Linear algebra and Galois theory: the Alon–Füredi theorem for endomorphisms

Alessandro Neri
Technical University of Munich (Germany)
(Joint work with Daniel Augot, Alain Couvreur and Julien Lavauzelle)

Abstract

In this work we present an approach for studying linear spaces of endomorphisms with high rank, when the ambient space is a finite dimensional vector space over a field $\mathbb{K}$ which possesses a Galois extension field $\mathbb{L}$. When its Galois group is abelian, we derive the analogues of the celebrated Alon–Füredi theorem and of the Schwartz-Zippel lemma for endomorphisms, which produce nontrivial lower bounds on the rank of a linear endomorphism.

The main motivation arises from algebraic coding theory, and in particular from the theory of rank-metric codes. In this setting, the most celebrated family of rank-metric codes is given by *Gabidulin codes*. It is well-known that they can be seen as analogues of Reed-Solomon codes in classical coding theory, which are codes constructed from spaces of univariate polynomials. The generalization of Reed-Solomon codes to multivariate polynomials lead to the family of Reed–Muller codes. In the last years, several researchers tried to adapt a Reed–Muller-type construction in the rank metric setting, unfortunately without success. This work provides a complete answer to this problem, showing also why it is not possible to construct such a family of codes over finite fields.

Keywords: Rank-metric codes; Alon-Füredi theorem; Galois theory; Reed-Muller codes; Dickson matrices