About the linear complexity of the almost perfect sequences

VLADIMIR EDEMSKIY
Novgorod State University
Department of Applied Mathematics
and Information Science
B. St. Petersburgskaya 41,
173003 Veliky Novgorod
Russia
Vladimir.Edemsky@novsu.ru

ALEKSEY MININ
Novgorod State University
Department of Applied Mathematics
and Information Science
B. St. Petersburgskaya 41,
173003 Veliky Novgorod
Russia
s208076@std.novsu.ru

Abstract: We calculate the linear complexity of almost perfect binary sequences. Also we study the linear complexity of binary sequences obtained from series of almost perfect ternary sequences and the ternary sequences with two nonzero autocorrelation sidelobe levels.

Key–Words: linear complexity, almost perfect sequences

1 Introduction

Pseudorandom sequences are widely used in cryptography and communication. The autocorrelation and the linear complexity are important parameters of pseudo-random sequences [2, 3]. Periodic sequences with good correlation properties have important applications in various areas of engineering [3].

Let (u_t) be a binary sequence of period N, i.e. $u_t = u_{t+N}$ and $u_t = 1$ or 0 for $t = 0, 1, 2, \dots$. The autocorrelation of the sequence at shift τ is defined by

$$C_u(\tau) = \sum_{t=0}^{N-1} (-1)^{u_{t+\tau} - u_t}.$$

The sequence (u_t) is said to be almost perfect if $C_s(\tau) = 0$ for all $\tau \not\equiv 0 \pmod N$ with exactly one exception. Almost perfect sequences were introduced by Wolfmann [13]. It is worth pointing out that there is other definition of almost perfect sequences. The sequence is called almost perfect if all the off-peak autocorrelation coefficients are as small as theoretically possible - with exactly one exception [5].

In this paper we will use the definition of Wolfmann. By [13] such binary sequence exist only if the period of sequence is a multiple of 4. In this case two definitions are the same (see [5]). Pott and Bradley [12] proved that an N-periodic sequence (u_t) is almost perfect if and only if support of (u_t) ($C = \{t | 0 \le t < N \text{ and } u_t = 1\}$) is a cyclic divisible difference set with the parameters

$$(N/2, 2, (N-2\theta)/2, \theta(\theta-1), (N-4\theta)/4)$$

where $(N-2\theta)/2$ is the number of entries 1 in a generating cycle. There are no almost perfect sequences for $\theta = 0$ with period $N > 4$ [13]. The case $\theta = 1$ was investigated in [13, 12, 10]. In this case, almost perfect sequences exist provided that $N = 2(q+1)$ for some odd prime power $q = p^n$. It has been proved in [1, 11] that almost perfect sequences with $\theta = 2$ exist if and only if $N = 8; 12$ or 28. The almost perfect sequences still poorly understood for case $\theta > 2$.

Further, almost perfect ternary sequences have been proposed by Langevin [9], Schotten and Luke [14], and Krengel [6, 7]. Krengel used the decomposition of m-sequences of length p^n-1 over $\mathbb{F}_p$, $n = km$, with p being an odd prime.

The linear complexity L of a sequence is an important parameter in its evaluation as a key stream cipher for cryptographic applications. A high linear complexity is necessary for a good cryptographic sequence. The linear complexity (also called linear span) of u_t is defined to be the smallest positive integer L such that there are constants $c_1, \dots, c_L \in \mathbb{F}_2$ satisfying

$$u_i = c_1 u_{i-1} + c_2 u_{i-2} + \dots + c_L u_{i-L}$$

for all $i \ge L$. The linear complexity also may be defined as the length of the shortest linear feedback shift register that is capable of generating the sequence. Knowledge of just $2L$ consecutive digits of the sequence is sufficient to enable the remainder of the sequence to be constructed. Thus, it is reasonable to suggest that 'good' sequences have L bigger than a half of the period of the sequence [2].

