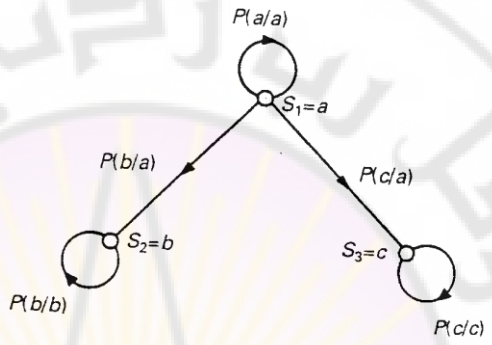


الشكل(3-4)a-مخطط الحالة، b-المخطط الشبكي

3 - 2 المعلومات للمنبع المتقطع مع الذاكرة:

توجد كمية محددة من التبعية بين الرموز المتتابعة للمنبع المتقطع مع الذاكرة. يمكن توسيع مفهوم التبعية هنا على تتابعات طويلة اعتباطية من الرموز.على كل حال نستطيع أن نفرض غالباً أن هذه التبعية توسع على عدد محدد من الرموز لجعل سلسلة ماركوف المذكورة في الفقرة (3-1) قابلة للاستخدام كنموذج لمنبع معلومات مع الذاكرة. يمكن تحديد درجة سلسلة ماركوف بالتجربة. توجد تقنيات تقدير متعددة للقيام بذلك ، لكن هذا لا يدخل في نطاق اهتمامنا في هذا المقرر ولن نعود إلى هذا الموضوع أبداً. سنفرض من الآن وصاعداً أن منبع المعلومات أرغدياً . وهذا يجعلنا نقول: إنه عند نقطة محددة من الزمن ، هناك شيء ما حول احتمال الرمز المحدد. هذا الاحتمال سيساوي احتمال ظهور الرمز نفسه ضمن سلسلة طويلة من الرموز المتتالية. المنبع المتقطع مع الذاكرة سينفع كنموذج للغة المكتوبة كمثال، وأيضاً كنمط لأي تتابع احتمالي مشتق

منها. مثال آخر وهو الإشارة المقطعة والمكماة، حيث لم نختر تردد الاعتيان بشكل صحيح، وحيث تظهر التبعية بين العينات (المكماة).



الشكل(3−5) سلسلة ماركوف غير إرغدية

3− 2 − 1 كمية المعلومات لسلسلة ماركوف من الدرجة الأولى:

من أجل سلسلة ماركوف من الدرجة الأولى لدينا عدد الرموز $u_i, i=1,2,...,m$ يساوي عدد الحالات S_i كما رأينا في الفقرات السابقة . سنفترض الآن الانتقالات من العنصر الاعتباطي u_{1i} في اللحظة الزمنية t_1 إلى الرمز u_{2j} في اللحظة t_2 حيث $i,j=1,2,...,m$. يمكن أن نرمز للاحتمال المشروط ، وهو احتمال الانتقال من u_{1i} إلى u_{2j} بـ $P(u_{2j}/u_{1i})$. يعطى الآن كمية المعلومات المتعلقة بالانتقال الاعتباطي بالعلاقة (الرجوع للمعادلة 1−29):

$$H(U_2/U_1)=-\sum_{i=1}^{m}\sum_{j=1}^{m}P(u_{1i},u_{2j})\log P(u_{2j}/u_{1i}) \qquad (4-3)$$

من أجل المعلومات المشتركة لرمزين لدينا :

$$H(U_1,U_2)=-\sum_{i=1}^{m}\sum_{j=1}^{m}P(u_{1i},u_{2j})\log P(u_{1i},u_{2j}) \qquad (5-3)$$

والأكثر من ذلك لدينا:

$$H(U_1,U_2) = H(U_1) + H(U_2/U_1), \qquad (6-3)$$

إذاً كمية المعلومات في رسالة بطول رمزين تساوي إلى مجموع كمية المعلومات الخاصة بالرمز الأول وكمية المعلومات الشرطية للرمز الثاني بالنسبة للرمز الأول. وكما رأينا سابقاً :

$$H(U_2/U_1) \le H(U_2) \qquad (7-3)$$

عندها ومن المعادلة (3-6) نجد:

$$H(U_1,U_2) \le H(U_1) + H(U_2) \qquad (8-3)$$

تتحقق المساواة فقط عندما تكون الرموز المتعاقبة مستقلة عن بعضها ، والمنبع أصبح من دون ذاكرة. ولأن المنبع مستقر وأرغدي $H(U_1) = H(U_2) = H(U)$ نعيد الكتابة لنحصل على :

$$H(U_1,U_2) \le 2H(U) \qquad (9-3)$$

وبالتالي كمية المعلومات الخاصة بالرسالة المؤلفة من رمزين في حالة المنبع مع الذاكرة أقل من المنبع من دون ذاكرة .

3– 2 – 2 كمية المعلومات لسلسلة ماركوف من الدرجات العالية:

يستطيع منبع المعلومات الاعتباطي توليد سلسلة ماركوف من الدرجة $k > 1$ ، لهذا فمن المرغوب فيه التوسع والانتقال إلى منبع بذاكرة عشوائية كبيرة . سوف نفرض لكمية المعلومات الشرطية للرمز u_N بـ $F_N(U)$ ، وفي حال معرفة N−1 رمز سابق نجد:

$$F_N(U) = H(U_N/U_{N-1},...,U_2,U_1). \qquad (10-3)$$

هناك العديد من الخصائص لكمية المعلومات الشرطية أولها هو:

$$H(U_N/U_{N-1},...,U_2,U_1 \le H(U_N/U_{N-1},...,U_2) \qquad (11-3)$$

مـا تقولـه هـذه الخاصـية هـو أن المعرفـة المنقولـة بواسـطة الرمـز الأول لا تستطيع أن تزيد في الغموض حول الرمز ذي الترتيب N، لكنها تنقصه أو تتركه من دون تغيير.

نظرية (3−1):

تتنـاقص كميـة المعلومـات الشـرطية $F_N(U) = H(U_N / U_{N-1},...,U_2,U_1)$. الرمز ذو الترتيب N في حال معرفة N−1 رمز سابق كتابع لـ N، أي:

$$H(U_N / U_{N-1},...,U_1) \le H(U_{N-1} / U_{N-2},...,U_1) \le ...$$
$$... \le H(U_2 / U_1) \le H(U_1) \qquad (12-3)$$

البرهان

بمـا أن المنبـع مسـتقر، فـإن كميـات المعلومـات الشـرطية مسـتقلة عـن موقـع الرمز N ضمن السلسلة، لذلك من أجل المثال

$$H(U_{N-1} / U_{N-2},...,U_1) = H(U_N / U_{N-1},...,U_2),$$

وبالاستناد إلى الخاصية الأولى (المعادلة 3−11) نستنتج مباشرة:

$$H(U_N / U_{N-1},...,U_1) \le H(U_{N-1} / U_{N-2},...,U_1)$$

وأيضاً:

$$F_N(U) \le F_{N-1}(U) \le ... \le F_2(U\ ) \le F_1(U)$$

تقول هذه النظريـة إنـه بزيـادة قيمـة N، تصـبح كميـة المعلومـات أقل أو تبقى نفسها من دون تغيير. ولأن أي كمية معلومات على الدوام أكبر أو تساوي الصفر، نستطيع أن نستنتج أن $F_N(U)$ تقترب من قيمتها الحدية المعطاة بالعلاقة التالية:

$$H_\infty(U) = \lim_{N\to\infty} F_N(U) = \lim_{N\to\infty} F_N(U_N,...,U_1) \qquad (13-3)$$

من الواضح أنه من أجل أبجدية المنبع Uالتي تتألف من m عنصر:

$$0 \le H_\infty(U) \le \log m \qquad (14-3)$$

تعرف $H_\infty(u)$ الآن بأنها كمية المعلومات لمنبع المعلومات المتقطع مع الذاكرة . ويمكن أن تكون هذه الذاكرة بطول غير محدد . وإذا ولد المنبع سلسلة ماركوف من الدرجة k فهذا يعني:

$$p(u_N / u_{N-1},.....,u_1) = p(u_N / u_{N-k},...,u_{N-1}) \qquad (15-3)$$

ولدينا من أجل كمية المعلومات المشروطة:

$$H(U_N / U_{N-1},....,U_1) = H(U_N / U_{N-k},...,U_{N-1})$$
$$= H(U_{k+1} / U_k,...,U_2,U_1) \qquad (16-3)$$

عند ذلك نلاحظ أن زيادة N لن تزيد من عمق الذاكرة لأنها أصلاً محددة بـ k ، وهذا يعني أنه عند $N = k+1$ المقدار $F_N(U)$ يبقى مساوياً لـ $F_{k+1}(U)$ وهذا لن ينقص أكثر من ذلك، وهذا يقودنا إلى القيمة الحدية لسلسلة ماركوف $H_\infty(U)$ من الدرجة k والتي تساوي:

$$H_\infty(U) = F_{k+1}(U) = H(U_{k+1} / U_k,...,U_2,U_1) \qquad (17-3)$$

فإذا كان المنبع من دون ذاكرة k=0 فإن $H_\infty(U)$ ستساوي $H(U)$. ومع زيادة عمق الذاكرة k ستتناقص $H_\infty(U)$ باستمرار.

إلى جانب التعامل مع الرموز المنفصلة يمكن التعامل مع رسائل بطول N رمز واستنتاج كمية المعلومات للرمز الواحد استناداً إلى كمية معلومات الرسالة $H(V)$ ، حيث تعرف الكمية $H(V)$:

$$H(V) = H(U_1,U_2,....,U_N) \ \ bits/message \qquad (18-3)$$

وعندها نعرف كمية المعلومات للرمز بالشكل:

$$H_N(U) = \frac{1}{N} H(V) = \frac{1}{N} H(U_1,U_2,...,U_N) \ \ bits/symbole \qquad (19-3)$$

فإذا كانت العناصر u_i مستقلة إحصائياً فإن:

$$H_N(U)=\frac{1}{N}\sum_{i=1}^{N}H(U_i)=\frac{1}{N}NH(U)=H(U)$$

لكن إذا كانت متعلقة فيما بينها فإن:

$$H_N(U)=\frac{1}{N}[(H(U_1)+H(U_2/U_1)+...+H(U_N/U_{N-1},....,U_2,U_1)]$$

$$=\frac{1}{N}\sum_{j=1}^{N}F_j(U) \qquad (20-3)$$

وكما هي حال $F_N(U)$ ، يتناقص المقدار $H_N(U)$ بشكل رتيب مع زيادة N ليصل إلى قيمته الحدية $H_\infty(U)$.

نظرية (3-2):

إذا كانت $H(U)$ هي كمية المعلومات لرسالة بطول N فإن كمية المعلومات للرمز الواحد المعرفة بالشكل $H_N(U)=H(V)/N$ أيضاً ستتناقص بشكل رتيب، لنحصل في النهاية على:

$$\lim_{N\to\infty}H_N(U)=H_\infty(U) \qquad (21-3)$$

البرهان:

باستخدام المعادلات (3-12) و(3-20) نجد أنه من أجل $H(V)$ أن :

$$H(V)=NH_N(U)=H(U_1)+H(U_2/U_1)+...+H(U_N/U_{N-1},...,U_2,U_1)$$
$$\geq NH(U_N/U_{N-1},...,U_2,U_1),$$

أو من المعادلة (3-10)

$$H_N(U)\geq F_N(U) \qquad (22-3)$$

ونستطيع الآن كتابة:

$$H(V) = H(U_1,...,U_N) = H(U_1,...,U_{N-1}) + H(U_N / U_{N-1},...,U_1)$$

أو

$$\begin{aligned} NH_N(U) &= (N-1)H_{N-1}(U) + F_N(U) \\ &\le (N-1)H_{N-1}(U) + H_N(U). \end{aligned}$$

وبالتالي:

$$(N-1)H_N(U) \le (N-1)H_{N-1}(U)$$

أو

$$H_N(U) \le H_{N-1}(U) \qquad (23-3)$$

وهذه تبرهن أن $H_N(U)$ تتناقص باضطراد، وطالما $H_N(U) \ge 0$ فيجب عليها أن تتقارب إلى حد مثل $H_\infty(U)$ كما ظهر سابقاً.

$$H_N(U) = \frac{1}{N}\sum_{j=1}^{N} F_j(U)$$

وبما أن المقدار $F_j(U)$ تتقارب إلى $H_\infty(U)$ من أجل $j \to \infty$ سنجد:

$$\lim_{N\to\infty} H_N(U) = \lim_{N\to\infty} \frac{1}{N}\sum_{j=1}^{N} F_j(U) = \frac{1}{N}[NH_\infty(U)] = H_\infty(U),$$

وهذا يتوافق تماماً مع المعادلة (3−21).

ونستنتج من المعادلة (3−13) والنظرية (3−2) أن كلا المقدارين $F_N(U)$ و $H_N(U)$ يتقاربان إلى النهاية نفسها ،وكما رأينا $H_N(U) \ge F_N(U)$ وهذا يعني أن $F_N(U)$ هي أسوأ تقريب لكمية المعلومات الفعلية $H_\infty(U)$ ، لكن فائدة القيمة $H_N(U)$ على كل حال في بساطتها .

مثال (3-2):

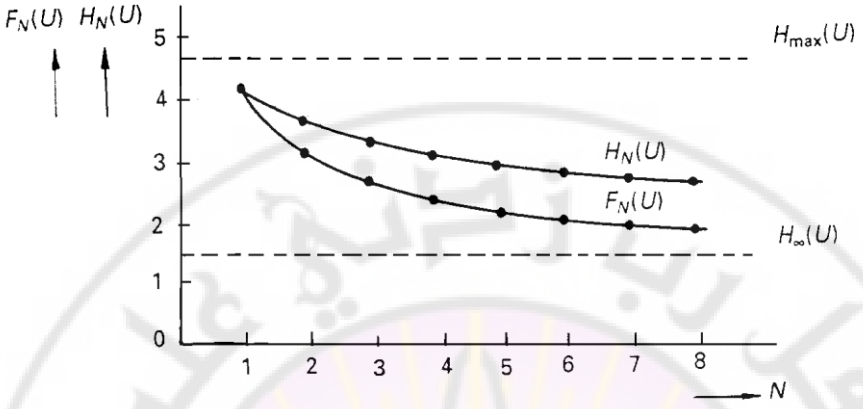
لنفرض أننا حددنا عدة قيم لـ $F_j(U)$ من أجل 26 حرف مختلف (حروف اللغة)

$F_1 = 4.15$	$H_1 = F_1$	$= 4.15$
$F_2 = 2.99$	$H_2 = \frac{1}{2}(F_1 + F_2)$	$= 3.75$
$F_3 = 2.56$	$H_3 = \frac{1}{3}(F_1 + F_2 + F_3)$	$= 3.23$
$F_4 = 2.20$	$H_4 = \frac{1}{4}(F_1 + ...)$	$= 2.98$
$F_5 = 1.95$	$H_5 = ---$	$= 2.77$
$F_6 = 1.72$	$H_6 = ---$	$= 2.60$
$F_7 = 1.63$	$H_7 = ---$	$= 2.46$
$F_8 = 1.60$	$H_8 = ---$	$= 2.35$
-------	------	-----

من الشكل(3-6) نستنتج أن حدود $F_N(U)$ و $H_N(U)$ تقريباً هي :

$H_\infty(U) = 1.50\ bits/symbol$ بينما الحد الأعظمي

$$\max_u H_N(U) = \log 26 = 4.70\ bits/symbol$$



الشكل (3–6) علاقة $H_N(U)$ و $F_N(U)$ مع عدد الأحرف الأبجدية

3 – 3 معالم الترميز *Coding aspects*:

كما هي الحال في المنبع من دون ذاكرة ، نستطيع أيضاً أن نحدد مقدار كم هو عدد الرسائل الأكثر احتمالاً أكبر والتي يولدها المنبع بذاكرة ، حيث سنتوقع وبسبب الذاكرة أن هذا العدد سيكون أصغر من حالة المنبع من دون ذاكرة. نستطيع هنا أن نبرهن أنه لو أخذنا l رمزاً بعضها مع بعض بدلاً من N فإن زيادة l ستجعل المقدار $-\log p(v)/l$ يتجه إلى القيمة $H_\infty(U)$.

نظرية (3–3):

من أجل أي قيمة $\varepsilon > 0$ وأيضاً $\delta > 0$ سنجد القيمة l_0 والتي هي تتابع بأي طول $l \geq l_o$ تقع ضمن صنفين:

I. المجموعة S' فيها مجموع الاحتمالات أقل من ε

II. المجموعة المتبقية S والتي لعناصرها الاحتمالات التي تحقق المتراجحة التالية :

$$\left| \frac{-\log p(v)}{l} - H_\infty(U) \right| < \delta \qquad (24-3)$$

وهذه المجموعة هي الرسائل الأكثر احتمالاً.

وهذه النظرية تتطابق مع نظرية شانون– مكميلان (النظرية 2–3) والمرتبطة بالمنابع من دون ذاكرة. من الواضح وفي مثل هذه الحالة تصبح المعادلة (3–24) مطابقة تماماً للمعادلة (2–24) أي أن $H_\infty(U)=H(U)$.

المجموعة ذات الرسائل الأكثر احتمالاً S تظهر باحتمال $p(S)>1-\varepsilon$ بحيث لكل رسالة منها الاحتمال:

$$p(v)\approx 2^{-lH_\infty(U)} \qquad (25-3)$$

وعدد هذه الرسائل بالتقريب:

$$M_\infty=\frac{1}{p(v)}\approx 2^{lH_\infty(U)} \qquad (26-3)$$

وبما أن $H_\infty(U)\le H(U)$ فإن عدد الرسائل الأكثر احتمالاً M_∞ للمنبع بذاكرة سيكون أصغر أو على الأكثر سيساوي عدد الرسائل الأكثر احتمالاً للمنبع من دون ذاكرة .

لقد عرفنا فيما سبق الفائض(redundancy) بالمعادلة :

$$red=1-\frac{H(U)}{\max\limits_{u} H(U)}=1-\frac{H(U)}{\log n} \qquad (27-3)$$

يعطي هذا المقياس انطباعاً عن جودة المنبع من دون ذاكرة .وفي هذا الفصل لاحظنا أيضاً أن الارتباطات أو التبعية بين الرموز نفسها ستؤدي إلى نقصان بكمية المعلومات ، وهذا يمكن التعبير عنه بما يسمى فائض التبعية dependence redundancy:

$$red_\infty=1-\frac{H_\infty(U)}{H(U)} \qquad (28-3)$$

حيث $H_\infty(U)$ هي كمية المعلومات للمنبع بذاكرة و $H(U)$ هي كمية المعلومات للمنبع من دون ذاكرة ، لاحتمالات الرموز نفسها في كلا المنبعين ، وفي النهاية يمكن تعريف الفائض الكلي total redundancy:

$$red_{tot} = 1 - \frac{H_\infty(U)}{\max\limits_{u} H(U)} = 1 - \frac{H_\infty(U)}{\log n} \qquad (29-3)$$

مثال (3-3):

في المثال (3-2) بالقيمة العظمى $\max H(U) = 4.70\, bits/symbol$ و $H(U) = 4.15\, bits/symbol$ وأيضاً $H_\infty(U) = 1.50\, bits/symbol$ سنجد القياسات التالية لمفاهيم الفائض المختلفة:

$$red = 1 - \frac{4.15}{4.70} = 0.12,$$

$$red_\infty = 1 - \frac{1.50}{4.15} = 0.64,$$

$$red_{tot} = 1 - \frac{1.50}{4.70} = 0.68,$$

فيما يخص المنابع بذاكرة هناك ثلاثة مقاييس مختلفة للفائض ، يظهر كل منها خاصية محددة للترابط الضمني بين الرموز ،ومن منبع ماركوف من الدرجة صفر سنجد أن $red = red_{tot}$ وأيضاً $red_\infty = 0$.

نظرية (3-4):

كمية المعلومات لمنبع المعلومات المتقطع بذاكرة $H_\infty(U)$ حيث الرسائل ذات الطول l ترمز بكلمات ترميز بطول L باستخدام أبجدية بحجم r سنصادف الحالة بالاحتمال p_l لوجود رسالة لا نستطيع إيجاد كلمة ترميز لها صغيرة $(p_l < \varepsilon)$ إذا حققت L العلاقة:

$$L \log r \geq l H_\infty(U), \qquad (30-3)$$

و l قيمة كبيرة بدرجة كافية.

كما رأينا من المثال (3–3) من بين الأمثلة الأخرى يمكن أن يكون الفائض كبيراً لدرجة كافية ليصبح مرغوباً ويمكن إزالته بواسطة الترميز. وقد رأينا كيف أنه من المنبع من دون ذاكرة يمكن تطوير طرق ترميز للحصول على الترميز المناسب القادر على تصغير الطول الوسطي لكلمات الترميز وبالتالي تصغير الفائض في الوقت نفسه. إحدى الطرق لإزالة فائض التبعية للمنبع بذاكرة هي تطبيق طرق ترميز على رسائل بطول l بدلا من تطبيقها على حروف منفصلة. تستند هذه الطريقة إلى توسيع الأبجدية. يمكن اختيار الطول l من درجة سلسلة ماركوف.

مثال (3–4):

لنأخذ منبع معلومات يولد سلسلة ماركوف من الدرجة الأولى أبجدية المنبع هي $U=\{A,B,C\}$ ،ولدينا الاحتمالات الانتقالية التالية:

$$p(A/A)=\frac{1}{2} \qquad p(B/A)=\frac{1}{2} \qquad p(C/A)=0$$

$$p(A/B)=\frac{1}{4} \qquad p(B/B)=0 \qquad p(C/B)=\frac{3}{4}$$

$$p(A/C)=\frac{1}{3} \qquad p(B/C)=\frac{1}{3} \qquad p(C/C)=\frac{1}{3}$$

نوجد الاحتمالات المنفردة من المعادلات التالية:

$$\begin{cases} p(A) = \frac{1}{2}p(A) + \frac{1}{4}p(B) + \frac{1}{3}p(C), \\ p(B) = \frac{1}{2}p(A) + \frac{1}{3}p(C), \\ p(C) = \frac{3}{4}p(B) + \frac{1}{3}p(C), \\ P(A) + p(B) + p(C) = 1 \end{cases}$$

لنحصل على النتيجة: $p(A) = \frac{10}{27}, p(B) = \frac{8}{27}, p(C) = \frac{9}{27}$

لنفرض أننا دمجنا فقط رمزي ترميز استناداً إلى الاحتمالات الانتقالية التي يمكن إيجادها من الاحتمالات المشتركة . هذه الاحتمالات المشتركة مع كلمات الترميز التي نحصل عليها من تطبيق طريقة فانو للترميز في حالة $r = 2$ نوردها في الجدول التالي:

	Probabilit y	code word
BC	$\frac{6}{27}$	$0\underline{0}$
AA	$\frac{5}{27}$	$\underline{01}$
AB	$\frac{5}{27}$	$10\underline{0}$
CA	$\frac{3}{27}$	$1\underline{01}$
CB	$\frac{3}{27}$	$11\underline{0}$
CC	$\frac{3}{27}$	$111\underline{0}$

BA	$\frac{2}{27}$	1111
AC	0	ـــــ
BB	0	ـــــ

الطول الوسطي لكلمة الترميز $L = \frac{75}{27} \approx 2.78 \; or 1.39 \; per \; symbol,$.

وبحساب كمية المعلومات المشتركة نجد: $H(U_1,U_2) = 2.72$ فإذاً نجد فعالية الترميز: $\eta = H(U_1,U_2)/L = 2.72/2.78 \approx 0.98$.

لكن إذا استخدمنا فانو للرموز المنفصلة نجد أن الطول الوسطي لكلمات الترميز هو $L = \frac{44}{27} \approx 1.63$ وهذا أكبر من 1.39 للرمز الواحد المحسوب سابقاً، وهنا تكون فعالية الترميز نقصت إلى $\eta = 0.97$.

3– 4 سعة القناة المتقطعة من دون ذاكرة:

لنأخذ منبعاً يولد الرموز $x_1, x_2, ..., x_r$ وبرسلها عبر قناة متقطعة من دون ذاكرة. يستقبل المستقبل الرموز $y_1, y_2, ..., y_s$. قد لا تتطابق مجموعة الرموز $\{y_k\}$ لمجموعة الرموز $\{x_k\}$ فهذا يعتمد على طبيعة المستقبل . فمن الممكن أن تتطابق مجموعة الرموز المستقبلة مع الرموز المرسلة (بالعدد) فقط لكن فيما بعد سنأخذ الحالة العامة ولن نتقيد بأن بتطابق المجموعتين.

فإذا كانت القناة من دون ضجيج فإن الرمز y_j سيحدد بشكل وحيد الرسالة المرسلة. لكن بسبب الضجيج هناك كمية محددة من الشك متعلقة بالرمز المرسل عندما نستقبل y_j . فإذا كانت $P(x_i / y_j)$ تمثل الاحتمال المشروط أن تكون x_i هي المرسلة عندما نستقبل الرمز y_j فإذاً هناك غموض (كمية المعلومات)أو شك مقداره $\log[1/P(x_i / y_j)$ حول x_i عندما نستقبل y_j . وعندما نأخذ المتوسط لهذه

القيمة لكامل x_i و y_j سنحصل على $H(X/Y)$ وهذه عبارة عن متوسط الشك (الانتروبية) حول الرموز المرسلة عندما نستقبل أي رمز، أي:

$$H(X/Y)=\sum_i\sum_j p(x_i,y_j)\log\frac{1}{p(x_i/y_j)}\ bits/symbol \quad (30-3)$$

فإذا كانت القناة من دون ضجيج ، سيصبح هذا الغموض مساوياً الصفر ،بالطبع هذا الغموض $H(X/Y)$ سببه ضجيج القناة ، وبالتالي هذا يمثل فقد المعلومات بالمتوسط للرموز المرسلة عند الاستقبال ، نسمي المقدار $H(X/Y)$ الالتباس حول x بالنسبة لـ y.

نلاحظ أن $p(y_j/x_i)$ تمثل احتمال أن نستقبل y_j عندما نرسل x_i. وهذه ستمثل خصائص القناة والمستقبل . لذلك سنصف القناة (مع مستقبلها) بما يسمى مصفوفة القناة channel matrix:

$$\begin{array}{c} \\ \text{Inputs} \end{array}\begin{array}{c} \text{Outputs} \\ \begin{array}{cccc} y_1 & y_2 & \cdots & y_s \end{array} \\ \begin{array}{c} x_1 \\ x_2 \\ \cdots \\ x_r \end{array}\begin{pmatrix} P(y_1|x_1) & P(y_2|x_1) & \cdots & P(y_s|x_1) \\ P(y_1|x_2) & P(y_2|x_2) & \cdots & P(y_s|x_2) \\ \cdots & \cdots & \cdots & \cdots \\ P(y_1|x_r) & P(y_2|x_r) & \cdots & P(y_s|x_r) \end{pmatrix} \end{array}$$

يمكن الحصول على الاحتمالات العكسية باستخدام قاعدة بايس :

$$p(x_i / y_j) = \frac{p(y_j / x_i)\, p(x_i)}{p(y_j)} \qquad (31a-3)$$

$$= \frac{p(y_j / x_i)\, p(x_i)}{\sum_i p(x_i, y_j)} \qquad (31b-3)$$

$$= \frac{p(y_j / x_i)\, p(x_i)}{\sum_i p(x_i)\, p(y_j / x_i)} \qquad (31c-3)$$

يمكن حساب الاحتمالات المشروطة العكسية إذا كان لدينا $p(x_i)$ ومصفوفة القناة من المعادلات (3−31)، الاحتمال المشروط العكسي $p(x_i / y_j)$ هو احتمال أن تكون x_i قد أرسلت عندما نستقبل y_j.

فإذا كانت القناة من دون ضجيج فإن كمية المعلومات المتوسطة المستقبلة هي $H(X)$ (وهي انتروبية المنبع) مقاسة بالبت للرمز المستقبل الواحد. نلاحظ أن $H(X)$ هي متوسط كمية المعلومات المرسلة عبر القناة. وبسبب وجود الضجيج سنفقد بالمتوسط $H(X/Y)$ بت للرمز الواحد. وبالتالي كمية المعلومات التي يحصل عليها المستقبل بالمتوسط هي $I(X;Y)$ حيث :

$$I(X;Y) = H(X) - H(X/Y) \quad bits/symbol \quad (32-3)$$

ندعو $I(X;Y)$ بالمعلومات المتبادلة (كما رأينا) بين X و Y لأن :

$$H(X) = \sum_i p(x_i) \log \frac{1}{p(x_i)} \qquad bits$$

ولدينا :

$$I(X;Y) = \sum_i p(x_i) \log \frac{1}{p(x_i)} - \sum_i \sum_j p(x_i, y_j) \log \frac{1}{p(x_i / y_j)}$$

وأيضاً لأن:

$$\sum_i p(x_i, y_j) = p(x_i)$$

ولدينا :

$$I(X;Y) = \sum_i \sum_j p(x_i, y_j) \log \frac{1}{p(x_i)} - \sum_i \sum_j p(x_i, y_j) \log \frac{1}{p(x_i / y_j)}$$

$$= \sum_i \sum_j p(x_i, y_j) \log \frac{p(x_i / y_j)}{p(x_i)} \qquad (33a-3)$$

$$= \sum_i \sum_j p(x_i, y_j) \log \frac{p(x_i, y_j)}{p(x_i) p(y_j)} \qquad (33b-3)$$

وبشكل آخر وباستخدام قاعدة بايس في المعادلة (33a–3) نوجد $I(X;Y)$ بالشكل التالي:

$$I(X;Y) = \sum_i \sum_j p(x_i, y_j) \log \frac{p(y_j / x_i)}{p(y_j)} \qquad (33c-3)$$

أو يمكن أن نعوض المعادلة (31c–3) في المعادلة (33a–3):

$$I(X;Y) = \sum_i \sum_j p(x_i) p(y_j / x_i)) \log \frac{p(y_j / x_i)}{\sum p(x_i) p(y_j / x_i)} \qquad (33d-3)$$

تحسب المعادلة (33d–3) المقدار $I(X;Y)$ عن طريق احتمالات رموز الدخل ومصفوفة القناة.

يجب أن ننتبه إلى واحدة قياس $I(X;Y)$ حيث $I(X;Y)$ هي كمية المعلومات المتوسطة للرمز الواحد المرسل، وبالتالي الواحدة هي البت للرمز الواحد. وإذا استخدمنا الخانات الثنائية على الدخل فالرمز هنا هو الخانة الثنائية وتصبح واحدة $I(X;Y)$ هي البت لكل خانة ثنائية.

بما أن $I(X;Y)$ في المعادلة (33b–3) هي متناظرة بالنسبة لـ x و y فنستنتج أن

$$I(X;Y) = I(Y;X) \qquad (34a-3)$$
$$= H(Y) - H(Y/X) \qquad (34b-3)$$

يمثل المقدار $H(Y/X)$ مقدار الالتباس في Y بالنسبة لـ X وهي بالمتوسط مقدار الشك حول الرمز المستقبل عند معرفة الرمز المرسل. يمكن إعادة كتابة المعادلة (3-34b) بالشكل:

$$H(X) - H(X/Y) = H(Y) - H(Y/X) \qquad (34c-3)$$

من الواضح من المعادلة (3-33d) أن $I(X;Y)$ هي تابع لاحتمالات الرموز المرسلة $p(x_i)$ ولمصفوفة القناة . ومن أجل قناة محددة يمكن أن يأخذ المقدار $I(X;Y)$ القيمة العظمى عند مجموعة قيم محددة من احتمالات $p(x_i)$ وهذه القيمة العظمى سنسميها سعة القناة C_s (channel capacity):

$$C_s = \max_{p(x_i)} I(X;Y) \; bits/symbol \qquad (35-3)$$

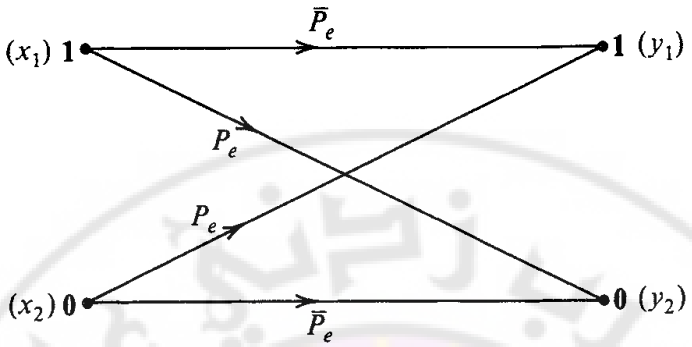
تمثل C_s كمية المعلومات العظمى التي يمكن أن ترسل برمز واحد عبر القناة . يمكن إيضاح هذا المفهوم من خلال المثال التالي لقناة ثنائية متناظرة (BSC).

مثال (3-5):

أوجد سعة القناة للقناة الثنائية المتناظرة المبينة بالشكل (3-7) التالي:

لنفرض أن $p(x_1) = \alpha$ و $p(x_2) = \overline{\alpha} = (1-\alpha)$ وأيضاً:

$$p(y_1/x_2) = p(y_2/x_1) = p_e$$
$$p(y_1/x_1) = p(y_2/x_2) = \overline{p_e} = 1 - p_e$$



الشكل (3-7) القناة الثنائية المتناظرة

وبتعويض هذه القيم في المعادلة (3-33d) سنجد:

$$I(X;Y) = \alpha\bar{p}_e \log\left(\frac{\bar{p}_e}{\alpha\bar{p}_e + \bar{\alpha}p_e}\right) + \alpha p_e \log\left(\frac{p_e}{\alpha p_e + \bar{\alpha}\bar{p}_e}\right)$$

$$+\bar{\alpha}p_e \log\left(\frac{p_e}{\alpha\bar{p}_e + \bar{\alpha}p_e}\right) + \bar{\alpha}\bar{p}_e \log\left(\frac{\bar{p}_e}{\alpha p_e + \bar{\alpha}\bar{p}_e}\right)$$

$$= (\alpha p_e + \bar{\alpha}\bar{p}_e)\log\left(\frac{1}{\alpha p_e + \bar{\alpha}\bar{p}_e}\right)$$

$$+(\alpha\bar{p}_e + \bar{\alpha}p_e)\log\left(\frac{1}{\alpha\bar{p}_e + \bar{\alpha}p_e}\right)$$

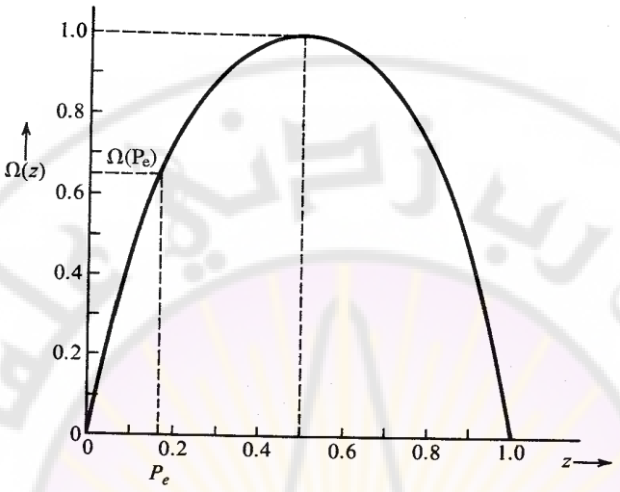
$$-\left(p_e \log\frac{1}{p_e} + \bar{p}_e \log\frac{1}{\bar{p}_e}\right)$$

لنفرض أن $\Omega(z) = z\log\frac{1}{z} + \bar{z}\log\frac{1}{\bar{z}}$ بحيث $\bar{z} = 1 - z$ عندها سنجد:

$$I(X;Y) = \Omega(\alpha p_e + \bar{\alpha}\bar{p}_e) - \Omega(p_e) \qquad (3-36)$$

يظهر الشكل (3-8) العلاقة بين $\Omega(z)$ و z حيث نلاحظ أنها تأخذ القيمة العظمى من أجل $z = 0.5$ وبالتالي من العلاقة (3-36) يأخذ المقدار $I(X;Y)$ قيمته العظمى عندما تكون $\Omega(\alpha p_e + \bar{\alpha}\bar{p}_e)$ قيمة عظمى وهذا يحدث عندما :

$$\alpha p_e + \overline{\alpha}\,\overline{p_e} = 0.5$$



الشكل(3–8) علاقة $\Omega(z)$ بالمتحول z (الاحتمال)

أو $\alpha p_e + (1-\alpha)(1-p_e) = 0.5$ وهذه المعادلة تتحقق عندما:

$$\alpha = 0.5 \qquad (37-3)$$

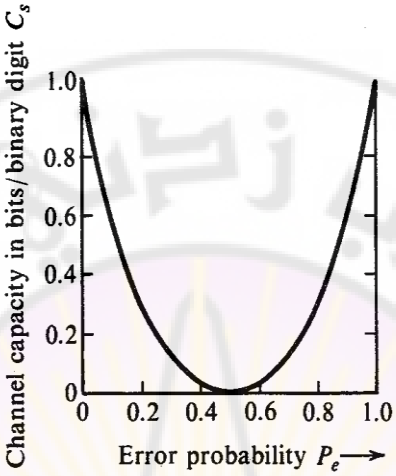
ومن أجل هذه القيمة لـ α ستكون $\Omega(\alpha p_e + \overline{\alpha}\,\overline{p_e}) = 1$ وأيضاً:

$$C_s = \max_{p(x_i)} I(X;Y) = 1 - \Omega(p_e)$$

$$= 1 - \left[p_e \log \frac{1}{p_e} + (1-p_e) \log\left(\frac{1}{1-p_e}\right) \right] \qquad (38-3)$$

يظهر الشكل (3–9) علاقة C_s بالاحتمال p_e ومنه نلاحظ أن القيمة العظمى لـ C_s هي الواحد وهذا يعني أننا نستطيع أن نرسل على الأكثر بتاً واحداً للخانة الثنائية الواحدة، ونلاحظ أيضاً أن C_s تأخذ القيمة العظمى عندما $p_e = 0$ أو

$p_e = 1$ ، حيث عندما تكون $p_e = 0$ فالقناة من دون ضجيج وسنتوقع أن C_s ستأخذ



الشكل(3–9) سعة القناة الثنائية

القيمة العظمى، لكن المفاجأة أن C_s أيضاً ستأخذ القيمة العظمى عندما $p_e = 1$ وهذا يعني أن القناة بشكل مقصود وموجه تقوم بصنع الأخطاء وهذا جيد كما لو أن القناة من دون ضجيج حيث كل ما نحتاجه عند الاستقبال هو عكس قيم القرار المتخذ للحصول على استقبال من دون أخطاء تماماً.

سعة القناة C_s تأخذ قيمة الصفر (الأصغرية) عندما $p_e = 0.5$ أي أن الرموز المستقبلة مستقلة إحصائياً عن الرموز المرسلة ،فإذا استقبلنا الرمز 0 على سبيل المثال فإنه على الأرجح الرمز 0 أو 1 وكلاهما بالاحتمال نفسه هو المرسل وعندها كمية المعلومات المستقبلة ستكون تساوي الصفر.

3–5 سعة القناة بالثانية:

تعطي سعة القناة C_s المعرفة بالمعادلة (3–35) كمية المعلومات العظمى الممكن نقلها عند إرسال رمز واحد(خانة)، فإذا أرسلنا k رمز بالثانية عندها المعدل الأعظمي لإرسال المعلومات بالثانية هو kC_s ، وهذا يمثل سعة القناة

بواحدة كمية المعلومات بالثانية الواحدة ، وسيكون لها فقط بالرمز C وستقاس بالبت في الثانية (bit/s):

$$C = kC_s \ bit/s$$

3– 5 – 1 بعض الملاحظات عن سعة القناة:

إن سعة القناة هي خاصية قناة فيزيائية محددة تقوم بنقل المعلومات من خلالها. ومصطلح القناة هنا لا يعني فقط وسط النقل بل يشمل أيضاً توصيف أنواع الإشارات المستخدمة وخصائصها ، ونوع المستقبل المستخدم ، كل هذا يجب أن يدخل في مصفوفة القناة، بحيث تصف هذه المصفوفة تماما القناة . فإذا قررنا على سبيل المثال استخدام خانات رباعية بدلاً من الخانات الثنائية للقناة الفيزيائية نفسها ، ستتغير مصفوفة القناة (ستصبح مصفوفة4x4 عنصر) وأيضا ستتغير سعة هذه القناة. وبشكل مشابه تغيير المستقبل أو استطاعة الإشارة أو الضجيج سيؤدي إلى تغيير في مصفوفة القناة وبالتالي تغيير في سعة القناة

3–6 سعة القناة للقناة المستمرة:

إذا أخذنا X مجموعة المتحولات العشوائية المتقطعة $x_1, x_2, ..., x_n$ باحتمالات $p(x_1), p(x_2), ..., p(x_n)$ وقد عرفنا سابقاً الانتروبية $H(X)$ بالعلاقة:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i) \qquad (39-3)$$

لكن من أجل البيانات التماثلية نتعامل مع متحولات عشوائية مستمرة، وبالتالي يجب أن نوسع تعريف الانتروبية ليشمل المتحولات العشوائية المستمرة. نحاول أن نوجد $H(X)$ للمتحولات العشوائية المستمرة باستخدام التكامل عوضاً عن الجمع المتقطع في المعادلة (3–39):

$$H(X) = \int_{-\infty}^{\infty} p(x) \log \frac{1}{p(x)} dx \qquad (40-3)$$

المتحـول العشـوائي x يأخـذ القـيم فـي المجـال $(n\Delta x,(n+1)\Delta x)$ باحتمـال $p(n\Delta x)\Delta x$ بشـرط $\Delta x\to 0$ ، سـيختفي خطـأ التقريـب عنـدما $\Delta x\to 0$ ، وبالتـالي الانتروبية $H(X)$ للمتحول العشوائي المستمر x تعطى بالشكل:

$$H(X)=\lim_{\Delta x\to 0}\sum_n p(n\Delta x)\Delta x\log\frac{1}{p(n\Delta x)\Delta x}$$

$$=\lim_{\Delta x\to 0}\left[\sum_n p(n\Delta x)\Delta x\log\frac{1}{p(n\Delta x)}-\sum_n p(n\Delta x)\Delta x\log\Delta x\right]$$

$$=\int_{-\infty}^{\infty}p(x)\log\frac{1}{p(x)}dx-\lim_{\Delta x\to 0}\log\Delta x\int_{-\infty}^{\infty}p(x)dx$$

$$=\int_{-\infty}^{\infty}p(x)\log\frac{1}{p(x)}dx-\lim_{\Delta x\to 0}\log\Delta x \qquad (41-3)$$

عنـدما تتجـه $\Delta x\to 0$ نجـد أن $\log\Delta x\to-\infty$ ، أي أن انتروبيـة المتحـول العشـوائي المسـتمر هـي لانهائيـة، وهـذه حقيقـة لأن الغمـوض المتعلـق بـالمتحول العشوائي المستمر ليس لـه حدود ،وهذا يظهر مباشرة حيث أن المتحول العشوائي يمكن أن يأخذ عدداً غير نهائي من القيم لذلك فالغموض لا حدود لـه (لانهائي). هل هذا يعني أن معادلة تعريف الانتروبية للمتحول العشوائي المستمر ليست بذات قيمـة. من جهـة أخرى نجد أن الحد الأول فـي المعادلـة (3−41) يمكـن أن يكـون مقياساً ذا معنـى للانتروبيـة (المعلومـات المتوسطة) للمتحول العشوائي المستمر x. نستطيع أن نفرض أن $\int p(x)\log[1/p(x)]dx$ هي الانتروبية النسبية ويصبح الحد $-\log\Delta x$ البيان أو المرجع لـه. إن المعلومات المرسلة عبر القناة عملياً هي الفرق بين قيمتين $H(X)$ و $H(X/Y)$ لذلك من الواضح إذا كان لدينا المرجع نفسه لكلا القيمتـين فـإن الفـرق $H(X)-H(X/Y)$ سـيكون هـو نفسـه الفـرق بـين قيمتـي الانتروبيـة النسـبية . لـذلك نكتفـي بالحـد الأول مـن المعادلـة (3−41) علـى أنـه الانتروبيـة التفاضـلية للمتحـول x . يجـب هنـا وباسـتمرار التـذكر بـأن هـذه هـي

انتروبيـة نسـبية وليسـت مطلقـة .يولـد الفشـل فـي تحقيـق نقطـة دقيقـة العديـد مـن المغالطات الظاهرية إحداها تظهر في المثال (3−5).

اسـتناداً إلـى مـا سـبق نعـرف $H(X)$ بأنهـا الانتروبيـة التفاضـلية للمتحـول العشوائي المستمر xوبالشكل التالي:

$$H(X)=\int_{-\infty}^{\infty} p(x)\log\frac{1}{p(x)}dx\ bits \qquad (42a-3)$$

$$=-\int_{-\infty}^{\infty} p(x)\log\ p(x)dx\ bits \qquad (42b-3)$$

وعلـى الـرغم مـن أن $H(X)$هـي الانتروبيـة التفاضـلية (النسـبية) لـ x، سنسميها انتروبية المتحول العشوائي x.

مثال (3−5):

مطـال الإشـارة x هـو متحـول عشـوائي يتـوزع بانتظـام علـى المجـال (−1,1)تمر هذه الإشارة عبر مضخم لـه ربـح قدره 2 . الخرج y هو أيضاً متحول عشوائي يتوزع بانتظام ضمن المجال (−2,2) أوجد الانتروبية التفاضلية لـ $H(X)$و $H(Y)$

لدينا:

$$P(x)=\begin{cases}\frac{1}{2} & |x|<1\\ 0 & otherwise\end{cases}$$

$$P(y)=\begin{cases}\frac{1}{4} & |y|<2\\ 0 & otherwise\end{cases}$$

إذا:

$$H(X)=\int_{-1}^{1}\frac{1}{2}\log 2dx=1bit$$

$$H(Y)=\int_{-2}^{2}\frac{1}{4}\log 4dy=2bits$$

نلاحظ أن المتحول العشوائي y هو ضعف المتحول x. والنتيجة التي حصلنا عليا تبدو غريبة بعض الشيء، لأن معرفة x ستحدد y بدقة، والعكس صحيح لأن $y = 2x$. ولهذا يجب أن يكون الغموض في y هو نفسه لـ x، حيث التضخيم نفسه لن يضيف أو ينقص من كمية المعلومات ، فلماذا إذاً $H(Y)$ هي ضعف $H(X)$؟ يمكن أن يتوضح ذلك إذا تذكرنا أن $H(X)$ و $H(Y)$ هما انتروبيات تفاضلية (نسبية) ويمكن أن يتساويان فقط إذا تساوت الانتروبيات المرجعية لكل منهما . الانتروبية المرجعية R_1 لـ x هي $-\log \Delta x$ والانتروبية المرجعية R_2 لـ y هي $-\log \Delta y$ حيث:

$$R_1 = \lim_{\Delta x \to 0} -\log \Delta x$$
$$R_2 = \lim_{\Delta y \to 0} -\log \Delta y$$

وأيضاً

$$R_1 - R_2 = \lim_{\Delta x, \Delta y \to 0} -\log \frac{\Delta y}{\Delta x}$$
$$= \log\left(\frac{dy}{dx}\right) = \log 2 = 1bit$$

أي أن الانتروبية المرجعية R_1 الخاصة بـ x أكبر من الانتروبية المرجعية R_2 الخاصة بـ y. وبالتالي إذا تساوت الانتروبيات المطلقة لـ x و y فإن الانتروبيات التفاضلية (النسبية) يجب أن تختلفا بمقدار 1 بت.

3- 7انتروبية الضجيج الغاوصي الأبيض محدود المجال:

ليكن لدينا ضجيج غاوصي محدود المجال $n(t)$ له كثافة استطاعة طيفية $N_0/2$ ولأن : $R_n(\tau) = N_0 B \sin c(2\pi B\tau)$ ولأننا نعرف أن $\sin c(2\pi B\tau)$ تأخذ قيم الصفر عند $\tau = \pm k/2B$ حيث k عدد صحيح سنجد :

$$R_n\left(\frac{k}{2B}\right)=0 \qquad k=\pm1,\pm2,\pm3,...$$

وبالتالي :

$$R_n\left(\frac{k}{2B}\right)=\overline{n(t)n\left(t+\frac{k}{2B}\right)}=0 \qquad k=\pm1,\pm2,\pm3,...$$

حيث $n(t)$ و $n(t+k/2B)$ عند $k=\pm1,\pm2,\pm3,...$ هي عينات تحقق شرط نايكويست من الإشارة $n(t)$ وهذه المعادلة تشير إلى أن هذه العينات غير مترابطة، ولأن الإشارة $n(t)$ غاوصية فإن عدم الترابط يفرض الاستقلالية ، وبالتالي كل عينات نايكويست من $n(t)$ مستقلة ، ولنلاحظ أن :

$$\overline{n^2}=R_n(0)=N_0B$$

وطالما التغاير (variance) لكل عينة من نايكويست هي N_0B ومن المعادلة (42a−3) نستنتج أن $H(n)$ لكل عينة من نايكويست للإشارة $n(t)$ هو:

$$H(n)=\frac{1}{2}\log(2\pi eN_0B) \qquad bits/symbol \qquad (43a-3)$$

ولأن $n(t)$ موصفة تماماً بـ $2B$ عينة من نايكويست بالثانية الواحدة ، فالانتروبية بالثانية للإشارة $n(t)$ هي نفسها لـ $2B$ عينة نايكويست، ولأن كل العينات مستقلة فإن معرفة واحدة لن يعطي أية معلومات عن العينة الأخرى. وبالتالي انتروبية $2B$ عينة نايكويست هي مجموع الانتروبيات لـ $2B$ عينة وأيضاً

$$H'(n)=B\log(2\pi eN_0B) \qquad bit/s \qquad (43b-3)$$

حيث $H'(n)$ هي الانتروبية في الثانية للإشارة $n(t)$.

