Algebra and Discrete Mathematics
Volume **18** (2014). Number 2, pp. 295–300

RESEARCH ARTICLE

On elements of high order in general finite fields

Roman Popovych

Communicated by I. P. Shestakov

Abstract. We show that the Gao's construction gives for any finite field F_{q^n} elements with the multiplicative order at least $\binom{n+t-1}{t}\prod_{i=0}^{t-1}\frac{1}{d^i}$, where $d = \lceil 2\log_q n \rceil$, $t = \lfloor \log_d n \rfloor$.

Introduction

It is well known that the multiplicative group of a finite field is cyclic. A generator of the group is called a primitive element. The problem of constructing efficiently a primitive element 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. 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. Such applications include but are not limited to cryptography, coding theory, pseudo random number generation and combinatorics.

Throughout this paper F_q is a field of q elements, where q is a power of prime number p. We use F_q^* to denote the multiplicative group of F_q.

Previous work. If no constraint is put on the extension degree n, very few results are known. Gao gives in [5] an algorithm for constructing high order elements for general extensions F_{q^n} of finite field F_q with lower bound on the order $n^{\frac{\log_q n}{4\log_q(2\log_q n)}-\frac{1}{2}}$. His algorithm assumes some

2010 MSC: 11T30.
Key words and phrases: finite field, multiplicative order, Diophantine inequality.

reasonable but unproved conjecture. Conflitti [4] provided a more careful analysis of results from [5].

A polynomial algorithm that find a primitive element in finite field of small characteristic is described in [8]. However, the algorithm relies on two unproved assumptions, and the second assumption is not supported by any computational example.

For special finite fields, it is possible to construct elements which can be proved to have much higher orders. Extensions connected with a notion of Gauss period are considered in [1, 6, 7, 10]. The lower bound on the order equals to $\frac{\exp\left(2.5\sqrt{n-2}\right)}{13(n-2)}$. Extensions based on the Kummer and Artin-Schreier polynomials are considered in [2, 11]. Some generalization of the extensions is given in [3].

Field extension based on the Kummer polynomial is of the form $F_q[x]/(x^n - a)$. It is shown in [2] how to construct high order element in the extension $F_q[x]/(x^n - a)$ with the condition $q \equiv 1 \pmod{n}$. The lower bound $5,8^n$ is obtained in this case. High order elements are constructed in [11] for Kummer extensions without the condition $q \equiv 1 \pmod{n}$ with lower bound $2^{\lfloor \sqrt[3]{2n} \rfloor}$.

Voloch [12, 13] proposed a method which constructs an element of order at least $\exp((\log n)^2)$ in finite fields from elliptic curves.

Our results. Set $F_q(\theta) = F_{q^n} = F_q[x]/f(x)$, where $f(x)$ is an irreducible polynomial over F_q of degree n and $\theta = x \mod f(x)$ is the coset of x.

We improve the Gao's construction and its modification by Conflitti for any finite field F_{q^n}. The method similar to that in [4, 5] is used for the proof. Our main result is the following theorem.

Theorem 1. *Set* $d = \left\lceil 2\log_q n \right\rceil$, $t = \lfloor \log_d n \rfloor$. *The* θ *has in the field* $F_q(\theta) = F_{q^n} = F_q[x]/f(x)$ *the multiplicative order at least*

$$\binom{n+t-1}{t} \prod_{i=0}^{t-1} \frac{1}{d^i}. \tag{1}$$

1. Preliminaries

We recall that the multiplicative order $ord(\beta)$ of the element $\beta \in F_{q^n}$ is the smallest positive integer u such that $\beta^u = 1$.

Let m be the smallest power of q greater or equal to n. The Gao approach [5] depends on the following conjecture.

Conjecture. *For any integer n, there exist a polynomial $g(x) \in F_q[x]$ of degree d at most $2\log_q n$ such that $x^m - g(x)$ has irreducible factor $f(x)$ of degree n.*

If the conjecture holds, then clearly $\theta^m = g(\theta)$. Gao considered the set $S = \left\{\sum_{i=0}^{t-1} u_i m^i | 0 \leqslant u_i \leqslant \mu\right\}$ and chase t and μ from the condition $\mu d^t < n$. He proved that θ^u are distinct elements for $u \in S$, took $t = \left\lfloor \frac{\log_q n}{2\log_q d} \right\rfloor$, $\mu = \sqrt{n}$ and showed $|S| = (\mu+1)^t \geqslant n^{\frac{\log_q n}{4\log_q(2\log_q n)} - \frac{1}{2}}$.

