Journal of Physics: Conference Series

PAPER • OPEN ACCESS

About the k-error linear complexity over $\mathbb{F}_p$ of sequences of length 2p with optimal three-level autocorrelation

To cite this article: V A Edemskiy 2019 *J. Phys.: Conf. Ser.* **1352** 012011

IOP Conf. Series: Journal of Physics: Conf. Series **1352** (2019) 012011 doi:10.1088/1742-6596/1352/1/012011

About the k-error linear complexity over $\mathbb{F}_\mathrm{p}$ of sequences of length 2p with optimal three-level autocorrelation

V A Edemskiy

Yaroslav-the-Wise Novgorod State University, ul. B. St. Petersburgskaya, 41
173003, Veliky Novgorod, Russia

E-mail: Vladimir.Edemsky@novsu.ru

Abstract. We investigate the k-error linear complexity over $\mathbb{F}_p$ of binary sequences of length $2p$ with optimal three-level autocorrelation. These balanced sequences are constructed from cyclotomic classes of order four using a method presented by Ding et al.

1. Introduction

Autocorrelation is an important measure of pseudo-random sequence for their application in code-division multiple access systems, spread spectrum communication systems, radar systems and so on [1]. An important problem in sequence design is to find sequences with optimal autocorrelation. In their paper, Ding et al. [2] gave several new families of binary sequences of period $2p$ with optimal autocorrelation $\{-2.2\}$.

The linear complexity is another important characteristic of pseudo-random sequence, which is significant for cryptographic applications. It is defined as the length of the shortest linear feedback shift register that can generate the sequence [3]. The linear complexity of above-mention sequences over the finite field of order two was investigated in [4] and in [5] over the finite field $\mathbb{F}_p$ of p elements and other finite fields. However, high linear complexity can not guarantee that the sequence is secure. For example, if changing one or few terms of a sequence can greatly reduce its linear complexity, then the resulting key stream would be cryptographically weak. Ding et al. [6] noticed this problem first in their book, and proposed the weight complexity and the sphere complexity. Stamp and Martin [7] introduced the k-error linear complexity, which is the minimum of the linear complexity and sphere complexity. The k-error linear complexity of a sequence r is defined by $L_k(r) = \min_t L(t)$, where the minimum of the linear complexity $L(t)$ is taken over all N-periodic sequences $t = (t_n)$ over $\mathbb{F}_p$ for which the Hamming distance of the vectors $(r_0, r_1, \dots, r_{N-1})$ and $(t_0, t_1, \dots, t_{N-1})$ is at most k. Complexity measures for sequences over finite fields, such as the linear complexity and the k-error linear complexity, play an important role in cryptology. Sequences that are suitable as keystreams should possess not only a large linear complexity but also the change of a few terms must not cause a significant decrease of the linear complexity.

In this paper we derive the k-error linear complexity of binary sequences of length $2p$ from [2] over $\mathbb{F}_p$. These balanced sequences with optimal three-level autocorrelation are constructed by cyclotomic classes of order four. Earlier, the linear complexity and the k-error linear complexity over $\mathbb{F}_p$ of the Legendre sequences and series of other cyclotomic sequences of length p were investigated in [8, 9].

2. Preliminaries

First, we briefly repeat the basic definitions from [2] and the general information.

Let p be a prime of the form $p \equiv 1(\mathrm{mod}\ 4)$, and let θ be a primitive root modulo p [10]. By definition, put $D_0 = \{\theta^{4s} \bmod p; s = 1, \dots, (p-1)/4\}$ and $D_n = \theta^n D_0, n = 1,2,3$. Then these D_n are cyclotomic classes of order four [10].

The ring of residue classes $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$ under the isomorphism $\phi(a) = (a \bmod 2, a \bmod p)$ [11]. Ding et al. considered balanced binary sequences defined as

$$u_i = \begin{cases} 1, & \text{if } i \bmod 2p \in C, \\ 0, & \text{if } i \bmod 2p \notin C, \end{cases} \tag{1}$$

for $C = \phi^{-1}\big(\{0\} \times (\{0\} \cup D_m \cup D_j) \cup \{1\} \times (D_l \cup D_j)\big)$ where m, j, and l are pairwise distinct integers between 0 and 3 [2]. Here we regard them as sequences over the finite field $\mathbb{F}_p$.

