مجلة جامعة تشرين للدراسات والبحوث العلمية - سلسلة العلوم الأساسية المجلد /16/ العدد /3/ 1414 هـ 1994م.

تحليل بنية وتركيب مولدات المتتالية المزدوجة غير الخطية

أحمد حمزة الشيخة*

☐ ملخص ☐

في هذا البحث تحليل المولدات المتتالية غير الخطية في GF(p) حيث **p** عدد أولي وهو تعميم للعمل [2] الذي يدرس هذا الموضوع من أجل p=2 فقط. وقد بينّا في عملنا هذا أنّ الحدّ

$$\underset{m\,r}{N} = \sum_{i=1}^{r} \binom{m}{i}.$$

المحسوب في [2] غير صحيح من أجل p≠2، كما أنّ تنظيم عمل **p** مولد المتتاليات من GF(p) بوساطة مولد يعمل كمنظم استلزم حل معادلة من الدرجة p بشكل خاص عندما p=2.

* مدرس تعليم عالي في قسم الرياضيات بكلية العلوم - جامعة تشرين - اللاذقية سوريا.

الدساتير التدريجية على GF(p):

نعتبر المتتالية $\{a_n\}$ المعينة بالمعادلة المتجانسة:

$$a_{n+m} + u_1 a_{n+m-1} + \dots\dots\dots + u_m a_n = 0 \; ; \; n \geq 0 \quad (1)$$

أو

$$a_{n+m} + \sum_{i=1}^{m} U_i . a_{n+m-i} = 0 \quad ; \; n \geq 0 \quad (\acute{1})$$

حيث $U_m \neq 0$ وأن $i=1,2,3,\dots.m$ و $U_i \ni GF(P)$ & $a_n \ni GF(p)$ وأن $GF(p)$ هو حقل غالوا Z/pz (حيث p عدد أولي).

إن المعادلة (1) أو ($\acute{1}$) تتعين تماماً بالقيم الإبتدائية $a_0,\dots\dots,a_{m-1}$ بمعنى أن لها m درجة فعالة (في حالة $p = 2$ يوجد m-1 درجة فعّالة). أو أنّ تعقيد المتتالية $\{ a_n \}$ هو m.

لنعتبر الآن المعادلة التفاضلية:

$$\left(E^m + \sum_{i=1}^{m} U_i . E^{m-i}\right) a_n = 0 \qquad (2)$$

حيث E مؤثر تفاضلي معين بالعلاقة:

$$Ea_n = a_{n+1}$$

إن المعادلة المميزة للمعادلة (2) هي:

$$X^m + \sum_{i=1}^{m} U_i . X^{m-i} = 0 \qquad (3)$$

إن جميع حلول المعادلة (3) والتي عددها يساوي m موجودة في الحقل $GF(p^r)$ حيث r هو المضاعف المشترك البسيط لدرجات الحدوديات غير الخزولة على GF(p) والتي جداءاتها المعادلة (3).

إذا كان β حلاً بسيطاً لـ(3) فإنّ $C\beta^n$ حلاً لـ(2) وإذا كانت جميع حلول (3) بسيطة والتي هي $\beta_1,\dots\dots\dots,\beta_m$ فإنها تكون مستقلة خطياً عن بعضها بعضاً ويكون الحل العام لـ(1) هو:

$$a_n = \sum_{i=1}^{m} C_i \beta_i^n \qquad (4)$$

حيث أن المعاملات $C_1,\dots\dots.,\ C_m$ تتعين من القيم الإبتدائية $a_0,\dots\dots.,a_{m-1}$

مثال: المتتالية $\{a_n\}$ معينة بالدستور التدريجي

$$a_{n+3} + 2a_{n+1} + a_n = 0 \qquad (5)$$

حيث أن القيم الإبتدائية $a_2=0$, $a_1=2$, $a_0=1$ من $GF(3)=\{0,1,2\}$ إنّ المعادلة التفاضلية لهذه المتالية هي:

$$(E^3 + 2E + 1)\, a_n = 0$$

والمعادلة المميزة هي:

$$X^3 + 2X + 1 = 0$$

وهذه المعادلة غير حلولة في GF(3) وأولية فيه وحلولة في $GF(3^3)$، بفرض β حل لها أي $\beta^3 + 2\beta + 1 = 0$ فإنّ حلولها هي $\beta, \beta^3, \beta^{(3^2)}$ والحل العام لـ(5) هو:

$$a^n = c_1 . \beta . n + c_2 \left(\beta^3\right) n + C_3 \left(\beta^{(3^2)}\right) n$$

