IOP Conf. Series: Journal of Physics: Conf. Series **1352** (2019) 012014 doi:10.1088/1742-6596/1352/1/012014

About the values of generating polynomials of cyclotomic classes

V A Edemskiy and A S Tsurina

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

E-mail: Vladimir.Edemsky@novsu.ru

Abstract. The trace representation of sequences is a powerful tool for the analysis and for the design of pseudorandom sequences. Z. Dai et al. (2011) reduce the problem of determining trace representation of series of binary eth power residue sequences to that of determining the values of generating polynomials of cyclotomic classes. We derive the values of generating polynomials of cyclotomic classes of order $4, 6, 8$ and consequently solve three problems pointed by Z. Dai et al. In fact, we study the discrete Fourier transform of cyclotomic sequences of order 4, 6, 8.

1. Introduction

A trace representation of a sequence gives very specific insight on its "easy" generation using one or more linear feedback shift registers for engineering applications [12]. In their paper, Z. Dai et al. [2] investigated the trace representation and the linear complexity of series of binary eth power residue sequences of period p generalizing results from [3, 4, 5, 6]. Authors reduce the problem of determining trace representation of above-mentioned sequences to that of determining the values of generating polynomials of cyclotomic classes of order e. In conclusion authors pointed out four open problems. In this paper we solve first three of these problems.

First of all, we briefly repeat the basic definitions from [2] and some general information. Let $p = 1 + ef$ be an odd prime for $e = 4,6,8$, and let $\mathbb{F}_p$ be the finite field of order p which we identify with the set of integers $\{0,1, \dots, p-1\}$. Denote by u a generator of the cyclic group $\mathbb{F}_p^* = \{1,2, \dots, p-1\}$. Put, by definition $H_e = \{x^e | x \in F_p^*\}$. Then H_e consists of the eth power residues $\bmod p$ and cosets $u^i H_e, 0 \le i \le e-1$ form a partition $\mathbb{F}_p^*$, i.e. $\mathbb{F}_p^* = \cup_{i=0}^{e-1} u^i H_e$. Cosets $u^i H_e$ are also called the cyclotomic classes of order e with respect to p [7].

The following definitions were presented in [2].

Definition 1 (Generating Polynomials of Cosets): Given $k \in \mathbb{F}_p^*$, the generating polynomial of the coset kH_e is defined as

$$\sum_{i \in kH_e} x^i (\bmod (x^p - 1))$$

which will be denoted by $c_k(x)$.

Let α be a primitive root pth power of unity in $\mathbb{F}_{2^n}$, where n is an order of $2 \bmod p$. It is well known that it exists [8]. Let $\beta = \alpha^j, 1 \le j \le p-1$.

Definition 2 (e-Tuples and Matrices Related to Cosets): The e elements $c_{u^i}(\beta)$,$0 \le i < e$, which are values of $c_{u^i}(x)$ at $x = \beta$, will be ordered as an e-tuple over $\mathbb{F}_{2^n}$ according to any given generator u of $\mathbb{F}_p^*$, and written as a vector

$$c_u(\beta) = (c_{u^0}(\beta), c_{u^1}(\beta), \dots, c_{u^{e-1}}(\beta)).$$

Let $d = gcd((p-1)/n, e)$. The values $c_u(\beta)$ were obtained in [2] for $e = 4$, $p \equiv 5 \pmod 8$, and $e = 6$, $p \equiv 7 \pmod{12}$, and $e = 8$, $p \equiv 9 \pmod{16}$, $d = 8$. But for all that in the first and the second cases for $d = 1$ were offered two possible e-tuples. At the end of the article, the authors noted that some problems remain open.

1. When $e = 4$ or $e = 6$ with $d = 1$, any $c_u(\beta)$ must be equivalent to only one of two possible e-tuples (not both). It is not known so far whether any one can be ruled out completely, or both occur as p changes.

2. Computations of $c_u(\beta)$ for the values of d other than those covered in the subsection for $e = 4$ or $e = 8$ also remain as future research.