By [2], if $\{u_i\}$ has an optimal autocorrelation value then $p \equiv 5 \ (\mathrm{mod}\ 8)$ and $p = 1 + 4y^2$, $(m, j, l) = (0,1,2), (0,3,2), (1,0,3), (1,2,3)$ or $p = x^2 + 4, y = -1$, $(m, j, l) = (0,1,3), (0,2,3)$, $(1,2,0), (1,3,0)$. Here x, y are integers and $x \equiv 1(\mathrm{mod}\ 4)$.

It is well known [12] that if r is a binary sequence with period N, then the linear complexity $L(r)$ of this sequence is defined by

$$L(r) = N - \deg(\gcd(x^N - 1, S_r(x))),$$

where $S_r(x) = r_0 + r_1 x + \ldots + r_{N-1} x^{N-1}$. Let's assume we investigate the linear complexity of u over $\mathbb{F}_p$ and with a period $2p$. So,

$$L(u) = 2p - \deg(\gcd((x^2-1)^p, S_u(x))).$$

The weight of $f(x)$, denoted as $w(f)$, is defined as the number of nonzero coefficients of $f(x)$. From our definitions it follows that if the Hamming distance of the vectors $(u_0, u_1, \dots, u_{2p-1})$ and $(t_0, t_1, \dots, t_{2p-1})$ is at most k then there exists $f(x) \in \mathbb{F}_p$, $w(f) \le k$ such that $S_t(x) = S_u(x) + f(x)$ and the reverse is also true. Therefore

$$L_k(u) = 2p - \max_{f(x)}(m_0 + m_1) \tag{2}$$

where $0 \le m_j \le p$, $S_u(x) + f(x) \equiv 0(\mathrm{mod}(x-1)^{m_0}(x+1)^{m_1})$ and $f(x) \in \mathbb{F}_p[x], w(f) \le k$.

Let g be an odd number in the pair $\theta, \theta + p$, then g is a primitive root modulo $2p$ [11]. By definition, put $H_0 = \{g^{4s} \bmod 2p; s = 1, \dots, (p-1)/4\}$. Denote by H_n a set $g^n H_0, n = 1,2,3$. Let us introduce the auxiliary polynomial $S_n(x) = \sum_{i \in H_n} x^i$. The following formula was proved in [5].

$$S_u(x) \equiv (x^p + 1) S_j(x) + x^p S_m(x) + S_l(x) + 1\big(\mathrm{mod}\ (x^{2p} - 1)\big). \tag{3}$$

By (3) we have

$$\begin{cases} S_u(x) \equiv 2S_j(x) + S_m(x) + S_l(x) + 1(\mathrm{mod}\ (x-1)^p), \\ S_u(x) \equiv S_l(x) - S_m(x) + 1(\mathrm{mod}\ (x+1)^p). \end{cases} \tag{4}$$

Let the sequences $\{q_i\}$ and $\{v_i\}$ be defined by

$$q_i = \begin{cases} 2, \text{if } i \bmod p \in D_j, \\ 1, \text{if } i \bmod p \in \{0\} \cup D_m \cup D_l, \\ 0, \text{otherwise}, \end{cases} \text{ and } v_i = \begin{cases} 2, \text{if } i \bmod p \in \{0\} \cup D_m, \\ 1, \text{ if } i \bmod p \in D_l, \\ 0, \text{ otherwise}. \end{cases} \tag{5}$$

By definition, put $S_q(x) = \sum_{i=0}^{p-1} q_i x^i$ and $S_v(x) = \sum_{i=0}^{p-1} v_i x^i$. Then by the choice of g we obtain that

$$\begin{cases} 2S_j(x) + S_m(x) + S_l(x) + 1 \equiv S_q(x)(\mathrm{mod}(x-1)^p), \\ S_m(x) - S_l(x) + 1 \equiv S_v(x)(\mathrm{mod}(x-1)^p). \end{cases} \tag{6}$$

As noted above, the k-error linear complexity of cyclotomic sequences was investigated in [9]. With the aid of methods from [9] it is an easy matter to prove the following

$$L_k(q) = \begin{cases} \frac{3(p-1)}{4} + 1, \text{if } 0 \le k \le \frac{p-1}{4}, \\ \frac{(p-1)}{2} + 1, \text{if } \frac{p-1}{4} + 1 \le k < \frac{p-1}{3}, \\ 1, \quad \text{if } k = \frac{p-1}{2}, \end{cases} \tag{7}$$

and $(p-1)/4 + 1 \le L_k(q) \le (p-1)/2 + 1$ if $(p-1)/3 \le k < (p-1)/2$.