من هذه النتائج نستطيع أن نستخلص نتيجة واحدة مهمة ،وهي أن إشارة الضجيج الغاوصي الأبيض محدود المجال هي الوحيدة من بين كل الإشارات محدودة المجال بالقيمة B والمقيدة بمربع المتوسط σ^2 التي تملك أكبر انتروبية

بالثانية. السبب في ذلك أنه من أجل قيمة مربع المتوسط محددة تملك العينات الغاوصية أكبر انتروبية، والأكثر من ذلك فإن مجموع العينات $2B$ كلها لهذه الإشارة مستقلة عن بعضها ، وبالتالي الانتروبية بالثانية هي مجموع الانتروبيات لكل العينات $2B$. في حال كون الإشارة ليست بيضاء فإن عينات نايكوست منها تصبح مترابطة وبالتالي الانتروبية بالثانية ستكون أقل من مجموع الانتروبيات لكل العينات $2B$. وإذا لم تكن الإشارة غاوصية فإن عيناتها أيضا غير غاوصية وبالتالي الانتروبية بالثانية أيضاً أقل من الانتروبية العظمى الممكنة من أجل قيمة مربع متوسط محددة، وللتكرار من أجل مجموعة الإشارات محدودة المجال والمقيدة بقيمة مربع متوسط مفروضة فإن الإشارة الغاوصية البيضاء تملك أكبر انتروبية بالثانية أو أكبر كمية من الغموض، وهذا أيضاً السبب بأن يكون الضجيج الغاوصي الأبيض أسوأ ضجيج ممكن من حيث التداخل مع الإشارة المرسلة.

3- 8المعلومات المتبادلة $I(x;y)$:

الاختبار النهائي لأي مبدأ هو مقدار المنفعة منه ، وهنا سنظهر أن الانتروبية المشروطة المعرفة بالمعادلة (3-42) ستقودنا إلى نتائج مفيدة عندما نفترض أن $I(x;y)$ كمية المعلومات المتبادلة للمتحولات العشوائية المستمرة $x;y$ ، حيث نرغب بإرسال المتحول العشوائي x عبر القناة ، فكل قيمة لـ x ضمن أي مجال مستمر مفروض هي رسالة يمكن إرسالها على شكل نبضة مثلاً بارتفاع x ، وتشكل الرسائل المكشوفة من المستقبل متحولاً عشوائياً مستمراً y . فإذا كانت القناة خالية من الضجيج فالقيم المستقبلة y ستتحدد تماما من خلال قيم x . لكن ضجيج القناة سيقدم بعض الغموض حول قيم x ، بفرض في لحظة ما عند المرسل أرسلت قيمة لـ x ضمن المجال $(x, x+\Delta x)$ حيث $(\Delta x \to 0)$. احتمال هذا الحدث هو $p(x)\Delta x$ وبالتالي كمية المعلومات المرسلة هي $\log[1/\, p(x)\Delta x]$.

وبفرض أننا استقبلنا القيمة y عند المستقبل فيكون $p(x/y)$ كثافة الاحتمالات الشرطية لـ x عند معرفة y. فإذاً $p(x/y)\Delta x$ هي احتمال وقوع x ضمن المجال $(x, x+\Delta x)$ عند معرفة y، من الواضح هنا بوجود عدم تأكد أو غموض بوقوع القيمة x ضمن المجال $(x, x+\Delta x)$، وهذا الغموض يعبر عنه بكمية المعلومات

$\log[1/p(x/y)\Delta x]$ والذي يظهر بسبب ضجيج القناة لذلك فإنه يعبر عن الفقد في المعلومات. وبما أن $\log[1/p(x)\Delta x]$ هي كمية المعلومات المرسلة وأن $\log[1/p(x/y)\Delta x]$ المعلومات المفقودة خلال القناة فإن المعلومات المستقبلة الصافية $I(x;y)$ تعطى بالمعادلة التالية:

$$I(x;y) = \log \frac{p(x/y)}{p(x)} \qquad (44-3)$$

إن هذه العلاقة صحيحة فقط عندما $(\Delta x \to 0)$، وبالتالي تمثل $I(x;y)$ المعلومات المرسلة عبر القناة عندما نستقبل $y(Y=y)$ وعندما نرسل $x(X=x)$. نحن عادة نهتم بإيجاد متوسط كمية المعلومات المرسلة عبر القناة عندما نرسل على سبيل المثال x واستقبلنا بالتحديد القيمة y. أي يجب علينا أخذ متوسط القيمة $I(x;y)$ على كل قيم x و y عندها نحسب متوسط كمية المعلومات المرسلة $I(X;Y)$ بالعلاقة:

$$I(X;Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)I(x;y)dx\,dy \qquad (45a-3)$$

$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)\log\frac{p(x/y)}{p(x)}dx\,dy \qquad (45b-3)$$

$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)\log\frac{1}{p(x)}dx\,dy + \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)\log\, p(x/y)dx\,dy$$

$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x)p(y/x)\log\frac{1}{p(x)}dx\,dy + \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)\log\, p(x/y)dx\,dy$$

$$= \int_{-\infty}^{\infty} p(x) \log \frac{1}{p(x)} dx \int_{-\infty}^{\infty} p(y/x) dy + \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} p(x,y) \log p(x/y) dx\, dy$$

$\int p(x) \log \frac{1}{p(x)} dx = H(x)$ وأيضاً $\int_{-\infty}^{\infty} p(y/x) dy = 1$ نلاحظ هنا أن :

وبالتالي:

$$I(X;Y) = H(x) + \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} p(x,y) \log p(x/y) dx\, dy \qquad (46a-3)$$

$$= H(x) - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} p(x,y) \log \frac{1}{p(x/y)} dx\, dy \qquad (46b-3)$$

يمثل التكامل في الطرف الأيمن المتوسط على المتحولين xو y بينما يمثل الحد $\log[1/p(x/y)]$ مقدار الشك حول x عندما نستقبل y . أي وكما نرى هناك ضياع للمعلومات عبر القناة. ومتوسط المقدار $\log[1/p(x/y)]$ هو متوسط فقد المعلومات عند إرسال x واستقبال y وهذا بالتعريف $H(x/y)$مقدار الالتباس بقيمة xبالاستناد إلى y.

$$H(x/y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} p(x,y) \log \frac{1}{p(x/y)} dx\, dy \qquad (47-3)$$

وبالتالي:

$$I(X;Y) = H(x) - H(x/y) \qquad (48-3)$$

بمعنى أنه عند إرسال قيمة ما لـ x واستقبلت قيمة ما لـ y فإن القيمة المتوسطة للمعلومات المرسلة عبر القناة هي $I(X;Y)$، وهنا نستطيع تعريف سعة القناة C_s بأنها كمية المعلومات العظمى الممكن إرسالها ،بالمتوسط للرمز أو للقيمة المرسلة:

$$C_s = \max I(x,y) \qquad (49-3)$$

ولأي قناة نجد أن $I(x,y)$ هي تابع لكثافة الاحتمال على الدخل $p(x)$ كما هو واضح مما يلي:

$$p(x,y) = p(x)\,p(y/x) \qquad (50-3)$$

$$\frac{p(x/y)}{p(x)} = \frac{p(y/x)}{p(y)}$$

$$= \frac{p(y/x)}{\int_{-\infty}^{\infty} p(x,y)dx}$$

$$= \frac{p(y,x)}{\int_{-\infty}^{\infty} p(x)\,p(y/x)dx} \qquad (51-3)$$

بتعويض المعادلات (3-50) و (3-51) في المعادلة (3-45b) نحصل على :

$$I(X;Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x)\,p(y/x)\log\left(\frac{p(y/x)}{\int_{-\infty}^{\infty} p(x)\,p(y/x)dx}\right)dxdy \qquad (52-3)$$

حيث كثافة الاحتمالات المشروطة $p(y/x)$ توصف القناة المعنية . وبالتالي ومن أجل قناة معنية المقدار $I(X;Y)$ هو تابع لكثافة الاحتمال على الدخل $p(x)$ فقط ومنه نجد أن :

$$C_s = \max_{p(x)} I(X;Y)$$

فإذا كانت القناة تمرر K قيمة بالثانية فإن C هي سعة القناة بالثانية وتعطى بالعلاقة :

$$C = KC_s \qquad (53-3)$$

وفقط من أجل المتحولات المتقطعة ستكون $I(X;Y)$ متناظرة بالنسبة لـ x و y المتحولات العشوائية المستمرة. وهذا سنلاحظه من خلال إعادة كتابة المعادلة (3–45b) بالشكل التالي:

$$I(X;Y)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}p(x,y)\log\frac{p(x,y)}{p(x)p(y)}dxdy \qquad (54-3)$$

تظهر هذه المعادلة أن المقدار $I(X;Y)$ متناظر بالنسبة x و y وبالتالي :

$$I(X;Y)=I(Y;X)$$

ومن المعادلة (3–48) نستنتج :

$$I(X;Y)=H(X)-H(X/Y)=H(Y)-H(Y/X) \qquad (55-3)$$

3– 9 سعة قناة الضجيج الغاوصي الجمعي محدودة المجال:

Capacity of Band–Limited AWGN Channel

إن سعة القناة C بالتعريف هي المعدل الأعظمي لإرسال المعلومات عبر القناة ، وحيث أن المعلومات المتبادلة $I(X;Y)$ معطاة بالمعادلة (3–55) :

$$I(X;Y)=H(Y)-H(Y/X) \qquad (56-3)$$

إن سعة القناة C هي القيمة العظمى للمعلومات المتبادلة $I(X;Y)$ بالثانية الواحدة. لنوجد في البداية القيمة العظمى لـ $I(X;Y)$ للرمز الواحد . أو يجب إيجاد سعة القناة محدودة المجال بالمقدار $B\ Hz$ مع وجود ضجيج غاوصي أبيض له كثافة طيفية للاستطاعة(PSD) هي $N_0/2$ ، إضافة إلى ذلك سنقوم بتحديد استطاعة الإشارة بالمقدار S ، ولنفرض أن الإشارة المستقبلة $y(t)$ تأخذ الشكل التالي:

$$y(t)=x(t)+n(t) \qquad (57-3)$$

وبما أن القناة محدودة المجال فإن كلا من الإشارة $x(t)$ والضجيج $n(t)$ محدودتين في المجال بالقيمة $B\ Hz$. ومن الواضح أيضا أن $y(t)$ هي محدودة المجال بـ $B\ Hz$، وبالتالي جميع هذه الإشارات يمكن توصيفها بشكل كامل بعينات مأخوذة بمعدل موحد مقداره $2B$ عينة بالثانية، ولنوجد المعلومات الأعظمية التي من الممكن إرسالها لكل عينة ، ولنفرض أن x, n, y تمثل عينات $x(t), n(t), y(t)$ على الترتيب. كمية المعلومات $I(X;Y)$ المرسلة لكل عينة معطاة بالمعادلة (56−3):

$$I(X;Y) = H(Y) - H(Y/X)$$

ويجب علينا إيجاد $H(Y/X)$ من المعادلة (47−3)

$$H(Y/X) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)\log\frac{1}{p(y/x)}dxdy$$

$$= \int_{-\infty}^{\infty} p(x)dx \int_{-\infty}^{\infty} p(y/x)\log\frac{1}{p(y/x)}dy$$

ولأن :

$$y = x + n$$

فمن أجل قيمة لـ x فإن y ستساوي لـ n زائد ثابت (x)، وبالتالي فإن توزع المتحول y عندما تأخذ x قيمة محددة مشابه لتوزع n. فإذا كان $p_n(\cdot)$ تمثل تابع كثافة الاحتمالات PDF لعينات الضجيج n، فعندها :

$$p(y/x) = p_n(y-x) \qquad (58-3)$$

$$\int_{-\infty}^{\infty} p(y/x)\log\frac{1}{p(y/x)}dy = \int_{-\infty}^{\infty} p_n(y-x)\log\frac{1}{p_n(y-x)}dy$$

وبوضع $y - x = z$ سنحصل على:

$$\int_{-\infty}^{\infty} p(y/x)\log\frac{1}{p(y/x)}dy = \int_{-\infty}^{\infty} p_n(z)\log\frac{1}{p_n(z)}dz$$

يمثل الطرف اليميني الانتروبية $H(n)$ لعينات الضجيج n، وعندها :

$$H(Y/X) = H(n)\int_{-\infty}^{\infty} p(x)dx = H(n) \qquad (59-3)$$

يمكن تطبيق هذه المعادلة العامة على كل أنواع الضجيج طالما أن تأثير هذا الضجيج على الإشارة كان بالإضافة (جمعي)، وبالتالي:

$$I(X;Y) = H(Y) - H(n) \qquad bitspersample \qquad (60-3)$$

لقد فرضنا أن متوسط مربع الإشارة $x(t)$ مقيد ليأخذ القيمة S ، وقيمة متوسط مربع الضجيج هو N ، سنفرض أيضاً أن الإشارة $x(t)$ والضجيج $n(t)$ مستقلان ، وبالتالي في هذه الحالة قيمة متوسط مربع الإشارة y سيساوي مجموع قيم متوسط مربعات الإشارتين x و n أي أن:

$$\overline{y^2} = S + N$$

من أجل ضجيج محدد $[H(n)]$ المقدار $I(X;Y)$ أعظمي عندما $H(Y)$ أعظمي. ولقد رأينا من أجل قيمة متوسط مربع y ، $(\overline{y^2} = S + N)$، ستكون $H(Y)$ أعظمية إذا كانت y غاوصية ولها الانتروبية الأعظمية $H_{\max}(Y)$ ومعطاة بالعلاقة :

$$H_{\max}(Y) = \frac{1}{2}\log[2\pi e(S+N)] \qquad (61-3)$$

لأن $y = x + n$ و n غاوصية ، و y ستكون غاوصية فقط إذا كانت x غاوصية . وبما أن قيمة متوسط مربع x هو S هذا سيؤدي إلى:

$$p(x) = \frac{1}{\sqrt{2\pi S}} e^{-x^2/2S}$$

وإلى :

$$I_{\max}(X;Y) = H_{\max}(Y) - H(n)$$
$$= \frac{1}{2}\log[\,2\pi e(S+N)] - H(n)$$

ومن أجل ضجيج الأبيض له متوسط مربع قيمته N نجد:

$$H(n) = \frac{1}{2}\log 2\pi eN; \qquad N = N_0 B$$

وأيضاً:

$$C_s = I_{\max}(X;Y) = \frac{1}{2}\log\left(\frac{S+N}{N}\right) \qquad (62a-3)$$
$$= \frac{1}{2}\log\left(1+\frac{S}{N}\right) \qquad (62b-3)$$

وستكون سعة القناة بالثانية هي كمية المعلومات الأعظمية التي من الممكن إرسالها بالثانية .وتمثل العلاقة (62−3) كمية المعلومات الأعظمية المرسلة لكل عينة . فإذا كانت العينات كلها مستقلة إحصائيا فيما بينها فإن كمية المعلومات الكلية المرسلة بالثانية ستساوي $2B$ ضعف من قيمة C_s، وإذا لم تكن مستقلة فإن المعلومات الكلية ستكون أقل من $2BC_s$ ، ولأن سعة القناة C تمثل كمية المعلومات العظمى الممكن إرسالها بالثانية نقول:

$$C = 2B\left[\frac{1}{2}\log\left(1+\frac{S}{N}\right)\right]$$
$$= B\log\left(1+\frac{S}{N}\right) \qquad bits/s \qquad (63-3)$$

إن عينات الإشارة الغاوصية محدودة المجال مستقلة إحصائياً إذا كانت الكثافة الطيفية لاستطاعة هذه الإشارة PSD منتظمة (uniform) على كامل المجال الترددي فقط ،ومن الواضح أن يكون PSD منتظما للإشارة $y(t)$ لإرسال

المعلومات بأعظم معدل عبر القناة ، تعطى الكثافة الطيفية PSD للإشارة $y(t)$ بالعلاقة :

$$S_y(\omega) = S_x(\omega) + S_n(\omega)$$

وبما أن $S_n(\omega) = N_0/2$ فإن PSD للإشارة $x(t)$ يجب أن تكون منتظمة ، وبالتالي فقد يمكن الوصول إلى المعدل الأعظمي $(C\ bits/s)$ عندما تكون $x(t)$ إشارة بيضاء وغاوصية .

الخلاصة :عندما يكون ضجيج القناة جمعياً، أبيضاً وغاوصياً وله متوسط مربع بقيمة N $(N = N_0 B)$ سعة القناة المحدودة المجال C تحت ظرف إشارة لها الاستطاعة S تعطى بالعلاقة:

$$C = B\log\left(1+\frac{S}{N}\right) \qquad bit/s$$

3– 10 سعة قناة غير محدودة المجال:

Capacity of a Channel of Infinite Bandwidth

يظهر من المعادلة (3–63)أن سعة القناة يمكن أن تصل إلى اللانهاية ∞ عندما يتجه عرض مجال القناة B إلى اللانهاية ∞ ، وهذا بالطبع غير صحيح . فمن أجل الضجيج الأبيض استطاعة الضجيج $N = N_0 B$ ستزداد مع زيادة B ، يمكن عند اقتراب عرض المجال من اللانهاية $B \to \infty$من استنتاج ما هي حدود السعة C:

$$C = B\log\left(1+\frac{S}{N}\right)$$

$$= B\log\left(1+\frac{S}{N_0 B}\right)$$

$$\lim_{B\to\infty} C = \lim_{B\to\infty} B\log\left(1+\frac{S}{N_0 B}\right)$$

$$= \lim_{B\to\infty} \frac{S}{N_0}\left[\frac{N_0 B}{S}\log\left(1+\frac{S}{N_0 B}\right)\right]$$

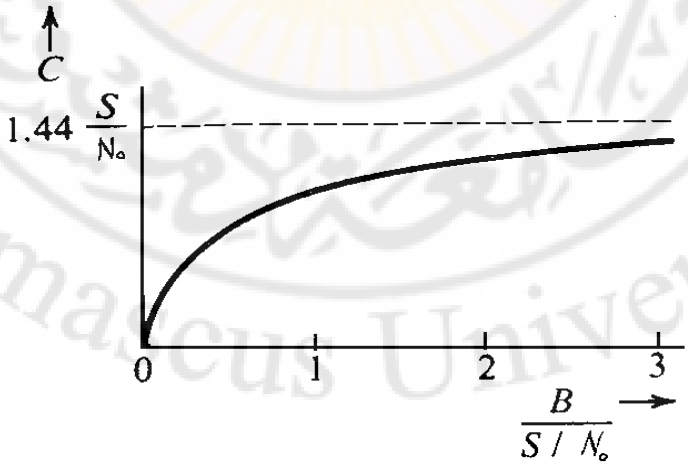
يمكن ايجاد هذه النهاية إذا لاحظنا أن:

$$\lim_{x\to\infty} x\log_2\left(1+\frac{1}{x}\right) = \log_2 e = 1.44$$

وبالتالي:

$$\lim_{B\to\infty} C = 1.44\frac{S}{N_0}\ \ bit/s \qquad (64-3)$$

إذاً سعة القناة في حالة الضجيج الأبيض الغاوصي ستقترب من الحد $1.44S/N_0$ عندما تتجه $B\to\infty$ ، يظهر الشكل (3=5) تغيرات السعة Cمع عرض المجال B ، حيث من الواضح هنا أن السعة يمكن أن تكون من دون حدود فقط عن طريق زيادة استطاعة الإشارة S إلى اللانهاية . لكن من أجل إشارة وضجيج محدودين بالاستطاعة ستبقى سعة القناة محدودة.



الشكل (3-5) تغيرات سعة القناة مع عرض المجال

وقل رب زدني علما
Damascus University

الفصل الرابع

4. ترميز القنوات ذات الضجيج

The Noisy Channel Coding Theorem

وقل رب زدني علما
جامعة دمشق
Damascus University

الفصل الرابع

4. ترميز القنوات ذات الضجيج

The Noisy Channel Coding Theorem

4-1 مقدمة

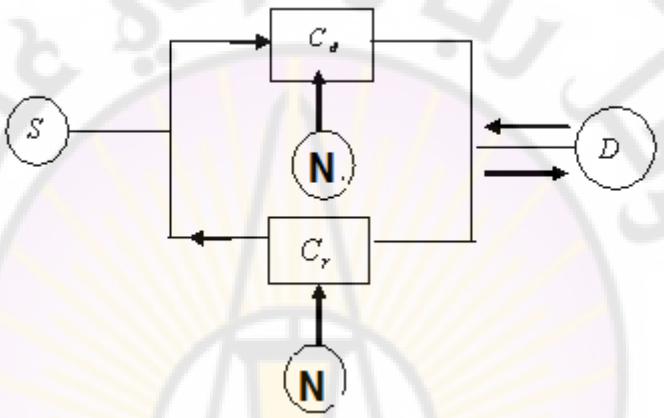
في الفصول السابقة كان الهدف من دراسة الترميز هو الحصول على أنتروبيا عظمى (جميع الرموز لها احتمالات متساوية) للمنبع، وقد أعدت القناة خالية من الضجيج ولذلك يمكن أن نطلق على التراميز السابقة بترميز المنبع (ترميز شانون وفانون) أما في هذه الفصول سنعد أن الأنتروبيا للمنبع عظمى ولكن قبل إرسال هذه الرموز في القناة سنحاول إضافة رموز أخرى تسمى (رموز المراقبة)، وتتم هذه الإضافة بطرق معينة تسمى عملية الترميز.

ترسل هذه الرموز ضمن قناة بعد عملية التعديل وذلك على اعتبار أن القناة ذات الضجيج بينما في التراميز السابقة كانت تفترض القناة بأنها خالية من الضجيج، هناك أمثلة على القناة ذات الضجيج نذكر منها (عملية التخزين والاستعادة للمعلومات، عملية الإرسال والاستقبال اللاسلكي...).

إن الرموز المضافة (رموز المراقبة) الهدف منها هو كشف الأخطاء الناتجة عن عملية الإرسال والتخزين للمعلومات وتصحيحها لذلك تسمى بالتراميز الكاشفة والمصححة للأخطاء.

أبسط نظام لكشف الأخطاء وتصحيحها هو نظام ذو القناة العكسية(قناة الإعادة) ويستخدم في حال أن كمية المعلومات قليلة، ويهدف عمل هذا النظام إلى إعادة المعلومات في الإرسال فيما لو حصل خطأ في الاستقبال. ويسمى ARQ

(Automatic Repetition Request) ويستخدم في أنظمة الإرسال عبر القناة ذات الضجيج القليل، ومنابع ذات تحكم في معدل المعلومات (S: المنبع، D: المستقبل، Cd: القناة المباشرة، Cr: القناة العكسية، N: الضجيج).



الشكل (4-1) نظام إرسال بوصلة عكسية

أما في القنوات ذات الضجيج الكبير فنستخدم نظام التصحيح الآلي (حيث أن عملية الإعادة) تصبح غير فعالة لأن الخطأ يصبح كبيراً وبالتالي عملية الإعادة تصبح كثيرة التكرار.

4-1-1 تصنيف الترميز الكاشفة والمصححة للأخطاء :

ا- **الترميز الكتلي** Block Coding: تتم عملية كشف الأخطاء وتصحيحها بتقسيم المعلومات إلى أقسام كل قسم يسمى كلمة وهناك نوعان للترميز الكتلية:

أ - **الترميز الزمري Group Coding:** تعد الكلمات هنا عبارة عن عناصر في الفراغ الشعاعي (أشعة) Vectors.

ب – الترميـز الـدوري Cyclic Coding: تعـد الـكلمات عبـارة عـن عناصر الجبر أي عبارة عن كثيرات حدود.

II– الترميـز الانطـوائي Convolutional Coding: تكـون معـالجة الرموز بشكل مستمر أي لا تجزأ إلى أقسام.

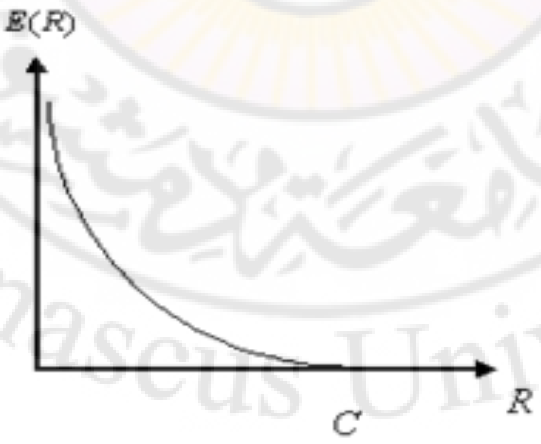
4 –2 نظرية شانون للأقنية ذات الضجيج :

تقول النظريـة: إذا كـان لديـنا منبع ذو معدل معلومات R bit/s وقناة ذات سعة C bit/s وإذا كان R < C فإنـه يوجد ترميز طول الكلمة فيه n يجعل احتمال الخطأ في حال كشف الترميز (P_E).

$$P_E \leq 2^{-nE(R)} \qquad (4-1)$$

حيث: n طول الكلمة المرمزة.

E(R): دالة غير سالبة تسمى دالة أسية الأخطاء ولها الشكل (4–2).



الشكل (4–2) تابع الأخطاء الأسي

تشير هذه النظرية إلى وجود ترميز لكن لا تبين كيف يتم تصميم هذا المرمز ولكن المهم في هذه النظرية بأنه مهما كان مستوى الضجيج في القناة فإنه يمكن إرسال المعلومات باحتمالية خطأ صغيرة جدا، وأدت هذه النظرية إلى تطور كبير في عالم الاتصالات.

عمليا في الحالة التي فيها $R < \frac{1}{2}C$ فإنه يوجد مرمزات تعطي P_E بأقل قيمة ممكنة.

4-3 الترميز الزمري:

تعد الكلمة هنا عبارة عن شعاع ومركبات هذا الشعاع هي رموز الكلمة وقد سمي بالترميز الزمري على اعتبار أن الفراغ الشعاعي هو عبارة عن زمرة (عملية الجمع والطرح داخلية) ويرمز للكلمة:

$$W = [a_1 \quad a_2 \quad ..... \quad a_n]$$

وبما أن الرموز في النظام الثنائي فإن ai هي عناصر في الحقل [1,0] ويرمز لهذا الحقل GF(2) فعملية الجمع والضرب من النموذج (2) هي على الشكل التالي :

*	0	1		+	0	1
0	0	0		0	0	1
1	0	1		1	1	1

من الناحية الفيزيائية فإن 0,1 تمثل فئة واسعة من الإشارات حيث:

0 : نبضة سالبة. 1: نبضة موجبة أو العكس.

0:إشارة جيبية طورها 0 1:إشارة جيبية طورها π.

0:وجود إشارة.	1: عدم وجود إشارة.

4-3-1 تعيين الكلمات ذات المعنى :

نقول عن كلمات ذات معنى إذا كانت كل كلمة تحتوي على معلومات صحيحة للمعلومات المرسلة.

إذا كانت الكلمة مكونة من n رمز فإنه يتشكل لدينا عدد من الكلمات $N = 2^n$ ، هذه الكلمات لها بنية الشعاع الفراغي, سنسمي مجموعة الكلمات التي لها معنى بالفراغ الشعاعي الجزئي S.

$$S = N = 2^n \qquad (4-2)$$

متوسط المعلومات في الكتلة الواحدة:

$$I = \log N = n \qquad (4-3)$$

ومتوسط المعلومات في الرمز (وهي القيمة العظمى):

$$i_n = \frac{I}{n} = 1bit \qquad (4-4)$$

إذا كانت كافة الكلمات ذات معنى, في هذه الحالة لا توجد إمكانية لكشف الأخطاء وتصحيحها التي تدخل في عملية الإرسال من خلال القناة، ففي حال تعرض أي كلمة إلى خطأ فستنتج كلمة أخرى أيضا لها معنى وبالتالي لا يمكن معرفة حصول خطأ في الكلمة، ولنتمكن من عملية كشف الخطأ وتصحيحه في الكلمة نقوم بالخطوة التالية:

يتم تقسيم مجموعة الكلمات W إلى مجموعتين جزئيتين V و F حيث الكلمات $N_i \in V$ لها معنى أي هي كلمات الترميز ونفترض عددهن $S = 2^k$

حيث $k < n$ أما الكلمات $w_j \in F$ فليس لها معنى (أي لا تحتوي على معلومات).

متوسط المعلومات المرسلة في الكلمة في هذه الحالة:

$$I = \log S = k \qquad (4-5)$$

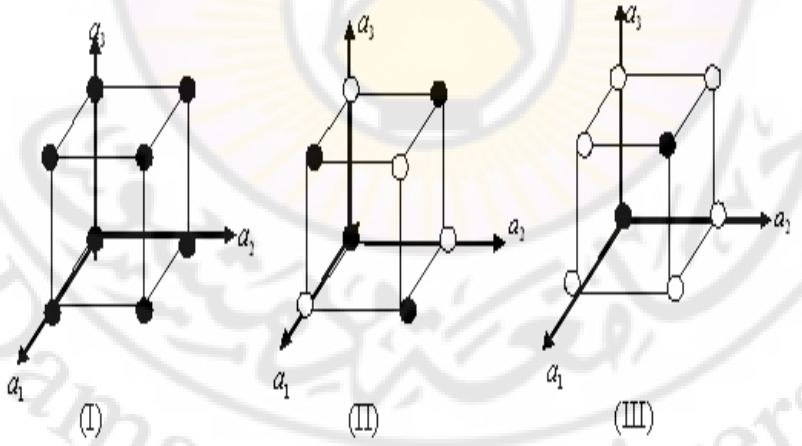
أما متوسط المعلومات في الرمز فيكون:

$$i_k = \frac{k}{n} \qquad (4-6)$$

حيث i_k أصغر من i_n المعطاة في العلاقة (4–4).

في الشكل (4–3) نبين هندسيا عملية اختيار كلمات الترميز عندما n=3.

تمثل الدوائر السوداء الكلمات المرمزة التي لها معنى، بينما تمثل الدوائر البيضاء الكلمات التي ليس لها معنى.



الشكل (4–3) اختيار الكلمات المرمزة في حالة n=3 رمز

في الحالة I جميع الكلمات لها معنى $N = 2^3 = 8$ وبالتالي ظهور الخطأ لا يمكن كشفه.

في الحالة II نختار $S = 2^2 = 4$ فظهور الخطأ في كلمات لها معنى يؤدي

إلى كلمة من دون معنى (يتم تغيير إحداثية واحدة للكلمة)، هنا يتم كشف الخطأ ولكن لا يتم التصحيح.

أما في الحالة III فنختار $S = 2^1 = 2$ كلمات لها معنى وبالتالي ظهور الخطأ يمكن كشفه وتصحيحه.

سنشير فيما يلي إلى الكلمات المرمزة (المرسلة) v_i، أما الكلمات المستقبلة (التي تنتج عن v_i ولكن تختلف عنها بسبب وجود أخطاء ناتجة عن عملية الضجيج) v_i' :

$$v_i = [a_{i1} \quad a_{i2} \quad ..... \quad a_{in}]$$
$$v_i' = [a_{i1}' \quad a_{i2}' \quad ..... \quad a_{in}'] \qquad (4-7)$$

إذا كانت:

$$v_i' = v_i \Rightarrow a_{i1}' = a_{i1} \quad a_{i2}' = a_{i2} \quad ..... \quad a_{in}' = a_{in}$$

نستنتج بأنه لم يحدث خطأ أثناء عملية الإرسال والاستقبال.

4-3-2 الكلمات كعناصر للفئات المتجاورة :

ليكن لدينا مجموعة العناصر w للفراغ الشعاعي W (بنية زمرة) ويكون الفراغ الشعاعي الجزئي V (له بنية زمرة جزئية) نعد هذه العناصر $v \in V$ لها معنى يمكن تشكيل فئات متجاورة بناء على الفراغ الجزئي كما يلي:

أ- تتشكل الفئة الأولى من عناصر (الكلمات التي لها معنى) $v \in V$ نبدأ بالكلمة صفر، ويختلف عن الصفر الثنائي في GF(2) على اعتبار أنه مصفوفة من العناصر ذات أصفار.

ب – نختار أول كلمة من الفئة الثانية (واحدة من الكلمات من دون معنى ذات عدد أقل ما يمكن من 1 وغير موجود في الفئة الأولى ونشير إليه ε_1.

ت – تتشكل بقية الكلمات من الفئة الثانية وذلك بالجمع ε_1 وكلمات الفئة الأولى.

$$\begin{array}{cccccc} 0 & v_1 & v_2 & v_3 & ..... & v_{s-1} \\ \varepsilon_1 & \varepsilon_1+v_1 & \varepsilon_1+v_2 & \varepsilon_1+v_3 & ..... & \varepsilon_1+v_{s-1} \\ \varepsilon_2 & \varepsilon_2+v_1 & \varepsilon_2+v_2 & \varepsilon_2+v_3 & ..... & \varepsilon_2+v_{s-1} \\ ..... & ..... & ..... & ..... & ..... & ..... \end{array} \qquad (4\text{-}8)$$

تستمر العملية حتى نحصل على جميع العناصر من المجموعة W التي تشكل الفراغ الشعاعي المعرف بالمعادلة:

$$\forall v_i \in V; \forall \varepsilon_j \in W \quad \mathbf{v_i + \varepsilon_i = v'_i \in W}$$

1	**1**	**1**		**0**	**0**	**0**
1	1	0		0	0	1
1	0	1		0	1	0
0	1	1		1	0	0

الجدول (4 – 1)

نلاحظ من الجدول أن جميع الكلمات المحتملة من W موجودة, نعد الصف الأول يمثل الكلمات ذات المعنى, تتم عملية كشف الترميز بمعرفة العمود الذي توجد فيه الكلمة المستقبلة ثم نذهب إلى بداية العمود (الصف الأول) لنحصل على أصل الكلمة ولتبسيط ذلك نعد المجموعة W تحتوي على العناصر $2^3 = 8$ كلمة

حيث $2 = 2^1$ هي كلمات لها معنى، يتم تشكيل الفئات المجاورة حسب الجدول التالي:

1. إذا كانت الكلمة المستقبلة 100 نستنتج أن الكلمة المرسلة هي 000، الخطأ في المكان الأول.
2. إذا استقبلنا الكلمة 101 نستنتج أن الكلمة المرسلة هي 111 وأنه حصل خطأ في المكان الثاني.
3. نلاحظ في العمود الأول بأن المكان الذي أصبح فيه خطأ هو 1 والرموز الباقية صفر.
4. هذا الترميز يستطيع تصحيح خطأ واحد في أي مكان كان.
5. الكلمات في العمود الأول تكون قريبة جدا من الكلمة في بداية العمود أكثر من أي كلمة أخرى في أي عمود آخر أو في العمود نفسه.

يعد استخدام هذه الطريقة غير مجدٍ في حال كان عدد الكلمات المرسلة كبيراً جدا، لكن هذه الطريقة تساعدنا على فهم تقنية تصحيح الأخطاء.

4-3-3 مسافة هامينغ:

تحدد مسافة هامينغ (نسبة لعالم الرياضيات هامينغ) بناء على مفهوم تابع المسافة الصغرى $D(\boldsymbol{v}i,\boldsymbol{v}j)$ في الفراغ الذي يحتوي على n كلمة والذي يحقق مفهوم الفراغ المتري(القياسي) ويعرف هذا التابع

$$D(v_i, v_j) = (a_{i1} \oplus a_{j1}) + (a_{i2} \oplus a_{j2}) + \ldots\ldots\ldots + (a_{in} \oplus a_{jn}) \qquad (4\text{-}9)$$

تتم عملية الجمع في الحقل $GF(2)$ المحدود بعنصرين $(1,0)$:

$$D(v_i, v_j) = \sum_{k=1}^{n} (a_{ik} \oplus a_{jk}) \qquad (4-10)$$

تحدد مسافة هامينغ بين كلمتين مرمزتين بمقدار عدد الرموز المختلفة بين هاتين الكلمتين.

نحسب المسافة في المثال السابق فنحصل على (D=1) في الحالة I, و (D=2) في الحالة II, و (D=3) في الحالة III.

4-3-4-1 اتخاذ القرار بناء على المسافة الصغرى

لنفترض أن عملية الإرسال تتم من خلال قناة ثنائية متناظرة وبدون ذاكرة (تكون فيها احتمالية الخطأ متساوية لكل الرموز وكل رمز مستقل عن الآخر)

ولنفترض كل رمز يمكن أن يرسل بشكل صحيح باحتمال q، وخطأ باحتمال p<1/2 حيث أن احتمالية الكلمة المستقبلة $\boldsymbol{v}'_i$ هي $\boldsymbol{v}_i$ المرسلة.

$$P(v_i / v'_i) = p^{D(v'_i / v_i)} q^{n - D(v'_i / v_i)} \qquad (4-11)$$

حيث $D(\boldsymbol{v}'_i, \boldsymbol{v}_i)$ المسافة الصغرى بين $\boldsymbol{v}$ و $\boldsymbol{v}'$، أما احتمالية أن تكون الكلمة المستقبلة $\boldsymbol{v}'_i$ هي $\boldsymbol{v}_j$ المرسلة:

$$P(v_j / v'_i) = p^{D(v'_i / v_j)} q^{n - D(v'_i / v_j)} \qquad (4-12)$$

وبما أن معظم الأقنية تحمل الميزة $p << 1$ و $q \sim 1$ وبالتالي تكتب العلاقة

$$P(v_i / v'_i) = p^{D(v'_i, vi)} \qquad (4-13)$$

$$P(v_j / v'_i) = p^{D(v'_i, v_j)} \qquad (4-14)$$

$$D(v'_i, v_i) < D(v'_i, v_j) \qquad \forall j \neq i \qquad (4-15)$$

إذاً:

$$p(v_i^{'}, v_i) < p(v_i^{'}, v_j) \qquad \forall j \neq i \qquad (4\text{-}16)$$

نستنتج من ذلك أنه إذا كانت المسافة بين الكلمة المستقبلة $\boldsymbol{v}_i$ و $\boldsymbol{v}_i'$ المرسلة هي أصغر مسافة من أي كلمة مرمزة مستقبلة أخرى فإن احتمالية $\boldsymbol{v}_i'$ هي $\boldsymbol{v}_i$ هو أكبر احتمال ممكن من أي كلمة أخرى.

4-3-3-2 منطقة أخذ القرار

يتم تجزئة المجموعة W إلى مجموعات جزئية منفصلة W_i حول نقاط $\boldsymbol{v}_i \in W_i$ لها خصائص جميع النقاط و $\boldsymbol{v}_{i'} \in W_i$ هي أقرب إلى $\boldsymbol{v}_i$، بناء على المسافة الصغرى أي أقرب الكلمات إلى $\boldsymbol{v}_i$ من النقطة $\boldsymbol{v}_i$ من اجل $j \neq i$.

من أجل النقطة $\boldsymbol{v}_i'$ لدينا العلاقة

$$D(v_i^{'}, v_i) < D(v_i^{'}, v_j) \qquad \forall j \neq i \qquad (4\text{-}15)$$

حينئذ

$$v^{'}{}_i \in W_i \qquad (4\text{-}18)$$

أما مجموعة النقاط $\boldsymbol{v}_i'$ التي تقع على مسافة واحدة من $\boldsymbol{v}_i$ و $\boldsymbol{v}_j$ فتنتمي إلى مجموعة W_0 أي

$$v^{'}{}_i \notin W_j \qquad \forall j \neq 0 \qquad (4\text{-}19)$$

من أجل أي قيمة j

$$v_i^{'} \in W_0 \qquad (4\text{-}20)$$

وبهذا فأن جميع نقاط الفراغ W تنتمي إما إلى $W_i (i=1,2,3,\ldots..s)$ أو إلى W_0 أي:

$$W_0 \cup W_1 \cup W_2 \cup \ldots\ldots\ldots \cup W_s = W = V \cup F \qquad (4-21)$$

حيث F مجموعة الكلمات التي من دون معنى .

أما الكلمات المستقبلة فيمكن أن تكون كما يلي إذا كانت:

$$\boldsymbol{v}_i' \in F \qquad (4-22)$$

الكلمة المستقبلة ليست من الكلمات المرمزة وبالتالي يمكن كشف الأخطاء.

أما إذا كانت:

$$\boldsymbol{v}_i' \in W_i \qquad i \neq 0 \qquad (4-23)$$

أي إن:

$$D(\boldsymbol{v}_i', \boldsymbol{v}_i) < D(\boldsymbol{v}_i', \boldsymbol{v}_j) \qquad \forall j \neq i \qquad (4-24)$$

يمكن تصحيح الأخطاء على اعتبار أن $\boldsymbol{v}_i'$ تنتج من $\boldsymbol{v}_j$.

إذا كانت:

$$\boldsymbol{v}_i' \in W0 \qquad (4-25)$$

يمكن القول إن:

$$D(\boldsymbol{v}_i', \boldsymbol{v}_i) = D(\boldsymbol{v}_i', \boldsymbol{v}_j) \qquad \forall j \neq i$$

من أجل حالات j لا يمكن تصحيح الأخطاء ولكن يمكن كشفها باعتبار:

$$W_0 \subset F \qquad (4-26)$$

إذا:

$$\boldsymbol{v}_{i'} \in F \qquad (4-27)$$

أما إذا كانت جميع الكلمات لها معنى فتصبح F خالية و لا يمكن كشف الأخطاء و لا تصحيحها.

ينتج مما سبق أن إمكانية كشف الأخطاء وتصحيحها تصبح كبيرة بقدر ما تحتوي Wi عناصر أكثر, حيث جميع العناصر $v_{i'} \in W_i$ هي من v_i.

يتم إنجاز ذلك إذا كان $v_i \in W_i$ موجودة على مسافة كبيرة من أقرب كلمة ذات معنى $v_j \in W_j$ ينتج عن ذلك، أن إمكانية كشف الكلمات وتصحيحها لترميز ما تعتمد على المسافة الصغرى بين الكلمتين المرمزتين بحيث أنه لكشف e خطأ في أي مكان من الكلمة فإن المسافة الصغرى يجب أن تكون:

$$D_{\min} = e + 1 \qquad (4-28)$$

ولتصحيح e خطأ في أي مكان تكون المسافة الصغرى:

$$D_{\min} = 2e + 1 \qquad (4-29)$$

ولتصحيح e خطأ وكشف d خطأ يجب أن تكون المسافة الصغرى:

$$D_{\min} = 2e + 1 + d \qquad (4-30)$$

4-3-4 كلمة الخطأ

لفهم تقنية كشف الأخطاء وتصحيحها لابد من تحليل الأخطاء التي يجب كشفها وتصحيحها.

يعد الضجيج عبارة عن موسط L يقوم بتحويل من فراغ الكلمات المرمزة v_i (المرسلة ضمن القناة) إلى فراغ الكلمات v_i' (على مخرج قناة الإرسال):

$$L\{v_i\} = v_i' \qquad (4-31)$$

تكتب هذه العلاقة بشكل مبسط بحيث تعرف الكلمة الخاطئة بأن لها نفس الطول n. تعد كلمة الخطأ أنها ضجيج القناة، وبالتالي تكتب على شكل مصفوفة:

$$\varepsilon = [\varepsilon_1 \quad \varepsilon_2 \quad ..... \quad \varepsilon_n] \qquad (4-32)$$

تأخذ الرموز $\varepsilon_i (i = 1,2,.....,n)$ القيم 0 أو 1 بحيث, تأخذ ε_i القيمة 1 إذا

كان الضجيج يدخل خطأ في المكان i (يغير 1 إلى الصفر وبالعكس) وبأخذ القيمة 0 في حال عدم وجود خطأ.

فيما يلي نشير إلى أماكن الرموز للكلمة بدءاً من اليسار إلى اليمين، فكلمة الخطأ يمكن أن تكتب:

$$\varepsilon = [..... \quad \alpha_{i1} \quad ..... \quad \alpha_{ie} \quad .....] \qquad (4-33)$$

حيث :

1) الرموز $\alpha_{i1}, \alpha_{i2}, ..., \alpha_{ie}$ هي الرموز 1 وبقية الرموز التي تكمل حتى n هي أصفار.

2) العلامات $i_1, i_2, ..., i_e$ هي عدد من (n−1) تشير إلى أماكن ظهور الخطأ.

تبين المعادلات (4−32) و (4−33) أن الرموز $\varepsilon_{i1}, \varepsilon_{i2}, ..., \varepsilon_{ie}$ مساوية إلى 1 والباقي يساوي إلى أصفار.

وبناءً على التعريف لكلمة الخطأ، فإن العلاقة (4−31) تكتب على الشكل التالي:

$$L\{v_i\} = v_i + \varepsilon = v_i' \qquad (4-34)$$

حيث + تشير إلى الجمع الثنائي للمصفوفات ε, v_i نشير إلى:

$$v_i = [a_{i1} \quad a_{i2} \quad ..... \quad a_{in}] \qquad (4-35)$$

$$v_i' = [a_{i1}' \quad a_{i2}' \quad ..... \quad a_{in}'] \qquad (4-36)$$

نحصل على:

$$a'_{i1} = a_{i1} + \varepsilon_1$$
$$a'_{i2} = a_{i2} + \varepsilon_2 \qquad (4-37)$$
$$\cdots\cdots\cdots$$
$$a'_{in} = a_{in} + \varepsilon_n$$

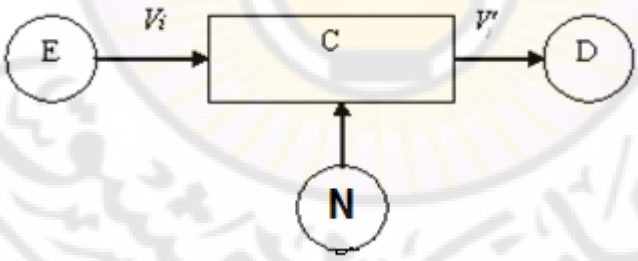
أو بالجمع الثنائي على الشكل التالي :

$$a_{i1} = a'_{i1} + \varepsilon_1$$
$$a_{i2} = a'_{i2} + \varepsilon_2 \qquad (4-38)$$
$$\cdots\cdots\cdots$$
$$a_{in} = a'_{in} + \varepsilon_n$$

تمثل هذه العلاقة تحويلة فوريه العكسية:

$$v_i = F^{-1}\{v'_i\} = v'_i + \varepsilon \qquad (4-39)$$

تتمثل عملية إدخال الخطأ في الشكل (4-4)



الشكل (4-4) المخطط التمثيلي لعملية إدخال الأخطاء

4-3-4-1 الأخطاء المنفردة

لنفترض أن كل رمز مرسل يتأثر بالضجيج بشكل مستقل عن الآخر, وبالتالي تظهر الأخطاء مستقلة عن بعضها وهذا ما نراه في الضجيج المتغير نشير إلى الأخطاء التي تظهر في الأقنية الثنائية التناظرية p.

يتم حساب احتمالية ظهور r خطأ مستقل ضمن كلمة طولها n بقانون التوزيع الثنائي

$$p(r) = C_n^r p^r (1-p)^{n-r} \qquad (4-40)$$

هذه العلاقة محققة من أجل أي ترميز, يبين الشكل أن الاحتمالية تهبط فجأة في حال تجاوز عدد الأخطاء حداً معيناً أما احتمالية ظهور e خطأ أو أقل فهي:

$$P\{r \le e\} = \sum_{r=0}^{e} p(r) = \sum_{r=0}^{e} C_n^r p^r (1-p)^{n-r} \qquad (4-41)$$

يتبين من المعادلتين أن احتمالية الخطأ تعتمد على عدد الأخطاء وليس على توضعها.

4-3-4 -2 رزمة الأخطاء

تظهر الأخطاء على شكل رزمة إذا كانت فترة الضجيج أكبر من فترة الرمز وتسمى رزمة الأخطاء، تنتج هذه الأخطاء نتيجة تأثير ضجيج النبضات أو قطع في القناة أو وسط التخزين للمعلومات (خطوط الهاتف – أنظمة الذاكرة –الأسطوانة المغناطيسية – القرص المدمج).

إذاً رزمة الأخطاء: هي سلسلة من الرموز (صحيحة أو خاطئة) حيث أول وآخر رمز يكون خطأ تظهر الرموز الصحيحة المتتالية كمجموعة أقل من p.

توصف رزمة الأخطاء بالموسط p ويعتمد على المواصفات الإحصائية لقناة الإرسال .

يوجد بين آخر رمز (خطأ) لرزمة الأخطاء وأول رمز (خطأ) للرزمة التالية، أكثر من p رمز صحيح متتالٍ.

إذا وجد خطآن بينهما $s < p$ رمز غير خاطئ (صحيح) فهما يشكلان قسماً من الرزمة، أما إذا كان $s \geq p$ رمزاً صحيحاً فإنهما يشكلان قسماً من رزمتين مختلفين.

ويعرف ℓ بأنه طول الرزمة والذي يساوي إلى العدد الكلي للرموز (الخاطئة والصحيحة) التي تشكل رزمة الخطأ حيث يكون أول رمز وآخر رمز خطأ.

توصف رزمة الأخطاء أيضا بموسط آخر وهو كثافة الأخطاء D : وهي النسبة بين عدد الرموز الخاطئة من الرزمة إلى العدد الكلي لرموز الرزمة.

تحتوي الكلمة الخطأ على رزمة من الأخطاء طولها (ℓ) يكتب بالشكل التالي:

$$\ell = [\ldots\ldots \quad \alpha_i \varepsilon_{i+1} \quad \ldots\ldots \quad \varepsilon_{i+\ell-2} \alpha_{i+\ell-1} \quad \ldots\ldots \quad] \qquad (4-42)$$

حيث:

α_i: رمز 1 و يتوضع في المكان i.

ε_{i+k}: يمثل الرمز 0 أو 1 و يتوضع في المكان $i+k$ مع التأكيد أنه لا يمكن أن تظهر مجموعة أصفار أكبر أو يساوي p.

4-3-5 تقنية كشف الأخطاء وتصحيحها :

يمثل الفراغ ذو الأبعاد m $(m = n - k)$، فراغ التصحيح Z حيث له 2^m عنصر, و يسمى $z \in Z$ بالمصحح أو شعاع المراقبة ويمثل بعامود.

