Some applications of linear algebra over finite fields

Simeon Ball

Universitat Politécnica de Catalunya

In this talk I will discuss a selection of problems relating to $\mathbb{F}_q^k$, the k-dimensional vector space over the finite field $\mathbb{F}_q$, where linear algebra has been used to solve, at least in part, problems where combinatorial and algebraic geometric methods, have not been totally successful.

The first problem to be considered is to determine the maximum size of a set S of vectors of $\mathbb{F}_q^k$ in which every subset of size k is a basis. For $k \geq q+1$ it is easily shown that $|S| \leq k+1$ and to classify the extremal example as equivalent to $S = \{e_1, \ldots, e_k, e_1 + \ldots + e_k\}$, where $\{e_1, \ldots, e_k\}$ is a basis. For $k \leq q$ the MDS conjecture from coding theory (MDS stands for maximum distance separable) states that $|S| \leq q+1$ unless q is even and $k = 3$ or $k = q-1$ in which case $|S| \leq q+2$. I shall outline a proof of this conjecture in the prime case and some recent developments in the case the q is the square of a prime. The relevant application of linear algebra here is the ability to prove equations involving functions of the vectors of S which do not rely on coordinates; in other words they are not dependent on any basis.

The second problem to be considered is to determine whether, with respect to a fixed basis, given any endomorphism from $\mathbb{F}_q^k$ to $\mathbb{F}_q^k$, there exists an $x \in \mathbb{F}_q^k$ with the property that x and $f(x)$ have no zero coordinate. Jaeger's conjecture states that for $q \geq 5$ such an x exists. This conjecture was proven by Alon and Tarsi (*Combinatorica*, **9** (1989) 393–395) in the case that q is not prime. I shall present a short proof of this using a simple change of basis.

The third problem I shall consider is to determine those functions f from $\mathbb{F}_q$ to $\mathbb{F}_q$, for which $N(f) = q - |D|$ is small, where $D = \{(f(y) - f(x))/(y-x) \mid x, y \in \mathbb{F}_q\}$. For q non-prime, these functions are determined for $N(f) \geq (q+1)/2$ and there seems little hope and determining those for which $|N(f)| \geq q/c$, where $c > 2$. However, for q prime, together with A. Gács, we conjectured that if $N(f) > (q-1)/t + t - 2$ then the graph of f, $\{(x, f(x)) \mid x \in \mathbb{F}_q\}$, is contained in an algebraic curve of degree $t-1$. This conjecture is true for $t = 2$ (Rédei) and $t = 3$ (Gács) and can be proved under the assumption that there are $t-1$ lines meeting the graph of f in at least t points. This proof uses the rank-nullity theorem for linear maps.