数理解析研究所講究録
932巻 1995年 82-102

GFSR法による生成列の重み分布の偏りについて*

栗田 良春†(KURITA Yoshiharu‡) 松本 眞§(MATSUMOTO Makoto¶)

平成7年 11月 3日

要旨

m-系列から構成されるGFSR(Generalized Feedback Shift Register)列が0,1の出現順序に関して偏りを持つことを連続した部分列の重みの平均的な推移を表す伝達関数を導入して示す．特に，原始3項式によるm-系列では，この偏りが大きい．この解析から，その欠陥へのparamterの依存性について明らかにし，GFSR法のための原始多項式の選択指針を示す．この指針による，最適な原始5項式の探索を行い結果を例示する．

1 GFSR(Generalized Feedback Shift Register)法

2値0,1をとる系列$\{a_0, a_1, \cdots\}$が次の2つの条件を満たす時，この列を最大周期列（maximum-length linear feedback shift register sequence, 略して m-系列）という．

(i) 次のp次の線型漸化式に従う列である：$a_i = h_1 a_{i-1} + h_2 a_{i-2} + \cdots + h_p a_{i-p} \mod 2$,
ここに$h_p = 1$, h_kは0または1 $(1 \leq k \leq p-1)$, $i = p, p+1, \cdots$.

(ii) 初期値$a_0, a_1, \cdots, a_{p-1}$をすべて0ではないように与えた時，周期は最大値$2^p - 1$である．

2値系列$\{a_i\}$がm-系列であるための条件は(i)に示した漸化式の特性多項式$x^p + h_{p-1}x^{p-1} + \cdots + 1$がGF(2)上の原始多項式であることである．

GFSR法とは，上の漸化式でa_iをword長のvectorとして生成したvector列を擬似一様乱数として使用するものである．従って，その各bitは同じ漸化式を満たすm-系列となり，最上位bitについても例外でないことに注意したい．

2 三項漸化式の非乱数性

m-系列は擬似乱数としての周期全体にわたるいくつかの望ましい性質をもつ．特にGolomb[2]によって指摘されたrandomnessの次の3つの要請，すなわち，(a) 0と1の個数のbalance，(b) 連の長さの分布，(c) two-leveled auto-correlation,を満たしている．上述のように，2値m-系列は

*Deviation of Weight Distribution of GFSR-sequences

†計量研究所，〒305 つくば市梅園1-1-4, e-mail kuri @nrlm.go.jp
‡National Research Laboratory of Metrology
§慶応義塾大学理工学部数理科学科，〒223 横浜市港北区日吉3-14-1, e-mail matumoto@math.keio.ac.jp
¶Dept. Math. Yagami, Keio Univ.

GF(2)上の原始多項式を特性多項式として生成されるが，その生成効率の観点から項数が最少である原始3項式を用いて，Lewis and Payne [6] によって実際的な生成algorithmが提案された．この方法はTLP法とも呼ばれ，乗算型線形合同式法の本質的な欠陥（超格子構造をもつこと）の指摘もあって，その優位性が注目され，広く使われていると思われる．

このTLP法は，しかしながら統計的検定に関する著者達の実験では，ほとんど常にrej ectされる．それは，後でより正確に述べることとするが，「原始3項式によるm-系列 では 0 の個数が期待値よりも多すぎる部分列があり，1についてはそうではない」と要約される非対称の性質を持ち，TLP 列の most significant bit にこの性質が直接に反映するという事実による．この報告の目的は，2つのtuple間の重みの推移を，すなわち部分列の性質を，重み伝達関数の導入によって解析し，その欠陥をより明確にするものである．

以下，具体的に述べる．

$$\{a_i\} = a_0, a_1, a_2, .., a_{N-1} \tag{1}$$

を0または1の値をとる周期Nのm-系列とし，

$$g(X) = X^p + X^q + 1, \tag{2}$$

ここに $p > 2q$ [1]，を列(1)の$GF(2)$上の特性多項式（原始3項式）とする[2]．このとき，m-系列(1)は$P = 2^p - 1$の周期を持ち，つぎの漸化式をみたす：

$$a_{n+p} + a_{n+q} + a_n = 0 \bmod 2. \tag{3}$$

次に，$A_{n,M}$を（1）の第n項から始まるM-tupleとする：$A_{n,M} = \{a_n, a_{n+1}, .., a_{n+M-1}\}$, そして$w(A_{n,M})$をこの$M$-tupleのwe ight，すなわち1の個数とする：$\sum_{k=0}^{M-1} a_{n+k}$，ここに添字$n+k$は周期を法としてとることとする．

さて，このm-系列が真の2値乱数列であるとすると，次の2つの性質(p1)と(p2)をもつことが期待される．

(p1) WをM-tupleの重みを表す確率変数とすると，Wの確率密度関数は次の二項分布に従う：

$$Prob(W = k) = B_{M,1/2} = \binom{M}{k} (\frac{1}{2})^M. \tag{4}$$

ここに，$\binom{M}{k}$は二項係数，$1 \le k \le M$．

(p2) 互いに素な任意の2つのM-tupleの重みは統計的に独立である．

次の定理は重みの分布に関して情報を与える：

［**定理A**］（例えば，Golomb[2], pp.43-44を参照）周期$2^p - 1$の任意のm-系列において，長さMのbit patternの1周期における出現回数は，すべて0のpatternについては$2^{p-M} - 1$，そうでないpatternについては2^{p-M}である，ここに$1 \le M \le p$.

---

[1] $q > p/2$の場合を考える必要はない：(2)の相反3項式$X^p \cdot g(1/X)$は再び原始的であって，この2つは順序が逆で同じ列を生成する．

[2] 実用上の目的からここではpは$89 \le p \le 1279$の範囲のMersenne指数とする（Zierler[7], Bright and Enison[1]を参照）

この定理で述べているのは，しかしながら，$M \leq p$の場合の出現回数についてだけであって，その出現順序についてではない．そして事実，上にのべた(p2)は成立していないことが次のような方法で簡単に確かめられる：$M \geq p$に対して列(1)からN個の引き続いた，互いに素なM-tuples: $A_{0,M}, A_{M,M}, .., A_{(N-1)M,M}$を取り出す．こうして得られる重み分布のヒストグラムと期待分布(4)を比較することにより，系統的偏りがほとんどいつでも検出できる．そこでは観測した実測分布の殆どは2項分布に比べて一般的に,「左の尾が長く，左肩は痩せ，右肩は太り，右尾はない」形をもち，skewnessを表わす3次momentは負である[3]．言葉を換えれば，隣り合う2つのp-tupleの遷移がuniformでないということになる．

3 p-tupleの重みの推移における平均的振舞いの解析

ここでは，重み伝達関数を導入し，それを用いて$M = p$の場合の前節でのべた偏りを解析する．

[定理B] $f(r)$を$w(A_{n,p}) = r$であるときの$w(A_{n+p,p})$の平均値とする．ここに，$r \in [1:p]$．このとき，

$$f(r) = \frac{r}{(p-1)(p-2)}\{4\lambda r^2 - 2((1+2\lambda)p - 2(1-\lambda))r + (2+\lambda)p^2 - (4-\lambda)p + 2\lambda\}, \quad (5)$$

ここに，$\lambda = q/p\ (0 < \lambda < 1/2)$.

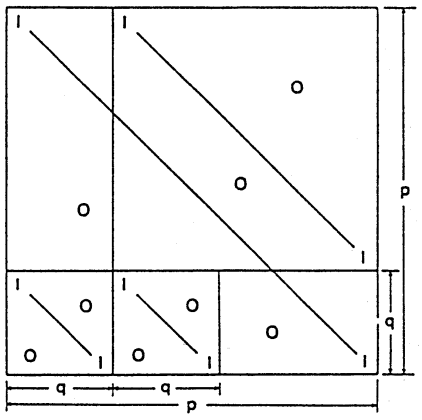
[証明] 次節定理Cの証明に含まれるので省略する．ただし，この場合の遷移行列Tを掲げておく：

p-tuple $A_{n,p}$を列ベクトルとする．漸化式(3)から，次式が成立する．

$$A_{n+p,p} = T \cdot A_{n,p} \bmod 2, \quad (6)$$

ここに，Tは次の形をもつ$(p \times p)$行列である．

$T =$



4 原始 t項式$(t \geq 3)$へのweight transfer functionの導入

[GF(2)]^{p}上の2つのvectorを考える：

[3] この偏りはtupleの長さ$M = \alpha \cdot p, (1 < \alpha <\sim 20)$でいつでも観測される．

$\mathbf{t}=(t_0,t_1,\cdots,t_{p-1}),\qquad \mathbf{x}=(x_0,x_1,\cdots,x_{p-1}).$

