ELSEVIER

Discrete Mathematics 219 (2000) 187–194

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

a finite alphabet

Max Landsberg

Emster Str. 74c, D-58093 Hagen, Germany

Received 4 February 1999; accepted 4 October 1999

Abstract

In this note, first there are established simple formulas enabling the calculation of feedback functions that generate a cycle of given length over a given finite field. A theorem communicated in the appendix says that feedback functions producing cycles over a finite field can also be utilized for constructing general feedback functions yielding cycles (in particular, de Bruijn cycles) over an arbitrarily given finite alphabet. © 2000 Elsevier Science B.V. All rights reserved.

Keywords: Feedback function; Shift register sequence; De Bruijn sequence

For the design of a shift register that is to produce a cycle of given length, the determination of a feedback function generating a cycle of the desired length is of some significance. While there are numerous papers on cycles — in particular, on de Bruijn cycles — (see the list of references in [1,2]) only little is known about the calculation of feedback functions that generate such cycles. For the binary case, some investigations have been carried out (see, e.g., [2,3,5]).

In this note, first general formulas are given which enable feedback functions generating cycles of any given length (over a given finite field) to be calculated in a particular simple way. The expressions obtained have an especially simple structure for feedback functions yielding de Bruijn cycles (thus also de Bruijn sequences).

Let E be a (nonempty) finite set and let $\mathsf{M}^n(E)$ denote the set of all words of length n over the alphabet E. The first letter of a word $W \in \mathsf{M}^n(E)$ is denoted by $u(W)$. Two words $V = a_1a_2\dots a_n$, $W = b_1b_2\dots b_n \in \mathsf{M}^n(E)$ are said to be *conjugate* if and only if $a_j = b_j$ $(j = 2, 3, \dots, n)$ and $a_1 \neq b_1$. Let $V = a_1a_2\dots a_n$, $W = b_1b_2\dots b_n \in \mathsf{M}^n(E)$. The fundamental shift relation $V \to W$ is defined by

$$V \to W \quad :\Leftrightarrow \quad a_2a_3\dots a_n = b_1b_2\dots b_{n-1}.$$

A sequence $C = V_1, V_2, \dots, V_k$ of words from $\mathsf{M}^n(E)$ is called a *k-cycle* (cycle of length k) *in* $\mathsf{M}^n(E)$ (or, alternatively, a *k-cycle of order n over E*), iff the V_j are pairwise

0012-365X/00/$ - see front matter © 2000 Elsevier Science B.V. All rights reserved.
PII: S0012-365X(99)00375-1

distinct and the relations $V_k \to V_1$, $V_j \to V_{j+1}$ $(j=1,2,\dots,k-1)$ hold. Cycles C, C' in $\mathsf{M}^n(E)$ are said to be *adjacent* iff they are disjoint and there are words $V \in C$, $W \in C'$ that are conjugate. A cycle $V_1, V_2, \dots, V_N$ in $\mathsf{M}^n(E)$, where $N=(\text{card } E)^n$, is called a *de Bruijn cycle*, the "corresponding ring sequence" $u(V_1), u(V_2), \dots, u(V_N)$ is called a *de Bruijn sequence*. Because of their interesting properties and numerous applications, de Bruijn sequences have been exhaustively investigated; in particular, there are remarkable algorithms for generating such sequences (see Fredricksen's [1] comprehensive report). A mapping from $\mathsf{M}^n(E)$ into E is called a *feedback function in* $\mathsf{M}^n(E)$. Let f be a feedback function in $\mathsf{M}^n(E)$ and assign to each word $a_1a_2\dots a_n \in \mathsf{M}^n(E)$ the word $a_2a_3\dots a_n f(a_1,a_2,\dots,a_n)$ to obtain a mapping F from $\mathsf{M}^n(E)$ into $\mathsf{M}^n(E)$. The function f is said to be nonsingular iff F is injective. In what follows, we assume that all feedback functions to be considered are nonsingular. Then, for every initial word $V \in \mathsf{M}^n(E)$, there is a k such that $C = V, F(V), F^2(V), \dots, F^{k-1}(V)$ is a cycle. The cycle C and the corresponding ring sequence $u(V), u(F(V)), u(F^2(V)), \dots, u(F^{k-1}(V))$ are said to be *generated* by f.

