مجلة جامعة تشرين للدراسات والبحوث العلمية – سلسلة العلوم الأساسية المجلد (18) العدد (5) 1996
Tishreen University Journal for Studies and Scientific Research –Basic Science Series Vol. (18) No (5) 1996

دراسة نظرية للنقص في طول المكافئ الخطي لمتتالية غير خطية

أحمد حمزة الشيخة*

(قبل للنشر في 1995)

☐ الملخّص ☐

هذا البحث يبرهن أن السبب في عدم بلوغ طول المكافئ الخطي لمتتالية جداء (على H مرتبة من متتالية $\{a_n\}$) الحد الأعظمي N_h، يتعلق ليس فقط بجذور كثير الحدود المميز للمتتالية $\{a_n\}$ وإنما أيضاً بالمعاملات التي تعين الحد العام a_n.

* مدرس تعليم عالي – قسم الرياضيات – كلية العلوم – جامعة تشرين – اللاذقية – سورية.

مجلة جامعة تشرين للدراسات والبحوث العلمية – سلسلة العلوم الأساسية المجلد (18) العدد (5) 1996
Tishreen University Journal for Studies and Scientific Research –Basic Science Series Vol. (18) No (5) 1996

Theoretical Study of the Decrease in the Lengths of Linear Equivalent for non linear sequence.

Ahmad Hamze AL-SHEIKHA*

(Accepted 1995)

❒ ABSTRACT ❒

This research proves that the reason that the length of the linear equivalent of cross-sequ (on h term of sequence $\{a_n\}$*) does not reach the maximum length* ${}_rN_h$ *is related to the roots of polynomial characteristic of the sequence* $\{a_n\}$*, and to the coefficients which specify the general term* a_n*.*

* Lecturer at Higher Education, Mathematics Department, Faculty of Science, Tishreen University, Lattakia, Syria.

تعاريف:

1- المولد الخطي لمتتالية خطية[1]: هو مولد انزياحي خطي ذو تغذية خلفية بدارات جمع فقط يتساوى العدد على مخرجه في النبضة n مع الحد العام للمتتالية $\{a_n\}$ ونرمز له بـ LFSR.

2- المكافئ الخطي لمتتالية غير خطية[2]: إذا كانت $\{a_n\}$ متتالية مولدها الخطي LFSR1 وكانت $\{d_n\}$ متتالية جداء لعناصر من $\{a_n\}$ (تنتج بدارات ضرب على المكافئ الخطي LFSR1) وكان LFSR2 مولداً خطياً للمتتالية $\{d_n\}$ فإن LFSR2 يسمى مكافئاً خطياً.

3- طول المكافئ الخطي: هو عدد مراتبه ويساوي درجة كثير الحدود المولد للمتتالية التي يولدها المكافئ الخطي.

4- الطول الأعظمي لمكافئ خطي: إن طول المكافئ الخطي LFSR2 (عدد مراتبه) دوماً أصغر أو يساوي $_rN_h$ المذكور في البحث ولا يمكن أن يتعداه لذلك نسمي $_rN_h$ الطول الأعظمي للمكافئ الخطي.

5- المسألة العكسية: توليد المتتالية الخطية $\{d_n\}$ بمتتالية غير خطية[3] (جداء على متتالية خطية $\{a_n\}$) حيث يطلب تعيين المتتالية $\{a_n\}$ والمراتب التي يتم الجداء عليها وهي أحد المسائل المطروحة حالياً ويتطلب إيجاد حل لها.

إن الطول الأعظمي للمكافئ الخطي لمتتالية $\{d_n\}$ غير خطية [(جداء) على h مرتبة من متتالية خطية $\{a_n\}$ من GF(p) – درجة تعقيدها r] والذي يُرمز له بـ $_rN_h$ (حيث في حالة p = 2 هو: $_rN_h = \binom{r}{1} + \binom{r}{2} .... + \binom{r}{h}$) قد لا يمكن بلوغه عندما $h \geq 3$.

تقدم في هذه المقالة دراسة نظرية للنقص في طول المكافئ الخطي عن $_rN_h$ لمتتالية جداء على ثلاث مراتب من متتالية خطية على GF(p) تستنتج من خلالها أسباب عدم بلوغ هذا الطول في الحالة العامة، لما لذلك من أهمية في دراسة المسألة العكسية.

لتكن المتتالية التدريجية $\{a_n\}$ ذات التعقيد r ولنفرض أن الحد العام لهذه المتتالية يتعين بالعلاقة:

$$a_n = A_1\alpha_1^n + A_2\alpha_2^n + ... + A_r\alpha_r^n = \sum_{i=1}^{r} A_i\alpha_i^n$$

* لنفرض $\{d_n\}$ متتالية تنتج عن جداء ثلاث مراتب من $\{a_n\}$ بالشكل التالي:

المرتبة الأولى a_n (في حال مغايرة ذلك يمكن إجراء انسحاب حتى نصل إلى المرتبة الأولى). المرتبة الثانية $b_n = a_{n+\delta}$ (الناتجة بانسحاب δ عن المرتبة الأولى). المرتبة الثالثة $c_n = a_{n+\gamma}$ (ناتجة بانسحاب γ عن المرتبة الأولى وان $\delta \leq r$ و $\gamma \leq r$) عندئذ:

$$b_n = a_n + \delta = A_1\alpha_1^\delta \alpha_1^n + A_2\alpha_2^\delta \alpha_2^n + \dots + A_r\alpha_r^\delta \alpha_r^n = \sum_{i=1}^{r} A_i\alpha_i^\delta \alpha_i^n$$

$$c_n = a_n + \gamma = A_1\alpha_1^\gamma \alpha_1^n + A_2\alpha_2^\gamma \alpha_2^n + \dots + A_r\alpha_r^\gamma \alpha_r^n = \sum_{i=1}^{r} A_i\alpha_i^\gamma \alpha_i^n$$

$$d_n = a_n b_n c_n = \sum_{i=1}^{r} A_i^3 \alpha_i^{\delta+\gamma} .\alpha_i^{3n} +$$

$$\sum_{i\neq d}^{r} A_i^2 A_j \left(\alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_i^\gamma\right) \alpha_i^{2n} \alpha_j^n +$$

$$\sum_{i\neq j\neq k} A_i A_j A_k \left(\alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\alpha \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta\right)\left(\alpha_i \alpha_j \alpha_k\right)$$

نرى أن:

1- كل حد من المجموع الأول لا ينعدم مطلقاً.

2- حتى ينعدم حد من المجموع الثاني يلزم ويكفي أن يتحقق:

$$\alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_i^\gamma = 0$$

أو

$$\left(\frac{\alpha_j}{\alpha_i}\right)^\gamma + \left(\frac{\alpha_j}{\alpha_i}\right)^\delta + 1 = 0$$

بفرض $A = \left(\frac{\alpha_j}{\alpha_i}\right)$ نجد أن الشرط السابق يكافئ:

$$A^\gamma + A^\delta + 1 = 0$$

3- إن الشرط اللازم والكافي حتى ينعدم حد من المجموع الثالث هو:

$$\alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_j^\delta = 0$$

بتقسيم الطرفين على $\alpha_i^{\gamma+\delta}$ نجد:

$$\left(\frac{\alpha_j}{\alpha_i}\right)^\delta \cdot \left(\frac{\alpha_k}{\alpha_i}\right)^\gamma + \left(\frac{\alpha_j}{\alpha_i}\right)^\gamma \cdot \left(\frac{\alpha_k}{\alpha_i}\right)^\delta + \left(\frac{\alpha_j}{\alpha_i}\right)^\gamma + \left(\frac{\alpha_j}{\alpha_i}\right)^\delta + \left(\frac{\alpha_k}{\alpha_i}\right)^\gamma \cdot \left(\frac{\alpha_k}{\alpha_i}\right)^\delta 1 = 0$$

بفرض $A = \frac{\alpha_j}{\alpha_i}$ و $B = \frac{\alpha_k}{\alpha_i}$ نجد:

$$A^\delta B^\gamma + A^\gamma B^\delta + A^\gamma + A^\delta + B^\gamma + B^\delta = 0$$

وهي معادلة متناظرة. فإذا كانت المتتالية $\{a_n\}$ من GF(2) فـان المعادلــة الأخيـرة تكتـب بالشكل:

$$(A^\delta + 1)(B^\gamma + 1) + (A^\gamma + 1)(B^\delta + 1) = 0$$

4- حتى ينعدم مجموع حد من المجموع الأول مع حد من المجموع الثاني يلزم تحقق:

$$\alpha_k^{3n}=\alpha_i^{2n}\alpha_j^{n}\Rightarrow\begin{cases}\alpha_k^3=\alpha_i^3\alpha_j\\ \&\\ (i\neq k, j\neq k)\end{cases}$$

وبالتالي حتى ينعدم مجموع الحدين المقابلين يستلزم:

$$A_k^3\alpha_k^{(\delta+\gamma)}+A_i^2A_j(\alpha_i^{\delta}\alpha_j^{\gamma}+\alpha_i^{\gamma}\alpha_j^{\delta}+\alpha_i^{\delta}\alpha_i^{\gamma})=0$$

$$A_k^3\left(\frac{\alpha_k}{\alpha_i}\right)^{\delta+\gamma}+A_i^2A_j\left[\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\delta}+1\right]=0$$

أو

$$\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\delta}+1=(p-1)\frac{A_k^3}{A_i^2A_j}\left(\frac{\alpha_k}{A_i}\right)^{\delta+\gamma}$$

بفرض $A=\dfrac{\alpha_j}{\alpha_i}$ و $B=\dfrac{\alpha_k}{\alpha_i}$

$$A^{\gamma}+A^{\delta}+1=(p-1)\frac{A_k^3}{A_i^2A_j}B^{\gamma+\delta}$$

5- حتى ينعدم مجموع حد من المجموع الأول مع حد من المجموع الثالث يستلزم:

$$\alpha_m^{3n}=(\alpha_i\alpha_j\alpha_k)^n,\alpha_m^3=\alpha_i\alpha_j\alpha_k,1\le m\le r$$

(حيث i,j,k مختلفة مثنى مثنى).

