© Algebra and Discrete Mathematics
Volume **29** (2020). Number 2, pp. 241–248
DOI:10.12958/adm1117

RESEARCH ARTICLE

Normal high order elements in finite field extensions based on the cyclotomic polynomials

R. Popovych and R. Skuratovskii

Communicated by A. P. Petravchuk

Abstract. We consider elements which are both of high multiplicative order and normal in extensions F_{q^m} of the field F_q. If the extension is defined by a cyclotomic polynomial, we construct such elements explicitly and give explicit lower bounds on their orders.

Introduction

Throughout this paper F_q is a field of q elements, where q is a power of prime number p.

High multiplicative order element is a very important notion in the theory of finite fields. A review of the obtained in this area results is provided in [6, section 4.4]. The problem of construction of such element is considered both for general and for special finite fields (extensions based on cyclotomic, Kummer or Artin-Schreier polynomials, recursive extensions) [1, 2, 7, 8]. For special finite fields, it is possible to construct elements which can be proved to have much higher orders.

Normal basis is also an important notion in the theory of finite fields, see [1, 5, 6, 9] for the definition, basic properties and references. One of the most interesting constructions of normal bases come from Gauss periods, see [2] and references therein. In particular, Gauss periods of type (n,2) are of special interest [2].

2010 MSC: 11T30.

Key words and phrases: finite field, cyclotomic polynomial, normal basis, high multiplicative order element.

It would be very useful to bring two mentioned notions together and consider elements which are both of high order and normal. The first step in this direction was made in [1, 2]. A lower bound on the order of Gauss periods of type $(n,2)$ was given by Gathen and Shparlinski [2], and later improved by Ahmadi, Shparlinski and Voloch [1]. Popovych [7, 8] obtained better lower bound on the order and for elements in a more general form. Then the question aroused: what high order elements considered in [7,8] remain normal.

It should be also noticed that, as a generalization of normal elements, Huczynska, Mullen, Panario and Thomson [3] introduce and characterize k-normal elements, proposing many problems based on theoretical considerations and computational tests. Particularly, they posed the following problem [3, problem 6.4]: to determine the existence of high-order k-normal elements.

The current paper enriches the list of normal high order elements in finite field extensions based on cyclotomic polynomials. More precisely, we show that a series of high order elements from [7, 8], which have more general form than Gauss periods of type $(n,2)$, are at the same time normal. One can also treat that the paper concerns with the mentioned above problem in the case $k = 0$ and finite field extensions based on cyclotomic polynomials. Our main result is Theorem 4.

1. Preliminaries

It is well known that the multiplicative group of a finite field is cyclic. A generator of the group is called primitive element. The problem of constructing efficiently a primitive element for a given finite field is notoriously difficult. 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. The use of high multiplicative order elements in cryptography is based on the discrete logarithm problem in a finite cyclic group [5, 6].

The multiplicative order $\mathrm{ord}(\alpha)$ of element $\alpha \in F_{q^m}^*$ is the smallest positive integer u such that $\alpha^u = 1$. "High order" means $\mathrm{ord}(\alpha) = N$ with N a large positive divisor of $q^m - 1$.

For any integer m, we can consider F_{q^m} as an m-dimensional vector space over F_q. Then any basis of F_{q^m} over F_q can be used to represent

the elements in F_{q^m}. A normal basis of F_{q^m} over F_q is a basis of the form $\{\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}\}$ for some $\alpha \in F_{q^m}$. In this case the element $\alpha \in F_{q^m}$ is called normal over F_q [5, 6].

It is known [6, Theorem 2.39] that $\alpha \in F_{q^m}$ is normal over F_q if and only if the polynomials $g_\alpha(x) = \sum_{i=0}^{m-1} \alpha^{q^i} x^{m-1-i}$ and $x^m - 1$ are coprime over F_{q^m}. Motivated by this fact, in [3], the authors introduce k-normal elements: for $0 \leqslant k \leqslant m-1$, an element $\alpha \in F_{q^m}$ is said to be k-normal over F_q if the greatest common divisor of $g_\alpha(x)$ and $x^m - 1$ over F_{q^m} has degree k. In this context, k-normal elements for $k = 0$ correspond to normal elements in the usual sense.