The important operations of splitting a cycle into two cycles, and of joining two cycles to form a single cycle, have efficiently been utilized for a long time already. Properties of certain feedback functions reflected in these operations are described in Lemmas 1 and 2 (for the binary case, see, e.g., [3,5]). These propositions are verified using the well-known fact that $a \in GF(q)$ $(q = p^m$ where p is a prime) and $a \neq 0$ imply $a^{q-1} = 1$. In what follows, let $\mathsf{M}^n_q := \mathsf{M}^n(GF(q))$.

Lemma 1. *Let f be a feedback function in M^n_q that generates a cycle C_1 of length L_1 and a cycle C_2 of length L_2 such that C_1 and C_2 are adjacent, implying that there is a word $W = Aa_1a_2\dots a_{n-1}$ in C_1 and a word $V = Ba_1a_2\dots a_{n-1}$ in C_2. Let $P = f(A,a_1,a_2,\dots,a_{n-1})$, $Q = f(B,a_1,a_2,\dots,a_{n-1})$. Then the function f_0 defined by*

$$f_0(x_1,x_2,\dots,x_n) = f(x_1,x_2,\dots,x_n) + (P-Q)((x_1-A)^{q-1} - (x_1-B)^{q-1}) \times \prod_{j=2}^{n}(1-(x_j-a_{j-1})^{q-1}) \qquad (*)$$

is a feedback function in M^n_q which amalgamates cycles C_1, C_2 into a single cycle of length L_1+L_2. Those cycles of f that are distinct from C_1, C_2 are not changed by f_0 (thus f_0 is nonsingular).

Lemma 2. *Let f be a feedback function in M^n_q generating the cycle $C=W_1,W_2,\dots,W_N$. Assume that there are a $j \in \{1,2,\dots,N\}$ and a k satisfying $1 \leqslant k \leqslant N-1$ such that W_j and W_{j+k} are conjugate. Let $W_j = Aa_1a_2\dots a_{n-1}$, $W_{j+k} = Ba_1a_2\dots a_{n-1}$; set $P = f(A,a_1,a_2,\dots,a_{n-1})$, $Q = f(B,a_1,a_2,\dots,a_{n-1})$. Then the function f_0 from formula $(*)$ (Lemma 1) is a feedback function in M^n_q generating the cycle $C_1 = W_{j+1}, W_{j+2}, \dots, W_{j+k}$ determined by the pair W_j, W_{j+k} (subscripts to be reduced mod N). For the initial word W_j, the function f_0 yields a cycle C_2 of length $N-k$. Cycles C_1, C_2 are adjacent, their amalgamation is the cycle C. Those cycles of f that are distinct from C are not changed by f_0 (thus f_0 is nonsingular).*

Definition. Let $C = W_1, W_2, \dots, W_k$ be a cycle in M_q^n and assume that, for some r and s satisfying $r \in \{1, 2, \dots, k\}$ and $0 \leqslant s \leqslant k-1$, $C' = W_r, W_{r+1}, \dots, W_{r+s}$ is also a cycle. Then C' is called a *subcycle of C*.

A feedback function f in M_q^n is called *linear* iff $f(x_1, x_2, \dots, x_n) = A_1x_1 + A_2x_2 + \cdots + A_nx_n$ with some coefficients A_j from GF(q).

Lemma 3. *Let C be a cycle of length* $q^n - 1$ *in* M_q^n *that can be generated by some linear feedback function. Then, for each k satisfying* $1 \leqslant k \leqslant q^n - 1$, *C has a subcycle of length k.*

The proof of Lemma 3 is omitted since the remarkably brief and constructive proof for the binary case $q = 2$ (see [2]) immediately — mutatis mutandis — extends to arbitrary sets M_q^n (however, see the following remark).

Remark. Let cycle C in Lemma 3 have the form $C = W_1, W_2, \dots, W_N$ where $N = q^n - 1$. Consider the corresponding ring sequence $g = u(W_1), u(W_2), \dots, u(W_N)$ and perform a cyclic permutation such that $-u(W_{k+1})$ occupies the first position ($1 \leqslant k \leqslant q^n - 2$). This operation results in the sequence $h = -u(W_{k+1}), -u(W_{k+2}), \dots, -u(W_{k+N})$, and by elementwise adding g and h we obtain $g + h = u(W_1) - u(W_{k+1}), u(W_2) - u(W_{k+2}), \dots, u(W_N) - u(W_{k+N})$. In this sequence find the first nonzero element — say, $u(W_r) - u(W_{k+r})$ — followed by $n-1$ zeros. Then W_r and W_{k+r} are conjugate and $W_{r+1}, W_{r+2}, \dots, W_{r+k}$ is a cycle of length k. In addition, r is the smallest j such that W_j and W_{k+j} are conjugate. Let this number r be denoted by $m(k)$. Evidently, $m(k)$ can easily be computed (for large values of n or q, there exist simple computer programs, see [2] for the binary case $q = 2$).

