The symmetric 2-adic complexity of sequences with optimal autocorrelation magnitude and length $8q$

Vladimir Edemskiy [*]

Department of Applied Mathematics and Information Science
Yaroslav-the-Wise Novgorod State University
Veliky Novgorod, Russia

vladimir.edemsky@novsu.ru

Yuhua Sun [†]

College of Science,
China University of Petroleum
Qingdao, Shandong, China

sunyuhua_1@163.com

Abstract

This paper is devoted to studying the symmetric 2-adic complexity of sequences with optimal autocorrelation magnitude and period $8q$, where q is a prime satisfying $q \equiv 5 \pmod 8$. These sequences were constructed by interleaving technique from Ding-Helleseth-Martinsen sequences and almost perfect binary sequences. They were presented by Krengel and Ivanov in 2016 and have been proved to have high linear complexity. Our result shows that they also have high symmetric 2-adic complexity.

1 Introduction

Binary sequences with low autocorrelation, large linear complexity and 2-adic complexity, are widely used in many areas of communication and cryptography. Interleaving technique was introduced by Gong [6] and has become an important method to construct binary sequences with good pseudo-random properties listed above. For example, Tang and Gong presented three classes of sequences with optimal autocorrelation value/magnitude from Legendre sequences, twin-prime sequences and a generalized GMW sequence, respectively [19]. Soon afterwards, Tang and Ding gave a construction of optimal binary sequences

[*] Vladimir Edemskiy is supported by RFBR and NSFC according to the research project No. 19-51-53003.

[†] Yuhua Sun is financially supported by the National Natural Science Foundation of China (No. 61902429), the Fundamental Research Funds for the Central Universities (No. 19CX02058A)

which generalized the constructions [18] introduced by Tang and Gong. Recently, from Ding-Helleseth-Lam sequences [1], Su et al. presented several sequences with optimal autocorrelation magnitude by interleaving technique [17], see also [14]. In fact, the famous Ding-Helleseth-Martinsen sequences [2] have also been showed to be with an interleaved structure [25]. What's encouraging is that all of the above mentioned sequences have been proved to have large linear complexity and 2-adic complexity [13, 23, 5, 4, 16, 24, 25, 26].

It should be pointed out that all of the above mentioned sequences are interleaved by 4-column except that Ding-Helleseth-Martinsen sequences are interleaved by 2-column. Specifically, the sequences interleaved by 4-column are of the form $s = I(s_1, s_2, s_3, s_4)$, i.e., s is obtained by concatenating the successive rows of the matrix $I(s_1, s_2, s_3, s_4)$, where each column is a periodic sequence s_i, $1 \le i \le 4$, and the sequences interleaved by 2-column are similar to that by 4-column except for the number of columns. Not only that, the base sequences s_i, $1 \le i \le 4$ which are used to construct the above sequences also belong to the same type which means that all of them either have ideal autocorrelation or one is a modified version of another.

However, because of the diversity of interleaving methods, it seems that new sequences emerge in endlessly. Just recently, Krengel and Ivanov presented a new construction in which two different types of sequences are used as the base sequences of an interleaved structure [11], i.e., they employed two classes of optimal sequences and an almost perfect sequence to produce two families of sequences with optimal autocorrelation. In quick succession, Edemskiy and Minin proved that these sequences have high linear complexity [3].

Comparing with the linear complexity, the 2-adic complexity of binary sequences with small autocorrelation has not been fully researched. The 2-adic complexity of the binary sequences with ideal autocorrelation and some other sequences with good autocorrelation were studied in [22, 21, 15, 16] (see also references here). Very recently, the 2-adic complexity of Ding-Helleseth-Martinsen sequence with period $2p$ was determined in [26] by using "Gauss periods" and "Gauss sums" on finite field $\mathbb{F}_q$ valued in the ring $\mathbb{Z}_{2^{2q}-1}$. With the help of this interesting approach, in this paper we will study the symmetric 2-adic complexity of one family of binary sequences suggested by Krengel and Ivanov which is obtained from Ding-Helleseth-Martinsen (DHM) sequences and an almost perfect binary sequences.

The rest of the paper is organized as follows. Some preliminaries are introduced in Section 2. In Section 3, we prove our main result.

2 Preliminaries

2.1 Autocorrelation and symmetric 2-adic complexity of sequences

Let $\mathbf{s} = (s_0, s_1, \dots, s_N)$ be a binary sequence of period N. The autocorrelation of $\mathbf{s}$ at shift τ is defined by

$$A_{\mathbf{s}}(\tau) = \sum_{i=0}^{N-1} (-1)^{s_i - s_{i+\tau}}.$$

A binary sequence of length $N = 4N_1$ is called to have optimal autocorrelation magnitude when its out-of-phase autocorrelation coefficients belong to the set $\{0, \pm 4\}$.

Klapper and Goresky introduced a new feedback architecture for shift register generation of pseudorandom binary sequences called feedback with carry shift register. The length of the shortest feedback with carry shift register is called 2-adic complexity of sequences. The term was initially used by Klapper who showed this indicator to be important pseudo-randoman measure [9, 10].

