# Existence of primitive 2-normal elements in finite fields

Victor Gonzalo Lopez Neumann*
Faculdade de Matemática
Universidade Federal de Uberlândia
Uberlândia, Brazil

**Abstract**

An element $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if $\mathcal{B} = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$ forms a basis of $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. It is well known that $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ and $x^n - 1$ are relatively prime over $\mathbb{F}_{q^n}$, that is, the degree of their greatest common divisor in $\mathbb{F}_{q^n}[x]$ is 0. Using this equivalence, the notion of $k$-normal elements was introduced in Huczynska et al. (see [2]): an element $\alpha \in \mathbb{F}_{q^n}$ is $k$-normal over $\mathbb{F}_q$ if the greatest common divisor of the polynomials $g_\alpha[x]$ and $x^n - 1$ in $\mathbb{F}_{q^n}[x]$ has degree $k$; so an element which is normal in the usual sense is 0-normal.

Huczynska et al. made the question about the pairs $(n, k)$ for which there exist primitive $k$-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and they got a partial result for the case $k = 1$, and later Reis and Thomson (see [4]) completed this case. The Primitive Normal Basis Theorem (see [3] and [1]) solves the case $k = 0$. In this paper, we solve completely the case $k = 2$ using estimates for Gauss sum and the use of the computer. This is a joint work with Josimar J.R. Aguirre.

## References

[1] S.D. Cohen and S. Huczynska, The primitive normal basis theorem without a computer, *Journal of London Mathematical Society* 67(1) (2003), 41-56.

[2] S. Huczynska; G.L. Mullen; D. Panario and D. Thomson, Existence and properties of k-normal elements over finite fields, *Finite Fields and Their Applications* 24 (2013), 170-183.

[3] H.W. Lenstra and R. Schoof, Primitive normal bases for finite fields, *Mathematics of Computation* 48 (1987), 217-231.

[4] L. Reis and D. Thompson, Existence of primitive 1-normal elements in finite fields, *Finite Fields and Their Applications* 51 (2018), 238-269.

*Partially supported by FAPEMIG, e-mail: `victor.neumann@ufu.br`