وبالتالي حتى ينعدم مجموع الحدين المقابلين يستلزم:

$$A_m^3(\alpha_m^{\delta+\gamma})+A_iA_jA_k(\alpha_j^{\delta}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\delta}+\alpha_i^{\delta}\alpha_j^{\gamma}+\alpha_i^{\delta}\alpha_k^{\gamma}+\alpha_i^{\gamma}\alpha_k^{\delta}+\alpha_i^{\gamma}\alpha_k^{\delta})=0$$

أو بالتقسيم على $\alpha_i^{\delta+\gamma}$ نجد:

$$A_m^3\left(\frac{\alpha_m}{\alpha_i}\right)^{\delta+\gamma}+A_iA_jA_k\left[\left(\frac{\alpha_j}{\alpha_i}\right)^{\delta}\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_k}{\alpha_i}\right)^{\delta}+\right.$$

$$\left.\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\delta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\delta}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}\right]=0$$

بفرض $A=\dfrac{\alpha_j}{\alpha_i}$ و $B=\dfrac{\alpha_k}{\alpha_i}$ و $C=\dfrac{\alpha_m}{\alpha_i}$ وبالتالي:

$$A_mC^{\delta+\gamma}+A_iA_jA_k\left[A^{\delta}B^{\gamma}+A^{\gamma}B^{\delta}+A^{\gamma}+A^{\delta}+B^{\gamma}+B^{\delta}\right]=0$$

أو

$$A^{\delta}B^{\gamma}+A^{\gamma}B^{\delta}+A^{\gamma}+A^{\delta}+B^{\gamma}+B^{\delta}=(p-1)\frac{A_m}{A_iA_jA_k}C^{\delta+\gamma}$$

6- حتى ينعدم مجموع حد من المجموع الثاني مع حد من المجموع الثالث يستلزم:

$$\alpha_\ell^2\alpha_m=\alpha_i\alpha_j\alpha_k$$

حيث (i,j,k مختلفة مثنى مثنى)

وبالتالي ينعدم المجموع إذا تحقق:

$$A_\ell^2A_m\left(\alpha_\ell^\delta\alpha_m^\gamma+\alpha_\ell^\gamma\alpha_m^\delta+\alpha_\ell^{\gamma+\delta}\right)+$$
$$A_iA_jA_k\left(\alpha_j^\delta\alpha_k^\gamma+\alpha_j^\gamma\alpha_k^\delta+\alpha_i^\delta\alpha_j^\gamma+\alpha_i^\gamma\alpha_k^\delta+\alpha_i^\gamma\alpha_k^\delta+\alpha_i^\delta\alpha_k^\gamma\right)=0$$

وبالتقسيم على $\alpha_i^{\delta+\gamma}$ والإصلاح وفرض $A=\dfrac{\alpha_j}{\alpha_i}$ و $B=\dfrac{\alpha_k}{\alpha_i}$ و $C=\dfrac{\alpha_m}{\alpha_i}$ و $D=\dfrac{\alpha_\ell}{\alpha_i}$ نجد:

$$\left(\frac{\alpha_j}{\alpha_i}\right)^\delta\left(\frac{\alpha_k}{\alpha_i}\right)^\gamma+\left(\frac{\alpha_j}{\alpha_i}\right)^\gamma\left(\frac{\alpha_k}{\alpha_i}\right)^\delta+\left(\frac{\alpha_j}{\alpha_i}\right)^\gamma+\left(\frac{\alpha_k}{\alpha_i}\right)^\delta+\left(\frac{\alpha_j}{\alpha_i}\right)^\delta+\left(\frac{\alpha_k}{\alpha_i}\right)^\gamma=$$
$$(p-1)\frac{A_\ell^2A_m}{A_iA_jA_k}\left[\left(\frac{\alpha_\ell}{\alpha_i}\right)^\delta\left(\frac{\alpha_m}{\alpha_i}\right)^\gamma+\left(\frac{\alpha_\ell}{\alpha_i}\right)^\gamma\left(\frac{\alpha_m}{\alpha_i}\right)^\delta+\left(\frac{\alpha_\ell}{\alpha_i}\right)^{\delta+\gamma}\right]$$

أو

$$A^\delta B^\gamma+A^\gamma B^\delta+A^\delta+A^\gamma+B^\delta+B^\gamma=(p-1)\frac{A_\ell^2A_m}{A_iA_jA_k}\left(D^\delta C^\gamma+D^\gamma C^\delta+D^{\delta+\gamma}\right)$$

7– حتى ينعدم مجموع حد من المجموع الأول وحد من المجموع الثاني وحد مــن المجمــوع الثالث يستلزم:

$$\alpha_m^{3n}=\alpha_h^{2n}\alpha_\ell^n=\left(\alpha_i\alpha_j\alpha_k\right)^n$$

وبالتالي ينعدم المجموع إذا تحقق:

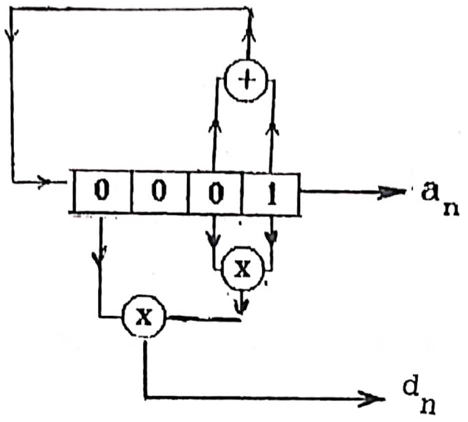
$$A_m^3\alpha_m^{\delta+\gamma}+A_h^2A_\ell\left(\alpha_h^\delta\alpha_\ell^\gamma+\alpha_h^\gamma\alpha_\ell^\delta+\alpha_h^{\gamma+\delta}\right)+$$
$$A_iA_jA_k\left(\alpha_j^\delta\alpha_k^\gamma+\alpha_j^\gamma\alpha_k^\delta+\alpha_i^\delta\alpha_j^\gamma+\alpha_i^\delta\alpha_k^\gamma+\alpha_i^\gamma\alpha_k^\delta+\alpha_i^\gamma\alpha_k^\delta+\right)=0$$

أو بفرض: $A=\dfrac{\alpha_j}{\alpha_i}$ و $B=\dfrac{\alpha_k}{\alpha_i}$ و $C=\dfrac{\alpha_m}{\alpha_i}$ و $D=\dfrac{\alpha_\ell}{\alpha_i}$ و $E=\dfrac{\alpha_h}{\alpha_i}$

$$A_mC^{\delta+\gamma}+A_h^2A_\ell+(E^\delta D^\gamma+E^\gamma D^\delta+E^{\gamma+\delta})+$$
$$A_iA_jA_k\left(A^\delta B^\gamma+A^\gamma B^\delta+A^\gamma+A^\gamma+B^\delta+B^\delta\right)=0$$

كل تحقق لــ2 أو 3 أو 4 أو 5 أو 6 أو 7 يؤدي إلى نقص في طول المكافئ الخطي بمقــدار واحد (من أجل كل حالة) عن الحد الأعظمي rNh.