In this paper we prove that the almost perfect binary sequences of length $2(p^n+1)$ have high linear complexity. Also we investigate the linear complexity of the series of binary sequences obtained from almost perfect ternary sequences [7] and the ternary sequences with two nonzero autocorrelation sidelobe levels. We have proved conjectures made in [7, 8] about the linear complexity of sequences.

2 The linear complexity of almost perfect binary sequences of length $2(p^n+1)$

Let p be an odd prime, $q = p^n, n = 1, 2, \ldots$. Throughout this paper, let (u_i) be almost perfect binary sequence with period $N = 2(q+1)$ for $\theta = 1$. In this section we will investigate the linear complexity of (u_i).

It is well known that if (u_t) is a sequence with period N, then the minimal polynomial $m(x)$ and the linear complexity L of this sequence can be defined by

$$m(x) = (x^N - 1)/\gcd\bigl(x^N - 1, S_u(x)\bigr),$$
$$L = N - \deg\gcd\bigl(x^N - 1, S_u(x)\bigr), \quad (1)$$

where $S_u(x) = u_0 + u_1 x + \ldots + u_{N-1}x^{N-1}$ [2]. Hence, in order to find the value L and $m(x)$ it is sufficient to find the $\gcd\bigl(x^N - 1, S_u(x)\bigr)$. It is worth pointing out that the minimal polynomials of $m(x)$ defined here may be the reciprocals of the minimal polynomials defined in other references.

Before we give the main result of this section, we establish the following lemmas.

Lemma 1 *Let $a = \min\limits_{u_j=0} j$. Then:*

(i) $u_a = u_{a+q+1} = 0$.

(ii) $u_j + u_{j+q+1} = 1$ for $0 < j < q+1, j \neq a$.

Proof: Since

$$((-1)^{u_0} + (-1)^{u_1} + \cdots + (-1)^{u_{N-1}})^2 = \sum_{w=0}^{N-1} C_u(w)$$

and $C_u(0) = 2(q+1)$, it follows that $C_u(q+1) = -2(q-1)$, i.e.,

$$\sum_{t=0}^{2q+1} (-1)^{u_{t+q+1} - u_t} = -2(q-1).$$

Thus, there is a unique a such that $u_a = u_{a+q+1} = 0$ and $u_j + u_{j+q+1} = 1$ for $0 < j < q+1, j \neq a$. □

Let $S_u(x) = \sum_{i=0}^{2q+1} u_i x^i$. Introduce the subsidiary polynomial $T(x) = \sum\limits_{i=0}^{q} u_i x^i$.

Lemma 2 $S_u(x) = T(x)(1 - x^{q+1}) + x^{a+q+1} + x^{q+1}(x^{q+1} - 1)/(x-1)$.

Proof: From our definition it follows that

$$S_u(x) = \sum_{i=0}^{2q+1} u_i x^i = T(x) + \sum_{i=q+1}^{2q+1} u_i x^i.$$

By Lemma 1 we see that $u_{j+q+1} = 1 - u_j$ for $0 < j < q+1, j \neq a$. Hence, we obtain $\sum_{i=q+1}^{2q+1} u_i x^i = x^{q+1}\sum_{i=0}^{q}(1 - u_i)x^i - x^{a+q+1} = x^{q+1}(1 + x + \cdots + x^q) - T(x)x^{q+1} - x^{a+q+1}$. This completes the proof of Lemma 2. □

Theorem 3 *Let (u_i) be the almost perfect binary sequence of period $N = 2(q+1)$. Then $L = 2(q+1)$ and $m(x) = x^N - 1$.*

Proof: By Lemma 2 we have $\gcd(x^N - 1, S_u(x)) = \gcd\bigl(x^{2(q+1)} - 1, x^{a+q+1} + (x^{q+1} - 1)/(x - 1)(T(x)(x-1) + x^{q+1})\bigr) = 1$. The conclusion of this theorem then follows from (1). □

It is worth noting that 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.

The k-error linear complexity of a sequence is defined by $L_k(u) = \min\limits_{t} L(t)$, where the minimum is taken over all binary N-periodic sequences $r = (r_n)$ for which the Hamming distance of the vectors $(r_0, r_1, \ldots, r_{N-1})$ and $(u_0, u_1, \ldots, u_{N-1})$ is at most k. 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.