ここに各要素はすべて0または1．この内積$\mathbf{t}\cdot\mathbf{x}$を次のように定義する：

$$\mathbf{t}\cdot\mathbf{x}=\sum_{i=0}^{p-1}t_ix_i \mod 2.$$

また，vector $\mathbf{a}$ の重み（要素中の1の個数）を$w(\mathbf{a})$で表す．このとき，次の定理がなりたつ．

［定理C］（[3]参照）$w(\mathbf{t})=\nu$，$w(\mathbf{x})=r$，$1\le\nu\le p$，$1\le r\le p$ とし，$\mathbf{x}$は，そのweightがrであるようなすべてのbit patternを平等に確からしくとるrandom vectorとする．この時，内積$\mathbf{t}\cdot\mathbf{x}$の期待値$\mathbf{E}(\mathbf{t}\cdot\mathbf{x})$は次のように求められる[4]．

$$\mathbf{E}(\mathbf{t}\cdot\mathbf{x})=\frac{1}{\prod_{k=0}^{\nu-1}(p-k)}\sum_{l=1,3,5,\cdots\le\nu}\binom{\nu}{l}\left\{\prod_{k=0}^{l-1}(r-k)\right\}\left\{\prod_{k=0}^{\nu-l-1}(p-r-k)\right\}$$

$$=\frac{1}{\binom{p}{r}}\sum_{l=1,3,5,\cdots\le\nu}\binom{p-\nu}{r-l}\binom{\nu}{l}.$$

但し，積記号$\prod_{k=0}^{*}$において，$*<0$の場合には，この積の値は1とする．

［証明1］$w(\mathbf{x})=r$であって，xのどの要素についても，その要素が1である確率はr/pであることに注意する．はじめに，$\nu=2,3$の場合について考え，それを一般化する．

i) $\nu=2$の場合．
$\mathbf{t}$の要素のうち，1である要素をt_{i_1}，t_{i_2}とする．
x_{i_1}またはx_{i_2}のどちらかだけが1である確率は$\binom{2}{1}\frac{r}{p}\cdot\frac{p-r}{p-1}$．これが$\mathbf{E}(\mathbf{t}\cdot\mathbf{x})$である．

ii) $\nu=3$の場合．
$\mathbf{t}$の要素のうち，1である要素をt_{i_1}，t_{i_2}，t_{i_3}とする．
x_{i_1},x_{i_2},x_{i_3}のうち，ひとつだけが1である確率は$\binom{3}{1}\frac{r}{p}\frac{p-r}{p-1}\frac{p-r-1}{p-2}$．
x_{i_1},x_{i_2},x_{i_3}の3つが共に1である確率は$\binom{3}{3}\frac{r}{p}\frac{r-1}{p-1}\frac{r-2}{p-2}$．これらの和が$\mathbf{E}(\mathbf{t}\cdot bfx)$である．

iii) $\nu=\nu$ の場合について，次のように書き下すことができる：$\mathbf{t}$の要素のうち，1である要素をt_{i_1}，$t_{i_2},\cdots$，t_{i_ν}とする．
x_{i_1}，$x_{i_2},\cdots,x_{i_\nu}$のうち，どれかひとつだけ1である確率は

$$\binom{\nu}{1}\frac{r}{p}\frac{p-r}{p-1}\frac{p-r-1}{p-2}\cdots\frac{p-r-(\nu-2)}{p-(\nu-1)}.$$

x_{i_1}，$x_{i_2},\cdots,x_{i_\nu}$のうち，3つだけ1である確率は

[4]ここで，二項係数$\binom{n}{k}$は一般的な規約に従うものとする．すなわち $n<k$ または $k<0$の時$\binom{n}{k}=0$，但し$n>0$.

$$\binom{\nu}{3}\frac{r}{p}\frac{r-1}{p-1}\frac{r-2}{p-2}\frac{p-r}{p-3}\frac{p-r-1}{p-4}\cdots\frac{p-r-(\nu-4)}{p-(\nu-1)}.$$

こうして，

$x_{i_1}, x_{i_2}, \cdots, x_{i_\nu}$のうち$l$ (odd, $\leq \nu$)個だけ1である確率は

$$\binom{\nu}{l}\cdot\frac{r}{p}\frac{r-1}{p-1}\cdots\frac{r-(l-1)}{p-(l-1)}\frac{p-r}{p-l}\frac{p-r-1}{p-l-1}\cdots\frac{p-r-(\nu-l-1)}{p-(\nu-1)}$$

$$=\binom{\nu}{l}\frac{1}{\prod_{k=0}^{\nu-1}(p-k)}\prod_{k=0}^{l-1}(r-k)\prod_{k=0}^{\nu-l-1}(p-r-k).$$

$\mathbf{E}(\mathbf{t}\cdot\mathbf{x})$は上式の$l=1,3,5,\cdots\leq\nu$についての総和である．

（証明終）

［別証］　$\mathbf{t}$の要素のうち，1である要素を$t_{i_1}, t_{i_2}, \cdots, t_{i_\nu}$とする．

これらのν個のbitのうちから，1を入れるべきl個のbitを選び出す場合の数は$\binom{\nu}{l}$．　但し，$l\leq\nu$．$(p-\nu)$個のbitのうちから，$(r-l$個ある残りの1を入れるべき$)$ $r-l$個のbitを選び出す場合の数は$\binom{p-\nu}{r-l}$．パタンの総数は，p個のbitのうちから，1を入れるべきr個のbitを選び出す場合の数$\binom{p}{r}$に等しい．こうして定理の第2式を得る．

（証明終）

さて，ここで$\mathbf{E}(\mathbf{t}\cdot\mathbf{x})$を（$p$をfixした時の）$r,\nu$の関数として考え，

$$h_p(r,\nu)=\mathbf{E}(\mathbf{t}\cdot\mathbf{x})$$

とする．このとき，次の補題が成り立つ：

［**補題1**］p,r,νを正整数，$1\leq\nu\leq p$, $1\leq r\leq p$であれば，$h_p(r,\nu)=h_p(\nu,r)$.

［**証明**］次式が成立する;

$$h_p(r,\nu)=\frac{1}{p!}\sum_{l=1,3,5,\cdots\leq\nu}\frac{\nu(\nu-1)\cdots(\nu-l+1)\cdot r(r-1)\cdots(r-l+1)\cdot(p-\nu)!(p-r)!}{(p-r-\nu+l)!\,l!}.$$

これから，$\sum$の右側はν,rについて対称であることが分かる．さて$\nu=r$の時は明らか．$\nu<r$と仮定すると

$$\begin{aligned}h_p(r,\nu)-h_p(\nu,r) &= \sum_{l=1,3,5,\cdots\leq\nu}\{\cdots\}-\sum_{l=1,3,5,\cdots\leq r}\{\cdots\}\\ &= -\sum_{\nu<l\leq r,\ l:\text{odd}}\{\cdots\}.\end{aligned}$$

$\{\cdots\}$について次式が成立する．

(1) $(p-\nu)! \geq 0$, $(p-r)! \geq 0$.

(2) $\nu(\nu-1)\cdots(\nu-l+1)$ については $\nu-l<0$ から $\nu-l+1<1$. 従って $\nu(\nu-1)\cdots(\nu-l+1)=0$.

(3) $(p-r-\nu+l)!$ については $\nu-l<0$ から $p-r-(\nu-l)>p-r>0$.
従って $(p-r-\nu+l)!>0$.

こうして $\sum_{\nu<l\leq r,\ l:\text{odd}}\{\cdots\}=0$. $\nu>r$ の時も全く同様に証明できる.

(証明終)

$h_p(r,\nu)$ では, r は1から p までの整数値をとるが, 以後しばらくの間, 関数の振舞いを調べるため, r は同範囲の連続値をとるものとしよう. 更に, 定義域, 値域ともに $(-1/2,1/2)$ とするために, 次のように $h_p(r,\nu)$ を再定義する:

$$y_p(x,\nu)=h_p((x+\frac{1}{2})p,\nu)-\frac{1}{2}.$$

すなわち,

$$y_p(x,\nu)=\frac{1}{\prod_{k=0}^{\nu-1}(p-k)}\left[\sum_{l=1,3,5,\cdots\leq\nu}\binom{\nu}{l}\prod_{k=0}^{l-1}\left\{(\frac{1}{2}+x)p-k\right\}\prod_{k=0}^{\nu-l-1}\left\{(\frac{1}{2}-x)p-k\right\}\right]-\frac{1}{2}.$$

この時, 次の補題が成立する.

[補題2] $y_p(x,\nu)$ は, 偶関数 (ν:even の時), または奇関数 (ν:odd の時) である.

[証明] 次式が成立することに注意する (その証明はたとえば Knuth[4], p58.):

$$\sum_{l=0,1,2,\cdots\nu}\binom{p-r}{\nu-l}\binom{r}{l}=\binom{p}{\nu}. \tag{7}$$

$z_p(x,\nu)=y_p(x,\nu)+1/2$ とおく. 更に $\nu-l=l'$ とおくと,

$$\binom{\nu}{l}=\binom{\nu}{l'},\quad \prod_{k=0}^{l-1}=\prod_{k=0}^{\nu-l'-1},\quad \prod_{k=0}^{\nu-l-1}=\prod_{k=0}^{l'-1}$$

であるから, 次の(i),(ii)が成立する:

(i) ν :even の時, $l=1,3,5,\cdots,\nu-1$ に対応して $l'=\nu-1,\nu-3,\cdots,1$.
故に $z_p(-x,\nu)=z_p(x,\nu)$, すなわち $y_p(-x,\nu)=y_p(x,\nu)$.