3. So do those for the case $e = 6$ with even f.

4. So do the cases with $e > 12$.

In this paper, we propose a solution of the first three problems. For computing the values $c_{u^i}(\alpha)$ we will use the method considered in [9].

2. The values of generating polynomials of cyclotomic classes

Let $(m,k)_e$ be cyclotomic numbers of order e [10]. The following lemma was proved in [11].

Lemma 1. Let $k, j = 0,1, \dots, e-1$. Then in $\mathbb{F}_{2^n}$ we have

$$c_{u^j}(\alpha)c_{u^k}(\alpha) = \sum_{i=0}^{m-1} (k-j,i)_e c_{u^{i+j}}(\alpha) + \delta.$$

Here $\delta = \begin{cases} 1, if\ f \equiv 1 \pmod 2, |j-k| = e/2, \\ 0, else. \end{cases}$

2.1. Case $e = 4$

Let $e = 4$. Since $p \equiv 1 \pmod 4$, p can be expressed as $p = x^2 + 4y^2; x \equiv 1 \pmod 4$, here y is two-valued, depending on the choice of the primitive root.

Denote by $ind_u 2$ a discrete logarithm of 2 base u in the field $\mathbb{F}_p$. If $f = (p-1)/4$ is odd then $ind_u 2 \equiv 1 \pmod 2$ [12].

Theorem 1. Let $p = x^2 + 4y^2$, $e = 4$, and f is an odd and a generator u of $\mathbb{F}_p^*$ such that $2 \in uH_4$. Then $c_u(\alpha) = (\theta, \theta^2, \theta^4, \theta^8)$ where $\theta^4 + \theta^3 + \theta^2 + \theta + 1 = 0$ if $x \equiv 1 \pmod 8$ and $\theta^4 + \theta^3 + 1 = 0$ if $x \equiv 5 \pmod 8$.

Proof. By Theorem 11 [2] it follows that $c_u(\alpha) = (\theta, \theta^2, \theta^4, \theta^8)$ where θ is a root of $f(x)$, where either $f(x) = x^4 + x^3 + x^2 + x + 1$ or $f(x) = x^4 + x^3 + 1$(but not both).

We consider the cyclotomic numbers of order 4 when f is an odd. By [10]

$$(1,0)_4 = (1,1)_4 = (p - 3 - 2x)/16,$$
$$(1,2)_4 = (p + 1 + 2x + 8y)/16, \quad (1,3)_4 = (p + 1 + 2x - 8y)/16. \tag{1}$$

By assumption of Theorem 1, $x = 1 + 4s$ and $f = 1 + 2t$ where s, t are integers. Using Lemma 1 and (1) we obtain that

$$c_{u^0}(\alpha)c_{u^1}(\alpha) = sc_{u^0}(\alpha) + sc_{u^1}(\alpha) + (1+t)c_{u^2}(\alpha) + tc_{u^3}(\alpha)$$

or $\theta^3 = s\theta + s\theta^2 + (1+t)\theta^4 + t\theta^8$. Hence, $t \equiv 1 \pmod 2$ and

$$\theta^3 = s\theta + s\theta^2 + \theta^8. \tag{2}$$

The conclusions of this theorem then follow from (2).

We note that if θ is a root of $f(x) = x^4 + x^3 + x^2 + x + 1$ then $\theta + 1$ is a root of $f(x) = x^4 + x^3 + 1$ and vice versa.

The values of $c_u(\alpha)$ when f is an even were obtained in [9]. If f is an even then $y \equiv 0 \pmod 2$ [12]. Further, without loss of generality, we can choose α such that $c_{u^0}(\alpha) \neq 0$.