From the proof of Theorem 3 it follows that here 1-error the linear complexity $L_1(u) \leq q + 2$.

3 Notes about the linear complexity of Krengel's sequences

The almost perfect autocorrelation ternary sequence of period $N = 4(q+1)$ and the four zeros on the period were investigated by Krengel in [7]. E. Krengel hazards a conjecture that the linear complexity of binary sequences obtained from of these almost perfect ternary sequences is equal to $N = 3(q+1)$. Here we prove this conjecture.

First, we briefly repeat the basic definitions from [7]. From now on, we suppose that $q = p^n, n = 1, 2, \ldots$ be an integer of the form $q \equiv 1 (\mathrm{mod}\ 4)$.

Let γ be the primitive element of $\mathbb{F}_{q^2}$ and $\theta = \gamma^{q+1}$. It is easy to prove that $\theta \in \mathbb{F}_q$ and θ is the primitive element of $\mathbb{F}_q$. We consider the ternary sequences defined by

$$y_i = \psi(Tr(\gamma^i), i = 0, 1, \dots, 4(q+1) - 1, \qquad (2)$$

where

$$\psi(x) = \begin{cases} (-1)^{\lfloor (\text{ind}_\eta x \bmod 4)/2 \rfloor}, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0. \end{cases} \quad x \in \mathbb{F}_q,$$

$\text{ind}_\eta x$ is a discrete logarithm on base η, $\lfloor u \rfloor = \max\{k : k < u, k \in \mathbb{N}\}$, and $Trx = x + x^q + \dots + x^{q(q-1)}$ is a trace function from $\mathbb{F}_{q^2}$ in $\mathbb{F}_q$.

By [7] (y_i) is the almost perfect autocorrelation ternary sequence of period $N = 4(q+1)$ and four zeros in the period.

Let $\{w_i\}$ be a binary sequence of period $4(q+1)$ defined as

$$w_i = \begin{cases} 1, & \text{if } y_i = 0, 1, \\ 0, & \text{if } y_i = -1. \end{cases} \qquad (3)$$

To begin with, we give another definition of the sequence. By definition, put $H_k = \{\theta^{k+4s} \bmod p; s = 1, ..., (q-1)/4\}, k = 0, 1, 2, 3$, where the arithmetic is as in $\mathbb{F}_q$. Then H_k are cyclotomic classes of order four [4].

Let $\xi_i = Tr\gamma^i, i = 0, 1, \dots, 4(q+1) - 1$. From our definitions, (2) and (3) it follows that

$$w_i = \begin{cases} 1, & \text{if } \xi_i \in H_0 \cup H_1 \cup \{0\}, \\ 0, & \text{if } \xi_i \in H_2 \cup H_3. \end{cases} \qquad (4)$$

Lemma 4 *(i) Let* $b = \min\limits_{\xi_i = 0} i$. *Then* $w_{b+k(q+1)} = 1$ *for* $k = 0, 1, 2, 3$.

(ii) Let $j : j \neq b + k(q+1), k = 0, 1, 2, 3, 0 \leq j \leq 2q+1$. *Then* $w_j + w_{j+2(q+1)} = 1$.

Proof: (i) By definition we have that $\xi_b = 0$ and

$$\xi_{b+k(q+1)} = Tr\gamma^{b+k(q+1)} = \theta^k Tr\gamma^a = \theta^k \xi_b = 0.$$

Hence, by (4) we get $w_{b+k(q+1)} = 1$ for $k = 0, 1, 2, 3$.

(ii) Suppose $w_j = 1$ and $j \neq b + k(q+1), k = 0, 1, 2, 3$; then by (4) $\xi_j \in H_0 \cup H_1$. Since

$$Tr\gamma^{j+2(q+1)} = \theta^2 Tr\gamma^j = \theta^2 \xi_j,$$

it follows that $\xi_{j+2(q+1)} \in H_2 \cup H_3$. So, $w_{j+2(q+1)} = 0$. The case when $w_j = 0$ may be proved similarly as the first. □

Let $P_w(x) = \sum_{i=0}^{2q+1} w_i x^i$, $S_w(x) = \sum_{i=0}^{4q+3} w_i x^i$. With similar arguments as above we obtain the following results for $S_w(x)$.

