UDC 512.624

**R. Popovych** (Nat. Univ. „Lviv Polytechnic")

# SHARPENING OF THE EXPLICIT LOWER BOUNDS ON THE ORDER OF ELEMENTS IN FINITE FIELD EXTENSIONS BASED ON CYCLOTOMIC POLYNOMIALS

# ПІДСИЛЕННЯ ЯВНИХ НИЖНІХ ГРАНИЦЬ ДЛЯ ПОРЯДКІВ ЕЛЕМЕНТІВ У РОЗШИРЕННЯХ СКІНЧЕННИХ ПОЛІВ НА ОСНОВІ ЦИКЛОТОМІЧНИХ ПОЛІНОМІВ

We explicitly construct elements with high multiplicative order in any extensions of finite fields based on cyclotomic polynomials.

Явно побудовано елементи великого мультиплікативного порядку у будь-яких розширеннях скінченних полів на основі циклотомічних поліномів.

**1. Introduction.** It is well known that the multiplicative group of a finite field is cyclic [1, 2]. The problem of constructing efficiently a generator of the group for a given finite field is notoriously difficult in the computational theory of finite fields. That is why one considers less restrictive question: to find an element with high multiplicative order [2]. We are not required to compute the exact order of the element. It is sufficient in this case to obtain a lower bound on the order. High order elements are needed in several applications: cryptography, coding theory, pseudo random number generation, combinatorics.

Throughout this paper $F_q$ is a field of $q$ elements, where $q$ is a power of prime number $p$. $F_q^*$ is the multiplicative group of $F_q$. $|S|$ denotes the number of elements of finite set $S$. A partition of an integer $c$ is a sequence of such nonnegative integers $u_1,\dots,u_c$ that $\sum_{j=1}^{c} ju_j = c$. $U(c,d)$ denotes the number of partitions of $c$, for which $u_1,\dots,u_c \le d$. $\langle\delta\rangle$ denotes the group generated by $\delta$, and $G\times H$ — the direct product of groups $G$ and $H$. For a prime $k$, $\rho_k(l)$ is the highest power of $k$ dividing integer $l$.

Gao [3] gives an algorithm for constructing high order elements for many (conjecturally all) general extensions $F_{q^m}$ of finite field $F_q$. Voloch [4, 5] proposed another method for general extensions. For special finite fields, it is possible to construct elements which can be proved to have much higher orders. Extensions based on the Kummer or Artin – Schreier polynomials are considered in [6 – 8]. A generalization of the extensions is given in [9].

Extensions connected with a notion of Gauss period are considered in [10 – 12]. More precisely, the following extensions are constructed. Let $r = 2s+1$ be a prime number coprime with $q$. Let $q$ be a primitive root modulo $r$, that is the multiplicative order of $q$ modulo $r$ equals to $r-1$. Set $F_q(\theta) = F_{q^{r-1}} = F_q[x]/\Phi_r(x)$, where $\Phi_r(x) = x^{r-1} + x^{r-2} + \dots + x + 1$ is the $r$ th cyclotomic polynomial and $\theta = x(\mathrm{mod}\,\Phi_r(x))$. It is clear that the equality $\theta^r = 1$ holds. The ele-

ment $\beta = \theta + \theta^{-1}$ is called a Gauss period of type $((r-1)/2, 2)$. It generates normal base over $F_q$ [11].

It is shown in [10] that $\beta$ has high multiplicative order: at least $2^{\sqrt{r-1}-2}$. Bounds of such kind: explicit and for any $p$ and $r$, are of special interest in applications (particularly, cryptography). The bounds allow to compare simply different field extensions.

The bounds using partitions $U((r-3)/2, p-1)$ [11], $U(r-2, p-1)$ [12] or asymptotic bound $\exp\left(\left(\frac{2,5}{\sqrt{2}}\sqrt{1-\frac{1}{p}}+o(1)\right)\sqrt{r-1}\right)$ [11] do not allow to obtain a bound on the element order for fixed finite field. Explicit bounds in terms of $p$ and $r$ are derived in [12] from bounds in terms of partitions. However, such bounds are obtained only for $r \geq p^2+2$ and $r < p+2$. Important in applications case $p+2 \leq r < p^2+2$ remains not described.

