Nonlinear Feedback Shift Registers With Maximal Period

Oleksandr Kazymyrov

Selmer Center, Department of Informatics,
University of Bergen, Norway
Oleksandr.Kazymyrov@uib.no

Spring 2013

Outline

Basic Definitions

Let S be the set of functions in $\mathbb{F}[x_1, \ldots, x_n] / < x_1^2 + x_1, \ldots, x_n^2 + x_n >$.

Let L be the subset of all linear polynomials in S.

A given $f(x_0, \ldots, x_n) = F(x_0, \ldots, x_{n-1}) + x_n$ in S generates an infinite binary sequence $a = (a(0)a(1)\cdots)$ satisfying

$$f(a(k), a(k+1), \ldots, a(k+n)) = 0, \text{ for } k = 0, 1, 2 \ldots$$

and initial condition on $a(0), \ldots, a(n-1)$

The period of a is denoted by $p(a)$.

The set of all sequences generated by f is denoted by $\Omega(f)$.

Example

$$g = x_0 + x_1 x_2 + x_3$$

$$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$$
$$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$$
$$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$$

g	$x_0x_1x_2$
	011

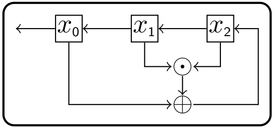

Figure : An example of NFSR

Example

$$\boldsymbol{g = x_0 + x_1 x_2 + x_3}$$

$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$

$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$

$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$

g	$x_0x_1x_2$
0	011
	11

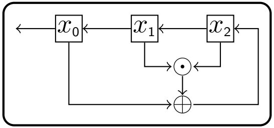

Figure : An example of NFSR

Example

$$\boldsymbol{g = x_0 + x_1 x_2 + x_3}$$

$$a_1 = \color{blue}{000}\ 000\ldots = (0) \qquad (p(a_1) = 1)$$
$$a_2 = \color{blue}{001}\ 001\ldots = (001) \qquad (p(a_2) = 3)$$
$$a_3 = \color{blue}{0111}\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$$

g	$x_0x_1x_2$
0	011
	111

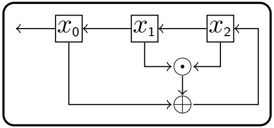

Figure : An example of NFSR

Example

$$g = x_0 + x_1 x_2 + x_3$$

$$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$$
$$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$$
$$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$$

g	$x_0x_1x_2$
0	011
1	111
	11

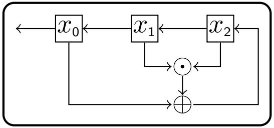

Figure : An example of NFSR

Example

$$g = x_0 + x_1 x_2 + x_3$$

$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$

$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$

$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$

g	$x_0x_1x_2$
0	011
1	111
	110

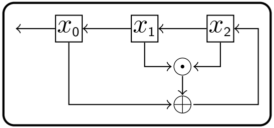

Figure : An example of NFSR

Example

$$g = x_0 + x_1 x_2 + x_3$$

$a_1 = 000\ 000 \ldots = (0) \qquad (p(a_1) = 1)$

$a_2 = 001\ 001 \ldots = (001) \qquad (p(a_2) = 3)$

$a_3 = 0111\ 0111 \ldots = (0011) \qquad (p(a_3) = 4)$

g	$x_0 x_1 x_2$
0	011
1	111
1	110
	10

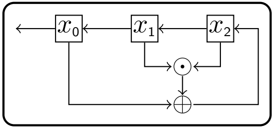

Figure : An example of NFSR

Example

$$\boldsymbol{g = x_0 + x_1 x_2 + x_3}$$

$$a_1 = 000\;000\ldots = (0) \qquad (p(a_1) = 1)$$
$$a_2 = 001\;001\ldots = (001) \qquad (p(a_2) = 3)$$
$$a_3 = 0111\;0111\ldots = (0011) \qquad (p(a_3) = 4)$$