(i) $c_u(\alpha) = (1,0,0,0)$ if $x \equiv 1 \pmod 8$ and $y \equiv 0 \pmod 4$;

(ii) $c_u(\alpha) = (1,1,0,1)$ if $x \equiv 5 \pmod 8$ and $y \equiv 0 \pmod 4$;

(iii) $c_u(\alpha) = (\omega, 1, 1+\omega, 1)$ if $x \equiv 1 (\mathrm{mod}\ 8)$ and $y \equiv 2 (\mathrm{mod}\ 4)$. Here ω satisfies the equation $\omega^2 + \omega + 1 = 0$;

(iv) $c_u(\alpha) = (\omega, 0, 1+\omega, 0)$ if $x \equiv 5 (\mathrm{mod}\ 8)$ and $y \equiv 2 (\mathrm{mod}\ 4)$.

2.2. *Case* $e = 6$

Let $e = 6$. Since $p \equiv 1 (\mathrm{mod}\ 6)$, p can be expressed as $p = A^2 + 3B^2; A \equiv 1 (\mathrm{mod}\ 3)$. The cyclotomic numbers of order 6 can be found through A and B, where $B \equiv -ind_u 2 (\mathrm{mod}\ 3)$ [10].

First of all, we study a case when f is an odd and $d = 1$. Since $d = 1$, we see that $ind_u 2 \equiv \pm 1 (mod\ 6)$. Without loss of generality, we can assume that $2 \in uH_6$.

Theorem 2. Let $p = A^2 + 3B^2$, $e = 6$, and f is an odd and a generator u of $\mathbb{F}_p^*$ such that $2 \in uH_6$ (in this case $B \equiv 2 (\mathrm{mod}\ 3)$). Then $c_u(\alpha) = (\vartheta, \vartheta^2, \vartheta^4, \vartheta^8, \vartheta^{16}, \vartheta^{32})$ where $\vartheta^6 + \vartheta^5 + \vartheta^2 + \vartheta + 1 = 0$ if $B \equiv 11 (\mathrm{mod}\ 12)$ and $\vartheta^6 + \vartheta^5 + 1 = 0$ if $B \equiv 5 (\mathrm{mod}\ 12)$.

Proof. By [2] it follows that $c_u(\alpha) = (\vartheta, \vartheta^2, \vartheta^4, \vartheta^8, \vartheta^{16}, \vartheta^{32})$. Here ϑ is a root of $f(x)$, where either $f(x) = x^6 + x^5 + x^2 + x + 1$ or $f(x) = x^6 + x^5 + 1$(but not both).

Let $A = 1 + 3k, B = 2 + 3l, k, l \in \mathbb{Z}$. In this case $p = 13 + 6k + 9k^2 + 36l + 27l^2$. Since $p \equiv 7 (\mathrm{mod}\ 12)$, it follows that k, l are odds, i.e., $A = 4 + 6t$, $B = 5 + 6s$; $s, t \in \mathbb{Z}$. Further, $2 \notin H_2$, hence $p \equiv \pm 3 (\mathrm{mod}\ 8)$[12]. So, $t \equiv 0 (\mathrm{mod}\ 2)$. From this we can establish that [10]

$$(1,0)_6 \equiv 1 + s (\mathrm{mod}\ 2), \quad (1,1)_6 \equiv s (\mathrm{mod}\ 2),$$
$$(1,2)_6 = (1,5)_6 \equiv 1 (\mathrm{mod}\ 2), \quad (1,3)_6 = (1,4)_6 \equiv 0 (\mathrm{mod}\ 2). \tag{3}$$

In this case, by Lemma 1 and (3) we obtain that

$$c_{u^0}(\alpha) c_{u^1}(\alpha) = (1+s) c_{u^0}(\alpha) + s c_{u^1}(\alpha) + c_{u^2}(\alpha) + c_{u^5}(\alpha)$$

or

$$\vartheta^3 = (1+s)\vartheta + s\vartheta^2 + \vartheta^4 + \vartheta^{32}.$$

To conclude the proof, it remains to note that $\vartheta^{32} = \vartheta^4 + \vartheta^3 + \vartheta^2$ if ϑ is a root of $f(x) = x^6 + x^5 + x^2 + x + 1$ and $\vartheta^{32} = \vartheta^4 + \vartheta^3 + \vartheta$ if ϑ is a root of $f(x) = x^6 + x^5 + 1$. Theorem 2 is proved.