Let $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$. According to [9] the 2-adic complexity of the sequence $\mathbf{s}$ can be defined as

$$\Phi(\mathbf{s}) = \left\lfloor \log_2 \left(\frac{2^N - 1}{\gcd\left(S(2), 2^N - 1\right)} + 1 \right) \right\rfloor,$$

where $\lfloor x \rfloor$ is the greatest integer that is less than or equal to x. Due to the rational approximation algorithm, 2-adic complexity has become an important security criteria.

Further, Hu and Feng [7] proposed a new measure $\bar{\Phi}(\mathbf{s}) = \min\left(\Phi(\mathbf{s}), \Phi(\widetilde{\mathbf{s}})\right)$ called symmetric 2-adic complexity, where $\tilde{s} = (s_{N-1}, s_{N-2}, \ldots, s_0)$ is the reciprocal sequence of $\mathbf{s}$. They also showed that symmetric 2-adic complexity is better than 2-adic complexity in measuring the security of a binary periodic sequence.

2.2 The definition of sequences

Let q be a prime of the form $q \equiv 1 (\text{mod } 4)$, and let θ be a primitive root modulo q. By definition, put

$$D_0 = \{\theta^{4s} \text{ mod } q; s = 1, ..., (q-1)/4\}$$

and $D_n = \theta^n D_0, n = 1, 2, 3$. Then D_k are cyclotomic classes of order four modulo q.

The residue classes ring $\mathbb{Z}_{2q} \cong \mathbb{Z}_2 \times \mathbb{Z}_q$ relative to isomorphism $\phi(a) = (a \text{ mod } 2, a \text{ mod } q)$. Ding et al. [2] considered sequences defined as

$$z_i = \begin{cases} 1, & \text{if } i \mod q \in C; \\ 0, & \text{if } i \mod q \notin C, \end{cases} \tag{1}$$

for $C = \phi^{-1}\left(\{0\} \times (D_k \cup D_j) \cup \{1\} \times (D_l \cup D_j)\right)$ where k, j, and l are pairwise distinct integers between 0 and 3 [2]. According to [2], the sequence $\mathbf{z}$ has an optimal autocorrelation value (its out-of-phase autocorrelation coefficients belong to the set $\{\pm 2\}$) when $q \equiv 5 (\text{mod } 8)$ and

1. $(k, j, l) = (1, 0, 3); (0, 1, 2)$ for $q = 1 + 4b^2$ and b is odd;

2. $(k, j, l) = (0, 1, 3); (0, 2, 1)$ for $q = a^2 + 4, b = 1$. Here a, b are integers, $a \equiv 1 (\text{ mod } 4)$ and a sign of b is defined by formulae for cyclotomic numbers.

A binary sequence is called almost perfect if all its out-of-phase autocorrelation values are 0 with one exception. A denotation of almost perfect binary (APB) sequences was introduced by Wolfmann [20]. There is also another definition of almost perfect sequences. The sequence is called almost perfect if all of its off-peak autocorrelation coefficients are as small as theoretically possible, with only one exception [8].

Let p be an odd prime and $m \geq 1$ be a positive integer. APB sequences of a length $2N = 2(p^m + 1)$ were studied in [20, 12, 8] (see also references here). Here we use a representation of APB sequences from [11].

Denote by α the primitive element of the finite field $GF(p^{2m})$ and $\beta = \alpha^N$. It is easy to prove that $\beta \in GF(p^m)$ and β is a primitive element of $GF(p^m)$. Then the APB sequence $\mathbf{x}$ with a period $2(p^m + 1)$ can be defined as

$$x_i = \begin{cases} 0, & \text{if } \mathrm{Tr}(\alpha^i) \neq 0 \text{ and } \mathrm{ind}_\beta \mathrm{Tr}(\alpha^i) \equiv 0 \pmod 2, \\ 1, & \text{if } \mathrm{Tr}(\alpha^i) \neq 0 \text{ and } \mathrm{ind}_\beta \mathrm{Tr}(\alpha^i) \equiv 1 \pmod 2, \\ 1(0), & \text{if } \mathrm{Tr}(\alpha^i) = 0, \end{cases}$$

where $\mathrm{ind}_\beta z$ is the discrete logarithm z to the base β, and $\mathrm{Tr}\ (x) = x + x^{p^m} + \cdots + x^{p^m(p^m-1)}$, $x \in GF(p^{2m})$ is the trace function from $GF(p^{2m})$ in $GF(p^m)$. It is clear by definition that $x_i + x_{i+N} = 1$ for $i = 1, 2, \ldots, N-1$ since $\mathrm{Tr}\ (\beta\alpha) = \beta \mathrm{Tr}\ (\alpha)$. Here, we can set the values x_0, x_N to 0 or 1. We take $x_0 = x_N = 1$ to obtain the balanced sequences below.