(ii) ν :odd の時, $l=1,3,5,\cdots,\nu$ に対応して $l'=\nu-1,\nu-3,\cdots,0$.

こうして,

$$z_p(x,\nu)+z_p(-x,\nu)=\frac{1}{\prod_{k=0}^{\nu-1}(p-k)}\sum_{l=1,2,3,\cdots,\leq\nu}\binom{\nu}{l}\prod_{k=0}^{l-1}\left\{(\frac{1}{2}+x)p-k\right\}\prod_{k=0}^{\nu-l-1}\left\{(\frac{1}{2}-x)p-k\right\}$$

$= 1$

が成立する．何故ならば，右辺はν次の多項式，従って異なる$\nu+1$個のxに対して1であれば，これは恒等的に1となる．ところで等式(7)から，$-1/2 \le x \le 1/2$に対応するr $(0 \le r/p \le 1)$のうちから$p+1$個の異なる値：$r = 0, 1, 2, \dots, p$を選ぶことができて補題が成立．更に，$p+1 \ge \nu+1$　であるから証明できた．

（証明終）

さて，関数$y_p(x,\nu)$がどのような関数であるかを具体的に知ることが重要であるが，次のような簡潔な漸化式がなりたつ．

［定理D］任意の$0 < p, \nu$と任意のxに対して，次の漸化式が成り立つ．

$$y_p(x,\nu+1) + \frac{2px}{p-\nu} \cdot y_p(x,\nu) + \frac{\nu}{p-\nu} \cdot y_p(x,\nu-1) = 0,$$

$$y_p(x,1) = x, \quad y_p(x,0) = 1/2.$$

［証明］y_pの定義にもどり，漸化式をh_pで書き直すと，

$$(p-\nu)h_p(r,\nu+1) + (2r-p)h_p(r,\nu) + \nu h_p(r,\nu-1) = r$$

と同値であることがわかる．さて，

$$h_p(r,\nu) = \frac{1}{\binom{p}{r}} \sum_{l=1,3,5,\cdots \le \nu} \binom{p-\nu}{r-l}\binom{\nu}{l}.$$

であったが，ここで，$\binom{\nu}{l}$などをνの多項式と見て実関数に拡張すると，$0 \le \nu < l$なる整数では0をとるようになる．これに注意すると，添字lは$0 \le l \le p$なる奇数を全て走るとしてもよい．(以後単にl : odd と書く．)

上式の両辺を$\binom{p}{r}$倍したものを証明する．

$\binom{\nu+1}{l} = \frac{\nu+1}{\nu-l+1}\binom{\nu}{l}$ の公式を使えば，左辺の三項は全て$F_{p,r,\nu,l} := \binom{p-\nu}{r-l}\binom{\nu}{l}$ の一次結合で表される．すなわち，左辺の三つの項の和は

$$\sum_{l:\mathrm{odd}} F_{p,r,\nu,l}\left\{(p-\nu)\frac{p-\nu-r+l}{p-\nu} \cdot \frac{\nu+1}{\nu-l+1} + (2r-p) + \nu\frac{p-\nu+1}{p-\nu-r+l+1} \cdot \frac{\nu-l}{\nu}\right\}$$

で表される．一方，右辺は

$$r\binom{p}{r} = (p-r+1)\binom{p}{r-1}$$

であるが，公式

$$\binom{p}{r} = \sum_l \binom{p-\nu}{r-l}\binom{\nu}{l}$$

でrを$r+1$に置き換え，lの奇遇を分けることにより

$$
\begin{aligned}
(p-r+1)\binom{p}{r} &= (p-r+1)\sum_{l:\text{odd}}\left\{\binom{p-\nu}{r-1-l}\binom{\nu}{l}+\binom{p-\nu}{r-l}\binom{\nu}{l}\right\} \\
&= (p-r+1)\sum_{l:\text{odd}} F_{p,r,\nu,l}\left\{\frac{r-l}{p-\nu-r+l+1}+\frac{l}{\nu-l+1}\right\}
\end{aligned}
$$

を得る．よって，

$$
\begin{aligned}
&(p-\nu)\frac{p-\nu-r+l}{p-\nu}\cdot\frac{\nu+1}{\nu-l+1}+(2r-p)+\nu\frac{p-\nu+1}{p-\nu-r+l+1}\cdot\frac{\nu-l}{\nu} \\
=\ &(p-r+1)\left\{\frac{r-l}{p-\nu-r+l+1}+\frac{l}{\nu-l+1}\right\}
\end{aligned}
$$

を証明すればよい．これは$A:=p-r+1$, $B:=\nu-l$とおき，p, l を消去すると「手計算」でも検証できる．

（証明終）

上の漸化式により，$h_p(x,\nu)$および$y_p(x,\nu)$を次々に計算できる．また，例えば定数項が

$$
y_p(0,\nu+1)=-\frac{\nu}{p-\nu}y_p(0,\nu-1)
$$

を満たすことがわかる．νが偶数の時にはこれは0であるが，奇数の時には決して0にならず，その絶対値の最小値はνが$p/2$にもっとも近い整数で達成されることがわかる（そこまでは絶対値が1つおきに単調に減少する）．また，xが十分0に近い時は，漸化式の中央の項の寄与は小さく，同様の計算によってνは$p/2$からあまり離れないところで$|y_p(x,\nu)|$は小さくなると考えられる．

参考までに$\nu=1,2,3,4,5,6$について，$h_p(r,\nu)$を書き下せば次の通りである．

$$
\begin{aligned}
h_p(r,1) &= r/p, \\
h_p(r,2) &= \frac{2r(p-r)}{p(p-1)}, \\
h_p(r,3) &= \frac{r(4r^2-6pr+3p^2-3p+2)}{p(p-1)(p-2)}, \\
h_p(r,4) &= \frac{4r(-2r^3+4pr^2-3p^2r+3pr-4r+p^3-3p^2+4p)}{p(p-1)(p-2)(p-3)}, \\
h_p(r,5) &= \frac{r(16r^4-40pr^3+40p^2r^2-40pr^2+80r^2-20p^3r+60p^2r}{p(p-1)(p-2)(p-3)(p-4)} \\
&\quad \frac{-120pr+5p^4-30p^3+75p^2-50p+24)}{}, \\
h_p(r,6) &= \frac{2r(-16r^5+48pr^4-60p^2r^3+60pr^3-160r^3+40p^3r^2}{p(p-1)(p-2)(p-3)(p-4)(p-5)} \\
&\quad \frac{-120p^2r^2+320pr^2-15p^4r+90p^3r-285p^2r+210pr-184r}{} \\
&\quad \frac{+3p^5-30p^4+125p^3-210p^2+184p)}{}.
\end{aligned}
$$

また，$\nu = 1,2,3,4,5,6$ について，$y_p(x,\nu)$ を書き下せば次の通りである．

$$
\begin{aligned}
y_p(x,1) &= x, \\
y_p(x,2) &= \frac{1-4px^2}{2(p-1)}, \\
y_p(x,3) &= \frac{x(4p^2x^2-3p+2)}{(p-1)(p-2)}, \\
y_p(x,4) &= -\frac{16p^3x^4-8(3p-4)px^2+3p-6}{2(p-1)(p-2)(p-3)}, \\
y_p(x,5) &= \frac{x(16p^4x^4-40(p-2)p^2x^2+15p^2-50p+24)}{(p-1)(p-2)(p-3)(p-4)}, \\
y_p(x,6) &= -\frac{64p^5x^6-80(3p-8)p^3x^4+4(45p^2-210p+184)px^2-15p^2+90p-120}{2(p-1)(p-2)(p-3)(p-4)(p-5)}.
\end{aligned}
$$