Lemmata 1 and 2 imply the following theorem.

Theorem 4. *For given values n and* $q = p^m$ *let*

$$P(X) = X^n + K_{n-1}X^{n-1} + K_{n-2}X^{n-2} + \cdots + K_1X + K_0$$

be a primitive polynomial of degree n with coefficients from GF(q). *This polynomial determines the linear feedback function*

$$L(x_1, x_2, \dots, x_n) = -K_0x_1 - K_1x_2 - \cdots - K_{n-1}x_n$$

in M_q^n. *Given an initial word* $W_1 \neq \underbrace{0\,0\,\dots\,0}_{n}$, *the function L generates a cycle* $C = W_1, W_2, \dots, W_N$ *of length* $N = q^n - 1$. *Then the following propositions hold*:

(a) *If in C the word* $\underbrace{0\,0\,\dots\,0}_{n}$ *is inserted immediately after the word* $1\underbrace{0\,0\,\dots\,0}_{n-1}$

then, obviously, what results is a de Bruijn cycle. This cycle is generated by the feedback function

$$f_0(x_1,x_2,\ldots,x_n)=L(x_1,x_2,\ldots,x_n)+K_0(x_1^{q-1}-(x_1-1)^{q-1})\prod_{j=2}^{n}(1-x_j^{q-1}).$$

(b) *For a given k satisfying* $1\leqslant k\leqslant q^n-2$ *let the words* $W_{m(k)}$ *and* $W_{m(k)+k}$ *in C have the forms*

$$W_{m(k)}=A^{(k)}a_1^{(k)}a_2^{(k)}\ldots a_{n-1}^{(k)},$$

$$W_{m(k)+k}=B^{(k)}a_1^{(k)}a_2^{(k)}\ldots a_{n-1}^{(k)}$$

(see the above remark). *Then* $W_{m(k)+1},W_{m(k)+2},\ldots,W_{m(k)+k}$ *is a cycle of length k generated by the feedback function*

$$f_0(x_1,x_2,\ldots,x_n)=L(x_1,x_2,\ldots,x_n)+K_0(A^{(k)}-B^{(k)})((x_1-B^{(k)})^{q-1}-(x_1-A^{(k)})^{q-1})\prod_{j=2}^{n}(1-(x_j-a_{j-1}^{(k)})^{q-1}).$$

It is plausible that the formulas given in Theorem 4 will reduce to considerably simpler ones for the binary case $q=2$ (in this case, the feedback functions are Boole functions). In particular, the expressions obtained for feedback functions yielding de Bruijn cycles (thus also de Bruijn sequences) are extremely simple. The important case $q=2$ is explicitly treated in the following corollary.

Corollary. *For* $q=2$ *and a given value n let*

$$P(X)=X^n+K_{n-1}X^{n-1}+K_{n-2}X^{n-2}+\cdots+K_1X+1$$

be a primitive polynomial of degree n with coefficients from GF(2). *This polynomial determines the linear feedback function*

$$L(x_1,x_2,\ldots,x_n)=x_1+K_1x_2+K_2x_3+\cdots+K_{n-1}x_n$$

in M_2^n. *Given an initial word* $W_1\neq\underbrace{0\,0\,\ldots\,0}_{n}$, *the function L generates a cycle* $C=W_1,W_2,\ldots,W_N$ *of length* $N=2^n-1$. *Then the following propositions hold*:

(a) *If in C the word* $\underbrace{0\,0\,\ldots\,0}_{n}$ *is inserted immediately after the word* $1\,\underbrace{0\,0\,\ldots\,0}_{n-1}$ *then what results is a de Bruijn cycle. This cycle is generated by the feedback function*

$$f_0(x_1,x_2,\ldots,x_n)=L(x_1,x_2,\ldots,x_n)+\overline{x_2}\,\overline{x_3}\ldots\overline{x_n}$$

(*where* $\bar{0}=1,\ \bar{1}=0$).

