Contact information

Valeriu Popa
Institute of Mathematics, and Computer Science, Kishinew, Moldova
Email address: vpopa@math.md

Key words and phrases. LCA groups, rings of continuous endomorphisms

Finite field elements of high order on a base of modified Gao approach

Bogdan Popovych

Elements of high multiplicative order in finite fields are of great interest in several applications (cryptography, error correcting codes) that use finite fields. Obviously, the best possible are primitive elements, but there is no any algorithm to find them. Therefore, they consider a less ambitious question: to find an element with provable high order [**3, 4**].

F_{q^n} is a field with q^n elements, where q is a power of a prime number p and n is an integer. u is the nearest larger integer to $\log_q n$.

Gao [**3**] described construction of high order elements for general extensions F_{q^n} of finite field F_q . For this goal, he searched for a polynomial $g(x) \in F_q[x]$ of small degree such that $x^{q^u} - g(x)$ has irreducible factor $f(x)$ of degree n. The method was improved in [**1, 2, 5**].

The modification is as follows [**1, 6**]: to search for polynomials $g(x), h(x) \in F_q[x]$ of small degrees such that $h(x)x^{q^u} - g(x)$ has an irreducible divisor $f(x)$ of degree n. However, the bound on the order was not improved.

We have performed calculations in Maple and obtained examples, which show that the modified Gao approach can give better lower bound on the order.

References

1. A. Conflitti, *On elements of high order in finite fields*, In Cryptography and computational number theory, Singapore (1999), volume 20 of Progr. Comput. Sci. Appl. Logic, Birkhauser, Basel (2001), 11–14.
2. R. Dunets, B. Popovych and R. Popovych, *On construction of high order elements in arbitrary finite fields*, JP J. Algebra Number Theory Appl. **42** (2019), no. 1, 71–76.
3. S. Gao, *Elements of provable high orders in finite fields*, Proc. Amer. Math. Soc. **127** (1999), no. 6, 1615–1623.
4. G. L. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, Boca Raton, 2013.
5. R. Popovych, *On elements of high order in general finite fields*, Algebra Discr. Math. **18** (2014), no. 2, 295–300.
6. M. Young, *On the multiplicative independence of rational iterates*, preprint (2018), available at https://arxiv.org/abs/1708.00944.

Contact information

Bogdan Popovych
Department of Specialized Computer Systems, Lviv Polytechnic National University, Lviv, Ukraine
Email address: bogdan.popovych@gmail.com

Key words and phrases. Finite field, multiplicative order, lower bound