これら $y_p(x,\nu)$ の振舞いの実例を Fig. 4A に示す．

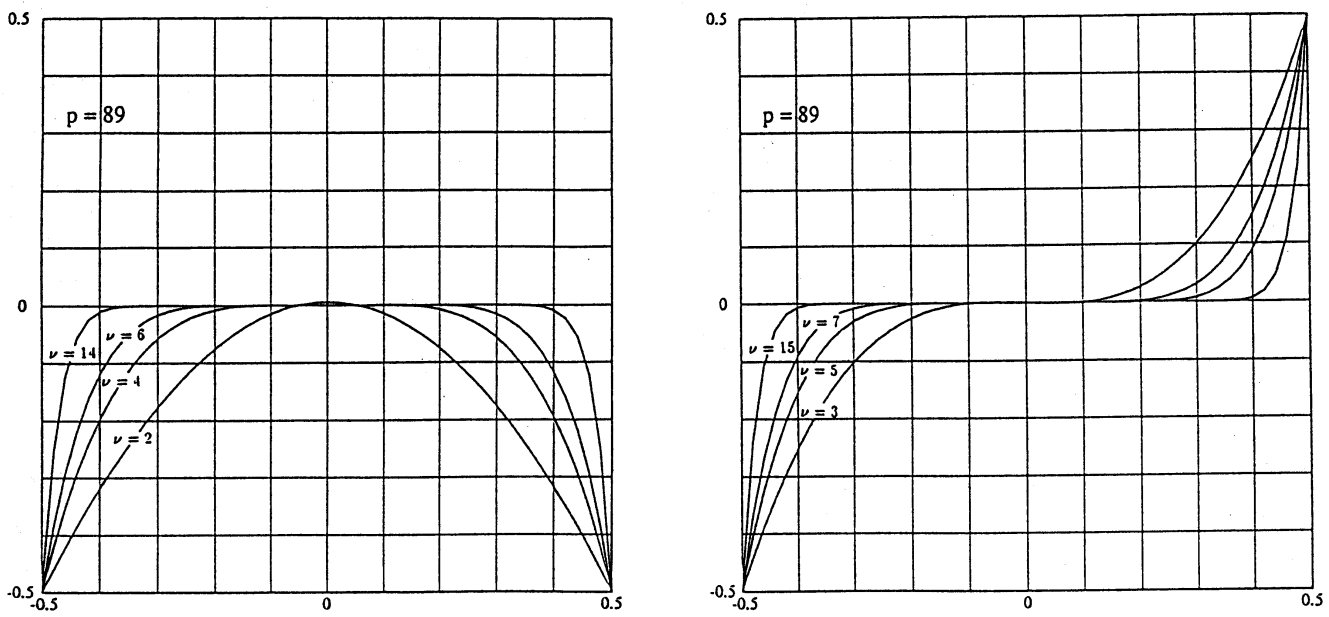


Fig. 4A Behavior of expected inner product of
two random vectors on GF(2): $y_p(x,\nu)$.

このgraphからも視覚的に分かるが,［定理D］の漸化式から, p,νを定数とし, rが平均的重み$p/2$付近を動く変数として$h_p(r,\nu)$ を一変数関数と考えると, これはν が$p/2$付近のとき定数関数（定数1/2）に近付く. したがって, 乱数性からみれば項数νが$p/2$付近になるのが望ましいといえる. 但し, 数値実験の結果から$|h_p(r,\nu)-1/2|$ のνについての単調性は成立しない. その数値例$(p=31, r=9)$をTABLE 4A に示す.

TABLE 4A
Numerical evaluation of $h_p(r,\nu)-1/2$

$p=31,\ r=9$			
ν	$h_p(r,\nu)-1/2$	ν	$h_p(r,\nu)-1/2$
0	- 0.500 00000	9	- 0.000 22859
1	- 0.209 67741	10	- 0.000 00136
2	- 0.074 19354	11	0.000 10801
3	- 0.018 79866	12	0.000 07095
4	- 0.000 77864	13	- 0.000 01966
5	0.002 41008	14	- 0.000 06545
6	0.001 35478	15	- 0.000 03385
7	0.000 12606	16	0.000 03385
8	- 0.000 32685	···	·····

ここまでの用意で［定理B］の一般化ができる. あるp−tuple $\mathbf{X}$（縦ベクトル）のweightをr, すなわち, $w(\mathbf{X})=r\ (1\le r\le p)$, 更に$(T_t)_{k*}$ （Tの第k行）のweightを$\nu, (0\le\nu\le p)$とする. この時$\sum_{l=1}^{p}(T_t)_{kl}\cdot(\mathbf{X})_l$のweightの期待値が$h_p(r,\nu)$である.

さて, 前節の（6）式の推移行列Tは, 原始3項式に対するものであったから, これをT_3と書くことにすると, T_3についてのweight transfer function: (5)式は, 実は, $f(r)=(p-q)h_p(r,2)+qh_p(r,3)$であった. すなわち, 原始3項式については, $\nu=2$のtが$(p-q)$個, $\nu=3$のtがq個あって, $\nu\ge 4$のtは存在しない. この事実に由来する欠陥は既に述べたが, Fig. 4A の$\nu=2$のgraphから, 更に（graphからは読みとり難いが）$\nu=3$からも, 明らかとなる.

$T_t(t\ge 5)$を, しかしながら, $p,q_1,q_2,\cdots$によって一般式として見通しよく表現することは難しいように思われる. 具体的な原始5項式に対応するT_5の計算結果例をFig. 4Bに示す[5]. この図において, 白丸は0, 黒丸は1を表し, T_5の左側の3列は左から順に, 通し番号, その（通し番号の）列のweight, その行のweightを表す. 行列右側のc欄はhistogramで, そのweightをもつ列数を, 最下行の%つき数は1の占める割合を示したものである. r欄は行についてである. 上図(12%)と下図(20%)を比較すると, 本章の結論から下図の行列の方が, 推移の独立性は高いことが予測される.

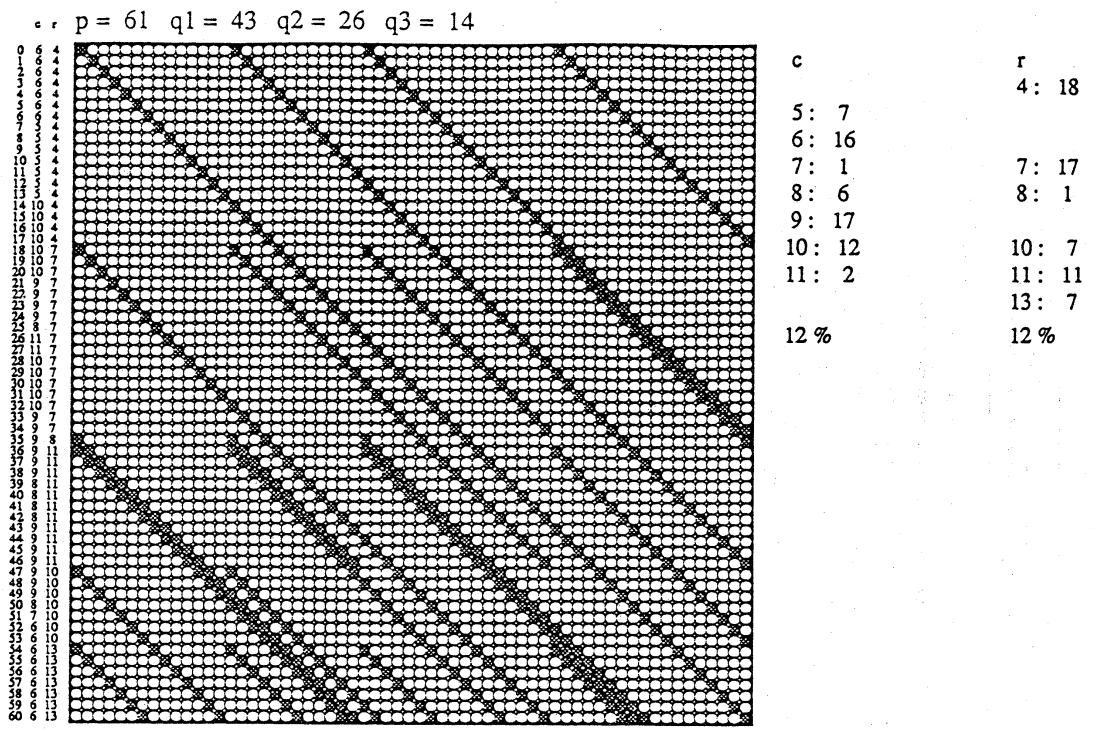
この2例についてのweight transfer functionの数値をTABLE 4Bに示す. このTABLEの左側第一列はrを, 第2列はFig. 4Bの上側の遷移行列, 第3列は下側の遷移行列に対応する数値である. たとえば, 第2列について書き下せば, $p=61$として,

$$(18h_p(r,4)+17h_p(r,7)+h_p(r,8)+7h_p(r,10)+11h_p(r,11)+7h_p(r,13))/p-1/2$$

[5]なお, 原始5項式の探索方法とその結果についてはKurita and Matsumoto[5]を参照されたい.