That is why we give in this paper better comparatively with [10] explicit lower bounds for any $p$ and $r$ both on the order of element $\beta$ and similar form elements. To obtain the bounds we count solutions of a linear Diophantine inequality instead of counting partitions. Our main result is Theorem 2.

**2. Preliminaries.** Let $c, d$ be positive integers ($d \leq c$). Denote by $L(c,d)$ the set of solutions $(u_1, \ldots, u_c)$ of the following linear Diophantine inequality:

$$\sum_{j=1}^{c} j u_j \leq c, \tag{1}$$

with the condition $0 \leq u_1, \ldots, u_c \leq d$.

For the extension $F_q(\theta)$ we prove the following three lemmas.

**Lemma 1.** *Let $a$ be any non-zero element in the finite field $F_q$. If solutions $(u_1, \ldots, u_{r-2})$ and $(v_1, \ldots, v_{r-2})$ from $L(r-2, p-1)$ are distinct, then the products $\prod_{j=1}^{r-2}(\theta^j + a)^{u_j}$ and $\prod_{j=1}^{r-2}(\theta^j + a)^{v_j}$ are not equal.*

***Proof.*** We prove Lemma 1 by the way of contradiction. Assume that solutions $(u_1, \ldots, u_{r-2})$ and $(v_1, \ldots, v_{r-2})$ from the set $L(r-2, p-1)$ are distinct, and the products are equal:

$$\prod_{j=1}^{r-2}(\theta^j + a)^{u_j} = \prod_{j=1}^{r-2}(\theta^j + a)^{v_j}.$$

Since the polynomial $\Phi_r(x)$ is minimal polynomial for the element $\theta$, we write

$$\prod_{j=1}^{r-2}(x^j + a)^{u_j} = \prod_{j=1}^{r-2}(x^j + a)^{v_j} (\mathrm{mod}\, \Phi_r(x)).$$

As there are polynomials of degree $r-2 < \deg \Phi_r(x)$ on the left- and on the right-hand side of the equality, these polynomials are equal as polynomials over $F_q$, i.e.,

$$\prod_{j=1}^{r-2}(x^j+a)^{u_j} = \prod_{j=1}^{r-2}(x^j+a)^{v_j}. \tag{2}$$

Let $k$ be the smallest integer for which $u_k \neq v_k$ and, say $u_k > v_k$. After removing common factors on both sides of (2), we obtain

$$(x^k+a)^{u_k-v_k}\prod_{j=k+1}^{r-2}(x^j+a)^{u_j} = \prod_{j=k+1}^{r-2}(x^j+a)^{v_j}. \tag{3}$$

Denote the absolute term of the polynomial $\prod_{j=k+1}^{r-2}(x^j+a)^{u_j}$ by $b$. It is clear that $b \neq 0$. Then there is the term

$$(u_k - v_k)a^{u_k-v_k-1}bx^k$$

on the left-hand side of (3) with minimal nonzero power of $x$. Since $0 \le u_k, v_k \le p-1$, $u_k \neq v_k$, $a, b \neq 0$, the term is nonzero. And such term does not occur on the right-hand side, which makes the identity (3) impossible.

Lemma 1 is proved.

**Lemma 2.** *Let $a$ be such nonzero element in the finite field $F_q$ that $a^2 \neq -1$. If solutions $(u_1,\ldots,u_{(r-3)/2})$ and $(v_1,\ldots,v_{(r-3)/2})$ from $L((r-3)/2, p-1)$ are distinct, then the products $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j}$ and $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{v_j}$ are not equal.*

***Proof.*** Assume that solutions $(u_1,\ldots,u_{(r-3)/2})$ and $(v_1,\ldots,v_{(r-3)/2})$ from the set $L((r-3)/2, p-1)$ are distinct, and the products are equal:

$$\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j} = \prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{v_j}.$$