Let $\{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ be a normal basis of F_{q^m} over F_q with $\alpha_i = \alpha^{q^i}$ and $A \in F_{q^m}$ have the form

$$A = (a_0, a_1, \dots, a_{m-1}) = \sum_{i=0}^{m-1} a_i \alpha_i.$$

Then, since $\alpha_i^q = \alpha_{i+1}$ for $i = 0, \dots, m-2$ and $\alpha_{m-1}^q = \alpha$, we have

$$A^q = \sum_{i=0}^{m-1} a_i \alpha_i^q = \sum_{i=0}^{m-1} a_i \alpha_{i+1} = (a_{n-1}, a_0, \dots, a_{n-2}).$$

That is, q-th power is the cyclic shift of coordinates. It means taking q-th powers has negligible cost.

Hence, useful properties of finite field elements from the point of view of the operation of raising to a power are as follows: high multiplicative order (provides resistance against breaking by unauthorized person) and normality (ensures less amount of calculations). This operation is particularly needed for the Diffie Hellman and El Gamal cryptographic protocols that are based on the discrete logarithm problem.

2. Field extensions based on cyclotomic polynomials

Extensions based on cyclotomic polynomials and connected with a notion of Gauss period are considered in [1, 2, 7, 8]. More precisely, the following extensions are constructed. Let $r = 2n + 1$ 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 $\theta = x \pmod{\Phi_r(x)}$ is the coset of element x modulo $\Phi_r(x)$. The polynomial is irreducible over the field F_q. It is clear that the equality

$\theta^r = 1$ holds. We have the following tower of fields $F_q \subset F_{q^n} \subset F_{q^{2n}}$. The element $\beta = \theta + \theta^{-1}$ is called a Gauss period of type $(n,2)$ [1]. It belongs to F_{q^n} and is normal over F_q [2].

A lower bound on the order of Gauss periods was given by Gathen and Shparlinski [2], and later improved by Ahmadi, Shparlinski and Voloch [1]. Popovych [7, 8] derived better than in [2] lower bound, and the bound is on the order of elements in a more general form. We show in this section that a series of elements from [7, 8] are normal.

Denote by $L(c,d)$ the number of solutions $(u_1,\dots,u_c)$ of the linear Diophantine inequality $\sum_{j=1}^{c} ju_j \leqslant c$ with the condition $0 \leqslant u_1,\dots,u_c \leqslant d$. The Lemma below gives a lower bound on this number.

Lemma 1. [8, Lemma 4] *The number $L(c,d)$ is at least $(\delta+1)^{\sqrt{2c/\delta}-2}$, where $\delta = d$ if $d = 1,2$ and $\delta = 4$ if $d \geqslant 4$.*

All lower bounds on elements order in Theorem 1 below involve a number of solutions of the linear Diophantine inequality.

Theorem 1. [8, Theorem 1] *Let e be any integer, f any integer coprime with r and a any non-zero element in the finite field F_q. Then*

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

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

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

Using Lemma 1 and Theorem 1, we obtain the following Theorem 2. It is a modification of theorem 2 from [8] and gives a lower bound on the order of elements in a more general form than Gauss periods.