を評価したものである．第2列，第3列の比較から予測どおり，第3列は約2倍第2列より精度が高く，最も出現頻度の高い$r = p/2$付近では7×10^{-5}程度である．TABLEの右の表は比較のための，3項式$(x^{89} + x^{38} + 1)$についてのものである（$p = 61$の原始3項式は存在しない）．次数が89とより高いにも拘わらず，偏りが極めて大きいこと（約50倍）がわかる．

このようにして，T_t $(T \geq 5)$の各行のweightが数値として具体的に与えられた場合には$p-$tupleのweightの平均的推移を求めることができることになり，この尺度からの最適化をはかることが可能となった．GFSR法のための原始多項式のひとつの選択指針がこうして得られたことになる．



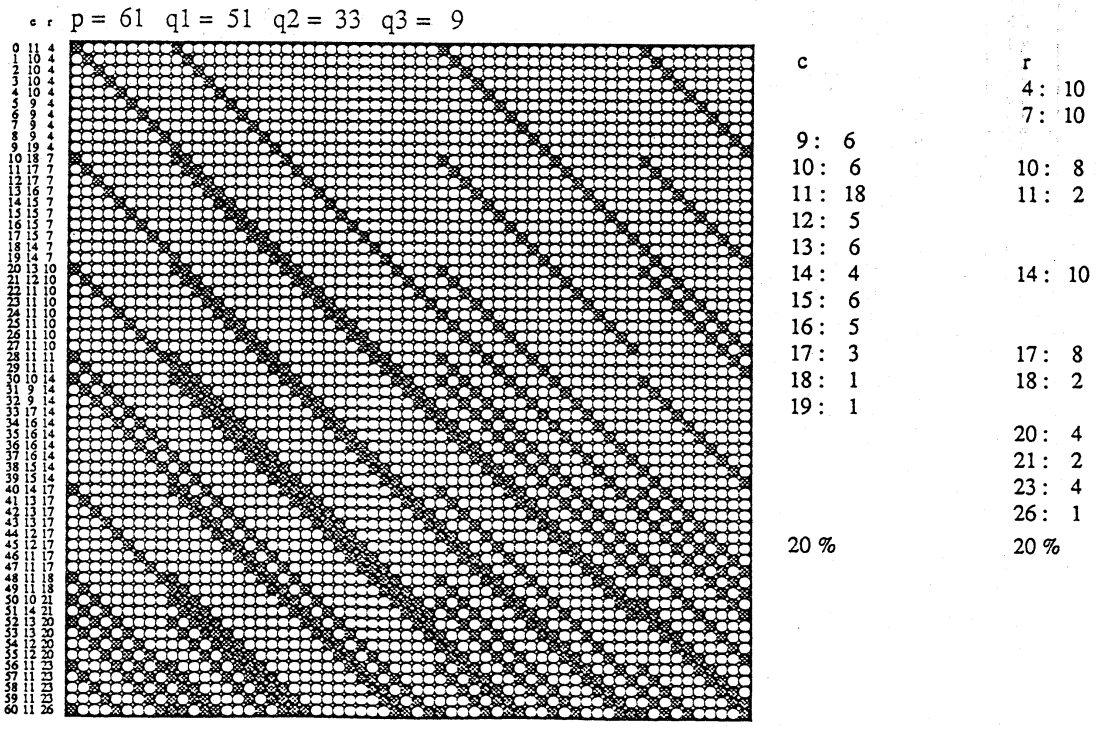


Fig. 4B Example of transition matrix T_5 (61×61) of two primitive pentanomials: $(x^{61} + x^{43} + x^{26} + x^{14} + 1)$ and $(x^{61} + x^{51} + x^{33} + x^9 + 1)$, where ○ means 0 and ● means 1.

TABLE 4B Numerical evaluation of weight transfer function corresponding to Fig. 4B and primitive trinomial $(x^{89} + x^{38} + 1)$.

	$x^{61}+x^{43}+x^{26}+x^{14}+1$	$x^{61}+x^{51}+x^{33}+x^{9}+1$
0	- 0.5	- 0.5
1	- 0.370 73367	- 0.294 67884
2	- 0.276 56543	- 0.188 99041
3	- 0.207 69293	- 0.129 55739
4	- 0.157 02494	- 0.093 05667
5	- 0.119 46413	- 0.068 89658
6	- 0.091 36656	- 0.051 96941
7	- 0.070 13836	- 0.039 62045
8	- 0.053 93757	- 0.030 35706
9	- 0.041 45625	- 0.023 27672
10	- 0.031 76284	- 0.017 79855
11	- 0.024 18939	- 0.013 52885
12	- 0.018 25186	- 0.010 18931
13	- 0.013 59434	- 0.007 57655
14	- 0.009 95044	- 0.005 53796
15	- 0.007 11680	- 0.003 95669
16	- 0.004 93497	- 0.002 74169
17	- 0.003 27914	- 0.001 82098
18	- 0.002 04767	- 0.001 13686
19	- 0.001 15730	- 0.000 64243
20	- 0.000 53899	- 0.000 29913
21	- 0.000 13500	- 0.000 07483
22	0.000 10331	0.000 05745
23	0.000 21717	0.000 12062
24	0.000 24162	0.000 13413
25	0.000 20644	0.000 11455
26	0.000 13685	0.000 07591
27	0.000 05394	0.000 02992
28	- 0.000 02506	- 0.000 01386
29	- 0.000 08676	- 0.000 04807
30	- 0.000 12164	- 0.000 06744
31	- 0.000 12429	- 0.000 06898
32	- 0.000 09362	- 0.000 05206
33	- 0.000 03323	- 0.000 01863
34	0.000 04833	0.000 02663
35	0.000 13739	0.000 07618
36	0.000 21493	0.000 11947
37	0.000 25675	0.000 14297
38	0.000 23366	0.000 13034
39	0.000 11201	0.000 06271
40	- 0.000 14550	- 0.000 08081
41	- 0.000 57886	- 0.000 32246
42	- 0.001 22934	- 0.000 68499
43	- 0.002 13792	- 0.001 19061
44	- 0.003 34346	- 0.001 85990
45	- 0.004 88052	- 0.002 71042
46	- 0.006 77687	- 0.003 75542
47	- 0.009 05040	- 0.005 00242
48	- 0.011 70508	- 0.006 45234
49	- 0.014 72538	- 0.008 09942
50	- 0.018 06782	- 0.009 93313
51	- 0.021 64827	- 0.011 94323
52	- 0.025 32213	- 0.014 12996
53	- 0.028 85392	- 0.016 52209
54	- 0.031 87091	- 0.019 20718
55	- 0.033 79376	- 0.022 37853
56	- 0.033 73425	- 0.026 39912
57	- 0.030 34730	- 0.031 86091
58	- 0.021 62030	- 0.039 55606
59	- 0.004 57762	- 0.050 13885
60	0.025 12765	- 0.063 02069
61	0.073 77049	- 0.073 77049

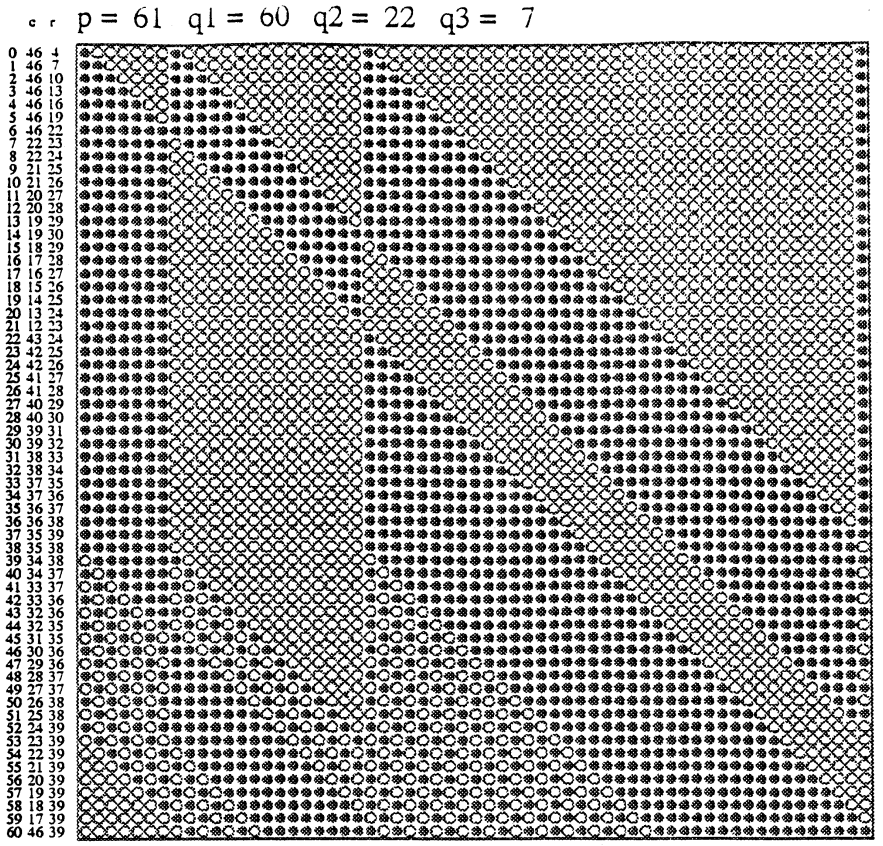
	$x^{89}+x^{38}+1$		$x^{89}+x^{38}+1$
0	- 0.5	45	0.003 13657
1	- 0.472 73071	46	0.002 68600
2	- 0.446 40828	47	0.001 96533
3	- 0.421 01765	48	0.000 98959
4	- 0.396 54380	49	- 0.000 22617
5	- 0.372 97169	50	- 0.001 66693
6	- 0.350 28627	51	- 0.003 31763
7	- 0.328 47250	52	- 0.005 16325
8	- 0.307 51535	53	- 0.007 18873
9	- 0.287 39978	54	- 0.009 37906
10	- 0.268 11075	55	- 0.011 71917
11	- 0.249 63323	56	- 0.014 19404
12	- 0.231 95216	57	- 0.016 78863
13	- 0.215 05252	58	- 0.019 48789
14	- 0.198 91926	59	- 0.022 27680
15	- 0.183 53735	60	- 0.025 14030
16	- 0.168 89174	61	- 0.028 06337
17	- 0.154 96741	62	- 0.031 03096
18	- 0.141 74930	63	- 0.034 02803
19	- 0.129 22238	64	- 0.037 03955
20	- 0.117 37162	65	- 0.040 05047
21	- 0.106 18197	66	- 0.043 04576
22	- 0.095 63839	67	- 0.046 01038
23	- 0.085 72585	68	- 0.048 92929
24	- 0.076 42930	69	- 0.051 78745
25	- 0.067 73372	70	- 0.054 56983
26	- 0.059 62405	71	- 0.057 26138
27	- 0.052 08526	72	- 0.059 84706
28	- 0.045 10232	73	- 0.062 31184
29	- 0.038 66017	74	- 0.064 64067
30	- 0.032 74379	75	- 0.066 81853
31	- 0.027 33814	76	- 0.068 83036
32	- 0.022 42817	77	- 0.070 66114
33	- 0.017 99885	78	- 0.072 29581
34	- 0.014 03514	79	- 0.073 71935
35	- 0.010 52200	80	- 0.074 91672
36	- 0.007 44439	81	- 0.075 87287
37	- 0.004 78728	82	- 0.076 57277
38	- 0.002 53561	83	- 0.077 00137
39	- 0.000 67437	84	- 0.077 14365
40	0.000 81150	85	- 0.076 98455
41	0.001 93703	86	- 0.076 50905
42	0.002 71727	87	- 0.075 70210
43	0.003 16724	88	- 0.074 54866
44	0.003 30200	89	- 0.073 03370