بملاحظـــــــة أن $\beta^{3^2} = \beta + 1$ و

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

يكون الحل العام لـ(5) هو

$$a_n = C_1\beta^n + C_2(\beta + 2)n + + C_3(\beta + 1)n$$

من الشروط الإبتدائية نجد أنّ:

$$C_1 = z\beta^2 + \beta + 1; C_2 = = 2\beta + 2; C_3 = 2\beta^2 + 2\beta + 1$$

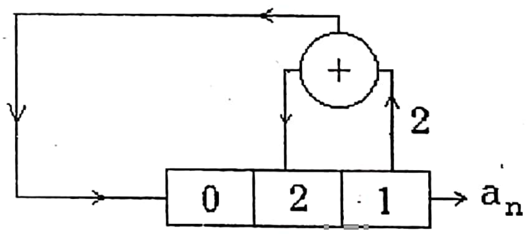
ويكون الحل العام هو

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

والمتتالية دورية دورها $T=3^3-1=26$

وهي:

{1,2,0,1,1,1,0,0,2,0,2,1,2,2,1,0,2,2,2,0,0,1,0,1,2,1}



شكل (1) مولد إنزياحي خطي.

في الحالة الخاصة إذا كان β جذراً للحدودية P(X) والتي درجتها d_d وهي قاسمة للحدودية الموجودة في الطرف الأيمن من (3) وغير حلولة على GF(p) فإنّ:

$$\beta^{p^k}; k = 0, \dots\dots, d_j - 1$$

تكون حلولاً متمايزة لـ(2) في $GF(P^{dj})$.

والحل العام لـ(1) في هذا الحقل هو:

$$a_n = \sum_{i=0}^{d_j - 1} C_i (\beta^{p^i})^n \quad (7)$$

أما إذا كان β جذراً مكرراً t مرة فإنّ β حل لجملة المعادلات

$$\begin{cases} mX^m + \sum_{i=1}^{m} U_i.(m-i)X^{m-i} = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ m^{(t-1)}X^m + \sum_{i=1}^{m} U_i.(m-i)^{t-1}X^{m-i} = 0 \end{cases}$$

وبالتـــــــالي فـــــــإن $\beta^n, n\beta^n, \dots\dots, n^{t-1}\beta^n$ حلـــول لــــ(2)

حيث تحسب n^i بالمقاس (mod p)p.

الدساتير غير الخطية والمكافئات الخطية على GF(p):

لتكن $\{b_n\}$ متتالية غير خطية على درجتين من المتتالية الخطية $\{a_n\}$ والتي حدوديتها المميزة من الدرجة m ولنفرض أن الحل العام للمتتالية $\{a_n\}$ هو:

$$a_n = \sum_{i=0}^{m-1} C_i (\beta^{p^i})^n \quad (8)$$

حيث β هو جذر المعادلة المميزة:

$$a_n^* = \sum_{i=0}^{m-1} C_i^* (\beta^{p^d})^n \quad (9)$$

و $b_n=a_n . a_n^*$ ويكون:

$$b_n = \sum_{i=0}^{m-1}\sum_{d=0}^{m-1} C_i C_d^* (\beta^{p^i + p^d})^n$$

من أجل I = d يوجد m حد في الحل العام ومن أجل I = d يوجد m (m-1)/2 حد في الحل العام وعدد الحدود الكلي هو:

$$\binom{m}{1} + \binom{m}{2} = m(m+1)/2$$

وذلك أنه:

$a_n^* = a_{n+\delta}$; $-m < \varepsilon < m$ ومنه:

$$a_n^* = \sum_{i=1}^{m} C_i (\beta^{p^i})^\delta (\beta^{p^i})^n$$

أي أنّ:

$$C_i^* = C_i\left(\beta^{P^i}\right)^\delta$$

من أجل i=d نجد أنّ:

$$C_i C_i^* = C_i 2\left(\beta^{P^i}\right)^\delta \neq 0$$

وهذا يعني يوجد m حد في الحل العام يقابل القيم $I = 0, 2, \ldots, m-1$

من أجل $i \neq d$ نجد أنّ:

$$C_d C_i^* = C_i C_d \left(\beta^{P^i}\right)^\delta \quad \text{و}$$

$$C_i C_d^* = C_i C_d \left(\beta^{P^d}\right)^\delta$$

ويكون مجموع الحدين معدوماً عندما:

$$C_i C_d^* = (P-1) C_d C_i^*$$

أو:

$$\left(\beta^{P^d}\right)^\delta = (P-1)\left(\beta^{P^d}\right) \Rightarrow$$

$$\Rightarrow \left(\beta^{(P^d - P^i)}\right)^\delta = P-1$$

أو بما أنّ $P-1 \in GF(P)$ فإنّ:

$$\left[\left(\beta^{P^d - P^i}\right)\right]^{P-1} = 1$$

ومنه:

$$\beta^{\delta(P-1)(P^d - P^i)} = 1$$

أو: $\beta^{\delta(P-1)P^d} = \beta^{\delta(P-1)P^i}$

ومنه: $\left(\beta^{\delta(P-1)}\right)^{P^d} = \left(\beta^{\delta(P-1)}\right)^{P^i}$

إنّ: $a = \beta^{\delta(P-1)} \ni GF(P^m)$ ومنه

$$a^{P^d} = a^{P^i}$$

حيث: $i \leq m$ و $d \leq m$ والمساواة السابقة لا تتحقق إلا إذا كان $i=d=m$ وهذا مخالف للغرض وبالتالي يوجد في الحل العام $m(m-1)/2$ حل مقابل للقيم $i \neq d$ ويكون العدد الكلي للحلول هو:

$$\binom{m}{1} + \binom{m}{2} = m + m(m-1)/2$$

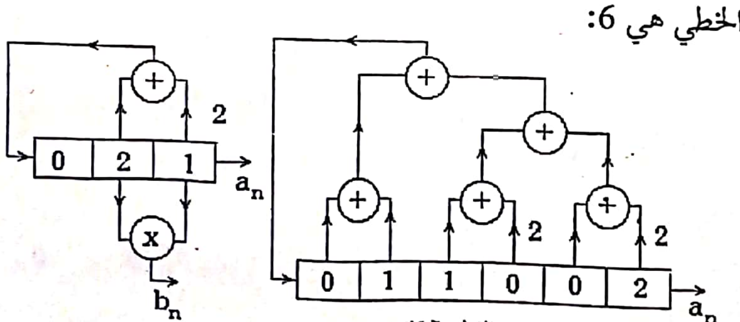
ويساوي $m(m+1)/2$ وهو درجة تعقيد المتتالية $\{b_n\}$ أو طول المكافئ الخطي (المعادلة المميزة لها من الدرجة $m(m+1)/2$).

مثال: بإعتبار المثال السابق ولنعتبر المتتالية $\{b_n\}$ حيث $b_n = a_n . a_{n+1}$

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

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

ودرجة المكافئ الخطي هي 6:



المولد الانزياحي الخطي المكافئ

والمتتالية هي:

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

والدستور التدريجي الخطي المكافئ هو:

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

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

إذا كانت $\{b_n\}$ غير خطية على r درجة فإنّ:

$$b_n = a_{1n} a_{2n} \ldots a_{rn} = \sum_{\substack{l=0 \\ d}}^{m-1} C_{1l1} C_{2l2} \ldots \left(\beta^{p^{l1} + p^{l2} + \ldots + p^{lr}}\right)^n ; d = 1, \ldots, r \tag{10}$$

حيث a_{nk} هو حد المتتالية الموجود في المخرج k المستخدم في عملية الجداء.

