On a Theorem of Kyureghyan and Pott

Minglong Qi · Shengwu Xiong

Received: date / Accepted: date

Abstract  In the paper of Gohar M. Kyureghyan and Alexander Pott (Designs, Codes and Cryptography, 29, 149-164, 2003), the linear feedback polynomials of the Sidel’nikov-Lempel-Cohn-Eastman sequences were determined for some special cases. When referring to that paper, we found that Corollary 4 and Theorem 2 of that paper are wrong because there exist many counterexamples for these two results. In this note, we give some counterexamples of Corollary 4 and Theorem 2 of that paper.

Keywords  linear feedback polynomial · linear complexity · the Sidel’nikov-Lempel-Cohn-Eastman sequences · Jacobsthal sums

Mathematics Subject Classification (2000)  94A55

1 Introduction

Let \( q \) be a prime power, \( \mathbb{F}_q \) be the finite field with \( q \) elements, and \( \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \). Let \( S = (s_0, s_1, s_2, \cdots) \) be a sequence each term of which is taken from \( \mathbb{F}_q \). Let \( N \) be a positive integer. The sequence \( S \) is said to be \( N \)-periodic if \( s_{i+N} = s_i \) for all \( i \geq 0 \). The \( N \)-periodic sequence \( S \) is denoted by \( S_N = (s_0, s_1, s_2, \cdots, s_{N-1}) \). Define \( S_N(x) \in \mathbb{F}_q[x] \) to be the polynomial

\[
S_N(x) = s_0 + s_1x + s_2x^2 + \cdots + s_{N-1}x^{N-1}.
\]

The linear complexity of \( S_N \) is defined to be the smallest positive integer, \( L \), such that there exist \( c_0 = 1, c_1, \cdots, c_L \in \mathbb{F}_q \) satisfying

\[
-a_i = c_1a_{i-1} + c_2a_{i-2} + \cdots + c_La_{i-L} \quad \text{for all} \quad L \leq i.
\]
It is clear that the linear complexity, $L$, of the sequence $S_N$, is the length of the shortest linear feedback register which generates the sequence. The polynomial
\[ c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_L x^L \]
is referred to as the linear feedback polynomial of the shortest linear feedback shift register that generates $S_N(x)$. It is well known \cite{1, 2}, that the linear feedback polynomial can be computed by
\[ c(x) = \frac{x^N - 1}{\gcd(S_N(x), x^N - 1)}. \] (1)
Hence, the linear complexity can be determined by
\[ L = N - \deg\left( \gcd(S_N(x), x^N - 1) \right). \] (2)

Let $q = df + 1$, and $\alpha$ be a primitive element of $F_q$. The cosets
\[ C_d^i = \{ \alpha^{kd+i} | 0 \leq k \leq f-1 \}, i = 0, \cdots, d-1 \]
are called the cyclotomic classes of order $d$ with respect to $F_q$. Note that the cyclotomic classes $C_d^i$ depend on the choice of the primitive element $\alpha$. It is clear that
\[ F_q^* = \bigcup_{i=0}^{d-1} C_d^i. \]
The constants
\[ (l, m)_d = | (C_d^l + 1) \cap C_d^m | \]
are called the cyclotomic numbers of order $d$ with respect to $F_q$.

Let $q = p^m$ where $p$ is an odd prime, and $m$ a positive integer. If $p \equiv 1 \pmod{4}$, then $q$ can be represented by the Diophantine equation $q = x^2 + 4y^2$. If $\gcd(x, q) = 1, x \equiv 1 \pmod{4}$, the representation is called the proper representation of $q$.

The quadratic character of $F_q^*$ is defined by
\[ \eta(\beta) = \begin{cases} 1 & \text{if } \beta \equiv \gamma^2 \text{ for some } \gamma \in F_q^* \\ 0 & \text{if } \beta = 0 \\ -1 & \text{otherwise.} \end{cases} \]

Let $a \in F_q^*$, and $n \in \mathbb{N}$. Based on the quadratic character of $F_q^*$, two types of Jacobsthal sums \cite{2, 3} are defined by
\[ I_n(a) = \sum_{c \in F_q^*} \eta(c^n + a), \]
\[ H_n(a) = \sum_{c \in F_q^*} \eta(c) \eta(c^n + a). \] (3)
Recall that $\alpha$ is a primitive element of $F_q$. The Sidel'nikov-Lempel-Cohn-Eastman sequence $S_q = (s_0, s_1, \ldots, s_{q-2})$ of period $q - 1$ over $F_2$ is defined by
\[
s_i = \begin{cases} 
1 & \text{if } \eta(\alpha^i + 1) = -1 \\
0 & \text{otherwise.} 
\end{cases}
\]
(4)