$$L_k(v) = \begin{cases} p, \quad \text{if } k = 0, \\ \frac{3(p-1)}{4} + 1, \text{if } 1 \le k < \frac{p-1}{4}, \\ \frac{p-1}{2} + 1, \ \text{if } \frac{(p-1)}{4} + 1 \le k < \frac{p-1}{3}, \\ 0, \quad \text{if } k \ge \frac{p-1}{2} + 1. \end{cases} \tag{8}$$

and $9(p-1)/16 \le L_{(p-1)/4}(v) \le 3(p-1)/4 + 1$, $(p-1)/4 \le L_k(v) \le (p-1)/2$ if $(p-1)/3 \le k < (p-1)/2$.

The following statements we also obtain by [9] or by Lemma 3 from [5].

Lemma 1.

1. $S_n(x) = -1/4 + (x-1)^{(p-1)/4} E_n(x)$ and $E_n(1) \ne 0, n = 0,1,2,3$;
2. $S_n(x) = -1/4 + (x+1)^{(p-1)/4} F_n(x)$ and $F_n(-1) \ne 0, n = 0,1,2,3$;
3. Let $S_l(x) + S_m(x) + g(x) \equiv 0(\text{mod } (x-1)^{(p-1)/4+1})$ and $|l-m| \ne 2$. Then $w(g(x)) \ge (p-1)/4$.

Let us introduce the auxiliary polynomial $R(x) = \sum_{i=0}^{4} c_i S_i(x), c_i \in \mathbb{Z}$. Denote a formal derivative of order n of the polynomial $R(x)$ by $R^{(n)}(x)$.

Lemma 2. Let $R^{(n)}(x)|_{x=\pm 1} = 0$ *if* $0 \le n \le (p-1)/4$. Then $R^{(n)}(x)|_{x=\pm 1} = 0$ for $(p-1)/4 + 1 < n < (p-1)/2$.

Proof. We consider the sequences $\{r_t\}$ of length p defined by

$$r_t = \begin{cases} 0, \text{if } t = 0, \\ c_i, \text{if } t \in D_i. \end{cases}$$

By the definition of the sequence, $S_r(x) \equiv R(x)(\text{mod } (x^p - 1))$, so that by the condition of this lemma $L(r) < 3(p-1)/4$. By Theorem 1 from [9] for the cyclotomic sequences $L(r) = p - c(p-1)/4, 1 \le c \le 3$. Hence, $L(r) \le p - (p-1)/2$. This completes the proof of Lemma 2.

This lemma can also be proved using Lemma 2 and 3 from [5].

3. The exact values of the k-error linear complexity of u for $1 \le k < (p-1)/4$

In this section we obtain the upper and lower bounds of the k-error linear complexity and determine the exact values for the k-error linear complexity $L_k(u), 1 \le k < (p-1)/4$.

First of all, we consider the case $k = 1$. Our first contribution in this paper is the following.

Lemma 3. Let $\{u_i\}$ be defined by (1) for $p > 5$. Then $L_1(u) = (7p+1)/4$.

Proof. Since $L_1(u) \le L(u)$ and $L(u) = (7p+1)/4$ [5], it follows that $L_1(u) \le (7p+1)/4$. Assume that $L_1(u) < L(u)$. Then there exists $f(x) = ax^b, a \ne 0$ such that $S_u(x) + ax^b \equiv 0(\text{mod}(x-1)^{m_0}(x+1)^{m_1})$ for $m_0 + m_1 > (p-1)/4$. By (4) the last comparison is impossible for $p \ne 5$.

If $p = 5$ then $L_1(u) = 8$.

Lemma 4. Let $\{u_i\}, \{q_i\}, \{v_i\}$ be defined by (1) and (5), respectively. Then $L_k(q) + L_k(v) \le L_k(u)$.

Proof. Suppose $S_u(x) + f(x) \equiv 0(\text{mod } (x-1)^{m_0}(x+1)^{m_1})$, $w(f) \le k$ and $m_0 + m_1 = 2p - L_k(u)$. Combining this with (4) and (6) we get $S_q(x) + f(x) \equiv 0(\text{mod}(x-1)^{m_0})$ and $S_l(x) - S_m(x) + 1 + f(x) \equiv 0(\text{mod}(x+1)^{m_1})$ or $S_m(x) - S_l(x) + 1 + f(-x) \equiv 0(\text{mod}(x-1)^{m_1})$ Hence $m_0 \le p - L_k(q)$ and $m_1 \le p - L_k(v)$. This completes the proof of Lemma 4.

