On a conjecture of Morgan and Mullen

Giorgos Kapetanakis (Sabancı Üniversitesi)

Joint work with T. Garefalakis

Abstract

Let $\mathbf{F}_q$ be the finite field of cardinality q and $\mathbf{F}_{q^n}$ its extension of degree n, where q is a prime power and n is a positive integer. A generator of the multiplicative group $\mathbf{F}_{q^n}^*$ is called *primitive*. Besides their theoretical interest, primitive elements of finite fields are widely used in various applications, including cryptographic schemes, such as the Diffie-Hellman key exchange.

An $\mathbf{F}_q$-*normal basis* of $\mathbf{F}_{q^n}$ is an $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$ of the form $\{x, x^q, \ldots, x^{q^{n-1}}\}$ and the element $x \in \mathbf{F}_{q^n}$ is called *normal over* $\mathbf{F}_q$. These bases bear computational advantages for finite field arithmetic, so they have numerous applications, mostly found in coding theory and cryptography. An element of $\mathbf{F}_{q^n}$ that is simultaneously normal over $\mathbf{F}_{q^l}$ for all $l \mid n$ is called *completely normal over* $\mathbf{F}_q$.

It is well-known that primitive and normal elements exist for every q and n. The existence of elements that are simultaneously primitive and normal is also well-known for every q and n.

Further, it is also known that for all q and n there exist completely normal elements of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$. Morgan and Mullen [*Util. Math.*, 49:21–43, 1996], took the next step and conjectured that for any q and n, there exists a primitive completely normal element of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.

In order to support their claim, they provided examples for such elements for all pairs (q, n) with $q \leq 97$ and $q^n < 10^{50}$. This conjecture is yet to be established for arbitrary q and n, but instead we have partial results, covering special types of extensions. Recently, Hachenberger [*Des. Codes Cryptogr.*, 80(3):577–586, 2016] using elementary methods, proved the validity of the Morgan-Mullen conjecture for $q \geq n^3$ and $n \geq 37$.

In this work, we use character sum techniques and prove the validity of the Morgan-Mullen conjecture for all q and n, provided that $q > n$. In the talk, the previous results will briefly be presented, our proof will be outlined and possible improvements will be discussed.