As noted in [11] there exist p, m and q such that $p^m + 1 = 2q$, for example $3^2 + 1 = 2 \cdot 5, 5^2 + 1 = 2 \cdot 13$ and so on. For these values p, m, q we form the sequence $\mathbf{y} = \mathbf{z} \cdot \mathbf{z}$ of length $2N = 2(p^m + 1) = 4q$ using a concatenation $\mathbf{z}$.

Let interleaved sequence $\mathbf{w}$ be defined by

$$w_i = \begin{cases} y_k, & \text{if } i = 2k, \\ x_k, & \text{if } i = 2k+1, \end{cases} \quad k = 0, 1, \ldots, 2N-1. \tag{2}$$

Thus, by the definition $8q$ is the period of $\mathbf{w}$. By [11] $\mathbf{w}$ has optimal autocorrelation magnitude. But for our purpose we need to consider the autocorrelation function of this sequence in more detail than it was done in [11]. A proof of the following lemma can be easily carried out by computation $A_{\mathbf{w}}(\tau)$, which is omitted here.

Lemma 1. *Let $\boldsymbol{w}$ be the binary sequence with period $8q$ defined by (2) and $\widetilde{\boldsymbol{w}} = w_{8q-1}, \ldots, w_1, w_0$ be the reciprocal sequence of w. Then for $\tau = 1, 2, \ldots, 8q-1$ we have*

$$A_{\boldsymbol{w}}(\tau) = \begin{cases} A_{\boldsymbol{y}}(k), & \text{if } \tau = 2k,\ k \neq 2q, \\ 4, & \text{if } \tau = 4q, \\ 4y_{-k} + 4y_{k+1} - 4, & \text{if } \tau = 2k+1, \end{cases}$$

Furthermore, since $A_{\widetilde{\boldsymbol{w}}}(\tau) = A_{\boldsymbol{w}}(-\tau)$ and $-\tau = 2(-m-1)+1$ for $\tau = 2m+1$, we have

$$A_{\widetilde{\boldsymbol{w}}}(\tau) = \begin{cases} A_{\boldsymbol{y}}(-k), & \text{if } \tau = 2k,\ k \neq 2q, \\ 4, & \text{if } \tau = 4q, \\ 4y_{k+1} + 4y_{-k} - 4, & \text{if } \tau = 2k+1. \end{cases}$$

Remark 2. Because of the relationship between $\mathbf{w}$ and $\widetilde{\mathbf{w}}$ listed in Lemma 1, in the later proof we always can get the corresponding properties of $\widetilde{\mathbf{w}}$ when we get some properties of $\mathbf{w}$. Due to the limitation of space, we will only give the relevant proof for $\mathbf{w}$.

Remark 3. In [11], Krengel and Ivanov used DHM sequences defined only for C, but Lemma 1 is true also when we use DHM for $C^{(0)} = C \cup \{0\}$(see [2]).

3 2-adic complexity of sequences

Let $\mathbf{w}$ be a binary sequence of period $8q$ defined in (2). For study of 2-adic complexity of our sequence we need to consider $\gcd(S_w(2), 2^{8q}-1)$, where $S_w(X) = \sum_{i=0}^{8q-1} w_i X^i \in \mathbb{Z}[X]$ and $S_{\tilde{w}}(X) = \sum_{i=0}^{8q-1} \tilde{w}_i X^i \in \mathbb{Z}[X]$. If d is a prime divisor of $\gcd(S_w(2), 2^{8q}-1)$ then d divides $\gcd(S_w(2), 2^{4q}-1)$ or $\gcd(S_w(2), 2^{4q}+1)$. Our study includes three steps. First, we find $\gcd(S_w(2), 2^{4q}+1)$.

Proposition 4. *With notations as above, we have*

(i) $\gcd(S_w(2), 2^{4q}+1) = 1$*;*

(ii) $\gcd(S_{\tilde{w}}(2), 2^{4q}+1) = 1$.

Proof. Let $T_w(x) = \sum_{i=0}^{8q-1}(-1)^{w_i} X^i \in \mathbb{Z}[X]$. By [16] we have

$$-2S_w(X)T_w(X^{-1}) \equiv 8q + \sum_{\tau=1}^{8q-1} A_{\mathbf{w}}(\tau)X^\tau - T(X^{-1})\sum_{i=0}^{8q-1} X^i \pmod{X^{8q}-1}.$$

From the latest congruence we obtain

$$-2S_w(2)T_w(2^{-1}) \equiv 8q + \sum_{\tau=1}^{8q-1} A_{\mathbf{w}}(\tau)2^\tau \pmod{2^{8q}-1}.$$

Since $\mathbf{y}$ is obtained by the concatenation of $\mathbf{z}$, it follows that $y_k = y_{k+2q} = z_k$ and $A_{\mathbf{y}}(k) = A_{\mathbf{y}}(k+2q) = 2A_{\mathbf{z}}(k)$ for $k = 0, 1, \ldots, 2q-1$. Hence by Lemma 1 we see that

$$\begin{aligned} -2S_w(2)T_w(2^{-1}) &\equiv 8q - 8(2^{8q}-1)/3 + 4\cdot 2^{4q} + 2(1+2^{4q})\sum_{k=1}^{2q-1} A_{\mathbf{z}}(k)2^{2k} \\ &\quad + 8(1+2^{4q})\sum_{k=0}^{2q-1}(z_{-k}+z_{k+1})2^{2k} \pmod{2^{8q}-1}. \quad (3) \end{aligned}$$