تشير هذه المصححات إلى مكان الخطأ في الكلمة المرمزة, ويتم وضع تقابل بين مجموعة الكلمات المستقبلة (الفراغ W) ومجموعة المصححات (الفراغ Z) يحدد هذا التقابل بموسط :

$$H\{v_i'\} = z \qquad \forall v_i' \in W, z \in Z \qquad (4-43)$$

إذا كانت $v_i' = v_i$ عندئذ لا يوجد خطأ في عملية الإرسال و المصحح z نفسه من أجل أي i وتكون قيمة z في هذه الحالة مساوية إلى الصفر وبالتالي تصبح العلاقة (43−4):

$$H\{v_i\} = 0 \qquad i:1 \longrightarrow s = 2^k \qquad (4$$

نكتب الموسط H بشكل $H\{v_i'\} = 0$ و $z = 0$ إذا وفقط إذا v_i' الكلمة المرسلة المرمزة أي $v_i' = v_i$.

لتصحيح الأخطاء الناتجة عن عملية الإرسال لابد أن يكون لكل كلمة خاطئة ناتجة عن الضجيج للقناة مصحح وحيد يختلف عن الصفر.

يجب أن تصحح مجموعة الكلمات الخاطئة الممثلة بنقاط في الفراغ E أبعاده n.

نحدد موسط $\wp$ وذلك بتقابل بين نقاط الفراغ E الذي يمثل الأخطاء التي يمكن تصحيحها والفراغ المصحح Z

$$\wp\{z\} = \varepsilon \qquad \varepsilon \in E \qquad (4-45)$$

$$\wp^{-1}\{\varepsilon\} = z \qquad z \in Z \qquad (4-46)$$

يتم كشف الأخطاء وتصحيحها بمساعدة الموسطين H و $\wp$ على الشكل التالي:

1. إذ تبين لنا

$$H\{v_i'\} \neq 0 \qquad (4-47)$$

دون أن نبين قيمة z نقول إنه تمت عملية كشف الخطأ.

2. إذ تمت معرفة قيمة z في الفراغ Z عندئذ يمكن تصحيح الخطأ

$$H\{v_i'\} = z \qquad (4-48)$$

إذ بمعرفة $\wp$ نحصل على

$$\wp\{z\} = \varepsilon \qquad (4-49)$$

وبمساعدة الكلمة الخاطئة المعروفة نحصل على الكلمة الصحيحة (الكلمة المرسلة).

$$F^{-1}\{v_i'\} = v_i' + \varepsilon = v_i \qquad (4-50)$$

4-3-6 مصفوفة التصحيح (المراقبة)

يحدد الموسط H بتحويلة أحادية الاتجاه بين فراغ الكلمات المستقبلة و فراغ المصححات (التحويلة العكسية غير معروفة) و نحصل على أبسط بنية للموسط H من هذه التحويلة:

$$\begin{aligned} &h_{11}a_1' + h_{12}a_2' + ... + h_{1n}a_n' = c_1 \\ &h_{21}a_1' + h_{22}a_2' + ... + h_{2n}a_n' = c_2 \\ &..... \\ &h_{m1}a_1' + h_{m2}a_2' + ... + h_{mn}a_n' = c_m \end{aligned} \quad ; h_{ij}, a_i, c_i \in GF(2) \qquad (4-51)$$

h_{ij} : موسطات تمثل المصفوفة H.

a_i : رموز الكلمة المستقبلة.

c_i : الإحداثيات التي تحدد النقطة z (مركبات المصحح).

يمكن أن تكتب العلاقة (51–4) بشكل مختصر:

$$H = \begin{bmatrix} h_{11} & h_{12} & .... & h_{1n} \\ h_{21} & h_{22} & .... & h_{2n} \\ .... & .... & .... & .... \\ h_{m1} & h_{m2} & .... & h_{mn} \end{bmatrix} \qquad (4-52)$$

وتسمى هذه المصفوفة بمصفوفة المراقبة.

نشير إلى الكلمات بشكل مصفوفة (صف):

$$v' = \begin{bmatrix} a'_1 & a'_2 & .... & a'_n \end{bmatrix} \qquad (4-53)$$

والمصححات على شكل مصفوفة (عامود):

$$z = \begin{bmatrix} c_1 \\ c_2 \\ ... \\ c_m \end{bmatrix} \qquad (4-54)$$

نستنتج من العلاقات السابقة أنه يمكن كتابة العلاقة (51–4) على الشكل التالي:

$$Hv'^T = z \qquad (4-55)$$

حيث v'^T مصفوفة النقل (التحويل) للمصفوفة v'.

وتكون الكلمة المستقبلة هي الكلمة المرسلة $(v' = v)$ طبقا للعلاقة (43–4) حيث المصحح يساوي الصفر.

$$Hv'^T = 0 \qquad (4-56)$$

من خلال المعالجة لهذه المصفوفة يمكن كتابتها على الشكل التالي:

$$H=\begin{bmatrix}1&0&....&0&q_{11}&q_{12}&....&q_{1k}\\0&1&....&0&q_{21}&q_{22}&....&q_{2k}\\0&0&....&....&....&&&\\0&0&....&1&q_{m1}&q_{m2}&....&q_{mk}\end{bmatrix}=[I_m Q] \qquad (4-57)$$

حيث I_m المصفوفة الأحادية من الدرجة m وتكون Q :

$$Q=\begin{bmatrix}q_{11}&q_{12}&....&q_{1k}\\q_{21}&q_{22}&....&q_{2k}\\....&....&....&....\\q_{m1}&q_{m2}&....&q_{mk}\end{bmatrix} \qquad (4-58)$$

يتبين من خلال تغيير ترتيب الرموز للكلمة المرمزة أنه لا تتغير خواص الكشف أو التصحيح للترميز ونقول إننا حصلنا على ترميز مكافئ. تنقل رموز كلمة الترميز إذا نقلنا أعمدة المصفوفة H ونقل أعمدة المصفوفة H تقودنا إلى ترميز مكافئ.

4-3-7 الترميز الزمري اعتمادا على مصفوفة المراقبة H

تكتب الكلمة المرمزة على شكل مصفوفة (صف):

$$v=[a_1 a_2 \quad .... \quad a_m a_{m+1} \quad .... \quad a_n] \qquad (4-59)$$

الرموز الأولى:

$$c=[a_1 \quad a_2 \quad .... \quad a_m] \qquad (4-60)$$

تعد رموزاً إضافية تساعد على كشف أو تصحيح الأخطاء وتسمى برموز المراقبة، أما بقية الرموز:

$$i = [a_{m+1} \quad .... \quad a_{m+k}] \qquad (4-61)$$

حيث

$$m + k = n$$

تسمى رموز المعلومات وبالتالي تكتب الكلمة المرمزة:

$$v = [c \quad i] \qquad (4-61-a)$$

يتم تحديد الرموز m (رموز المراقبة) بناء على رموز المعلومات (k) نستعين بالمعادلة (44−4) :

$$Hv^T = 0 \qquad (4-62)$$

نستنتج مما سبق:

$$Hv^T = [I_m \quad Q]\begin{bmatrix} c^T \\ i^T \end{bmatrix} = 0 \Rightarrow c^T + Qi^T = 0 \qquad (4-63)$$

أو:

$$c^T = Qi^T \qquad (4-64)$$

تحدد عملية رموز المراقبة بدلالة رموز المعلومات وتسمى هذه العملية بالترميز، فالعلاقة (64−4) يمكن كتابتها:

$$\begin{bmatrix} q_{11} & q_{12} & .... & q_{1k} \\ q_{21} & q_{22} & .... & q_{2k} \\ .... & .... & .... & .... \\ q_{m1} & q_{m2} & .... & q_{mk} \end{bmatrix}\cdot\begin{bmatrix} a_{m+1} \\ a_{m+2} \\ ... \\ a_{m+k} \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ ... \\ a_m \end{bmatrix} \qquad (4-65)$$

ينتج عن ذلك:

$$a_j = \sum_{i=1}^{k} q_{ji}.a_{m+i} \qquad j = \overline{1 \to m} \qquad (4-66)$$

أي أننا نحصل على رموز المراقبة من تشكيلة خطية باستخدام الجمع الثنائي لرموز المعلومات.

تطبق خاصية المصحح على كلمات الترميز بحيث تصبح النتيجة تساوي الصفر، وإذا حصل أثناء عملية الإرسال أي خطأ فإن المصحح يصبح لا يساوي الصفر.

تصحح الأخطاء من العلاقات (4-43) و (4-49) و (4-50), ويسمى **الترميز نظامياً** فيما لو كانت رموز المعلومات المختارة عشوائيا موجودة في بداية (أو نهاية الكلمة المرمزة)، وهذا الترميز له ميزة وهي أن عملية التصحيح تكون بسيطة, حيث أنه في عملية كشف الترميز نستخدم فقط بوابة يتم وصلها في زمن وصول رموز المعلومات فقط وهي الرموز التي تهمنا في الاستقبال.

4-3-7-1 العلاقة بين أعمدة المصفوفة H في حال تصحيح الأخطاء

يتم تحديد الشروط التي يجب أن تتحقق في المصفوفة H لتصحيح الأخطاء e ، لنفترض أن الكلمة المستقبلة:

$$v' = v + \varepsilon \qquad (4-67)$$

حيث

$$\varepsilon = [..... \quad \alpha_{i1} \quad ..... \quad \alpha_{ie} \quad .....] \qquad (4-68)$$

هي كلمة الخطأ وفيها e رمز يساوي 1.

المصحح المقابل للكلمة v' :

$$z = Hv'^T = H(v+\varepsilon)^T = Hv^T + H\varepsilon^T \qquad (4-69)$$

وبما أن : $Hv^T = 0$ ينتج من ذلك:

$$z = H\varepsilon^T \qquad (4-70)$$

أو:

$$z = \begin{bmatrix} h_{11} & h_{12} & .... & h_{1n} \\ h_{21} & h_{22} & .... & h_{2n} \\ .... & .... & .... & .... \\ h_{m1} & h_{m2} & .... & h_{mn} \end{bmatrix} \cdot \begin{bmatrix} ... \\ \alpha_{i1} \\ ... \\ \alpha_{ie} \\ ... \end{bmatrix} \qquad (4-71)$$

وللتبسيط نشير إلى أعمدة المصفوفة H بـ $h_1 \quad h_2 \quad .... \quad h_n$ والعلاقة (4–71) تكتب بالشكل التالي:

$$z = \begin{bmatrix} h_1 & h_2 & .... & h_n \end{bmatrix} \cdot \begin{bmatrix} ... \\ \alpha_{i1} \\ ... \\ \alpha_{ie} \\ ... \end{bmatrix} \qquad (4-72)$$

$$z = \left[.....\alpha_{i1}h_{i1} + ... + \alpha_{ie}h_{ie} + ...\right] \qquad (4-73)$$

وبما أن: $\alpha_{i1} = \alpha_{i2} = ... = 1$ ينتج لدينا

$$z = \left[h_{i1} + ... + h_{ie}\right] \qquad (4-74)$$

يتبين أن تصحيح e خطأ في أي موضع يجب أن يكون المجموع (الجمع يكون ثنائياً) لـ e عامود من المصفوفة H لا يساوي الصفر وذلك حسب العلاقة (4–74)، وهكذا نحصل على مصححات منفصلة لكل كلمة خاطئة تحتوي على e خطأ.

يتم اختيار أعمدة المصفوفة H بحيث يكون مجموع e عامود لا يساوي مجموع e لأعمدة أخرى:

$$h_{i1} + ... + h_{ie} \neq h_{j1} + ... + h_{je} \qquad (4-75)$$

فمن أجل أي قيمة $i_1.....i_e$ منفصلة تقع بين 1 و n وقيم $j_1.....j_e$ منفصلة تقع بين 1 و n (التي يمكن أن تتساوى بعدد ما $i_1.....i_e$ وليس بالكل)

حينئذ يمكن جمع كل عناصر الأعمدة

$$h_{i1} + ... + h_{ie} + h_{j1} + ... + h_{je} \neq 0 \qquad (4-76)$$

وبإجراء عملية الترتيب :

$$h_{i1} + ... + h_{i2e} \neq 0 \qquad (4-77)$$

وذلك من أجل قيمة من $i_1....i_{2e}$ ضمن المجال $1 \to n$، نطبق على المصفوفة H المعادلة (4–75) التي تعطي إمكانية تصحيح e خطأ، كما يمكن أن نبين في هذه الحالة أن المسافة بين كلمتين تساوي إلى $2e+1$. إن المسافة بين كلمتين:

$$D(v_i, v_j) = \sum_{k=1}^{n} a_{ik} \oplus a_{jk} = \sum_{k=1}^{n} b_k \qquad (4-78)$$

حيث: $b_k = a_{ik} \oplus a_{jk}$

إن الرموز b_k التي حصلنا عليها هي رموز لكلمة ترميز تحقق العلاقة:

$$Hw^T = 0 \qquad (4-79)$$

حيث:

$$w = \lfloor b \quad b_2 \quad ..... \quad b_n \rfloor = v_i + v_j \qquad (4-80)$$

في الحقيقة:

$$Hw^T = H(v_i + v_j)^T = Hv_i^T + Hv_j^T = 0 \qquad (4-81)$$

من العلاقة (4–78) فإن المسافة بين كلمتين مرمزتين لا على التعيين تساوي إلى عدد المركبات التي تختلف عن الصفر بالنسبة لكلمة مرمزة أخرى.

يعرف وزن كلمة الترميز بعدد الرموز التي تختلف عن الصفر في الكلمة الواحدة. إذا المسافة الصغرى بين كلمتين مرمزتين يساوي إلى وزن كلمة ترميز أخرى. وتحدد المسافة الصغرى بين كلمتين مرمزتين بأقل وزن للكلمة المرمزة.

لنفترض أن w هي كلمة مرمزة تساوي إلى وزن $2e+1$، نشير إلى الكلمة:

$$w=[.... \quad \alpha_{i1} \quad .... \quad \alpha_{i2e+1} \quad ....] \qquad (4-82)$$

وبما أن w هي كلمة مرمزة، إذا لدينا العلاقة:

$$Hw^T=0 \qquad (4-83)$$

فمن أجل أي كلمة ترميز ذات وزن $2e+1$:

$$\alpha_{i1}h_1+.....+\alpha_{i2e+1}h_{i2e+1}=0 \qquad (4-84)$$

أو:

$$h_{i1}+.....+h_{i2e+1}=0 \qquad (4-85)$$

وبناء على العلاقة (4–77) فلا يمكن أن تكون العلاقة التالية محققة:

$$h_{i1}+.....+h_{i2e}=0 \qquad (4-86)$$

وبالتالي لا يوجد أي كلمة ذات وزن أقل من $2e+1$ التي هي الوزن الأصغري (المسافة الصغرى).

ولتقييم الحد الأعلى للمسافة الصغرى $D_{\min}$ سنشكل كلمة ترميز ذات وزن w بحيث الوزن الأصغري لا يتجاوز w أي $D_{\min}\le w$ ويتم إنشاء هذه الكلمة على الشكل التالي:

تلغى الكلمة المرمزة التي لها رمز وحيد من المعلومات يساوي 1 والبقية صفر ولكن الكلمة التي فيها m رمز للمراقبة ذات 1، فإن وزن هذه الكلمة هو $w=1+m$، ومن البديهي فإن الوزن الأصغري لا يمكن أن يكون أكبر من w بالرغم من أن $D_{\min}\le 1+m$، ولتصحيح e خطأ طبقا للعلاقة (4–29) لدينا

$2e < m \Leftarrow D_{\min} \geq 2e+1$ أي أنه لتصحيح e خطأ لمرمز يجب أن يكون أقل ما يمكن 2e رمز للمراقبة.

معظم الكلمات المرمزة لها عدد من رموز المراقبة أكبر من 2e.

4-3-7-2 العلاقة بين أعمدة المصفوفة H في حال كشف الأخطاء :

تكون الشروط في حال كشف الأخطاء أكثر مرونة مما هو عليه في حال تصحيح الأخطاء، فالعلاقة (4-70) تصبح مختلفة عن الصفر دون أن تكون منفصلة، لنفترض أن عدد الأخطاء المراد كشفها هو d، في هذه الحالة الكلمة الخاطئة لها الشكل التالي:

$$\varepsilon = [..... \quad \alpha_{i1} \quad ..... \quad \alpha_{id} \quad .....] \qquad (4-87)$$

ومن العلاقة $H'w^T \neq 0$ حيث H' لها الأعمدة $h_1' \quad h_2' \quad .... \quad h_n'$ (نشير إليها بفتحة حتى نميزها عن الحالة السابقة) نحصل على :

$$\left[h_1' \quad h_2' \quad .... \quad h_n'\right] \cdot \begin{bmatrix} ... \\ \alpha_{i1} \\ ... \\ \alpha_{id} \\ ... \end{bmatrix} \neq 0$$

وبالتالي :

$$h'_{i1} + ... + h'_{id} \neq 0 \qquad (4-88)$$

$i_1 ..... i_d$ منفصلة بين $1 \rightarrow n$.

من العلاقة (4-88) ينتج أنه في حال كشف خطأ واحد في المصفوفة H' يجب أن تكون جميع أعمدتها مخالفة للصفر.

من العلاقة (87 −4) و (88 −4) فإن كشف $d = 2e$ خطأ يكافئ تصحيح e خطأ وبالعكس إذا كان عدد الأخطاء التي يجب كشفها عدد فردياً.

$$d = 2p + 1 \qquad p = 0,1,.... \qquad (4-89)$$

إذا مصفوفة المراقبة H' يمكن تحديدها بسهولة وذلك بناء على العلاقة (4−88) :

$$h'_{i1} + ... + h'_{i2p+1} \neq 0 \qquad (4-90)$$

تكون محققة فيما لو أخذنا صفا ذا واحدات:

$$h'_{i1} = \begin{bmatrix} h_{i1} \\ 1 \end{bmatrix}, \quad h'_{i2} = \begin{bmatrix} h_{i2} \\ 1 \end{bmatrix}, \quad ..... \qquad (4-91)$$

أي :

$$H' = \begin{bmatrix} h_1 & h_2 & ..... & h_n \\ 1 & 1 & ..... & 1 \end{bmatrix} \qquad (4-92)$$

في الحقيقة بإدخال العلاقات (90−4) و (91−4) وبناء على أن المجموع الثنائي لعدد زوجي من الرموز هو صفر نحصل على ما يلي:

$$\begin{bmatrix} h_{i1} + ... + h_{i2p} \\ 0 \end{bmatrix} + \begin{bmatrix} h_{i2p+1} \\ 1 \end{bmatrix} \neq 0 \qquad (4-93)$$

هذه العلاقة محققة من أجل أي قيمة للأعمدة $h_1, h_2, ..., h_n$ وفي الحالة الخاصة من أجل القيم المعدومة (التي تساوي الصفر)، وبالتالي إذا كان المطلوب من المرمز هو كشف الأخطاء المفردة فالمصفوفة تكتب على الشكل التالي:

$$H' = [1,1,.....,1] \qquad (4-94)$$

في هذه الحالة الكلمة المرمزة:

$$v = [a_1 \quad a_2 \quad ..... \quad a_n] \qquad (4-95)$$

تمثل الرموز التي عددها $k = n-1$ رمزا نختارها عشوائيا رموز المعلومات والرمز الأول يمثل رمز المراقبة ومحدد بالعلاقة $Hv^T = 0$ وبناء على العلاقة (4– 95) يمكن أن تكتب:

$$a_1 = a_2 + a_3 + ... + a_n \qquad (4-96)$$

وإذا استقبلنا $H'v^T \neq 0$ أي:

$$a'_1 + a'_2 + ... + a'_{n-1} + a'_n \neq 0 \qquad (4-97)$$

يمكن أن نقول أن عملية الإرسال أدخل فيها عدد فردي من الأخطاء.

لإضافة رمز مراقبة بالإضافة إلى رموز التصحيح نحصل على معلومة إضافية وهي أن عدد رموز المعلومات فردية أو زوجية.

ففي حال هذه الإضافة لهذا المرمز تصحح خطأ واحداً فإنه يقوم أيضا بكشف أخطاء مضاعفة (خطأين)، في هذه الحالة مصفوفة المراقبة هي من الشكل (4–92) وإذا تم إضافة رمز المراقبة دون التقليل من رموز المعلومات فتصبح من الشكل:

$$H' = \begin{bmatrix} 0 & h_1 & h_2 & .... & h_n \\ 1 & 1 & 1 & .... & 1 \end{bmatrix} \qquad (4-98)$$

طول كلمة الترميز في هذه الحالة $n+1$ رمز ويكون:

$$z = H''v^T = \begin{bmatrix} C_1 \\ c_2 \end{bmatrix} \qquad c_2 \in GF(2) \qquad (4-99)$$

بينما C_1' هو مصفوفة عامودية أي:

$$\begin{bmatrix} 0 & h_1 & h_2 & .... & h_n \\ 1 & 1 & 1 & .... & 1 \end{bmatrix} . \begin{bmatrix} a_0' \\ a_1' \\ ... \\ a_n' \end{bmatrix} = \begin{bmatrix} 0 + a_1'h_1 + ... + a_n'h_n \\ a_0' + a_1' + ... + a_n' \end{bmatrix} \qquad (4-100)$$

لنعد المصفوفة العامودية $h_1, h_2, ..., h_n$ من المصفوفة H تحقق الشروط الضرورية لتصحيح خطأ ونعد فيما يلي الحالات التالية:

- $C_1 = 0$ و $c_2 = 0$ حيث C_1 المصفوفة العامودية من m عنصر، في هذه الحالة فإنه لا يوجد أي خطأ.
- $C_1 \neq 0$ و $c_2 = 1$ نستنتج أنه يوجد خطأ يمكن تصحيحه.
- $C_1 = 0$ و $c_2 = 1$ نستنتج أن الرمز a_0' خطأ.
- $C_1 \neq 0$ و $c_2 = 0$ نستنتج أنه يوجد خطآن لا يمكن تصحيحهما.

4-3-8 ترميز المجموعة بالاعتماد على المصفوفة المولدة G :

تعرف المصفوفة المولدة بأنها تحقق العلاقة التالية:

$$v = iG \qquad (4-101)$$

ولبيان العلاقة بين المصفوفة H والمصفوفة G نبدل v من العلاقة $Hv^T = 0$ فنحصل على:

$$H(iG)^T = HG^T i^T = 0 \qquad (4-102)$$

وبما أن هذه العلاقة محققة لجميع رموز المعلومات بالتالي:

$$HG^T = 0 \qquad (4-103)$$

وطبقاً للعلاقة (4–57) :

$$H = [I_m \quad Q] \qquad (4-104)$$

حيث Q مصفوفة من m صف و k عامود وذلك من العلاقة (4–58)

نلاحظ أن G هي من الشكل:

$$G = [Q^T I_k] \qquad (4-105)$$

تكون العلاقة (4–103) محققة:

$$HG^T = [I_m \quad Q]\begin{bmatrix} Q \\ I_k \end{bmatrix} = [Q + Q] = 0 \qquad (4-106)$$

نشير إلى المصفوفة Q^T بالمصفوفة p :

$$p = Q^T \qquad (4-107)$$

حيث:

k = P صف، m عامود.

m = Q صف، k عامود.

$$p = \begin{bmatrix} p_{11} & p_{12} & .... & p_{1m} \\ p_{21} & p_{22} & .... & p_{2m} \\ .... & .... & .... & .... \\ p_{k1} & p_{k2} & .... & p_{km} \end{bmatrix} \qquad (4-108)$$

أي:

$$G = [P \quad I_k] \tag{4-109}$$

$$G = \begin{bmatrix} p_{11} & .... & p_{1m} & 1 & 0 & .... & 0 \\ .... & .... & .... & 0 & 1 & .... & 0 \\ .... & .... & .... & .... & .... & .... & .... \\ p_{k1} & .... & p_{km} & 0 & 0 & .... & 1 \end{bmatrix} \tag{4-110}$$

وطبقاً للعلاقات (4–61–a) و (4–101) و (4–109) :

$$v = [c \quad i] = i[p \quad I_k] = [ip \quad \text{i}] \tag{4-111}$$

حيث ينتج:

$$c = ip \tag{4-112}$$

وهي العلاقة التي تعطينا رموز المراقبة بدلالة رموز المعلومات وبناء على العلاقة (4–112) لدينا:

$$c = [a_{m+1} \quad a_{m+2} \quad .... \quad a_{m+k}] \begin{bmatrix} p_{11} & p_{12} & .... & p_{1m} \\ p_{21} & p_{22} & .... & p_{2m} \\ .... & .... & .... & .... \\ p_{k1} & p_{k2} & .... & p_{km} \end{bmatrix} \tag{4-113}$$

رموز المراقبة:

$$a_j = \sum_{i=1}^{k} a_{m+1} p_{i,j} \qquad a_{ij} \le m \qquad (4\text{-}114)$$

يسمى الترميز الذي حصلنا عليه بالترميز الازدواجي (dual) للترميز الذي تم الحصول عليه من H.

4-3-9 تشكيل المصححات:

يكون المصحح المعطى بالعلاقة $Hv'^T = z^T$ على الشكل:

$$z^T = v'H^T \qquad (4\text{-}115)$$

أو:

$$z^T = [c' \quad i'][I_m \quad p^T]^T \qquad (4\text{-}116)$$

حيث:

c' مصفوفة رموز المراقبة المستقبلة.

i' مصفوفة رموز المعلومات المستقبلة.

عند عملية النقل

$$z^T = [c' \quad i'] \cdot \begin{bmatrix} I_m \\ p \end{bmatrix} = [c' + i'p] \qquad (4\text{-}117)$$

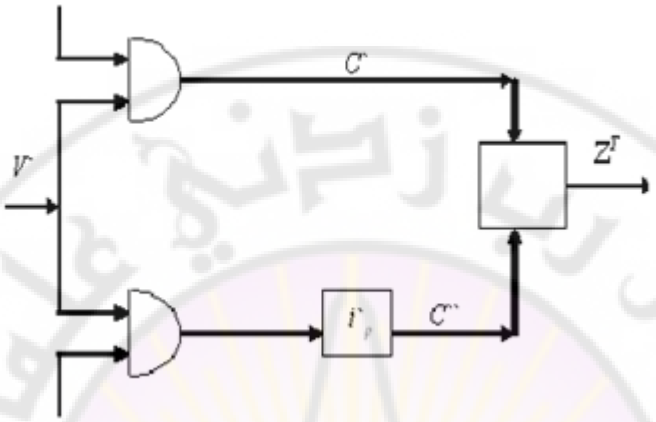
وطبقا للعلاقة (4-112) ندخل العلاقة التالية:

$$c'' = i'p \qquad (4\text{-}118)$$

التي تمثل رموز المراقبة الناتجة عن عملية الترميز لرموز العمليات المستقبلة، ومن المعادلات السابقة:

$$z^T = [c' + c''] \qquad (4\text{-}119)$$

يتم إنجاز هذه المعادلة كما في الشكل. من خلال هذه الطريقة نشكل المصححات، وبإدخال عملية الضرب الضرورية نطبق العلاقة (4-115).



الشكل (4-5) تحديد المصححات

4-3-10 ترميز هامينغ الزمري المصحح لخطأ واحد :

إن تصحيح خطأ واحد في كلمة يجب أن يكون عدد المصححات 2^m أكبر أو يساوي $n+1$ على اعتبار أن طول الكلمة يساوي n رمز بالإضافة إلى عدم وجود أي خطأ:

$$2^m \geq n+1 \qquad (4\text{-}120)$$

أو

$$2^m \geq k+m+1 \qquad (4\text{-}121)$$

وهي العلاقة التي تحدد عدد رموز المراقبة عندما يعطى عدد k من رموز المعلومات في حالة تصحيح خطأ.

يتكون ترميز هامينغ من مصفوفة مراقبة H، يمثل العامود h_i ثنائيا العدد i.

$$H = \begin{bmatrix} 0 & 0 & .... & .... & .... & 1 \\ .... & .... & .... & .... & .... & 1 \\ .... & .... & .... & .... & .... & .... \\ .... & .... & .... & .... & .... & .... \\ 0 & 0 & 0 & .... & .... & .... \\ 0 & 1 & 1 & .... & 1 & .... \\ 1 & 0 & 1 & .... & 0 & 1 \end{bmatrix} \qquad (4\text{-}122)$$

حيث: $\forall i \neq j \quad h_i + h_j \neq 0$ (من شروط تصحيح خطأ واحد)

تمثل الكلمة الخاطئة بخطأ واحد:

$$\varepsilon = [.... \quad \alpha_i \quad ....] \qquad (4\text{-}123)$$

إذا أرسلت v_j نستقبل:

$$v'_j = v_j + \varepsilon \qquad (4\text{-}124)$$

ويكون المصحح المقابل:

$$z = Hv'^{T}_j = H\varepsilon^T \qquad (4\text{-}125)$$

أو

$$z = [h_1 \quad h_2 \quad .... \quad h_n] \cdot \begin{bmatrix} ... \\ \alpha_i \\ ... \end{bmatrix} = h_i \qquad (4\text{-}126)$$

أي أن المصحح ممثل ثنائيا بالعدد I الذي يشير إلى المكان الذي يوجد فيه خطأ، وهذا يجعل كاشف الترميز بسيطاً ونحتاج فيه إلى مبدل من ثنائي إلى عشري.

يصحح ترميز هامينغ جميع الأخطاء البسيطة ولا يمكن أن يصحح أخطاء مضاعفة ونقول عنه إنه مرمز كامل، حيث أن الترميز الذي يمكن أن يصحح e

خطأ في أي مكان ولكن لا يمكن أن يصحح أي شكل من $e+1$ خطأ أو أكثر يسمى المرمز الكامل.

في حالة الرموز الكاملة عدد المصححات مساو إلى عدد الكلمات الخاطئة المشكلة من e خطأ أو أقل.

التراميز الكاملة هي تراميز مكافئة.

4-3-10-1 مرمز هامينغ:

لتبسيط الحساب نختار m رمز مراقبة بحيث تلائم الأعمدة h_i وبمركبة تختلف عن الصفر، هذه الأماكن $2^0,2^1,2^2,.....,2^{m-1}$ تشير إلى رموز المراقبة c_i والمعلومات i_i ولذلك يكتب الشعاع المرمز على الشكل:

$$v=[c_1 \quad c_2 \quad i_3 \quad c_4 \quad i_5 \quad .... \quad i_n] \qquad (4-127)$$

ونتيجة توضع رموز المراقبة ينتج من ذلك أن هذا المرمز غير نظامي وتعطى رموز المراقبة من العلاقة:

$$Hv^T=0$$

$$[h_1 \quad h_2 \quad .... \quad h_n]\cdot\begin{bmatrix} c_1 \\ c_2 \\ i_3 \\ ... \\ i_n \end{bmatrix}=0 \qquad (4-128)$$

أو

$$c_1\begin{bmatrix}0\\...\\...\\1\end{bmatrix}+c_2\begin{bmatrix}0\\...\\1\\0\end{bmatrix}+i_3\begin{bmatrix}0\\...\\1\\1\end{bmatrix}+.....+i_n\begin{bmatrix}1\\...\\...\\1\end{bmatrix}=0 \qquad (4-129)$$

وتكون العلاقة المكافئة مكونة من m معادلة حيث الرموز $c_1, c_2, \ldots\ldots$ لا تعاد أكثر من مرة ويعبر عن رموز المراقبة بناء على رموز المعلومات، بدأ من آخر خط يمكن أن نكتب:

$$\begin{aligned} c_1 &= i_3 + i_5 + \ldots\ldots + i_n \\ c_2 &= i_3 + i_6 + \ldots\ldots + i_n \\ c_4 &= i_5 + i_6 + \ldots\ldots + i_n \\ &\ldots\ldots\ldots \\ c_m &= \ldots\ldots\ldots \end{aligned} \qquad (4\text{-}130)$$

4-3-10-2 كاشف ترميز هامينغ:

في الاستقبال فإن الكلمة المرمزة تطبق على خلية ثنائية في الذاكرة بعد ذلك نحسب المصحح:

$$z = H' v^T = \begin{bmatrix} e_1 \\ \ldots \\ e_m \end{bmatrix} = \begin{bmatrix} h_1 & \ldots\ldots & h_n \end{bmatrix} \cdot \begin{bmatrix} c_1' \\ c_2' \\ \ldots \\ i_n' \end{bmatrix} \qquad (4\text{-}131)$$

وبناء على بنية المصفوفة H تتم عملية حساب:

$$\begin{aligned} e_m &= c_1' + i_3' + i_5' + \ldots\ldots + i_n' \\ e_{m-1} &= c_2' + i_3' + i_6' + \ldots\ldots + i_n' \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ e_1 &= \ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \qquad (4\text{-}132).$$

العدد الثنائي يتم حسابه $(e_1 \quad e_2 \quad \ldots\ldots \quad e_m)$ ضمن كاشف الترميز (ضمن مبدل ثنائي عشري) على الخرج نحصل على إشارة تشير إلى أماكن الأخطاء تساعدنا على عملية التصحيح.

مثال :

ليكن لدينا k=4 رموز المعلومات:

حدد رموز المراقبة ورموز الكلمة ثم بين عملية الترميز وكاشف الترميز.

الحل:

من العلاقة $2^m \geq k + m + 1$ ينتج أن m=3 وبالتالي n=3+4=7

وتكون المصفوفة H

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

والكلمة المرمزة :

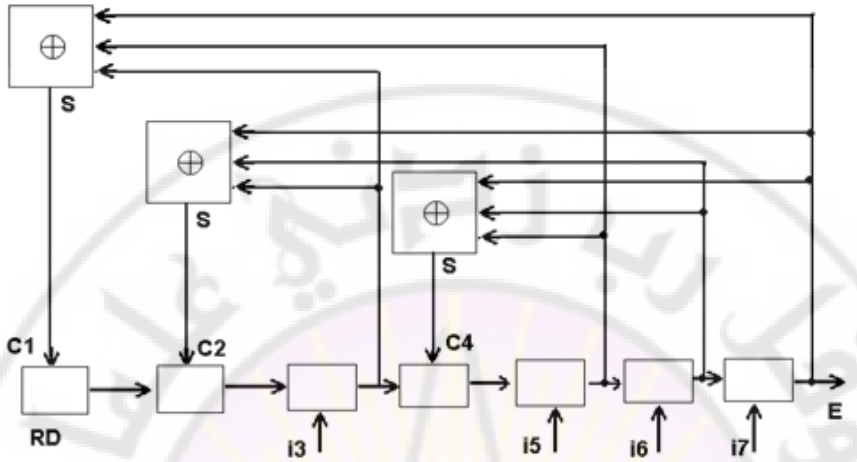
$$V =[C_1,C_2,i_3,C_4,i_5,i_6,i_7]$$

ويتم تحديد رموز المراقبة من المصفوفة (من رموز المعلومات)

$$C_1 = i_3 + i_5 + i_7$$

$$C_2 = i_3 + i_6 + i_7$$

$$C_4 = i_5 + i_6 + i_7$$



مرمز هامينغ

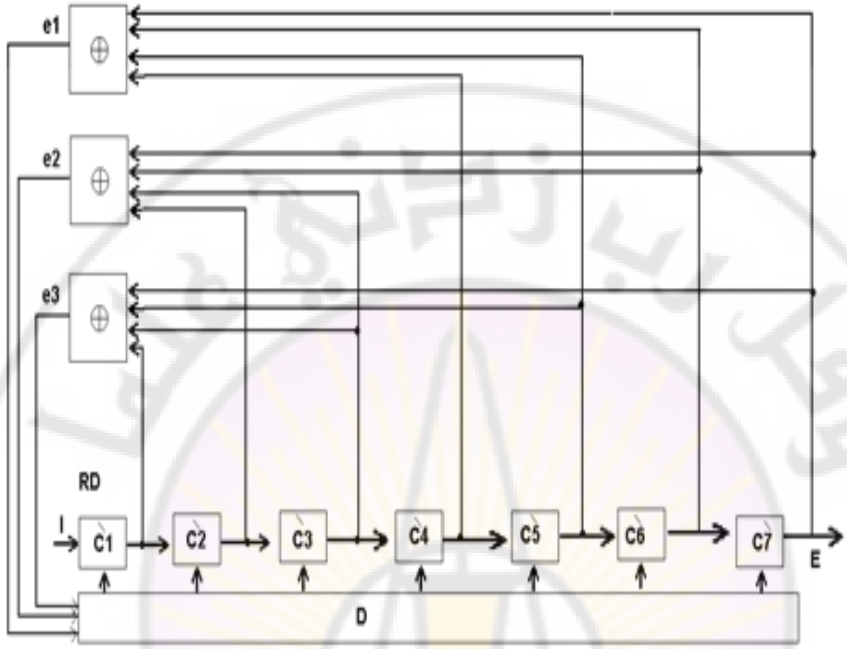
ويـتم إنجـاز عمليـة الترميـز بواسـطة مسـجل إزاحـة RD وتحسـب رمـوز التصـحيح مـن عمليـات الجمـع ذات النمـوذج الثنـائي. بعـد تشـكيل الكلمـة المرمـزة يتم قطـع الدخل إلـى المسـجل ويبدأ تفريـغ محتوى المسـجل علـى الخرج علـى شكل متوالية من النبضات (و ذلك بتزامن من نبضات الساعة بحيث في النهاية نحصل على كلمة الترميز).

أمـا عمليـة كاشـف الترميـز (فـي الاسـتقبال) فيـتم حسـاب المصـححات علـى الشكل التالي:

$$e_1 = c`_4 + i`_3 + i`_6 + i`_2$$

$$e_2 = c`_2 + i`_3 + i`_6 + i`_7$$

ويتم إدخال المصححات (e_1 , e_2 ,e_3) بإدخال كاشف الترميز Δ الذي يعطي إشارة التصحيح للأخطاء في الخلية التي يكون فيها عدد الترتيب ممثلاً ثنائيا (e_1 ,e_2 ,e_3) .



دارة كشف الترميز

يتم فصل رموز المعلومات بدارة البوابة الموضوعة على الخرج التي توصل في اللحظات رموز المعلومات التي تظهر على الخرج(المرمز غير النظامي في هذه العملية , تعقد تجهيزات كاشف الترميز).

مسائل الفصل الرابع

المسألة (1) :

لتكن مصفوفة المراقبة

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

أ- بين من خلال تحويل عناصر هذه المصفوفة أنه يمكن أن تصبح من الشكل $H' = [\ I_3\ Q\ ]$.

ب- أثبت أنه من خلال عمليات التحويل هذه بأن خواص الكشف و التصحيح تبقى كما هي.

ج – حدد رموز المراقبة بدلالة رموز المعلومات في كل من الحالتين H' ., H

المسألة (2):

حدد من المصفوفة H من المسألة (1) المصفوفة $G = |\ PI_K|$، و من ثم إنجاز عملية الترميز باستخدام المصفوفة G .

المسألة (3):

لتكن لدينا المصفوفة H لمرمز هامينغ n =7، m =3, K= 4 تتم إضافة صف واحد لهذه المصفوفة كما في المعادلة (98 – 4). و المطلوب:

احسب المصحح في كل من الحالات التالية :

أ. $a_2' = a_2 + 1$

ب. $a_0' = a_0 + 1$

ت. $a_3' = a_3 + 1$, $a_4' = a_4 + 1$

ثم اتخذ القرار بدلالة قيم هذه المصححات

المسألة (4):

حدد عدد العمليات الحسابية الضرورية لحساب المصحح Z في حالة استعمال العلاقة.

$$Z^T = V' H^T$$

أو العلاقة

$$Z^T = [C' + C'']$$

المسألة (5):

ليكن ترميز هامينغ المصحح لخطأ واحد $n = 7$. أحد رموز المعلومات الأربع يتحول إلى رمز مراقبة وذلك لكشف أخطاء مضاعفة. حدد الكلمات التي لها معنى في هذا المرمز.

المسألة (6):

لنعد الترميز $n=6$, $k=3$ ومصفوفة المراقبة

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

أ- بين إذا كان الترميز كاملاً أم لا.

ب- ما هو القرار الذي تم اتخاذه فيما لو كانت قيم المصححات في كلا من الحالات التالية:

$$Z^T = 010 \quad , \quad Z^T = 111$$

المسألة(7):

لنفترض مرمز زمري مصحح لخطأ واحد (تام) و ترميز تكراري قادر على تصحيح خطأ واحد.

قارن بين كلا المرمزين من حيث معدل المعلومات k/n.

وقل رب زدني علما
جامعة دمشق
Damascus University

الفصل الخامس

الترميز الدوري cyclic coding

وقل رب زدني علما
جامعة دمشق
Damascus University

الفصل الخامس

الترميز الدوري cyclic coding

5-1 مقدمة

هي جزء من الترميز الكتلي تتشكل الكلمة من كثير حدود من الدرجة $n-1$ أمثاله رموز لهذه الكلمة عددها n.

$$v(x) = a_0 + a_1 x + ...a_{n-1} x^{n-1} \qquad (5-1)$$

كما في الترميز الزمري فإن رموز الكلمة تمثل على شكل مصفوفة خطية (صف) من أمثال كثير الحدود $v(x)$.

$$v = [a_0 \quad a_1 ..... \quad a_{n-1}] \qquad (5-2)$$

من خواص الترميز الدوري أنه إذا كان v كلمة لها معنى فإن أي عملية نقل دورية للرموز يبقى للكلمة معنى

$$[a_i \quad a_{i+1} ..... \quad a_{n-1} \quad a_0 \quad a_{i-1}]$$

تشكل مجموعة الكلمات الكلية بما يسمى (الجبر), و مجموعة الكلمات التي لها معنى بـ (المثالي) ideal

مجموعة عناصر A التي تحقق شروط الفراغ الشعاعي و داخلية بالنسبة لعملية ضرب عنصرين تسمى هذه بالجبر.....

مجموعة العناصر I التي فيها عمليات الجبر (الضرب و الجمع) و عكس الجمع تسمى المثالي.

1. I_1 هي زمرة جزئية من I

2. فمـــن أجـــل $\forall x \in I_1, \forall y \in I_1$ فـــإن

$$X \cdot Y = Y \cdot X \in I_1$$

2-5 توليد الكلمات

تتمثل مجموعة الكلمات التي لها معنى و من دون معنى بفئات الباقي من نموذج كثير الحدود $P(x)$ من الدرجة n وأمثاله في حقل غالواس $GF(2) \in \{0,1\}$.

تعد الحلقة هي جميع كثيرات الحدود وفي هذه الحلقة يعد ideal مشكلاً من مضاعفات كثير الحدود $P(x)$ من الدرجة n.

تشكل فئات الباقي من خلال تقنية الترميز الزمري، فالفئة الأولى هي ideal المشكل من $P(x)$

$$\begin{array}{llll} 0 & P(x) & xP(x) & (1+x)P(x)\ldots\ldots\ldots \text{ multipl P(x)} \\ 1 & 1+P(x) & 1+xP(x) & 1+(1+x)P(x)\ldots\ldots\ldots\ldots\ldots 1+multipl \text{ P(x)} \\ x & x+P(x) & x+xP(x) & x+(1+x)P(x)\ldots\ldots x+multipli\ P(x) \\ 1+x & 1+x+P(x) & 1+x+xP(x) & 1+x+(1+x)P(x)\ldots\ldots\ldots multipl \text{ P(x)} \\ a_0+a_1x+\ldots+a_{n-1}x^{n-1} & \ldots\ldots\ldots\ldots & 1+x+\ldots\ldots x^{n-1}+multiple \text{ P(x)} & \end{array} \quad (5-3)$$

تشكل فئات الباقي للنموذج $P(x)$ بما يسمى الجبر.

وبما أننا نتحدث عن فئات الباقي ندخل المعادلات التالية:

$$a_0 + a_1 x + \ldots\ldots\ldots\ldots + a_{n-1}x^{n-1}$$

أو

$$a_0 + a_1 X + \ldots\ldots\ldots\ldots + a_{n-1}X^{n-1}$$

حيث يتم إبدال x بـ X حتى لا يتم التباس بين كثير الحدود و فئات الباقي سنشير بـ x بدلاً من X.

نعد فيما يلي مجموعة الكلمات التي تشكل الجبر المولد من كثير الحدود $P(x)$ من الدرجة n يمكن اختيار كثير الحدود $P(x)$ عشوائياً. وللحصول على نتائج مشابهة للترميز الزمري بحيث الجداء $u(X)\cdot v(X)=0$ حيث $u(X)\cdot v(X)$ وتكون عناصر الجبر من النموذج $P(x)$ يتم شرحها على شكل جداء سلمي $\langle u\cdot v\rangle = 0$ ويتم هذا باختيار

$$P(x)=x^n+1$$

مثال :

$$P(X)=x^3+1$$
$$u(X)=a_0+a_1X+a_2X^2$$
$$v(X)=b_0+b_1X+b_2X^2$$
$$u(X)\cdot v(X)=a_0b_0+(a_0b_1+a_1b_0)X+(a_0b_2+a_1b_1+a_2b_0)X^2+(a_1b_2+a_2b_1)X^3+a_2b_2X^4$$

معطى بكثير الحدود نجد أن أول فئة الباقي

$$P(X)=X^3+1=0 \qquad X^3=1 \qquad X^4=X$$

بالتبديل نحصل على:

$$u(x)\cdot v(x)=a_0b_0+a_1b_2+a_2b_1+(a_0b_1+a_1b_0+a_2b_2)X+(a_0b_2+a_1b_1+a_2b_0)X^2$$

فإذا كان:

$$u(X)\cdot v(X)=0$$

يكون

$$\begin{aligned} a_2b_2+\ a_1b_1+\ a_0b_0&=\ 0\\ a_2b_1+\ a_1b_0+\ a_0b_2&=\ 0\\ a_2b_0+\ a_1b_2+\ a_0b_1&=\ 0 \end{aligned} \qquad (5-4)$$

نلاحظ أن المعادلة الأولى هي ناتج الجداء السلمي $\langle u \cdot v \rangle = 0$ حيث أن مركبات الشعاع مكتوبة بشكل عكسي، وبشكل عام أي نقل دوري للأمثال يعطي جداء سلمياً مساوياً للصفر.

5-3 توصيف الكلمات ذات المعنى

نشكل مجموعة فئات الباقي من النموذج $P(x) = x^n + 1$ فيكون عدد عناصر (الكلمات) لهذه المجموعة 2^n نختار منها 2^k كلمة لها معنى (عنصر له معنى)، وهي ناتجة عن كثير حدود مولد $g(x)$ (ideal) من الدرجة m أو بنموذج مكافئ عناصر من الفراغ صفر لل ideal المولد من كثير الحدود $h(x)$ من الدرجة k، وبما أن العنصر "0" هو جزء من ideal ينتج من ذلك أنه يوجد كثير حدود $h(x)$ بحيث:

$$g(x) \cdot h(x) = 0 = P(x) \qquad (5-5)$$

من هذه العلاقة ينتج أن كثير الحدود و هو مقسم $P(x)$

$$g(x) = \frac{P(x)}{h(x)} = \frac{x^n + 1}{h(x)} \qquad (5-6)$$

مما سبق فإن الكلمات المرمزة يمكن أن توصف بطريقتين:

5-2 -1 الكلمات المرمزة عبارة عن عناصر ideal مولدة من كثير الحدود $g(x)$ من الدرجة m:

في هذه الحالة $v(X)$ عبارة عن مضاعف لـ $g(x)$

$$v(X) = q(X) \cdot g(X) \qquad (5-7)$$

حيث $q(X)$ كثير حدود من الدرجة $k-1$.

يشار إلى كثير الحدود المولد

$$g(x) = g_0 + g_1\alpha + \ldots\ldots g_{m-1}x^{m-1} + x^m \qquad (5-8)$$

من الواضح فإنه لا بد من أن يكون من الدرجة m على اعتبار $g_m = 1$ فإذاً:

$$q(x) = i(x) \qquad (5-9)$$

حيث i(x) هو كثير حدود لرموز المعلومات

$$i(x) = a_m + a_{m+1}x + \ldots\ldots\ldots + a_{m+k-1}x^{k-1} \qquad (5-10)$$

تعطينا العلاقة (5-7) عملية الترميز ولكنه ليس ترميزاً نظامياً وللحصول على ترميز نظامي نجري العملية التالية:

ليكن $c(x)$ كثير حدود لرموز التحكم

$$c(x) = a_0 + a_1x + \ldots\ldots\ldots + a_{m-1}x^{m-1} \qquad (5-11)$$

وتصبح عملية الترميز للكلمة المرمزة

$$v(x) = c(x) + x^m i(x) = q(x)\cdot g(x) \qquad (5-12)$$

حيث:

$$x^m i(x) = q(x)\cdot g(x) + c(x) \qquad (5-13)$$

وبما أن درجة $c(x) < m$ ودرجة $g(x) = m$ يمكن أن نكتب

$$c(x) = rest\,\frac{x^m i(x)}{g(x)} \qquad (5-14)$$

أي أن كثير الحدود لرموز المراقبة يستخرج من تقسيم كثير الحدود للمعلومات مضروباً بـ x^m على كثير الحدود $g(x)$، في هذه الحالة فإن $v(x)$ هي كلمة الترميز من ترميز نظامي و بما أن:

$$v(x) = q(x)\cdot g(x) \qquad (5-15)$$

$$q(x) = q_0 + q_1x + q_2x^2 + \ldots\ldots\ldots + q_{k-1}x^{k-1} \qquad (5-16)$$

ويمكن كتابة $v(X)$:

$$v(x) = q_0 g(x) + q_1 x g(x) + ... + q_{k-1} x^{k-1} g(x)$$

بمعنى آخر فإن $v(x)$ ستكون في صف المصفوفة

$$G = \begin{bmatrix} g(X) \\ Xg(X) \\ : \\ X^{k-1} g(X) \end{bmatrix} \qquad (5-17)$$

حيث أن صف المصفوفة مشكل من مجموعة المكونات الخطية لأشعة الصف للمصفوفة وطبقاً للعلاقة (5-8) يمكن كتابة:

$$G = \begin{bmatrix} g(X) \\ Xg(X) \\ : \\ X^{k-1} g(X) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & ... & g_m & 0 & ... & 0 \\ 0 & g_0 & ... & ... & g_m & ... & 0 \\ : & ... & ... & ... & ... & ... & ... \\ : & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & g_0 & g_1 & ... & g_m \end{bmatrix} \qquad (5-18)$$

حيث أن عناصر الصف هي أمثال كثير الحدود من الدرجة $n-1$ ($v(x)$ هي من الدرجة $n-1$) ولكن أمثال القوى لـ x غير موجودة تم تبديلها بصفر

تسمى المصفوفة G بالمصفوفة المولدة لها k صف و n عمود ويمكن باستخدامها إجراء عملية الترميز طبقاً للعلاقة (4-101).

$$v = i \cdot G$$

وهي مكافئة للعلاقة (5-15) حيث يمكن استخراج رموز التحكم منهما معاً.