مثال1: لتكن المتتالية $\{a_n\}$ من GF(2) الناتجة عن المولد الخطي الظاهر في الشكل (1) .



شكل (1) مولد انزياحي خطي على أربع درجات من GF(2)

إن المعادلة المميزة للمتالية $\{a_n\}$ هي:

$$X^4 + X + 1 = 0$$

وجذور هذه المعادلة هي:

$$\alpha, \alpha^2, \alpha^4 = \alpha + \alpha^8 = \alpha^2 + 1$$

والحد العام للمتتالية $\{a_n\}$ يعين بالعلاقة:

$$a_n = A_1\alpha^n + A_2\alpha^{2n} + A_3(\alpha+1)^n + A_4(\alpha^2+1)^n$$

نلاحظ ان كلا من 1 و2 و3 و5 و6 و7 غير محقق في حين نرى أن 4 محقق من أجل القـيم التالية لكل من i وj وk:

$$\begin{aligned} &a)\ i = 1,\ j = 3,\ k = 2 \\ &b)\ i = 2,\ j = 4,\ k = 3 \\ &c)\ i = 3,\ j = 1,\ k = 4 \\ &d)\ i = 4,\ j = 2,\ k = 1 \end{aligned}$$

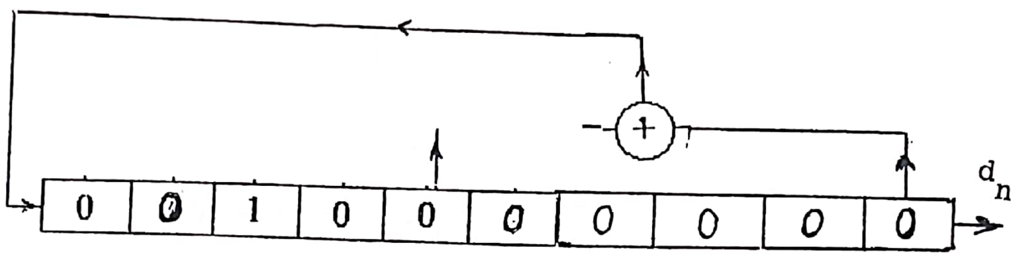
وبالتالي فإن طول المكافئ الخطي المولد للمتتالية $\{d_n\}$ هو:

$$_4N_3 - 4 = \begin{pmatrix}4\\1\end{pmatrix} + \begin{pmatrix}4\\2\end{pmatrix} + \begin{pmatrix}4\\3\end{pmatrix} - 4 = 4 + 6 + 4 - 4 = 10$$

ومتتالية الجداء $\{d_n\}$ تحدد بالعلاقة:

$$\begin{aligned} d_n &= (\alpha^3+\alpha^2+1)\alpha^n + (\alpha^3+\alpha^2+\alpha)(d^2)^n(\alpha^3+\alpha+1)(\alpha+1)^n \\ &= (\alpha^3+1)(\alpha^2+1)^n + (\alpha^2+\alpha)(\alpha^2+\alpha)^n + (\alpha^2+\alpha+1) \\ &= (\alpha^2+\alpha+1)^n + (\alpha^2+1)(\alpha^3+\alpha^2+\alpha)^n + (\alpha+1)(\alpha^3+\alpha^2+1)^n \\ &\quad + \alpha(\alpha^3+\alpha+1)^n\alpha^2(\alpha^3+\alpha)^n \end{aligned}$$

وشكل المكافئ الخطي هو شكل (2) .



شكل (2) مكافئ خطي بعشرة درجات من GF(2)

في حالة p≥3 فإن:

$$_hN_2 = \binom{h}{1} + \binom{h}{2} = h + \frac{h(h-1)}{2}$$

$$_hN_3 = \binom{h}{1} + h(h-1) + \binom{h}{3}$$

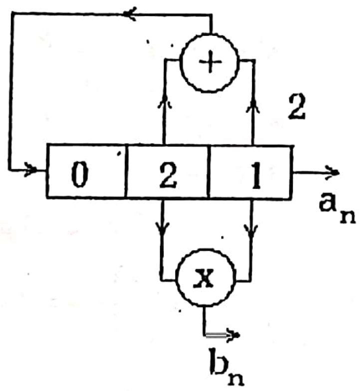
$$_hN_3 = \binom{h}{1} + h(h-1) + \binom{h-1}{2} + h\binom{h-1}{3} + \binom{h}{4}$$

أيضاً هنا كما في حالة GF(2) فإنه إذا كان $r > 2$ فإن طول المكافئ الخطي دوماً أصغر أو يساوي $_hN_r$ (حيث أن $_hN_r$ المحسوب في [2] غير صحيح). في حالة $r = 3$ نأخذ:

مثال: بفرض المتتالية $\{a_n\}$ حيث $\forall n \in N: a_n \in GF(3)$

و $a_{n+3} + 2a_{n+1} + a_n = 0; a_0 = 1; a_1 = 2; a_2 = 0$

كما في الشكل (3)



شكل (3) متتالية جداء بدرجتين من GF(3)

إن

$$a_n = (2\beta^2 + \beta + 1)\beta^n + (2\beta^2 + 2)(\beta + 2)^n + (2\beta^2 + 2\beta + 1)(\beta + 1)^n$$

حيث β تحقق المعادلة:

$$\beta^3 + 2\beta + 1 = 0$$

لنعتبر المتتالية $\{b_n\}$ حيث $b_n = a_n . a_{n+1}$

إن

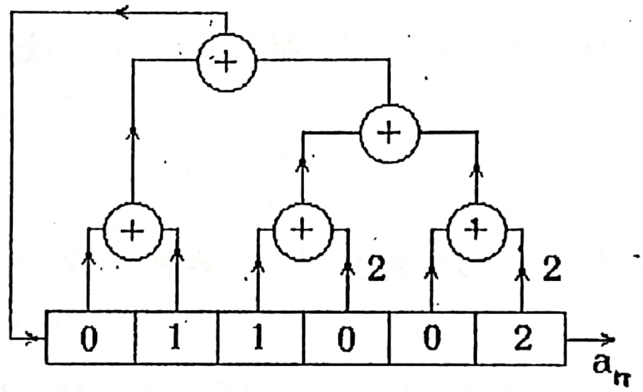
$$a_{n+1} = (2\beta^2 + \beta + 1)\beta^{n+1} + (2\beta^2 + 2)(\beta + 2)^{n+1} + (2\beta^2 + 2\beta + 1)$$

$$(\beta + 1)^{n+1} = (\beta^2 + 1)\beta^n + (\beta^2 + \beta + 2)(\beta + 2)^n + (\beta^2 + 2\beta + 2)(\beta + 1)^n$$

و

$$b_n = 2\beta^2(\beta^2)^n + (2\beta^2 + 2\beta + 1)(\beta^2 + 2\beta)^n +$$
$$(2\beta^2 + 2)(\beta^2 + \beta)^n + (2\beta^2 + 2\beta + 2)(\beta^2 + \beta + 1)^n + (2\beta^2 + \beta + 1)(\beta^2 + 2)^n +$$
$$(2\beta^2 + \beta + 2)(\beta^2 + 2\beta + 1)^n$$

ودرجة المكافئ الخطي هي 6 كما في الشكل (4):



شكل (4) مكافئ خطي بست درجات من GF(3)

والمتتالية هي:

$$b_n = \{2,0,0,1,1,0,0,0,0,0,2,2,1,2,0,0,1,1,0,0,0,0,0,1,...\}$$

والدستور التدريجي الخطي المكافئ هو:

$$a_{n+6} = a_{n+5} + a_{n+4} + a_{n+3} + 2a_{n+2} + a_{n+1} + 2a_n$$

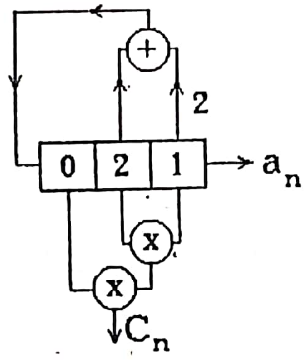
أو

$$a_{n+6} + 2a_{n+5} + 2a_{n+4} + 2a_{n+3} + a_{n+2} + 2a_{n+1} + a_n = 0$$

لنفرض الآن المتتالية $\{C_n\}$ حيث:

$$C_n = a_n . a_{n+1} . a_{n+2} = b_n . a_{n+2}$$

كما في الشكل (5).



شكل (5) متتالية جداء على ثلاث درجات من GF(3)

فنجد أن:

$$C_n = (\beta^2+\beta+2)(\beta+2)^n + (2\beta^2+2\beta)(2\beta^2+\beta+2)^n + 2(\beta^2+\beta+2).$$
$$(\beta^2+2\beta+2)^n + (2\beta^2+1)(2\beta^2+2\beta+2)^n + (2\beta^2+2) + (\beta+1)^n +$$
$$(2\beta^2+\beta)(2\beta^2)^n + (2\beta^2+2\beta+2)(\beta^2+1)^n + (\beta^2+1)(\beta)^n$$

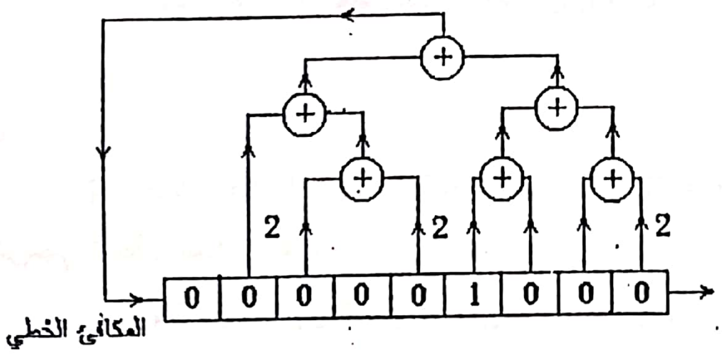
الطول الأعظمي المفروض هو:

$$_3N_3 = \binom{3}{1} + 6 + 1 = 10$$

بينما نجد أن الطول الناتج هو 9 وهو أصغر من $_3N_3$ (وهو أكبر من الحد المذكور في [2]) والدستور التدريجي للمتتالية هو:

$$a_{n+9} = 2a_{n+7} + a_{n+6} + a_{n+4} + a_{n+3} + a_{n+2} + a_{n+1} + 2a_n$$

كما في الشكل (6).