We note that if ϑ is a root of $f(x) = x^6 + x^5 + x^2 + x + 1$ then $\vartheta + 1$ is a root of $f(x) = x^6 + x^5 + 1$ and vice versa.

Further, we investigate the values $c_u(\alpha)$ for an even value of f. Let $p = A^2 + 3B^2, A \equiv 1 (\mathrm{mod}\ 3)$. We consider two cases, when $ind_u 2 \equiv 0 (\mathrm{mod}\ 3)$ and $ind_u 2 \not\equiv 0 (\mathrm{mod}\ 3)$.

1. Suppose $ind_u 2 \equiv 0 (\mathrm{mod}\ 3)$; then $B \equiv 0 (\mathrm{mod}\ 3)$ and $A = 1 + 6t, B = 6s, t, s \in \mathbb{Z}$ and $p \equiv 1 - 24t + 36s (\mathrm{mod}\ 72)$. In this case, we obtain by [10]

$$(3,0)_6 \equiv (3,3)_6 \equiv s (\mathrm{mod}\ 2),$$
$$(3,1)_6 \equiv (3,2)_6 \equiv (3,4)_6 \equiv (3,5)_6 \equiv s + t (\mathrm{mod}\ 2). \tag{4}$$

From [2] it follows that in this case $c_u(\alpha) = (1,0,0)$ for $e = 3$. Since $H_3 = H_6 \cup u^3 H_6$, we see by Lemma 1 and (4) that

$$c_{u^0}(\alpha) + c_{u^3}(\alpha) = 1, \quad c_{u^0}(\alpha) c_{u^3}(\alpha) = s,$$
$$c_{u^j}(\alpha) + c_{u^{j+3}}(\alpha) = 0, \quad c_{u^j}(\alpha) c_{u^{j+3}}(\alpha) = s + t, j = 1,2.$$

From this we can establish that:

(i) $c_u(\alpha) = (1,0,0,0,0,0)$ if $A \equiv 1 (\mathrm{mod}\ 12)$ and $B \equiv 0 (\mathrm{mod}\ 12)$;

(ii) $c_u(\alpha) = (1,1,1,0,1,1)$ if $A \equiv 7 (\mathrm{mod}\ 12)$ and $B \equiv 0 (\mathrm{mod}\ 12)$;

(iii) $c_u(\alpha) = (\omega, 1, 1, \omega + 1, 1, 1)$ if $A \equiv 1 (\mathrm{mod}\ 12)$ and $B \equiv 6 (\mathrm{mod}\ 12)$. Here ω is a root of $x^2 + x + 1$ as before;

(iv) $c_u(\alpha) = (\omega, 0, 0, \omega + 1, 0, 0)$ if $A \equiv 7 (\mathrm{mod}\ 12)$ and $B \equiv 6 (\mathrm{mod}\ 12)$.

2. If $ind_u 2 \equiv 2 (\mathrm{mod}\ 3)$ then $ind_{u^{-1}} 2 \equiv 1 (\mathrm{mod}\ 3)$. Hence, without loss of generality, we can assume that $ind_u 2 \equiv 1 (\mathrm{mod}\ 3)$. Since $B \equiv 2 (\mathrm{mod}\ 3)$, we obtain that $A = 1 + 6t, B = 2 + 6s, t, s \in \mathbb{Z}$ and $p \equiv 13 - 24t + 36s (\mathrm{mod}\ 72)$. In this case, for $e = 3$ by [2] we have that $c_u(\alpha) = (\varepsilon, \varepsilon^2, \varepsilon^2 + \varepsilon + 1)$, where ε is a root of $f(x) = x^3 + x^2 + 1$.Therefore, using the formulae for computation of the cyclotomic numbers and Lemma 1, we can write

$$c_{u^0}(\alpha)+c_{u^3}(\alpha)=\varepsilon,\quad c_{u^0}(\alpha)c_{u^3}(\alpha)=t\varepsilon^2+(1+t+s)(\varepsilon^2+\varepsilon+1),$$
$$c_{u^1}(\alpha)+c_{u^4}(\alpha)=\varepsilon^2,\quad c_{u^1}(\alpha)c_{u^4}(\alpha)=(1+t+s)\varepsilon+t(\varepsilon^2+\varepsilon+1),$$
$$c_{u^2}(\alpha)+c_{u^5}(\alpha)=\varepsilon^2+\varepsilon+1,\ c_{u^2}(\alpha)c_{u^5}(\alpha)=t\varepsilon+(1+t+s)\varepsilon^2.$$