g	$x_0x_1x_2$
0	011
1	111
1	110
	101

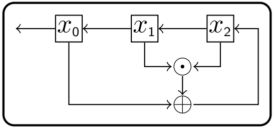

Figure : An example of NFSR

Example

$$\boldsymbol{g = x_0 + x_1 x_2 + x_3}$$

$$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$$
$$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$$
$$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$$

g	$x_0x_1x_2$
0	011
1	111
1	110
1	101
	01

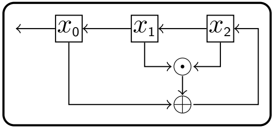

Figure : An example of NFSR

Example

$$g = x_0 + x_1 x_2 + x_3$$

$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$

$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$

$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$

g	$x_0 x_1 x_2$
0	011
1	111
1	110
1	101
	011

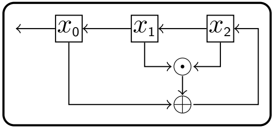

Figure : An example of NFSR

Example

$$\boldsymbol{g = x_0 + x_1x_2 + x_3}$$

$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$

$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$

$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$

g	$x_0x_1x_2$
0	011
1	111
1	110
1	101
0	011

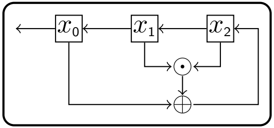

Figure : An example of NFSR

Example

$$g = x_0 + x_1 x_2 + x_3$$

$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$

$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$

$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$

g	$x_0x_1x_2$
0	011
1	111
1	110
1	101
0	011

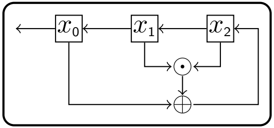

Figure : An example of NFSR

$$\boldsymbol{g = x_0 + x_1 x_2 + x_3}$$

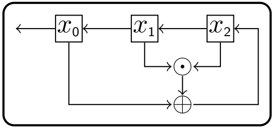

Figure : An example of NFSR

$a_1 = 000\ 000\ldots = (0) \qquad (p(a_1) = 1)$

$a_2 = 001\ 001\ldots = (001) \qquad (p(a_2) = 3)$

$a_3 = 0111\ 0111\ldots = (0011) \qquad (p(a_3) = 4)$

g	$x_0x_1x_2$
0	011
1	111
1	110
1	101
0	011

g	$x_0x_1x_2$
0	001
0	010
1	100
0	001

$$\Omega(g) = \{a_1, a_2, a_3\}$$

Basic Definitions

The sequence is called M-sequence if the period equals 2^n.

f generates a periodic sequence iff f is nonsingular

$$f(x_0, \ldots, x_n) = x_0 + F(x_1, \ldots, x_{n-1}) + x_n.$$

If F is linear then f is also linear of the form

$$f(x_0, \ldots, x_n) = x_0 + c_1 x_1 + \ldots + c_{n-1} x_{n-1} + x_n.$$

Outline

Nonlinear Product And Representation

Suppose $g(x_0, \ldots, x_m)$ and $f(x_0, \ldots, x_n)$ are polynomials in S. Then the composition $g \circ f$ is presented as

$$g \circ f = g(f(x_0, \ldots, x_n), f(x_1, \ldots, x_{n+1}), \ldots, f(x_m, \ldots, x_{n+m})).$$

- Note that $g \circ f \neq f \circ g$ in general.
- The composition $g \circ f$ corresponds to cascade connection of the shift register of g to that of f.

Operations With Composition

Three operations: addition $(+)$, multiplication $(\cdot)$ and composition $(\circ)$.

$$(x_i) + (x_j) = (x_i + x_j)$$
$$(x_i) \cdot (x_j) = (x_i)(x_j) = (x_i x_j)$$
$$(x_i) \circ (x_j) = (x_{j+i})$$

Two special cases

$$(x_i) \circ (x_i) = (x_{2i})$$
$$(x_i)(x_i) = (x_i)$$

Distributive properties

$$(x_i) \circ (x_j + x_k) = x_{j+i} + x_{i+k}$$
$$(x_i)(x_j + x_k) = x_i x_j + x_i x_k$$
$$(x_i + x_j) \circ (x_k + x_p) = x_{i+k} + x_{i+p} + x_{k+j} + x_{p+j}$$