شكل (6) مكافئ خطي بتسع درجات

نلاحظ في هذا المثال أن 3 فقط هو المحقق حيث أن المجموع الثالث مؤلف من حد واحد. إن معامل:

$$(\alpha_i\alpha_j\alpha_k)^n = \beta[(\beta+2)(\beta+1)]^n$$

هو

$$(\beta+2)^2(\beta+1)+(\beta+1)(\beta+2)^2+\beta^2(\beta+2)+$$
$$\beta(\beta+2)^2+\beta^2(\beta+1)+\beta(\beta+1)^2=0$$

وبالتالي طول المكافئ الخطي هو 9 بدلاً من 10.

•• لنفرض $\{d_n\}$ متتالية تنتج من جداء أربع مراتب من $\{a_n\}$ بالشكل التالي المرتبة الأولى a_n (في حال مغايرة ذلك يمكن إجراء انسحاب حتى نصل إلى المرتبة الأولى) المرتبة الثانية $b_n = a_{n+\beta}$ (الناتجة بانسحاب β عن المرتبة الأولى) المرتبة الثالثة $c_n = a_{n+\mu}$ (الناتجة بانسحاب μ عن المرتبة الأولى) المرتبة الثالثة $d_n = a_{n+\gamma}$ (الناتجة بانسحاب γ عن المرتبة الأولى وأن كلاً من β و μ و γ أصغر أو تساوي r) أي:

$$a_n = A_1\alpha_1^n + A_2\alpha_2^n + \dots + A_r\alpha_r^n = \sum_{i=1}^{r} A_i\alpha_i^n$$

$$b_n = A_1\alpha_1^\beta\alpha_1^n + A_2\alpha_2^\beta\alpha_2^n + \dots + A_r\alpha_r^\beta\alpha_r^n = \sum_{i=1}^{r} A_i\alpha_i^{n+\beta}$$

$$c_n = A_1\alpha_1^\mu\alpha_1^n + A_2\alpha_2^\mu\alpha_2^n + \dots + A_r\alpha_r^\mu\alpha_r^n = \sum_{i=1}^{r} A_i\alpha_i^{n+\mu}$$

$$D_n = A_1\alpha_1^\gamma\alpha_1^n + A_2\alpha_2^\gamma\alpha_2^n + \dots + A_r\alpha_r^\gamma\alpha_r^n = \sum_{i=1}^{r} A_i\alpha_i^{n+\gamma}$$

$$\begin{aligned}
d_n &= a_n b_n c_n D_n \\
&= \sum_{i=1}^{r} A_i^4\alpha_i^{\beta+\mu+\gamma}\alpha_i^{4n} + \\
&+ \sum_{\substack{i=1\\ i\neq j}}^{r} A_i^3A_j\left(\alpha_i^{\beta+\mu}\alpha_j^\gamma + \alpha_i^{\beta+\gamma}\alpha_j^\mu + \alpha_i^{\mu+\gamma}\alpha_j^\beta + \alpha_i^{\beta+\mu+\gamma}\right)\alpha_i^{3n}\alpha_j^n \\
&+ \sum_{\substack{i=1\\ i\neq j,k\neq i}}^{r} A_i^2A_jA_k\begin{bmatrix}\alpha_i^\beta\left(\alpha_j^\mu\alpha_k^\gamma\alpha_j^\gamma\alpha_k^\mu\right)+\alpha_i^\mu\left(\alpha_j^\beta\alpha_k^\gamma\alpha_j^\gamma\alpha_k^\beta\right)\\ \alpha_i^\gamma\left(\alpha_j^\beta\alpha_k^\mu\alpha_j^\mu\alpha_k^\beta\right)+\alpha_i^{\beta+\mu}\left(\alpha_j^\gamma+\alpha_k^\gamma\right)+\alpha_i^{\beta+\gamma}\\ \left(\alpha_j^\mu+\alpha_k^\mu\right)+\alpha_j^{\mu+\gamma}\left(\alpha_j^\beta+\alpha_k^\beta\right)\end{bmatrix} \\
&\qquad \alpha_i^{2n}\alpha_j^n\alpha_k^n \\
&+ \sum_{\substack{i=1\\ i\neq j,k\neq 1}}^{r} A_iA_jA_kA_l\begin{bmatrix}\sum_{(j,k,l)}\left(\alpha_j^\beta\alpha_k^\mu\alpha_l^\gamma\right)+\alpha_i^\beta\left(\alpha_j^\mu\alpha_k^\gamma\alpha_j^\gamma\alpha_k^\mu\right)\\ +\alpha_i^\mu\left(\alpha_j^\gamma\alpha_l^\beta\alpha_j^\beta\alpha_l^\gamma\right)+\alpha_i^\gamma\left(\alpha_k^\beta+\alpha_l^\mu+\alpha_k^\mu\alpha_l^\beta\right)\end{bmatrix} \\
&\qquad \left(\alpha_i\alpha_j\alpha_k\alpha_l\right)^n
\end{aligned}$$

حيث يرمز (j,k,l) إلى مجموعة تباديل {j,k,l}

نجد أن:

1- كل حد من المجموع الأول لا ينعدم.