5 – 2 – 2 الكلمات المرمزة كعناصر في الفراغ صفر للمثالي ideal المولد من $h(x)$ من الدرجة k :

لنبدأ من العلاقة (5-15) و بضربها ب $h(x)$

$$h(x) = h_0 + h_1 x + ...h_k x^k \qquad (5\text{-}19)$$

$$v(x).h(x) = q(x).g(x)h(x) \qquad (5\text{-}20\text{-a})$$

وبما أن كثيرات الحدود هي عبارة عن فئات الباقي ومن العلاقة (5−5)

$$v(x).h(x) = q(x).g(x)h(x) = q(x)(x^n + 1) \qquad (5\text{-}20\text{-b})$$

أي أن :

$$v(x)\cdot h(x) = 0 \qquad (5\text{-}21)$$

تشير هذه العلاقة إلى أن $v(x)$ هي موجودة في الفراغ الصفي ideal المولد من $h(x)$ الناتج $v(x)\cdot h(x)$ ، ومن خلال تعميم العلاقة (5−4) يمكن كتابة الجداء السلمي لمركبات الشعاع $h(x)$ مكتوبة بترتيب عكسي:

$$\begin{aligned}
&\langle (a_0 \quad a_1 \quad a_{n-1}), (0 \quad ... \quad 0 \quad h_k \quad h_{k-1} \quad ... \quad h_0) \rangle = 0 \\
&\langle (a_0 \quad a_1 \quad a_{n-1}), (0 \quad ... \quad h_k \quad h_{k-1} \quad ... \quad h_0 \quad 0) \rangle = 0 \\
&..... \qquad (5\text{-}22) \\
&..... \\
&\langle (a_0 \quad a_1 \quad a_{n-1}), (h_k \quad h_{k-1} \quad ... \quad h_0 \quad 0 \quad ... \quad 0) \rangle = 0
\end{aligned}$$

باقي المعادلات ليست مهمة , يوجد من عملية النقل فقط $n-k=m$ معادلة مستقلة من n معادلة.

تسمح المعادلات في العلاقة (5−22) لنا بتحديد رموز المراقبة بدلالة رموز العمليات وذلك على الشكل التالي:

$$\begin{bmatrix} 0 & ... & 0 & h_k & h_{k-1} & ... & ... & h_0 \\ 0 & ... & h_k & ... & ... & ... & h_0 & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... \\ h_k & ... & h_0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ : \\ a_{n-1} \end{bmatrix} = 0 \qquad (5\text{-}23)$$

$$H=\begin{bmatrix} 0\ 0 & \dots & h_k & \dots & h_0 \\ 0\dots & h_k & \dots & h_0 & 0 \\ \dots\dots & \dots & \dots & \dots & \dots \\ h_k\dots & h_0 & & \dots & 0 \end{bmatrix} \qquad (5-24)$$

$$H.v^T = 0 \qquad (5-25)$$

إذاً المصفوفة H المعطاة في العلاقة (5–24) هي مصفوفة التحكم و العلاقة (5–25) مكافئة للعلاقة (5–21) ومن العلاقة (5–5) والعلاقة (5–18) والعلاقة (5–24) يمكن أن نبين

$$GH^T = HG^T = 0 \qquad (5-26)$$

5 – 3 كاشف الترميز:

تقوم مشكلة كاشف الترميز بإيجاد التقابل بين الكلمة الخطأ المستقبلة $v'(x)$ والكلمة $\varepsilon(x)$ التي تمثل نوعية الخطأ في هذه الكلمة الناتج عن القناة

$$v'(x)=v(x)+\varepsilon(x) \qquad (5-27)$$

فإذا استقبلنا $v'(x)$ يمكن حساب $\varepsilon(x)$, حينئذ تنجز عملية التصحيح من خلال الجمع ذي النموذج الثنائي

$$v(x)=v'(x)+\varepsilon(x) \qquad (5-28)$$

من العلاقة (113–4) نحصل على المصحح من خلال جمع رموز المراقبة المستقبلة $c'(x)$ مع رموز المراقبة الناتجة من عملية الترميز للمعلومات المستقبلة:

$$C''(x)=rest\frac{x^m i'(x)}{g(x)} \qquad (5-29)$$

$$Z(x)=c'(x)+c''(x) \qquad (5-30)$$

$$Z(x)=c'(x)+rest\frac{\alpha^m i'(x)}{g(x)} \qquad (5-31)$$

كثير الحدود $c'(x)$ له درجة أقل من m إذاً يمكن الكتابة

$$Z(x) = rest\frac{c'(x) + x^m i'(x)}{g(x)} \qquad (5-32)$$

$$Z(x) = rest\frac{v'(x)}{g(x)} \qquad (5-33)$$

ومن العلاقة (5−27) :

$$Z(x) = rest\frac{\varepsilon(x)}{g(x)} \qquad (5-34)$$

يعد كثير الحدود $Z(x)$ أكبر درجة له $m-1$ وبالتالي عدد هذه المصححات 2^m (m عدد حدوده) و من مجموعة تشكيلة الأخطاء ينتج أن كثير الحدود $\varepsilon(x)$ ذو 2^n تشكيلة, فقط هناك عدد يقابل عدد المصححات $Z(x)$ وهو 2^m تشكيلة أخطاء يمكن تصحيحها.

وتكون العلاقة (5−34) مكافئة للعلاقة:

$$Z = H\varepsilon^T \qquad (5-35)$$

حيث ε هو مصفوفة (صف) متمثلة بأمثال $\varepsilon = (x)$ والمصفوفة H هي من الشكل $H = [I_m\ Q]$

ودرجة (ترتيب) الأعمدة لـ Q يتم اختياره بحيث

$$Z = rest\frac{\varepsilon(x)}{g(x)} = H\varepsilon^T \qquad (5-36)$$

5– 3 – 1 كاشف الترميز على أساس جدول الفئات الباقية :

أول فئة مكونة منideal المولد ويكون أول عامود من كثيرات الحدود التي تعد الكلمات الخاطئة وبالتالي يتم حجز عامود للمصححات التي تحسب من العلاقة (5–34) أو(5–35)

يلاحظ من الجدول (5 – 1) أنه لجميع الكلمات من فئة الباقي في صف واحد لها نفس المصحح نفسه بحيث أن أي فئة يكون أول عنصر ε_j لكل كلمة من هذه الفئة المصحح.

$$Z(x) = rest\frac{v'(x)}{g(x)} = rest\frac{\varepsilon_j(x) + v_k(x)}{g(x)} \qquad ;k = T,s$$

أي

$$Z(x) = Z_j(x) = rest\frac{\varepsilon_j(x)}{g(x)} \qquad (5-36)$$

ينتج من ذلك أن عملية كاشف الترميز تتم على الشكل التالي:

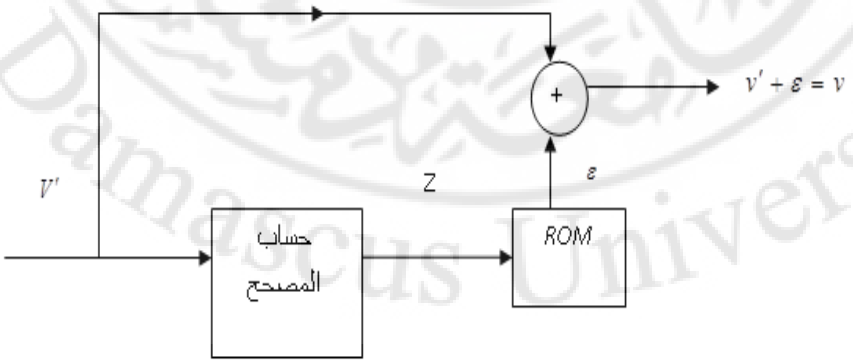
- يتم حساب المصحح لكل كلمة مستقبلة $z(x) = rest\frac{v'(x)}{g(x)}$ أو $Z = Hv'^{T}$.
- نلاحظ أن كلمة الخطأ من جدول فئات الباقي تقابل ε يقابلها مصحح.
- يتم جمع εمع V' لنحصل على V.

المصححات Z(X)	الكلمات المستقبلة		
		الكلمة الخاطئة	
	$v_1(x)$ ..... $v_5(x)$	0	كلمة ذات معنى
$Z_1 = rest\frac{\varepsilon_1(x)}{g(x)} = H{\varepsilon_1}^T$	ε_1+v_1 ..... ε_1+v_5	$\varepsilon_1(x)$	كلمة بدون معنى
$Z_2 = rest\frac{\varepsilon_2(x)}{g(x)} = H{\varepsilon_2}^T$	ε_2+v_1 ..... ε_2+v_5	$\varepsilon_2(x)$	

الجدول (5 – 1)

تعد عملية كشف الترميز هذه صحيحة فقط إذا كان لكل كلمة خاطئة مصحح ومع ذلك يمكن إجراء عملية الكشف من دون تصحيح الخطأ في الشكل(5–1) نبين المخطط العام لكاشف الترميز حيث الذاكرة التي يتم عنونتها عن طريق المصحح نقوم بإدخال الكلمات الخاطئة بالتقابل مع كل مصحح

لم يتم حتى الآن وضع الشروط لكثير الحدود g(x) حتى يكون قادراً على تصحيح كافة الأخطاء التي تحدث وهذه المشكلة سيتم علاجها لاحقاً



الشكل (5–1) طريقة الترميز على أساس فئات الباقي

5 – 4 إنجاز عملية الترميز وكشف الترميز لكشف الأخطاء وذلك من خلال دارات الضرب و التقسيم:

لقد بينا سابقاً أن عملية الترميز تنجز بطريقتين:

1. من خلال الضرب

$$v(x) = i(x)g(x) \qquad (5-37)$$

حيث نحصل على ترميز غير نظامي وعملية كشف الترميز تتم بإجراء عملية التقسيم

$$z(x) = rest\frac{v'(x)}{g(x)} \qquad (5-38)$$

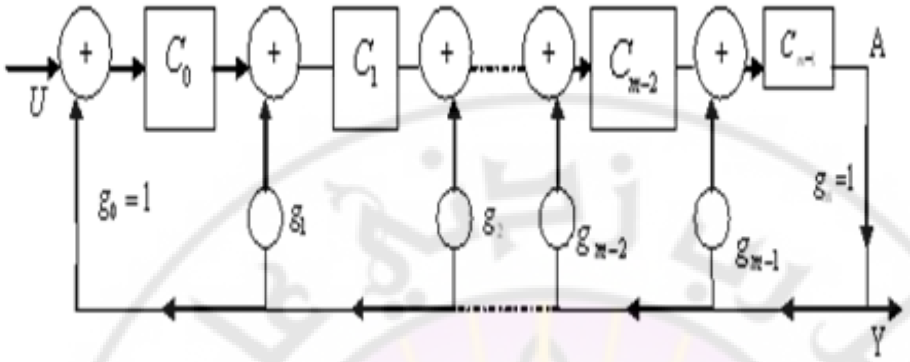
2. من خلال التقسيم

$$v(x) = rest\frac{x^m i(x)}{g(x)} + x^m i(x) \qquad (5-39)$$

هنا يتم الحصول على ترميز نظامي و تتم عملية الكشف بإجراء عملية التقسيم كما في العلاقة (5–38) يوجد للترميز النظامي ميزات بالمقارنة مع الترميز غير النظامي.

5 – 4 – 1 دارات التقسيم :

ليكن مسجل الإزاحة في الشكل(5–2):



الشكل (5−2) دارة التقسيم على g(x)

نستعمل خلايا ثنائية نشير إليها C_i ودارات الضرب بثوابت $g_i \in GF(2)$ وجوامع من النوع الثنائي نطبق على دخل دارة التقسيم كثير الحدود على التسلسل

$$V(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \qquad (5-40)$$

ومن أجل كثير الحدود

$$g(x) = g_m x^m + g_{m-1}x^{m-1} + ... + g_0 \qquad (5-41)$$

يتم تخزين باقي عملية التقسيم ضمن خلايا المسجل يرمز له R(x)

أمثال كثير الحدود V(x) هي $a_n, a_{n-1}, ..., a_0$

تطبق على دخل دارة التقسيم بترتيب متناقص بدءاً من

$$\alpha_0 ..... a_{n-2} \leftarrow a_{n-1} \leftarrow a_n$$

يستخدم معامل التأخير لتحليل عمل هذه الدارة ونشير إليه بـ Δ الذي يتمثل بتأخير نبضة لكل خلية

$$V = a_n\Delta^0 + a_{n-1}\Delta + ... + a_0\Delta^n \qquad (5-42)$$

يمثل معامل التأخير صفر (معامل الوحدة) في هذه العلاقة $\Delta^0 = I$, يشير هذا إلى أن الرمز a_n يوجد على مدخل الخلية C_0 أما الحد $a_0\Delta^n$ فيشير إلى أن الرمز a_0 يصل إلى مدخل الخلية C_0 بعد n نبضة.

فتكون دالة النقل (التحويل) للدارة Tحيث

U هو التابع المطبق على الدخل

Y هي الإشارة التي نحصل عليها على الخرج

$$T = \frac{Y}{U} \qquad (5-43)$$

نعد حالة خاصة لتحديد هذا التابع

$$U = a_m\Delta^0 + g_{m-1}\Delta + ... + g_0\Delta^m \quad ; \quad g_m = g_0 = 1 \qquad (5-44)$$

يطبق على الدخل أول رمز $g_m = 1$ بعد m نبضة سيظهر في الخلية C_{m-1} على الخرج بتأخير Δ^m الذي يكون أول نبضة على الخرج

$$Y = g_m\Delta^m = \Delta_m \qquad (5-45)$$

يصل الرمز $g_m = 1$ إلى الخرج من خلال وصلات التغذية العكسية سيتم ضربه بأمثال $g_0, g_1, ..., g_{m-1}$ ومن ثم الجمع من النموذج الثنائي حيث يجمع g_0 مع آخر رمز g_0 من السلسلة U الذي يصل على مدخل الخلية C_0 بالإضافة إلى محتوى الخلايا $C_0, C_1, ..., C_{m-2}$ أي الرموز $g_1, ..., g_{m-1}$مع بقية الأمثال و يظهر الرمز "0"في النبضة التالية m+1 في كافة خلايا المسجل نتيجة عملية الجمع من النموذج الثنائي على مدخل جميع الخلايا وبالمحصلة فإن Δ^mهو الحد الوحيد في السلسلة Y

$$Y = \Delta^m \qquad (5-46)$$

$$T = \frac{Y}{U} = \frac{\Delta^m}{g_m\Delta^0 + g_{m-1}\Delta' + ... + g_0\Delta^m} \qquad (5-47)$$

$$\frac{Y}{U}=\frac{I}{g_m\Delta^{-m}+g_{m-1}\Delta^{-(m-1)}+.....+g_0 I} \qquad (5-48)$$

حيث:

$$Y=\frac{U}{g_m\Delta^{m}+g_{m-1}\Delta^{m-1}+.....+g_0 I} \qquad (5-49)$$

تكتب في هذه العلاقة U المبينة في العلاقة (42) على الشكل التالي:

$$U=\Delta^{n}(\alpha_n\Delta^{-n}+\alpha_{n-1}\Delta^{-(n-1)}+.....+\alpha_0 I) \qquad (5-50)$$

وبتبديل $\Delta^{-1}=x$ ينتج بأن تقوم الدارة بعملية تقسيم كثير الحدود v(x) على كثير الحدود g(x) نحصل على ناتج التقسيم (الكم) على الخرج بتأخير Δ^{n} أي بعد n نبضة أما الباقي فينبغي أن يكون مخزناً في المسجل.

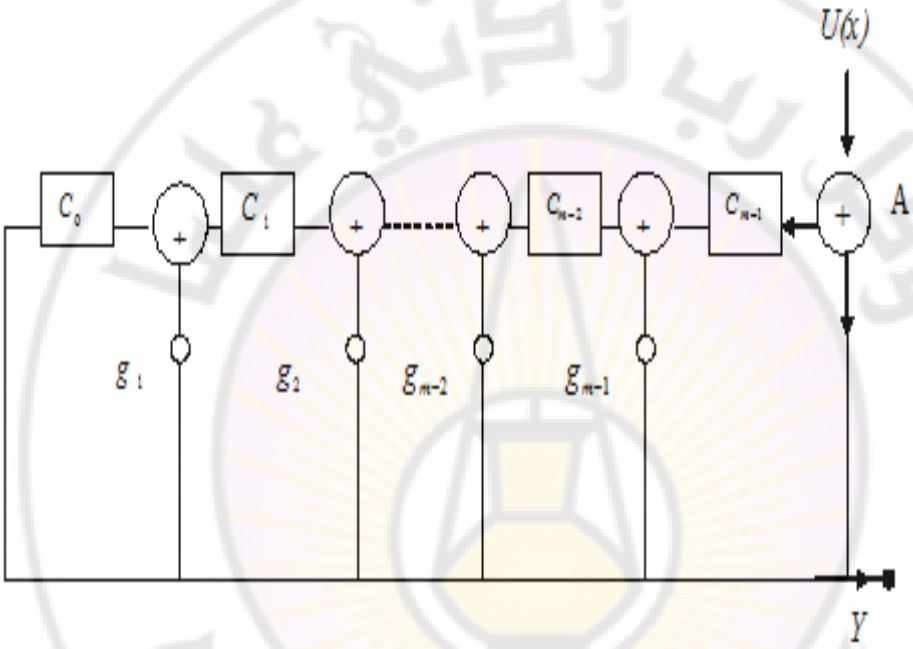
في الحالة الخاصة $U(x)=g(x)$ عند النبضة $n+1$ $(n=m)$ محتوى المسجل (الباقي) يكون صفراً, يمكن لهذا الناتج أن يعمم من أجل أي كثير حدود $v(x)=q(x)g(x)$ مقسم على g(x).

فإذا كان كثير الحدود U(x) من الدرجة $(n<m)$ يكون الباقي بعد نبضة $n+1$ مخزناً في المسجل بأمثال X^0 في الخلية C_0.

يمكن في عملية التحليل للمسجل أن نرى أنه من أجل n عند النبضة $n+1$ يكون الباقي مخزناً في المسجل.

5 – 4 – 2الترميز من خلال دارة التقسيم:

تستخدم دارة التقسيم وذلك لتطبيق العلاقة (5-39) , و يتم تطبيق $u(x)=i(x)$ في النقطة A كما في الشكل (5-3)



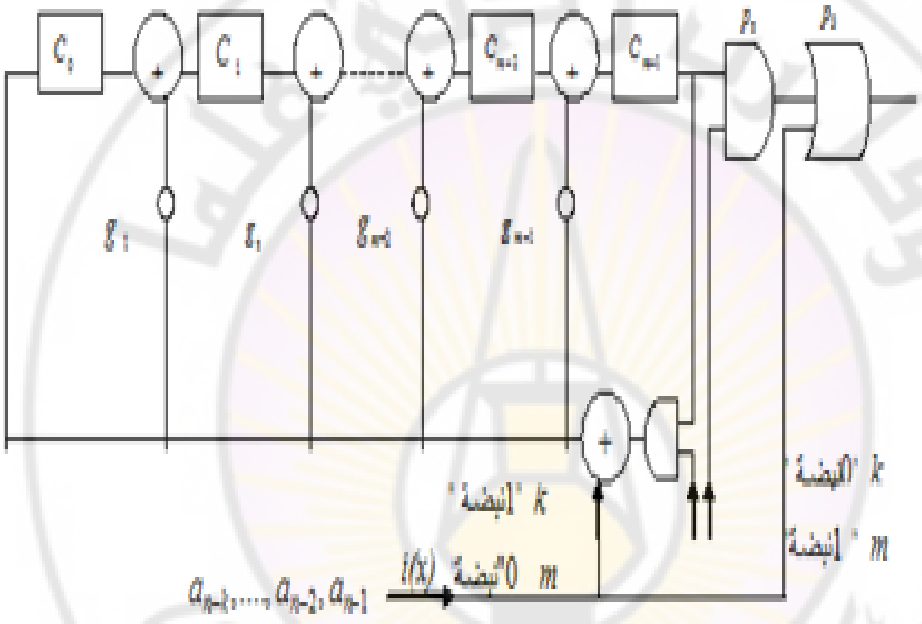
الشكل (5-3) دارة تقسيم كثير الحدود xmu(x) على g(x)

وليس على مدخل الدارة كما في الشكل السابق عندئذ تقوم الدارة بعملية $x^m i(x)$ على $g(x)$ وليس $i(x)$ على $g(x)$, لإثبات ذلك نفترض كثير الحدود $i(x)=1$ ومطبق على النقطة A كما في الشكل في هذه الحالة يكون محتوى المسجل في أول نبضة $g_0, g_1, \ldots\ldots, g_{m-1}$ أي باقي تقسيم X^m على $g(x)$.

إذاً إما أن نطبق X^m على المدخل أو أن نطبق $U(x)=1$ في النقطة A و نحصل على الباقي نفسه (إذ بتطبيق كثير الحدود $i(x)$ في النقطة A تكافئ عملية الضرب بـ X^m ونحصل على الباقي

$$c(x) = rest\frac{x^m i(x)}{g(x)} \qquad (5-51)$$

الدارة التي تقوم بعملية الترميز هي في الشكل(5−4):

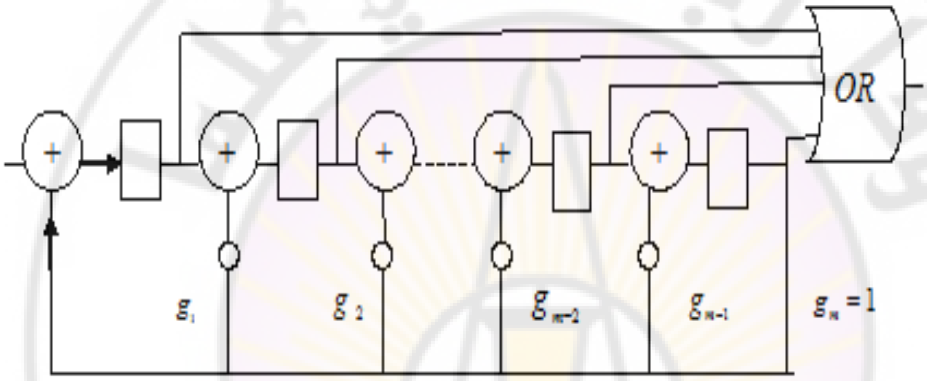


الشكل (5−4) الترميز بدارة التقسيم

نطبق رموز المعلومات $a_{n-1} \leftarrow a_{n-2}.....\alpha_{n-k}$ كما في الشكل لتظهر في الوقت نفس ه على الخرج من خلال البوابة P_3 وتكون البوابة p_1 في حالة وصل لمدة k نبضة أما P_2 فتكون في حالة قطع وفي الوقت نفسه تقوم الدارة بعملية الحساب للباقي الذي يظهر في المسجل. عند النبضة $K+1$ تصبح البوابة p_2 في حالة وصل و البوابة P_1 في حالة قطع لفترة m نبضة لتسمح بتفريغ المسجل (رموز المراقبة) من خلال البوابة P_3 وذلك بعد رموز المعلومات ليتم الحصول على كلمة الترميز.

5- 4 – 3 كاشف الترميز من خلال دارة التقسيم:

يعتمد كاشف الترميز على حساب المصحح $z(x) = rest\dfrac{V'(x)}{g(x)}$ طبقاً للدارة من الشكل:



الشكل (5-5) كاشف الترميز بدارة التقسيم

حتى يتم كشف الأخطاء نتحقق فيما إذا كان $z(x)$ يساوي الصفر أم لا و هذا العمل يتم بواسطة بوابة " OR" على الخرج فإذا كان يساوي 1 أي $z(x) \neq 0$ (على اعتبار أن محتوى الخلايا هو الباقي أي $z(x)$) يشير ذلك إلى أن الكلمة التي نستقبلها قد تعرضت للخطأ لذلك لا بد من إعادة إرسالها, في حال الباقي يساوي الصفر على خرج البوابة " OR" سيكون لدينا صفر أي أن الكلمة ليست فيها أخطاء.

عملية الترميز وكشف الترميز لها القدرة على كشف رزمة من الأخطاء طولها m أو أقل. لنفترض أن رزمة الأخطاء تبدأ في مكان ما j يمكن أن نكتب:

$$\ell(x) = x^j + \varepsilon_{j+1}x^{j+1} + ... + x^{j+m-1} \qquad (5-52)$$

و بما أن أول وآخر أمثال كثير الحدود للأخطاء هو "1" أما البقية فيمكن أن تكون

"1" أو "0" وبالتالي يمكن أن تكتب رزمة الأخطاء على الشكل التالي:

$$\ell(x) = x^j(1+\varepsilon_{j+1}x+.....+x^{m-1}) = x^j b(x) \qquad (5-53)$$

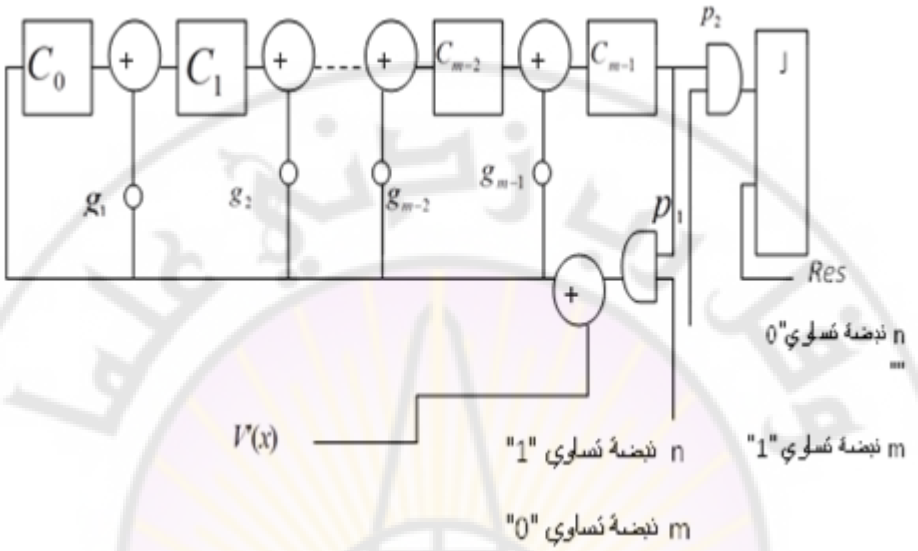
$$v'(x) = v(x) + \ell(x) \qquad (5-54)$$

$$z(x) = rest\,\frac{\ell(x)}{g(x)} = rest\,\frac{x^j b(x)}{g(x)} \qquad (5-55)$$

بما أن $b(x)$ من الدرجة $m-1$ ليس مقسماً على $g(x)$ وبما أن $g(x)$ لا يقبل التحليل (ليس له جذور) وهو مقسم لكثير الحدود x^n+1 فالباقي $\frac{x^j b(x)}{g(x)}$ يختلف عن الصفر إذاً المرمز قادر على كشف رزمة من الأخطاء طوله m في أي مكان.

حتى يكون لدينا كاشف ترميز مطابق للمرمز نستخدم الدارة في الشكل (6-5).

حيث دارة القلاب تكون في وضعية العمل , إذ كان محتوى المسجل يختلف عن الصفر في هذه الحالة يكون الباقي الذي نحصل عليه مساوياً لما هو عليه في الدارة المبينة في الشكل الأول مضروباً بـ X^m وهذه لها أهمية فقط في حالة القيام بعملية كشف الترميز.



الشكل (5–6) كاشف الترميز بدارة التقسيم

5 – 5 عملية الترميز وكشف الترميز بمسجلات الإزاحة ذات التغذية العكسية:

هي دارة تسلسلية خطية تعمل ذاتياً أي من دون أن نطبق عليها إشارة خارجية فقط الإشارة الناتجة عن التغذية العكسية كما في الشكل (5–7).

يتم إجراء وصلات المسجل حسب كثير الحدود المولد(أمثال كثير الحدود المولد)

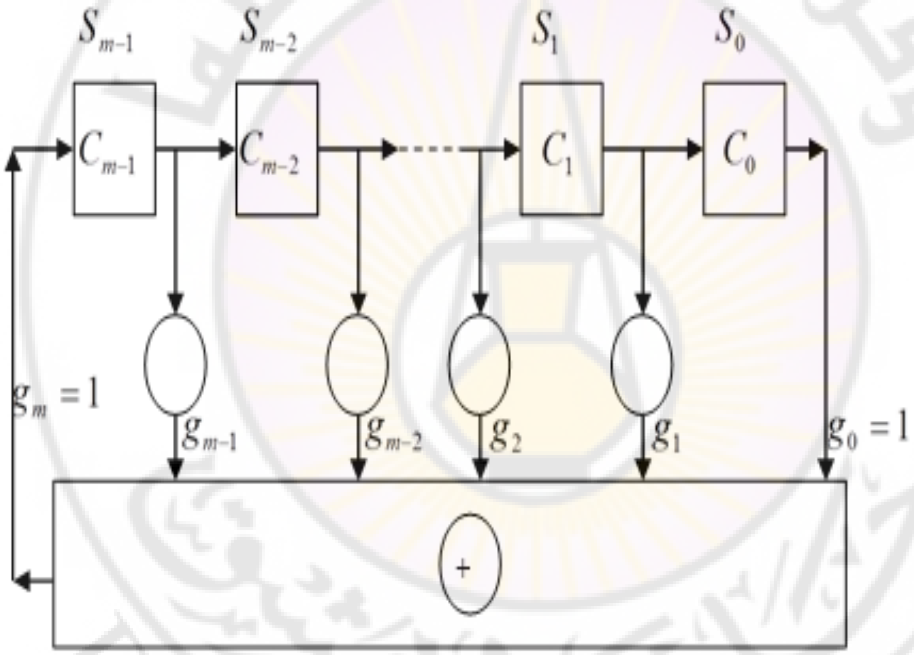
$$g(x) = g_0 + g_1 x + ... + g_{m-1} x^{m-1} + x^m \qquad (5-56)$$

S_i هي حالة الخلية C_i عند اللحظة t

$S`_i$ هي حالة الخلية C_i عند اللحظة t+1

وتكون العلاقة بين حالات المسجل المتتالية معطاة في المعادلات التالية:

$$S`_0 = S_1$$
$$S`_1 = S_2$$
$$:$$ (5 - 57)
$$:$$
$$S`_{m-2} = ...S_{m-1}$$
$$S`_{m-1} = g_0 S_0 + g_1 S_1 + ... + g_{m-1} S_{m-1}$$



الشكل (5–7) دارة مسجل إزاحة ذي تغذية عكسية

$$S` = TS$$ (5 - 58)

$$S=\begin{bmatrix} S_0 \\ S_1 \\ : \\ : \\ : \\ S_{m-1} \end{bmatrix} \quad , \quad S`=\begin{bmatrix} S`_0 \\ S`_1 \\ : \\ : \\ : \\ S`_{m-1} \end{bmatrix} \qquad (5-59)$$

$$T=\begin{bmatrix} 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & 0 & . & . & 0 \\ 0 & 0 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & . & . & . & . & 0 & 1 \\ g_0 & g_1 & . & . & . & . & g_{m-1} \end{bmatrix} \qquad (5-60)$$

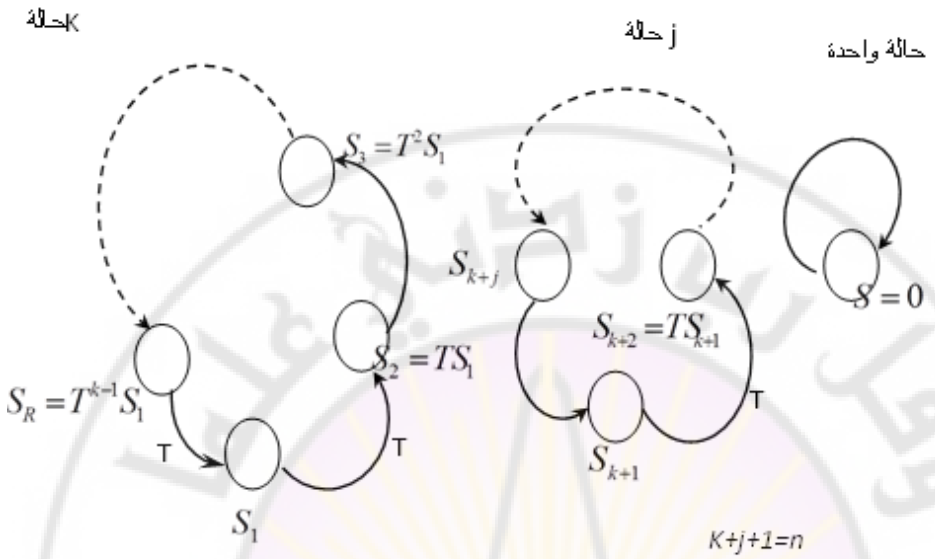
فإذا كانت الحالة الأولى للمسجل في S فتكون الحالات المتعاقب

$$T^n S = S, T^2 S, TS$$

يتم الحصول على هذه الحالات من خلال الضرب المتتالي بـ T.

بما أن عدد الحالات محدد فمن البديهي أن يعود المسجل إلى الحالة الابتدائية حتى يكون لكل حالة في المسجل حالة سابقة لابد وأن يكون موجوداً مصفوفة T^{-1} أي $g_0 = 1$ ، يمكن لكل مسجل أن يكون له عدد من الدورات كما في الشكل (5-8).

العدد الكلي للحالات التي لا تساوي الصفر $2^m - 1$ يتم إنجازها بدورة أو أكثر:



الشكل (5-8) دورات لمسجل إزاحة ذي تغذية عكسية

هناك حالة يمكن للمسجل C1 أن يعطي كافة الحالات في دورة واحدة فقط أي $2^m - 1$ كثير الحدود الذي يميز (يوصف) به المصفوفة T محدد بالعلاقة:

$$\phi(x) = \det|T - XI| \quad \text{فإذا} \qquad (5-61)$$

كانت المصفوفة هي المعطاة في العلاقة (5-60)

$$\phi = \begin{vmatrix} -x & 1 & 0 & . & . & . & . & 0 \\ 0 & -x & 1 & 0 & . & . & . & 0 \\ : & : & : & : & : & : & : & : \\ : & : & : & : & : & : & : & : \\ 0 & 0 & 0 & 0 & 0 & 0 & -x & 1 \\ g_0 & g_1 & . & . & g_{m-2} & g_{m-1} & & -x \end{vmatrix} \qquad (5-62)$$

وبإجراء عملية الحساب للمحدد نحصل على

$$\phi(x) = g_0 + g_1 x + ... + g_{m-1} x^{m-1} + x^m \qquad (5-63)$$

أي أن كثير الحدود للمصفوفة T هو كثير الحدود المولد الذي يحدد نوعية المسجل ذ التغذية العكسية.

طبقاً لنظرية (كايلي هاملتون) فالمصفوفة T هي جذر لكثير الحدود

$$\phi(x) = g(x)$$

$$g(T) = 0 \qquad (5-64)$$

نختار الحالة البدائية أي أن جميع خلايا المسجل تحتوي على حالة "0" ما عدا الخلية C_{m-1} تحتوي على "1"

$$U = \begin{bmatrix} 0 \\ 0 \\ : \\ 1 \end{bmatrix} \qquad (5-65)$$

بناء على ذلك فإن حالات المسجل المتتالية ستكون:

$$U = T^0U, T^1U, T^2U, T^{n-1}U \ , T^nU = U \qquad (5-66)$$

حيث $T^0 = I$

تسمى فترة (دورة) المصفوفة T أو طول الدورة للمصفوفة أقل عدداً من الدورات بحيث

$$T^n = T^0 = I \qquad (5-67)$$

أي

$$T^n U = U \qquad (5-68)$$

بعد ذلك تحديد الشرط من أجل m رمز، الطول الأعظمي n، الذي يساوي إلى العدد الكلي للحالات التي لا تساوي الصفر يكون $n = 2^m - 1$ طبقاً لنظرية وجود جذور لكثير الحدود يمكن أن نقول:

أي كثير حدود g(x) من الدرجة m (كثير حدود لا يقبل التحليل أو التقسيم على أي كثير حدود أمثاله في GF(2)) تشكل فئات الباقي من النموذج g(x) حقل مكون من 2^m عنصر يسمى امتداداً للحقل GF(2) ويشار إليه ب $GF(2^m)$ إذا أشرنا إلى α جذر g(x) النظرية تقول إن $\alpha \in GF(2^m)$ نشير إلى α عنصر أولي إذا كانت كل العناصر $2^m - 1$ التي لا تساوي الصفر في $GF(2^m)$ يمكن أن تفسر على أساس القوة ل α أي أن العناصر التي لا تساوي الصفر من الحقل $GF(2^m)$ تشكل زمرة (مجموعة) من الدرجة 2^{m-1} .

$$\alpha = 1, \alpha, \alpha^2, ..., \alpha^{2^m - 1} = 1 \qquad (5-69)$$

كثير الحدود g(x) الذي لا يقبل التحليل(غير القابل للاختزال) (irreducible) وله جذر α عبارة عن عنصر أولي في الحقل $GF(2^m)$ يسمى كثير حدود أولي.

وطبقا للعلاقة (5) كثير الحدود الأولي g(x) هو مقسم لكثير الحدود $P(x) = x^n + 1$ ينتج الجذر α لكثير الحدود g(x) هو جذر $x^n + 1$ اذاً:

$$\alpha^n = 1 \qquad (5-70)$$

بما أن α هو عنصر ضمن الزمرة "المجموعة" المضاعفة من الدرجة $2^m - 1$ أي أن $\alpha^{2^m - 1} = 1$ ينتج أن

$$n = 2^m - 1 \qquad (5-71)$$

في هذه الشروط مجموعة الدورات المولدة من العنصر الأولي α هي العناصر التالية:

$$\alpha^0 = 1, \alpha, \alpha^2, ... \alpha^n = 1 \qquad (5-72)$$

هذه تقابل الحالات التي لا تساوي الصفر للمسجل المعطى في العلاقة(66–5) أي أن المسجل يأخذ جميع الحالات الممكنة أي طول الدورة الأعظمي.

بالنتيجة: نقول اذا كانت وصلات المسجل مطابقة لكثير الحدود الأولي من الدرجة m فسيكون في هذه الحالة عدد الدورات أعظمياً

$$n = 2^m - 1$$

مثال: لنعد مسجل الإزاحة ذا التغذية العكسية له المواصفات التالية m=3 وصلاته طبقاً لكثير الحدود الأولي من الدرجة m=3 يتم اختيار كثير الحدود $g(x) = 1 + x + x^3$ وإذا كان α هو جذر لكثير الحدود ينتج أن $1 + \alpha + \alpha^3 = 0$ بناء على هذه العلاقة يتم الحصول على فئات الباقي وذلك برفع α إلى القوى فينتج:

أول فئة للباقي للعنصر "0" غير مبينة في الجدول.

نشكل في العمود الثاني من الجدول جميع فئات الباقي المولدة من كثير الحدود من الدرجة "3" أي جميع كثيرات الحدود ذات الدرجة أقل من 3، ويمكن شرح كثيرات الحدود على قوى αعلما أن $g(x) = 1 + x + x^3$ هو أولي نلاحظ أن الفئات المتبقية المشكلة عند تقسيم أي كثير حدود ينتج كثير حدود جديداً موجوداً ضمن فئات الباقي أي أن فئات الباقي تشكل حقلا عدد فئات الباقي التي لا تساوي الصفر وتكون $n = 2^3 - 1 = 7$ وعلى أساس التقابل باتجاهين $\alpha \Leftrightarrow T^k U$ نقول

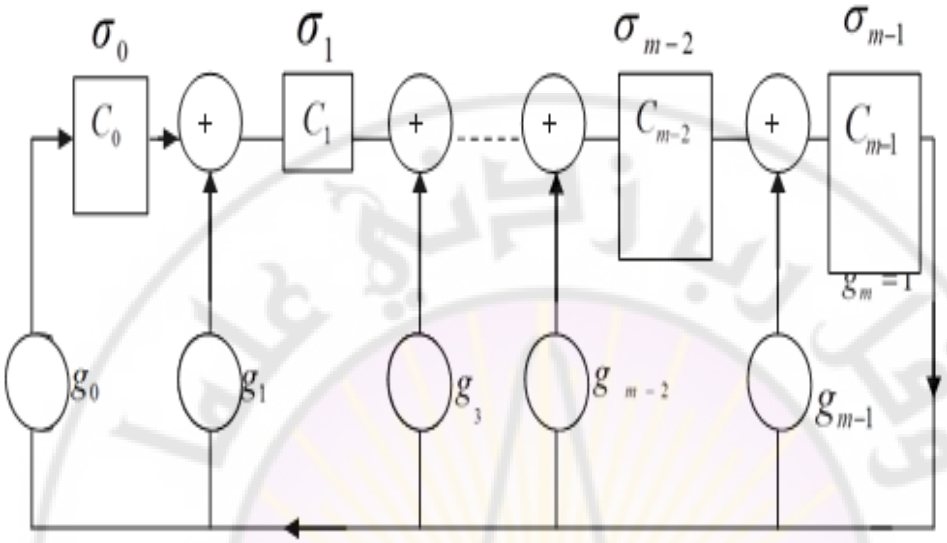
إن مسجل الإزاحة ذا التغذية العكسية المقابل يولد جميع الحالات التي لا تساوي الصفر.

قوى α	فئات الباقي للنموذج $g(x)=1+x+x^3$	تمثيل العنصر كمصفوفة
α^0	1	0 0 1
α	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha+1$	0 1 1
α^4	$\alpha^2+\alpha$	1 1 0
$\alpha^5=\alpha^3+\alpha^2$	$\alpha^2+\alpha+1$	1 1 1
$\alpha^6=\alpha^3+\alpha^2+\alpha$	α^2+1	1 0 1
$\alpha^7=\alpha^3+\alpha$	1	0 0 1

الجدول (5 – 2)

يشار إليها في آخر عامود من الجدول (على شكل مصفوفة صف وذلك لعملية التوافق) مع الإشارة i=0,1,2,….,7 القوى K نأخذ القيم نفسها ولكن بترتيب آخر.

جميع الاعتبارات السابقة هي صالحة للمسجل المكافئ المبين في الشكل(5-9) :



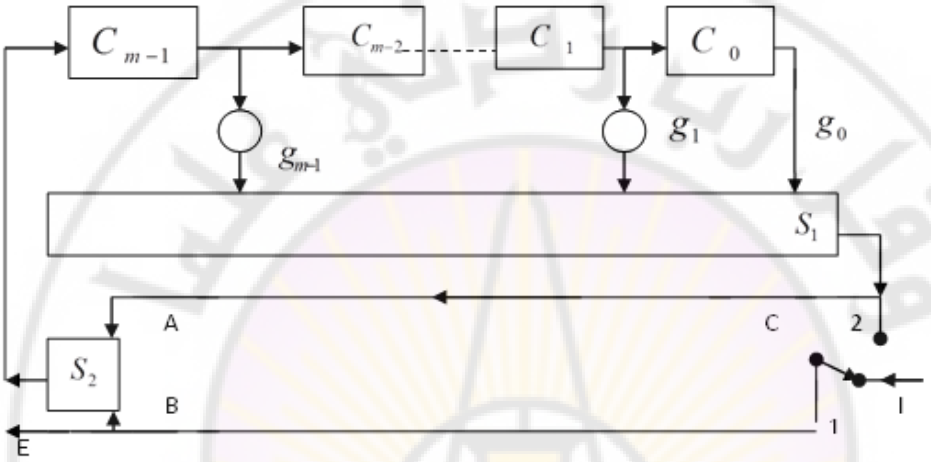
الشكل (5–9) دارة مسجل إزاحة ذي تغذية عكسية مكافئ

التي مصفوفته من الشكل:

$$\tau = T^T \begin{bmatrix} 0 & 0 & 0 & .. & g_0 \\ 1 & 0 & 0 & .. & g_1 \\ 0 & 1 & 0 & .. & .. \\ .. & .. & .. & 1\ 0 & g_{m-2} \\ 0 & .. & 0 & .. \ .. \ 1 & g_{m-1} \end{bmatrix} \qquad (5-73)$$

5 – 5 – 1 مرمز مسجل إزاحة ذي تغذية عكسية :

هذا المسجل مشكل من m=n–k خلية مع وصلات مطابقة لكثير الحدود المولد كثير حدود أولي



الشكل (5–10) دارة ترميز بمسجل إزاحة ذي تغذية العكسية

$$g(x) = g_0 + g_1 x + ... + g_{m-1} x^{m-1} + g_m x^m \qquad (5-74)$$

حيث

$$g_m = g_0 = 1$$

في البداية يوجد المفتاح C في الوضعية 1 يتم إدخال K رمز معلومات

$$\alpha_{n-1}, \alpha_{n-2}, ..., \alpha_{n-k}$$

تظهر هذه الرموز في الوقت نفسها على الخرج , تكون جميع الخلايا مخزنة بأصفار وتسمى الحالة البدائية للمسجل.

يطبق في النبضة الأولى الرمز α_{n-1} وتوصف حالات المسجل على شكل مصفوفة وتظهر حالة المسجل على A على الشكل التالي:

$$\alpha_{n-1}\begin{bmatrix}0\\0\\:\\:\\0\\1\end{bmatrix}=\alpha_{n-1}U \qquad (5-75)$$

تكون حالة المسجل في النبضة الثانية:

$$\alpha_{n-1}TU+\alpha_{n-1}U \qquad (5-76)$$

حيث T هي مصفوفة المسجل.

في النبضة الثالثة حالة المسجل:

$$\alpha_{n-1}T^2U+\alpha_{n-2}TU+\alpha_{n-3}U \qquad (5-77)$$

بعد K نبضة تكون حالة المسجل:

$$\alpha_{n-1}T^{k-1}U+\alpha_{n-2}T^{k-2}U+...+\alpha_{n-k}U \qquad (5-78)$$

ينقل المفتاح C إلى الوضعية 2 بعد إدخال جميع رموز المعلومات, يوصل خرج من الجامع S_1 إلى خط الخرج وعلى خطين A و B إلى الجامع S_2 وفي الوقت نفسه ترسل إلى الخرج بحيث تشير إليهما:

$$\alpha_{m-k-1}=\alpha_{m-1},\alpha_{m-2},...,\alpha_1,\alpha_0$$

بعد نقل المفتاح C أي في النبضة K+1 تكون الحالات المتتالية للمسجل

$$\alpha_{n-1}T^kU+\alpha_{n-2}T^{k-1}+....+\alpha_{n-k}TU+\alpha_{n-k-1}U \qquad (5-79)$$

وهكذا حتى تظهر جميع رموز المراقبة

$$\alpha_{n-1}T^{n-1}U+\alpha_{n-2}T^{n-2}U+....+\alpha_1TU+\alpha_0U \qquad (5-80)$$

في اللحظة نفسها نطبق في آن واحد رموز المراقبة على المدخلينA وB للجامع S2 بحيث سيظهر الصفر على مدخل المسجل في كل إزاحة, وبعد m إزاحة نصل إلى الحالة البدائية أي أننا يمكن أن نكتب الحالة الأخيرة في العلاقة (5 – 80) بأنها تساوي الصفر

$$\alpha_0 U + \alpha_1 T U + ... + \alpha_{n-2} T^{n-2} U + \alpha_{n-1} T^{n-1} U = 0 \qquad (5-81)$$

وهذه العلاقة يمكن أن تكتب بشكل جداء متري (قياسي):

$$\begin{bmatrix} U & TU & T^2U & ... & T^{n-2}U & T^{n-1}U \end{bmatrix} \begin{bmatrix} \alpha_0 & \alpha_1 & ... & \alpha_{n-1} \end{bmatrix}^T = 0 \qquad (5-82)$$

وهي مطابقة للعلاقة:

$$HV^T = 0 \qquad (5-83)$$

حيث:

$$H = \begin{bmatrix} U & TU & T^2U & T^3U & ... & T^{n-2}U & T^{n-1}U \end{bmatrix} \qquad (5-84)$$

والكلمة المرمزة:

$$V = \begin{bmatrix} \alpha_0 & \alpha_1 & ... & \alpha_{n-1} \end{bmatrix} \qquad (5-85)$$

حيث $\alpha_{n-k-1} \ ... \ \alpha_1 \ \alpha_0$ هي رموز مراقبة , $\alpha_{n-1} \ ... \ \alpha_{n-k}$ هي رموز معلومات

تعد الحالات $2^m - 1$ للمسجل ذي m خلية حيث $n = 2^m - 1$ هي عناصر في الحقل $GF(2^m)$ مولدة من جذور α لكثير الحدود الأولي من الدرجة m.