Lemma 5 $S_w(x) = P(x)(1 - x^{2(q+1)}) + x^{2(q+1)}(x^{2(q+1)} - 1)/(x-1) + x^{b+2(q+1)}(1 + x^{q+1})$.

Theorem 6 *Let* (w_i) *be defined by* (3). *Then* $L = 3(q+1)$ *and* $m(x) = (x^{q+1} - 1)^3$.

Proof: Since by Lemma 4 $S_w(x)/(1 + x^{q+1}) = P(x)(1 + x^{q+1}) + x^{2(q+1)}(x^{q+1} - 1)/(x-1) + x^{b+2(q+1)}$ and

$$x^{(q+1)} - 1)/(x-1)| \,|_{x=1} = 0,$$

it follows that

$$\gcd(x^{4(q+1)} - 1, S_w(x)) = x^{q+1} + 1.$$

This completes the proof of Theorem 6. □

Remark 7 *We can also consider the balanced binary sequence* $(\widetilde{w}_i)$ *of length* $4(q+1)$ *defined by*

$$\widetilde{w}_i = \begin{cases} w_i, & \textit{if } i \neq b, b + 3(q+1), \\ 0, & \textit{if } i = b, b + 3(q+1). \end{cases}$$

In this case we also have that $S_w(x) = P(x)(1 + x^{2(q+1)}) + x^{2(q+1)}(x^{2(q+1)} - 1)/(x-1) + x^{b+2(q+1)}$. *Hence, the linear complexity of* $(\widetilde{w}_i)$ *is equal to* $L = 3(q+1)$.

Remark 8 *If* $(\bar{w}_i)$ *is defined by*

$$\widetilde{w}_i = \begin{cases} 1, & \textit{if } \xi_i \in H_0 \cup H_1, \\ 0, & \textit{if } \xi_i \in H_2 \cup H_3 \cup \{0\}. \end{cases}$$

then the linear complexity of $(\widetilde{w}_i)$ *is also equal to* $L = 3(q+1)$.

Remark 9 *From the proof of Theorem 6 it follows that 2-error the linear complexity* $L_2(w) \leq 2q + 4$.

4 About the linear complexity of the sequences of length $8(q+1)$

New ternary sequences of length $8(q+1)$ with two nonzero autocorrelation sidelobe levels and peak factor close to unity were proposed in [8]. Authors hazard a conjecture that the linear complexity of binary sequences obtained from these new ternary sequences is equal to $N = 6(q+1)$. Here we prove this conjecture.

Let (h_i) be a sequence of length $4(q+1)$ obtained by combining two perfect binary sequences (u_i), i.e., $h_i = u_i$ for $i = 0, 1, \dots, 4q+3$.

Let (z_i) be a balanced sequence of length $8(q+1)$ defined as

$$z_k = \begin{cases} h_i, & \text{if } k = 2i, \\ w_i, & \text{if } k = 2i+1, \end{cases} \quad k = 0, 1, \ldots, 8(q+1)-1. \tag{5}$$

Thus the above expression is equivalent to the following $z = I(h, w)$ where I is the interleaved operator.

Let $S_z(x) = \sum_{i=0}^{8q+7} z_i x^i$, $S_h(x) = \sum_{i=0}^{4q+3} v_i x^i$. From our definition it follows that [15]

$$S_z(x) = S_h(x^2) + xS_w(x^2) \tag{6}$$

Theorem 10 *Let (z_i) be a binary sequence of period $N = 8(q+1)$ defined by* (5). *Then $L = 6(q+1)$ and $m(x) = (x^{q+1} - 1)^6$.*

Proof: By definition,

$$S_h(x) = S_u(x) + x^{2(q+1)} S_u(x)$$

so that

$$S_h(x^2) = S_u(x^2)(1 + x^{4(q+1)}).$$

Further, by Lemma 5 we have $S_w(x^2) = P(x^2)(1 + x^{4(q+1)}) + x^{4(q+1)+1}((x^{4(q+1)} - 1)/(x^2 - 1) + x^{2b+4(q+1)}(1 + x^{2(q+1)})$.