Then, analogously to the proof of Lemma 1, we obtain the following equality for polynomials of degree $r-3 < \deg \Phi_r(x)$:

$$\prod_{j=1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{u_j} = \prod_{j=1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{v_j}. \tag{4}$$

Let $k$ be the smallest integer for which $u_k \neq v_k$ and $u_k > v_k$. After removing common factors on both sides of (4), we have

$$[ax^{2k}+(a^2+1)x^k+a]^{u_k-v_k}\prod_{j=k+1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{u_j}=\prod_{j=k+1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{v_j}. \qquad (5)$$

Denote the absolute term for the polynomial $\prod_{j=k+1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{u_j}$ by $b$. Obviously $b\neq 0$. Applying the multinomial formula to $[ax^{2k}+(a^2+1)x^k+a]^{u_k-v_k}$, we obtain that there is the term

$$(u_k-v_k)(a^2+1)a^{u_k-v_k-1}bx^k$$

in the polynomial on the left-hand side of (5) with minimal nonzero power of $x$. Since $0\le u_k$, $v_k\le p-1$, $u_k\neq v_k$, $a^2\neq -1$, $a,b\neq 0$, the term is nonzero. And such term does not occur on the right-hand side, which leads to a contradiction.

Lemma 2 is proved.

**Lemma 3.** *Let $a$ be such nonzero element in the finite field $F_q$ that $a^2\neq 1$. If solutions $(u_1,\dots,u_{r-2})$ and $(v_1,\dots,v_{r-2})$ from $L((r-3)/2,p-1)$ are distinct, then the products $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}$ and $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{v_j}$ are not equal.*

***Proof.*** Assume that solutions $(u_1,\dots,u_{(r-3)/2})$ and $(v_1,\dots,v_{(r-3)/2})$ from the set $L((r-3)/2,p-1)$ are distinct, and the products are equal:

$$\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}=\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{v_j}.$$

Then, analogously to the proof of Lemma 1, we obtain the following equality for polynomials of degree $r-3<\deg\Phi_r(x)$:

$$\prod_{j=1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}=\prod_{j=1}^{(r-3)/2}[(ax^j+1)^{v_j}(x^j+a)^{u_j}. \qquad (6)$$

Let $k$ be the smallest integer for which $u_k\neq v_k$ and $u_k>v_k$. After removing common factors on both sides of (6), we obtain

$$(ax^k+1)^{u_k-v_k}\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}=(x^k+a)^{u_k-v_k}\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{v_j}(x^j+a)^{u_j}. \qquad (7)$$

Denote the absolute term for the polynomial $\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}$ by $b$, and the absolute term for the polynomial $\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{v_j}(x^j+a)^{u_j}$ by $c$. Obviously $b,c\neq 0$. Since absolute terms on both sides of (7) are equal, the identity $b=a^{u_k-v_k}c$ holds. As coefficients near

$x^k$ on both sides of (6) are equal, we have $(u_k - v_k)ab = (u_k - v_k)a^{u_k - v_k - 1}c$, which implies the identity $b = a^{u_k - v_k - 2}c$. Comparing the identities, we obtain $a^2 = 1$ — a contradiction to the lemma assumption $a^2 \neq 1$.

Lemma 3 is proved.

**3. Lower bounds based on a number of linear Diophantine inequality solutions.** All lower bounds on elements order in Theorem 1 below involve a number of solutions $(u_1, \ldots, u_c)$ of the linear Diophantine inequality (1), where $0 \le u_1, \ldots, u_c \le p-1$. We use for the proof of parts (a), (b), (c) of the theorem a technique similar to that in [10 – 12]. The idea was introduced by Gathen and Shparlinski [10], and developed in [11, 12]. We take a linear binomial of some power of $\theta$ and all conjugates of it, that also belong to the group generated by the binomial, and construct their distinct products. In this case, the conjugates are nonlinear binomials. To obtain the bounds we count solutions of a linear Diophantine inequality instead of counting integer partitions.