Lemma 5. Let $\{u_i\}$ be defined by (1) and $k \ge 2$. Then $L_k(u) \le 3(p-1)/4 + 1 + L_{k-2}(q)$.

Proof. From our definition it follows that there exists $h(x)$ such that

$$S_q(x) + h(x) \equiv 0(\text{mod } (x-1)^{p-L_{k-2}(q)}), w(h) \le k-2.$$

Then, by Lemma 1 $h(x) \equiv 0(\text{mod } (x-1)^{(p-1)/4})$. Let $h(x) = \sum h_i x^{a_i}$. We consider $f(x) = \sum f_i x^{b_i}$ where

$$b_i = \begin{cases} a_i, & \text{if } a_i \text{ is an even,} \\ a_i + p, & \text{if } a_i \text{ is an odd.} \end{cases}$$

By definition $f(x) \equiv h(x)(\text{mod } (x-1)^p)$, hence $S_q(x) + f(x) \equiv 0(\text{mod } (x-1)^{p-L_{k-2}(q)})$. Further, since $h(x) \equiv 0(\text{mod } (x-1)^{(p-1)/4})$ and $f(x) = f(-x)$, it follows that

$$f(x) \equiv 0 \ (\text{mod } (x+1)^{(p-1)/4}).$$

Using (3), we obtain that

$$S_u(x) + (x^p - 1)/2 + f(x) \equiv (x^p - 1)(S_j(x) + S_m(x) + 1/2) + S_q(x) + f(x)(\text{mod } (x^2-1)^p).$$

From this by Lemma 1 we can establish that

$$S_u(x) + (x^p - 1)/2 + f(x) \equiv 0 \ (\text{mod } (x-1)^{p-L_{k-2}(q)}(x+1)^{(p-1)/4}).$$

The conclusion of this lemma then follows from (2).

Theorem 1. Let $\{u_i\}$ be defined by (1) and $2 \le k < (p-1)/4$. Then $L_k(u) = 3(p-1)/2 + 2$.

Proof. By Lemmas 3 and 4 it follows that $L_k(v) + L_k(q) \le L_k(u) \le 3(p-1)/4 + 1 + L_{k-2}(q)$. To conclude the proof, it remains to note that $L_k(v) = L_k(q) = L_{k-2}(q) = 3(p-1)/4 + 1$ for $2 \le k < (p-1)/4$ by (7), (8).

4. The estimates of k-error linear complexity

In this section we determine the exact values of the k-error linear complexity of u for $(p-1)/4 + 2 \le k < (p-1)/3$ and we obtain the estimates for the other values of k. Farther, we consider two cases.

Let $(m, j, l) = (0,1,3), (0,2,3), (1,2,0), (1,3,0)$

Lemma 6. Let $\{u_i\}$ be defined by (1). Then $21(p-1)/16 + 1 \le L_{(p-1)/4}(u) \le 3(p-1)/2 + 2$ and $p + 1 \le L_{(p-1)/4+1}(u) \le 3(p-1)/2 + 2$ for $p > 5$.

The statement of this lemma follows from Lemmas 4, 5 and (7), (8).

Theorem 2. Let $\{u_i\}$ be defined by (1) for $(m, j, l) = (0,1,3), (0,2,3), (1,2,0), (1,3,0)$ and $(p-1)/4 + 2 \le k < (p-1)/3$. Then $L_k(u) = p + 1$.