Let r be an odd prime divisor of $S_w(2)$ and $2^{4q}+1$. Then by (3) r divides $8q-4$. Since $2^{4q} \equiv -1 \pmod r$, it follows that $2^{8q} \equiv 1 \pmod r$ and the order 2 modulo r equals 8 or $8q$. In the second case $8q$ divides $r-1$ and we obtain the contradiction. If order 2 modulo r is equal to 8 then r divides 255, i.e., $r = 17$. Further, since $8q-4 = 4p^m$ it follows that $p = 17$. In this case $p^m \equiv 1 \pmod{16}$ and $q \equiv 1 \pmod 8$. We again have the contradiction. Thus, $\gcd(S_w(2), 2^{4q}+1) = 1$. □

Immediately, we can get the following corollary from the proof of Proposition 4.

Corollary 5. *With notations as above. We have that*

$$-2S_w(2)T_w(2^{-1}) \equiv 8q - 16(2^{4q}-1)/3 + 4\sum_{t=1}^{2q-1} A_z(t)2^{2t} + 4 + 16\sum_{t=0}^{2q-1}(z_{-t}+z_{t+1})2^{2t} \pmod{2^{4q}-1},$$

$$-2S_{\tilde{w}}(2)T_{\tilde{w}}(2^{-1}) \equiv 8q - 16(2^{4q}-1)/3 + 4\sum_{t=1}^{2q-1} A_z(-t)2^{2t} + 4 + 16\sum_{t=0}^{2q-1}(z_{-t}+z_{t+1})2^{2t} \pmod{2^{4q}-1}.$$

3.1 Subsidiary lemmas

Now we make some preparations to finish the proof. The generating polynomial of following auxiliary sequence will be heavily used sequel. Let $\overline{\mathbf{z}}$ be a binary sequence defined by (1) for $(k+2, j+2, l+2) \pmod 4$. Put, by definition, $S_{\bar{z}}(x) = \sum_{i=0}^{2q-1} \bar{z}_i x^i$. Since $q \equiv 5 \pmod 8$, it follows that $-1 \in D_2$ and $\sum_{t=0}^{2q-1} z_{-t} 2^{2t} = S_{\bar{z}}(4)$. Further,

$$16 \sum_{t=0}^{2q-1} z_{t+1} 2^{2t} = 4 \sum_{t=0}^{2q-1} z_{t+1} 2^{2(t+1)} = 4S_z(4) - 4z_0 + 4z_{2q} 2^{4q}.$$

Thus,

$$16 \sum_{t=0}^{2q-1} (z_{-t} + z_{t+1}) 2^{2t} \equiv 16 S_{\bar{z}}(4) + 4S_z(4) \pmod{2^{4q} - 1}.$$

Lemma 6. *Let $S_w(X)$ and $S_{\tilde{w}}(X)$ be the generation polynomials of $\boldsymbol{w}$ and $\widetilde{\boldsymbol{w}}$ respectively. Then we have the following statements:*

(i) $S_w(2) \equiv 0 \pmod 3$ and $S_w(2) \not\equiv 0 \pmod 9$ (The conclusion also holds for $S_{\tilde{w}}(2)$);

(ii) Let d be a divisor of $2^{4q} - 1$. If d divides $S_w(2)$ and $d \neq 3$ then $S_z(4) \equiv -1 \pmod d$ and vice versa (The conclusion still holds if we substitute $S_{\tilde{w}}(2)$ for $S_w(2)$ and $S_{\bar{z}}(4)$ for $S_z(4)$);

(iii) $S_w(2) \not\equiv 0 \pmod 5$ (The conclusion also holds for $S_{\tilde{w}}(2)$).

Proof. By definition $S(2) = S_y(4) + 2S_x(4) = (1 + 4^{2q}) S_z(4) + 2S_x(4)$, where $S_y(4) = \sum_{i=0}^{4q-1} y_i 4^i$ and $S_x(4) = \sum_{i=0}^{4q-1} x_i 4^i$. Further, $S_x(4) = \sum_{i=0}^{2q-1} x_i 4^i + \sum_{i=0}^{2q-1} x_{i+2q} 4^{i+2q}$. Since $x_{i+2q} = 1 - x_i$ for $i \neq 0$, it follows that

$$S_x(4) = 4^{2q}(4^{2q} - 1)/3 + 4^{2q} + (1 - 4^{2q}) \sum_{i=0}^{2q-1} x_i 4^i.$$

Thus,

$$S_w(2) = (1 + 4^{2q}) S_z(4) + 2 \left(4^{2q}(4^{2q} - 1)/3 + 4^{2q} + (1 - 4^{2q}) \sum_{i=0}^{2q-1} x_i 4^i \right). \qquad (4)$$

Hence, $S_w(2) \equiv 2wt(S_z(x)) + 2(2q+1) \pmod 3$, where $wt(S_z(x))$ is a weight of $S_z(x)$. Since $wt(S_z(x)) = q - 1$, it follows that $S_w(2) \equiv 0 \pmod 3$. Further, $2^{8q} - 1 = (2^q - 1)(2^q + 1)(2^{2q} + 1)(2^{4q} + 1)$ and 3 divides only $2^q + 1$. It is clear that 9 does not divide $2^q + 1$ for $q \equiv 5 \pmod 8$. So, we obtain the first statement of this lemma.