Let $LC_q$ denote the linear complexity of $S_q$ over $F_2$ and
\[
S_q(x) = \sum_{i=0}^{q-2} s_i x^i \in F_2[x].
\]
(5)

Then, the linear feedback polynomial of $S_q$ is
\[x^{q-1} + 1 \quad \text{gcd}(x^{q-1} + 1, S_q(x))\]
and the linear complexity
\[LC_q = q - 1 - \deg(\text{gcd}(x^{q-1} + 1, S_q(x))).\]

In this paragraph, when we say Corollary 4, Lemma 5, and Theorem 2, we refer to those of [4]. In [4], G. Kyureghyan and A. Pott determined the linear complexity and the linear feedback polynomials of the Sidel’nikov-Lempel-Cohn-Eastman sequences for some special cases. When studying the similar problems and referring to that paper, we found that Corollary 4 and Theorem 2 are wrong because there exist many counterexamples. It can be easily seen that the cause making Corollary 4 and Theorem 2 wrong is that, the necessary and sufficient conditions of Corollary 4 and Theorem 2 are not equivalent to the negation of the condition of Lemma 5, from which Corollary 4 and Theorem 2 follow. The rest of the note is structured as follows: in second section, some counterexamples of Corollary 4 and Theorem 2 are provided, and the correction of them is given by readopting the negation of the condition of Lemma 5. In section 3, a brief conclusion is given.

2 Counterexamples of Corollary 4 and Theorem 2 and Correction of the Two Results

Next lemma strengthens an observation in [5].

Lemma 1 (Lemma 4 in [4]) (a) If $q \equiv 5 \pmod{8}$, then $x + 1$ divides $\text{gcd}(x^{q-1} + 1, S_q(x))$, and $(x + 1)^2$ does not divide $\text{gcd}(x^{q-1} + 1, S_q(x))$ over $F_2$.
(b) If $q - 1 = 8f \equiv 0 \pmod{8}$, then $(x + 1)^i, i \geq 2$ divides $\text{gcd}(x^{q-1} + 1, S_q(x))$ over $F_2$. Moreover, $(x + 1)^d$ does not divide $\text{gcd}(x^{q-1} + 1, S_q(x))$ over $F_2$ if $f + y/2$ is odd, where $y$ is determined from the proper representation of $q = x^2 + 4y^2$.

Next lemma is a key one in [4], that gives the necessary and sufficient condition by which the factor $g(x) = x^{d-1} + x^{d-2} + \cdots + 1 \in F_2[x]$ divides $\text{gcd}(x^{q-1} + 1, S_q(x)) \in F_2[x]$, where $q = df + 1$. 


Lemma 2 (Lemma 5 in [4]) If \( q = df + 1, d \) is odd, 4 divides \( f \) and \( \alpha \) is a primitive element of \( \mathbb{F}_q \), then \( \gcd(x^{q^d-1} + 1, S_q(x)) \in \mathbb{F}_2[x] \) is divisible by

\[
g(x) = x^{d-1} + x^{d-2} + \cdots + 1 \in \mathbb{F}_2[x]
\]

if and only if

\[
I_d(1) \equiv -d \pmod{4}
\]

and

\[
I_d(\alpha^{-t}) \equiv 0 \pmod{4} \quad \text{for all } 1 \leq t \leq d - 1.
\]

Lemma 2 (Lemma 5 in [4]) was rigorously proved. Through the proving process, the authors of [4] discovered a new polynomial over \( \mathbb{F}_2 \), namely,

\[
S_2(x) = \sum_{t=0}^{d-1} c_t x^t \in \mathbb{F}_2[x],
\]

where

\[
c_t = \sum_{k=0}^{f-1} s_{t+kd}, 0 \leq t \leq d - 1.
\]

The authors of [4] deduced the necessary and sufficient condition of Lemma 2 is equivalent to \( S_2(x) = 0 \).

The negation of the necessary and sufficient condition of Lemma 2 is stated by

\[
I_d(1) \not\equiv -d \pmod{4} \quad \text{or} \quad I_d(\alpha^{-t}) \not\equiv 0 \pmod{4} \quad \text{for some } \beta \in \{\alpha^{-t} | 1 \leq t \leq d - 1\}.
\]

(6)