بفرض: N_{mr} حيث

$$N_{m2} = \binom{m}{1} + \binom{m}{2} = m + \frac{m(m-1)}{2}$$

$$N_{m3} = \binom{m}{1} + m(m-1) + \binom{m}{3}$$

$$N_{m4} = \binom{m}{1} + m(m-1) + \frac{m(m-1)}{2} + \binom{m-1}{2} + m\binom{m-1}{2} + \binom{m}{4}$$

أيضاً هنا كما في حالة GF(2) فإنه إذا كان r >2 فإن طول المكافئ الخطي دوماً أصغر أو يساوي N_{mr} (حيث أنّ N_{mr} المحسوب في [2] غير صحيح). في حالة r = 3 نأخذ

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

فنجد أنّ:

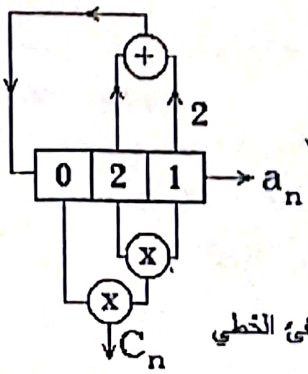
$$C_n = (\beta^2+\beta+2)(\beta+2)^n + (2\beta^2+2\beta).(2\beta^2+\beta+2)^n + 2(\beta^2+\beta+2)^n + (\beta^2+\beta).(\beta^2+2\beta+2)^n + (2\beta^2+1)(2\beta^2+2\beta+2)^n + (2\beta^2+2)(\beta+1)^n + (2\beta^2+\beta).(2\beta^2)^n + (2\beta^2+2\beta+2)(\beta^2+1)^n + (\beta^2+1)(\beta)^n$$

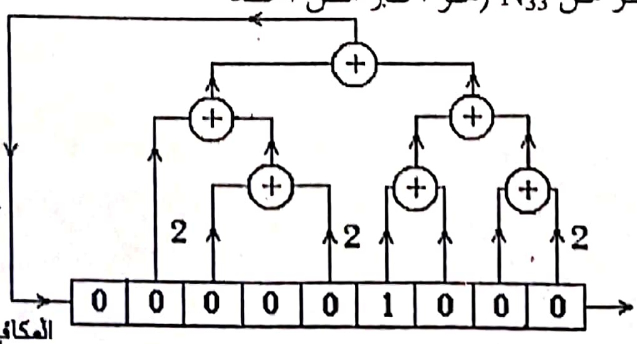
وتعقيد المتتالية المفروض هو:

$N_{33} = \binom{3}{1} + 6 + 1 = 10$

بينما نجد أن التعقيد الناتج هو 9 وهو أصغر من N_{33} (هو أكبر من الحد المذكور في [2]) والدستور التدريجي للمتتالية هو:

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





المكافئ الخطي

إن المتتاليات غير الخطية السابقة تكون على عناصر من متتالية خطية حيث الحلول ومضاعفاتها وجداءاتها من نفس الحقل.

مستنتجة: إذا كان α و β عنصرين من $GF(P^r)$ و$GF(P^S)$ على التوالي ولا ينتميان إلى الحقل $GF(P)$ و r و s أوليان فيما بينهما فإنّ $\alpha.\beta \in GF(P^{r+S})$ و$\alpha.\beta \notin GF(P^r)$ و $\alpha.\beta \notin GF(P^S)$

لنفرض أن $\{a_n\}$ متتالية خطية من $GF(p)$ وحلولها في الحقل الأصغري[1] $GF(P^r)$ وأن المتتالية $\{b_n\}$ خطية من $GF(p)$ وحلولها في الحقل الأصغري $GF(P^S)$ وأن r و s أوليان فيما بينهما فإن متتالية الجداء $\{C_n\} = \{a_n.b_n\}$ من $GF(p)$ وحلولها في الحقل الأصغري $GF(P^{r+S})$ وهذه الحلول مترافقة[2] لحدودية غير حلولة من الدرجة $r.s$ ودور المتتالية $\{C_n\}$ هو$(P^{r-1})(P^{S-1})$

مثال: لتكن المتتالية المعطية في المثال الأول

$$a_{n+3}+2a_{n+1}+a_n = 0 \;;\; a_n \in GF(3)$$

وجدنا أن حل هذه المتتالية هو (موجود في $GF(3^3)$).