Proof. We consider the case when $(m, j, l) = (0,1,3)$. Let $f(x) = x^p/2 - (\rho+3)/4 - (\rho+1)x^p S_0(x)$ where $\rho = \theta^{(p-1)/4}$ is a primitive 4-th root of unity modulo p. Then $w(f) = 2 + (p-1)/4$. Denote $S_u(x) + f(x)$ by $h(x)$. Under the conditions of this theorem we have

$$h(x) = (x^p + 1)S_1(x) + x^p S_0(x) + S_3(x) + 1 + \frac{x^p}{2} - \frac{\rho+3}{4} - (\rho+1)x^p S_0(x).$$

Hence $h(1) = 0$. Let $h^{(n)}(x)$ be a formal derivative of order n of the polynomial $h(x)$. By Lemmas 2 and 3 from [5] we have that $h^{(n)}(1) = 0$ if $1 \le n < (p-1)/4$ and by Lemma 3 from [5] $h^{(p-1)/4}(1) = (2\rho + 1 + \rho^3 - (\rho+1))(p-1)/4 = 0$. Hence, by Lemma 2 $h^{(n)}(1) = 0$ if $(p-1)/4 < n < (p-1)/2$ and $h(x) \equiv 0(\text{mod } (x-1)^{(p-1)/2})$.

Further, $h(-1) = -1/4 + 1/4 + 1 - 1/2 - (\rho+3)/4 + (\rho+1)/4 = 0$ and $h^{(p-1)/4}(-1) = (-1 + \rho^3 + (\rho+1))(p-1)/4 = 0$. So, by Lemma 2 $h^{(n)}(1) = 0$ if $1 < n < (p-1)/2$ and $h(x) \equiv 0(\text{mod}(x+1)^{(p-1)/2})$. Therefore, by (2) we see that $L_{(p-1)/4+2} \le p + 1$. On the other hand, by Lemma 4 $L_k(u) \ge L_k(v) + L_k(q)$. To conclude the proof, it remains to note that $L_k(v) + L_k(q) = p + 1$ for $(p-1)/4 + 2 < k < (p-1)/3$ by (7), (8). The other cases may be considered similarly. Theorem 2 is proved.

Farther, if $(p-1)/3 \le k < (p-1)/2$ then by Lemma 4, Theorem 2 and (7), (8) we have that $(p-1)/2 + 1 \le L_k(u) \le p + 1$. It is simple to prove that $L_{(p-1)/2+2}(u) \le (p-1)/2 + 2$.

Let $(m, j, l) = (0,1,2), (0,3,2), (1,0,3), (1,2,3)$. Similarly as in subsection 4.1, we have that $21(p-1)/16 + 1 \le L_{(p-1)/4}(u) \le 3(p-1)/2 + 2$.

Theorem 3. Let $\{u_i\}$ be defined by (1) for $(m, j, l) = (0,1,2), (0,3,2), (1,0,3), (1,2,3)$ and $(p-1)/4 + 1 \le k < (p-1)/3$ then $L_k(u) = 5(p-1)/4 + 2$.

Proof. We consider the case when $(m, j, l) = (0,1,2)$. Let here $f(x) = -1/2 - 2S_2(x)$ and $h(x) = S_u(x) + f(x)$. Since $(m, j, l) = (0,1,2)$ it follows that

$$h(x) = (x^p + 1)S_1(x) + x^p S_0(x) + S_2(x) + 1 - 1/2 - 2S_2(x).$$

Hence $h(1) = 0$. By Lemma 2 from [5] we have that $h^{(n)}(1) = 0$ if $1 \le n < (p-1)/4$. Hence $h(x) \equiv 0(\mathrm{mod}\ (x-1)^{(p-1)/4})$.

Further, $h(-1) = 0$ and $h^{(p-1)/4}(-1) = (-1 + \rho^2 - 2\rho^2)(p-1)/4 = 0$. So, $h^{(n)}(-1) = 0$ if $1 < n < (p-1)/2$ and $h(x) \equiv 0(\mathrm{mod}\ (x+1)^{(p-1)/2})$. Therefore, by (2) we see that $L_{(p-1)/4+2} \le 2p - 3(p-1)/4$.

Suppose $L_{(p-1)/4+2} < 2p - 3(p-1)/4$; then by (2) there exist m_0, m_1 such that $m_0 + m_1 > 3(p-1)/4$ and $S_u(x) + f(x) \equiv 0(\mathrm{mod}\ (x-1)^{m_0}(x+1)^{m_1})$, $w(f) \le k < (p-1)/3$.

We consider two cases.

(i) Let $m_0 \le (p-1)/4$ or $m_1 \le (p-1)/4$. Then $m_1 > (p-1)/2$ or $m_0 > (p-1)/2$ and by (4) and (6) we obtain $L_k(q) < (p+1)/2$ or $L_k(v) < (p+1)/2$. This is impossible for $k < (p-1)/3$ by (7) or (8).