Theorem 2. *Let e be any integer, f any integer coprime with r and $a \in F_q^*$. Then*

(a) *$\theta^e(\theta^f + a)$ has the multiplicative order at least*

$$\begin{cases} 2^{\sqrt{2(r-2)}-2} & \text{if } p = 2, \\ 3^{\sqrt{r-2}-2} & \text{if } p = 3, \\ 5^{\sqrt{(r-2)/2}-2} & \text{if } p \geqslant 5; \end{cases}$$

(b) *$\theta^e(\theta^f + a)$ for $a^2 \neq \pm 1$ has the multiplicative order at least*

$$\begin{cases} 2^{2\sqrt{r-3}-5} & \text{if } p = 2, \\ 3^{\sqrt{2(r-3)}-4}/2 & \text{if } p = 3, \\ 5^{\sqrt{r-3}-4}/2 & \text{if } p \geqslant 5; \end{cases}$$

(c) $(\theta^{-f}+a)(\theta^{f}+a)$ *for* $a^2\neq -1$ *has the multiplicative order at least*

$$\begin{cases} 2^{\sqrt{r-3}-2} & \text{if } p=2,\\ 3^{\sqrt{(r-3)/2}-2} & \text{if } p=3,\\ 5^{\sqrt{r-3}/2-2} & \text{if } p\geqslant 5. \end{cases}$$

Proof. (a) By Theorem 1 (a) and Lemma 1.

(b) By Theorem 1 (c) and Lemma 1.

(c) By Theorem 1 (b) the element $(\theta^{-f}+a)(\theta^{f}+a)$ for $a^2\neq -1$ has the multiplicative order at least $L((r-3)/2,p-1)$. Now the result follows from Lemma 1. □

If we take in Theorem 2 $e=-1$, $f=2$, $a=1$, then we obtain the Gauss period of the type $(n,2)$. Note that, since $\theta^r=1$ holds, one can take e between 0 and $r-1$, and f between 1 and $r-1$. Then f will be automatically coprime with r.

Element $\theta\in F_{q^{2n}}$, which generates the extension, is normal over F_q. We show in Theorem 3 that elements in a more general form $\theta+b\in F_{q^{2n}}$, where $b\in F_q$ and b satisfies a certain condition, are also normal over F_q.

Theorem 3. *Let* b *be element of the field* F_q *such that* $2nb\neq 1$. *Then element* $\theta+b\in F_{q^{2n}}$ *is normal over* F_q.

Proof. Since q is primitive modulo $2n+1$, then the set $\theta^{q^k}+b$ $(k=0,\dots,2n-1)$ coincides with θ^i+b $(i=1,\dots,2n)$.

Show that the set θ^i+b $(i=1,\dots,2n)$ is a basis, i. e. its elements are linear independent over F_q. Really, if these elements are linear dependent, there exists the set of coefficients $c_i\in F_q$ $(i=1,\dots,2n)$ with at least one non-zero coefficient (say $c_j\neq 0$, $1\leqslant j\leqslant 2n$) and $\sum_{i=1}^{2n}c_i(\theta^i+b)=0$. As θ is a root of the polynomial $\Phi_{2n+1}(x)$, we have $\theta^{2n}=-\sum_{i=0}^{2n-1}\theta^i$. Therefore, we obtain the relation $\sum_{i=1}^{2n-1}(c_i-c_{2n})\theta^i+(b\sum_{i=1}^{2n}c_i-c_{2n})=0$. Hence, θ is a root of the polynomial of degree $2n-1$. At the same time, θ is a root of the irreducible polynomial $\Phi_{2n+1}(x)$ of degree $2n$. Therefore, all coefficients of the polynomial must be equal to zero. So, elements c_i $(i=1,\dots,2n)$ are equal and $b\sum_{i=1}^{2n}c_i-c_{2n}=0$. This implies $(2nb-1)c_j=0$. Since $c_j\neq 0$, we have $2nb-1=0$, so this is a contradiction. □

Remark that the inequality $2nb\neq 1$ in the statement of Theorem 3 is modulo p. If $n=0$, then, clearly, the condition $2nb\neq 1$ holds for any $b\in F_q$. If $n\neq 0$, then this condition is true for all elements b of the field F_q, but $b=(2n)^{-1}$.