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

ولتكن المتتالية:

$$b_{n+2}+b_{n+1}+2b_n = 0 \;;\; b_n \in GF(3)$$

إن المعادلة المميزة لهذه المتتالية هي:

$$X^2+X+2=0$$

بفرض α حل لها أي $\alpha^2+\alpha+2 = 0$ فإن حلها العام هو (وهو موجود في $GF(3^2)$).

$$b_n = (\alpha+2)\,\alpha^n + (2\alpha+1)(2\alpha+2)^n$$

وهي متتالية دورية دورها $8 = 3^2 - 1$

(حيث $b_0 = 0$ و $b_1 = 1$)

لنفرض الآن أنّ المتتالية $\{C_n\}$ هي متتالية الجداء حيث $C_n = a_n \,.\, b_n$ نجد أنّ:

---

[1] الحقل الأصغري لمتتالية خطية تدريجية هو أصغر حقل يحوي حلول معادلتها المميزة (3).

[2] مشابه لكون i و $-i$ حلين مترافقين للحدودية $X^2+1=0$ في حقل الأعداد المركبة C الناتج من توسيع حقل الأعداد الحقيقية R.

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

وهي متالية تدريجية من GF(p) حلها في GF(3^6). دستورها

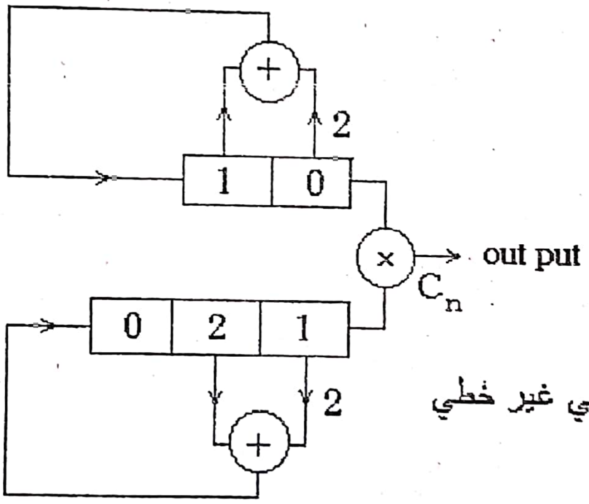
$a_{n+6}+2a_{n+3}+a_{n+2}+a_{n+1}+2a_n = 0$

ومعادلتها المميزة هي:

$X^6+2X^3+X^2+X+2=0$

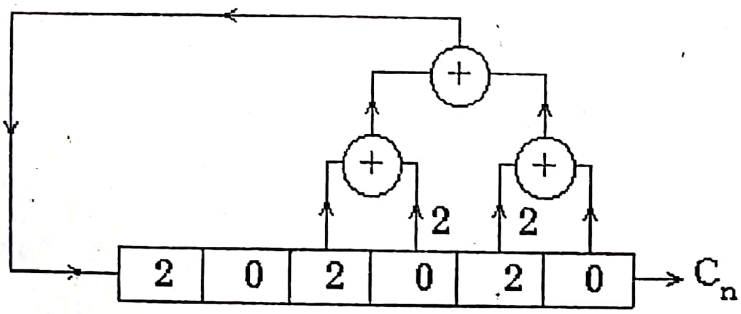
والمتتالية هي:

{0,2,0,2,0,2,0,0,0,0,1,2,0,1,1,0,...}



مولد انزياحي غير خطي

وهي متتالية دورية دورها $3^6 - 1 = 728$



مولد انزياحي خطي مكافئ

إن الصفة غير الخطية يُمكن إستخدامها في الحصول على متتاليات ذات دور كبير جداً. وبصورة خاصة يُمكن إستخدام مولد LFSR يستخدم كمولد مراقبة لـ p مولدات أُخر LFSR(p-1)......, LFSR(0).