(ii) By (4) we see that $S_w(2) \equiv 2S_z(4) + 2 \pmod d$. This proves (ii).

(iii) The third statement of this lemma follows from (ii). □

Then we can directly get the following corollary.

Corollary 7. *If d divides* $\gcd(2^{4q}-1, S_w(2))$ *with* $d \neq 3$ *and* r *divides* $\gcd(2^{4q}-1, S_{\tilde{w}}(2))$ *with* $r \neq 3$ *then*

$$-2S_w(2)T_w(2^{-1}) \equiv 8q + 4\sum_{t=1}^{2q-1} A_z(t)2^{2t} + 16S_{\bar{z}}(4) \pmod{d}. \tag{5}$$

$$-2S_{\tilde{w}}(2)T_{\tilde{w}}(2^{-1}) \equiv 8q + 4\sum_{t=1}^{2q-1} A_z(-t)2^{2t} - 12 + 4S_z(4) \pmod{r}. \tag{6}$$

By Proposition 4 and Lemmas 6 it is sufficient to study $\gcd\left((16^q-1)/15, S_w(2)\right)$ and $\gcd\left((16^q-1)/15, S_{\tilde{w}}(2)\right)$ to complete the proof of Theorem 10.

Further, we will use generalized "Gauss periods" and "Gauss sums" presented in [26]. Only here, we will employ them with values from $Z_{2^{4q}-1}$ and not from $Z_{2^{2q}-1}$ as it was done in [26].

Let $\zeta_t = \sum_{i\in D_t} 16^i$, $t = 0,1,2,3$. If $t = \phi^{-1}(a,b)$ then $t \equiv qa + (q+1)b \pmod{2q}$. Thus, $\sum_{t\in\{0\}\times D_i} 4^t \equiv \sum_{b\in D_i} 4^{(q+1)b} \pmod{4^{2q}-1}$. Let $e = \mathrm{ind}_g 2 \pmod 4$. For any $b \in D_i$ there to exist $c \in D_{i-e}$ such that $b \equiv 2c \pmod q$. Then $(q+1)b \equiv 2(q+1)c \pmod{2q}$ and $\sum_{t\in\{0\}\times D_i} 4^t \equiv \sum_{c\in D_{i-e}} 16^{(q+1)c} \equiv \sum_{c\in D_{i-e}} 16^c \pmod{4^{2q}-1}$. Similarly, we get that $\sum_{t\in\{1\}\times D_i} 2^{2t} \equiv 4^q \sum_{b\in D_{i-e}} 16^c \pmod{4^{2q}-1}$.

Thus we see that

$$\sum_{t\in\{0\}\times D_i} 2^{2t} \equiv \zeta_{i-e} \pmod{4^{2q}-1} \text{ and } \sum_{t\in\{1\}\times D_i} 2^{2t} \equiv 4^q\zeta_{i-e} \pmod{4^{2q}-1}, \tag{7}$$

and $\zeta_0 + \zeta_1 + \zeta_2 + \zeta_3 = (16^q-1)/15 - 1$.

Let $\omega_i = \sum_{t\in D_i\cup D_{i+2}} 16^t$, $i = 0,1$. Then $\omega_0 = \zeta_0 + \zeta_2$, $\omega_1 = \zeta_1 + \zeta_3$ and $\omega_0 + \omega_1 \equiv -1 \pmod{(16^q-1)/15}$.

Denote by χ a quadratic character of $\mathbb{F}_q$ and put by definition $H = \omega_0 - \omega_1 = \sum_{i\in\mathbb{F}_q^*} 16^i\chi(i)$. Then as in [26] we have the following statement.

Lemma 8. *(i)* $H^2 \equiv q - (16^q-1)/15 \pmod{16^q-1}$*;*

(ii) $(2w_i+1)^2 \equiv q \pmod{(16^q-1)/15}$ *for* $i = 0,1$.

Proof. (i) The first statement we can obtain in the same way as in [26]

(ii) From (i) we obtain $H^2 \equiv q \pmod{(16^q-1)/15}$ and $2w_i + 1 = \pm H \pmod{(16^q-1)/15}$. □

Remark 9. Of course, we can study $S(4)$ in the same way that $S(2)$ is investigated in [26]. But we will obtain our results in a more simple way.

3.2 Main result

Our main result is the following statement.

Theorem 10. *Let* $\boldsymbol{w}$ *be a binary sequence with period* $8q$ *defined by* (2)*. Then we have* $\bar{\Phi}(\boldsymbol{w}) = 8q - 2$.