2- حتى ينعدم حد من المجموع الثاني يلزم ويكفي أن يتحقق:

$$\alpha_i^{\beta+\mu}\alpha_j^\gamma + \alpha_i^{\beta+\gamma}\alpha_j^\mu + \alpha_i^{\mu+\gamma} + \alpha_i^{\beta+\mu\gamma} = 0$$

أو (بالتقسيم على: $\alpha_i^{\beta+\mu+\gamma}$ وتغير ترتيب الحدود)

$$\left(\frac{\alpha_j}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\mu}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}+1=0$$

بفرض $A=\dfrac{\alpha_j}{\alpha_i}$ نجد:

$$A^{\beta}+A^{\mu}+A^{\gamma}+1=0$$

3- حتى ينعدم حد من المجموع الثالث يلزم ويكفي أن يتحقق:

$$\alpha_i^{\beta}.\left(\alpha_j^{\mu}.\alpha_k^{\gamma}+\alpha_j^{\gamma}.\alpha_k^{\mu}\right)+\alpha_i^{\mu}.\left(\alpha_j^{\beta}.\alpha_k^{\gamma}+\alpha_j^{\gamma}.\alpha_k^{\beta}\right)+\alpha_i^{\gamma}.\left(\alpha_j^{\beta}.\alpha_k^{\mu}.\alpha_j^{\mu}.\alpha_k^{\beta}\right)+$$
$$\alpha_i^{\beta+\mu}\left(\alpha_j^{\gamma}+\alpha_k^{\gamma}\right)+\alpha_i^{\beta+\gamma}\left(\alpha_j^{\mu}+\alpha_k^{\mu}\right)+\alpha_i^{\mu+\gamma}\left(\alpha_j^{\beta}+\alpha_k^{\beta}\right)=0$$

أو (بتقسيم الطرفين على $\alpha_i^{\beta+\mu+\gamma}$ وتغيير ترتيب الحدود بما يناسب):

$$\left(\frac{\alpha_j}{\alpha_i}\right)^{\beta}\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\mu}\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\beta}\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\mu}\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}+$$
$$+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}=0$$

بفرض:

$$\frac{\alpha_j}{\alpha_i}=A,\frac{\alpha_k}{\alpha_i}=B$$
$$A^{\beta}B^{\mu}+A^{\mu}B^{\beta}+A^{\beta}B^{\gamma}+A^{\gamma}B^{\beta}+A^{\mu}B^{\gamma}A^{\gamma}B^{\mu}$$
$$+\left(A^{\beta}+A^{\mu}+A^{\gamma}\right)+\left(B^{\beta}+B^{\mu}+B^{\gamma}\right)=0$$

وهي معادلة متناظرة بالنسبة لـA وB فإذا كانت المتتالية $\{a_n\}$ من GF(2) فـإن المعادلـة الأخيرة تكتب بالشكل:

$$(A^{\beta}+1)(B^{\mu}+1)+(A^{\mu}+1)(B^{\beta}+1)+(A^{\beta}+1)(B^{\gamma}+1)+(A^{\gamma}+1)(B^{\beta}+1)+$$

$$(A^{\mu}+1)(B^{\gamma}+1)+(A^{\gamma}+1)(B^{\mu}+1)+(A^{\beta}+A^{\mu}+A^{\gamma})+\left(B^{\beta}+B^{\mu}+B^{\gamma}\right)=0$$

4- حتى ينعدم حد من المجموع الرابع يلزم ويكفي أن يتحقق:

$$\sum_{(i,k,l)}\alpha_j^{\beta}\alpha_k^{\mu}\alpha_l^{\gamma}+\alpha_i^{\beta}.\left(\alpha_j^{\mu}.\alpha_k^{\gamma}+\alpha_j^{\gamma}.\alpha_k^{\mu}\right)+$$
$$\alpha_i^{\mu}.\left(\alpha_j^{\gamma}.\alpha_l^{\beta}+\alpha_j^{\beta}.\alpha_l^{\gamma}\right)+\alpha_i^{\gamma}.\left(\alpha_k^{\beta}.\alpha_l^{\mu}+\alpha_k^{\mu}.\alpha_l^{\beta}\right)$$

أو

$$(\alpha_i^{\beta}+\alpha_l^{\beta})(\alpha_j^{\mu}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\mu})+(\alpha_i^{\mu}+\alpha_k^{\mu})(\alpha_j^{\gamma}\alpha_l^{\beta}+\alpha_j^{\beta}\alpha_l^{\gamma})$$
$$+(\alpha_i^{\gamma}+\alpha_k^{\gamma})(\alpha_k^{\beta}\alpha_l^{\mu}+\alpha_k^{\mu}\alpha_l^{\beta})=0$$

بالتقسيم على $\alpha_i^{\beta+\mu+\gamma}$ نجد أن المساواة الأخيرة تكتب بالشكل:

$$\left[1+\left(\frac{\alpha_l}{\alpha_i}\right)^{\beta}\right]\left[\left(\frac{\alpha_j}{\alpha_i}\right)^{\mu}\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}\right]+\left[1+\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}\right]$$
$$\left[\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_l}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\beta}\left(\frac{\alpha_l}{\alpha_i}\right)^{\gamma}\right]+\left[1+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\right]$$
$$\left[\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}\left(\frac{\alpha_l}{\alpha_i}\right)^{\mu}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_l}{\alpha_i}\right)^{\mu}\right]=0$$

بفرض: $C=\frac{\alpha_l}{\alpha_i}$ و $B=\frac{\alpha_k}{\alpha_i}$ و $A=\frac{\alpha_j}{\alpha_i}$