Operations With Composition

Nontrivial cases

$$(x_i) \circ (x_j x_k) = x_{i+j} x_{i+k}$$
$$(x_j x_k) \circ (x_i) = x_{i+j} x_{i+k}$$
$$(x_i + x_j) \circ (x_k x_p) = x_{i+k} x_{i+p} + x_{j+k} x_{j+p}$$

$$\begin{aligned}(x_k x_p) \circ (x_i + x_j) &= (x_{k+i} + x_{k+j})(x_{i+p} + x_{j+p}) = \\ &= x_{k+i} x_{i+p} + x_{k+i} x_{j+p} + x_{k+j} x_{i+p} + x_{k+j} x_{j+p}\end{aligned}$$

Example

$$g = x_0 + x_1x_2 + x_3$$
$$f = x_0 + x_1$$

$$\begin{aligned} g \circ f &= (x_0 + x_1x_2 + x_3) \circ (x_0 + x_1) = \\ &= x_0 + x_1 + (x_1 + x_2)(x_2 + x_3) + x_3 + x_4 = \\ &= x_0 + x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_4 \end{aligned}$$

$$\begin{aligned} f \circ g &= (x_0 + x_1) \circ (x_0 + x_1x_2 + x_3) = \\ &= x_0 + x_1x_2 + x_3 + x_1 + x_2x_3 + x_4 \end{aligned}$$

Periods of Polynomials in S

Shift Operator

Shift operator $\delta^i : S \mapsto S$ is defined by

$$\delta^i f(x_0, \ldots, x_n) = f(x_i, \ldots, x_{n+i})$$

For $\alpha_i, f \in S$ the polynomial $\sum \alpha_i(\delta^i f)$ is denoted by $P(\delta)f$, where $P(\delta) = \sum \alpha_i \delta^i$.

Order of f

By the order of f, denoted by $ord(f)$, means the highest subscript i for which x_i occurs in f. For $f = 0$ or $f = 1$ the $ord(f)$ equals -1.

Periods of Polynomials in S

Lemma 1. Division Algorithm

Let $g(x_0, \dots, x_m) \in S$ and $f(x_0, \dots, x_n) = F(x_0, \dots, x_{n-1}) + x_n \in S$; then there exists unique $P(\delta) = \sum_{i=0}^{m-n} \alpha_i \delta^i$ with $\alpha_i \in S$, $ord(\alpha_i) < n + i$ and unique $r \in S$ with $r = 0$ or $ord(r) < n$ such that $g = P(\delta) f + r$.

Note: if $m < n$ then $P(\delta) = 0$.

Let $g(x_0, \dots, x_m) \in S$ and $f(x_0, \dots, x_n) = F(x_0, \dots, x_{n-1}) + x_n$ be arbitrary functions in S, then

$$g = \sum_{i=0}^{m-n} \alpha_i (\delta^i f) + r.$$

Periods of Polynomials in S

If $r = 0$ then $g = P(\delta)f$ and defined by $f||g$.

- If $f||g$ and $g||h$ then $f||h$.
- If $f||g$ then $n = ord(f) \leq ord(g) = m$.
- If $g = h \circ f$ then $f||g$. The converse is always true for $f, g \in L$.

Theorem 1

Let $f = F(x_0, \ldots, x_{n-1}) + x_n \in S$ and $g = G(x_0, \ldots, x_{m-1}) + x_m \in S$; then $f||g$ if and only if $\Omega(f) \subset \Omega(g)$.

Let L_f be linear polynomial in S of smallest order such that $f \mid\mid L_f$.

Theorem 2

Let f be a nonsingular linear polynomial and
$g = x_0 + G(x_1, \ldots, x_{m-1}) + x_m \in S$; then $L_{g \circ f} = L_g \circ L_f$.

Periods of Polynomials in S

Theorem 3

Let $f = F(x_0, \ldots, x_{n-1}) + x_n \in S$; then there exist a positive integer t such that $f || x_0 + x_t$.