**Theorem 1.** *Let $e$ be any integer, $f$ be any integer coprime with $r$, $a$ be any nonzero element in the finite field $F_q$. Then*:

(a) $\theta^e(\theta^f + a)$ *has the multiplicative order at least* $\left|L(r-2, p-1)\right|$,

(b) $(\theta^{-f} + a)(\theta^f + a)$ *for* $a^2 \neq -1$ *has the multiplicative order at least* $\left|L((r-3)/2, p-1)\right|$ *and this order divides* $q^{(r-1)/2} - 1$,

(c) $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$ *for* $a^2 \neq 1$ *has the multiplicative order at least* $\left|L((r-3)/2, p-1)\right|$ *and this order divides* $q^{(r-1)/2} + 1$,

(d) $\theta^e(\theta^f + a)$ *for* $a^2 \neq \pm 1$ *has the multiplicative order at least* $\left|L((r-3)/2, p-1)\right|^2/2$.

***Proof.*** (a) First we show that $\theta^e(\theta^f + a)$ has the same order as $\theta^g(\theta + a)$, where $g \equiv ef^{-1} \pmod r$. Clearly the map, taking $\theta$ to $\theta^p$, is the Frobenius automorphism of the field $F_q(\theta)$. Since $q$ is primitive modulo $r$, the congruence $f \equiv q^m \pmod r$ holds for some integer $m$. As $q$ is a power of $p$, the map, sending $\theta$ to $\theta^f = \theta^{q^m}$, is a power of the Frobenius automorphism and, therefore, is also an automorphism of the field $F_q(\theta)$. Since the last examined automorphism takes $\theta^g(\theta + a)$ to $\theta^e(\theta^f + a)$, multiplicative orders of these elements coincide.

So, to prove (a), it is sufficient to show that $\theta^g(\theta + a)$ has the multiplicative order at least $\left|L(r-2, p-1)\right|$.

As $q$ is primitive modulo $r$, for each $j = 1, \ldots, r-2$, an integer $\alpha(j)$ exists such that $q^{\alpha(j)} \equiv (j \bmod r)$. The powers

$$\left(\theta^g(\theta + a)\right)^{q^{\alpha(j)}} = \theta^{gq^{\alpha(j)}}(\theta^{q^{\alpha(j)}} + a) = \theta^{gj}(\theta^j + a)$$

belong to the group $\langle \theta^g(\theta + a) \rangle$. For every solution from $L(r-2, p-1)$ we construct the following product:

$$\prod_{j=1}^{r-2}[\theta^{gj}(\theta^j+a)]^{u_j} = \theta^{g\sum_{j=1}^{r-2} ju_j}\prod_{j=1}^{r-2}(\theta^j+a)^{u_j} = \theta^{g(r-2)}\prod_{j=1}^{r-2}(\theta^j+a)^{u_j}$$

that also belong to the group. Note that all these products have the same factor $\theta^{g(r-2)}$. According to Lemma 1, if two solutions $(u_1,\dots,u_{r-2})$ and $(v_1,\dots,v_{r-2})$ from $L(r-2,p-1)$ are distinct, then the products $\prod_{j=1}^{r-2}(\theta^j+a)^{u_j}$ and $\prod_{j=1}^{r-2}(\theta^j+a)^{v_j}$ are not equal. Hence, the products $\theta^{g(r-2)}\prod_{j=1}^{r-2}(\theta^j+a)^{u_j}$ and $\theta^{g(r-2)}\prod_{j=1}^{r-2}(\theta^j+a)^{v_j}$, corresponding to distinct solutions, cannot be equal and the result follows.