(ii) Let $\min(m_0, m_1) > (p-1)/4$. We can write that $f(x) = f_0(x^2) + xf_1(x^2)$. Therefore, since $2S_1(x) + S_0(x) + S_2(x) + 1 + f(x) \equiv 0(\mathrm{mod}\ (x-1)^{m_0})$ and $S_2(x) - S_0(x) + 1 + f(x) \equiv 0(\mathrm{mod}\ (x+1)^{m_1})$ or $-S_2(x) + S_0(x) + 1 + f_0(x^2) - xf_1(x^2) \equiv 0(\mathrm{mod}\ (x-1)^{m_1})$ we see that $S_1(x) + S_0(x) + 1 + f_0(x^2) \equiv 0(\mathrm{mod}\ (x-1)^{\min(m_0,m_1)})$. Hence, $w(f_0) \ge (p-1)/4$ by Lemma 1.

Similarly, $-2S_1(x) - S_0(x) - S_2(x) + 1 + f_0(x^2) - xf_1(x^2) \equiv 0(\mathrm{mod}\ (x+1)^{m_1}))$ and $S_2(x) - S_0(x) + 1 + f_0(x^2) + xf_1(x^2) \equiv 0\ (\mathrm{mod}(x+1)^{m_1})$ so $S_1(x) + S_2(x) + 1 + xf_1(x^2) \equiv 0(\mathrm{mod}\ (x-1)^{\min(m_0,m_1)})$. Hence, $w(f_1) \ge (p-1)/4$ by Lemma 1. This contradicts the fact that $w(f) < (p-1)/3$.

Similarly, if $(p-1)/3 \le k < (p-1)/2$ then by Lemma 4, Theorem 2 and (7), (8) we have that $(p-1)/2 + 1 \le L_k(u) \le 2p - 3(p-1)/4$. Here $L_{(p-1)/2+2}(u) \le 3(p-1)/4 + 2$.

In the conclusion of this section note that we can improve the estimate of Lemma 5 for $k \ge (p-1)/2 + 1$. With similar arguments as above we obtain the following results for u.

Lemma 7. Let $\{u_i\}$ be defined by (1) and $k = (p-1)/2 + f, f \ge 0$. Then $L_k(u) \le L_{[f/2]}(v) + 1$ where $[f/2]$ is the integral part of number $f/2$.

5. Conclusion

We investigated the k-error linear complexity over $\mathbb{F}_p$ of sequences of length $2p$ with optimal three-level autocorrelation. These balanced sequences are constructed from cyclotomic classes of order four using a method presented by Ding et al. We obtained the upper and lower bounds of k-error linear complexity and determine the exact values of the k-error linear complexity $L_k(u)$ for $1 \le k < (p-1)/4$ and $(p-1)/4 + 2 \le k < (p-1)/3$.

Acknowledgements

The reported study was funded by RFBR and NSFC according to the research project no. 19-51-53003.

References

[1] Golomb S W and Gong G 2005 *Signal Design for Good Correlation*: *For Wireless Communications, Cryptography and Radar Applications* (Cambridge University Press)
[2] Ding C, Helleseth T and Martinsen H 2001 *IEEE Trans. Info. Theory* **47** 428 – 433.
[3] Lidl R and Niederreiter H 1983 *Finite Fields* (Addison-Wesley)
[4] Zhang J and Zhao C 2015 *Appl. Algebra Eng. Commun. Comput*. **26 (5)** 475–491.
[5] Edemskiy V and Palvinskiy A 2015 *Inf. Process. Lett*. **116 (2)** 153–156
[6] Ding C, Xiao G. and Shan W 1991 *The Stability Theory of Stream Ciphers in Lecture Notes in Computer Science* (Springer-Verlag, Berlin) p 561
[7] Stamp M and Martin C F 1993 *IEEE Trans. Inform. Theory* **39** 1398–1401
[8] Aly H and Winterhof A 2006 *Des. Codes Crypt.* **40** 369–374
[9] Aly H, Meidl W and Winterhof A 2007 *J. Math. Crypt*. **1** 1–14

[10] Hall M 1975 *Combinatorial Theory* (Wiley, New York)
[11] Ireland K and Rosen M 1982 *Classical Introduction to Modern Number Theory* (Springer, Berlin)
[12] Cusick T, Ding C and Renvall A 1998 *Stream Ciphers and Number Theory* (North-Holland Publishing Co., Amsterdam)