Clearly, by Lemma 2, \( g(x) = x^{d-1} + x^{d-2} + \cdots + 1 \in \mathbb{F}_2[x] \) does not divide \( \gcd(x^{q^d-1} + 1, S_q(x)) \in \mathbb{F}_2[x] \) if only if Eq. (6) holds. Meanwhile, the authors of [4] gave another necessary and sufficient condition, by which \( g(x) \in \mathbb{F}_2[x] \) is excluded from being a factor of \( \gcd(x^{q^d-1} + 1, S_q(x)) \in \mathbb{F}_2[x] \). We will show that that condition is not equivalent to the condition stated in Eq. (6). In many counterexamples, both the condition of Corollary 4 in [4] and the condition of Lemma 2 hold at the same time, which is absurd. According to the authors of [4], next corollary is an important one of Lemma 2:

Corollary 1 (Corollary 4 in [4]) If \( q = 2^k r + 1, k \geq 2, r \) is an odd prime and 2 is a primitive root modulo \( r \), then

\[
\gcd(x^{q^i-1} + 1, S_q(x)) = (x + 1)^i \quad \text{for some } i \geq 1
\]

if and only if

\[
I_r(a) \not\equiv -r \pmod{4} \quad \text{for some } a \in \langle \alpha^r \rangle
\]

or

\[
I_r(a) \not\equiv 0 \pmod{4} \quad \text{for some } a \notin \langle \alpha^r \rangle,
\]

where \( \alpha \) is a primitive element of \( \mathbb{F}_q \).
Remark that the condition of Eq. (7) is not always equivalent to that of Eq. (6). Sometimes, the condition of Lemma 2 and that of Corollary 1 hold for a same case, which leads to the absurd situation: \( \gcd(x^{q-1} + 1, S_q(x)) \in \mathbb{F}_2[x] \) has the factor \( g(x) = x^{r-1} + x^{r-2} + \cdots + 1 \in \mathbb{F}_2[x] \) because the condition of Lemma 2 is true, and \( \gcd(x^{q-1} + 1, S_q(x)) = (x + 1)^i \) for some \( i \geq 1 \) because the condition of Eq. (7) hold too. This situation is well illustrated by the following counterexamples:

**Counterexample 1** Let \( q = 2^4 \cdot 3 + 1 = 7^2, \alpha \) be a primitive element of \( \mathbb{F}_{7^2} \). Then,

\[
I_1(1) = 0, \\
(\alpha_3^i + 1) \quad (mod 4) \quad for all \quad \beta \in \{\alpha^3\}, \quad and \\
I_1(\beta) \equiv 0 \quad (mod 4) \quad for all \quad \beta \in \mathbb{F}_{7^2}^* \backslash \{\alpha^3\}.
\]

It means that there are some \( \beta \in \{\alpha^3\} \) such that \( I_1(\beta) + 3 \equiv 2 \quad (mod 4) \), i.e., \( I_1(\beta) \equiv -1 \not\equiv -3 \quad (mod 4) \). Hence, the condition of Corollary 1 is true, and it should be expected that \( \gcd(x^{48} + 1, S_{49}(x)) = (x + 1)^i \) for some \( i \geq 1 \). However, \( \gcd(x^{48} + 1, S_{49}(x)) = (x + 1)^6(x^2 + x + 1)^2 \), meaning that Corollary 1 is wrong. On the other hand, the condition of Lemma 2 is true for this case, which further demonstrates that the condition of Eq. (6) is not equivalent to that of Eq. (7).

**Counterexample 2** Let \( q \in \{193 = 2^6 \cdot 3 + 1, 769 = 2^8 \cdot 3 + 1, 12289 = 2^4 \cdot 3 + 1\}, \alpha \) be a primitive element of \( \mathbb{F}_q \). Then,

\[
I_1(1) = 0, \\
(\alpha_3^i + 1) \quad (mod 4) \quad for all \quad \beta \in \{\alpha^3\}, \quad and \\
I_1(\beta) \equiv 0 \quad (mod 4) \quad for all \quad \beta \in \mathbb{F}_q^* \backslash \{\alpha^3\}.
\]

Clearly, the condition of Corollary 1 is satisfied. However, \( \gcd(x^{48} + 1, S_q(x)) = (x + 1)^i(x^2 + x + 1)^2 \not\equiv (x + 1)^i \) for some \( i \geq 1 \), meaning that Corollary 1 is wrong. Note that the condition of Lemma 2 holds too, which is absurd.