(b) The order of the group $F^*_{q^{r-1}}$ equals to $q^{r-1}-1=(q^{(r-1)/2}-1)(q^{(r-1)/2}+1)$. Note that since $q$ is primitive modulo $r$, and $r$ is prime, the congruencies $q^{r-1}\equiv 1(\mathrm{mod}\, r)$ and $q^{(r-1)/2}\equiv -1(\mathrm{mod}\, r)$ are true. Then

$$[\theta^e(\theta^f+a)]^{q^{(r-1)/2}+1} = \theta^{e(q^{(r-1)/2}+1)}(\theta^{fq^{(r-1)/2}}+a)(\theta^f+a) = (\theta^{-f}+a)(\theta^f+a),$$

and so, the order of $(\theta^{-f}+a)(\theta^f+a)$ divides $q^{(r-1)/2}-1$. We show that $(\theta^{-f}+a)(\theta^f+a)$ generates the group of the order at least $\left|L((r-3)/2,p-1)\right|$. Indeed, since the field automorphism, taking $\theta$ to $\theta^f$, sends $(\theta^{-1}+a)(\theta+a)$ to $(\theta^{-f}+a)(\theta^f+a)$, multiplicative orders of these elements coincide. Hence, it is sufficient to prove that

$$(\theta^{-1}+a)(\theta+a) = \theta^{-1}(a\theta+1)(\theta+a)$$

has the multiplicative order at least $\left|L((r-3)/2,p-1)\right|$.

As $q$ is primitive modulo $r$, for $j=1,\dots,(r-3)/2$, an integer $\alpha(j)$ exists such that $q^{\alpha(j)}\equiv j(\mathrm{mod}\, r)$. The powers

$$[\theta^{-1}(a\theta+1)(\theta+a)]^{q^{\alpha(j)}} = \theta^{-j}(a\theta^j+1)(\theta^j+a)$$

belong to the group $\langle\theta^{-1}(a\theta+1)(\theta+a)\rangle$. For every solution from the set $L((r-3)/2,p-1)$, we construct the following product:

$$\prod_{j=1}^{(r-3)/2}[\theta^{-j}(a\theta^j+1)(\theta^j+a)]^{u_j} =$$

$$= \theta^{-\sum_{j=1}^{(r-3)/2} ju_j}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j} = \theta^{-(r-3)/2}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j}$$

that also belong to the group. Note that these products have the same factor $\theta^{-(r-3)/2}$. According

to Lemma 2, if two solutions from $L((r-3)/2, p-1)$ are distinct, then the products $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j}$ and $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{v_j}$ are not equal. Hence, the result follows.

(c) Since

$$[\theta^e(\theta^f+a)]^{q^{(r-1)/2}-1} = \theta^{e(q^{(r-1)/2}-1)}(\theta^{fq^{(r-1)/2}}+a)(\theta^f+a)^{-1} = \theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1},$$

the order of $\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}$ is a divisor of $q^{(r-1)/2}+1$. We show that $\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}$ generates the group of the order at least $\left|L((r-3)/2, p-1)\right|$. Indeed, since the field automorphism, taking $\theta$ to $\theta^f$, sends $\theta^{-2ef^{-1}}(\theta^{-1}+a)(\theta+a)^{-1}$ to $\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}$, multiplicative orders of these elements coincide. Hence, it is sufficient to prove that

$$\theta^{-2ef^{-1}}(\theta^{-1}+a)(\theta+a)^{-1} = \theta^t(a\theta+1)(\theta+a)^{-1},$$

where $t=-2ef^{-1}-1$, has the multiplicative order at least $\left|L((r-3)/2, p-1)\right|$.

As $q$ is primitive modulo $r$, for $j=1,\ldots,(r-3)/2$, an integer $\alpha(j)$ exists such that $q^{\alpha(j)} \equiv j \pmod r$. The powers

$$[\theta^t(a\theta+1)(\theta+a)^{-1}]^{q^{\alpha(j)}} = \theta^{jt}(a\theta^j+1)(\theta^j+a)^{-1}$$

belong to the group $\langle\theta^t(a\theta+1)(\theta+a)^{-1}\rangle$. For every solution from the set $L((r-3)/2, p-1)$, we construct the following product:

$$\prod_{j=1}^{(r-3)/2}[\theta^{jt}(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j} = \theta^{t\sum_{j=1}^{(r-3)/2} ju_j}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j} =$$

$$= \theta^{t(r-3)/2}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}$$

that also belong to the group. Note that these products have the same factor $\theta^{t(r-3)/2}$. According to Lemma 3 if two solutions from $L((r-3)/2, p-1)$ are distinct, then the products $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}$ and $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{v_j}$ are not equal. Hence, the result follows.