Under the condition of $2\in uH_6\cup u^4H_6$ we have that:

(i) $c_u(\alpha)=(\varepsilon,0,\varepsilon^2+\varepsilon+1,0,\varepsilon^2,0)$ if $A\equiv 1 \pmod{12}$ and $B\equiv 8 \pmod{12}$;

(ii) $c_u(\alpha)=(\varepsilon+1,1,\varepsilon^2+\varepsilon,1,\varepsilon^2+1,1)$ if $A\equiv 7 \pmod{12}$ and $B\equiv 8 \pmod{12}$;

(iii) $c_u(\alpha)=(\gamma,\gamma^2,\gamma^4,\gamma^8,\gamma^{16},\gamma^{32})$ if $A\equiv 1 \pmod{12}$ and $B\equiv 2 \pmod{12}$. Here γ is a root of $x^2+\varepsilon x+\varepsilon^4$ or $f(x)=x^6+x^5+x^4+x+1=(x^2+\varepsilon x+\varepsilon^4)(x^2+\varepsilon^2x+\varepsilon)(x^2+\varepsilon^4x+\varepsilon^2)$;

(iv) $c_u(\alpha)=(\gamma+1,\gamma^2+1,\gamma^4+1,\gamma^8+1,\gamma^{16}+1,\gamma^{32}+1)$ if $A\equiv 7 \pmod{12}$ and $B\equiv 2 \pmod{12}$. Here $\gamma+1$ is a root of $f(x)=x^6+x^5+x^4+x^2+1=(x^2+\varepsilon x+\varepsilon^2)(x^2+\varepsilon^2x+\varepsilon^4)(x^2+\varepsilon^4x+\varepsilon)$.

So, in this section we determine all the values of generating polynomials of cyclotomic classes of order six. For Hall's sextic sequence these values were studied in [13].

2.3. Case $e=8$

Let $e=8$ and $p=1+8f$. Then $p=x^2+4y^2=a^2+2b^2; x\equiv a\equiv 1 \pmod 4$ where x,a,y,b are integers. The formulae for cyclotomic numbers depend on the values f,y. There exist four cases [10, 13]. We consider only case when f is odd.

2.3.1. Let f be an odd and $y\equiv 0 \pmod 4$. If $y\equiv 0 \pmod 4$ then $y=4g, g\in\mathbb{Z}$. In this case from our definitions and Section 1 it follows that

$$c_{u^j}(\alpha)+c_{u^{j+4}}(\alpha)=1, j=0,1,3 \ and\ c_{u^2}(\alpha)+c_{u^6}(\alpha)=0. \quad (5)$$

Since f is odd, under the condition of $y=4g$ we have $x=5+8h, a=1+8s, b=2+4t, h,s,t\in\mathbb{Z}$ and $p\equiv 25+16h+64g \pmod{128}$. By [10] we obtain that

$$(4,0)_8=(4,4)_8=g,\quad (4,1)_8=(4,5)_8=1+g+h,$$
$$(4,2)_8=(4,6)_8=(4,3)_8=(4,7)_8=1+g+h.$$

By Lemma 1 and (5), using the formulae for cyclotomic numbers of order eight we obtain that

$$c_{u^j}(\alpha)+c_{u^{j+4}}(\alpha)=1\ and\ c_{u^j}(\alpha)c_{u^{j+4}}(\alpha)=g+1, j=0,1,3.$$

So, $c_{u^j}(\alpha), c_{u^{j+4}}(\alpha)\in\{0,1\}$ if $g\equiv 1 \pmod 2$, and $c_{u^j}(\alpha), c_{u^{j+4}}(\alpha)\in\{\omega,\omega+1\}$ if $g\equiv 0 \pmod 2$.