Corollary 1. *Let b be element of the field F_q such that $2nb \neq 1$. Then element $\theta + \theta^{-1} + 2b \in F_{q^n}$ is normal over F_q.*

Proof. Consider the trace of $\theta + b$ over F_{q^n}. Taking into account, that the trace of a sum equals a sum of traces and $Tr_{q^{mn}/q^n}(b) = mb$ for $b \in F_q \subset F_{q^n}$ [5, Theorem 2.23 (i), (iv)], we obtain:

$$Tr_{q^{2n}/q^n}(\theta + b) = Tr_{q^{2n}/q^n}(\theta) + Tr_{q^{2n}/q^n}(b) = (\theta + \theta^{-1}) + 2b.$$

Hence, the element $(\theta + \theta^{-1}) + 2b$ is normal over F_q as the trace $Tr_{q^{2n}/q^n}(\theta + b)$ of the element $\theta + b$, which is normal over F_q [6, Proposition 5.2.3, 1]. □

Corollary 1 is a generalization of the known fact, that the Gauss period $\theta + \theta^{-1}$is normal over F_q.

Recall that for $b = 0$ we have $2nb \neq 1$, and by Theorem 3 element $\theta \in F_{q^{2n}}$ is normal over F_q. However, the order of this element equals r and is small comparatively with the order of the group $F^*_{q^{2n}}$. By Theorem 3, for $b \neq 0$ and $2nb \neq 1$, the element $\theta + b \in F_{q^{2n}}$ is normal over F_q. It has high order according to the following Theorem 4.

Theorem 4. *Let $b \neq 0$ be element of the field F_q such that $2nb \neq 1$. Then, for $f = 1, \ldots, r-1$,*

(a) *$\theta^f + b \in F_{q^{2n}}$ is normal over F_q and has the multiplicative order at least*

$$\begin{cases} 2^{\sqrt{2(r-2)}-2} & \text{if } p = 2, \\ 3^{\sqrt{r-2}-2} & \text{if } p = 3, \\ 5^{\sqrt{(r-2)/2}-2} & \text{if } p \geqslant 5; \end{cases}$$

(b) *$\theta^f + b \in F_{q^{2n}}$ for $b^2 \neq \pm 1$ is normal over F_q and has the multiplicative order at least*

$$\begin{cases} 2^{2\sqrt{r-3}-5} & \text{if } p = 2, \\ 3^{\sqrt{2(r-3)}-4}/2 & \text{if } p = 3, \\ 5^{\sqrt{r-3}-4}/2 & \text{if } p \geqslant 5; \end{cases}$$

(c) *$\theta^f + \theta^{-f} + 2b \in F_{q^n}$ for $a \in F^*_q$ and $2b = (a^2+1)a^{-1}$ is normal over F_q and has the multiplicative order at least*

$$\begin{cases} \frac{2^{\sqrt{r-3}-2}\,\mathrm{ord}(a)}{(q-1)^2} & \text{if } p = 2, \\ \frac{3^{\sqrt{(r-3)/2}-2}\,\mathrm{ord}(a)}{(q-1)^2} & \text{if } p = 3, \\ \frac{5^{\sqrt{r-3/2}-2}\,\mathrm{ord}(a)}{(q-1)^2} & \text{if } p \geqslant 5. \end{cases}$$

Proof. (a) Since elements $\theta^f + b$ $(f = 1, \dots, r-1)$ are conjugates over F_q, it is enough to prove (a) only for the case $f = 1$. The result follows by Theorem 3 and Theorem 2 (a).

(b) Analogously to (a), it is enough to prove (b) only for $f = 1$. The result follows by Theorem 3 and Theorem 2 (b).