(d) Recall that the order of $F^*_{q^{r-1}}$ equals to $q^{r-1}-1=(q^{(r-1)/2}-1)(q^{(r-1)/2}+1)$. Factors $q^{(r-1)/2}-1$ and $q^{(r-1)/2}+1$ have the greatest common divisor 2, since their sum equals to $2q^{(r-1)/2}$. Consider the subgroup of $F^*_{q^{r-1}}$ generated by $\theta^e(\theta^f+a)$. This subgroup contains two subgroups: first one is generated by

$$w_1 = [\theta^e(\theta^f + a)]^{q^{(r-1)/2}+1} = (\theta^{-f} + a)(\theta^f + a),$$

and second one — by

$$w_2 = [\theta^e(\theta^f + a)]^{q^{(r-1)/2}-1} = \theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}.$$

According to part (b), the order of $w_1$ divides $q^{(r-1)/2} - 1$, and according to part (c), the order of $w_2$ divides $q^{(r-1)/2} + 1$.

Construct the element

$$w = \begin{cases} w_1^2 w_2 & \text{if} \quad \rho_2(q^{(r-1)/2} - 1) = 2, \\ w_1 w_2^2 & \text{if} \quad \rho_2(q^{(r-1)/2} + 1) = 2. \end{cases}$$

If $\rho_2(q^{(r-1)/2} - 1) = 2$, then $(q^{(r-1)/2} - 1)/2$ is odd and coprime with $q^{(r-1)/2} + 1$. Clearly the order of $w_1^2$ is a divisor of $(q^{(r-1)/2} - 1)/2$. Hence, in this case, $\langle z \rangle = \langle w_1^2 \rangle \times \langle w_2 \rangle$. Similar to the previous consideration, if $\rho_2(q^{(r-1)/2} + 1) = 2$, then $\langle z \rangle = \langle w_1 \rangle \times \langle w_2^2 \rangle$. In both cases, the order of $w$ is the product of the orders of $w_1$ and $w_2$ divided by 2. According to part (b) and part (c), the order of $w$, and so, the order of $\theta^e(\theta + a)$ is at least $\left|L((r-3)/2, p-1)\right|^2/2$.

Theorem 1 is proved.

***Corollary* 1.** *The Gauss period* $\beta$ *has the multiplicative order at least* $\left|L(r-2, p-1)\right|$ *and this order divides* $q^{(r-1)/2} - 1$.

***Proof.*** It follows from Theorem 1, part (a) that the multiplicative order of $\beta = \theta + \theta^{-1} = \theta^{-1}(\theta^2 + 1)$ is at least $\left|L(r-2, p-1)\right|$. Since

$$(\theta + \theta^{-1})^{q^{(r-1)/2}-1} = (\theta^{q^{(r-1)/2}} + \theta^{-q^{(r-1)/2}})(\theta + \theta^{-1})^{-1} = (\theta^{-1} + \theta)(\theta + \theta^{-1})^{-1} = 1,$$

the order of $\beta$ divides $q^{(r-1)/2} - 1$.

Corollary 1 is proved.

Let $a$ be any nonzero element in $F_q$. We use below the following denotations:

$$\gamma = (\theta^{-1} + a)(\theta + a)^{-1} \quad \text{and} \quad z = \begin{cases} \beta^2\gamma & \text{if} \quad \rho_2(q^{(r-1)/2} - 1) = 2, \\ \beta\gamma^2 & \text{if} \quad \rho_2(q^{(r-1)/2} + 1) = 2. \end{cases}$$

***Corollary* 2.** *The element* $z$ *for* $a^2 \neq 1$ *has the multiplicative order at least* $\left|L(r-2, p-1)\right|\left|L((r-3)/2, p-1)\right|/2$.