5 – 5 – 2 كاشف الترميز بمسجل الإزاحة ذي التغذية العكسية:

تحتوي وحدة كاشف الترميز بمسجل الإزاحة ذي التغذية العكسية على مسجل أولي (RP) وكاشفي ترميز(Dc1,Dc2), ومسجلي إزاحة ذو تغذية

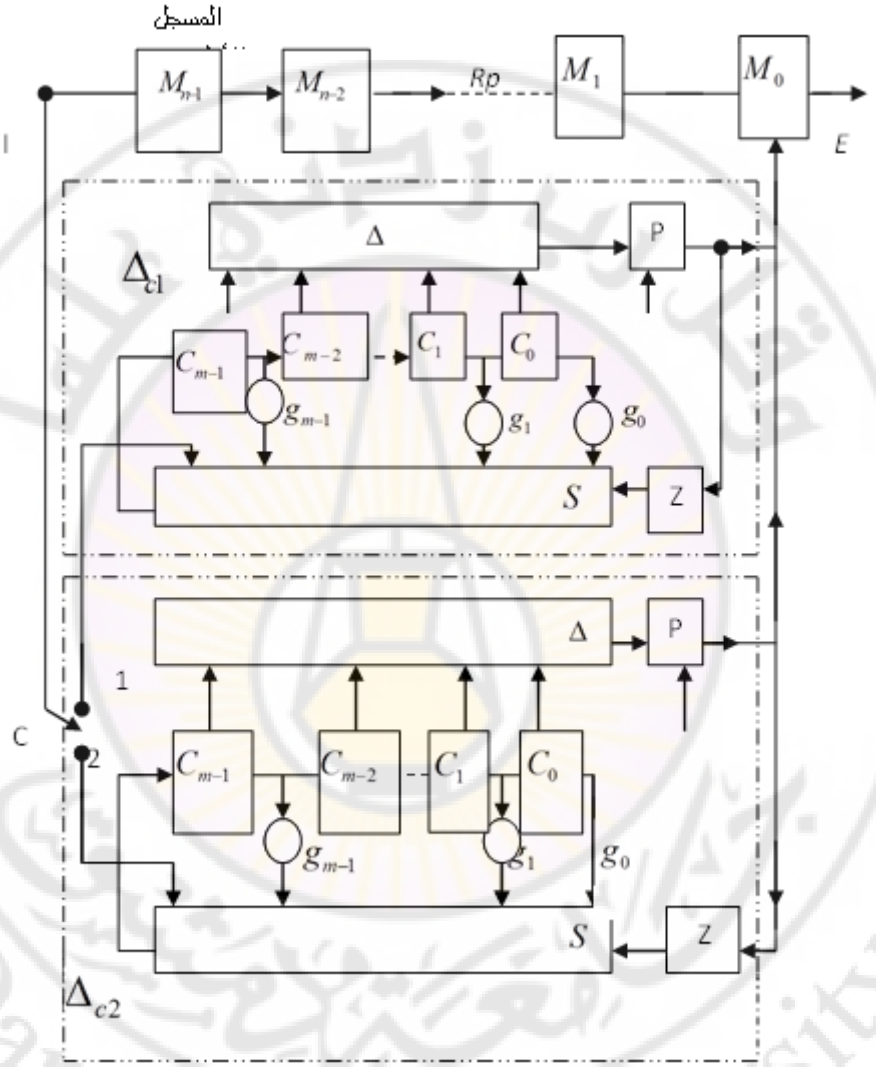
عكسية مشبهان للمسجل في المرمز , يخزن المسجل الأولي كلمة الاستقبال بطول n يتم حساب المصحات الضرورية, وتخزن في خلايا مسجلات الإزاحة بتغذية عكسية هذه الخلايا موصولة مع كاشف الخطأ (D) وظيفة كاشف الترميز كشف حالات المسجل ذو التغذية العكسية ليعطي 1 وذلك عندما تكون جميع خطوط المطبقة على كاشف الخطأ واحدات أي عندما يكون المسجل في الخلية C0 في حالة 1وبقية الخلايا أصفار، سيجمع هذا الرمز "1" ثنائيًا مع الرمز الخاطئ عندما يوجد في آخر الخلية M_0 للمسجل الأولي (الرئيسي) وذلك لتنفيذ عملية التصحيح. في الوقت نفسه سيظهر الصفر هذا الرمز "1" يطبق بتأخير نبضة على مجمع مسجل إزاحة التغذية العكسية لتصفير المسجل.

في حال كشف الأخطاء وليس تصحيحها تكون دالة كشف الأخطاء أبسط حيث ترسل "1" إذاً الحالة النهائية (بعد استقبال كافة رموز الكلمة) لمسجل الإزاحة ذي التغذية العكسية تختلف عن الصفر.

تعمل وحدة الكاشف على الشكل التالي:

يتم إدخال كلمة الاستقبال في آن واحد في مسجل الإزاحة الرئيسي الذي يعمل كذاكرة وفي مسجل الإزاحة ذي التغذية العكسية، يتم حساب المصحح عند

آخر رمز للكلمة المستقبلة التي تدخل إلى المسجل الرئيسي وكاشف الترميز.



الشكل (5-11) دارة ترميز بمسجل إزاحة ذو تغذية العكسية

يتم إيصال الكاشف وتفتح البوابة p وتنفذ عملية التصحيح في هذه اللحظة

يمرر المفتاح C إلى الوضعية 2 تدخل الكلمة المستقبلة إلى كاشف الترميز2 ومن ثم إلى المسجل الرئيسي في الوقت الذي يتم فيه تفريغ الكلمة السابقة.

تكون حالة المسجل للإزاحة ذي التغذية العكسية طبقا لعملية الترميز:

$$z = \alpha'_0 U + \alpha'_1 TU + ... + \alpha'_{n-2} T^{n-2} U + \alpha'_{n-1} T^{n-1} U \qquad (5-86)$$

نشير إلى α'_i بالرمز المستقبل و α_i بالرمز المرسل. إذا لم يوجد خطأ $\alpha'_i = \alpha_i$ فإن $z = 0$

تبقى حالة المسجل (بسبب $T.0 = 0$) كما هي و الكاشف لا يرسل أي إشارة تصحيح.

أما إذا وجدت أخطاء $\alpha'_i \neq \alpha_i$ في أماكن معينة, $Z \neq 0$ فإن هذه النتيجة تساعد في كشف الأخطاء.

إذا كان لا بد لكل خطأ من أن يصحح فلا بد من وجود مصححات منفصلة يتم التعرف عليهن من الكاشف للأخطاء الذي يعطي إشارة التصحيح.

تتم هذه العملية بمعرفة المصحح من قبل الكاشف في اللحظة التي يوجد الرمز الخاطئ في آخر خلية للمسجل الرئيسي M_0، تنفذ في هذه الخلية عملية الجمع الثنائي للرمز المخزن مع 1 المعطى منفذاً عملية التصحيح.

5 – 5 – 3 ترميز هامينغ الدوري المصحح لخطأ واحد:

يتميز ترميز هامينغ بمصفوفة المراقبة

$$H = \begin{bmatrix} U & TU & T^2U & ... & T^{n-1}U \end{bmatrix} \qquad (5-87)$$

حيث $n = 2^m - 1$ عدد رموز الكلمة

تتم عملية الترميز طبقا للعلاقة:

$$H v^T = 0 \qquad (5-88)$$

إذا كان كثير الحدود المولد g(x) أولياً فيكون :

$$g(x) = 1 + g_1 x + g_2 x^2 + ... + g_{m-1} x^{m-1} + x^m \qquad (5-89)$$

يصمم مسجل الإزاحة ذي التغذية العكسية طبقا لكثير الحدود المولد و يولد ترميز دوري هامينغ ذي m رمز مراقبة و $k = n - m$ رمز معلومات.

يختلف هذا المرمز عن مرمز هامينغ الزمري بأنه مرمز نظامي.

يتميز مرمز هامينغ المعطى بالعلاقة (5−287) بأنه قادر على تصحيح خطأ واحد أي أن يكون عامودان مستقلان خطياً

$$T^i U + T^k U = (T^i + T^k) U = T^j U \neq 0$$

يمثل شعاع الخطأ في المصفوفة

$$\varepsilon = [..... \quad \alpha_{n-r} \quad .....] \qquad (5-90)$$

يظهر خطأ واحد في الوضعية n−r ويعطى المصحح في هذه الحالة بالعلاقة:

$$z = H\varepsilon^T = T^{n-r} U \qquad (5-91)$$

نفترض أن الرمز α'_{n-r} رمز خاطئ يدخل إلى مسجل الإزاحة بعد r نبضة

$$\alpha'_{n-r} = \alpha_{n-r} + 1 \qquad (5-92)$$

وبما أن $n = 2^m - 1$ هي فترة المصفوفة T (كثير الحدود g(x) للمصفوفة T هو أولي) فإن الدورة تكون عظمى وتساوي إلى العدد الكلي للحالات الممكنة التي تختلف عن الصفر أي $2^m - 1$

$$T^n = I \qquad (5-93)$$

أي

$$z = T^{-r}U \qquad (5-94)$$

ينتج من ذلك أنه في اللحظة التي يتم فيها إدخال كل رموز كلمة الاستقبال في مسجل الإزاحة يصبح محتوى مسجل الإزاحة ذي التغذية العكسية $z = T^{-r}U$ في هذه اللحظة يمر المفتاح C إلى الوضعية 2 و ستكون الحالات المتتالية $z, T^1z, T^2z, ..., T^{r-1}z$ في الوقت التي تتوالى الرموز $\alpha'_{n-1}, \alpha'_{n-2}, ..., \alpha'_{n-r}$ في الخلية M_0 للمسجل الرئيسي.

بعد r−1 إزاحة يصل الرمز الخاطئ α'_{n-r} إلى M_0 في هذه اللحظة محتوى مسجل الإزاحة ذي التغذية العكسية

$$S_{r-1} = T^{r-1}z = T^{r-1}T^{-r}U = T^{-1}U \qquad (5-95)$$

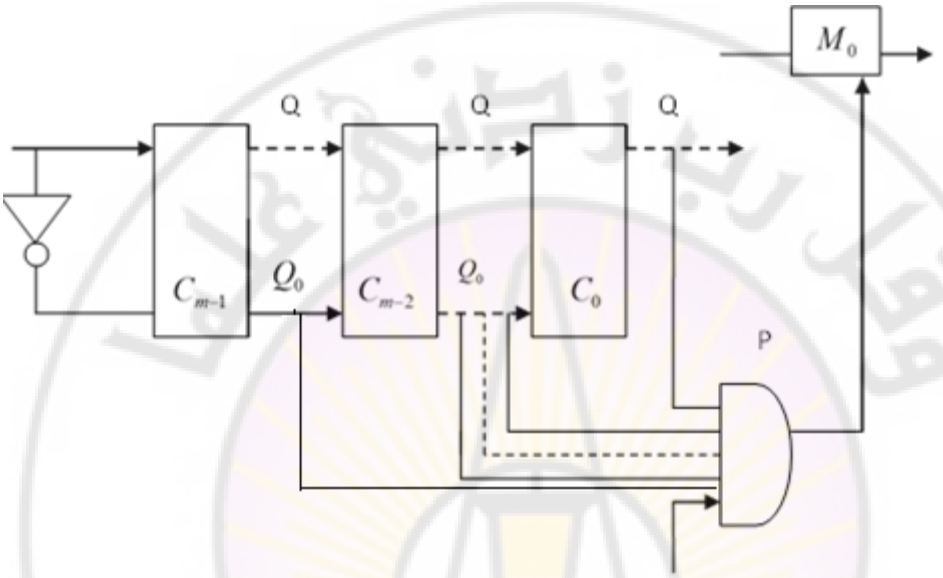
حالة $T^{-1}U$ وهي الحالة التي تسبق U

$$T^{-1}U = \begin{bmatrix} 1 \\ 0 \\ : \\ 0 \end{bmatrix} \qquad (5-96)$$

إذاً يجب تصميم كاشف الأخطاء بحيث يتحسس للحالة $T^{-1}U$ ويعطي الرمز "1" الذي يجمع جمعا ثنائيا مع محتوى الخلية M_0 وذلك لإجراء عملية التصحيح .

يتم إنجاز هذا العمل في الدارة المبينة، عندما يصل مسجل الإزاحة إلى الحال (0,....,0,1) يعطي كاشف الأخطاء الإشارة "1" التي ستجمع مع محتوى

الخلية M_0، ماعدا ذلك تبقى دارة البوابة p في حالة قطع طالما أننا نقوم نحن في حساب المصحح



الشكل (5-12) دارة تحسس الخطأ

من جهة أخرى إذا مر المسجل في الحالة (0,….,0,1) أثناء حساب المصحح ولم يتم الحصول على المصحح بعد عند ذلك ستنفذ الدارة عملية تصحيح خاطئة. حتى نعيد مسجل التغذية العكسية إلى الصفر (ليتم تصحيح كلمة أخرى) يتم تطبيق إشارة التصحيح "1 " على الجامع S_1بتأخير نبضة τ لمسجل الإزاحة ذي التغذية العكسية.

تصبح حالة المسجل ذي الإزاحة عند النبضة r (أول نبضة بعد عملية التصحيح) .

$$T\,S_{r-1}+U=TT^{-1}U+U=U+U=0 \qquad (5-97)$$

تبقى حالة مسجل الإزاحة ثابتة حتى ظهور أول رمز للكلمة التالية والتي نرغب في تصحيحها.

مثال:

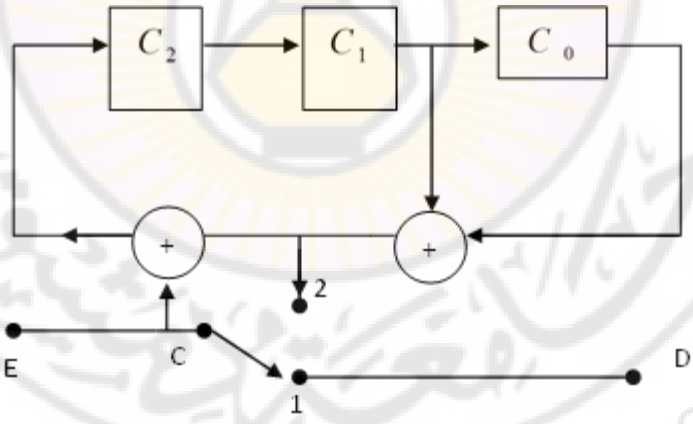
ليكن لدينا الترميز الدوري (n=7 , k=4 , m=3) كلمات الترميز للشكل

$$u(x) = \alpha_0 + \alpha_1 x + ... + \alpha_6 x^6$$

$\alpha_0, \alpha_1, \alpha_2$ رمـوز المراقبـة $\alpha_3, \alpha_4, \alpha_5, \alpha_6$ هـي رمـوز معلومـات $2^3 - 1$ عنصر غير معدوم في حقول $GF = (2^3)$ والتي تنتج (تولد) عن كثير حدود أولي من الدرجة (3) نختار كثير الحدود

$$g(x) = 1 + x + x^3$$

الترميز : مسجل الإزاحة ذي التغذية العكسية من الإرسال بوصلات مصممة طبقاً لكثير الحدود المولد $g(x) = 1 + x + x^3$ المبين في الشكل:



الشكل (5-13) دارة الترميز

لتحديد رموز المراقبة لابد من معرفة المصفوفة H

$$H = \begin{bmatrix} U & TU & T^2U & ... & T^6U \end{bmatrix}$$

حيث أن مصفوفة المسجل هي الحالات المتتالية للمسجل هي:

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

العنصر الأولي للحقل $GF=(2^3)$ حيث $\alpha=TU$

$$\alpha=\begin{bmatrix}0&1&0\\0&0&1\\1&1&0\end{bmatrix}\cdot\begin{bmatrix}0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\\0\end{bmatrix}\quad;\quad \alpha^2=T^2U=\begin{bmatrix}1\\0\\1\end{bmatrix}\quad;\quad \alpha^3=T^3U=\begin{bmatrix}0\\1\\1\end{bmatrix}$$

$$\alpha^4=T^4U=\begin{bmatrix}1\\1\\1\end{bmatrix}\quad;\quad \alpha^5=T^5U=\begin{bmatrix}1\\1\\0\end{bmatrix}\quad;\quad \alpha^6=T^6U=\begin{bmatrix}1\\0\\0\end{bmatrix}$$

يلاحظ أن هذه الحالات (على شكل مصفوفة النقل) في الجدول 5 وتكون مصفوفة المراقبة

$$u=\alpha^0\quad;\quad TU=\alpha\quad;\quad \alpha^6=T^2U\quad;\quad \alpha^3=T^3U$$
$$\alpha^5=T^4U\quad;\quad \alpha^4=T^5U\quad;\quad \alpha^2=T^6U$$

هذه المصفوفة هي المصفوفة الموجودة في العلاقة(24-5):

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

وذلك بتبديل أمثال H(x)

ومن العلاقة:

$$h(x)=\frac{x^7-1}{g(x)}=x^4+x^2+x+1$$

$$Hv^T=0\Rightarrow\begin{cases}a_2=a_4+a_5+a_6\\ a_1=a_3+a_4+a_5\\ a_0=a_2+a_3+a_4=a_3+a_5+a_6\end{cases}$$

بالنتيجة نفسها يمكن أن نوصل لعملية الترميز المعادلة:

$$C(x)=rest\frac{x(a_3+a_4x+a_5x^2+a_6x^3)}{1+x+x^3}$$

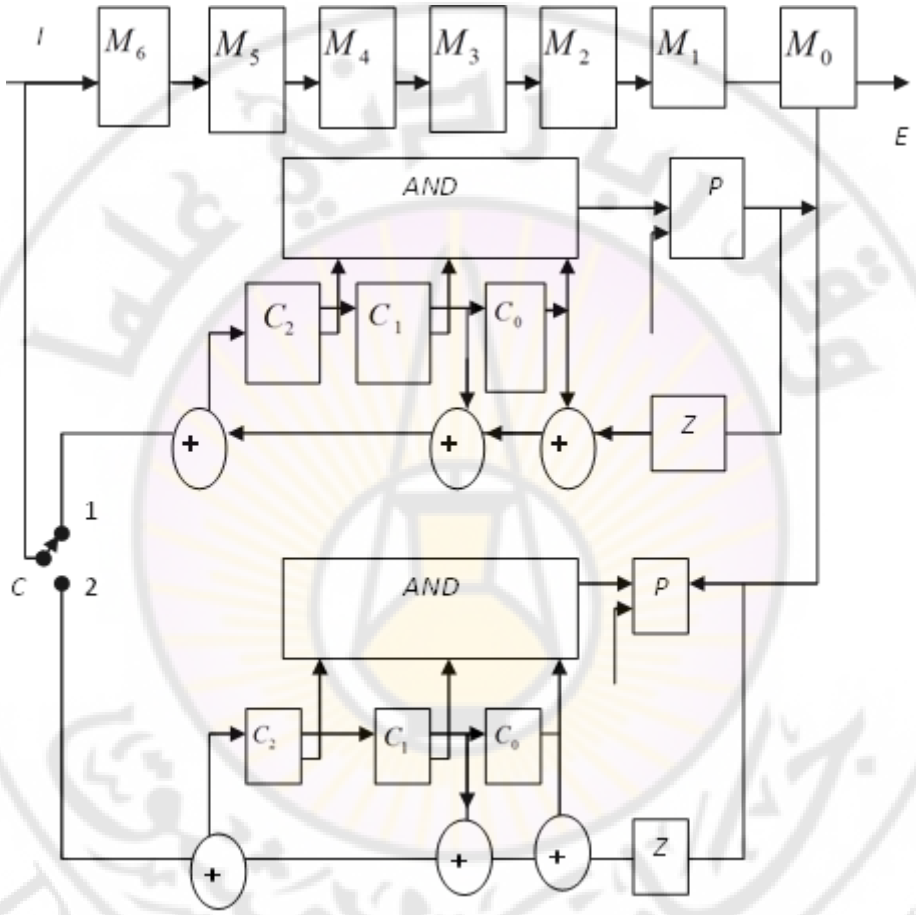
$$C(x)=(a_3+a_5+a_6)+(a_3+a_4+a_5)x+(a_4+a_5+a_6)x^2$$

تساوي الأمثال كما هو في المعادلة:

$$C(x)=a_0+a_1x+a_2x^2$$

نبين فيما يلي عمل كاشف ترميز المبين في الشكل (5-14).

يعمل مسجل الإزاحة على حساب المصحح.



الشكل (5-14) دارة كاشف الترميز

نفترض أن الرمز α'_4 خاطئ $\alpha'_4 = \alpha_4 + 1$ في هذه الحالة n-r=4

تكون حالة المسجل بعد إدخال كافة الرموز للكلمة في مسجل الإزاحة:

$$Z = T^4 U = T^{-3} U$$

عندما يصل الرمز α'_4 إلى آخر خلية للمسجل الرئيسي (Rp) أي بعد نبضتين إضافيتين تكون حالة مسجل الإزاحة ذي التغذية العكسية:

$$T^2T^{-3}U = T^{-1}U$$

أي الحالة $(0,0,1)$ في هذه اللحظة يظهر الرمز 1 المعطى من كاشف الترميز ليجمع مع محتوى الخلية M_0:

$$\alpha'_4 + 1 = \alpha_4$$

تم تصحيح الرمز و يصبح محتوى خلايا المسجل أصفاراً.

5 – 6 الترامیز الكاشفة والمصححة لرزمة (رزمة من الأخطاء)

5-6- 1 إنجاز الترميز وكاشف الترميز لتصحيح رزمة من الأخطاء:

تكون عملية كاشف الترميز بسيطة في حال رزمة من الأخطاء محددة في مكان معين من الكلمة المرمزة و يمكن تمثيلها بمصفوفة:

$$e = [....\alpha_i\ \varepsilon_{i+l}.....\alpha_i\ \varepsilon_{i+\ell-2}\varepsilon_{i+\ell-1}.....] \qquad (5-98)$$

تمثل على شكل كثير حدود نشير إليه بـ $e(x)$

لنفترض رزمة من الأخطاء طولها ℓ تؤثر في الرموز الأولى من الكلمة $V(x)$ أي من $a_0, a_1, a_2 .....a_{\ell-1}$ يشار إليها $b(x)$ وتكتب على الشكل التالي:

$$b(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ...\alpha_{\ell-1}x^{\ell-1} \qquad (5-99)$$

إذا كان باكيت الأخطاء يؤثر في مجموعة من الرموز بدءاً من الرمز a_i في كلمة مرمزة عندئذ تكتب الكلمة الخاطئة

$$e(x) = x^i b(x) \bmod \left(x^n + 1\right) \qquad (5-99-a)$$

حيث أن $e(x)$ باقي القسمة $x^n + 1$ لإنه لا يمكن أن تكون درجته أكثر من $n-1$. إذا تجاوزت $x^i b(x)$ درجة $n-1$ تعود إلى بداية الكلمة الخاطئة.

بسبب البنية الدوري للترميز فهو قادر على أن يصحح هذه الأخطاء أيضاً حيث تعد جزءاً من رزمة الأخطاء. إذاً $b(x)$ يبين بنية الأخطاء ولكن x^i يشير إلى مكان الرزمة في المرمز.

تحدد رموز المراقبة بالعلاقة:

$$C(x) = rest\,\frac{x^{m_t} i(x)}{g(x)} \qquad (5-100)$$

حيث $g(x)$ كثير حدود من الدرجة m_t الشكل (5-15)

تستعمل دارات التقسيم نفسها في كواشف الترميز ولكن الدخل يكون بعد m_t خلية (أي على خرج المسجل) أو بالتالي تكون علاقة المصحح.

$$Z(x) = rest\,\frac{x^{m_t} v'(x)}{g(x)} = rest\,\frac{x^{m_t} e(x)}{g(x)} = rest\,\frac{x^{m_t+i} b(x)}{g(x)} \qquad (5-101)$$

يكون المصحح مخزناً في المسجل بعد استقبال كامل الكلمة المرمزة (في الحقيقة يعين المصحح بمعرفة $rest\,\frac{v'(x)}{g(x)}$) ولكن يعين المصحح بشكل عام بالعلاقة:

$$rest\ \frac{x^{m_t} v'(x)}{g(x)} \qquad (5-101-a)$$

5-6-2 تقنية كشف الأخطاء:

إذا أدخلنا $V(x)$ ضمن مسجل إزاحة بعد P خلية يكون الباقي

$$S_{p.n}(x) = rest\ \frac{x^P V(x)}{g(x)} \qquad (5-102)$$

يشار إلى الباقي $S_n(x)$

$$S_n(x) = rest\ \frac{V(x)}{g(x)} \qquad (5-103)$$

ينتج من العلاقتين السابقتين:

$$S_{p.n}(x) = rest\ \frac{x^P S_n(x)}{g(x)} \qquad (5-104)$$

في الحقيقة لدينا:

$$x^P V(x) = q(x)g(x) + S_{p.n}(x) \qquad (5-105)$$

$$V(x) = S(x)g(x) + S_n(x) \qquad (5-106)$$

حيث $S(x), q(x)$ هما الباقي لكثيرات الحدود من العلاقات السابقة:

$$x^p\left[S(x)g(x) + S_n(x)\right] = q(x)g(x) + S_{p.n}(x) \qquad (5-107)$$

أو:

$$x^P S_n(x) = g(x)\left[x^P S(x) + q(x)\right] + S_{p.n}(x) \qquad (5-108)$$

عندئذ:

$$S_{p.n}(x) = rest\ \frac{x^P S_n(x)}{g(x)} \qquad (5-109)$$

في العلاقة(5−102) و (5−103) نبدل كثير الحدود $V(x)$ بكثير الحدود $b(x)$ ولكن $P = m_t + i$ فنحصل على:

$$S_{p.n}(x) = Z(x) = rest\ \frac{x^{mt+i} b(x)}{g(x)} \qquad (5-110)$$

$$S_n(x) = rest\ \frac{b(x)}{g(x)} \qquad (5-111)$$

إذا $\ell \le m_t$ لدينا $S_n(x) = b(x)$ ندخل هذه القيمة بالعلاقة (5−104) لنحصل على:

$$Z(x) = rest\ x^{mt+i} \quad b(x)/g(x) \qquad (5-113)$$

وبناءً على التكافؤ بين (5−104) والعلاقة $S_{p.n} = \tau^P S_n$ ، يمكن كتابتها على شكل مصفوفة

$$Z = \tau^{m_t+i} b \qquad (5-114)$$

حيث Z,b مصفوفات من عمود واحد و m_t صف

$$b=\begin{bmatrix}\alpha_0\\ \varepsilon_1\\ .\\ .\\ \alpha_{\ell-1}\\ 0\\ .\\ .\end{bmatrix} \qquad Z=\begin{bmatrix}Co\\ C_1\\ .\\ .\\ .\\ .\\ .\\ C_{m_t}-1\end{bmatrix} \qquad (5-115)$$

مما سبق نستنتج أن المرمز قادر على كشف رزمة من الأخطاء ذات طول أعظمي $\ell = m_t$، في هذه الحال الباقي $rest\, b(x)/g(x)=t(x)$ إذا $b(x)$ لا يساوي الصفر، أي إزاحة دورية $b(x)$ سوف تختلف أيضاً عن الصفر أي أن $Z\neq 0$، هذا يعني وجود أخطاء.

يجب الإشارة إلى أن العلاقة البسيطة (5-114) بين المصحح ورزمة الأخطاء تشير إلى وجود الأخطاء على طول $\ell \le m_t$.

يتبين مما سبق لنا أنه بعد n نبضة تكون الكلمة المستقبلة قد دخلت إلى المسجل ويخزن باقي تقسيم $V'(x)$ على $g(x)$ هو $Z(x)$ في المسجل ويساوي إلى $b(x)$ مزاح m_t مرة.

5-6-3 تقنية تصحيح الأخطاء:

تحدد بنية رزمة الأخطاء ومكانها بمعرفة المصحح $Z(x)$ يلي ذلك بأن مرمزاً قادراً على تصحيح رزمة أخطاء ذات طول ℓ يجب أن يكون $m_t \ge 2\ell$، لنفترض رزمة أخطاء طولها ℓ تؤثر في ℓ رمزاً $a'_i, a'_{i+1}....a'_{i+\ell-1}$، تكون الكلمة المستقبلة :

$$V'(x) = a'_o + a'_1 x + ...a'_i x^i + ...a'_{i+\ell-1} x^{i+\ell-1} ....a'_{m-1} x^{n-1}$$

من هذه الحالة:

$$e(x) = x^i \left(\alpha_o + \varepsilon_1 x + ... + \alpha_{\ell-1} x^{\ell-1}\right) = x^i b(x) \qquad (5-116)$$

يحسب المصحح من المسجل طبقاً للعلاقات السابقة (5-101)، (5-114) بعد ذلك يتم تفريغ المسجل الشكل (5-15).

يصل أول رمز خاطئ $a'_{i+\ell-1} = a_{i+\ell-1} + 1$ إلى آخر خلية m_t للمسجل بعد (r) نبضة. العدد (r) يساوي إلى عدد الرموز الصحيحة التي تسبق $a'_{i+\ell-1}$ أي:

$$r = n-1-(i+\ell-1)n = \ell \qquad (5-117)$$

يكون محتوى المسجل، بعد إدخال $V'(x)$ هو $Z = Z^{m_t+i} b$ ويصبح بعد $r = n-i-l$ نبضة (أي عندما أول رمز خاطئ يكون قد وصل إلى آخر (M) للمسجل.

$$Z = \tau^r z = \tau^{n-i-\ell} \tau^{m_t+i} b = \tau^{m_t-\ell} b \qquad (5-118)$$

يمثل مسجل الإزاحة ذو التغذية العكسية بكثير الحدود المولد $g(x)$ من الدرجة m_t الذي يولد (n) دورة ، إذاً $\tau^n = I$ (المصفوفة الأحادية).

يمكن كتابة العلاقة (5-118) كعلاقة بين كثيرات حدود

$$Z_c(x) = rest\,\frac{x^{m_t-\ell}b(x)}{g(x)} \qquad (5\text{-}119)$$

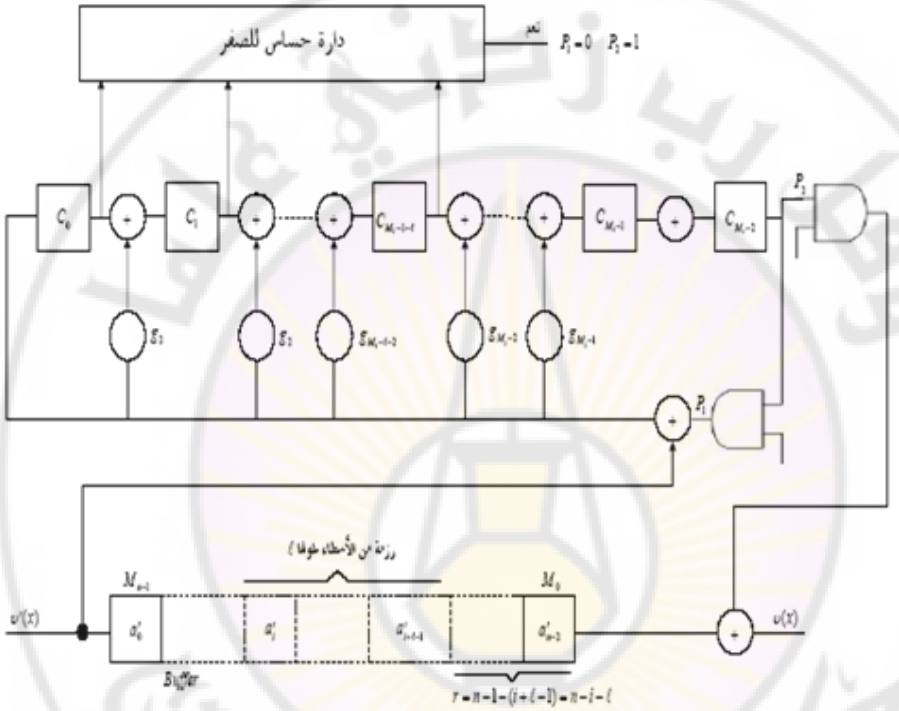
وبما أن درجة $X^{m_t-\ell}b(x)$ أكبر ما يمكن m_{t-1}، يمثل الناتج $Z_c(x) = x^{mt-\ell}b(x)$ بحيث تحتوي $Co, C_1 \ldots C_{mt-\ell-1}$ على "0" والبقية من الخلايا $C_{mt-\ell}, C_{m_{t1}}, \ldots C_{mt-1}$ تحتوي على ثوابت $b(x)$.

تتحسس هذه الحالة الدارة المنطقية المبينة في الشكل (5-15) , تقطع البوابة P_1 (لن تمرر رموزاً) وتوصل البوابة P_2. تكون دارة الحساس المنطقية فعالة فقط بعد حساب المصحح $Z(x)$.

يتم تعريف رزمة الأخطاء $b(x)$ المخزنة ضمن الخلايا ℓ الأخيرة للمسجل من خلال توصيل البوابة P_2، وتجمع ثنائياً مع رموز الكلمة الخاطئة $v'(x)$ و تتم عملية التصحيح باختيار كثير الحدود $g(x)$ من الدرجة m_t والطول الأعظمي ℓ لرزمة الأخطاء التي يمكن تصحيحها يخضع Z_C لقيود وناتجة عن تشكيله بحيث أن المسجل يمر مرة واحدة في الحالة التي فيها الخلايا الأولى $m_t - \ell - 1$ "صفر",الحالة هذه تتحسس لها الدارة المنطقية الحساسة للصفر.

من أجل القيم الكثيرة n و ℓ لعينات معينة $(b(x))$ هذا العمل ليس دائماً ممكناً ويمكن أن يكون التصحيح خاطئاً، من خلال برنامج معين يمكن إيجاد عائلة من كثيرات الحدود المولدة حيث التصحيح الخاطئ يمكن أن يكون أقل ما يمكن

في الجدول I من الملحق جـ يوجد عدد من كثيرات الحدود المرمزة ذات معدل $\frac{k}{n}$ ، ونسبة $\frac{\ell}{n}$ وعدم الكفاءة $i - m_t - 2\ell \geq 0$.



الشكل (5-15) كاشف ترميز تقنية تصحيح رزمة (باكيت) من الأخطاء

تكون التراميز المصححة لرزم من الأخطاء قادرة على كشف أخطاء غير قابلة للتصحيح. إذاً الحالات m_t لا تحتوي جميعاً مرة واحدة على "الصفر". الخطأ الذي لا يمكن تصحيحه يمكن كشفه.

5-7 تراميز فاير *(FIRE)*:

يمكن تحديد معاملات ترميز فاير دون الحاجة إلى برنامج على الحاسب وكثير الحدود المولد من الدرجة m_t مشكل من عاملين يقسمان كثير الحدود $X^n + 1$.

$$g(x) = q(x) \cdot P(x) \qquad (5-120)$$

حيث أن بنية هذا الترميز سوف تخضع إلى الأمور التالية:

عملية الترميز تبقى من دون أي تغيير

$$C(x) = rest\, x^{mt} i(x) / g(x) = rest\, x^{mt} i(x) / q(x) \cdot p(x) \qquad (5-121)$$

أما في حالة كشف الترميز فيمكن استخدام المخطط في الشكل (5-15) من أجل إيجاد بنية $P(x)$ الذي يسمح بسهولة تحديد طول الكلمة المرمزة n نختار $P(x)$ كثير الحدود الأولي الذي يولد الدورة دورتها العظمى $Z^P - 1$ حيث درجة كثير الحدود $P(x)$ ينتج من ذلك أن n، يجب أن تكون من مضاعفات $2^P - 1$.

كثير الحدود $q(x)$ نختار كبنية بسيطة $q(x) = x^Q + 1$ دورته Q، في هذه الحالة المسجل يقوم بعملية الإزاحة فقط. حيث $q(x)$ يكون قاسماً لكثير الحدود $x^n + 1$. n يجب أن يكون المضاعف المشترك البسيط للمعاملين $2^P - 1$، Q. إذا $2^P - 1$ و Q هما عددان أوليان نسبياً حينئذ يمكن كتابة العلاقة:

$$n = (2^P - 1)Q \qquad (5-122)$$

فيما يلي سوف نتحدث عن المخطط الموجود في الشكل (5-16) حيث لدينا مسجلان للتقسيم. المسجل P يقسم كثير الحدود $P(x)$ من الدرجة P، والمسجل Q يقسم كثير الحدود $q(x)$ من الدرجة Q. $P+Q=m_t$ (يساوي إلى عدد رموز المراقبة).

لتحديد درجة P و Q. بدلالة الطول ℓ لرزمة الأخطاء بقيم محتوى المسجلين P و Q في الشكل (5-16).

بعد إدخال $V'(x)$ يكون محتوى المسجل P

$$z_p(x)=rest\, x^P V'(x)/P(x)=rest\, x^P e(x)/P(x)=rest\, x^{P+i}b(x)/P(x) \quad (5\text{-}123)$$

أي أن باقي $b(x)/P(x)$ مزاح $(P+i)$ مرة.

إذاً:

$$rest\, b(x)/P(x)=b(x), P\geq \ell \quad (5\text{-}124)$$

إذاً:

Z_P يساوي b بإزاحة $p+i$ مرة

$$Z_P=\tau_P^{P+i}\cdot b \quad (5\text{-}125)$$

نختار $P=\ell$ إذاً:

$$Z_P = \tau_P^{\ell+i}\ b \qquad (5-126)$$

محتوى المسجل Q

$$Z_q(x) = rest\ x^P V'(x)/q(x) = rest\ \frac{x^P e(x)}{q(x)} = rest\ \frac{x^{P+i} b(x)}{q(x)} \qquad (5-127)$$

(الدخل إلى المسجل Q يتم بعد $P = \ell$ خلية)

إذ كان $Q \geq \ell$ حينئذٍ Z_q يساوي إلى b بإزاحة مرة

$$Z_q = \tau_q^{\ell+i} b \qquad (5-128)$$

حيث أن المصفوفة b تكمل بأصفار حتى يصبح عدد سطورها Q، بما أن المسجل Q له وصلة فقط بين الدخل والخرج (بين C_0, C_{Q-1}) هذا المسجل ينفذ عملية كشف الترميز (أي كشف b دون أن يغير أي شيء لنفترض رزمة الأخطاء طولها $P = \ell$ تؤثر في الرموز ℓ التالي:

$$a'_i, a'_{i+1} \ldots . a'_{i+\ell-1}$$

$$e(x) = x^i \left[\alpha_o + \varepsilon_1 x + \ldots . . \alpha_{\ell-1} x^{\ell-1}\right] = x^i\ b(x) \qquad (5-129)$$

أول رمز خاطئ $a'_{i+\ell-1}$ يصل إلى آخر خلية للمسجل بعد $r=n-\ell-i$ نبضة العلاقة(117−5)، محتوى المسجل Pسوف يكون

$$Z_{P_C}=\tau_P^r Z_P=\tau_P^{n-\ell-i} Z_P=\tau_p^{\ell-i} Z_P=\tau_P^{-\ell-i} \tau_P^{\ell+i} b=b \qquad (5\text{-}130)$$

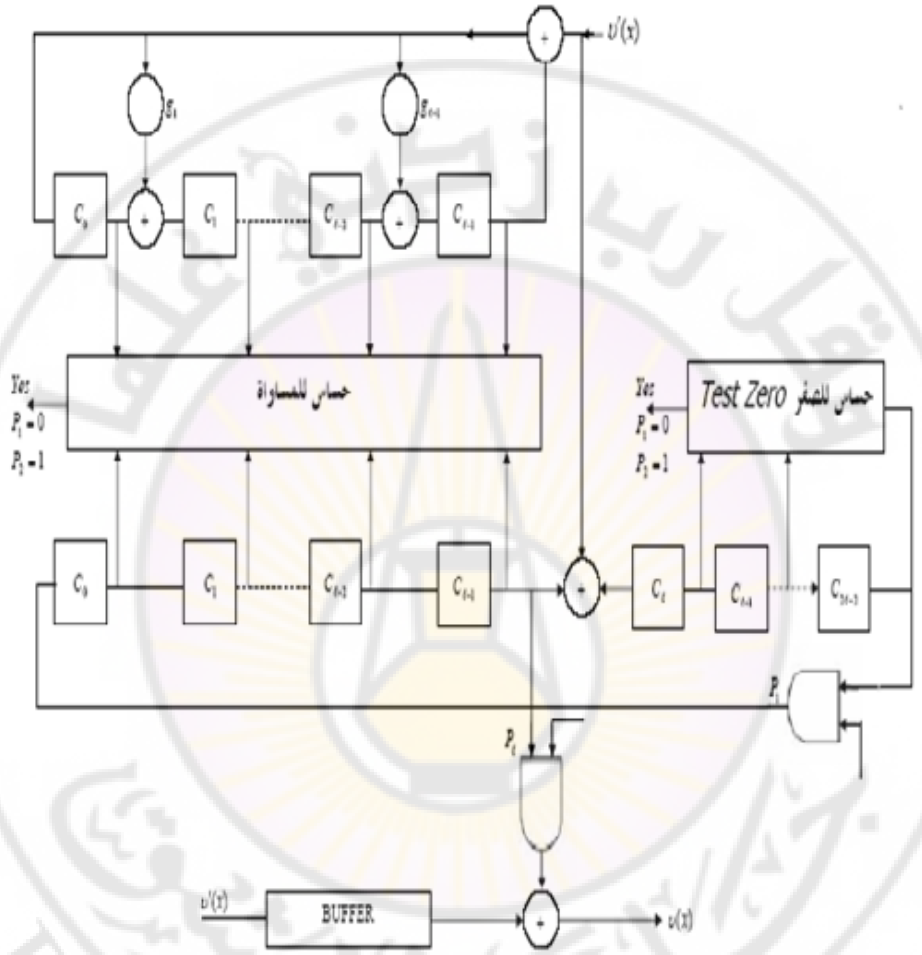
محتوى المسجل Q يكون

$$Z_{qc}=\tau_q^r Z_q=\tau_q^{n-\ell-i} \tau_q^{\ell+i}.b=b \qquad (5\text{-}131)$$

إذاً الخلايا الأولى $P=\ell$ من المسجل Q تحتوي على b.

الدارة المنطقية لاختبار المساواة تشير إلى هذه المساواة بين محتوى المسجلين. اختبار المساوة ليس كافياً ليضمن وجود رزمة الأخطاء b في الخلايا $C_0C_1....C_{\ell-1}$ بسبب أن المسجل P يولد جميع الحالات، لذا فيمكن أن يولد حالة

بحيث يوجد قسم من رزمة الأخطاء في الخلايا $C_0\, C_1 .... C_{\ell-1}$ للمسجل Q.



الشكل (5-16) كاشف ترميز فاير

إذا وجد b كاملاً في الخلايا $C_0 C_1 .... C_{\ell-1}$ فبقية الخلايا $C_\ell .... C_{Q-1}$ يجب أن تحتوي على أصفار، هذه الحالة تتحسس لها الدارة المنطقية.

لتحديد العدد الأصغري لخلايا المسجل Q أي درجة $q(x)$ نفترض بنية خاصة لرزمة الأخطاء b ذات طول أعظمي.

$$b(x) = \alpha_0 + \alpha_{\ell-1}\, x^{\ell-1} \qquad (5\text{-}131)$$

$$\alpha_0 = \alpha_{\ell-1} = 1 \qquad (5\text{-}131\text{-}a)$$

لنعد هذه الرزمة أثناء تشكيل $Z(x)$ تزاح في المسجل المقترح ذي $Q = 2\ell - 1$ خلية بحيث أن أول رمز خاطئ $\alpha_{\ell-1}$ يصل إلى الخلية $\alpha_{2\ell-1}$ (آخر خلية من Q) V' آخر رمز خاطئ سيوجد في الخلية $C_{\ell-1}$.

في هذه الحالة المفروضة بما أن المسجل يولد جميع الحالات الممكنة $(2^P - 1)$ ما عدا الحالة "صفر" يمكن أن يحدث اختبار التساوي متطابقاً.

ولكن بما أن $\alpha_{\ell-1}$ توجد في آخر خلية $C_{2\ell-2}$ فاختبار "الصفر" ليس مطابقاً والبوابة P_2 تبقى مغلقة، ولكن إذا كان المسجل Q يحوي أقل من الرمز $\alpha_{\ell-1} = 1$ فيمكن أن ننتقل إلى الخلية C_O وبجانب التطابق الممكن لاختبار المادة نبين اختبار "الصفر" وبشكل خاطئ تفتح البوابة P_2.

ينتج من ذلك أن عدد خلايا المسجل Q يجب أن يكون $2\ell - 1$ ودرجة كثير الحدود $q(x)$.

$$Q = 2\ell - 1 \qquad (5\text{-}132)$$

5 – 8 الترميز بمسجل إزاحة ذي K خلية:

دارة الترميز التي تم شرحها سابقا تبين أن الكلمة المرمزة هي عنصر في مولد لكثير حدود g(x) من الدرجة m

سنشرح طريقة على أساس أن الكلمة المرمزة هي عنصر في الفراغ "صفر" للمثالي المولد لكثير الحدود $h(x)$ من الدرجة K المبينة في العلاقة (5−20−b)

$$v(x)\cdot h(x) = q(x)(x+1) = x^n q(x) + q(x) \qquad (5\text{-}133)$$

وبما أن درجة $z(x)$ هي $K-1$ أو أقل من القوى $x^k, x^{k+1}, ..., x^{n-1}$ فلن يظهر الجداء $v(x)*h(x)$ إذا أمثال هذه القوى يجب أن تكون معدومة (تساوي الصفر).

$$\sum h_i a_{n-i-j} = 0 \qquad 1 \le j \le m \qquad (5\text{-}134)$$

حيث: $h_0 = 1, h_k = 1$

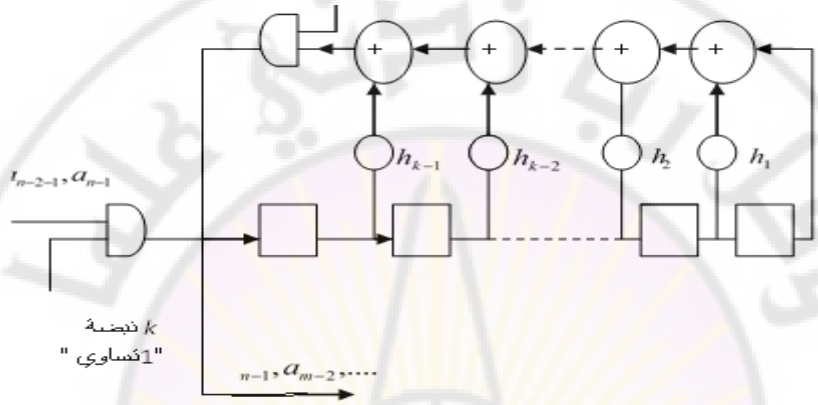
من العلاقة السابقة نحصل على:

$$a_{m-j} = \sum_{i=0}^{k-1} h_i a_{n-i-j} \qquad 1 \le j \le m \qquad (5\text{-}135)$$

حيث: a_{m-j} هي رموز مراقبة ولكن a_{n-i-j} هي رموز معلومات.

هذه العلاقة مبينة في الشكل (5−17) وهذه الدارة معروفة باسم دارة

ترميز بمسجل إزاحة ذي K خلية: *K Stag Shift Register Encoding Circuit*



الشكل (5-17) . مرمز على أساس كثير الحدود h(x)

5 – 9 الترميز لتصحيح أخطاء مضاعفة:

درسنا سابقاً تصحيح الخطأ وتم اختيار كثير حدود مولد من الدرجة m أولي الذي يولد حقل (Galois) مكون من $n = 2^m - 1$ عنصراً لا تساوي الصفر حيث n عدد الرموز للكلمة المرمزة V(x). وبمعنى آخر يولد المسجل الترميز دورة طولها أعظمي n فإن أضفنا بنفس العدد n لرموز الكلمة ولكن نرغب أن نصحح عدد أخطاء هنا سنشير لعدد رموز المراقبة M ومن الطبيعي سنقلل من عدد رموز المعلومات K بحيث يبقى (n=M+k) بزيادة M.

M>m يزداد عدد المصححات Z (يصبح عدداً من $2^M - 1$) الذي سيقابل عدد الكلمات الخاطئة وبالتالي تزداد مقدرة التصحيح للمرمز لكن طول الدورة يجب أن يبقى $n < 2^M - 1$ فينتج في هذه الحالة كثير الحدود والمولد g(x) ولا يمكن أن يكون أولياً حيث أنه في هذه الحالة سوف نحصل على:

$$n' = 2^M - 1 > n$$

5 – 9 – 1 تعيين كلمات الترميز من خلال جذور كثير الحدود للمولد:

كانت الكلمة سابقاً عبارة عن عنصر للمثالي *ideal* المولد من *g(x)*

$$V(x) = q(x)g(x) \qquad (5\text{-}136)$$

أو عنصر في الفراغ (صفر) للمثالي المولد لكثير الحدود *h(x)*

$$V(x)h(x) = 0 \qquad (5\text{-}137)$$

يكون الشكل المكافئ لتعيين الكلمات المرمزة على الشكل التالي.

كثير الحدود *v(x)* من الدرجة $n-1$ هو كلمة مرمزة إذا وفقط إذا كانت له جذور هي جذور *g(x)* وبالتالي فإن كثير الحدود *g(x)* هو مقسم لكثير الحدود *v(x)* الذي هو المثال (ideal) ل *g(x)*

وطبقا للعلاقة (5 – 6) كثير الحدود *g(x)* هو مقسم لكثير الحدود المولد $x^n + 1$ (الذي يطلق عليه اسم الجبر وعناصره هي كلمات ذات معنى ومن دون معنى) وينتج أن جذور *g(x)* هي جذور *v(x)* وهي جذور لكثير الحدود $x^n + 1$ أيضا

والعكس إذ كان لدينا مرمز لكلمات طولها n ونريد تعيين كثير الحدود المولد أي كلمات الترميز نختارها بناء على القواعد التالية ,ليكن r جذر لكثير الحدود $x^n + 1$ ونشكل كثير حدود الذي له الجذور نفسها والذي سيكون كثير الحدود المولد ,إن الجذور r المختارة هي جذور كثير الحدود المولد وهي جذور للكلمة *v(x)*.