(b) *For a given k satisfying* $1\leqslant k\leqslant 2^n-2$ *let the words* $W_{m(k)}$ *and* $W_{m(k)+k}$ *in C have the forms*

$$W_{m(k)}=A^{(k)}a_1^{(k)}a_2^{(k)}\ldots a_{n-1}^{(k)},$$

$$W_{m(k)+k} = B^{(k)} a_1^{(k)} a_2^{(k)} \dots a_{n-1}^{(k)}.$$

Then $W_{m(k)+1}, W_{m(k)+2}, \dots, W_{m(k)+k}$ *is a cycle of length* k *generated by the feedback function*

$$f_0(x_1, x_2, \dots, x_n) = L(x_1, x_2, \dots, x_n) + (\overline{x_2} + a_1^{(k)})(\overline{x_3} + a_2^{(k)}) \dots (\overline{x_n} + a_{n-1}^{(k)}).$$

Example 1. Find in M_3^3 a feedback function that generates a de Bruijn sequence.

For $n = 3$, $q = 3$, the tables in Lidl/Niederreiter [4] give the primitive polynomial $P(X) = X^3 + 2X + 1$ which yields the linear feedback function $L(x_1, x_2, x_3) = 2x_1 + x_2$ in M_3^3. With the initial word 1 1 1 (inserting 0 0 0 after 1 0 0), L determines a de Bruijn cycle with corresponding ring sequence (de Bruijn sequence)

1 1 1 0 0 0 2 0 2 1 2 2 1 0 2 2 2 0 0 1 0 1 2 1 1 2 0

which, according to Theorem 4(a), is generated by the feedback function

$$\begin{aligned} f_0(x_1, x_2, x_3) &= 2x_1 + x_2 + (x_1^2 - (x_1 - 1)^2)(1 - x_2^2)(1 - x_3^2) \\ &= 2 + x_1 + x_2 + x_2^2 + x_3^2 + x_1 x_2^2 + x_1 x_3^2 + 2x_2^2 x_3^2 + 2x_1 x_2^2 x_3^2. \end{aligned}$$

Example 2. Find in M_3^3 a feedback function that yields a ring sequence of length $k = 20$.

As in Example 1, we obtain the linear feedback function $L(x_1, x_2, x_3) = 2x_1 + x_2$. With the initial word $W_1 = 1\ 1\ 1$, L defines a cycle $W_1, W_2, \dots, W_N$ ($N = 3^3 - 1 = 26$) in M_3^3. Using the procedure described in the above remark, it is easy to find $m(20) = 12$, thus $W_{m(20)} = W_{12} = 1\ 0\ 2$, $W_{m(20)+20} = W_{32} = W_6 = 2\ 0\ 2$. With the initial word $W_{m(20)+1} = W_{13} = 0\ 2\ 2$ we find a cycle of length $k = 20$ with corresponding ring sequence

0 2 2 2 0 0 1 0 1 2 1 1 2 0 1 1 1 0 0 2

which, according to Theorem 4(b), is generated by the feedback function

$$\begin{aligned} f_0(x_1, x_2, x_3) &= 2x_1 + x_2 + ((x_1 - 1)^2 - (x_1 - 2)^2)(1 - x_2^2)(1 - (x_3 - 2)^2) \\ &= 2x_1 + x_2 + x_1 x_3^2 + 2x_1 x_3 + 2x_1 x_2^2 x_3^2 + x_1 x_2^2 x_3. \end{aligned}$$

Appendix

A theorem to be quoted (without proof) in this appendix (Theorem 7) says that feedback functions generating cycles over a finite field can be used to construct also feedback functions yielding cycles (in particular, de Bruijn cycles) over an arbitrary given finite alphabet. For the representation of such functions certain 'projections' are of some significance.

For any integer $m \geqslant 2$, set $E_m := \{0, 1, \dots, m - 1\}$ and (more generally than above) $\mathsf{M}_m^n := \mathsf{M}^n(E_m)$. In what follows, z will always denote an integer greater than 1.

We need a simple number-theoretical proposition (the proof of which is omitted).

Lemma 5. *Let $z = q_1 q_2 \ldots q_r$ be the decomposition of z into powers of pairwise distinct primes. Then for every $a \in E_z$ there is precisely one r-tuple $a_1 a_2 \ldots a_r$ with $a_j \in E_{q_j}$ $(j = 1, 2, \ldots, r)$ such that*

$$a = a_1 q_2 q_3 \ldots q_r + a_2 q_3 q_4 \ldots q_r + \cdots + a_{r-1} q_r + a_r.$$

By virtue of Lemma 5, we may set $P_j(a) := a_j$ thus defining the r 'projections' $P_j : E_z \to E_{q_j}$. These mappings can easily be computed, as shown by the following lemma.

