On subsets of a finite vector space in which every subset of basis size is a basis

Simeon Ball

In this talk we consider sets of vectors S of the vector space $\mathbb{F}_q^k$ with the property that every subset of S of size k is a basis.

The classical example of such a set is the following.

Example (Normal Rational Curve) The set

$$S = \{(1,t,t^2,\ldots,t^{k-1}) \mid t \in \mathbb{F}_q\} \cup \{(0,\ldots,0,1)\},$$

is a set of size $q+1$. It is easily shown that S has the required property by checking that the $k \times k$ Vandermonde matrix formed by k vectors of S, has non-zero determinant.

For q even and $k=3$, one can add the vector $(0,1,0)$ to S and obtain an example with $q+2$ vectors. For these parameters, such a set of $q+2$ vectors is called a *hyperoval*, and these have been studied extensively. There are many examples of hyperovals known which are not equivalent (up to change of basis and field automorphisms) to the example above. The only other known examples of size $q+1$ is an example of size 10 in $\mathbb{F}_9^5$, due to Glynn, and an example in $\mathbb{F}_{2^h}^4$ due to Hirschfeld.

The following conjecture exists in various areas of combinatorics. It is, known as the main conjecture for maximum distance separable codes, the representability of the uniform matroid in matroid theory, the embeddability of the complete design in design theory and Segre's arcs problem in finite geometry.

Conjecture A set of vectors S of the vector space $\mathbb{F}_q^k$, $k \leq q-1$, with the property that every subset of S of size k is a basis, has size at most $q+1$, unless q is even and $k=3$ or $k=q-1$, in which case it has size at most $q+2$.

I shall present a proof of the conjecture for q prime and discuss the non-prime case. I shall also explain how to then prove the following theorem, which is a generalisation Segre's "oval is a conic" theorem in the case $k=3$.

Theorem If $p \geq k$ then a set S of $q+1$ vectors of the vector space $\mathbb{F}_q^k$, with the property that every subset of S of size k is a basis, is equivalent to the Normal Rational Curve example, where $q = p^h$.