طبقا لنظرية "كثير الحدود $x^n + 1$ حيث $n = 2^n - 1$ له جذور كل العناصر التي لا تساوي الصفر للحقل 2^m بعدد $n = 2^n - 1$" فالجذور (β_i)

لكثير الحدود x^n+1 هي عناصر α_i من $GF(2^m)$ مولدة من كثير الحدود الأولي $q(x)$ من الدرجة m (على اعتبار أن $g(x)$ أصبح هنا غير أولي)

$$\beta_0 = 1, \beta_1 = \alpha, \beta_2 = \alpha^2, ..., \beta_{n-1} = \alpha^{n-1} \qquad (5-138)$$

حيث هذه العناصر هي عبارة عن مصفوفات.

لنفترض أن الكلمة المرمزة:

$$v(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} \qquad (5-139)$$

ولها من خلال جذور العناصر $\beta_{i1}, \beta_{i2}, ..., \beta_{ir}$ للحقل $GF(2^m)$ بالتبديل في العلاقة (5−139) نحصل على:

$$v(\beta_{ik}) = \alpha_0 \beta_{ik}^{\ 0} + \alpha_1 \beta^1{}_{ik} + ... + \alpha_{n-1} \beta_{ik}^{\ n-1} = 0 \qquad (5-140)$$

من أجل $\beta_i^{\ 0} = 1$; $k = \overline{1-r}$

يمكن كتابة العلاقة (5−140) على شكل مصفوفة:

$$\left[\beta_{ik}^{\ 0} \quad \beta_{ik}^{\ 1} \quad ... \quad \beta_{ik}^{\ n-1}\right]\left[a_0 \quad a_1 \quad ... \quad a_{n-1}\right]^T = 0 \qquad (5-141)$$

ونشير:

$$H = \begin{bmatrix} \beta_{i_1}^0 & \beta_{i_1}^1 & ... & \beta_{i_1}^{n-1} \\ \beta^0{}_{i2} & \beta_{i2}^{\ 1} & ... & \beta_{i_2}^{n-1} \\ : & : & : & : \\ \beta_{i_r}^0 & \beta_{i_r}^1 & ... & \beta_{i_r}^{n-1} \end{bmatrix} \qquad (5-142)$$

فالعلاقة (5−141) يمكن كتابتها على الشكل التالي:

$$Hv^T = 0 \qquad (5-143)$$

أي نحصل على علاقة الترميز.

. كثير الحدود $m_i(x)$ من الدرجة الصغرى بأمثال في حقل $GF(2)$ والذي له جذر هوعنصر في $\beta_i \in GF(2^m)$ يسمى كثير حدود أصغرياً لـ β_i

. أي عنصر $\beta_i \in GF(2^m)$ له كثير حدود أصغري من المرتبة "الدرجة " m أو أقل.

إذاً كثير حدود $v(x)$ ذو أمثال من $GF(2)$ له جذر β_i حينئذ $v(x)$ يقسم على $m_i(x)$ ، كثير الحدود الأصغري لـ β_i. إذاً ما يقابل r جذر β_i سيكون لدينا r كثيرات حدود أصغرية $m_i(x)$ التي تقسم $v(x)$ على العموم ليست جميع كثيرات الحدود هذه هي كثيرات الحدود منفصلة أصغر مضاعف مشترك لكثيرات الحدود هذه يقسم به $v(x)$

$$g(x) = L.C.M.\, m_1(x) \quad m_2(x) \quad .... \quad m_n(x) \qquad (5-144)$$

هو عبارة عن كثيرالحدود المولد الذي يلائم $v(x)$.

مسألة اختيار r جذر بحيث يمكن للترميز أن يصحح e خطأ سيتم معالجتها فيما يلي.

سيتم فيما يلي معالجة مشكلة اختيار r جذر بحيث يمكن للترميز أن يصحح e خطأ

5 – 9 – 2 الترميز Bose – chaud huri. Hocquenghem (B.C.H)

يمكن إثبات أنه باختيار $\beta_{i_1} = \alpha, \beta_{i_2} = \alpha^3, ..., \beta_{i_r} = \alpha^{2e-1}$

نحصل على ترميز قادر على تصحيح e خطأ مستقل في هذه الحالة المصفوفة H المعطاة في العلاقة (142–5) تصبح

$$H=\begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \dots & \alpha^{n-1} \\ \alpha^0 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^0 & \alpha^{2e-1} & \alpha^{(2e-1)^2} & \dots & \alpha^{(2e-1)(n-1)} \end{bmatrix} \qquad (5\text{-}145)$$

ببرهان النظرية نبين أنه $q \le 2e$ عامود من هذه المصفوفة يكون مستقلات وفي هذه الشروط الترميز الناتج قادر أن يصحح e خطأ أو أقل.

تسمى التراميز التي تشكل رموزها المصفوفة H السابقة بتراميز B.C.H.

مثال:

لنفترض كلمة مرمزة طولها (15) وطبقا لنظرية فإن $n = 2^n - 1$ ولتصحيح $e = 3$ فإن كثير الحدود المولد سيكون:

$$\alpha, \alpha^3, \alpha^{2e-1} = \alpha^5$$

وبما أن $m = 4 \Leftarrow n = 2^n - 1 = 15$

أي أن جذور $x^{15}+1$ وعناصر $GF(2^4)$ تكون مولدة بكثير حدود أولي من الدرجة 4 كما في حال: $q(x) = 1 + x + x^4$

ولتحديد كثيرات الحدود الأصغرية (التي لا يمكن تحليلها (تفكيكها)) سنقوم بما يلي:

كثير الحدود الأصغري $m_1(x)$ للعنصر α له الجذور التالية:

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16} = \alpha$$

إذا هو كثير حدود من الدرجة 4

$$m_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$$

نقوم بإجراء عملية الضرب وبناء على الجدول

$$m_1(x) = 1 + x + x^4$$

كثير الحدود ألأصغري لـ α^3 هو $m_3(x)$ وله الجذور:

$$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$$

كذلك هو من الدرجة 4 ويتم تحديده بالطريقة نفسها السابقة

$$m_n(x) = 1 + x + x^2 + x^3 + x^4$$

$$\{ m_3(x) = (x + \alpha^3)(x + \alpha^6)(x + \alpha^{12})(x + \alpha^9) \}$$

كثير الحدود ألأصغري لـ α^5 له الجذور التالية:

$$\alpha^5, \alpha^{10}, \alpha^{20} = \alpha^5, \alpha^{40} = \alpha^{10}$$

إذا كثير حدود من الدرجة الثانية:

$$m_5(x) = 1 + x + x^2$$

إذا كثير الحدود المولد:

$$g(x) = m_1(x)m_3(x)m_5(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)(1 + x + x^2)$$

من الدرجة 10 إذا" $K=5$, $M=10$

يمكن أن نصل إلى النتيجة نفسها فيما لو استخدمنا مفهوم المصفوفة α^i المعطى في الجدول (5 – 3) كثير الحدود الأصغري يمكن أن يكتب على الشكل التالي:

$$m(x) = 1.x^0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \alpha_4 x^4$$

ولتحديد $m_1(x)$ من الدرجة 4 اذا $(a_4 = 1)$ نطبق واحدة من جذور $(\alpha, \alpha^2, \alpha^4, \alpha^8)$ مثال α وسيكون لدينا:

$$m_1(\alpha) = 1\alpha^0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^4 + \alpha^8 = 0$$

واعتمادا على الجدول:

$$\begin{bmatrix}0\\0\\0\\1\end{bmatrix}+a_1\begin{bmatrix}0\\0\\1\\0\end{bmatrix}+a_2\begin{bmatrix}0\\1\\0\\0\end{bmatrix}+a_3\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\1\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\end{bmatrix}$$

حيث: $a_1=1, a_2=0, a_3=0$

إذاً

$m_1(x)=1+x+x^4$

قوى α	فئـــــات البـــــاقي للنمـــــوذج $q(x)=1+x+x^4$	تمثيل المصفوفة $[\alpha]^T$
α^0	1	0 0 0 1
α	α	0 0 1 0
α^2	α^2	0 1 0 0
α^3	α^3	1 0 0 0
α^4	$\alpha+1$	0 0 1 1
α^5	$\alpha^2+\alpha$	0 1 1 0
α^6	$\alpha^3+\alpha^2$	1 1 0 0
α^7	$\alpha^3+\alpha+1$	1 0 1 1
α^8	α^2+1	0 1 0 1
α^9	$\alpha^3+\alpha$	1 0 1 0
α^{10}	$\alpha^2+\alpha+1$	0 1 1 1
α^{11}	$\alpha^3+\alpha^2+\alpha$	1 1 1 0
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1 1 1 1
α^{13}	$\alpha^3+\alpha^2+1$	1 1 0 1
α^{14}	α^3+1	1 0 0 1
α^{15}	1	0 0 0 1

الجدول (5 – 3)

وبشكل مماثل نحدد أمثال كثيرات الحدود الأصغرية $m_3(x), m_5(x)$:

$$m_3(\alpha) = 1\alpha^0 + a_1\alpha^3 + a_2\alpha^6 + a_3\alpha^9 + a_4\alpha^{12} = 0$$

$$\begin{bmatrix}0\\0\\0\\1\end{bmatrix} + a_1\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + a_2\begin{bmatrix}1\\1\\0\\0\end{bmatrix} + a_3\begin{bmatrix}1\\0\\1\\0\end{bmatrix} + \begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix}$$

$$\begin{aligned} a_1 + a_2 + a_3 + 1 &= 0 \\ a_2 + 1 &= 0 \\ a_3 + 1 &= 0 \end{aligned}$$

$$m_3(x) = 1 + x + x^2 + x^3 + x^4$$

وبشكل مماثل نحدد أمثال كثيرات الحدود الأصغرية $m_3(x), m_5(x)$:

$$m_3(\alpha) = 1\alpha^0 + a_1\alpha^3 + a_2\alpha^6 + a_3\alpha^9 + a_4\alpha^{12} = 0$$

$$\begin{bmatrix}0\\0\\0\\1\end{bmatrix} + a_1\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + a_2\begin{bmatrix}1\\1\\0\\0\end{bmatrix} + a_3\begin{bmatrix}1\\0\\1\\0\end{bmatrix} + \begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix}$$

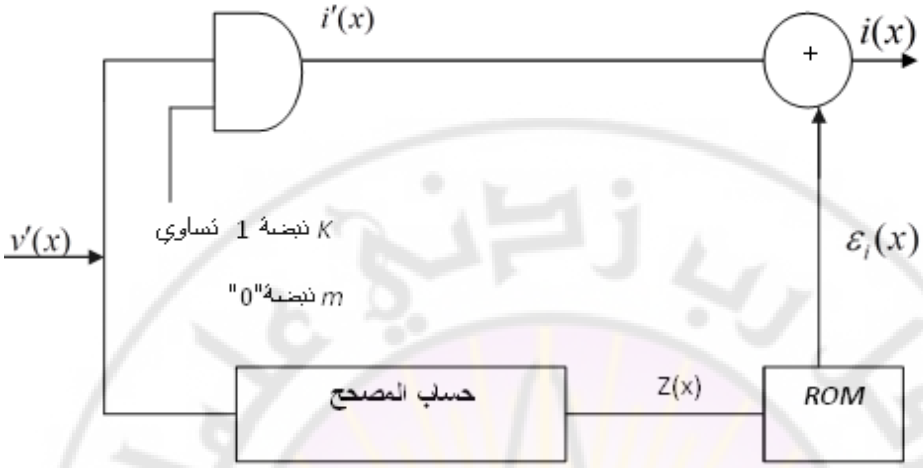
$$a_1 + a_2 + a_3 + 1 = 0$$
$$a_2 + 1 = 0$$
$$a_3 + 1 = 0$$

$$m_3(x) = 1 + x + x^2 + x^3 + x^4$$

لإجراء عملية الترميز ليس من الضروري أن نستعمل المصفوفة H المعطاة في المعادلة (5-145) ولكن من المفيد أن نلاحظ أنه في المثال لدينا عامود مشكلة من العناصر $\propto^3 ; \propto^2 ; \propto$ وسيكون لدينا 3×4=12 صف بدلاً من 10، عدد رموز المراقبة ينتج من ذلك أن صفين من هذه المصفوفة مستقلان فعليا" أي يمكن تشكيلهما من مجموع الصفوف الأخرى.

عملية الترميز يمكن إنجازها بدارة التقسيم المبينة في الشكل (5-4) أو بمسجل إزاحة ذي تغذية عكسية كما في الشكل (5-10) كثير الحدود المولد g(x) معطى في العلاقة (5-144).

من أجل كاشف ترميز (B.C.H) هناك عدة خوارزميات ولكن أبسط طريقة هي التي تقوم على أساس التقابل بين المصحح والكلمة الخاطئة المخزنة في الذاكرة لاستخدام ذاكرة بسعة صغيرة يمكن استخدام الدارة التالية:



الشكل (5–18) كاشف ترميز B.C.H

حيث يتم تصحيح رموز المعلومات المستقبلة $i'(x)$ فقط وفي هذه الحالة في الذاكرة *ROM* ندخل عدداً أقل من الكلمات الخاطئة من طول أقل يساوي إلى K ويشار إليه $\varepsilon_i(x)$

ففي المثال السابق عدد المصححات $1023 = 2^{10} - 1$ عدد الكلمات الخاطئة المشكلة في1, 2 و3 أخطاء ويكون:

$$C_{15}^{1} + C_{15}^{2} + C_{15}^{3} = 575$$

إذاً هذا المرمز ليس كاملاً (تاماً) عدد الأخطاء المصححة أقل بكثير من عدد المصححات.

5 – 9 –3 ترميز *Golay*

ترميز جولاي و ترميز هامينغ المصحح لخطأ واحد هما التراميز الوحيدة الثنائية المصححة للأخطاء الكاملة التامة.

معاملات ترميز جولاي M=11 , k=12 , n=23 يمكن أن يصحح 3 أخطاء أو أقل

إنه ترميز تام طالما أن عدد المصححات يساوي عدد الكلمات

$$C_{23}^{1}+C_{23}^{2}+C_{23}^{\ 3}=2^{11}-1 \qquad (5\text{-}146)$$

حيث $n=2^{11}-1$ مصحح لا يساوي الصفر مولدات من كثير حدود أولي q(x) من الدرجة m=11 إذا أشرنا لـ α عنصر أولي من الحقل $GF(2^{11})$ المولد من $q(x)$ عندئذ $\alpha^{N}=1$

يتم تعيين الكلمات المرمزة $v(x)$ بناء على الجذر $\beta=\alpha^{i}\in GF(2^{11})$ الذي هو جذر كثير الحدود المولد $g(x)$ في نفس الوقت

بما أن β_i هو جذر لكثير الحدود $g(x)$ هو أيضاً جذر لكثير الحدود x^n+1 أي أن:

$$(\alpha^{i})^{n}=1 \Leftarrow \beta^{n}=1$$

حيث: $i=\dfrac{N}{n}$

$$i=\frac{N}{n}=\frac{2^{11}-1}{23}=89 \qquad (5\text{-}147)$$

ليكن لدينا عدد أصغري من رموز المراقبة نضع الشرط $g(x)$ أن يكون كثير حدود أصغري لـ $\beta=\alpha^{89}$

وبما أن كثير الحدود الأصغري ليس له جذور (غير قابل للتفكيك) وطبقا للنظرية في الملحق يكون لدينا الجذور:

$$\beta\ ,\beta^{2},\beta^{4},\beta^{8},\beta^{16},\beta^{32},\beta^{36}=\beta^{13},\beta^{26}=\beta^{3},\beta^{6},\beta^{12},\beta^{24}=\beta$$

كثير الحدود الأصغري $g(x)$ له 11 جذر منفصل وهو من الدرجة M=11

ومن جدول فئات الباقي $q(x)$ من الدرجة $m=11$ والتقنية المبينة في المثال السابق نجد كثير الحدود الأصغري للعنصر $\beta = \alpha^{89}$ وذلك باختيار عشوائي لـ $q(x)$ يمكن أن نكتب:

$$g_1(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11} \qquad (5-148)$$

حيث

$$g_2(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11} \qquad (5-149)$$

عندئذ

$$x^{23} - 1 = (1+x)g_1(x)g_2(x) \qquad (5-150)$$

لإجراء عملية كشف الترميز يمكن استخدام طريقة التقابل بين المصححات و الكلمات الخاطئة المبينة في الشكل السابق وبما أن العنصر β هو جذر $v(x)$ من الدرجة $n-1$ لدينا $v(\beta) = 0$ يمكن أن نكتب العلاقة:

$$HV^T = 0$$

حيث: $H = \left[\beta^0 \quad \beta^1 \quad \ldots \quad \beta^{n-1}\right]$

العناصر β^i للمصفوفة H تمثل بمساعدة الجدول لفئات الباقي من النموذج $q(x)$ كمصفوفة عامودية $M=11$ عنصراً.

يمكن أن نبين 6 أعمدة أي كانت من المصفوفة H هي مستقلة خطياً أي أن الترميز يمكن أن يصبح $e=3$ خطأ.

5 – 10 تراميز ريد– سولومون (*REED – SOLOMON*):

5 – 10 –1 مبدأ ترميز ريد – سولومون :

في حالة ترميز ريد سولومون ($R - S$) رموز الكلمة المرمزة أي ثوابت $V(x)$ تكون عناصر في الحقل الممتد $GF(2^m)$

$$v(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} \qquad (5-151)$$

$$a_i \in GF(2^m)$$

إذاً كثير الحدود المولد $g(x)$ له الجذور $\alpha, \alpha^3, \alpha^{(2t-1)}$ و هي عناصر في $GF(2^m)$ فيكون الترميز المولد من كثير الحدود قادراً على تصحيح t من الأخطاء (يشار إلى t بعدد الأخطاء و ذلك طبقا للمراجع الإنكليزية)

يمكن أن نبين أن $g(x)$ له الجذور $\alpha, \alpha^2, \alpha^3, ..., \alpha^{2t}$ و هذه الجذور تحدد بنية $g(x)$ كثير الحدود المولد لترميز $(R-S)$ المصحح t خطأ.

يعد المضاعف المشترك البسيط

$$g(x) = \{ m_1(x) m_2(x) ..... m_{2t}(x) \} \qquad (5-152)$$

لكن إذا كانت ثوابت كثيرات الحدود البسيطة $m_i(x)$ في نفس الحقل $GF(2^m)$ بمجاهيل (x) ، عندئذ كثيرات الحدود هذه ستكون من الدرجة الأولى.

لكن

$$g(x) = (x+\alpha)(x+\alpha^2).....(x+\alpha^{2t}) \qquad (5-153)$$

من الدرجة $m_t = 2t$

كثير الحدود الأولي $g(x)$ الذي حصلنا عليه له الثوابت $g_i \in GF(2^m)$ ، في هذه الحالة m ليس هو عدد رموز المراقبة ، عدد رموز المراقبة سنشير إليه بالرمز m_t و يساوي درجة كثير الحدود المولد $m_t = 2t$

طول الكلمة المرمزة المشكلة من الرموز الموجودة في الحقل $GF(2^m)$ تساوي إلى $n = 2^m - 1$ حيث $v(x)$ هن عناصر في فئات الباقي ذي القاعدة $(x^n + 1)$ ، نشير إلى α بدلا من x فينتج لدينا :

أن : $\alpha^n - 1 = 0$ و بهذا $\alpha^n = 1$ أي أن n هو ترتيب العنصر الأولي أو (درجته) في الحقل $GF(2^m)$ حيث النتيجة $n = 2^m - 1$ عدد رموز المعلومات $k=n-m_t$

نحتاج إلى دارات تعالج عناصر موجودة في الحقل $GF(2^m)$ في عمليات الترميز و فك الترميز لمرمزات $(R - S)$.

هذه الدارات مكونة من مسجلات إزاحة – ضوا رب – مجمعات لعنصرين في الحقل $GF(2^m)$.

تكون مسجلات الإزاحة قادرة على تخزين و نقل العناصر $\beta_i \in GF(2^m)$ و ذلك بوضع المسجلات في الشكل (5 – 19) على التوازي

تتكون المجمعات في الحقل $GF(2^m)$ من مجمعات ذات الجمع الثنائي كما في الشكل (5 – 20)

و السبب أن الجمع و الطرح في $GF(2^m)$ متطابق لتحديد دارة الضرب يجب أن نشكل الحقل $GF(2^m)$ بمساعدة كثير الحدود الأولي $f(x)$ من الدرجة m أي نشكل فئات الباقي للتابع على أساس $f(x)$

لنفترض العنصر $\gamma \in GF(2^m)$ التي نرغب بعمل الضرب السلمي به ، هذا العنصر γ يمثل الحقل $GF(2^m)$ عن طريق كثير حدود من الدرجة $m-1$ أو أقل و نشير إليه $C(\alpha)$

ليكن لدينا عنصر $\beta \in GF(2^m)$ يمثل كثير الحدود b(α) الذي سيضرب ب γ الذي يمثل كثير الحدود $C(\alpha)$ ونشير إلى جداء الضرب ب $\partial(\alpha)$

$$\partial(\alpha) = \gamma\beta = C(x).b(x) \qquad (5-154)$$

كثير الحدود و $\partial(\alpha)$ من الدرجة $m-1$ أو أقل و هو عنصر في $GF(2^m)$ و نشير إليه بـ δ إذا :

$$\delta = \gamma\beta$$

مثال :

$$m = 3 \qquad f(x) = x^3 + x + 1$$

و ليكن $\gamma = \alpha^2$ و β عنصر في $GF(2^m)$

$$\beta = b_0 + b_1\alpha + b_2\alpha^2$$

ناتج الضرب :

$$\gamma\beta = b_0\alpha^2 + b_1\alpha^3 + b_2\alpha^4 = b_0\alpha^2 + b_1(\alpha+1) + b_2(\alpha^2+\alpha)$$

حيث :

$$\gamma\beta = b_1 + (b_1 + b_2)\alpha + (b_0 + b_2)\alpha^2 = \delta = \partial_0 + \partial\alpha + \partial_2\alpha^2$$

تقوم بهذه العملية الدارة التي المبينة في الشكل (5 – 21)

5 – 10 – 2 ترميز مرّمزات ريد سولومون :

حسب ما رأينا فإن كثير الحدود المولد $g(x)$ لمرمز درجته $m_t = 2t$)
حيث t عدد الأخطاء المراد تصحيحها)

نحصل على كثير الحدود لرموز المراقبة من العلاقة :

$$C(x) = rest\,\frac{X^{mt} i(x)}{g(x)} \qquad (5-155)$$

حيث أن ثوابت كثير الحدود $i(x), g(x), c(x)$ هي عناصر في $GF(2^m)$

للتبسيط نفترض أن $m = 3$ ، $t = 2$ ينتج من ذلك أن ($n = 2^3 - 1 = 7$) بايت و ($m_t = 2t = 4$) بايت ، إذاً ($k = 7 - 4 = 3$) بايت ولكن ..

$$g(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4) \qquad (5\text{-}156)$$

نختار كثير الحدود الأولي $f(x)$ من الدرجة $m = 3$ و نشكل $GF(2^3)$ طبقا للجدول ، نجري عملية الضرب بناء على هذا الجدول و $(x + \alpha)(x + \alpha^2)$ و $(x + \alpha^3)(x + \alpha^4)$

نحصل على $g(x)$

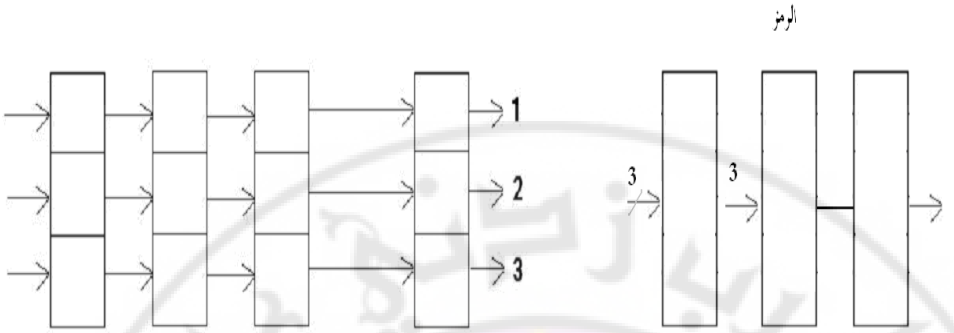
$$g(x) = [x^2 + (\alpha + \alpha^2)x + \alpha^3][x^2 + (\alpha^3 + \alpha^4)x + 1] \qquad (5\text{-}156)$$

أي

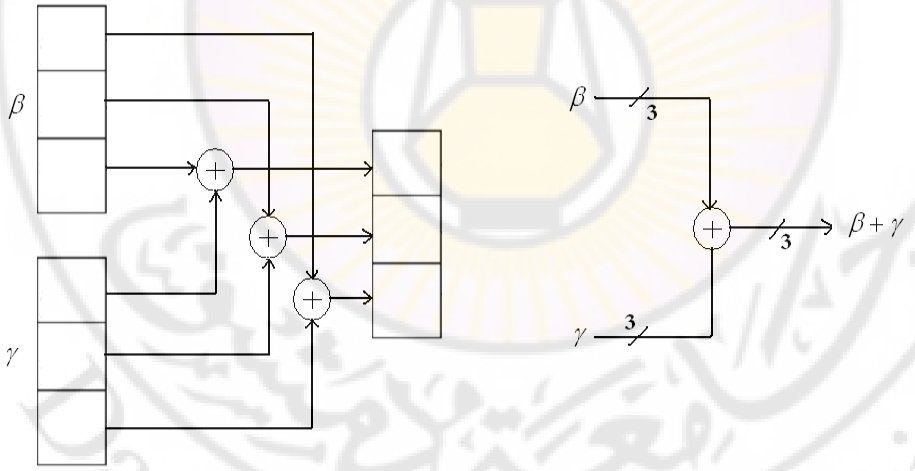
$$g(x) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3 \qquad (5\text{-}157)$$

دارة الترميز المبينة في الشكل (5 – 22) لها بنية دارة الترميز نفسها من خلال عملية التقسيم المبينة في الشكل (5 – 4) باختلاف بسيط هو أن مسجل الإزاحة مشكل من ثلاثة مسجلات إزاحة ثنائية موضوعة على التوازي ، الوصلات ثلاثية ، المجمعات – دارات الضرب تنفذ فيها العمليات ضمن الحقل $GF(2^3)$

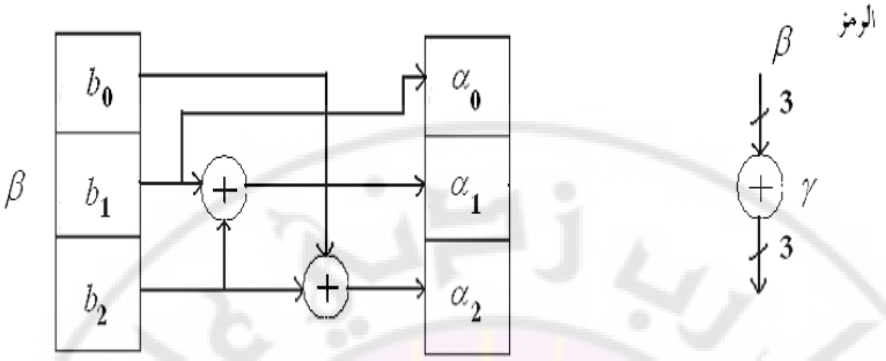
على العموم، يعطي المنبع رموز المعلومات على التسلسل، المبدل التسلسلي المتوازي ذي k خرج فيكون المرّمز ذا k دخل، و مبدلاً(توازي تسلسلي) على الخرج (في حال القنوات الثنائية) كما في الشكل (5 – 22)



الشكل (5 – 19) مسجل إزاحة للحقل $GF(2^3)$



الشكل (5 – 20) جامع في الحقل $GF(2^3)$



الشكل (5 – 21) مضاعفة عنصر β **في** γ، $\gamma = C(\alpha) = \alpha^2$

5 – 10 – 3 خصائص الأخطاء :

تكون قناة الإرسال قناة ثنائية تناظرية الرموز لمرمز (R–S) و α_i عناصر في $GF(2^m)$ تبدل بالتتالي إلى رموز ثنائية مطابقة لأمثال كثيرات الحدود من الدرجة $m-1$ التي تشكل $GF(2^m)$

هذه المتتالية من الرموز الثنائية يمكن أن تتغير ضمن القناة نتيجة التشويش , أي أن الرموز المرسلة $\alpha_i \in GF(2^m)$ تتحول إلى رموز $\alpha_i' \in GF(2^m)$

يتم هذا التحويل على الشكل التالي :

$$\alpha_i' = \alpha_i + \varepsilon_i \qquad (5\text{-}158)$$

حيث أن ε_i ينتمي إلى الحقل $GF(2^m)$ ، وتتمثل بكثير الحدود درجته أكبر ما يمكن $m-1$ وله ثوابت تساوي (1) في الأماكن الخاطئة و(0) في البقية .

جمع $\alpha_i + \varepsilon_i$ يتم على شكل جمع ثنائي لثوابت كثيرات الحدود (α_i و ε_i) لنحصل على كثير حدود ذي ثوابت α_i'

وبناء على ما ذكرناه سابقا فإن دخول أخطاء على الكلمة $v(x)$ يتم بجمع كثير الحدود $\varepsilon(x)$ مع $v(x)$ حيث

$$\varepsilon(x) = \varepsilon_0 + \varepsilon_1 x + ... + \varepsilon_{n-1} x^{n-1} \qquad (5-159)$$

حيث :

$$\varepsilon_i \in GF(2^m) \quad n = 0,1,2,.....n-1$$

وبهذه الرموز تكون الكلمة المستقبلة

$$v'(x) = v(x) + \varepsilon(x) \qquad (5-160)$$

5 – 10 – 4 كاشف ترميز ريد سولومون :

الطريقة العامة لمفكك ترميز ريد سولومون مماثلة لطريقة كاشف الترميز *B.C.H* من أجل t خطأ مستقل فقط هنا العناصر تنتمي إلى الحقل $GF(2^m)$

- إذا عدد الأخطاء ε_i أقل من t أو يساويه يدخل في رزمة طولها $mt \rangle \frac{m_t}{2} \rangle \ell$ درجة كثير الحدود (المولد)

إذا عدد الأخطاء ε_i يساوي t وتكون مستقلة، ولكن تدخل ضمن مجال أقل من m_t يمكن أن نطبق طريقة أبسط لكاشف الترميز لتصحيح الأخطاء المعروفة تحت اسم (*error trapping*) أي أخطاء على شكل رزم متفرقة ، أو أخطاء مستقلة لكنها تنتمي إلى $GF(2^m)$

مثال :

لنعد الرمز $n=7$, $t=2$ ينتج من ذلك أن $m=2t=4$ ، $k=3$ ، $m=3$

وسندرس كلا الحالتين السابقتين

- _عندما كلا الخطأين المصححين يشكلان رزمة من الأخطاء طولها $\ell = t = \frac{m_t}{2}$ ومستقلة , شروط الكشف لهذه الخطاء مبينة في الطريقة الموضحة في الفقرة (5 – 6 – 3) ونستخدم الدارة في الشكل (5– 23) التي تماثل الشكل (5–15) .

الكلمة المستقبلة

$$v'(x) = \alpha'_0 + \alpha'_1 x + \alpha'_2 x^2 + \alpha'_3 x^3 + \alpha'_4 x^4 + \alpha'_5 x^5 + \alpha'_6 x^6$$

حيث : $\alpha'_i \in GF(2^3)$ $i = 0,1,2,....$

لنفرض أن الأخطاء قد وقعت على الرموز α'_3 و α'_4 بقية الرموز لم يحدث لها أي شيء.

$$\alpha'_0=\alpha_0\ ;\alpha'_1=\alpha_1\ ;\alpha'_2=\alpha_2\ ;\alpha'_3=\alpha_3+\varepsilon_3\ ;\alpha'_4=\alpha_4+\varepsilon_4\ ;\alpha'_5=\alpha_5\ ;\alpha'_6=\alpha_6$$

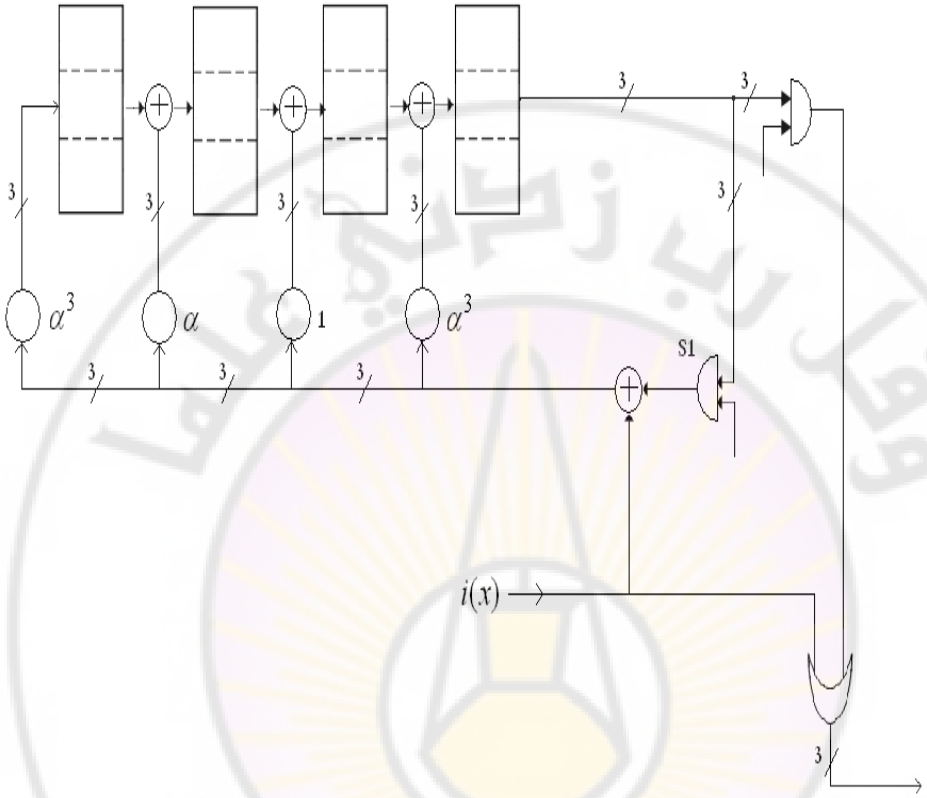
لنفترض أن الأخطاء قد وقعت في الكتلة α'_3 ذات طول m مشار إليها ε_3 تقابل العنصر α^2 الذي ينتمي إلى الحقل $GF(2^3)$، و يشار إليها ثنائيا $[1\ 0\ 0]$ ولكن بنية الأخطاء في الكتلة α'^4 المشار إليها ε_4 تقابل العنصر $\alpha^4 \in GF(2^3)$ الذي يشار إليها ثنائيا $[1\ 1\ 0]$.

في هذه الحالة الكلمة الخاطئة هي :

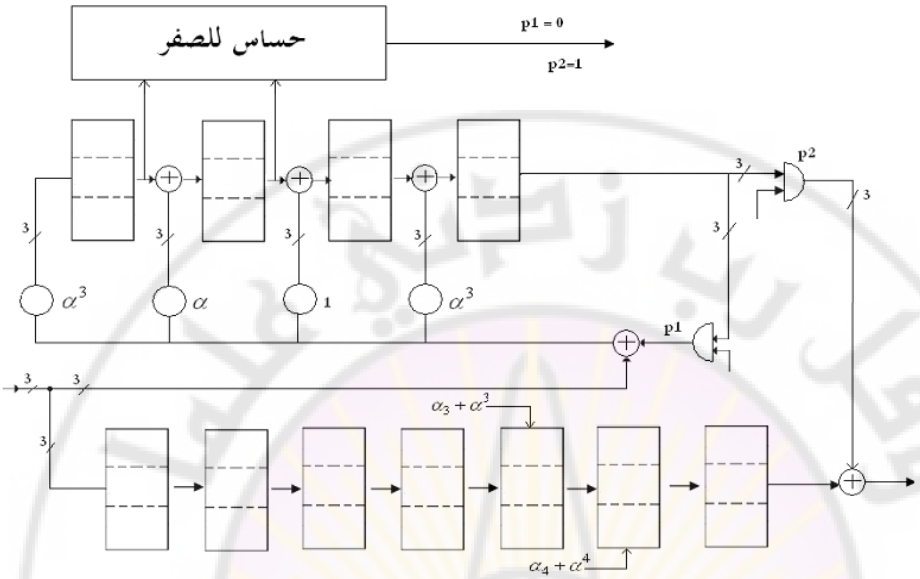
$$e(x)=\alpha^2x^3+\alpha^4x^4=x^3(\alpha^2+\alpha^4x)=x^3.b(x)$$

حيث $b(x)=\alpha^2+\alpha^4x$

تدخل الكلمة المستقبلة إلى المسجل الذي يقوم بعملية التقسيم على $g(x)$ كما في الشكل (5 – 22)



الشكل (5 – 22) مرّمز من خلال التقسيم (R– S)



الشكل (5 –23) كاشف ترميز (R – S)

بعد إدخال الكلمة $V'(x)$ إلى المسجل يبقى مخزناً في المسجل المصحح

$$Z(x) = rest\frac{x^{mt}v'(x)}{g(x)} = rest\frac{x^{mt}e(x)}{g(x)} = rest\frac{x^{4+3}(\alpha^2 + \alpha^4 x)}{g(x)}$$

أو

$$Z(x) = rest\frac{x^7(\alpha^2 + \alpha^4 x}{g(x)} = rest\frac{\alpha^4 x^8 + \alpha^2 x^7}{g(x)}$$

يكون ناتج التقسيم :

$$Z(x) = \alpha x^4 + \alpha^2$$

بعد إدخال الكلمة المستقبلة $V'(x)$ في المصد (buffer) و المسجل نحصل على المصحح و تبدأ عملية التصحيح .

أول رمز خاطئ α^4 إلى آخر خلية من المصدر بعد نبضتين وفي هذه اللحظة يكون محتوى المسجل

$$Z_c(x) = rest\,\frac{x^2 z(x)}{g(x)} = rest\,\frac{\alpha^4 x^3 + \alpha^2 x^2}{x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3}$$

وبالتقسيم نحصل على :

$$Z_c(x) = \alpha^4 x^3 + \alpha^2 x^2$$

هذا يعني أن المسجل يحتوي على

$$C_3 = \alpha^2,\ C_2 = \alpha^2,\ C_1 = 0,\ C_0 = 0$$

لكن دارة التحسس للصفر تغلق البوابة P_1 وتفتح P_2 ومن خلال تفريغ محتوى المسجل والمصدر يتم التصحيح .

محتوى المسجل بعد نبضتين يمكن أن يحسب بطريقة أخرى وذلك بافتراض أن المسجل يتمثل بمصفوفة كما في العلاقة 1 من الملحق (بـ) حيث $g_1 \in GF(2^3)$

$$\tau = \begin{bmatrix} 0 & 0 & 0 & \alpha^3 \\ 1 & 0 & 0 & \alpha \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & \alpha^3 \end{bmatrix}$$

أما τ^2 :

$$\tau^2 = \begin{bmatrix} 0 & 0 & \alpha^3 & \alpha^6 \\ 0 & 0 & \alpha & \alpha^6 \\ 1 & 0 & 1 & \alpha \\ 0 & 1 & \alpha^3 & \alpha^2 \end{bmatrix}$$

نشير إلى b بالمصفوفة التي تقابل $b(x)$

$$b(x) = \alpha^2 + \alpha^4 x$$

يكون المصحح طبقا للعلاقة : (114 – 5)

$$\tau = \alpha^{4+3} b = \begin{bmatrix} \alpha^3 \\ \alpha^4 \\ 0 \\ 0 \end{bmatrix}$$

و بما أن $\tau^T = I$ محتوى المسجل بعد نبضتين سيكون ..

$$Z_c = \tau^2 Z = \begin{bmatrix} 0 & 0 & \alpha^3 & \alpha^6 \\ 0 & 0 & \alpha & \alpha^6 \\ 1 & 0 & 1 & \alpha \\ 0 & 1 & \alpha^3 & \alpha^2 \end{bmatrix} \begin{bmatrix} \alpha^2 \\ \alpha^4 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \alpha^2 \\ \alpha^4 \end{bmatrix}$$

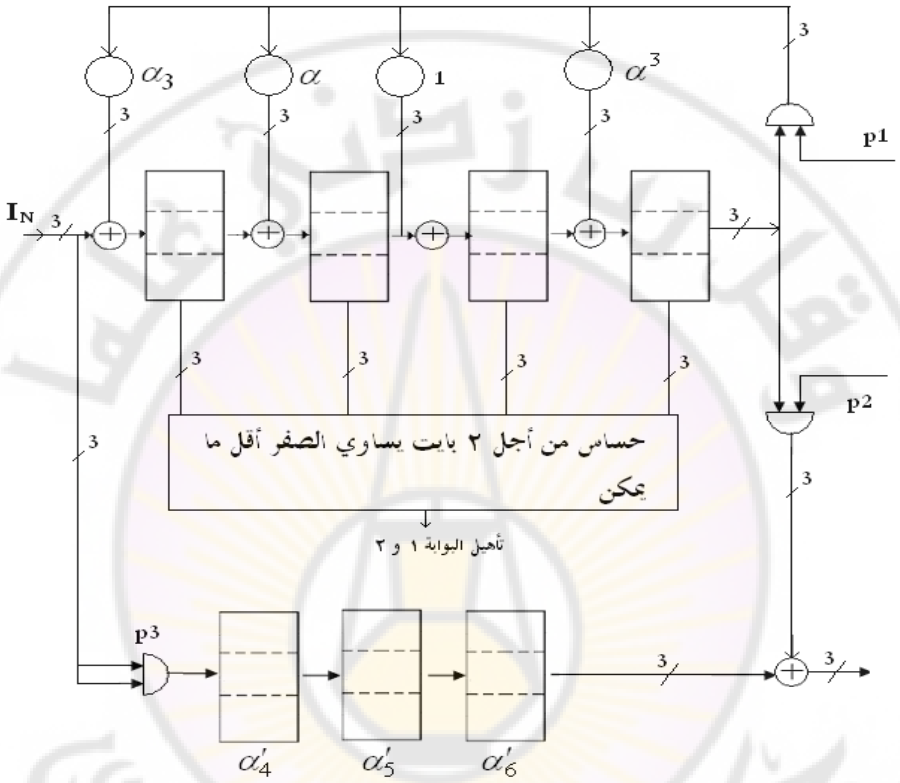
أي أن $C_3 = \alpha^4$ ، $C_2 = \alpha^2$ ، $C_1 = 0$ ، $C_0 = 0$.

أما في حالة الخطأين المستقلين ولكن ضمن المجال $m_t = 4$ فيمكن تصحيح الرموز بسهولة ،

في هذه الحالة الكلمة الخاطئة يمكن أن تكتب على الشكل التالي على أساس القاعدة $x^n + 1$ ، $e(x) = x^i(\beta + \gamma . x^\ell)$

حيث : $GF(2^3), \quad \ell < 4, \quad i = 0,1,2,.....,6$

بما أن التصحيح فقط لرموز المعلومات , المصدر يجب أن يختزن فقط الرموز α'_6 ، α'_5 ، α'_4 كما في الشكل (5 – 24) بعد إدخال الكلمة المستقبلة في المسجل الإزاحة (الذي يقوم بعملية التقسيم) يكون المصحح



الشكل (5 – 24) كاشف ترميز لمرّمز R – S

$$Z_c(x) = rest\,\frac{e(x)}{g(x)} = \beta + \gamma.x^{\ell}$$

أي في هذه الحال

$$Z_c(x) = C_0 + C_1x + C_2x^2 + C_3x^3$$

له أقل ما يمكن حدان يساويان الصفر أي له أكثر ما يمكن حدان يختلفان عن الصفر .

إذا دارة الاختبار تشير إلى وجود أقل ما يمكن حدين مساويين للصفر (أي خليتين من المسجل يساويان الصفر أقل ما يمكن) هذا يعني أن المصحح $Z_0(x)$ يساوي الكلمة الخاطئة التي لا تؤثر في رموز المعلومات وبالتالي يتم التفريغ من المصد والبوابة P_2 مغلقة ،

إذا دارة الاختبار تشير إلى وجود "صفر "(هذا يعني أن $Z_0(x)$ له أكثر من حدين لا يساويان الصفر ولا يمثل كلمة الخطأ)

فننجز إزاحة للمسجل بحيث أن البوابة P_1 مفتوحة و البوابة P_2 مغلقة و يصبح محتوى السجل :

$$Z_1(x) = rest\frac{x.v'(x)}{g(x)}$$

أي أن محتوى المسجل هو مصحح الكلمة الخاطئة

$$x.v'(x) = \alpha'_6 + \alpha'_0 x + ... + \alpha'_5 x^6$$

إذاً $Z_1(x)$ يحتوي أقل ما يمكن على حدين يساويان الصفر فهو يمثل الكلمة الخاطئة

$$Z_1(x) = \beta + \gamma.x^{\ell}$$

التي تؤثر في الكلمة $x.v'(x)$ أي على α^6 هذا يعني أن $\alpha'_6 = \alpha_6 + \beta$ و يؤثر أيضا في رمز للمراقبة لتصحيح α'_6 لابد من وصول β إلى آخر خلية C_3 للمسجل في هذه الحالة نقوم بعدد من الإزاحات ($m_t - 1 = 3$) للمسجل، و البوابتان *P1* ، *P2* مغلقتان .

في اللحظة التي يصل فيها β إلى الخلية C_3 تفتح البوابة P_2 و يتم تصحيح α'_6 من خلال الجمع مع β ، $\alpha'_6 + \beta = \alpha_6$

بعد إزاحة واحدة إذا لم يمكن محتوى المسجل له أقل ما يمكن حدان يساويان الصفر ، نقوم بإزاحة ثانية للمسجل بحيث تكون البوابة P_1 مفتوحة و البوابة P_2 مغلقة ، و نحصل على محتوى جديد .

$$Z_2(x) = rest\ \frac{x^2.v'(x)}{g(x)}$$

الذي هو المصحح للكلمة

$$x^2.v'(x) = \alpha'_5 + \alpha'_6 x + \alpha'_0 x^2 + ... + \alpha'_4 x^6$$

إذا وجد في $Z_2(x)$ أقل ما يمكن حدان يساويان الصفر حينئذ

$$Z_2(x) = \beta + \gamma.x^{\ell}$$

مما سبق يشير إلى أن α'_5 هو الرمز الخاطئ

$$\alpha'_5 = \alpha_5 + \beta$$

إذا $\ell = 1$ ما تزال متأثراً و رمز المعلومات ، $\alpha'_6 = \alpha_6 + \gamma$ إذا ($\ell > 1$ يتأثر فقط رموز المراقبة) .

لتصحيح α'_5 و α'_6 و إذ $\ell = 1$ يكون من الضروري أن تصل β إلى الخلية C_2 و γ إلى C_3 ، لهذا السبب ينزاح المسجل مرتين $m_t = 2$ و البوابات P_1 ، P_2 مغلقة بعد هذه الإزاحة ،

يتم فتح البوابة P_2 و يفرغ محتوى الخلايا C_2 ، C_3 و محتوى المصد ليتم تصحيح الرمزين α'_5 و α'_6 .

إذا لم يكن محتوى خليتين من المسجل يساوي الصفر بعد إزاحتين ننجز إزاحة ثالثة ليصبح محتوى المسجل:

$$Z_3(x) = rest\,\frac{x^3.v'(x)}{g(x)}$$

الذي هو مصحح الكلمة ،

$$x^3.v'(x) = \alpha'_4 + \alpha'_5 x + \alpha'_6 x^6 + \alpha'_0 x^3 + \ldots\ldots + \alpha'_3 x^6$$

إذا $Z_3(x)$ له أقل ما يمكن حدان يساويان الصفر :

$$Z_3(x) = \beta + \gamma.x^{\ell}$$

هذا يعني أن الرمز α'_4 خطأ

$$\alpha'_4 = \alpha_4 + \beta$$

إذا $\ell = 1$ يكون الرمز α'_5 خطأ

$$\alpha'_5 = \alpha_5 + \gamma$$

إذا $\ell = 2$ إلى جانب الرمز α'_4 يكون الرمز α'_6 خطأ

$$\alpha'_6 = \alpha_6 + \gamma$$

(إذا $\ell = 2$ إلى جانب α'_4 يكون رمز المراقبة α'_0 خطأ ،

لتصحيح α'_4 يجب أن يصل الرمز β إلى الخلية C_1 إذا أنجزنا إزاحة واحدة , ($m_t - 3 = 1$) و البوابات *P1* ، *P2* مغلقة .

إذا $\ell = 1$ سيكون محتوى المسجل $[0 \;\; \beta \;\; \gamma \;\; 0]$

إذا $\ell = 2$ سيكون محتوى المسجل $[0 \;\; \beta \;\; 0 \;\; \gamma]$

سيتم تفريغ المصدر والبوابة P_2 مفتوحة ويفرغ معه في آن واحد محتوى المسجل ليتم تصحيح α'_4 ، α'_5 أو α'_6 طبقا للحالة المفروضة

إذا لم يحتو المسجل أقل ما يمكن على صفرين في خلاياه حتى ولو بعد ثلاث إزاحات ، هذا يعني أن الترميز غير قادر على تصحيح الأخطاء

(على العموم يكون المرّمز غير قادر على تصحيح الأخطاء إذا تجاوز عدد الأخطاء المجال m_t)

بناء على ما ذكرناه يمكن أن نعمم طريقة كاشف الترميز (*error trapping*) لتصحيح t أخطاء مستقلات .