Conflitti [4] considered the following set

$$S = \left\{ \sum_{i=0}^{t-1} u_i m^i | 0 \leqslant u_i \leqslant \mu_i, \frac{n}{td^i} - 1 \leqslant \mu_i \leqslant \frac{n}{td^i} \right\}$$

and chase t and μ from the condition $\sum_{i=0}^{t-1} \mu_i d^i < n$. He proved that θ^u are distinct elements for $u \in S$, took $t = \lfloor \log_d n \rfloor$ and showed

$$|S_t| = \prod_{i=0}^{t-1} (\mu_i + 1) \geqslant \left(\frac{n}{t}\right)^t \prod_{i=0}^{t-1} \frac{1}{d^i}. \tag{2}$$

Substituting $t = \lfloor \log_d n \rfloor$ into (2), we obtain

$$ord(\theta) \geqslant \left(\frac{nd}{\log_d^2 n}\right)^{\frac{1}{2}\log_d n}.$$

The results from [4, 5] are based on the following statement (see [5, Theorem 1.4]).

Lemma 1. *Suppose that $f(x) \in F_q[x]$ is not a monomial nor a binomial of the form $ax^{p^l} + b$, where p is the characteristic of F_q. Then the polynomials*

$$f^{(1)}(x) = f(x), \quad f^{(k)}(x) = f^{(k-1)}(x), \quad k \geqslant 2$$

are multiplicatively independent in $F_q[x]$, that is, if

$$(f^{(1)}(x))^{k_1} (f^{(2)}(x))^{k_2} \ldots (f^{(s)}(x))^{k_s} = 1$$

for any integers $s \geqslant 1$, $k_1, \ldots, k_s$, then $k_1 = k_2 = \ldots = k_s = 0$.

The following lemma [9] gives lower bound for the number of non-negative solutions of linear Diophantine inequality.

Lemma 2. *Let* $a_0, \dots, a_{r-1}$ *be positive integers with* $\gcd(a_0, \dots, a_{r-1}) = 1$. *Then the number of non-negative integer solutions* $x_0, \dots, x_{r-1}$ *of the linear Diophantine inequality*

$$\sum_{i=0}^{r-1} a_i x_i \leqslant m,$$

is at least

$$\binom{m+r}{r} \prod_{i=0}^{r-1} \frac{1}{a_i}.$$

2. Main result

To improve the Conflitti result we consider the set of solutions $u_0, \dots, u_{r-1}$ of the linear Diophantine inequality

$$\sum_{i=0}^{r-1} d^i u_i \leqslant m,$$

and show that θ^u are distinct elements in F_{q^n} for all $u \in S$.

We give below the proof of our main result.

Proof of Theorem 1. If θ is a root of $x^m - g(x)$, then since m is a power of q, applying iteratively the Frobenius automorphism we have

$$\theta^{m^i} = g^{(i)}(\theta), i \in N. \tag{3}$$

where as in the statement of lemma 1, $g^{(i)}(x)$ is the polynomial obtained by composing $g(x)$ with itself i times.

Consider the set

$$S = \left\{ \sum_{i=0}^{t-1} u_i m^i | \sum_{i=0}^{t-1} d^i u_i \leqslant n-1, \quad u_i \geqslant 0 \right\}.$$

For every element $u \in S$ we construct the power θ^u that belongs to the group generated by θ. We show that if two elements $u, v \in S$ are distinct, then the correspondent powers do not coincide.

Assume that elements $u = \sum_{i=0}^{t-1} u_i m^i$ and $v = \sum_{i=0}^{t-1} v_i m^i$ from S are distinct, and the correspondent powers are equal: $\theta^u = \theta^v$. Then we have

$$\prod_{i=0}^{t-1} \left(\theta^{m^i}\right)^{u_i} = \prod_{i=0}^{t-1} \left(\theta^{m^i}\right)^{v_i}.$$

Taking into account the equality (3), we get

$$\prod_{i=0}^{t-1}\left(g^{(i)}(\theta)\right)^{u_i}=\prod_{i=0}^{t-1}\left(g^{(i)}(\theta)\right)^{v_i}.$$

Define the following polynomials $h_1(x)=\prod_{u_i>v_i}\left(g^{(i)}(\theta)\right)^{u_i-v_i}$ and $h_2(x)=\prod_{v_i>u_i}\left(g^{(i)}(\theta)\right)^{v_i-u_i}$. Then $h_1(\theta)=h_2(\theta)$, and since $g(x)$ is the characteristic polynomial of θ , we write: $h_1(x)=h_2(x) \mod f(x)$. As $g^{(i)}(x)$ has degree d^i, $h_1(x)$ is of degree at most $\sum_{i=0}^{t-1}u_id^i\leqslant n-1$ and $h_2(x)$ is of degree at most $\sum_{i=0}^{t-1}v_id^i\leqslant n-1$. Thus $h_1(x)$ and $h_2(x)$ must be equal as polynomials over F_q. Therefore

$$\prod_{i=0}^{t-1}\left(g^{(i)}(x)\right)^{u_i-v_i}=1.$$

According to lemma 1 the polynomials $g^{(i)}(x)$ are multiplicatively independent in $F_q[x]$. So $u_i=v_i$ for $i=0,\dots,t-1$, and thus $u=v$ - a contradiction.