(c) Since elements $\theta^f + \theta^{-f} + 2b$ $(f = 1, \dots, r-1)$ are conjugates over F_q, it is enough to prove (c) only for $f = 1$. We can write

$$(\theta + a)(\theta^{-1} + a) = a(\theta + \theta^{-1}) + (a^2 + 1) = a[\theta + \theta^{-1} + (a^2 + 1)a^{-1}].$$

Set $2b = (a^2 + 1)a^{-1}$. The condition $a^2 \neq -1$ is equivalent to $b \neq 0$. If $2nb \neq 1$, then the element $\theta + \theta^{-1} + (a^2 + 1)a^{-1}$ is normal over F_q by Corollary 1. Then $a[\theta + \theta^{-1} + (a^2 + 1)a^{-1}]$ is also normal over F_q by the following clear fact: if γ is normal over F_q and $a \in F_q$ $(a \neq 0)$, then $a\gamma$ is normal over F_q (because $a^q = a$).

According to [4], if α and β are elements of a finite abelian group, then

$$\operatorname{ord}(\alpha\beta) \geqslant \frac{\operatorname{ord}(\alpha)\operatorname{ord}(\beta)}{[\gcd(\operatorname{ord}(\alpha), \operatorname{ord}(\beta))]^2}. \tag{1}$$

Set $\alpha = a[\theta + \theta^{-1} + (a^2 + 1)a^{-1}]$, $\beta = a^{-1}$. Taking into account that by Theorem 2(c) the element α for $a^2 \neq -1$ has the multiplicative order

$$\operatorname{ord}(\alpha) = U \geqslant \begin{cases} 2^{\sqrt{r-3}-2} & \text{if } p = 2, \\ 3^{\sqrt{(r-3)/2}-2} & \text{if } p = 3, \\ 5^{\sqrt{r-3}/2-2} & \text{if } p \geqslant 5, \end{cases}$$

$\operatorname{ord}(\beta) \leqslant q-1$ and the inequality (1), we obtain $\operatorname{ord}(\theta+\theta^{-1}+(a^2+1)a^{-1}) \geqslant \frac{U \cdot \operatorname{ord}(a)}{(q-1)^2}$ and the result follows. □

Note that if the number q is not too large, then $\operatorname{ord}(a)$ can be obtained by direct computer calculations in the field F_q.

Acknowledgements

The authors are grateful to the referee for comments and suggestions which improved the quality of this paper.

References

[1] *Ahmadi O., Shparlinski I. E., Voloch J. F.* Multiplicative order of Gauss periods, Int. J. Number Theory, 2010, 6(4), P. 877-882.

[2] *Gathen J., Shparlinski I. E.* Orders of Gauss periods in finite fields, Appl. Algebra Engrg. Comm. Comput., 1998, 9 (1), P. 15-24.

[3] *Huczynska S., Mullen G.L., Panario D., Thomson D.* Existence and properties of k-normal elements over finite fields, Finite Fields Appl., 2013, 24, P. 170-183.

[4] Jungnickel D. On the order of a product in a finite abelian group, Math. Magazine, 1996, 69 (1), P. 53-57.

[5] Lidl R., Niederreiter H. Finite Fields. – Cambridge: Cambridge University Press, 1997, 755 p.

[6] Mullen G.L., Panario D. Handbook of finite fields. – Boca Raton: CRC Press, 2013, 1068 p.

[7] Popovych R. Elements of high order in finite fields of the form, Finite Fields Appl., 2012, 18 (4), P. 700-710.

[8] Popovych R. Sharpening of explicit lower bounds on elements order for finite field extensions based on cyclotomic polynomials, Ukr. Math. J., 2014, 66 (6), P. 815-825.

[9] Skuratovskii R. V. Constructing of finite field normal basis in deterministic polynomial time, Bulletin of Taras Shevchenko National University of Kyiv. Series: Physics and Mathematics, 2011 (1), P. 49-54 (in Ukrainian).

CONTACT INFORMATION

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

Ruslan Skuratovskii Igor Sikorsky Kiev Polytechnic Institute, av. Pobedy, 03056, Kiev, Ukraine
E-Mail(*s*): ruslcomp@mail.ru, r.skuratovskii@kpi.ua

Received by the editors: 02.04.2018
and in final form 10.02.2019.