***Proof.*** According to Corollary 1, $\beta$ has the order that divides $q^{(r-1)/2}-1$ and is at least $|L(r-2,p-1)|$. According to Theorem 1, part (c) (if to put $e=2^{-1}(\mathrm{mod}\, r)$, $f=1$), $\gamma$ has the order that divides $q^{(r-1)/2}+1$ and is at least $|L((r-3)/2,p-1)|$. Analogously to the proof of Theorem 1, part (d), the order of $z$ is the product of the orders of $\beta$ and $\gamma$ divided by 2. Hence, the result follows.

Corollary 2 is proved.

**4. Explicit lower bounds on orders for any $p$ and $r$.** Explicit lower bounds on the orders of finite field elements in terms of $p$ and $r$ are of special interest in applications. That is why we count in this section a number of solutions of the linear Diophantine inequality to derive explicit lower bounds on the multiplicative orders of the examined elements $\theta^e(\theta^f+a)$ and $z$.

**Lemma 4.** *The number* $|L(c,d)|$ *of solutions of linear Diophantine inequality* (1) *with the condition* $0\le u_1,\dots,u_c\le d$, *is at least*

$$\begin{cases} (d+1)^{\sqrt{c/2}-2} & \text{if} \quad d=1,2, \\ 5^{\sqrt{c/2}-2} & \text{if} \quad d\ge 4. \end{cases}$$

***Proof.*** Let $\delta$, $1\le\delta\le d$, be an integer which we shall choose later. Take the biggest integer $\alpha$ such that $\sum_{i=1}^{\alpha} i\delta\le c$. Since

$$\sum_{i=1}^{\alpha} i\delta = \delta\alpha(\alpha+1)/2 < \delta(\alpha+1)^2/2,$$

we choose $\alpha$ from the inequality $\delta(\alpha+1)^2\le 2c$, that is $\alpha=\left\lfloor\sqrt{2c/\delta}\right\rfloor-1$. Clearly, if to take $u_i\in\{0,\dots,\delta-1\}$ for $i=0,\dots,\alpha$ and $u_i=0$ for $i=\alpha+1,\dots,c$, we obtain a solution of (1). The number of such solutions equals to $(\delta+1)^{\alpha}\ge(\delta+1)^{\sqrt{2c/\delta}-2}=(\delta+1)^{\sqrt{2c/\delta}}/(\delta+1)^2$.

To choose $\delta$, we find maximum of the numerator $f(\delta)=(\delta+1)^{\sqrt{2c/\delta}}$ of the last bound. Obviously $\delta=d$ in the case $d=1,2$.

So, we assume below that $d\ge 4$. Represent the numerator in the form $f(\delta)=$ $=\exp\left(\ln(\delta+1)\sqrt{2c/\delta}\right)$. Then we have

$$f'(\delta) = (\delta+1)^{\sqrt{2c/\delta}}\sqrt{2c/\delta}\left(\frac{1}{\delta+1}-\frac{\ln(\delta+1)}{2\delta}\right).$$

If to write $f'(\delta)=0$, then $\dfrac{1}{\delta+1}-\dfrac{\ln(\delta+1)}{2\delta}=0$. The value $3{,}92155<\delta_0<3{,}921555$ is a point

of function maximum. The nearest integer to maximum is $\delta = 4$. The function $f(\delta)$ monotonically decreases for $\delta \geq \delta_0$, and the denominator $(\delta+1)^2$ monotonically increases. Hence, we take $\delta = 4$ in this case, and the result follows.

Lemma 4 is proved.

Our main result is the following theorem that gives explicit lower bounds on the elements orders.