Similarly, we get that

$$c_{u^2}(\alpha)=c_{u^6}(\alpha)\ and\ c_{u^2}(\alpha)c_{u^6}(\alpha)=h+g.$$

Thus, $c_{u^2}(\alpha)=c_{u^6}(\alpha)=0$ if $h+g\equiv 0 \pmod 2$, and $c_{u^2}(\alpha)=c_{u^6}(\alpha)=1$ if $h+g\equiv 1 \pmod 2$. From this by Lemma 1 we can establish as in Theorem 2 that

(i) $c_u(\alpha)=(\omega,\omega+1,0,\omega+1,\omega+1,\omega,0,\omega)$ if $x\equiv 5 \pmod{16}$ and $y\equiv 0 \pmod 8$ and $b\equiv 2 \pmod 8$;

(ii) $c_u(\alpha)=(\omega,\omega,0,\omega,\omega+1,\omega+1,0,\omega+1)$ if $x\equiv 5 \pmod{16}$ and $y\equiv 0 \pmod 8$ and $b\equiv 6 \pmod 8$;

(iii) $c_u(\alpha)=(\omega,\omega+1,1,\omega+1,\omega+1,\omega,1,\omega)$ if $x\equiv 13 \pmod{16}$ and $y\equiv 0 \pmod 8$ and $b\equiv 2 \pmod 8$;

(iv) $c_u(\alpha)=(\omega,\omega,1,\omega,\omega+1,\omega+1,1,\omega+1)$ if $x\equiv 13 \pmod{16}$ and $y\equiv 0 \pmod 8$ and $b\equiv 6 \pmod 8$;

(v) $c_u(\alpha)=(1,1,1,0,0,0,1,1)$ if $x\equiv 5 \pmod{16}$ and $y\equiv 4 \pmod 8$ and $b\equiv 2 \pmod 8$;

(vi) $c_u(\alpha)=(1,1,1,1,0,0,1,0)$ if $x\equiv 5 \pmod{16}$ and $y\equiv 4 \pmod 8$ and $b\equiv 6 \pmod 8$;

(vii) $c_u(\alpha)=(1,0,0,0,0,1,0,1)$ if $x\equiv 13 \pmod{16}$ and $y\equiv 4 \pmod 8$ and $b\equiv 2 \pmod 8$;

(viii) $c_u(\alpha)=(1,1,0,1,0,0,0,0)$ if $x\equiv 13 \pmod{16}$ and $y\equiv 4 \pmod 8$ and $b\equiv 6 \pmod 8$.

2.3.2. Let f be an odd and $y\equiv 2 \pmod 4$. In this case $y=2+4g, g\in\mathbb{Z}$ and $2\in u^2H_8\cup u^6H_8$. Without loss of generality, we can assume that $2\in u^2H_8$. For $y=2+4g$ we see that $p\equiv 41+16h \pmod{128}$, $x=5+8h, a=5+8s, b=4t, h,s,t\in\mathbb{Z}$ and $h+s\equiv 1 \pmod 2$.

In this case from results of Section 1 we have that

$$c_{u^0}(\alpha)+c_{u^4}(\alpha)=\omega,\quad c_{u^1}(\alpha)+c_{u^5}(\alpha)=0. \quad (6)$$

Likewise, using Lemma 1 and the formulae for cyclotomic numbers of order eight we obtain as before that

$$\begin{aligned} c_{u^0}^2(\alpha) &= g c_{u^2}(\alpha) + (1+g) c_{u^6}(\alpha), \\ c_{u^0}(\alpha) c_{u^4}(\alpha) &= (1+h)(\omega+1) + 1, \\ c_{u^1}(\alpha) c_{u^5}(\alpha) &= \omega + h + t + g + 1. \end{aligned} \tag{7}$$