- عندما يكون مخرج LFSR هو 0 فإن ناتج المخرج الكلي هو ناتج مخرج LFSR(0).
- عندما يكون مخرج LFSR هو k فإن ناتج المخرج الكلي هو ناتج مخرج LFSR(k).

حيث $0 < k < p-1$ وهذا متعلق بحل المعادلة:

$$S = a_0 I^{p-1} + a_1 I^{p-2} + \dots + a_{p-2} I + a_{p-1} \quad (11)$$

حيث I هو ناتج مخرج LFSR و S هو ناتج مخرج المجموعة وأنّ:

$$I^k = \underbrace{IxIxIx\_\_.xI}_{k\ \text{مرة}}\ ; \quad (\text{mod } p)$$

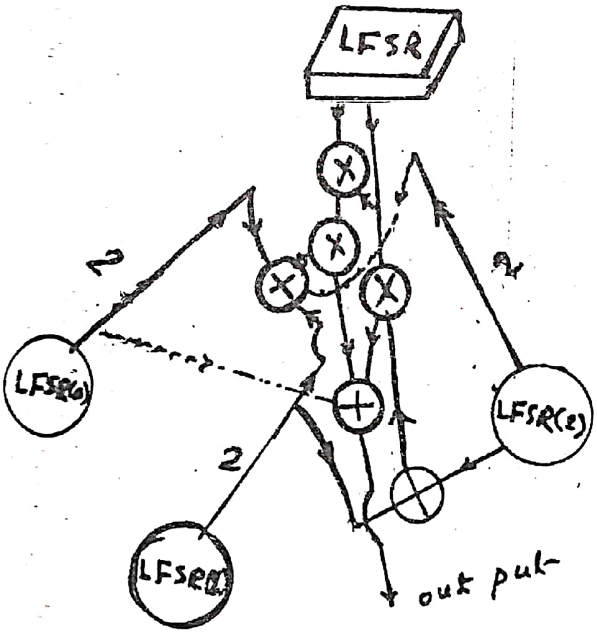
في الحالة الخاصة لـ I=3 نجد:

$$I = 0 \Rightarrow S = I_0 = a_2$$
$$I = 1 \Rightarrow S = I_1 = a_0 + a_1 + a_2$$
$$I = 2 \Rightarrow S = I_2 = a_0 + 2a_1 + a_2$$

ومنه:

$$S = (2I_0+2I_1+2I_0)I^2 + (I+2I_1)I + I_0$$

حيث I_0 هو مخرج LFSR(0) و I_1 مخرج LFSR(1) و I_2 مخرج LFSR(2).



إن إستخدام المجموعة السابقة كمولد مراقبة لـ p-1 مجموعة أخرى من نفس الشكل يؤدي إلى الحصول على مجموعة جديدة عالية التعقيد وتكون المتتالية الجديدة لها دور كبير جداً.

في الحالة الخاصة لما $p = 2$ تصبح المعادلة (11):

$$S = a_0 I + a_1$$
$$I_0 = a_1$$
$$I_1 = a_0 + a_1 = a_0 = I_0 + I_1$$
$$S = (I_0 + I_1)I + I_0$$
$$= (I+1)\, I_0 + I_1\, I$$

وعندئذ يكون شكل المجموعة كما هو معروف في [2].

Abstract

The non-linear-Consequence generators GF(p) when p is a premery number have been studied, in general cose for the previous work [2], and when p = 2 only.

In our present work, we proved that the term:

$$N_{mr} = \sum_{i=1}^{r} \binom{m}{i}$$

Calculated in the previously mentioned work [2] was incorrects when p≠2. Also, soluing the problem to regulation work p generators for the consequences GF(p) by means - off a generator (works a regulator) require soluing that equation of order (p) especially for p=2.

المراجع

[1]- F. D MACWILLAMS ANS N. J. A SLANE the theory of error-correcting Codes North-HOLLAND 1978.

[2]- An Analysis of the structure and Complexity of Nolinear Binary Sequence Generators IEEE Transaction on information theory vol PP22-NE 6 November 1926.

[3]- S. W. Golamb, Shift Register Sequencs San Francisco, Holden day 1967.