**Theorem 2.** *Let $q$ be a power of prime number $p$, $r = 2s+1$ be a prime number coprime with $q$, $q$ be a primitive root modulo $r$, $\theta$ generates the extension $F_q(\theta) = F_{q^{r-1}}$, $e$ be any integer, $f$ be any integer coprime with $r$, $a$ be any nonzero element in the finite field $F_q$. Then*:

(a) $\theta^e(\theta^f + a)$ *has the multiplicative order at least* $\begin{cases} 2^{\sqrt{2(r-2)}-2} & \text{if} \quad p = 2, \\ 3^{\sqrt{r-2}-2} & \text{if} \quad p = 3, \\ 5^{\sqrt{(r-2)/2}-2} & \text{if} \quad p \geq 5, \end{cases}$

(b) $\theta^e(\theta^f + a)$ *for* $a^2 \neq \pm 1$ *has the multiplicative order at least* $\begin{cases} 2^{2\sqrt{r-3}-5} & \text{if} \quad p = 2, \\ 3^{\sqrt{2(r-3)}-4}/2 & \text{if} \quad p = 3, \\ 5^{\sqrt{r-3}-4}/2 & \text{if} \quad p \geq 5, \end{cases}$

(c) $z$ *for* $a^2 \neq 1$ *has the multiplicative order at least* $\begin{cases} 2^{(\sqrt{2}+1)\sqrt{r-3}-5} & \text{if} \quad p = 2, \\ 3^{(\sqrt{2}+1)\sqrt{r-3}/2-4}/2 & \text{if} \quad p = 3, \\ 5^{(\sqrt{2}+1)\sqrt{r-3}/2-4}/2 & \text{if} \quad p \geq 5. \end{cases}$

***Proof.*** (a) According to Theorem 1, part (a) and Lemma 4.

(b) According to Theorem 1, part (d) and Lemma 4.

(c) According to Corollary 2 and Lemma 4.

Theorem 2 is proved.

We obtain the following corollary from Theorem 2.

***Corollary* 3.** *The Gauss period $\beta$ has the multiplicative order at least* $\begin{cases} 2^{\sqrt{2(r-2)}-2} & \text{if} \quad p = 2, \\ 3^{\sqrt{r-2}-2} & \text{if} \quad p = 3, \\ 5^{\sqrt{(r-2)/2}-2} & \text{if} \quad p \geq 5. \end{cases}$

The bound in Corollary 3 improves the previous bound $2^{\sqrt{r-1}-2}$ from [10] on the multiplicative order of the element $\beta$.

1. *Lidl R., Niederreiter H.* Finite fields. – 2nd ed. – Cambridge: Cambridge Univ. Press, 1997. – 755 p.
2. *Mullen G. L., Panario D.* Handbook of finite fields. – CRC Press, 2013. – 1068 p.
3. *Gao S.* Elements of provable high orders in finite fields // Proc. Amer. Math. Soc. – 1999. – **127**, № 6. – P. 1615 – 1623.
4. *Voloch J. F.* On the order of points on curves over finite fields // Integers. – 2007. – **7**. – P. 49.
5. *Voloch J. F.* Elements of high order on finite fields from elliptic curves // Bull. Austral. Math. Soc. – 2010. – **81**, № 3. – P. 425 – 429.

6. *Cheng Q.* On the construction of finite field elements of large order // Finite Fields Appl. – 2005. – **11**, № 3. – P. 358 – 366.
7. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ // Finite Fields Appl. – 2013. – **19**, № 1. – P. 86 – 92.
8. *Попович Р.* Елементи великого порядку в розширеннях Артіна – Шраєра скінченних полів // Мат. студ. – 2013. – **39**, № 2. – С. 115 – 118.
9. *Cheng Q., Gao S., Wan D.* Constructing high order elements through subspace polynomials // Proc. 23rd ACM-SIAM Symp. Discrete Algorithms (Kyoto, Japan, 17 – 19 January 2012). – Philadelphia, USA, 2011. – P. 1457 – 1463.
10. *Gathen J., Shparlinski I. E.* Orders of Gauss periods in finite fields // Appl. Algebra Engrg. Comm. Comput. – 1998. – **9**, № 1. – P. 15 – 24.
11. *Ahmadi O., Shparlinski I. E., Voloch J. F.* Multiplicative order of Gauss periods // Int. J. Number Theory. – 2010. – **6**, № 4. – P. 877 – 882.
12. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ // Finite Fields Appl. – 2012. – **18**, № 4. – P. 700 – 710.

Received 29.07.13