To prove our theorem we will show $\gcd(S_w(2), 2^{8q}-1) = \gcd(S_{\tilde{w}}(2), 2^{8q}-1) = 3$. Then

$$\Phi(\mathbf{w}) = \Phi(\widetilde{\mathbf{w}}) = \left\lfloor \log_2\left(\frac{2^{8q}-1}{3}+1\right)\right\rfloor = 8q-2.$$

According to Lemma 6, we see that 3 divides $\gcd(16^q-1, S_w(2))$ and $\gcd(16^q-1, S_{\tilde{w}}(2))$, also 5 does not divide $\gcd(16^q-1, S_w(2))$ and $\gcd(16^q-1, S_{\tilde{w}}(2))$. In this subsection, let always d be a prime divisor of $\gcd(16^q-1, S(2))$, $d>5$ and r be a prime divisor of $\gcd(16^q-1, S_{\tilde{w}}(2))$, $r>5$. Further, we need to consider a few cases.

Lemma 11. *Let* $\boldsymbol{z}$ *be a sequence defined by* (1) *for* $q = 1+4b^2$, $(k,j,l) = (1,0,3); (0,1,2)$ *and let* $\boldsymbol{w}$ *be a binary sequence of period* $8q$ *defined by* (2)*. Then* $\gcd(16^q-1, S(2))) = 3$ *and* $\gcd(16^q-1, S_{\tilde{w}}(2))) = 3$.

Proof. First, we study the $\gcd(16^q-1, S_w(2))$. For $(k,j,l) = (1,0,3)$ according to [2] the autocorrelation of $\mathbf{z}$ is defined as

$$A_{\mathbf{z}}(\tau) = \begin{cases} -2, & \text{if } \tau \bmod 2 = 0, \tau \bmod q \neq 0 \text{ or } \tau \bmod 2 = 1, \tau \bmod q \in D_1 \cup D_3, \\ 2, & \text{if } \tau \bmod 2 = 1, \tau \bmod q = 0 \text{ or } \tau \bmod 2 = 1, \tau \bmod q \in D_0 \cup D_2. \end{cases}$$

Then by (7) we obtain that

$$\sum_{t=1}^{2q-1} A_{\mathbf{z}}(t)2^{2t} \equiv -2\left(\sum_{i=0}^{3}\zeta_i + 4^q(\zeta_{1-e}+\zeta_{3-e})\right) + 2\cdot 4^q + 2\cdot 4^q(\zeta_{0-e}+\zeta_{2-e}) \pmod{4^{2q}-1}.$$

Note that $e=1$ or 3. Then by Lemma 6, we get

$$4\sum_{t=1}^{2q-1} A_{\mathbf{z}}(t)2^{2t} \equiv 8 - 8\cdot 4^q H + 8\cdot 4^q \pmod{d}.$$

We see that $(k+2, j+2, l+2) \pmod 4 = (3,2,1)$ for $(k,j,l) = (1,0,3)$. Thus,

$$S_z(4) + S_{\bar{z}}(4) = \sum_{i=1, i\neq q}^{2q-1} 4^i = (4^{2q}-1)/3 - 1 - 4^q.$$

Again by Lemma 6 we obtain $S_{\bar{z}}(4) \equiv -4^q \pmod{d}$. So, by (5) we have

$$-2S_w(2)T_w(2^{-1}) \equiv 8q + 8 - 8\cdot 4^q H - 8\cdot 4^q \pmod{d}. \tag{8}$$

Suppose d is a prime divisor of 4^q-1; then by (8) we have $q \equiv H \pmod{d}$ and by Lemma 8.(i) $q^2 \equiv q \pmod{d}$. Thus, $q \equiv 1 \pmod{d}$. Here q divides $d-1$, this is impossible.

Suppose d divides 4^q+1; then by (8) we have $q+2 \equiv -H \pmod{d}$ or by Lemma 8 $q^2+3q+4 \equiv 0 \pmod{d}$. Since d is a prime, it follows that $d = 1+2nq, n \in \mathbb{N}$. Then

$$0 \equiv 2n(q^2+3q+4) \equiv -q-3+8n \pmod{d}$$

and $-q-3+8n$ is even. Thus, $-q-3+8n = 2m(1+2nq)$ for $m \in \mathbb{Z}$. It is clear that $m=0$. Hence $8n = q+3$ and $d = 1+q(q+3)/4$.

Here $2^{2q} \equiv -1 \pmod{d}$ and $2^{4q} \equiv 1 \pmod{d}$. Thus, the order of 2 modulo d equals 4 or $4q$. In the first case $d=5$. This is impossible by Lemma 6. Thus $4q$ divides $d-1$ or 4 divides $(q+3)/4$. By condition $q = 1+4b^2$ and b is odd, then we have that $q \equiv 5 \pmod{32}$ and $(q+3)/4 \equiv 2 \pmod{8}$. We obtain the contradiction.