Lemma 6. *Let, as in Lemma 5, $z = q_1 q_2 \ldots q_r$ and $a \in E_z$. 'Division with remainders' yields*

$$\begin{aligned} a &= a_1 q_2 q_3 \ldots q_r + b_1 \quad (b_1 < q_2 q_3 \ldots q_r), \\ b_1 &= a_2 q_3 q_4 \ldots q_r + b_2 \quad (b_2 < q_3 q_4 \ldots q_r), \\ &\vdots \\ b_{r-2} &= a_{r-1} q_r + b_{r-1} \quad (b_{r-1} < q_r). \end{aligned}$$

Then $P_j(a) = a_j$ for $j = 1, 2, \ldots, r-1$ and $P_r(a) = b_{r-1}$.

Theorem 7. *Let $z = q_1 q_2 \ldots q_r$ be the decomposition of z into powers of pairwise distinct primes, further let $k_j \in \{1, 2, \ldots, q_j^n\}$ for $j = 1, 2, \ldots, r$ and $k = \mathrm{lcm}(k_1, k_2, \ldots, k_r)$. For $j = 1, 2, \ldots, r$, let f_j denote a feedback function in $\mathsf{M}_{q_j}^n$ generating a cycle C_j of length k_j and let $a_1^{(j)}, a_2^{(j)}, \ldots, a_{k_j}^{(j)}$ be the ring sequence corresponding to C_j.*

Then the function

$$\begin{aligned} F(z_1, z_2, \ldots, z_n) = {} & f_1(P_1(z_1), P_1(z_2), \ldots, P_1(z_n)) q_2 q_3 \ldots q_r \\ & + f_2(P_2(z_1), P_2(z_2), \ldots, P_2(z_n)) q_3 q_4 \ldots q_r + \cdots \\ & + f_{r-1}(P_{r-1}(z_1), P_{r-1}(z_2), \ldots, P_{r-1}(z_n)) q_r \\ & + f_r(P_r(z_1), P_r(z_2), \ldots, P_r(z_n)) \end{aligned} \tag{1}$$

is a feedback function in M_z^n that produces a cycle of length k. The ring sequence $s_1, s_2, \ldots, s_k$ corresponding to this cycle is given by

$$s_j = a_j^{(1)} q_2 q_3 \ldots q_r + a_j^{(2)} q_3 q_4 \ldots q_r + \cdots + a_j^{(r-1)} q_r + a_j^{(r)} \tag{2}$$

for $j = 1, 2, \ldots, k$.

Evidently, also in sets M_z^n that are not derived from a field GF(z) (i.e., if z is not a prime power), feedback functions can be represented by means of a function equation.

Example 3. Let $n = 3$ and $z = 12$; find in M_{12}^3 a feedback function that generates a de Bruijn sequence.

With $z = q_1 q_2$, $q_1 = 2^2$, $q_2 = 3$, first the task reduces to finding in $\mathsf{M}_{2^2}^3$ and in M_3^3 feedback functions that generate de Bruijn sequences. For $\mathsf{M}_{2^2}^3$, the primitive polynomial

$P(X)=X^3+X^2+3X+2$ (with coefficients from GF(2^2)) yields the linear feedback function $L(x_1,x_2,x_3)=2x_1+3x_2+x_3$ which — using the initial word 1 1 1 and inserting 0 0 0 after 1 0 0 — produces the de Bruijn sequence

$$B_1 = 1\ 1\ 1\ 0\ 1\ 3\ 0\ 0\ 1\ \ldots\ 2\ 3\ 2\ 3\ 3\ 2$$

of length $k_1=64$. By Theorem 4, B_1 is generated by

$$f_1(x_1,x_2,x_3)=2x_1+3x_2+x_3+2(x_1^3+(x_1+1)^3)(1+x_2^3)(1+x_3^3). \tag{3}$$

According to Example 1, in M_3^3 the feedback function

$$f_2(x_1,x_2,x_3)=2x_1+x_2+(x_1^2-(x_1-1)^2)(1-x_2^2)(1-x_3^2) \tag{4}$$

generates the de Bruijn sequence

$$B_2 = 1\ 1\ 1\ 0\ 0\ 0\ 2\ 0\ 2\ \ldots\ 1\ 2\ 1\ 1\ 2\ 0$$

of length $k_2=27$. By (2), from sequences B_1, B_2 in M_{12}^3 the de Bruijn sequence

$$B_3 = 4\ 4\ 4\ 0\ 3\ 11\ 0\ 2\ 4\ \ldots\ 7\ \ 11\ 7\ 10\ 11\ 6$$

(consisting of $12^3=1728$ terms) is obtained. According to (1), B_3 is generated by the feedback function

$$F(z_1,z_2,z_3)=3f_1(P_1(z_1),P_1(z_2),P_1(z_3))+f_2(P_2(z_1),P_2(z_2),P_2(z_3)),$$

where f_1, f_2 are given by (3) and (4).