Hence, the number of elements of S (and the multiplicative order of θ) is at least the number of nonnegative integer solutions of the Diophantine inequality $\sum_{i=0}^{t-1}d^ix_i\leqslant n-1$. Finally, applying lemma 2, we have

$$|S|\geqslant\binom{n+t-1}{t}\prod_{i=0}^{t-1}\frac{1}{d^i},$$

and the result follows. □

Now we compare our result with the Conflitti result. Let us calculate for this purpose the ratio R of the bound (1) to the bound (2):

$$R=\prod_{i=1}^{t-1}\frac{n+i}{n}\cdot\frac{t}{i}.$$

It is clear that $R>1$ for any q and n (recall that t depends on q and n).

We provide below a few numerical examples of lower bounds on the multiplicative orders of the considered previously element θ. Denote lower bounds on the orders of θ obtained in [4] and in this paper by b_1 and b_2 respectively. Values of q, n, d, t, b_1, b_2 and R in examples 1-3 are given in the table.

No.	q	n	d	t	b_1	b_2	R
1	127	1000	3	6	$1,49 \cdot 10^6$	$9,82 \cdot 10^7$	65,77
2	257	10000	3	8	$2,6 \cdot 10^{11}$	$1,08 \cdot 10^{14}$	417,26
3	19991	100000	2	16	$4,07 \cdot 10^{24}$	$3,59 \cdot 10^6$	882716,52

References

[1] O. Ahmadi, I. E. Shparlinski, J. F. Voloch, *Multiplicative order of Gauss periods*, Int. J. Number Theory, Vol.6 (2010), No.4, pp.877-882.

[2] Q. Cheng, *On the construction of finite field elements of large order*, Finite Fields Appl., Vol.11 (2005), No.3, pp.358-366.

[3] Q. Cheng, S. Gao, D. Wan, *Constructing high order elements through subspace polynomials*, Discrete algorithms: Proc. 23rd ACM-SIAM Symp. (Kyoto, Japan, 17–19 January 2012). – Omnipress, Philadelphia, USA, 2011, pp.1457–1463.

[4] A. Conflitti, *On elements of high order in finite fields*, Cryptography and computational number theory: Proc. Workshop (Singapore, 22-26 November 1999). – Birkhauser, Basel, 2001, pp.11–14.

[5] S. Gao, *Elements of provable high orders in finite fields*, Proc. Amer. Math. Soc., Vol.127 (1999), No.6, pp.1615-1623.

[6] J. von zur Gathen, I.E. Shparlinski, *Orders of Gauss periods in finite fields*, Appl. Algebra Engrg. Comm. Comput., Vol.9 (1998), No.1, pp.15-24.

[7] J. von zur Gathen, I.E. Shparlinski, *Gauss periods in finite fields*, Finite Fields and their Applications: Proc. 5th Conf. (Ausburg, Germany, 2–6 August 1999). – Springer, Berlin, 2001, pp.162-177.

[8] M.-D.Huang, A. K. Narayanan, *Finding primitive elements in finite fields of small characteristic*, arXiv 1304.1206, 2013.

[9] T. A. Lambe, *Bounds on the Number of Feasible Solutions to a Knapsack Problem*, SIAM J. Applied Math., Vol.26 (1974), No.2, pp.302-305.

[10] R. Popovych, *Elements of high order in finite fields of the form* $F_q[x]/\Phi_r(x)$, Finite Fields Appl., Vol.18 (2012), No.4, pp.700-710.

[11] R. Popovych, *Elements of high order in finite fields of the form* $F_q[x]/(x^m - a)$, Finite Fields Appl., Vol.19 (2013), No.1, pp.86-92.

[12] J.F. Voloch, *On the order of points on curves over finite fields*, Integers, Vol.7 (2007), A49.

[13] J.F. Voloch, *Elements of high order on finite fields from elliptic curves*, Bull. Austral. Math. Soc., Vol.81 (2010), No.3, pp.425-429.

Contact information

R. Popovych Lviv Polytechnic National University, Institute of Computer Technologies, Bandery Str., 12, Lviv, 79013, Ukraine
E-Mail(s): rombp07@gmail.com

Received by the editors: 13.02.2013
and in final form 08.12.2014.