TABLE Some Primitive Polynomials

m		m	
3	$1 + X + X^3$	14	$1 + X + X^6 + X^{10} + X^{14}$
4	$1 + X + X^4$	15	$1 + X + X^{15}$
5	$1 + X^2 + X^5$	16	$1 + X + X^3 + X^{12} + X^{16}$
6	$1 + X + X^6$	17	$1 + X^3 + X^{17}$
7	$1 + X^3 + X^7$	18	$1 + X^7 + X^{18}$
8	$1 + X^2 + X^3 + X^4 + X^8$	19	$1 + X + X^2 + X^5 + X^{19}$
9	$1 + X^4 + X^9$	20	$1 + X^3 + X^{20}$
10	$1 + X^3 + X^{10}$	21	$1 + X^2 + X^{21}$
11	$1 + X^2 + X^{11}$	22	$1 + X + X^{22}$
12	$1 + X + X^4 + X^6 + X^{12}$	23	$1 + X^5 + X^{23}$
13	$1 + X + X^3 + X^4 + X^{13}$	24	$1 + X + X^2 + X^7 + X^{24}$

مسائل الفصل الخامس

مسألة(1):

لنفترض فئات الباقي من النموذج $p(x) = x^3+1$ بيّن أن هذه الفئات تشكل قانون الجبر

مسألة (2):

بين أن العلاقات $v(x) = i(x)\ g(x)$ و $V = iG$ متطابقة البرهان في حالة

$m = 3\ ,\ n = 7$

مسألة(3):

أثبت أن : $GH^T = HG^T = 0$ باعتبار أن $m = 3\ ,\ n = 7$

مسألة(4):

بين أوجه التقابل بين الكلمات الخاطئة والمصححات في حال الترميز (التام) يوصف المرمز بكثير الحدود $g(x) = 1 + x + x^3$

مسألة(5):

ليكن مرمز مصمم بدارة التقسيم على كثير الحدود $g(x)=1+ x^2 + x^3$ و $n = 7$ طبقاً لمخطط الدارة:

آ – ارسم المخطط لدارة التقسيم في هذه الحالة

ب – أوجد قيم رموز المراقبة بناء على هذه الدارة التي هي a0 a1 a2

ج – احسب كثير الحدود $C(X)$ لرموز المراقبة

مسألة (6):

أرسم كاشف الترميز للمسألة السابقة مبيناً أنه قادر على كشف رزمة من الأخطاء طولها $\ell = 3$

مسألة (7) :

حدد الدورات المولدة من مسجلات الإزاحة التالية ثم علل النتائج:

آ- مسجل فيه $m=3$ ووصلاته طبقا لكثير الحدود $g(x) = 1+x+x^3$

ب- $g(x) = 1+x+x^2 x^3+x^4, m= 4$

ج- $g(x) = 1+x+x^2+ x^3 ,m=3$

مسألة(8):

ليكن مسجل الإزاحة ذي التغذية العكسية في الشكل (5 - 9):

آ- أثبت أن المصفوفة المميزة لهذا المسجل هي ζ

ب- بين أن هذا المسجل يولد الدورات نفسها للمسجل من الشكل معتبرين المثال ب و ج المعطاة في المسألة السابقة.

مسألة(9):

لتكن دارة الترميز من الشكل: $g(x) = 1+x+x^3$

آ- ارسم الدارة من أجل $n= 7$

ب- اشرح عمل الدارة من خلال جدول الحالات وقارن النتائج مع النتائج في دارة التقسيم في المسألة 12:

الفصل السادس

الترميز الانطوائي convolutional coding

وقل رب زدني علما
جامعة دمشق
Damascus University

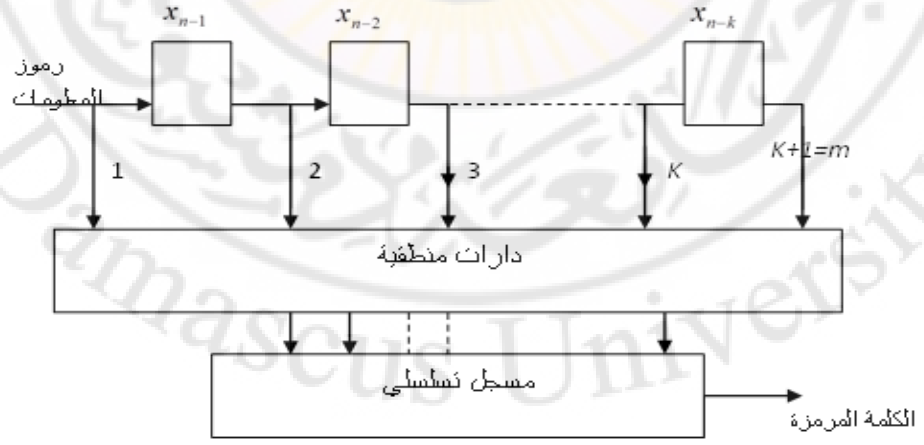
الفصل السادس

الترميز الانطوائي convolutional coding

6 – 1 مقدمة

تعالج رموز المعلومات المولدة من المنبع باستمرار دون أن تقسم إلى كلمات المرمزة كما هو الحال في الترميز الزمري. ولكن حتى نتمكن من تطبيق مفاهيم الترميز الزمري على الترميز الانطوائي. سوف نقسم المجال المستمر إلى رموز معلومات ورموز مراقبة على شكل مجموعات أقسام ولكنها لا تحمل معنى كلمات مرمزة في هذه الحالة رموز المراقبة الموجودة في مجموعة يمكن أن تراقب رموز معلومات أخرى موجودة في المجموعة التالية.

المخطط العام لمرمز تفاضلي مبين في الشكل(6–1):



الشكل(6–1) المخطط الصنوقي لمرمز انطوائي بمسجل ازاحة

6 – 2 بنية الترميز الانطوائي

تحدد كل متتالية من الرموز بمجموعة تتميز بطول n_0 وتشكل من k_0 رموز معلومات m_0 رموز مراقبة.

إن رموز المراقبة ضمن مجموعة طولها n_0 يمكن أن تراقب رموز معلومات من مجموعات صناديق أخرى يتضمن العدد الكلي للمجموعات أول مجموعة وآخر مجموعة حيث توجد رموز المعلومات المراقبة من خلال رموز المراقبة من المجموعة المعتبرة يشار إليه بـ m ويسمى الضغط ولكن العدد n يسمى طول عملية الضغط

$$n = m.n_0 \qquad (6-1)$$

في حال الترميز الانطوائي تعرف الكلمات المرمزة كمتتالية نصف منتهية من رموز المعلومات ورموز المراقبة

$$V = \left[x_1^{(1)}....x_1^{(k_0)} \quad y_1^{(1)}....y_1^{(m_0)} \quad x_2^{(1)}.....x_2^{(k_0)} \quad y_2^{(1)}....y_2^{(m_0)} \quad .....\right] \qquad (6-2)$$

حيث $x_j^{(i)}$ رمز المعلومات الذي يشغل المكان i في المجموعة j

$y_j^{(\ell)}$ رمز المراقبة الذي يشغل المكان ℓ في المجموعة j

k_0 عدد رموز المعلومات ضمن المجموعة.

m_0 عدد رموز المراقبة ضمن المجموعة.

$n_0 = m_0 + k_0$ عدد الرموز ضمن (المجموعة)الواحدة.

وللكتابة بشكل مفصل نشير إلى:

$$X_j = \left[x_j^{(1)} \quad ..... \quad x_j^{(k_0)}\right] \qquad (6-3)$$

$$Y_j = \left[y_j^{(1)} \quad ..... \quad y_j^{(M)} \right] \qquad (6-4)$$

وبذلك تكتب الكلمة المرمزة:

$$v = \left[X_1 Y_1 \quad X_2 Y_2 \quad .... \quad X_j Y_j \quad ..... \right] \qquad (6-5)$$

أو بالشكل التالي:

$$V_j = \left[X_j Y_j \right] \qquad (6-6)$$

ويكون لدينا:

$$v = \left[V_1 \quad V_2 \quad .... \quad V_j \quad ..... \right] \qquad (6-7)$$

أول $n = mn_0$ رمز:

$$W = \left[X_1 Y_1 \quad X_2 Y_2 \quad .... \quad X_m Y_m \quad \right] \qquad (6-8)$$

نشكل من الكلمة المرمزة V الكلمة الابتدائية للمرمز.

في الحالة الخاصة: عندما طول الضغط n يساوي n_0 رمزاً ضمن المجموعة أي *(m=1)* فالمصفوفة $W = [X_1 Y_1]$ تمثل أول كلمة مرمزة لترميز المجموعة، ولكن المصفوفة V معطاة بالعلاقة (6) تتمثل بمتتالية من الكلمات لترميز المجموعة.

في هذه الحالة طبقاً لما سبق فالعلاقة بين رموز المراقبة ورموز المعلومات تحدد بمصفوفة المراقبة:

$$H_0 = \left[RI_{m0} \right] \qquad (6-9)$$

حيث: R هي مصفوفة m_0 صف و K_0 عامود (هذه المؤشرات تختلف عما هو عليه في تراميز المجموعة).

المصفوفة L_{m0} مصفوفة أحادية من الدرجة m_0 .

الإختلاف بين هذه المصفوفة ومصفوفة المراقبة H (هو أنه هنا لدينا تبديل بالعناصر) بدلاً من $[\mathrm{I_{m0}R}]$ لدينا $[RI_{m0}]$ حيث كلمة الترميز عكس ترتيب رموز للمعلومات مع رموز المراقبة فبدلاً من $[Y_1X_1]$ لدينا $[X_1Y_1]$

ويكون ترميز المجموعة طبقاً للعلاقة:

$$H_0W^T = [RI_{m0}].[X_1Y_1]^T = [RI_{m0}].\begin{bmatrix} X_1^T \\ Y^T{}_1 \end{bmatrix} = 0 \qquad 6\text{-}10)$$

$$Y_1^T = RX_1^T \qquad (6\text{-}11)$$

إذ بدلنا الكلمة W ذات الطول المحدد بالكلمة v التي هي سلسلة نصف محددة من المجموعات في الحالة الخاصة عندما لا يكون لدينا بين هذه المجموعات ضغط (تجميع) أي (m=1).

المصفوفة H تقوم بعملية الترميز طبقاً للعلاقة $Hv^T = 0$ لها الشكل:

$$H = \begin{bmatrix} R & I_{m0} & 0 & 0 & .. & .. & .. \\ 0 & 0 & R & I_{m0} & .. & .. & .. \\ 0 & 0 & .. & .. & R & I_{m0} & .. \\ .. & .. & .. & .. & .. & .. & .. \end{bmatrix} \qquad (6\text{-}12)$$

حيث أن العناصر القطرية فقط تختلف عن الصفر. هذه العناصر تعطينا العلاقة بين رموز المراقبة ورموز المعلومات في المجموعات المتتالية طبقا للعلاقة (5-11).

6 – 3 الترميز الانطوائي اعتمادا على مصفوفة المراقبة *H*:

في الحالة العامة طول عملية الضغط هو $n = m.n_0$. في مصفوفة المراقبة H يتم إدخال عناصر (مصفوفات) التي تشير إليها $R_1,...,R_m$ التي تعطينا علاقة الربط بين رموز المراقبة ورموز المعلومات في m مجموعة التي يوجد فيهما الضغط.

يتم تحقيق ذلك فيما لو كانت المصفوفة H على الشكل:

$$H = \begin{bmatrix} R_1 & I_{m0} & 0 & .. & .. & .. & .. & .. & .. & .. \\ R_2 & 0 & R_1 & I_{m0} & 0 & .. & .. & .. & .. & .. \\ : & : & : & & & & & & & \\ R_m & 0 & R_{m-1} & 0 & .. & 0 & R_1 & I_{m0} & & \\ 0 & 0 & R_m & 0 & R_{m-1} & 0 & 0 & R_1 & I_{m0} & 0 \end{bmatrix} \qquad (6\text{-}13)$$

العناصر التي يشار إليها هي مصفوفة صفرية.

العلاقة $Hv^T = 0$ تعطينا ما يلي:

$$\begin{aligned} & R_1 X_1^T + Y_1^T = 0 \\ & R_2 X_1^T + R_1 X_2^T + Y_2^T = 0 \qquad (6\text{-}14) \\ & : \\ & R_m X_1^T + R_{m-1} X_2^T + ... + R_1 X_m^T + Y_m^T = 0 \end{aligned}$$

المصفوفة:

$$h = [R_m \quad 0 \quad R_{m-1} \quad 0 \quad .. \quad .. \quad 0 \quad R_1 \quad I_{m0}] \qquad (6-15)$$

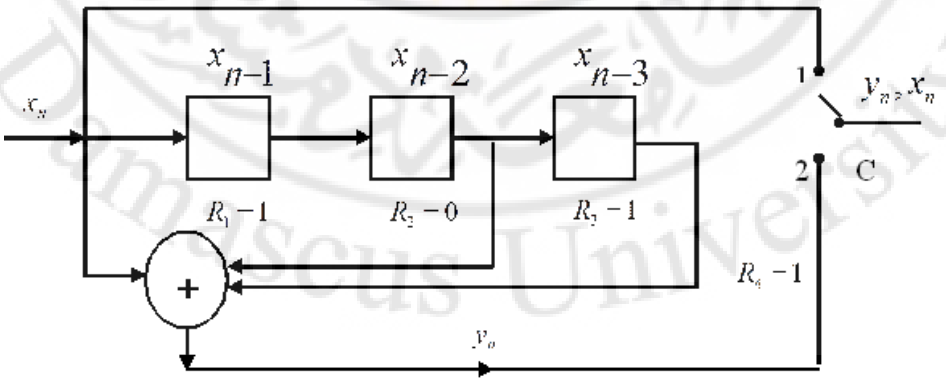
تسمى هذه مصفوفة الأساس. يلاحظ أنه بعد m كتلة ، صفوف المصفوفة H مشكلة من المصفوفة h مزاحة في كل صف بعنصر H_0 نحو اليمين.

هذا العمل يعني أن المصفوفة h تراقب بشكل تتابعي m كتلة من الكلمة المرمزة v.

لبيان ذلك نفترض أن $m = 4$:

$$Hv^T = 0 \qquad (6-16)$$

$$\begin{bmatrix} R_1 & I_{m0} & 0 & .. & .. & .. & .. & .. & .. & .. & .. & .. \\ R_2 & 0 & R_1 & I_{m0} & 0 & .. & .. & .. & .. & .. & .. & .. \\ R_3 & 0 & R_2 & 0 & R_1 & I_{m0} & 0 & .. & .. & .. & .. & .. \\ R_4 & 0 & R_3 & 0 & R_2 & 0 & R_1 & I_{m0} & 0 & .. & .. & .. \\ 0 & 0 & R_4 & 0 & R_3 & 0 & R_2 & 0 & R_1 & I_{m0} & 0 & .. \\ : & : & : & : & : & : & & & & & & \\ : & : & : & : & & & & & & & & \\ : & : & & & & & & & & & & \end{bmatrix} \cdot \begin{bmatrix} X_1^T \\ Y_1^T \\ X_2^T \\ Y_2^T \\ X_3^T \\ Y_3^T \\ X_4^T \\ Y_4^T \end{bmatrix} = 0 \qquad (6-17)$$



الشكل (6-2) الترميز الانطوائي

$$
\begin{aligned}
&R_1 X_1^T + Y_1^T = 0 \\
&R_2 X_1^T + R_1 X_2^T + Y_2^T = 0 \\
&R_3 X_1^T + R_2 X_2^T + R_1 X_3^T + Y_3^T = 0 \\
&R_4 X_1^T + R_3 X_2^T + R_2 X_3^T + R_1 X_4^T + Y_4^T = 0
\end{aligned}
\qquad (6-18)
$$

نفترض واحداً من الترميز التي $K_0 = 1, m_0 = 1, n_0 = 2$ ، في هذه الحالة المصفوفات R_i متشكلة من عنصر واحد، إذاً $R_i \in GF(2)$ ، ولكن

$$V = [X_1 \quad Y_1 \quad X_2 \quad Y_2 \quad .. \quad X_n \quad Y_n \quad ..] \qquad (6-19)$$

.

للحصول على بعض خواص التعامد التي تسهل عملية الترميز نختار المصفوفة *[h]* :

$$R_1 = 1, R_2 = 0, R_3 = R_4 = 1$$

$$h = [1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1]$$

في هذه الحالة تصبح العلاقات في (17) على الشكل التالي:

$$
\begin{aligned}
&y_1 = x_1 \\
&y_2 = x_2 \\
&y_3 = x_3 + x_1 \\
&y_4 = x_4 + x_2 + x_1
\end{aligned}
\qquad (6-20)
$$

على العموم:

$$y_n = x_n + x_{n-2} + x_{n-3} \qquad (6-21)$$

حيث $X_n = 0$ من أجل $n \le 0$.

المرمز الذي يحقق هذه المعادلة في الشكل السابق المفتاح C يوجد في الوضعية "1" لرموز المعلومات. في الوضعية "2" من أجل رموز المراقبة.

6 – 4 كاشف الترميز الانطوائي اعتمادا على منطق الأكثرية:

في الحالة المماثلة الكلمة المرمزة يمكن تعريف شعاع الخطأ:

$$E = \left[\varepsilon_1^{(1)} \quad .. \quad \varepsilon_1^{(K_0)} \quad \mu_1^{(1)} \quad .. \quad \mu_1^{(m_0)} \quad ..\right] \qquad (6-22)$$

حيث $\varepsilon_1^{(j)} = 1$ إذاً الرمز $x_1^{(j)}$ يكون خاطئاً.

و $\mu_1^{(\ell)} = 1$ إذا الرمز $y_1^{(\ell)}$ يكون خاطئاً. وتكون الكلمة المستقبلة

$$V' = V + E \qquad (6-23)$$

$$Z = HV'^T = HE^T \qquad (6-24)$$

بينما المصحح في المثال السابق

$$E = \left[\varepsilon_1 \quad \mu_1 \quad \varepsilon_2 \quad \mu_2 \quad .. \quad .. \quad ..\right] \qquad (6-25)$$

$$\varepsilon, \mu \in GF(2)$$

ومن العلاقة (24–5) وطبقاً للمثال السابق

$$\begin{aligned} Z_1 &= y_1' + x_1' = \mu_1 + \varepsilon_1 \\ Z_2 &= y_2' + x_2' = \mu_2 + \varepsilon_2 \\ Z_3 &= y_3' + x_3' + x_1' = \mu_3 + \varepsilon_3 + \varepsilon_1 \qquad (6-26) \\ Z_4 &= y_4' + x_4' + x_2' + x_1' = \mu_4 + \varepsilon_4 + \varepsilon_2 + \varepsilon_1 \end{aligned}$$

عملية التصحيح تتم رمزاً برمز فقط لرموز المعلومات.

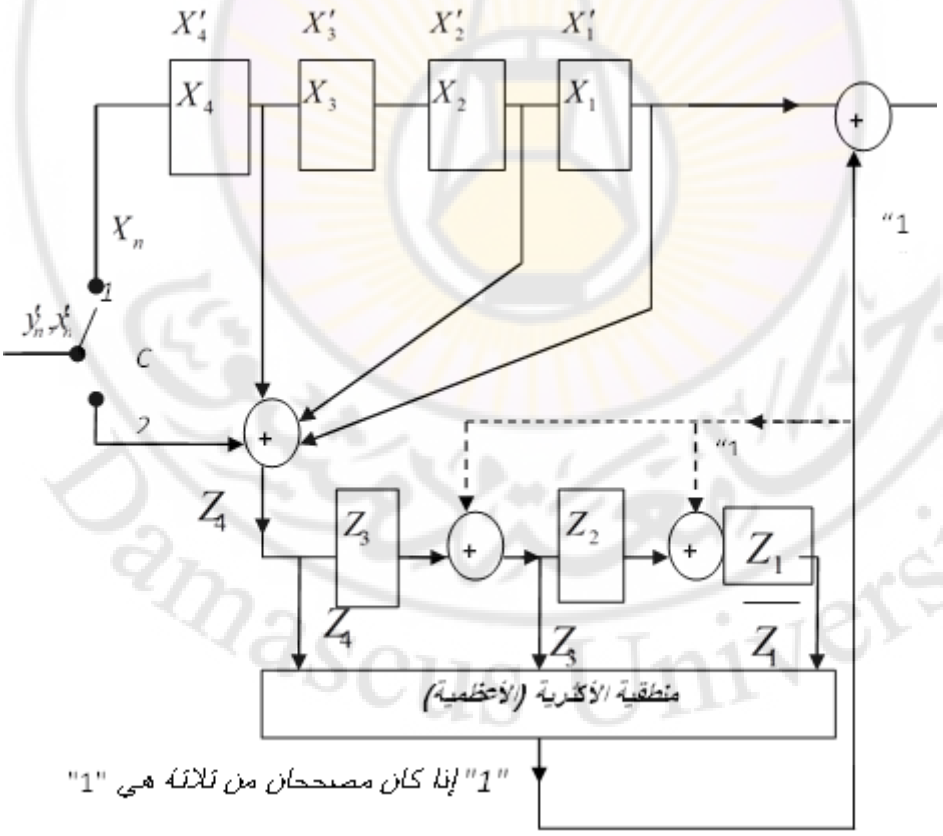
أول خطأ نصححه إذا وجد ε_1 من المعادلات السابقة نحذف المعادلة الثانية التي لا تحتوي على معلومات من خلال ε_1 لنحصل على:

$$Z_1 = \mu_1 + \varepsilon_1$$

$$Z_3 = \mu_3 + \varepsilon_3 + \varepsilon_1 \qquad (6-27)$$

$$Z_4 = \mu_4 + \varepsilon_4 + \varepsilon_2 + \varepsilon_1$$

نلاحظ أن جميع المعادلات السابقة تحتوي على ε_1 ولا يوجد رمز آخر موجود في معادلتين بآن واحد في هذه الحالة نقول إن التركيبة الخطية (24) هي تعامدية بالرمز ε_1.



الشكل (6-3) كاشف الترميز الانطوائي

إذا حصل خطأ في الرمز الأول x_1' وهو $\varepsilon_1 = 1$ وخطأ آخر في أي مكان فإن معظم المصححات من (24) تختلف عن الصفر.

إذاً معظم المصححات (24) تساوي إلى "1" نقر أن لدينا خطأ في الوضعية x_1' أي $\varepsilon_1 = 1$ غير ذلك فإن $\varepsilon_1 = 0$ أي ليس لدينا خطأ في المكان الأول.

نشير هنا إلى أن كاشف الترميز يعمل بشكل صحيح بالإضافة لـ x_1' الذي يمكن أن يكون خطأ أو صحيح. يوجد على الأكثر خطأ في أي مكان على طول القسم المضغوط. مما سبق ينتج أن كاشف الترميز يجب أن يحتوي على دارات منطقية التي تتحسس إذا كانت الأعظمية (الأكثرية) "1" أو "0" في الشكل(6-3)

يبين كاشف الترميز عندما يكون C في الوضعية "1" يتم إدخال رموز المعلومات، في الوضعية "2" رموز المراقبة.

لتسهيل عملية فهم كاشف الترميز نعطي حالات المسجل المختلفة:

clck / cell	1	2	3	4	5
x_4	x_1^1	x_2^1	x_3^1	x_4^1	x_5^1
x_3	0	x_1^1	x_2^1	x_3^1	x_4^1
x_2	0	0	x_1^1	x_2^1	x_3^1
x_1	0	0	0	x_1^1	x_2^1
Z_4	$x_1^1 + y_1^1$	$x_2^1 + y_2^1$	$x_3^1 + y_3^1 + x_1^1$	$x_4^1 + y_4^1 + x_2^1 + x_1^1$	$x_5^1 + y_5^1 + x_3^1 + x_2^1$
Z_3	0	$x_1^1 + y_1^1$	$x_2^1 + y_2^1$	$x_3^1 + y_3^1 + x_1^1$	$x_4^1 + y_4^1 + x_2^1 + x_1^1$
Z_2	0	0	$x_1^1 + y_1^1$	$x_2^1 + y_2^1$	$x_3^1 + y_3^1 + x_1^1$
Z_1	0	0	0	$x_1^1 + y_1^1$	$x_2^1 + y_2^1$

يلاحظ أنه في النبضة الرابعة تم تشكيل المصححات طبقاً للعلاقة (23) ستتم عملية التصحيح لـ x_1' الذي يكون في هذه اللحظة على الخرج.

وبالتالي لكشف الرمز التالي x_2' في المصفوفة H يجب أن نضيف الصف التالي من المصفوفة وبالتالي نلغي المعادلة الأولى من (23) وتضاف معادلة جديدة:

$$\begin{aligned} Z_2 &= \mu_2 + \varepsilon_2 \\ Z_3 &= \mu_3 + \varepsilon_3 + \varepsilon_1 \\ Z_4 &= \mu_4 + \varepsilon_4 + \varepsilon_2 + \varepsilon_1 \\ Z_5 &= \mu_5 + \varepsilon_5 + \varepsilon_3 + \varepsilon_2 \end{aligned} \qquad (6-28)$$

نلغي المعادلات التي لا تحوي على ε_2 كما فعلنا سابقاً:

$$\begin{aligned} Z_2 &= \mu_2 + \varepsilon_2 \\ Z_4 &= \mu_4 + \varepsilon_4 + \varepsilon_2 + \varepsilon_1 \\ Z_5 &= \mu_5 + \varepsilon_5 + \varepsilon_3 + \varepsilon_2 \end{aligned} \qquad (6-29)$$

هذه المعادلات مشابهة (20) حيث مؤشرات Z_i ازداد بمقدار واحد وبالتالي ε_1يجب أن يساوي "0"

إذا المكان الأول لم يوجد فيه خطأ $\varepsilon_1 = 0$ نحصل:

$$\begin{aligned} Z_2 &= \mu_2 + \varepsilon_2 \\ Z_4 &= \mu_4 + \varepsilon_4 + \varepsilon_2 \\ Z_5 &= \mu_5 + \varepsilon_5 + \varepsilon_3 + \varepsilon_2 \end{aligned} \qquad (6-30)$$

أي أن مجموع المركبات الخطية العامودية ε_2. إذاً كاشف الترميز سيقوم بأداء العملية السابقة نفسها.

إذا الوضعية الأولى X_1' كانت خاطئة بعد تنفيذ التصحيح $X_1' + \varepsilon_1 = X_1$

نقوم بإلغاء قيم ε_1 من المعادلات (25) أي من الخلايا Z_2 و Z_3 وذلك من خلال إجراء عملية الجمع الثنائي (1) كما بينا سابقاً.

إذاً عملية التصحيح بكاشف الترميز تؤدي خطأ سيتبع ذلك أخطاء بعد عملية التصحيح حيث أنه بعد عملية التصحيح يعود إلى حالته الطبيعية.

6 – 5 خوارزمية كاشف ترميز فيتربي *Viterbi* :

خوارزمية فيتربي تطبق في الترميز الانطوائي النظامي وغير النظامي فيما يلي سنشرح طريقة الترميز الانطوائي غير النظامي وفيما يتعلق بالترميز الانطوائي غير النظامي نتذكر الفقرات التالية:

ـ في المجموعة n_0 رمزاً رموز المعلومات و رموز المراقبة غير منفصلة لذلك سنسميهم رموز الكلمة المرمزة و تشير إليها u_i .

ـ إذا المجموعة n_0 على الخرج تكون ناتجة من تطبيق k_0 على الدخل (رموز المعلومات) نقول أن المعدل $R = \frac{k_0}{n_0}$.

. تجميع m يساوي إلى عدد المجموعات ذات n_0 رمزاً التي لها علاقة فيما بينها بسبب أن رمز المعلومات X_i المطبق على الدخل يدخل في حساب أقل ما يمكن n_0 رمزاً. في كل m مجموعة.

. لإجراء عملية كشف الترميز الانطوائي نأخذ القرار على أساس الاحتمالات المسبقة الأعظمية (أي المسافة الصغرى) بين الكلمة المستقبلة والكلمة التي لها معنى.

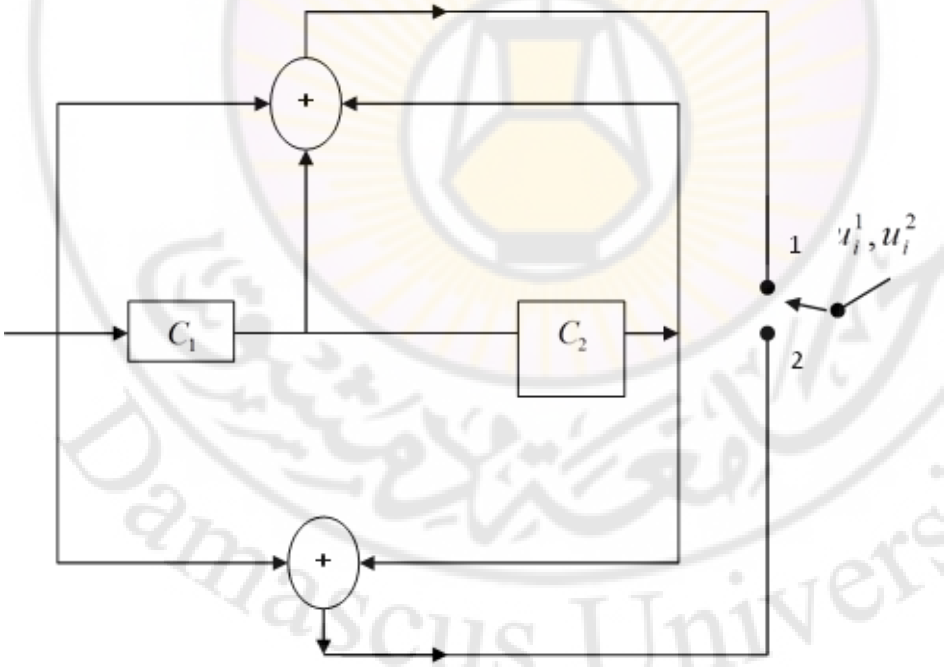
لهذه الغاية بعد استقبال N مجموعة من n_0 رمز على اعتبار أن N أكبر بعدد من المرات من m نقوم بإجراء عملية المقارنة مع جميع الكلمات التي لها

معنى ذات الطول $m_0 N$ ونختار الكلمة ذات المعنى الأقرب إلى السلسلة من الرموز المستقبلة، على العموم تؤخذ مسافة هامينغ.

يمكن أخذ طريقة أخرى تسمى علاقة الترابط الذاتي الأعظمية عملية مقارنة N مجموعة تستمر من خلال تمرير سلسلة من الرموز التي على شكل مجموعات، مما سبق ينتج أن كشف الترميز لأول مجموعة يتم بتأخير N مجموعة.

6 – 5 – 1 الترميز الانطوائي غير النظامي:

لنفترض الترميز الانطوائي بمعدل $\frac{1}{2}$ ذي تجميع (ضغط) $m = 3, n_0 = 2$ وتتم عملية الترميز بمسجل إزاحة *k=2* خلية ومبين في الشكل:



الشكل (6–4) دارة ترميز غير نظامي m=3 ,n0=2

عمل هذه الدارة مبين في الجدول التالي:

t_i	1	2	3	4	5	6	7	8
X_i	1	1	1	0	1	0	0	0
C_1, C_2	00	10	11	11	01	10	01	00
$u_i^{(1)}, u_i^{(2)}$	11	01	10	01	00	10	11	00

الجدول (6-2) عمل دارة ترميز غير نظامي

محتوى المسجل يسمى بحالة المرمز العدد الكلي للحالات $2^2 = 4$.

في البداية نفترض أن المسجل يوجد في الحالة 00 وعلى الدخل في اللحظة $t = 1$ يوجد الرمز $x_1 = 1$ على مخرج المرمز تظهر الرموز $u_1^{(1)} = 1, u_1^{(2)} = 1$ لتشكل المجموعة $u_i = 11$.

النبضة التالية $t = 2$ يمر المسجل إلى الحالة 10 على الدخل نطبق $x_2 = 1$ على الخرج تظهر الرموز 01 هذه العملية يمكن أن تستمر من أجل سلسلة عشوائية من رموز المعلومات.

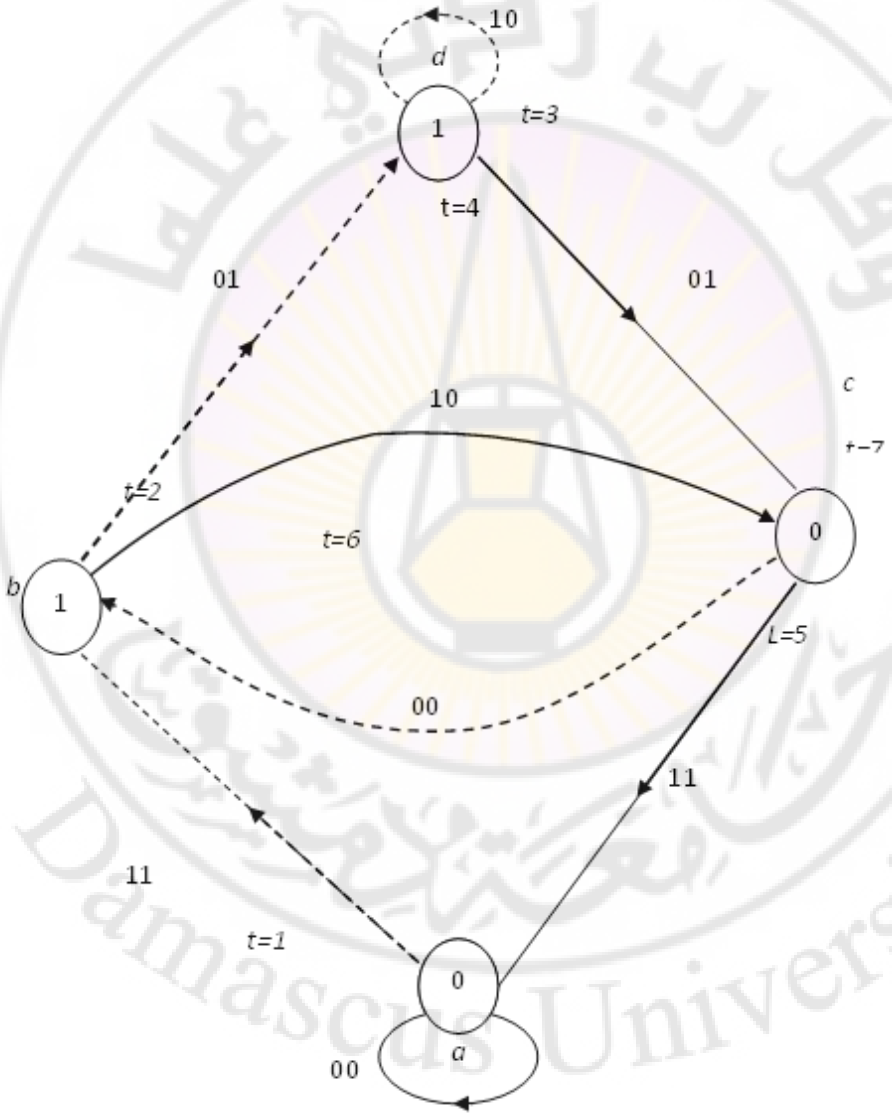
كل رمز مطبق على الدخل يظهر على الخرج رمزين للكلمة المرمزة على الخرج الذي يشكل مجموعة ($n_0 = 2$) .

يشير إلى ظهور مجموعة مثال (11) تعتمد على حالة المسجل (01) وعلى الرمز المطبق على الدخل (1) أي أنه لدينا سلسلة ماركورف التي يمكن أن تتمثل في مخطط الحالات للمسجل المبين في الشكل(6-5)

هذا المخطط يسمح بتحديد مجموعات الخرج للمرمز بدلالة الرموز المطبقة على الدخل. تطبيق الرمز 1على الدخل يشار إليه بخط منقط أما الرمز 0 فمن خلال خط مستمر.

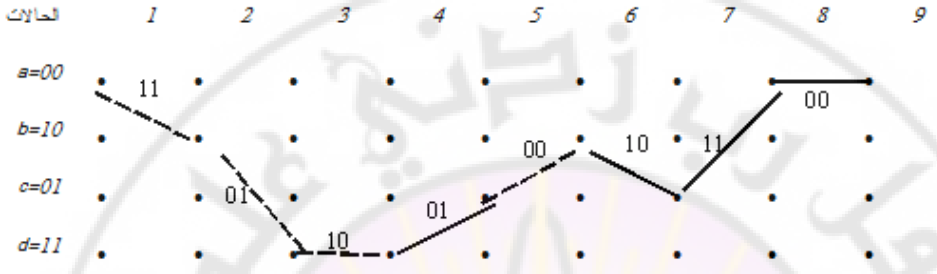
بدلالة حالة المسجل في لحظة تطبيق رمز الدخل نحصل على الخرج مجموعات مختلفة التي يشار إليها على الفروع للمخطط.

يسمح مخطط الحالات بتمثيل سير المتتالية مع مرور الزمن (كلمات الترميز) التي تولد الترميز المعد.



الشكل (6-5) مخطط حالات ترميز غير نظامي

يسمى هذا التمثيل trellis المبينة في الشكل(6 –5):



الشكل(6 –5) تمثيل مخطط الشجيرات (trellis)

حالات المرمز ممثلة بنقاط (عقد) العددي الكلي 4 حالات أي أربعة خطوط بدلالة السلسلة المطبقة على الدخل يمكن فحص الطريق في اللحظات *t=1,2,.....* الذي يمر من خلال النقاط التي تمثل حالات المسجل في تلك اللحظة.

على الخرج لكل نقطة (عقدة) إلى نقطة أخرى يكون الخط مستمراً فيما لو كان على الدخل 0 ومتقطعاً فيما لو كان 1 .

على كل خط يصل بين نقطتين نشير إلى أن الرموز المولدة على الخرج في هذه الحالة فالمسار يحتوي على رموز الدخل (خطوط مقطعة أو مستمرة) ورموز الخرج من كاشف الترميز (مكتوبة على الخطوط في الشكل السابق بينما رموز المعلومات المعطاة في الجدول).

يمثل مخطط الشجيرات (*trellis*) جميع الكلمات التي لها معنى (التي تمثل رموز المعلومات المطبقة على الدخل) ولتوضيح ذلك قمنا برسم سلسلة واحدة فقط.

لكل كلمة مرمزة ممثلة على المخطط يمكن أن نحدد بسهولة وزن (عدد المركبات التي تساوي الواحد؛ المسافة بالنسبة للكلمة 00.....)

الحالة المبينة في الرسم تشير إلى أن الوزن يساوي إلى 8 وطبقاً للتعريف السابق فهو يساوي إلى المسافة الصغرى لتحديد عدد الأخطاء التي يمكن تصحيحها لهذا المرمز مثال $N=9$ يجب تمثيل جميع المسارات بدءاً بالحالة 00 في اللحظة $t=1$ حتى اللحظة $t=9$ باستثناء المسار 0...00 نحسب وزن الكلمة أي المسافة الصغرى 23 $d_{\min}=2et$ حيث e عدد الأخطاء التي يمكن تصحيحها ضمن كلمة طولها $n_0.N=2N$

الوزن الأصغري للكلمة المرمزة يمكن أن يحدد بسهولة من مخطط الحالات وذلك من خلال إيجاد أقصر طريق بين الحالة a والعودة إليها من جديد بعد Nمجموعة باستثناء aa...a من المخطط الناتج فإن المسار abcca التي تقابل المجموعات ....001110110000.

إذاً الوزن الأصغري هو5 ينتج بأن المرمز قادر على تصحيح خطأين.

6 – 5 – 2 خوارزمية كاشف الترميز :

من مخطط الحالات من كل عقدة ينطلق فرعان وفي كل عقدة يدخل فرعان وهذا يظهر في مخطط (*trellis*) فإذا رسمنا جميع الخطوط الممكنة (أي أن جميع الكلمات المرمزة).

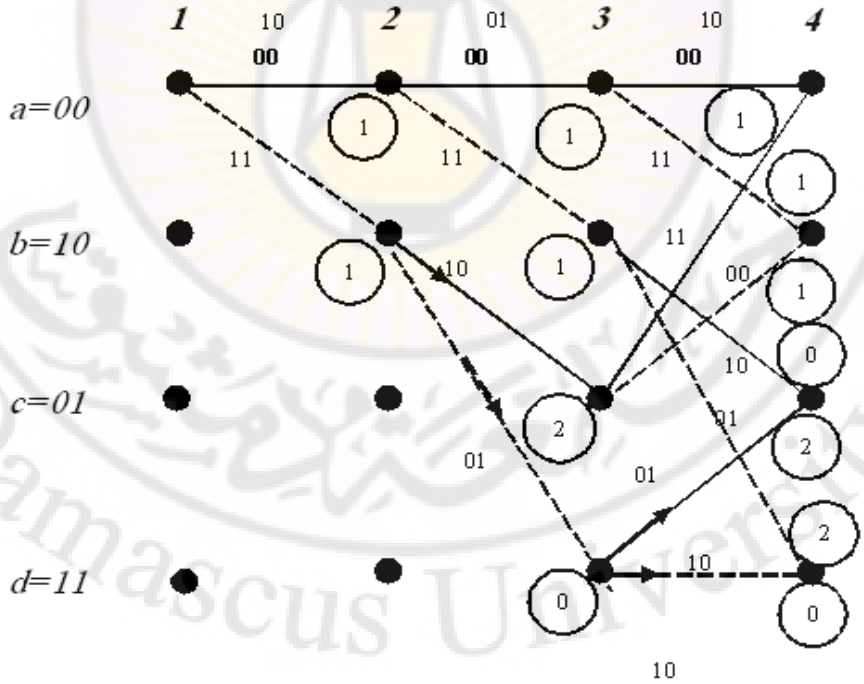
سلسلة الرمز المستقبلة المشكلة من N مجموعة يشار إليه $u'_1,u'_2,.....,u'_N$ ويقارن مع كل مجموعة موجودة في مخطط الشجيرات.

تتم عملية المقارنة في اللحظات $t=2,3,...N+1$ مع $2\times4=8$ مجموعة المتصلة بأربع نقاط (عقد) هذه المقارنة تساعدنا في تحديد مسافة هامينغ بين المجموعة المستقبلة u'_i والمجموعات الموجودة في مخطط الشجيرات في اللحظات

$i.....,\ell,i$ (عـدد‌ياً 8) علـى كـل خـط أو فـرع يشـار إلـى المسـافة كمـا فـي الشكل(6-6)(في هذا المخطط فإن قيم الزمن ليس لها أهمية) هي تساعد فقط على رسم المسارات في الشكل السابق.

لكل عامود من مخطط الشجيرات نعتبر 4 نقاط (في ترتيب عشوائي) وكل نقطة *(a,b,c,d)* مخطط الحالات يبين المجموعتين المولدتين ونشير إليها على الفروع التي تخرج من العقدة.

لنفترض أن السلسلة المستقبلة هي 100110 نرى أنها ليست كلمة مرمزة إذا لا نراها على المخطط لإيجاد الكلمة المرسلة نحسب المسافة بين أول مجموعة مستقبلة 10 والمجموعات التي على مخطط الشجرات 11 , 10.



الشكل (6-6) المخطط الشجري لكلمات الترميز المكونة من ثلاث كتل

بعد ذلك نحسب المسافة بين المجموعة المستقبلة 01 والمجموعات 00,11,10 من مخطط الشجرات وتستمر العملية من أجل كافة المجموعات.

يشار إلى المسافة المحسوبة على مخطط الشجيرات (ذلك ضمن دوائر).

للتبسيط نفترض أننا نقف عند مقارنة $N=3$ نلاحظ أن المسافة الصغرى للمسار ($d=1$) بالمقارنة مع السلسلة المستقبلة هو المسار a,b,c,d أي مكونة من المجموعات 110110

بناء على هذه المسافة الصغرى نقر بأن السلسلة المستقبلة 100110 تأتي من الكلمة التي لها معنى 110110 حيث كان الخطأ في المكان الأول.

إذا كان لدينا خطأن 000110 فمن أجل كاشف الترميز يجب أن نأخذ بعين الاعتبار أكثر ما يمكن من مجموعات وفي هذه الحالة نجري المقارنة لعدد أكبر من الأعمدة لمخطط الشجيرات المستخدم.

الأعمدة المقابلة للحظات $t=4,5,6....$ في كل عقدة يطبق خطان مساران من هذين المسارين نلغي المسار الأطول حيث أنه في زيادة طول الخط تزداد المسافة وهذا لايقودنا إلى المسافة الصغرى.

1. . المسار ذي المسافة الصغرى الذي يدخل في العقدة يسمى(*survivor*)
2. . نأخذ بالاعتبار فقط(*survivor*) لكل عامود سيكون لدينا فقط 4 مقارنات وليس 8.
3. . إذاً كلا المسارين يدخلان في العقدة لهما الطول نفسه يمكن اختيار أي واحد منها.
4. . مما سبق فإن خوارزمية كاشف الترميز يمكن أن تعمم بسهولة الى أشكال أخطاء أخرى غير المعطاة في المثال خوارزمية فيتربي لها تطبيقات في مجالات معرفة الأشكال في نظريات التعديل.

6 – 6 طريقة التداخل (الحشو):

الهدف من هذه الطريقة أنه يمكن استخدام ترميز الأخطاء المنفردة في الكلمات ذات رزمة من الأخطاء حيث تقوم هذه الطريقة بتحويل رزمة الأخطاء إلى أخطاء منفردة.

تقوم هذه الفكرة على إرسال رموز الكلمة المرمزة بتداخل مع كلمة مرمزة أخرى أن بحيث أن رمزين متتاليين من كلمة واحدة يوجدان على مسافة أكبر من طول رزمة الأخطاء ℓ. وبهذا فإن رزمة من الأخطاء لا يمكن أن يؤثر في أكثر من رمز في الكلمة الواحدة، وبالتالي فإن رموز الكلمة التي تتعرض إلى أخطاء من رزمات من الأخطاء المختلفة فتأثير هذه الرزمة عبارة عن أخطاء منفردة مستقلة.

هذه الطريقة مبينة في الشكل (6-7)

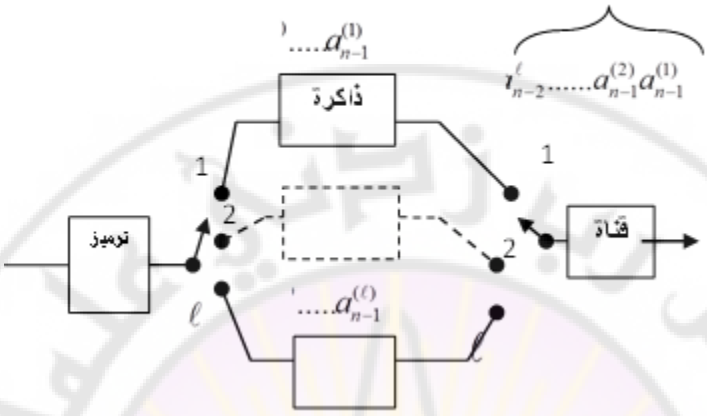
يتبين إذا أشرنا بالرمز العلوي إلى رقم الكلمة أن القناة ترسل بالتتالي:

$$a_{n-1}^{(1)} \quad a_{n-1}^{(2)} \quad \ldots\ldots \quad a_{n-1}^{(1)} \quad a_{n-2}^{(1)} \quad a_{n-2}^{(2)}$$

ينتج رزمة من الأخطاء طوله ℓ لا يؤثر إلا في رمز واحد فقط للكلمة المرمزة وبهذا نحصل على أخطاء منفردة .

لتمثيل ترميز آخر نعتبر في البداية حالة مبسطة بحيث نقوم بتداخل لكلمتين مرمزتين.

تداخل هاتين الكلمتين (عملية التداخل لكلمتين تستمر بشكل غير محدود) ونشير لذلك



الشكل (6-7) طريقة التداخل

$$V^{(1)}(x) = a_0^{(1)} + a_1^{(1)}x + ... + a_{m-1}^{(1)}x^{m-1} + a_m^{(1)}x^m + ... + a_{n-1}^{(1)}x^{n-1} \qquad (6-31)$$

$$V^{(2)}(x) = a_0^{(2)} + a_1^{(2)}x + ... + a_{m-1}^{(2)}x^{m-1} + a_m^{(2)}x^m + ... + a_{n-1}^{(2)}x^{n-1} \qquad (6-31)$$

كثير الحدود المراقب لهذه الكلمات نشير إليه:

$$C^{(1)}(x) = a_0^{(1)} + a_1^{(1)}x + ... + a_{m-1}^{(1)}x^{m-1} \qquad (6-32)$$

$$C^{(2)}(x) = a_0^{(2)} + a_1^{(2)}x + ... + a_{m-1}^{(2)}x^{m-1} \qquad (6-33)$$

وكثير الحدود للمعلومات

$$i^{(1)}(x) = a_m^{(1)} + a_{m+1}^{(1)}x + ... + a_{n-1}^{(1)}x^{k-1} \qquad (6-34)$$

$$i^{(2)}(x) = a_m^{(2)} + a_{m+1}^{(2)}x + ... + a_{n-1}^{(2)}x^{k-1} \qquad (6-35)$$

ترميز كلا الكلمتين منفذ بكثير الحدود المولد $g(x)$ طبقاً للعلاقة:

$$C(x) = rest\,\frac{x^m i(x)}{g(x)} \qquad (6-36)$$

وبهذه المؤشرات كلا الكلمتين المرمزتين يمكن كتابة:

$$V^{(1)}(x) = c^{(1)}(x) + x^m i^{(1)}(x) \qquad (6-37)$$

$$V^{(2)}(x) = c^{(2)}(x) + x^m i^{(2)}(x) \qquad (6-38)$$

ومن خلال عملية التداخل لهاتين الكلمتين ينتج لدينا:

$$a_0^{(1)} \quad a_0^{(2)} \quad a_1^{(1)} \quad a_1^{(2)} \quad a_2 \quad \ldots\ldots \quad a_{n-1}^{(1)} \quad a_{n-1}^{(2)} \qquad (6-39)$$

هذه المتتالية يمكن أن تمثل بكثيرالحدود:

$$V(x) = a_0^{(1)} + a_0^{(2)}x + a_1^{(1)}x^2 + a_1^{(2)}xx^2 + a_2^{(1)}x^4 + a_2^{(2)}xx^4 + \ldots + a_{n-1}^{(1)}(x^2)^{n-1} + a_{n-1}^{(1)}x(x^2)^{n-1} \qquad (6-40)$$

بالاحتفاظ بالمؤشرات السابقة:

$$V(x) = c^{(1)}(x^2) + xc^{(2)}x^2 + x^{2m}\left[\, i^{(1)}(x^2) + xi^{(2)}(x^2) \,\right] \qquad (6-41)$$

وإذا أدخلنا المؤشرات التالية:

$$C(x) = c^{(1)}(x^2) + xc^{(2)}x^2 \qquad (6-42)$$

$$I(x) = i^{(1)}(x^2) + xi^{(2)}(x^2) \qquad (6-43)$$

لدينا

$$V(x) = c(x) + x^{2m}I(x) \qquad (6-44)$$

إذاً الكلمة ***V(x)*** ذات الطول ***2n*** نحصل عليها من ترميز المجموعة ذات ***2k*** رمزاً للمعلومات وممثلة بكثير الحدود ***I(x)*** .