この指針から原始5項式を選択した例を挙げる：第5章で述べるalgorithmによって次数pの原始5項式を探索し，それぞれのpについて，得られた数百個の原始5項式からT_5の中の1の占める割合が50%に最も近い3例ずつをTABLE 4Cに示す.

TABLE 4C
Examples of optimum primitive pentanomials

p	q_3	q_2	q_1	max	mean	σ	%
	60	22	7	39	30.39	8.39	49.83
61	59	34	3	46	30.44	11.55	49.91
	60	33	18	49	30.64	10.03	50.23
	87	38	9	65	44.37	17.07	49.85
89	87	43	7	59	44.51	15.98	50.01
	88	45	29	65	44.62	12.95	50.13
	106	43	21	76	53.44	14.06	49.94
107	106	89	22	74	53.60	14.07	50.09
	105	50	29	80	53.93	21.48	50.41
	125	86	9	95	63.46	24.47	49.97
127	126	28	13	99	63.50	26.82	50.00
	126	21	18	106	63.53	32.19	50.02
	520	125	57	431	260.07	110.52	49.92
521	520	342	308	402	260.72	91.80	50.04
	520	415	293	325	260.74	67.56	50.05
	606	44	4	563	302.99	170.46	49.92
607	605	418	123	446	303.05	123.05	49.93
	606	465	127	396	303.35	81.78	49.98
	1278	292	274	1252	639.10	346.12	49.97
1279	1278	366	354	1261	639.34	350.74	49.99
	1278	804	792	1249	643.25	346.07	50.29

この表では，左4列にp, q_3, q_2, q_1を，各行のweightの最大値(max)を第5列に，行についてのweightの平均値(mean)を第6列に，その標準偏差(σ)を第7列に，そして，最右列には，行列全体の中の1の占める割合(%)を示す．なお，予想されるように，q_3はこの場合pに極めて近い．この表のはじめの6行に対応するT_5をFig.4C(a),(b),(c);(e),(f),(g)に，また対角的なpatternをもつ原始5項式のT_5をFig.4C(d)に示す.



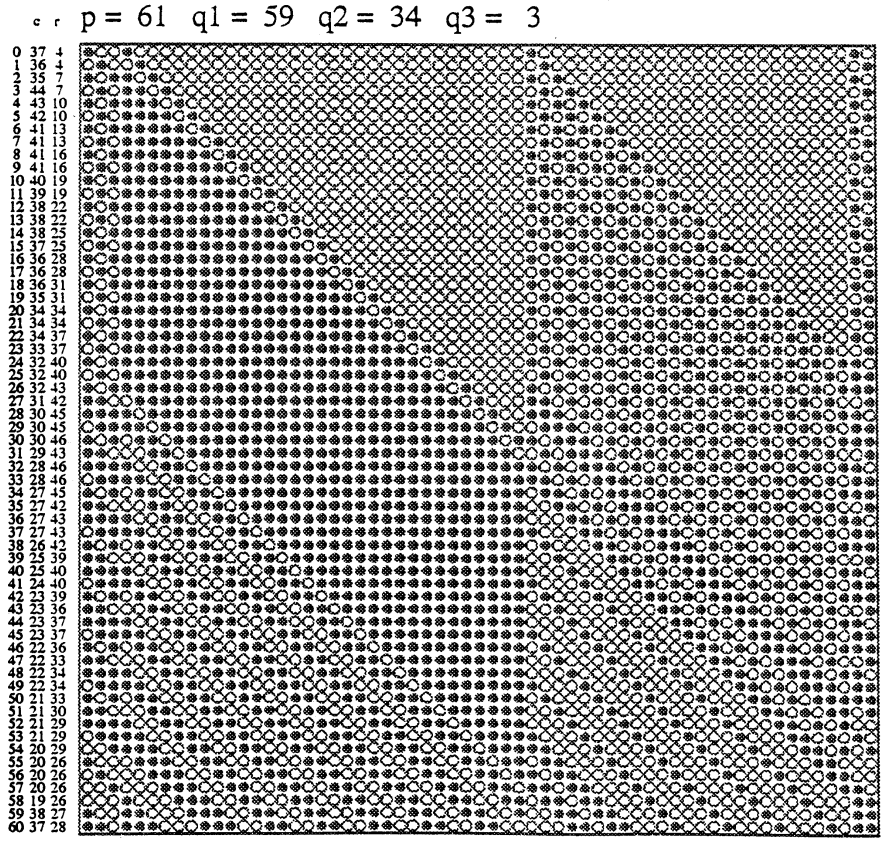
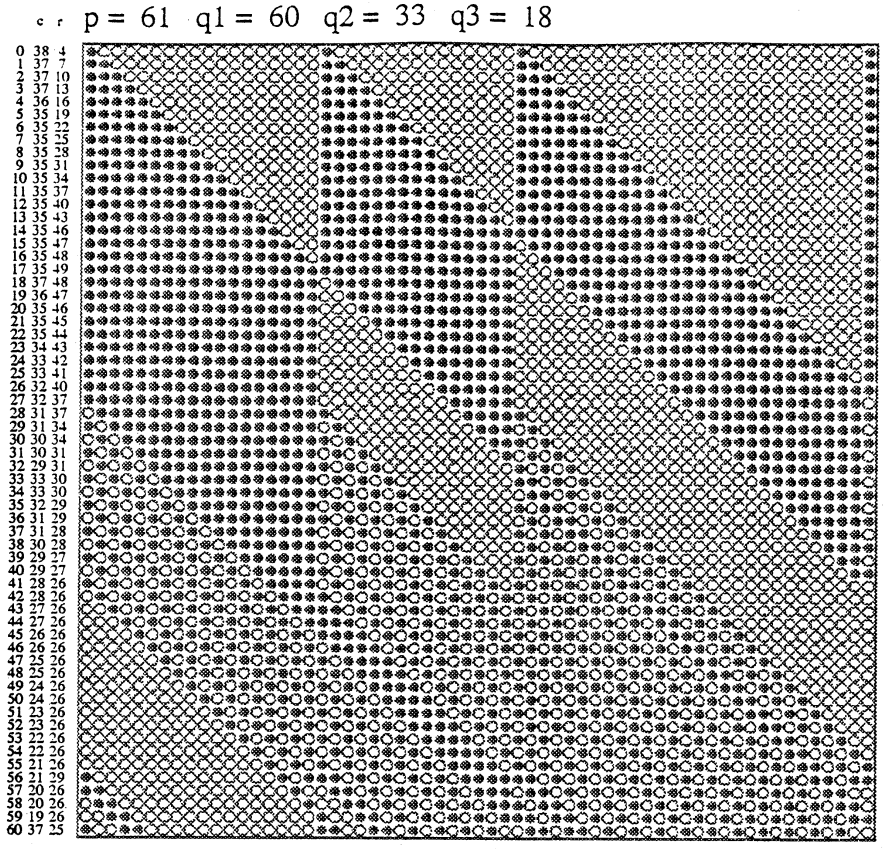


Fig. 4C(a),(b) Example of transition matrix T_5 (61×61) of two primitive pentanomials $(x^{61} + x^{60} + x^{22} + x^7 + 1)$ and $(x^{61} + x^{59} + x^{34} + x^3 + 1)$, where ∘ means 0 and • means 1.



