On Arcs and MDS Codes

Simeon Ball

Universitat Politécnica Catalunya

Barcelona

A block code C of length n, minimum distance d over an alphabet with q symbols, satisfies,

$$|C| \leqslant q^{n-d+1},$$

which is known as the *Singleton bound*. A block code attaining this bound is known as a *Maximum Distance Separable code* or simply an MDS code.

An *arc* S in $\mathbb{F}_q^k$ is a subset of vectors with the property that every subset of size k of S is a set of linearly independent vectors. Equivalently, an arc is a subset of points of $\mathrm{PG}(k-1,q)$, the $(k-1)$-dimensional projective space over $\mathbb{F}_q$, for which every subset of k points spans the whole space.

If C is a k-dimensional linear MDS code over $\mathbb{F}_q$ then the columns of a generator matrix for C are an arc in $\mathbb{F}_q^k$ and vice-versa.

The classical example of a linear MDS code is the Reed-Solomon code, which is the evalutaion code of all polynomials of degree at most $k-1$ over $\mathbb{F}_q$. As an arc, the Reed-Solomon code is a normal rational curve in $\mathrm{PG}(k-1,q)$.

The trivial upper bound on the length n of a k-dimensional linear MDS code over $\mathbb{F}_q$ is

$$n \leqslant q+k-1.$$

The (doubly-extended) Reed-Solomon code has length $q+1$.

The dual of a k-dimensional linear MDS code is a $(n-k)$-dimensional linear MDS code, thus if we can assume that $k \leqslant \frac{1}{2}n$ and therefore that $k \leqslant q-1$.

The MDS conjecture states that if $4 \leqslant k \leqslant q-2$ then an MDS code has length at most $q+1$. In other words, there are no better MDS codes than the Reed-Solomon codes.

In 2012, the linear MDS conjecture was verified for q prime. In this talk I will talk about various advances since then, survey the non-linear case and highlight the lack of examples of known MDS codes of length more than $k+\frac{1}{2}q$.