From this by (6) we can establish that

$$S_z(x) = (1 + x^{2(q+1)})R(x)$$

where

$$R(x) = S_h(x^2)(1+x^{2(q+1)}) + xP(x^2)(1+x^{2(q+1)})$$
$$+ x^{4(q+1)+1}(x^{2(q+1)} - 1)/(x^2 - 1) + x^{2b+4(q+1)}.$$

To conclude the proof, it remains to note that in this case $\gcd(x^{8(q+1)} - 1, R(x)) = 1$. □

Remark 11 *From the proof of Theorem 10 it follows that 2-error the linear complexity $L_2(z) \leq 4q + 4$.*

5 Conclusion

We calculated the linear complexity of almost perfect binary sequences. Also we studied the linear complexity of binary sequences obtained from series of almost perfect ternary sequences and the ternary sequences with two nonzero autocorrelation sidelobe levels. All sequences considered in this paper have high linear complexity.

Acknowledgements: This work was supported by the Ministry of Education and Science of the Russian Federation as a part of state-sponsored project no 1.949.2014/K.

References:

[1] K.T. Arasu, S.L. Ma, N.J. Voss, On a class of almost perfect sequences, *J. Algebra*, 192, 1997, pp. 47–56.

[2] T.W. Cusick, C. Ding, A. Renvall. *Stream Ciphers and Number Theory*, North-Holland Publishing Co., Amsterdam 1998

[3] S.W. Golomb, G. Gong. *Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Applications.* Cambridge University Press 2005

[4] M. Hall, *Combinatorial Theory*, Wiley, New York 1975

[5] D. Jungnickel, A. Pott, Perfect and almost perfect sequences, *Discrete Applied Mathematics*, 95, 1999, pp. 331–359.

[6] E.I. Krengel, Almost-perfect and odd-perfect ternary sequences, *Proc. 2004 Inter. Conf. on Sequences and Their Applications (SETA '04), Seoul, Korea*, LNCS 3486, Springer-Verlag Berlin, 2005, pp.197-207.

[7] E.I. Krengel, A method of construction of perfect sequences, *Radiotehnika*, 11, 2009, pp. 15–21 (in Russian).

[8] E.I. Krengel, P.V. Ivanov, New terhary sequences with two nonzero autocorrelation sidelobe levels and peak factor close to unity, *DSPA-2016* (in Russian).

[9] Ph. Langevin, Some sequences with good autocorrelation properties, *Finite Fields*, 168, 1994, pp. 175-185.

[10] Ph. Langevin, Almost perfect binary function, *Applicable Algebra in Engineering, Communication and Computing*, 4, 1993, pp.95–102.

[11] K.H. Leung, S. Ling, S.L. Ma, K.B. Tay, Almost perfect sequences with $\theta = 2$, *Arch. Math.*, 70, 1998, pp. 128–131.

[12] A. Pott, S. Bradley, Existence and nonexistence of almost-perfect autocorrelation sequences, *IEEE Trans. Inf. Theory*, IT-41 (1), 1995, pp. 301–304.

[13] Wolfmann J. Almost perfect autocorrelation sequences, *IEEE Trans. Inf. Theory*, IT-38 (4), 1992, pp. 1412–1418.

[14] H. D. Schotten, H. D. Luke, New perfect and w-cyclic-perfect sequences, *IEEE International Symposium on Information Theory*, 12, 1996, pp. 82–85

[15] Q. Wang, X.N. Du, The linear complexity of binary sequences with optimal autocorrelation, *IEEE Trans. Inf. Theory*, 56 (12), 2010, pp. 6388–6397