Counterexample 1 and 2 show that Corollary 1 is wrong. This is because the necessary and sufficient condition of Corollary 1 stated by Eq. (7), is not always equivalent to the negation of the condition of Lemma 2 expressed by Eq. (6). The correct version of Corollary 1 is given by

**Corollary 2 (Correction of Corollary 4 in [4])** If \( q = 2^k r + 1, k \geq 2, r \) is an odd prime and \( 2 \) is a primitive root modulo \( r \), then

\[
\gcd(x^{q-1} + 1, S_q(x)) = (x + 1)^i \quad for \quad some \quad i \geq 1
\]

if and only if

\[
I_i(1) \not\equiv -r \quad (mod 4) \quad or \\
I_i(\beta) \not\equiv 0 \quad (mod 4) \quad for \quad some \quad \beta \in \{\alpha^i \mid 1 \leq i \leq d - 1\},
\]

where \( \alpha \) is a primitive element of \( \mathbb{F}_q \).
Proof We have
\[ x^{q-1} + 1 = x^{2^r} + 1 = (x^r + 1)^{2^i} = (x^r - 1 + x^r - 2 + \cdots + 1)^{2^i}. \]

From the assumption of Corollary 2, \( g(x) = x^{r-1} + x^{r-2} + \cdots + 1 \) is irreducible over \( \mathbb{F}_2 \). By Lemma 2, \( g(x) = x^{r-1} + x^{r-2} + \cdots + 1 \in \mathbb{F}_2[x] \) is not a factor of \( \gcd(x^{q-1} + 1, S_q(x)) \in \mathbb{F}_2[x] \). Hence, \( \gcd(x^{q-1} + 1, S_q(x)) \) must only have the factor \((x + 1)^i\) for some \( 0 \leq i \leq 2^k \). Note that for \( q - 1 \equiv 0 \pmod{4} \), \( x + 1 \) is always a factor of \( S_q(x) \) \( [5] \). Therefore,
\[ \gcd(x^{q-1} + 1, S_q(x)) = (x + 1)^i \text{ where } 1 \leq i \leq 2^k. \]

\( \square \)

Theorem 2 of \([4]\) was deduced from Lemma 4 and Corollary 4 of the same paper. Since Corollary 4 of \([4]\) is wrong, Theorem 2 of \([4]\) is wrong too. We give the correct version of Theorem 2 of \([4]\) by readopting the condition expressed in Eq. (6) which excludes \( g(x) = x^{r-1} + x^{r-2} + \cdots + 1 \in \mathbb{F}_2[x] \) from being a factor of \( \gcd(x^{q-1} + 1, S_q(x)) \) by Corollary 2.

**Theorem 1 (Correction of Theorem 2 in \([4]\))** Let \( q = 2^k r + 1, k \geq 1, r \) be an odd prime and \( q = x^2 + 4 y^2 \) be the proper representation of \( q \). If \( 2 \) is a primitive root modulo \( r \), then the feedback polynomial of \( S_q \) over \( \mathbb{F}_2 \) is
\[ \frac{x^{q-1} + 1}{x + 1} \text{ if } k = 2 \text{ and } \frac{x^{q-1} + 1}{(x + 1)^i} \text{ for some } i \geq 2 \text{ if } k \geq 3, \]
(where \( i \leq 4 \) if \( \frac{2^{k-1} + 1}{2} \) is odd) if and only if
\[ I_r(1) \not\equiv -r \pmod{4} \text{ or } I_r(\beta) \not\equiv 0 \pmod{4} \text{ for some } \beta \in \{ \alpha^{-t} | 1 \leq t \leq r - 1 \}, \]
where \( \alpha \) is a primitive element of \( \mathbb{F}_q \).

**Proof** Follows from Lemma \([1]\) and Corollary \([2]\) \( \square \)

3 Conclusion

In this note, we show that Corollary 4 and Theorem 2 of \([4]\) are wrong by some counterexamples. We point out that the necessary and sufficient condition of Corollary 4 of \([4]\) is not equivalent to the negation of the condition of Lemma 5 in \([4]\), which is the cause making Corollary 4 and Theorem 2 of \([4]\) wrong. And finally, we correct Corollary 4 and Theorem 2 of \([4]\) by readopting the condition stated in Eq. (6).
References

1. Cusick T.W., Ding C., Renvall A.: Stream Ciphers and Number Theory, North-Holland Publishing Co., Amsterdam (1998).
2. Lidl R., Niederreiter H.: Finite Fields, Encyclopedia of Mathematics and Its Applications, 2nd ed., Cambridge University Press, Vol. 20 (1997).
3. Berndt B.C., Evans R.J., Williams K.S.: Gauss and Jacobi sums, John Wiley & Sons Inc., New York (1998).
4. Kyureghyan G.M., Pott A.: On the Linear Complexity of the Sidelnikov-Lempel-Cohn-Eastman Sequences. Designs, Codes and Cryptography, 29, 149-164 (2003).
5. Helleseth T., Yang K.: On binary sequences of period $n = p^m - 1$ with optimal autocorrelation, In (Helleseth T., Kumar P., Yang K., eds.), Proceedings of SETA01, 209-217 (2002).