The values of the function F given in formula (1) can easily be computed, e.g., calculate the value $F(9,8,11)$ for the function F of Example 3. From

$$9=P_1(9)q_2+P_2(9)=3\cdot 3+0,$$

$$8=P_1(8)q_2+P_2(8)=2\cdot 3+2,$$

$$11=P_1(11)q_2+P_2(11)=3\cdot 3+2,$$

we obtain $F(9,8,11)=3f_1(3,2,3)+f_2(0,2,2)=11$.

In many cases, a feedback function F in a set M_z^n can be constructed by means of formula (1) from linear feedback functions only. This means that, in these cases, F provides the scheme of a simple circuit consisting of linear shift registers.

Example 4. Let $n=4$ and $z=60$; find a feedback function F in M_{60}^4 that generates a cycle of length $k=280$ (note that M_{60}^4 consists of $60^4=12\,960\,000$ quadruples).

We have $z=q_1q_2q_3$ where $q_1=2^2$, $q_2=3$, $q_3=5$.

Let $Q_1(X)=X^4+X^2+X+1\in F_{2^2}[X]$ (where F_q stands for GF(q)). In $\mathsf{M}_{2^2}^4$, Q_1 generates the linear feedback function $f_1(x_1,x_2,x_3,x_4)=x_1+x_2+x_3$ which, starting from the initial word 2 2 3 3, yields a cycle C_1 of length $k_1=7$ with corresponding ring sequence 2 2 3 3 3 2 3.

Let $Q_2(X)=X^4+X^3+X^2+X+1\in F_3[X]$. In M_3^4, Q_2 generates the linear feedback function $f_2(x_1,x_2,x_3,x_4)=2x_1+2x_2+2x_3+2x_4$ which, with the initial word 1 1 1 1, yields a cycle C_2 of length $k_2=5$ with corresponding ring sequence 1 1 1 1 2.

Eventually, let $Q_3(X)=X^4+1\in F_5[X]$. In M_5^4, Q_3 generates the linear feedback function $f_3(x_1,x_2,x_3,x_4)=4x_1$ which, with the initial word 1 1 1 1, yields a cycle C_3 of length $k_3=8$ with corresponding ring sequence 1 1 1 1 4 4 4 4.

Using the above results we obtain the feedback function

$$\begin{aligned}F(z_1,z_2,z_3,z_4) &= 15f_1(P_1(z_1),P_1(z_2),P_1(z_3),P_1(z_4))\\ &\quad +5f_2(P_2(z_1),P_2(z_2),P_2(z_3),P_2(z_4))\\ &\quad +f_3(P_3(z_1),P_3(z_2),P_3(z_3),P_3(z_4))\\ &= 15(P_1(z_1)+P_1(z_2)+P_1(z_3))\\ &\quad +5(2P_2(z_1)+2P_2(z_2)+2P_2(z_3)+2P_2(z_4))\\ &\quad +4P_3(z_1)\end{aligned}$$

in M_{60}^4 which, with the initial word 36 36 51 51, yields a cycle C of length $k=\operatorname{lcm}(7,5,8)=280$ with corresponding ring sequence

36 36 51 51 59 39 54 … 51 54 54 39 59.

References

[1] H. Fredricksen, A survey of full length nonlinear shift register cycle algorithms, SIAM Rev. 24 (1982) 195–221.

[2] S.W. Golomb, Shift Register Sequences, Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982.

[3] A. Lempel, On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers, IEEE Trans. Comput. C-19 (1970) 1204–1209.

[4] R. Lidl, H. Niederreiter, Introduction to Finite Fields and their Applications Cambridge University Press, Cambridge, 1986.

[5] M. Yoeli, Counting with nonlinear binary feedback shift registers, IEEE Trans.Electronic Comput. EC-12 (1963) 357–361.