Corollary 1

Let $f = x_0 + F(x_1, \ldots, x_{n-1}) + x_n \in S$; then $p(f) = LCM\{p(a) | a \in \Omega(f)\}$.

Corollary 2

Let $f = x_0 + F(x_1, \ldots, x_{n-1}) + x_n \in S$; then f generates M-sequence if and only if $p(f) = 2^n$.

Extra Notations

If a is $\Omega(f)$, then its i-fold translate

$$\rho^i(a) = (a(i)a(i+1)\cdots),$$

is also in $\Omega(f)$ for $0 \leq i \leq p(a) - 1$.

Let P be the set of all periodic sequences. For $f \in S$

$$\theta(f) : P \mapsto P$$
$$\theta(f)(a) = b$$
$$b(k) = f(a(k), a(k+1), \ldots, a(k+n))$$

for $k = 0, 1, 2, \ldots$

Cycle Structure of $\Omega(g \circ f)$

Theorem 4

Suppose $f = x_0 + F(x+1, \ldots, x_{n-1}) + x_n$ and $g = x_0 + G(x_1, \ldots, x_{m-1}) + x_m$ are in S, and suppose $\Omega(g)$ consists of E cycles. Let a_j $(j = 1, \ldots, E)$ be sequences, one from each cycle in $\Omega(g)$, and let C_j be defined by

$$C_j = \cup\{\theta(f)^{-1}(\rho^i(a_j)) | i = 0, 1, \ldots, p(a_j) - 1\}$$

then

- $\Omega(g \circ f) = \cup\{C_j | 1 \leq j \leq E\}$
- $|C_j| = 2^n p(a_j)$
- C_j is closed under ρ, i.e. $\rho(C_j) = C_j$
- if $b \in C_j$, then $p(a_j) | p(b)$

Cycle Structure of $\Omega(g \circ f)$

h
a_1
a_2
$\vdots$
a_E

Figure : The Function $\theta(f)$

Cycle Structure of $\Omega(g \circ f)$

h		
a_1	$\overset{\theta(f)}{\mapsto}$	b_1
a_2	$\overset{\theta(f)}{\mapsto}$	b_2
$\vdots$	$\vdots$	$\vdots$
a_E	$\overset{\theta(f)}{\mapsto}$	b_E

Figure : The Function $\theta(f)$

Cycle Structure of $\Omega(g \circ f)$

h		$h^{'}$
a_1	$\overset{\theta(f)}{\mapsto}$	b_1
a_2	$\overset{\theta(f)}{\mapsto}$	b_2
$\vdots$	$\vdots$	$\vdots$
a_E	$\overset{\theta(f)}{\mapsto}$	b_E

Figure : The Function $\theta(f)$

Cycle Structure of $\Omega(g \circ f)$

h		h'
a_1	$\overset{\theta(f)}{\mapsto}$	b_1
a_2	$\overset{\theta(f)}{\mapsto}$	b_2
$\vdots$	$\vdots$	$\vdots$
a_E	$\overset{\theta(f)}{\mapsto}$	b_E

Figure : The Function $\theta(f)$

g
a_1
a_2
$\vdots$
a_E

Figure : Description of Theorem 4

Cycle Structure of $\Omega(g \circ f)$

h		h'
a_1	$\overset{\theta(f)}{\mapsto}$	b_1
a_2	$\overset{\theta(f)}{\mapsto}$	b_2
$\vdots$	$\vdots$	$\vdots$
a_E	$\overset{\theta(f)}{\mapsto}$	b_E

Figure : The Function $\theta(f)$

g
$\rho^i(a_1)$
$\rho^i(a_2)$
$\vdots$
$\rho^i(a_E)$

Figure : Description of Theorem 4

Cycle Structure of $\Omega(g \circ f)$

h		h'
a_1	$\overset{\theta(f)}{\mapsto}$	b_1
a_2	$\overset{\theta(f)}{\mapsto}$	b_2
$\vdots$	$\vdots$	$\vdots$
a_E	$\overset{\theta(f)}{\mapsto}$	b_E