لتحديد كثير الحدود المولد ***G(x)*** الذي له دور في عملية الترميز طبقاً للعلاقة (100–5) نأخذ الاعتبارات التالية:

1. ـ كلمات الترميز من فئات الباقي من النموذج x^n+1 أما كلمات الترميز ***V(x)*** فهي أضعاف كثير الحدود المولد ***g(x)*** القاسم x^n+1 .

2. ـ كلمات الترميز المتداخلة هي فئات الباقي من النموذج $x^{2n}+1$ الكلمات المرمزة ***V(x)*** هي مضاعف كثير الحدود المولد ***G(x)*** القاسم $x^{2n}+1$.

3. ـ وبما أن x^n+1 يقسم بكثير الحدود ***g(x)*** ينتج أن $x^{2n}+1$ يقسم $g(x^2)$ للحصول على ***V(x)*** نستعمل علاقة الترميز (100-5) بكثير الحدود المولد $g(x^2)$

$$C(x) = rest\,\frac{x^{2m} i(x)}{g(x^2)} \qquad (6-45)$$

$$C(x) = rest\,\frac{x^{2m}\left[\, i^{(1)}(x^2) + x i^{(2)}(x^2)\,\right]}{g(x^2)} \qquad (6-46)$$

حيث

$$+\, x.rest\,\frac{x^{2m} i^{(2)}(x^2)}{g(x^2)} \qquad (6-47)$$

$$C(x) = rest\,\frac{x^{2m} i^{(1)}(x)}{g(x^2)}$$

وطبقاً للعلاقة (49) في الفصل الثاني نلاحظ أن:

$$rest\,\frac{x^{2m} i^{(1)}(x^2)}{g(x^2)} = c^{(1)}(x^2) \quad rest\,\frac{x^{2m} i^{(2)}(x^2)}{g(x^2)} = c^{(2)} \; and$$

إذاً:

$$C(x) = c^{(1)}(x^2) + x c^{(2)}(x^2) \qquad (6-49)$$

العلاقة مطابقة للعلاقة (14–5) التي تبين الترميز بـ $2k$ رمزاً للمعلومات بكثير الحدود $g(x^2)$ وكنتيجة نحصل على ترميز التداخل.

العدد j للكلمات يسمى درجة التداخل. المثال السابق درجة التداخل $j=2$.

في الحالة العامة عندما نداخل j كلمة مرمزة الكلمة المتداخلة لها طول jn ونحصل عليها من ترميز jk رمز معلومات لكثير حدود $g(x^j)$ من السهولة رؤية الترميز المتداخل له سعة تصحيح رزمة من الأخطاء أكبر من ترميز التداخل لبيان هذا العمل نفترض $j=2$ والترميز غير المتداخل يمكن أن يصحح خطأين متجاورين (أي أن طول رزمة الأخطاء $\ell = 2$) نفترض أنه ظهر رزمة من الأخطاء المضاعفة طوله $\ell = 4$ وهو يؤثر على الرموز $a_0^{(1)}$ $a_0^{(2)}$ $a_1^{(1)}$ $a_1^{(2)}$

هذه الأخطاء يمكن تصحيحها حيث إذ إنها تحتوي على رمزين متجاورين من كل كلمة $a_0^{(1)}$ $a_1^{(1)}$ و $\alpha_0^{(2)}$ $\alpha_1^{(2)}$ من الترميز المتداخل.

على العموم يمكن القول إن الترميز غير المتداخل يمكن تصحيح رزمة من الأخطاء طوله ℓ. ترميز التداخل له درجة تداخل j يمكن تصحيح رزمة من الأخطاء طوله $j\ell$.

إذاً الأخطاء لا تدخل في الرزم (هي مستقلة) يكون ترميز المتداخل يكافئ بالترميز غير المتداخل بحيث أن التطبيقات المتداخلة على العموم بأخطاء مستقلة (المعطيات ضجيج التشويش) وكذلك رزمة الأخطاء (معطيات الضجيج للنبضات) طريقة التداخل تمثل أهمية عظمى.

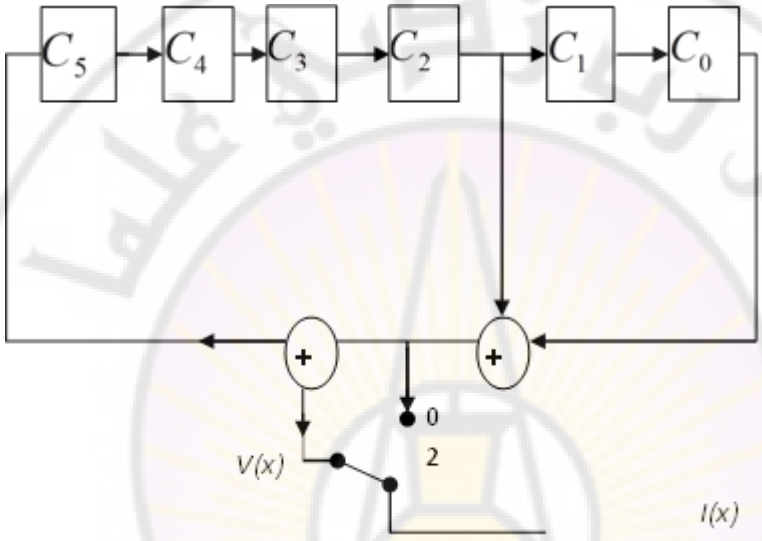
<u>مثال:</u>

لنفترض مصحح أخطاء $n=7$, $k=4$, $m=3$ بترميز $g(x)=1+x+x^3$

من أجل درجة تداخل $j=2$ سنقوم بترميز $2k=8$ كرموز معلومات

$g(x^2)=1+x^2+x^6$

من الدرجة $2m=6$ وطبقاً للمخطط:



الشكل (6-8) دارة ترميز حسب كثير الحدود $g(x^2)=1+x^2+x^6$

وقل رب زدني علما
جامعة دمشق
Damascus University

حل مسائل الفصل الرابع

المسألة (1):

الحل:

تتمم عمليات التحويل بين العناصر على الشكل التالي:

– نبدل بين العامودين الأول و الثالث

– ثم نبدل بين العامود الأول (الجديد و الرابع)، نحصل على المصفوفة التالية:

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

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

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

ب – نتحقق بسهولة بأن المصفوفة H تجمع كل عامودين و لا تعطي عاموداً يساوي الصفر (أي كل عامودين هما مستقلان خطيا) إذاً هذا الترميز يستطيع أن يكشف خطأين و يصحح خطأ واحد.

المصفوفة 'H لها نفس الأعمدة و لكنها مرتبة بشكل آخر، إذاً المصفوفة 'H هي مصفوفة مراقبة لترميز يكشف خطأين أو يصحح خطأ واحد.

ج) بما أن $n = 7$، ينتج أن $m=3$، $K = 4$، و للحصول على معادلات تظهر فيها إحدى رموز المراقبة مرة واحدة نختار ما يلي:

في حال المصفوفة H و الرموز التي تقابل الأعمدة التي تحتوي على عنصر واحد و الباقي أصفار أي:

$C_1 = a_1 , C_2 = a_2 , C_3 = a_4$

$C_1 = a_1 = a_3 + a_5 + a_7$

$C_2 = a_2 = a_3 + a_6 + a_7$

$C_3 = a_4 = a_5 + a_6 + a_7$

و في حال المصفوفة 'H:

$C_1 = a_1 = a_5 + a_6 + a_7$

$C_2 = a_2 = a_4 + a_6 + a_7$

$C_3 = a_3 = a_4 + a_5 + a_7$

المسألة (2):

نضع المصفوفة H على شكل $H'=[\ I_3\ Q\ ]$ وحسب المسألة (1) ينتج :

$$P= Q^T = \begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\end{bmatrix} \qquad Q = \begin{bmatrix}0 & 1 & 1 & 1\\ 1 & 0 & 1 & 1\\ 1 & 1 & 0 & 1\end{bmatrix}$$

$$G= [\ P\ I_K\ ]= \begin{bmatrix}0 & 1 & 1 & 1 & 0 & 0 & 0\\ 1 & 0 & 1 & 0 & 1 & 0 & 0\\ 1 & 1 & 0 & 0 & 0 & 1 & 0\\ 1 & 1 & 1 & 0 & 0 & 0 & 1\end{bmatrix}$$

$$C = ip = [\ a_4\ a_5\ a_6\ a_7\ ] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = [\ a1\ a2\ a3\ ]$$

أي نحصل على رموز المركبة كما حصلنا عليها في المسألة (1) في حالة المصفوفة 'H

$a_1 = a_5 + a_6 + a_7$

$a_2 = a_4 + a_6 + a_7$

$a_3 = a_4 + a_5 + a_7$

المسألة (3):

الحل :

أ–هذا يعني أنه يوجد خطأ واحد في الوضعية المشار إليها بالرقم الثنائي أي في الوضعية (2).

$$Z = \begin{bmatrix} C_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} h_2 \\ 1 \end{bmatrix} \quad , \ h_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$Z = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, الوضعية a'_0 خاطئة

ج –

$$Z = \begin{bmatrix} h_3 + h_4 \\ 0 \end{bmatrix}$$

يوجد خطآن لا يمكن تصحيحهما.

المسألة (4):

الحل:

في الحالة الأولى m.n (عملية الضرب) و m.n (عملية جمع)

أما في الحالة الثانية m. k (عملية ضرب) و m. k + k (عملية جمع)

يتم حساب المصحح من العلاقة $Z^T = [C' + C'']$

المسألة (5):

الحل:الكلمة الخاطئة في هذه الحالة

$\varepsilon = [\varepsilon_0\ \varepsilon_1\ \varepsilon_2\ \varepsilon_3\ \varepsilon_4\ \varepsilon_5\ \varepsilon_6\ \varepsilon_7]$

في حالة المصحح Z_1العدد الثنائي 001 يشير إلى الخطأ في المكان $\varepsilon_1=1$، بقية رموز الكلمة $\varepsilon_0 = \varepsilon_2 = \varepsilon_3 = \varepsilon_4= \varepsilon_5= \varepsilon6= \varepsilon_7 = 0$.

في حال المصحح Z_2 , $\varepsilon_5= 1$ وفي حال المصححZ_3 , $\varepsilon_0 =1$ في حال المصحح Z_4 لدينا خطآن وبالتالي لن يكون تقابل بين الكلمة الخاطئة و المصحح في هذه الحالة الكلمة الخاطئة لا يمكن تحديدها.

المسألة (6):

الحل :

آ – الترميز ليس كاملاً بسبب أن عدد المصححات $nz = 23 = 8$ ولكن عدد الكلمات الخاطئة برمز واحد هو 6 كلمات، ينتج من ذلك أنه إلى جانب عملية التصحيح لخطأ واحد فإن هذا الترميز قادر على تصحيح بعض من الأخطاء المضاعفة.

ب – إذا اعتبرنا العلاقة $Z = H\varepsilon^T$ نحصل على التقابل بين الكلمات الخاطئة و المصححات.

ε	000001	000010	000100	001000	010000	100000	010010 001100 100001
z^T	011	101	100	110	010	100	111

إذا كان المصحح 010 نأخذ قرارا أنه حصل خطأ في المكان الثاني.

إذا كان المصحح 111 الاحتمال الأكبر أنه لدينا كلمة بخطأين في الأماكن المشار إليهما في الجدول السابق إذ لهما المصحح نفسه 111.

الاحتمالية الأقل أن المصحح 111 يمكن أن يكون من كلمة خاطئة مكونة من ثلاثة أخطاء مثال 111000.

مسألة(7):

الحل :

في المرمز (التام) لدينا $2^m = n+1 = k+m+1$ إذاً معدل المعلومات

$$R = k/n = \frac{2^m - m - 1}{2^m}$$

في الترميز التكرارية عدد رموز المعلومات هو SK_0 (S :عدد الصفوف, K_0 عدد الأعمدة في المصفوفة لرموز المعلومات).

عدد رموز المراقبة $m_i = S + k_0 + 1$

إذا $n = Sk_0 + S + k_0 + 1$

ولكن معدل المعلومات يكون

$$R_i = \frac{sk0}{sk0 + s + k0 + 1}$$

وبمقارنة كلا العلاقتين نرى أن R تمتد بسرعة نحو 1 أكثر من R_i

في عبارات R و R_i نضع m = 5

$$R = [32 - 5 - 1] / [32 - 1] = 0,84 \text{ bit/ symbol}$$

m = 10 يكون لدينا:

$$R = [1024 - 10 - 1] / [1024 - 1] = 0,99 \text{ bit/ symbol}$$

ب- في حالة الترميز التكراري بالعدد نفسه من رموز المعلومات يكون لدينا في الحالة الأولى

$$R_i = [26] / [26 + S + k_0 + 1]$$

وبما أن $Sk_0 = k$ ثابت فإن المجموع $S + k_0$ يكون أصغرياً عندما $S = k`_0$

إذا في هذه الحالة $S = 5$

ولكن

$$R_i = [26] / [26 + 2.5 + 1] = 0,7 \text{ bit/symbol}$$

في الحالة التي $k = Sk_0 = 1013$ لدينا $s \approx 32$

$$R_i = [1013] / [1013 + 32.2 + 1 = 0,94 \text{ bit/ symbol}$$

مما سبق: ينتج أن معدل المعلومات للترميز التامة هو أفضل مما هو عليه في الترميز التكرارية.

حل مسائل الفصل الخامس

مسألة (1):

الحل :

فئـــــات البـــــاقي للنمـــــوذج $p(x)=x^3+1$ هـــــي مـــــن الشـــــكل

$\{a_0 + a_1x + a_2x^2\} = a_0 + a_1 X + a_2 X^2 \in A$ حيث $a_i \in GF(2)$

إذا كانت فئات الباقي تشكل الجبر A لابد من أن ناتج جداء فئتين للباقي يعطي فئة الباقي للنموذج p(x).

ليكن الجداء لفئتين باقي

$$u(X).v(X) = (a_0 + a_1 X + a_2 X^2)(b_0 + b_1 X + b_2 X^2) =$$
$$a_0b_0+(a_0b_1+a_1b_0)X+(a_0b_2+a_1b_1+a_2b_0)X^2+(a_1b_2+a_2b_1)X^3+a_2b_2X^4$$

وبما أن p(x) يوجد في الفئة الأولى $p(X)= X^3 + 1 = 0$ فيكون الجداء السابق

$$u(X).\ v(X) = a_0b_0 + a_1b_2 + a_2b_1 + (a_0b_1 + a_1b0 + a_2b_2)X + (a_0b_2 + a1b_1 + a_2b_0)X^2 = C_0 + C_1X + C_2X^2$$

حيث أن C_i , (i= 0, 1, 2.....) أمثال X^i

إذا $u(X) \in A$ و $v(X) \in A$

حينئذ بسبب أن $P(X) = X^3 + 1 = 0$ لدينا $u(X).v(X) \in A$

مسألة (2):

الحل:

$$v(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6$$

$i(x) = i_0 + i_1x + i_2x^2 + i_3x^3$

$g(x) = g_0 + g_1x + g_2x^2 + x^3$

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & 1 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & 1 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & 1 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & 1 \end{bmatrix}$$

$$V = iG =$$

$$[i_0\ i_1\ i_2\ i_3] \begin{bmatrix} g_0 & g_1 & g_2 & 1 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & 1 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & 1 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & 1 \end{bmatrix}$$

ينتج من ذلك أن :

$a_0 = g_0\, i_0$, $a_1 = g_1\, i_0 + g_0\, i_1$,$a_2 = g_2\, i_0 + g_1\, i_1 + g_0\, i_2$

$a_3 = i_0 + g_2\, i_1 + g_1 i_2 + g_0\, i_3$, $a_4 = i_1 + g_2\, i_2 + g_1\, i_3$,

$a_5 = i_2 + g_2\, i_3$, $a_6 = i_3$

من جهة أخرى:

$V(x) = i(x).g(x) = g_0\, i_0 + (g_1\, i_0 + g_0\, i_1)x + (g_2\, i_0 + g_1\, i_1 + g_0\, i_2)x^2 + (i_0 + g_2 i_1 + g_1 i_2 + g_0 i_3)x^3 + (i_1 + g_2 i_2 + g_1 i_3)x^4 + (i_2 + g_2\, i_3)x^5 + i_3 x6$

ينتج من التدقيق $v = iG$ مع $v(x) = i(x).g(x)$ يعطيان نفس الكلمة.

مسألة(3):

الحل:

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & 1 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & 1 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & 1 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 0 & 0 & h_4 & h_3 & h_2 & h_1 & h_0 \\ 0 & h_4 & h_3 & h_2 & h_1 & h_0 & 0 \\ h_4 & h_3 & h_2 & h_1 & h_0 & 0 & 0 \end{bmatrix}$$

ناتج جداء المصفوفتين

$$G.H^T \begin{bmatrix} e_{11} & e_{12} & e_{13} \\ e_{21} & e_{22} & e_{23} \\ e_{31} & e_{32} & e_{33} \end{bmatrix}$$

e_{11}=<$g_0g_1g_21000$><$00h_4h_3h_2\ h_1h_0$>

e_{12} = < $g_0\ g_1g_2\ 1000$ > < $0h_4\ h_3\ h_2\ h_1\ h_0\ 0$>

e_{13} = < $g_0\ g_1g_2\ 1000$ > < $h_4\ h_3\ h_2\ h_1h_00$>

وبالطريقة نفسها نحصل على بقية الأمثال (المعاملات) من العلاقة

$g(x).h(x)=0$

ينـتج أن الجـداء السـلمي معـدوم حيـث أن مركبـات الشـعاع h(x) مكتوبـة بالترتيب العكسي

$< g_0\ g_1 g_2\ 1000\ > <\ 00 h_4\ h_3\ h_2\ h_1\ 00> = 0$

إذا جميـع الجـداءات السـلمية التـي نحصـل عليهـا مـن خـلال النقـل الـدوري للمركبات تكون معدومة. ينتج من ذلك أن جميع عناصر e_{ij} معدومة أي أن $GH^T = 0$ ومن خلال عملية النقل لهذه العلاقة ينتج $HG^T = 0$

مسألة(4):

الحل :

فـي حـال المرمز التـام عدد المصـححات يسـاوي إلـى عدد الكلمـات الخاطئـة التـي يمكـن تصـحيحها $N_\varepsilon = 2^m - 1 = 7$ إذاً هنـاك 7 مصـححات للكلمـة الخاطئة لتصحح رمزا واحداً في أي مكان من الكلمة.

$$Z_i(x) = rest\frac{\varepsilon(x)}{g(x)} \qquad i = 1,2\ldots\ ,7$$

$$Z_1(x) = rest\frac{\varepsilon_1(x)}{g(x)} = rest\frac{1}{1+x+x^3} = 1$$

$$Z_2(x) = rest\frac{\varepsilon_2(x)}{g(x)} = rest\frac{x}{1+x+x^3} = x$$

$$Z_3(x) = rest\frac{\varepsilon_3(x)}{g(x)} = rest\frac{x^2}{1+x+x^3} = x^2$$

$$Z_4(x) = rest\frac{\varepsilon_4(x)}{g(x)} = rest\frac{x^3}{1+x+x^3} = x+1$$

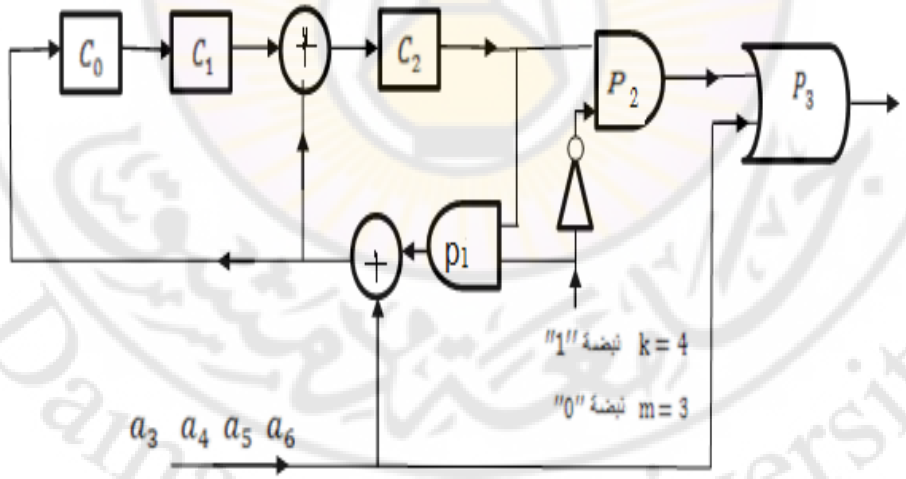
$$Z_5(x) = rest\frac{\varepsilon_5(x)}{g(x)} = rest\frac{x^4}{1+x+x^3} = x^2+x$$

$$Z_6(x) = rest\frac{\varepsilon_6(x)}{g(x)} = rest\frac{x^5}{1+x+x^3} = x^2 + x + 1$$

$$Z_7(x) = rest\frac{\varepsilon_7(x)}{g(x)} = rest\frac{x^6}{1+x+x^3} = x^2 + 1$$

ε	0000001	0000010	0000100	0001000	0010000	0100000	1000000
z	001	010	100	011	110	111	101

مسألة(5):



الدارة	I(X)	C0	C1	C2	Z(X)
0	0	0	0	0	0
1	a_6	a_6	0	a_6	a_6
2	a_5	a_5+a_6	a_6	a_5+a_6	a_5
3	a_4	$a_4+a_5+a_6$	a_5+a_6	a_4+a_5	a_4
4	a_3	$a_3+a_4+a_5$	$a_4+a_5+a_6$	$a_3+a_4+a_6$	a_3
5		0	$a_3+a_4+a_5$	$a_4+a_5+a_6$	$a_2=a_3+a_4+a_6$
6		0	0	$a_3+a_4+a_5$	$a_1=a_4+a_5+a_6$
7		0	0	0	$a_0=a_3+a_4+a_5$

ب – نحصل على رموز المراقبة من الجدول بدلالة رموز المعلومات حسب المعادلات:

$$a_0 = a_3 + a_4 + a_5$$
$$a_1 = a_4 + a_5 + a_6$$
$$\boldsymbol{a_2} = a_3 + a_4 + a_6$$

ج –

$$c(x) = rest\frac{x^m . i(x)}{g(x)}$$
$$= rest\frac{a_3\,x^3 + a_4\,x^4 + a_5\,x^5 + a_6\,x^6}{1 + x^2 + x^3}\; a_2 = a_3 + a_4 + a_6$$

$$a_6\,x^3+(a_5+a_6)\,x^2+(a_4+a_5+a_6)x+(\,a_3+a_4+a_5)$$

x^3+x^2+1 | $a_6\,x^6+a_5\,x^5+a_4\,x^4+a_3\,x^3$

$$a_6\,x^6+a_6\,x^5+a_6\,x^3$$

$$(a_5+a_6)\,x^5+a_4\,x^4+(a_3+a_6)\,x^3$$

$$(a_5+a_6)\,x^5+(a_5+a_6)\,x^4+(a_5+a_6)\,x^2$$

$$(a_4+a_5+a_6)\,x^4+(a_3+a_6)\,x^3+(a_5+a_6)\,x^2$$

$$(a_4+a_5+a_6)\,x^4+(a_4+a_5+a_6)\,x^3+(a_4+a_5+a_6)x$$

$$(a_3+a_4+a_5)\,x^3+(a_5+a_6)\,x^2+(a_4+a_5+a_6)x$$

$$(a_3+a_4+a_5)\,x^3+(a_3+a_4+a_5)\,x^2+(a_3+a_4+a_5)$$

$$\underbrace{(\,a_3+a_4+a_6}_{a_2}\,)\,x^2+\underbrace{(\,a_4+a_5+a_6}_{a_1}\,)x+\underbrace{(\,a_3+a_4+a_5}_{a_0}\,)$$

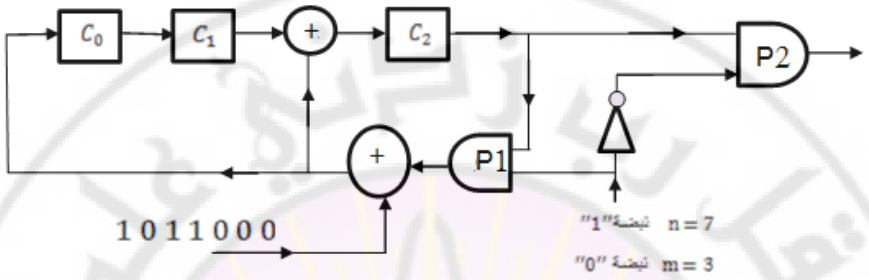
رموز المراقبة بدلالة رموز المعلومات (معادلات الترميز) :

$a_0=a_3+a_4+a_5$

$a_1=a_4+a_5+a_6$

$a_2=a_3+a_4+a_6$

مسألة(6):



كما رأينا المسألة في السابقة فان هذه الدارة تقوم بعملية التقسيم $x^m v'(x)$ على $g(x)= 1+x^2+x^3$ (حيث هنا بدل $i(x)$ أصبح $v'(x)$)

نفترض أن رزمة الأخطاء L=4

$\varepsilon = [0001111]$

$\varepsilon(x) = x^2 + x^3 + x^4 + x^5$

لنفترض أن الرسالة المرسلة هي:

$k = [0001]$ أي $a_3 =1, a_4 = 0, a_5 = 0, a_6 = 0$

$a_3\ a_4\ a_5\ a_6$

ومن المسألة السابقة يعطي $a_2 =1\ ,\ a_1 = 0, a_0 = 1$

حيث

$a_2 = a_6 + a_4 + a_3 = 1$

$a_1 = a_6 + a_5 + a_4 = 0$

$a_0 = a_5 + a_4 + a_3 = 1$

إذا الكلمة المرمزة المرسلة هي من الشكل [1011000] , $v(x) = x^3 +$

$x^2 + 1$

والكلمة المستقبلة هي

$v'(x) = v(x) + \varepsilon(x) = x^5 + x^4 + 1$

وسيتم عمل كاشف الترميز على الشكل التالي :

أ- عندما لا يوجد أخطاء

$v'(x) = v(x) = x^3 + x^2 + 1$

$v(x)$	C_0	C_1	C_2	الخرج
0	0	0	0	0
$a_6 = 0$	0	0	0	0
$a_5 = 0$	0	0	0	0
$a_4 = 0$	0	0	0	0
$a_3 = 1$	1	0	1	0
$a_2 = 1$	0	1	0	0
$a_1 = 0$	0	0	1	0
$a_0 = 1$	0	0	0	0

يفرغ المسجل0

ب – الحالة الثانية وجود أخطاء

$$v'(x) = v(x) + \varepsilon(x) = x^5 + x^4 + 1$$

ويكون الجدول على الشكل التالي:

	$V_1(X)$	C_0	C_1	C_2	الخرج
0		0	0	0	0
a_6=0		0	0	0	0
a_5=0		0	0	0	0
a_4=1		0	1	0	0
a_3=0		0	0	1	0
a_2=0		1	0	1	0
a_1=0		1	1	1	0
a_0=1		0	1	1	0

1

1 إفراغ المسجل

0

وبما أن محتوى المسجل هو "0" فإن رزمة الأخطاء تم كشفه على اعتبار أنه يوجد في المسجل c_0,c_1,c_2

0 0 1

يمكن أن نصل إلى هذه النتيجة إذا حسبنا محتوى المسجل المشار إليه

$$r(x) = rest\ [\frac{x^m\, v(x)}{g(x)} = rest\ \frac{x^3(1+x^4+x^5)}{1+x^2+x^3}$$

إذا الباقي $r(x) = x^2+x$

مسألة (7) :

الحل: نفترض الحالة الأولى:

$$T= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \; ; \quad U_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

وتكون الحالات المتتالية حسب المصفوفة T:

$$T^4U_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \; ; T^3U_1 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} ; T^2U_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} ; TU_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$; \; T^7U_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} ; T^6U_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} ; \; T^5U_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

إذاً يولد المسجل جميع الحالات غير المعدومة وهي $2^3-1 = 7$ ضمن دورة واحدة وذلك بسبب أن كثير الحدود $g(x) = x^3+x+1$ هو أولي.

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

$$U_1 = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \quad , \quad TU_1 = \begin{bmatrix}0\\0\\1\\1\end{bmatrix} \; ; T^2U_1 = \begin{bmatrix}0\\1\\1\\0\end{bmatrix} ; \; T^3U_1 = \begin{bmatrix}1\\1\\0\\0\end{bmatrix} \; ;$$

$$T^4U_1 = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} ; \; T^5U_1 = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} = U_1$$

إذاً الدورة انتهت بعد 5 حالات إذا اعتبرنا الحالة الثانية :

$$U_2 = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \; ; TU_2 = \begin{bmatrix}0\\1\\0\\1\end{bmatrix} \quad ; T^2U_2 = \begin{bmatrix}1\\0\\1\\0\end{bmatrix} ;$$

$$T^5U_2 = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} = U_2 \; ; T^4U_2 = \begin{bmatrix}1\\0\\0\\1\end{bmatrix} ; T^3U_2 = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

كذلك الدورة هنا 5 حالات:

لنعتبر الحالة البدائية والتي لم تكتب مولدة في دورات المسجل السابقة

$$U_3 = \begin{bmatrix}1\\1\\1\\1\end{bmatrix} ; TU_3 = \begin{bmatrix}1\\1\\1\\0\end{bmatrix} ; T^2U_3 = \begin{bmatrix}1\\1\\0\\1\end{bmatrix} ; T^3U_3 = \begin{bmatrix}1\\0\\1\\1\end{bmatrix} ; T^4U_3 = \begin{bmatrix}0\\1\\1\\1\end{bmatrix}$$

$$T^3U_3 = \begin{bmatrix}1\\1\\1\\1\end{bmatrix} = U_3$$

في النتيجة جميع الحالات $2^4 - 1 = 15$ التي لا تساوي الصفر مولدات بثلاث دورات طول كل واحدة "5" التساوي في طول الدورات هو ناتج عن أن كثير الحدود $g(x) = 1+ x+x^2+x^3+x^4$ ليس له جذور و ليس أولياً (ليس لدينا دورة بطول أعظمي).

ج-

$$T = \begin{bmatrix}0 & 1 & 0\\0 & 0 & 1\\1 & 1 & 0\end{bmatrix}; U_1 = \begin{bmatrix}0\\0\\1\end{bmatrix}; TU_1 = \begin{bmatrix}0\\1\\1\end{bmatrix};$$

$$T^2U_1 = \begin{bmatrix}1\\1\\0\end{bmatrix}; T^3U_1 = \begin{bmatrix}1\\0\\0\end{bmatrix}; T^4U_1 = \begin{bmatrix}0\\0\\1\end{bmatrix} = U_1$$

إذا أول دورة لها أربع حالات:

لنعتبر الحالة البدائية

$U_2 = \begin{bmatrix}1\\0\\1\end{bmatrix}$ التي لم تكن مولدة مسبقا , الدورة الثانية لها حالتان:

$$TU_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} ; T^2U_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = U_2$$

لنعتبر الحالة البدائية: $U_3 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ التي لم تكن مولدة

الدورة الثالثة حالة واحدة فقط : $TU_3 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = U_3$

في النتيجة إن جميع الحالات التي لا تساوي الصفر للمسجل مولدة بثلاث دورات طول كل واحدة (4,2,1) ينتج عن ذلك أن كثير الحدود هو ليس أولياً و ليس من النوع الذي له جذور.

النتيجة النهائية إذا كان كثير الحدود المولد أولياً يولد جميع الحالات في دورة واحدة و إذا كان ليس له جذور وليس أولياً يولد عدد دورات متساوية الحالات وإذا كان غير أولي ومحللاً لجذور فإن عدد الدورات غير متساوية .

مسألة(8):

الحل:

طبقا للرموز الموجودة على الشكل , نعتبر أن حالة المسجل Σ في اللحظة t و Σ' في اللحظة t' التالية:

$$\Sigma = \begin{bmatrix} \boldsymbol{\sigma}0 \\ \sigma 1 \\ \boldsymbol{\sigma}2 \\ . \\ . \\ \sigma m-1 \end{bmatrix} \qquad \boldsymbol{\Sigma}' = \begin{bmatrix} \boldsymbol{\sigma}_0' \\ \boldsymbol{\sigma}_1' \\ . \\ . \\ \boldsymbol{\sigma}_{m-1}' \end{bmatrix}$$

وبتتبع مراحل المخطط (الشكل) للمسجل نحصل على :

$\boldsymbol{\sigma}_0' = \ldots\ldots\ldots \ldots . \ g_0 \ \boldsymbol{\sigma}_{m-1}$

$\boldsymbol{\sigma}_1' = \boldsymbol{\sigma}_0 + \ldots\ldots \ldots . \ g_1 \ \boldsymbol{\sigma}_{m-1}$

$\boldsymbol{\sigma}_2' = \boldsymbol{\sigma}_1 + \ldots\ldots \ldots . \ g_2 \ \boldsymbol{\sigma}_{m-1}$

$\boldsymbol{\sigma}_{m-1}' = \ldots\ldots\ldots \ldots \boldsymbol{\sigma}_{m-2} + g_{m-1} \ \boldsymbol{\sigma}_{m-1}$

$$\boldsymbol{\tau} = \begin{bmatrix} 0 & 0 & 0 & 0 & \ldots & \ldots 0 & 0 & g_0 \\ 1 & 0 & 0 & 0 & \ldots \ldots & & & g_1 \\ 0 & 1 & 0 & 0 & & & & g_2 \\ . & \ldots & & \ldots & \ldots & .. & .. & \ldots \\ . & & \ldots & . & . & & . & \\ 0 & 0 & 0 & 0 & \ldots . & & 1 & g_{m-1} \end{bmatrix}$$

وبالتالي يمكن أن نكتب :

$\Sigma' = \boldsymbol{\tau} \ \Sigma$

ب–لنعتبر كثير الحدود لهذه الدارة:

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

$$\boldsymbol{\tau} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\boldsymbol{\Sigma}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \; ; \; \boldsymbol{\tau}^0\boldsymbol{\Sigma}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \; ; \; \boldsymbol{\tau}\boldsymbol{\Sigma}_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$\boldsymbol{\tau}^2\boldsymbol{\Sigma}_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \; ; \; \boldsymbol{\tau}^3\boldsymbol{\Sigma}_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} ; \boldsymbol{\tau}^4\boldsymbol{\Sigma}_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \; ; \; \boldsymbol{\tau}^5\boldsymbol{\Sigma}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

إذاً طول الدورة يساوي 5 كما هو الحال في الشكل(5-7) ولكن:

$$\boldsymbol{\Sigma}_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \; ; \boldsymbol{\tau}^0\boldsymbol{\Sigma}_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \boldsymbol{\tau}\boldsymbol{\Sigma}_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \; ; \; \boldsymbol{\tau}^2\boldsymbol{\Sigma}_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

$$\boldsymbol{\tau}^3\boldsymbol{\Sigma}_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} ; \quad \boldsymbol{\tau}^4\boldsymbol{\Sigma}_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \; ; \; \boldsymbol{\tau}^5\boldsymbol{\Sigma}_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

الدورة طولها 5 :

إذا كان كثير الحدود $g(x)= 1+x+x^2+x^3$

$$\tau = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \; ; \; \Sigma_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \; ; \; \tau^0 \Sigma_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \; ;$$

$$\tau\Sigma_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} ; \; \tau^2 \Sigma_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \; ; \; \tau^3 \Sigma_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \; ; \; \tau^4 \Sigma_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

إذا الدورة تساوي 4 حالات:

إذا كانت الحالة :

$$\Sigma_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \; , \tau\Sigma_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \; , \; \tau^2 \Sigma_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

إذا الدورة مكونة من حالتين.

إذا كانت الحالة :

$$\Sigma_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \; ; \; \tau\Sigma_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

إذا الدورة مكونة من حالة واحدة فقط.

فـي النتيجـة نقول إن المسـجلات فـي الشكلين(5–7) و (5–9) تولـد دورة ذات طول واحد.

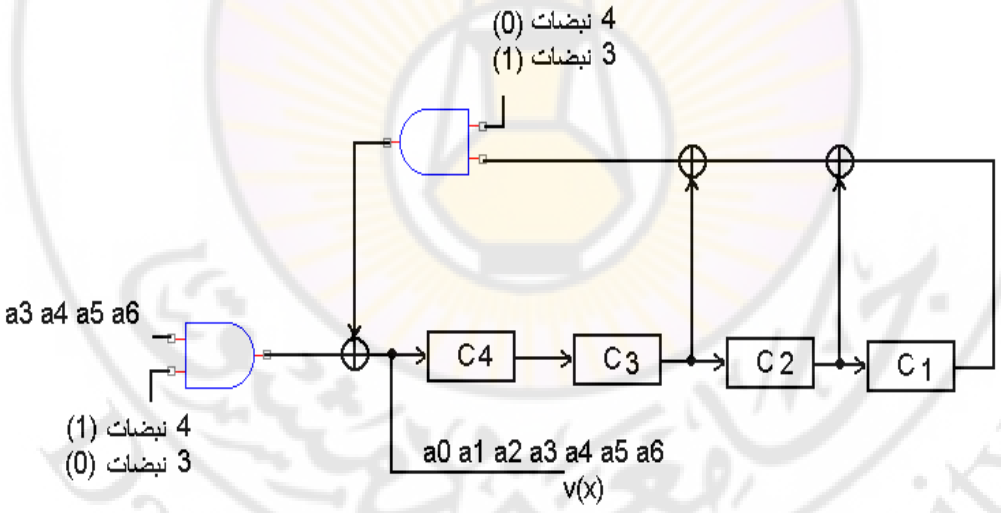
مسألة(9):

الحل:

كثير الحدود :

$$h(x) = \frac{1+x^7}{1+x+x^3} = 1 + x + x^2 + x^4$$

مخطط الدارة



جدول الحالات:

i(x)	C_4	C_3	C_2	C_1	v(x)
0	0	0	0	0	0
a_6	a_6	0	0	0	a_6
a_5	a_5	a_6	0	0	a_5
a_4	a_4	a_5	a_6	0	a_4
a_3	a_3	a_4	a_5	a_6	a_3
0	$a_4+a_5+a_6$	a 3	a_4	a_5	$a_2=a_4+a_5+a_6$
0	$a_3+a_4+a_6$	$a_4+a_5+a_6$	a_3	a_4	$a_4=a_3+a_4+a_5$
0	$a_3+a_5+a_6$	$a_3+a_4+a_5$	$a_4+a_5+a_6$	a_3	$a_0=a_3+a_5+a_6$

المصطلحات

Communications	الاتصالات
Monolithic	أحادي
Framing	إحاطة الإطار
Burst Errors	الأخطاء الحزمية
Random Errors	الأخطاء العشوائية
Transmission Modes	أساليب التراسل
Signal	إشارة
automatic Repeat Request –ARQ	إعادة الإرسال تلقائيا
Semaphore	أعلام الإشارة
Virtual	افتراضي
Error Detection	اكتشاف الأخطاء
Cross entropy	الإنتروبية المتقاطعة
Conditional Entropy	الإنتروبية المشروطة
Information entropy	إنتروبية المعلومات
Joint entropy	إنتروبية المفصل
Differential entropy	إنتروبية تفاضلية
Rényi entropy	إنتروبية رينيي

Conditional entropy	إنتروبية شرطية
Technology Planning Model	أنموذج للخطة المعلوماتية
Types of Errors	أنواع الأخطاء
Objectives	الأهداف الخاصة
Goals	الأهداف العامة
Bit Stuffing	بت الحشو
Cyclic Redundancy Check–CRC	البت الزائدة الدوري
Longitudinal Redundancy Check–LRC	البت الزائدة الطولي
Parity check Bit	البت المكافئة
Utilities	البرامج المساعدة
Network Card	بطاقة أو كارت الشبكة
Gateways	بوابات العبور
parsed data	بيانات التحليل
Error Control	التحكم و معالجة الأخطاء
Technology Planning	التخطيط المعلوماتي
Inter–symbol Interference	تداخل الرموز
Cross Talk	التداخل المتعارض أو اعتراض الكلام
Attenuation	التدهور أو التوهين
Logging	تدوين الأحداث
Simplex Mode	التراسل الأحادي البسيط

Full Duplex Mode–FDX	التراسل الثنائي
Parallel Transmission	التراسل المتوازية
Serial Transmission	التراسل المتوالية
Half Duplex Mode –HDX	التراسل نصف الثنائي
Expression	تركيب
Syntax	التركيب النحوي
Prefix code	ترميز البادئة
Character encoding	ترميز الحروف
Scrambled Encoding	الترميز المختلط
Source coding	ترميز المصدر
Encoding	الترميز
Time Jitter	التزحزح الزمني
Encryption	التشفير
Delay Distortion	تشوه التأخير
Error Correction	تصحيح الأخطاء
Error Correction	تصحيح الأخطاء
Forward Error Correction–FEC	تصحيح الأخطاء الأمامي
Orthogonally	تعامد
Regular expression	تعبير نمطي
Definition	تعريف

Reinforcement	التعزيز
Evaluation	التقويم
Quantification	تكمية
Telegraphers	التلغراف
Casting	تمثيل
Initialization	تهيئة
Constant	ثابت
Bridges	الجسور
Race condition	حالة تسابق
Subject	حد
Module	حزمة
loop	حلقة
Digital Data Service –DDS	خدمة البيانات الرقمية
Technology Plan	الخطة المعلوماتية
Constructor	الدالة المنشئة
Member function	دالة عضو
ISBN	الرقم الدولي المعياري للكتاب
Color code	رمز اللون
literal	رمز حرفي
Country calling codes	رموز الاتصال للبلدان

Variable-length code	رموزمتغيرة الطول
Symbols	رموز
Vision	الرؤية
Static	ساكن
Enumeration	سرد
Channel capacity	سعة القناة
Channel capacity	سعة القناة
Wide Web Site	الشبكة العنكبوتية
Asynchronous Transfer Mode (ATM)	شبكة النقل غير المتزامن
Code pages	صفحات الترميز
Type, data type	صنف
Buffer	صُوَان
Impulse Noise	الضجيج النبضي
Encoding of Digital Data	ترميز البيانات الرقمية
Template	طبعة
Digital Data Transmission Methods	طرق تراسل البيانات الرقمية
Member	عضو
Technology Plan Elements	عناصر الخطة المعلوماتية
Redundancy	فائض
Class	فئة

Linked list	قائمة متصلة
Channel communications	قناة معلومات
Null value	قيمة باطلة
Object	كائن
Singleton	كائن مفرد
Keyword	كلمة تعريفية
Entropy	كمية المعلومات
Secret code	للرموز السرية
Signaler	لمشير
Binary logarithm	اللوغاريتم الثنائي
Modifier	مبدِّل
Switches	المبدلات
Dynamic	متحرك
Compiler	المترجم
Variable	متغيّر
Member variable	متغير عضو
Global variable	متغير عمومي
Receiver information theory	متلقي نظرية المعلومات أو مستقبل
Space	مجال
Hubs	المجمعات

Basic Group	المجموعة الأساسية
Escape sequence	محرف مركب
Decoder	محلل الشفرة
Independent	مستقلان إحصائيًا أي
Encoder	مشفر
Source	المصدر
Communication source	مصدر اتصال
Information processing	معالجة المعلومات
Error Rate	معدل الخطأ
Symmetric	المعلومات المتبادلة
Mutual information	المعلومات المتبادلة
Mutual information	معلومات متبادل
Metadata	معلومات وصفية
Self-information	معلومة ذاتية
Transmission Impairments	معوقات التراسل
Specification	مواصفة
Standard	معيارية
Technology Plan Components	مقومات الخطة المعلوماتية
library	مكتبة
Stack	مكدِّس

Repeaters	المكررات
Interfacing	المواجهة بقنوات تراسل البيانات
Video Conferencing	المؤتمرات الفيديوفونية
operator	مؤثر
Routers	الموجهات
plain pointer	مؤشر بسيط
Smart pointer	مؤشر ذكي
Network Operating System	نظام تشغيل الشبكة
Formal language theory	نظرية اللغات الشكلية
Information theory	نظرية المعلومات
Codepoint	نقطة ترميز
Target	الهدف
Virtual Reality	الواقع الافتراضي
Inheritance	وراثة (توريث)
"Secondary Synchronization Codes	ورموز التزامن الثانوي
Multimedia	الوسائط المتعددة
Interface	وسيط
Concatenate	وصل

المراجع

1) E. Agrell, A. Vardy, and K. Zeger, "A table of upper bounds for binary codes," IEEE Trans. Inform. Theory, Vol. 47, No. 7, pp. 3004-3006, November 2001 S.
2) Benedetto and E. Biglieri, Digital Transmission Principles with Wireless Applications New York: Kluwer/Plenum, 1999.
3) R. E. Blahut, Algebraic Codes for Data Transmission. Cambridge, UK: Cambridge
4) University Press, 2003.
5) G. D. Forney, Jr., "Geometrically uniform codes," IEEE Trans. Inform. Theory, Vol.37, No. 5, pp. 1241-1260, September 1991.
6) G. D. Forney, Jr., and G. Ungerboeck, "Modulation and coding for linear Gaussian channels," IEEE Trans. Inform. Theory, Vol. 44, No. 6, pp. 2384-2415, October 1998.

7) W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes. Cambridge,UK: Cambridge University Press, 2003.

8) S. Lin and D. J. Costello, Jr, Error Control Coding (2nd edition). Upper Saddle River, NJ: Pearson Prentice Hall, 2004.

9) F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1977.

10) J. L. Massey, "Towards an information theory of pread-spectrum systems," in: S. G.Glisic and P. A. Leppanen (eds.), Code Division Multiple Access Communications, pp. 29-46. Boston, MA: Kluwer, 1995.

11) R. J. McEliece, The Theory of Information and Coding (2nd edition). Cambridge,UK: Cambridge University Press, 2002.

12) D. Slepian, "On bandwidth," IEEE Proc., Vol. 64, No. 3, pp. 292-300, March 1976.

A. J. Viterbi, Principles of Coherent Communication. New York: McGraw-Hill,1966.

13) L. Zheng and D. N. C. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple antenna

channels," IEEE Trans. Inform. Theory, Vol. 49, No. 5, pp. 1073-1096, May 2003.

14) S. Benedetto and E. Biglieri, Digital Transmission Principles with Wireless Applications.New York: Kluwerfflenum, 1999.

15) J. B. Cain, G. C. Clark, Jr., and J. M. Geist, "Punctured convolutional codes of rate (n - I) / n and simplified maximum likelihood decoding: IEEE Trans. Inform.Theory, Vol. 25, No. 1, pp. 97-100, January 1979.

16) J.-J. Chang, D.-J. Hwang, and M.-C. Lin, "Some extended results on the search for good convolutional codes," IEEE Trans. Inform. Theory, Vol. 43, No. 5, pp.1682-1697, September 1997.

17) G. D. Forney, Jr., "Convolutional codes. I: Algebraic structure," IEEE Trans. Inform.Theory, Vol. IT-16, No. 6, pp. 720-738, November 1970.

18) J. Hagenauer, "Rate-compatible punctured convolutional codes (RCPC codes) and their applications," IEEE Trans. Commun., Vol. 36, No. 4, pp. 389-400, April 1988.

19) . Heegard and S. B. Wicker, Turbo Coding. Boston, MA: Kluwer Academic, 1999.

20) R. Johannesson and Z.-X. Wan, "A linear algebra approach to minimal convolutional encoders," IEEE Trans. Inform. Theory, Vol. 39, No. 4, pp. 12 19-1233, July1993.

21) R. Johannesson and K. Sh. Zigangirov, Fundamentals of Convolutional Coding.Piscataway, NJ: IEEE Press, 1999.[6.9] R. Knopp, Coding and Multiple Access over Fading Channels, Ph.D. Thesis, ~ c o l ePolytechnique F6dbale de Lausanne, Lausanne, Switzerland, 1997.

22) K. J. Larsen, "Short convolutional codes with maximal free distance for rates 112,113 and 114," IEEE Trans. Inform. Theory, Vol. 19, No. 3, pp. 371-372, May 1973.

23) H. H. Ma and J. K. Wolf, "On tail biting convolutional codes," IEEE Trans. Commun.,Vol. 34, No. 2, pp. 104-1 11, February 1986.

24) H. Moon, "Improved upper bound on bit error probability for truncated convolutional codes," IEE Electronics Letters, Vol. 34, No. 1, pp. 65-66,8th January 1998.

A. J. Viterbi and J. K. Omura, Principles of Digital Communication and Coding.New York: McGraw-Hill, 1979.

25) Y. Yasuda, K. Kashiki, and Y. Hirata, "High-rate punctured convolutional codes for soft-decision Viterbi decoding," IEEE Trans. Commun., Vol. 32, No. 3, pp. 315-319, March 1984.

وقل رب زدني علما
جامعة دمشق
Damascus University

اللجنة العلمية:

الأستاذ الدكتور المهندس نديم شاهين

الأستاذ المساعد الدكتور المهندس محمد خالد شاهين

الدكتور المهندس محمد ميهوب

المدقق اللغوي

الأستاذ المساعد الدكتور حمود يونس