فإن المساواة الأخيرة تكتب بالشكل:

$$\left(1+C^{\beta}\right)\left(A^{\mu}B^{\gamma}+A^{\gamma}B^{\mu}\right)+\left(1+B^{\mu}\right)\left(A^{\gamma}C^{\beta}+A^{\beta}C^{\gamma}\right)+$$
$$\left(1+A^{\gamma}\right)\left(A^{\beta}C^{\mu}+A^{\mu}C^{\beta}\right)$$

5- حتى ينعدم مجموع حد من المجموع الأول مع حد من المجموع الثاني يلزم:

i و j و k مختلفة مثنى مثنى: $\alpha_k^{4n}=\alpha_i^{3n}\alpha_j^{n}$

وبالتالي حتى ينعدم مجموع الحدين المقابلين يستلزم:

$$A_k^4\alpha_k^{\beta+\mu+\gamma}+A_i^3A_j=\left(\alpha_j^{\beta+\mu+\gamma}\alpha_j^{\gamma}+\alpha_i^{\beta+\gamma}\alpha_j^{\gamma}+\alpha_i^{\mu+\gamma}\alpha_j^{\beta}+\alpha_i^{\beta+\mu+\gamma}\right)=0$$

بالتقسيم على $\alpha_i^{\beta+\mu+\gamma}$ واعتبار $B=\frac{\alpha_k}{\alpha_i}$ و $A=\frac{\alpha_j}{\alpha_i}$ نجد:

$$A_k^4A^{\beta+\mu+\gamma}+A_i^3A_j\left(A^{\beta}+A^{\mu}A^{\gamma}+1\right)=0$$

6- حتى ينعدم مجموع حد من المجموع الأول وحد من المجموع الثالث يستلزم:

$$\alpha_m^{4n}=\alpha_i^{2n}\alpha_j^{n}\alpha_k^{n}$$

وبالتالي حتى ينعدم مجموع الحدين السابقين نجد:

$$A_m^4\alpha_m^{\beta+\mu+\gamma}+A_1^2A_jA_k\begin{bmatrix}\alpha_i^{\beta}.\left(\alpha_j^{\mu}.\alpha_k^{\gamma}+\alpha_j^{\gamma}.\alpha_k^{\mu}\right)+\alpha_i^{\mu}.\left(\alpha_j^{\beta}.\alpha_k^{\gamma}+\alpha_j^{\gamma}.\alpha_k^{\beta}\right)\\+\alpha_i^{\gamma}.\left(\alpha_j^{\beta}.\alpha_k^{\mu}+\alpha_j^{\mu}.\alpha_k^{\beta}\right)+\alpha_i^{\beta+\mu}.\left(\alpha_j^{\gamma}+\alpha_k^{\gamma}\right)\\+\alpha_i^{\beta+\gamma}\left(\alpha_j^{\mu}+\alpha_k^{\mu}\right)+\alpha_j^{\mu+\gamma}\left(\alpha_j^{\beta}+\alpha_k^{\beta}\right)\end{bmatrix}=0$$

بتقسيم الطرفين على $\alpha_i^{\beta+\mu+\gamma}$ وفرض: $C=\frac{\alpha_l}{\alpha_i}$ و $B=\frac{\alpha_k}{\alpha_i}$ و $A=\frac{\alpha_j}{\alpha_i}$ نجد:

$$A_m^4C^{\beta+\mu+\gamma}+A_1^2A_jA_k\left[A^{\mu}B^{\gamma}+A^{\gamma}B^{\mu}+A^{\beta}B^{\gamma}+A^{\gamma}B^{\beta}+A^{\mu}B^{\mu}+A^{\mu}B^{\beta}\right.$$
$$\left.+\left(A^{\beta}+A^{\mu}+A^{\gamma}\right)+\left(B^{\beta}+B^{\mu}+B^{\gamma}\right)\right]=0$$

وهكذا بالتتالي نحصل على علاقات مقابلة له.

7- مجموع حد من المجموع الثاني مع حد من المجموع الثالث مساو للصفر.

8- مجموع حد من المجموع الثاني مع حد من المجموع الرابع مساو للصفر.

9- مجموع حد من المجموع الثالث مع حد من المجموع الرابع مساو للصفر.

10- مجموع ثلاثة حدود من المجاميع الأربعة مساوٍ للصفر.

11- مجموع أربعة حدود من المجاميع الأربعة مساوٍ للصفر.

من دراسة المكافئ الخطي لمتتالية جداء $\{d_n\}$ على ثلاث مراتب من $\{a_n\}$ وخاصة من 4 و5 و6 و7، أو على أربع مراتب نرى أنه ليس فقط جذور كثير الحدود المميز للمتتالية $\{a_n\}$ تلعب دوراً كبيراً في طول المكافئ الخطي لمتتالية الجداء وإنما أيضاً معاملات الحد العام لها ومنه النتيجة التالية:

نتيجة: طول المكافئ الخطي لمتتالية جداء $\{d_n\}$ على H مرتبة من متتالية $\{a_n\}$ -من GF(P)- يتعلق ليس فقط بجذور كثير الحدود المميز للمتتالية $\{a_n\}$ وإنما أيضاً بالمعاملات التي تعين الحد العام للمتتالية $\{a_n\}$.

REFERENCES المراجع

[1]- F.D. MACWILLAMS AND N.J.A. SLOANE – the theory of error correcting codes North – Holland 1978.

[2]- An Analysis of the structure and Complexity of nolinear Bianary sequence generators. IEEE TRANSACTION OF INFORMATION THEORY. Vol. Pp22 – N 6 November 1976.

[3]- S.W. GOLAMB Shift Register Sequences San Francisco - Holden day 1967.