Figure : The Function $\theta(f)$

g		
$\rho^i(a_1)$	$\overset{\theta(f)^{-1}}{\mapsto}$	$C_1 = \{b_1^1, \dots, b_{2^n p(a_1)}^1\}$
$\rho^i(a_2)$	$\overset{\theta(f)^{-1}}{\mapsto}$	$C_2 = \{b_1^2, \dots, b_{2^n p(a_2)}^2\}$
$\vdots$	$\vdots$	$\vdots$
$\rho^i(a_E)$	$\overset{\theta(f)^{-1}}{\mapsto}$	$C_E = \{b_1^E, \dots, b_{2^n p(a_E)}^E\}$

Figure : Description of Theorem 4

Cycle Structure of $\Omega(g \circ f)$

h		$h^{'}$
a_1	$\overset{\theta(f)}{\mapsto}$	b_1
a_2	$\overset{\theta(f)}{\mapsto}$	b_2
$\vdots$	$\vdots$	$\vdots$
a_E	$\overset{\theta(f)}{\mapsto}$	b_E

Figure : The Function $\theta(f)$

g		$g \circ f$
$\rho^i(a_1)$	$\overset{\theta(f)^{-1}}{\mapsto}$	$C_1 = \{b_1^1, \dots, b_{2^n p(a_1)}^1\}$
$\rho^i(a_2)$	$\overset{\theta(f)^{-1}}{\mapsto}$	$C_2 = \{b_1^2, \dots, b_{2^n p(a_2)}^2\}$
$\vdots$	$\vdots$	$\vdots$
$\rho^i(a_E)$	$\overset{\theta(f)^{-1}}{\mapsto}$	$C_E = \{b_1^E, \dots, b_{2^n p(a_E)}^E\}$

Figure : Description of Theorem 4

Example

$$
\begin{aligned}
g(x_0, x_1, x_2, x_3) &= x_0 + x_1x_2 + x_3 \\
f(x_0, x_1) &= x_0 + x_1 \\
h(x_0, \ldots, x_4) &= g \circ f = x_0 + x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_4
\end{aligned}
$$

$\Omega(g)$ consist of the following cycles

$$
\begin{array}{ll}
(0) & p(a_1) = 1 \\
(001) & p(a_2) = 3 \\
(0111) & p(a_3) = 4
\end{array}
$$

$\Omega(h)$ consist of the cycles

$$
\begin{array}{ll}
(0)(1) & C_1 \\
(000111) & C_2 \\
(00101101) & C_3
\end{array}
$$

Periods of Polynomials in S

Theorem 5

Let f be an irreducible linear polynomial and $g = x_0 + G(x_1, \ldots, x_{m-1}) + x_m \in S$, $a \in \Omega(g)$.

- If $p(f) \nmid p(a)$, then $\theta(f)^{-1}(a)$ contains one sequence of period $p(a)$ and $2^n - 1$ sequences of period equal to LCM{p(a),p(f)}.
- If $p(f) \mid p(a)$, then for $x \in \theta(f)^{-1}(a)$

$$p(x) = \begin{cases} p(a), & \text{if } f \mid\mid l(x) \\ 2p(a), & \text{otherwise} \end{cases}$$

where $l(x) = a(p(a)-1)x_0 + a(p(a)-2)x_1 + \cdots + a(0)x_{p(a)-1}$.

Outline

Example 1. Lempel (1970)

The polynomial $t_1 \ldots t_n$ where $t_i = x_i$ if $b_i = 1$ and $t_i = x_i + 1$ if $b_i = 0$ is defined by $X(n; b_1, \ldots, b_n)$.

Theorem 6

Let $g = x_0 + G(x_1, \ldots, x_{n-1}) + x_n$ in S with $n \geq 2$, which generates M-sequence (of period 2^n), and let $f = x_0 + x_1$. Then both

$$h_1 = (g \circ f) + X(n; 1, 0, 1, 0, \ldots), h_2 = (g \circ f) + X(n; 0, 1, 0, 1, \ldots),$$

generate M-sequences of period 2^{n+1}.