Hence, if $2 \in u^2 H_8$ then $g \equiv 0 \pmod 2$, i.e., $y \equiv 2 \pmod 8$. Denote by η a root of the polynomial $x^2 + \omega x + \omega$. From (6) and (7) with similar arguments as above we obtain the following results:

(i) $c_u(\alpha) = (\eta, \omega+1, \omega\eta+\omega, \omega, \omega+\eta, \omega+1, \omega\eta+1, \omega)$ if $x \equiv 5 \pmod{16}$ and $y \equiv 2 \pmod 8$, and $b \equiv 4 \pmod 8$;

(ii) $c_u(\alpha) = (\eta, \omega, \omega\eta+\omega, \omega+1, \omega+\eta, \omega, \omega\eta+1, \omega+1)$ if $x \equiv 5 \pmod{16}$ and $y \equiv 2 \pmod 8$, and $b \equiv 0 \pmod 8$;

(iii) $c_u(\alpha) = (\eta+1, \omega+1, \omega\eta+\omega+1, \omega, \omega+\eta+1, \omega+1, \omega\eta, \omega)$ if $x \equiv 13 \pmod{16}$ and $y \equiv 2 \pmod 8$, and $b \equiv 0 \pmod 8$;

(iv) $c_u(\alpha) = (\eta+1, \omega, \omega\eta+\omega+1, \omega+1, \omega+\eta+1, \omega, \omega\eta, \omega+1)$ if $x \equiv 13 \pmod{16}$ and $y \equiv 2 \pmod 8$, and $b \equiv 4 \pmod 8$.

It is easy to see that $x^4 + x^3 + 1 = (x^2 + \omega x + \omega)(x^2 + (\omega+1)x + \omega + 1)$, i.e. η is a root of $x^4 + x^3 + 1$.

The case when *f* is even can be studied in the same way as for odd *f*.

3. Conclusion

We derive the values of generating polynomials of cyclotomic classes of order $4, 6, 8$, and find the solutions of three open problems pointed out by *Z.* Dai et al. [2]. Using these values and the results from [2] we can easily investigate the linear complexity and the trace representation of all binary sequences obtained from cyclotomic classes of order four, six or eight. Our method can be useful to calculate the values of generating polynomials of cyclotomic classes of order twelve. But, from our results, it follows that for $e = 12$ (or $e > 12$) we will have a lot of different cases depending on the values of f, x, y, A, B and indexes 2, 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] Dai Z, Gong G, Song H-Y and Ye D 2011 *IEEE Tran. Inform. Theory* **57 (3)** 1530–1547
[3] Kim J H and Song H Y 2001 *Designs, Codes, Cryptogr.* **24 (3)** 343–348
[4] Kim J H, Song H Y and Gong G 2003 *Mathematical Properties of Sequences and Other Related Structures* ed J S No, H Y Song et al. (Boston, MA: Kluwer) 23–32
[5] Lee H K, No J S, Chung H, Yang K, Kim J H and Song H Y 1997 *Proc. APCC'97. APCC* 536–540
[6] No J S, Lee H K, Chung H, Song H Y and Yang K 1996 *IEEE Tran. Inform. Theory* **42 (11)** 2254–2255
[7] Cusick T, Ding C and Renvall A 1998 *Stream Ciphers and Number Theory* (North-Holland Publishing Co. Amsterdam)
[8] Lidl R and Niederreiter H 1983 *Finite Fields* (Addison-Wesley)
[9] Edemskii V A 2010 *Discret. Math. Appl.* **20 (1)** 75–84; translation from *Diskretn. Mat.* **22 (4)** 74–82
[10] Ding C 2015 *Codes from Difference Sets* (World Scientific)

[11] Hall M 1975 *Combinatorial Theory* (Wiley New York)
Ireland K and Rosen M 1982 *Classical Introduction to Modern Number Theory* (Springer, Berlin)
[12] Ye R 2013 *Proc. 3rd Intern. Conf. on Electric and Electronics* 116–118
[13] Lehmer E 1995 *Pacific J. Math.* 5103–118