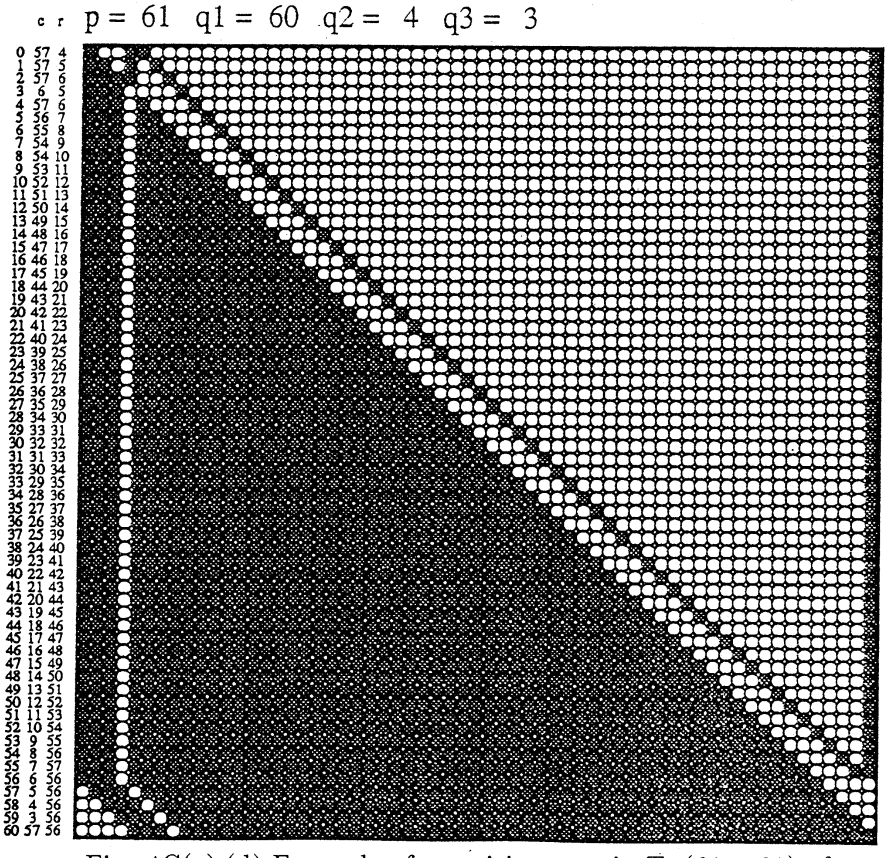


Fig. 4C(c),(d) Example of transition matrix T_5 (61×61) of two primitive pentanomials $(x^{61} + x^{60} + x^{33} + x^{18} + 1)$ and $(x^{61} + x^{60} + x^4 + x^3 + 1)$, where $\circ$ means 0 and $\bullet$ means 1.

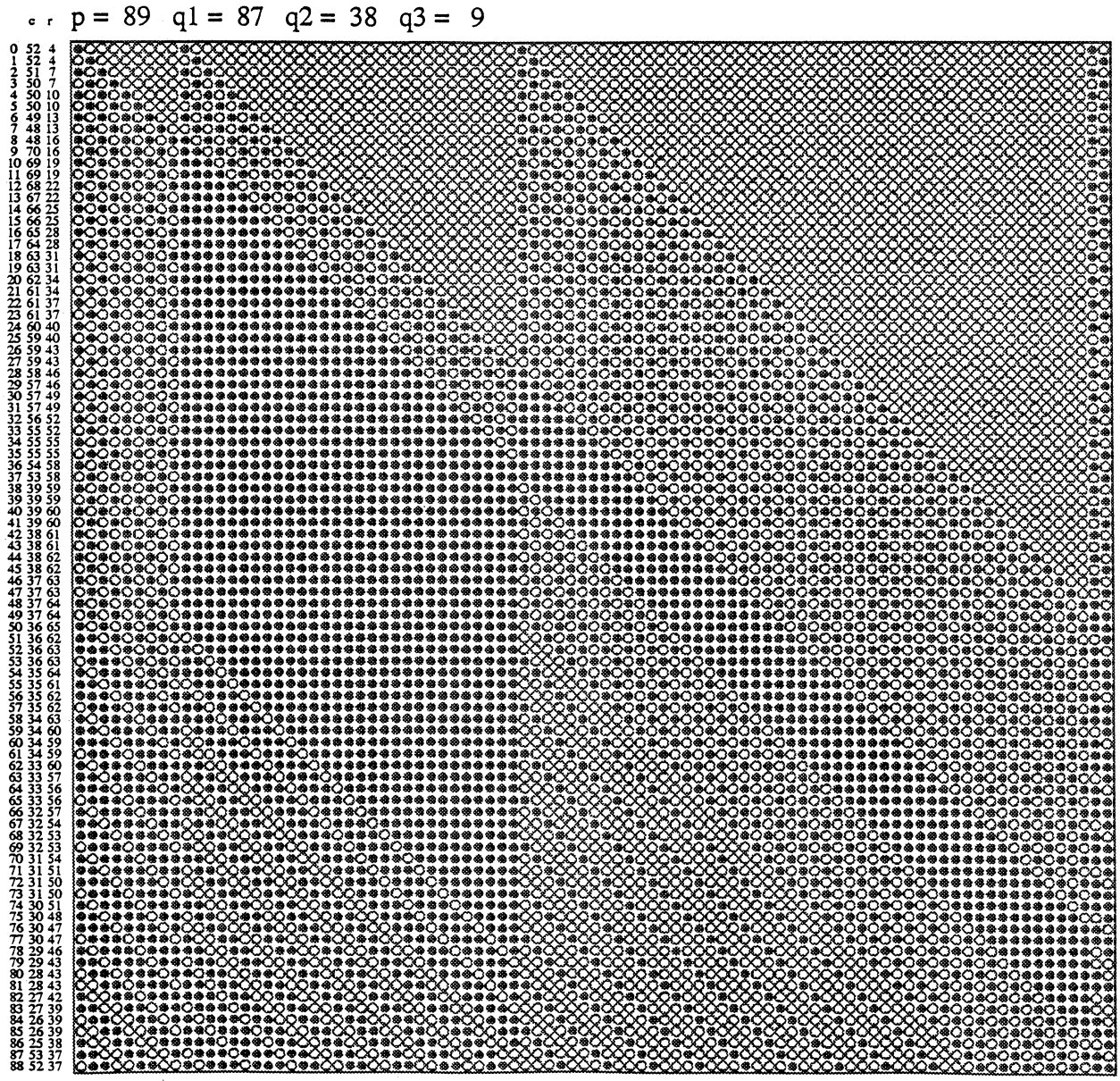


Fig. 4C(e) Example of transition matrix T_5 (89×89) of primitive pentanomial corresponding to TABLE 4C $(x^{89} + x^{87} + x^{38} + x^9 + 1)$, where $\circ$ means 0 and $\bullet$ means 1.