Corollary

Since $g(x_0, x_1, x_2) = 1 + (x_0 + x_1) \circ (x_0 + x_1)$ generates M-sequence of period 2^2, then the following polynomial generates M-sequence of period 2^n $(n \geq 2)$

$$\begin{aligned} h(x_0, \ldots, x_n) = 1 + (x_0 + x_1)^2 + k(2) \circ (x_0 + x_1)^{n-3} + \cdots \\ + k(n-2) \circ (x_0 + x_1) + k(n-1), \end{aligned}$$

where $k(j) = X(j; 1, 0, 1, 0, \ldots)$ or $X(j; 0, 1, 0, 1, \ldots)$ $(j = 2, \ldots, n-1)$ and

$$(x_0 + x_1)^n = \underbrace{(x_0 + x_1) \circ (x_0 + x_1) \circ \cdots \circ (x_0 + x_1)}_{n \text{ times}}.$$

Example 1. Calculations

Let $n = 4, k(2) = X(2;1,0), k(3) = X(3;0,1,0)$; then

$$\begin{aligned} f &= 1 + (x_0 + x_1)^4 + k(2) \circ (x_0 + x_1)^1 + k(3) = \\ &= 1 + (x_0 + x_4) + (x_1x_2 + x_1x_3 + x_2 + x_2x_3 + x_1 + x_2) + \\ &+ (x_1x_2x_3 + x_1x_2 + x_3x_2 + x_2) = \\ &= 1 + x_0 + x_1 + x_2 + x_4 + x_1x_3 + x_1x_2x_3 \end{aligned}$$

f generates M-sequence (0000110101111001).

Example 2. Mykkeltveit and et al. (1979)

Theorem 7

Let $h = x_0 + c_1 x_1 + \cdots + c_{n-1} x_{n-1} + x_n$ be a primitive polynomial and $g = h + X(n-1; 0, 0, \ldots)$; then

$$[g \circ (x_0 + x_1)] + X(n; a_1, \ldots, a_n),$$

where $(a_1, \ldots, a_n) \in \mathbb{F}_2^n \;\; (0, 0, \ldots, 0), (1, 1, \ldots, 1)$ generates M-sequences of period 2^{n+1}.

Example 2. Calculations

Let $h = x_0 + x_1 + x_3$ and $(a_1, a_2, a_3) = (1, 1, 0)$; then

$$
\begin{aligned}
g &= h + (x_1 + 1)(x_2 + 1) = x_0 + x_1 + x_3 + x_1x_2 + x_1 + x_2 + 1 = \\
&= 1 + x_0 + x_2 + x_1x_2 + x_3 \\
g \circ (x_0 + x_1) &= 1 + x_0 + x_1 + x_2 + x_3 + (x_1 + x_2)(x_2 + x_3) + x_3 + x_4 = \\
&= 1 + x_0 + x_1 + x_2 + (x_1x_2 + x_1x_3 + x_2 + x_2x_3) + x_4 = \\
&= 1 + x_0 + x_1 + x_1x_2 + x_1x_3 + x_2x_3 + x_4 \\
f &= [g \circ (x_0 + x_1)] + x_1x_2x_3 + x_1x_2 = \\
&= 1 + x_0 + x_1 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4
\end{aligned}
$$

M-sequence is (0000110010111101).

References

D.H. Green, K.R. Dimond, "Nonlinear product-feedback shift registers," Electrical Engineers, Proceedings of the Institution of , vol.117, no.4, pp.681-686, April 1970.

D.H. Green, R.G. Kelsch, "Some polynomial compositions of nonlinear feedback shift registers and their sequence-domain consequences," Electrical Engineers, Proceedings of the Institution of , vol.117, no.9, pp.1750-1756, September 1970.

Johannes Mykkeltveit, Man-Keung Siu, Po Tong, On the cycle structure of some nonlinear shift register sequences, Information and Control, Volume 43, Issue 2, November 1979, Pages 202-215.