LOWER BOUNDS FOR THE ORDER OF ELEMENTS IN FINITE FIELD EXTENSIONS

F. E. BROCHERO MARTÍNEZ
FBROCHER@MAT.UFMG.BR

DEPARTAMENTO DE MATEMÁTICA
UNIVERSIDADE FEDERAL DE MINAS GERAIS
BELO HORIZONTE, MG, BRASIL

JOINT WORK WITH L. REIS, T. GARAFALAKIS AND E. TZANAKI

Abstract. For many important applications (for example AKS algorithm), it is interesting to find an element of very high order in a finite extension field $\mathbb{F}_{q^n}$. Ideally, one would choose a primitive element, but actually finding such an element is a notoriously hard computation problem. Many author have work, in order to show an elements for which a reasonably large lower bound on the order can be guaranteed.

In this work, we find a lower bound for the order of the group $\langle \theta + \alpha \rangle \subset \overline{\mathbb{F}}_q^*$, where $\alpha \in \mathbb{F}_q$, θ is a generic root of the polynomial $F_{A,r}(X) = bX^{q^r+1} - aX^{q^r} + dX - c \in \mathbb{F}_q[X]$ and $ad - bc \neq 0$. In addition, we find a lower bounds for the order of a generic element of $\mathbb{F}_q(\theta)$ of the form $\theta^e(\theta^f + a)$, where $a \in \mathbb{F}_q^*$ and $-1 \in \langle q \rangle \subset \mathbb{Z}^*_{\mathrm{ord}(\theta)}$.

Palavras-chave: multiplicative order, AKS method, Invariant polynomial, Gauss Period.