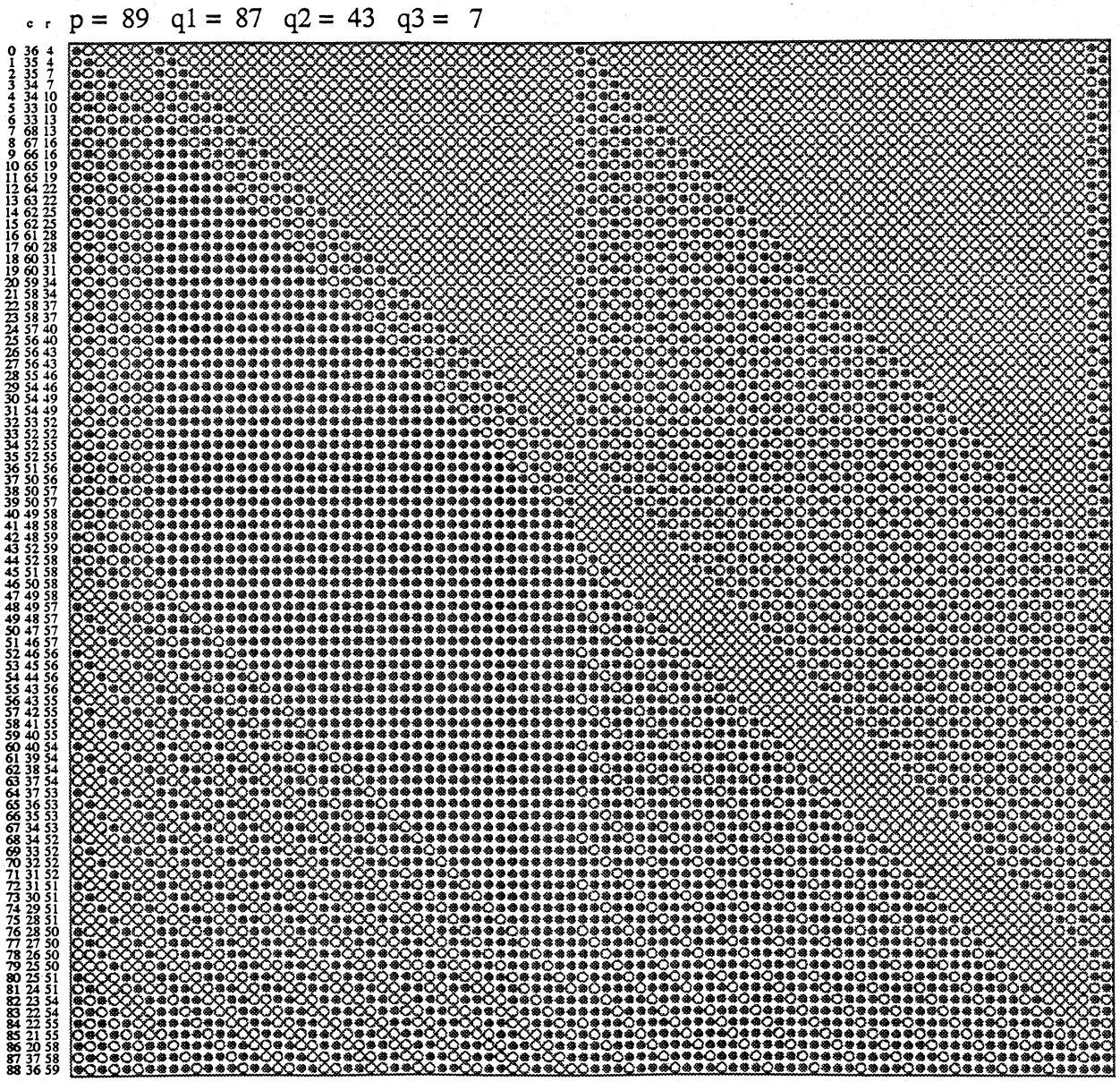


Fig. 4C(f) Example of transition matrix T_5 (89×89) of primitive pentanomial corresponding to TABLE 4C $(x^{89} + x^{87} + x^{43} + x^7 + 1)$, where $\circ$ means 0 and $\bullet$ means 1.

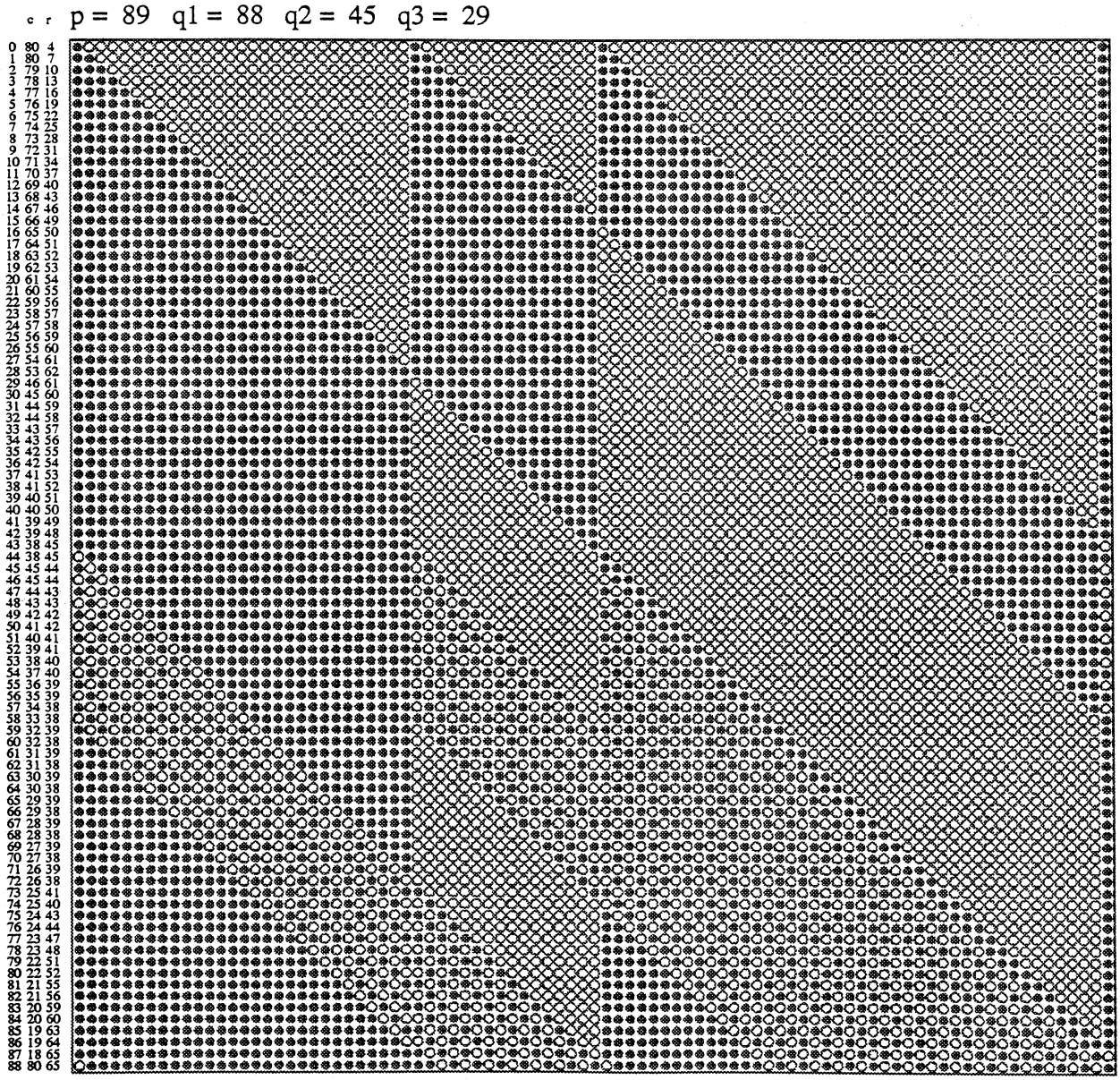


Fig. 4C(g) Example of transition matrix T_5 (89×89) of primitive pentanomial corresponding to TABLE 4C $(x^{89} + x^{88} + x^{45} + x^{29} + 1)$, where ∘ means 0 and • means 1.

5 まとめ

主要な結果を以下に要約する：

(i) 2値の擬似乱数列として，3項原始多項式を特性多項式とするすべてのm系列は平均として系統的な偏りをもつ．平均としての性質であるから重大な欠陥である．すなわち，引き続く重みw_kとw_{k+1}は相関を持つ．この性質により，3項m系列は統計的に多すぎる0を含む部分列をもち，これら過多の0がTLP列のmost significant bit に直接的に反映することになる．

(ii) 原始3項式で，この偏りを最小にするためには，できるだけ大きいpの値を採用し，qの値をなるべく$p/2$に近づけることである．しかしながら，それに近い実用的な1つの組み合わせ：$p = 1279, q = 418$の場合でも偏りは依然として検出される．

(iii) これを避けるためには，原始t-項式$(t > 3)$を用い，その推移行列の各行のweightが$p/2$になるべく近く，かつ，どの行も3以下でないものを選ぶ必要がある．また，奇数のweightをもつ行の数と偶数のweightをもつ行がほぼ等しいような推移行列を選ぶことも必要であろう．

(iv) size p, weight r のrandom vectorからν個成分を選んだ和(mod 2)が1となる期待値を与える関数$h_p(r, \nu)$の漸化式を求めた．これから，νが$p/2$よりあまり離れていない時には定数関数に近いことがわかる．T_t $(T \geq 5)$の各行のweightが数値として具体的に与えられた場合にp−tupleのweightの平均的推移を与える関数は，これらの和として書ける．この尺度からの最適化をはかることができて，GFSR法のための原始多項式のひとつの選択指針が得られた．これに基づいて最適な5項原始多項式の探索を行い結果を示した(TABLE 4C)．

参考文献

[1] H. S. Bright and R. L. Enison. Quasi-random number sequences from a long-period tlp generator with remarks on application to cryptography. *Comput. Surv*, 11(4):357–370, Dec. 1979.

[2] S. W. Golomb. *Shift Register Sequences, revised ed.* Aegean Park Press, Laguna Hills, Calif., 1982.

[3] H. F. Jordan and D. C. M. Wood. On the distribution of sums of successive bits of shift-register sequences. *IEEE Trans. Comput.*, C-22(4):400–408, Apr. 1973.

[4] D. E. Knuth. *The Art of Computer Programing, Vol.1, Fundamental Algorithms.* Addison-Wesley, Reading, Massachusetts, 1976.

[5] Y. Kurita and M. Matsumoto. Primitive t-nomials (t=3,5) over gf(2) whose degree is a mersenne exponent $\leq$ 44 497. *Math. Comput.*, 56(194):817–821, Apr. 1991.

[6] T.G. Lewis and W.H. Payne. Generalized feedback shift register pseudorandom number algolithms. *J. ACM*, 20(3):456–468, Mar 1973.

[7] N. Zierler. Primitive trinomials whose degree is a mersenne exponent. *Inform. Contr.*, 15:67–69, 1969.