In this case, using (6) for $\tilde{w}$ we similarly get that

$$-2S_{\tilde{w}}(2)T_{\tilde{w}}(2^{-1}) \equiv 8q-4-8\cdot 4^q H + 4\cdot 4^q \pmod{r}.$$

Thus, we can get the desired conclusion for $\tilde{w}$ in the same way as before.

Now, let $(k,j,l)=(0,1,2)$. In this case, the autocorrelation of $\mathbf{z}$ is defined as [2]:

$$A_{\mathbf{z}}(\tau) = \begin{cases} -2, & \text{if } \tau \bmod 2 = 0, \tau \bmod q \neq 0 \text{ or } \tau \bmod 2 = 1, \tau \bmod q \in D_0 \cup D_2, \\ 2, & \text{if } \tau \bmod 2 = 1, \tau \bmod q = 0 \text{ or } \tau \bmod 2 = 1, \tau \bmod q \in D_1 \cup D_3. \end{cases}$$

Thus, by (7) we obtain

$$4\sum_{t=1}^{2q-1} A_{\mathbf{z}}(t)2^{2t} \equiv 8 + 8\cdot 4^q H + 8\cdot 4^q \pmod{d}.$$

We see that $(k+2, j+2, l+2) \pmod{4} = (2,3,0)$ for $(k,j,l) = (0,1,2)$. Hence, as earlier $S_{\tilde{z}}(4) \equiv -4^q \pmod{d}$. So, by (5) we have

$$-2S_w(2)T_w(2^{-1}) \equiv 8q + 8 - 8\cdot 4^q H - 8\cdot 4^q \pmod{d}.$$

Then we can get the result for $(k,j,l) = (0,1,2)$ as above. Thus, we derived the $\gcd(16^q-1, S_w(2)) = 3$. □

Lemma 12. *Let* $\boldsymbol{z}$ *be a sequence defined by* (1) *for* $p = a^2+4, b=1$*,* $(k,j,l) = (0,1,3), (0,2,1)$ *and let* $\boldsymbol{w}$ *be a binary sequence of period* $8q$ *defined by* (2)*. Then* $\gcd(16^q-1, S(2)) = 3$ *and* $\gcd(16^q-1, S_{\tilde{w}}(2)) = 3$*.*

Proof. For $p = a^2+4$ and $(k,j,l)=(0,1,3)$, through similar discussion to that in the proof of Lemma 11, we can get the following series of results:

$$\sum_{t=1}^{2q-1} A_{\mathbf{z}}(t)2^{2t} \equiv 2 - 2\cdot 4^q H + 2\cdot 4^q \pmod{d},$$
$$S_z(4) + S_{\tilde{z}}(4) \equiv (4^{2q}-1)/15 - 1 + 2\cdot 4^q\omega_0 \pmod{4^{2q}-1},$$
$$S_{\tilde{z}}(4) \equiv 2\cdot 4^q\omega_0 \pmod{d},$$

$$-2S_w(2)T_w(2^{-1}) \equiv 8q + 8 + 8\cdot 4^q + 4^q(24\omega_0 + 8\omega_1) \pmod{d}. \tag{9}$$

Suppose d is a prime divisor of 4^q-1; then by (9) we have $q \equiv -(2\omega_0+1) \pmod{d}$ and by Lemma 8. (iii) $q^2 \equiv q \pmod{d}$. Hence, $q \equiv 1 \pmod{d}$. This is impossible.

Suppose d is a prime divisor of 4^q+1; then by (9) we have $q+2 \equiv 2\omega_0 + 1 \pmod{d}$ and by Lemma 8 $q^2+3q+4 \equiv 0 \pmod{d}$. As earlier we see that this is impossible.

Similarly, let $(k, j, l) = (0, 2, 1)$. We get the following series results:

$$\begin{aligned}\sum_{t=1}^{2q-1} A_{\mathbf{z}}(t)2^{2t} &\equiv 2 + 2\cdot 4^q + 2\cdot 4^q H \pmod{r},\\ S_z(4) + S_{\tilde{z}}(4) &\equiv 2\omega_1 + 4(4^{2q}-1)/15 - 4^q \pmod{4^{2q}-1},\\ S_{\tilde{z}}(4) &\equiv 1 + 2\omega_1 - 4^q \pmod{d},\\ -2S_w(2)T_w(2^{-1}) &\equiv 8q + 24 + 8\cdot 4^q H - 8\cdot 4^q + 32\omega_1 \pmod{d}.\end{aligned}$$

In this case, we can get the desired conclusion in the same way as before.

So we complete the proof. □

Thus, Theorem 10 follows from Proposition 4 and Lemmas 11, 12.

Example 13. 1. Let $\mathbf{z}$ be defined by (1) for C, $(k, j, l) = (0, 1, 3)$ and $q = 5$. Then $\mathbf{z} = 0, 0, 0, 1, 0, 0, 1, 1, 1, 0$ and $\widetilde{\mathbf{z}} = 0, 1, 1, 1, 0, 0, 1, 0, 0, 0$ per period (here $g = 3$). We take APB sequences $\mathbf{x} = 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0$ [11]. Then
$\mathbf{w} = 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0$
and
$\widetilde{\mathbf{w}} = 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0$
per period. In this case, $\gcd(2^{8q}-1, S_w(2)) = 3$ and $\gcd(2^{8q}-1, S_{\tilde{w}}(2)) = 3$. Then $\bar{\Phi}(w) = 38$.

Remark 14. We can study in the same way the symmetric 2-adic complexity of sequences with the optimal autocorrelation magnitude when these sequences are obtained from almost perfect binary sequences and Ding-Helleseth-Martinsen sequences for $C^{(0)} = C \cup \{0\}$.

Acknowledgements

The authors wish to thank the anonymous reviewers for their very valuable comments that helped to improve the presentation and quality of this paper.

References

[1] C. Ding, T. Helleseth, K. Lam. Several classes of sequences with three-level autocorrelation. *IEEE Trans. Inf. Theory*, 45(7): 2606-2612, 1999.

[2] C. Ding, T. Helleseth, H. Martinsen. New families of binary sequences with optimal three-valued autocorrelation. *IEEE Trans. Inf. Theory*, 47(1): 428-433, 2001

[3] V. A. Edemskiy, A. B. Minin. Linear complexity of binary sequences with optimal autocorrelation magnitude of length. *MMPAM'2019. IOP Conf. Series: Journal of Physics: Conf. Series.* 1352, 012013, 2019.

[4] C. Fan. The linear complexity of a class of binary sequences with optimal autocorrelation. *Designs, Codes and Cryptography*, 86:2441-2450, 2018.

[5] H. Hu. Comments on "a new method to compute the 2-adic complexity of binary sequences". *IEEE Trans. Inform. Theory*, 60:5803-5804, 2014.

[6] G. Gong. Theory and applications of q-ary interleaved sequences. *IEEE Trans. Inform. Theory*, 41(2):400-411, 1995.

[7] H. Hu, D. Feng. On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences. *IEEE Trans. Inf. Theory*, 54(2): 874-883, 2008.

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

[9] A. Klapper, M. Goresky. Cryptanalysis based on 2-adic rational approxiamtion. *In: CRYPTO 1995, LNCS*, 963: 262-273, 1995.

[10] A. Klapper, M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *Journal of Cryptology*, 10: 111-147, 1997.

[11] E.I Krengel, P.V. Ivanov. Two costructions of binary sequences with optimal autocorrelationmagnitude. *Electron. Lett.*, 52: 1457-1459, 2016.

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

[13] N. Li, X. Tang. On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation/magnitude. *IEEE Trans. Inform. Theory*, 57:7597-7604, 2011.

[14] Y. Sun, H. Shen New binary sequences of length $4p$ with optimal autocorrelation magnitude, *Ars Combinatoria*, 89:255-262, 2008.

[15] Y. Sun, Q. Wang, T. Yan. The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation. *Cryptography and Communications*, 10 (3): 467-477, 2018.

[16] Y. Sun, T. Yan, Z. Chen. The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude, *Cryptogr. Commun.*. 2019, https://doi.org/10.1007/s12095-019-00411-4.

[17] W. Su, Y. Yang, C. Fan. New optimal binary sequences with period $4p$ via interleaving Ding-Helleseth-Lam sequences, *Designs, Codes and Cryptography*, 86:1329-1338, 2018.

[18] X. Tang, C. Ding. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value, *IEEE Trans. Inform. Theory*, 56(3):6398-6405, 2010.

[19] X. Tang, G. Gong. New constructions of binary sequences with optimal autocorrelation value/magnitude. *IEEE Trans. Inform. Theory*, 56(12):1278-1286, 2010.

[20] J. Wolfmann. Almost perfect autocorrelation sequences. *IEEE Trans. Inf. Theory*, 38(4):1412-1418, 1992.

[21] Z. Xiao, X. Zeng, Z. Sun. 2-Adic complexity of two classes of generalized cyclotomic binary sequences. *Internationl Journal of Foundations of Comput. Sci.*, 27 (7): 879-893, 2016.

[22] H. Xiong, L. Qu, C. Li. A new method to compute the 2-adic complexity of binary sequences. *IEEE Trans. Inform. Theory*, 60: 2399-2406, 2014.

[23] H. Xiong, L. Qu, C. Li. 2-Adic complexity of binary sequences with interleaved structure. *Finite Fields and Their Applications* , 33:14-28, 2015.

[24] M. Yang, L. Zhang, K. Feng. On the 2-adic complexity of a class of binary sequences of period $4p$ with optimal autocorrelation magnitude. https://arxiv.org/abs/1904.13012.

[25] S. Zhang, T. Yan. Linear Complexity and Autocorrelation of two Classes of New Interleaved Sequences of Period 2N. CoRR abs/1801.08664 (2018).

[26] L. Zhang, J. Zhang, M. Yang, K. Feng. On the 2-Adic Complexity of the Ding-Helleseth-Martinsen Binary Sequences. *in IEEE Trans. Inform. Theory*, 2020. DOI: 10.1109/TIT.2020.2964171.