Maximum Distance Separable Codes: Recent advances and applications

Simeon Ball
Universitat Politécnica Catalunya

Let A be a finite set and let C be a subset of A^n.

Let d be minimal such that any two codewords (elements of C) differ in at least d coordinates. Fixing any $n-d+1$ coordinates, one obtains the (Singleton) bound

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

since if C was larger then the pigeon-hole principle would imply that two codewords agree on these $n-d+1$ coordinates and therefore differ on at most $d-1$ coordinates.

A **maximum distance separable code** (MDS code) is a code C for which $|C| = |A|^{n-d+1}$. Thus, C has the property that for any k-tuple ($k = n-d+1$) of elements of A on any k coordinates, there is a unique codeword of C which agrees with the k-tuple on these k coordinates.

Two important applications of MDS codes are to distributed storage systems and to error-correcting communication (particularly to channels susceptible to burst-errors).

In this talk, I will start with a description of the classical Reed-Solomon codes and mention decoding algorithms for these codes. But for the main part of the talk, I will consider the geometrical object (known as an **arc**) which one obtains by taking the set of columns of a generator matrix of a linear MDS code over a finite field $\mathbb{F}_q$ and considering this set of columns as a set of points in $\mathrm{PG}(k-1,q)$, the $(k-1)$-dimensional projective space.

The main conjecture for linear MDS codes (also known as the MDS conjecture) states, in terms of arcs, that if $4 \leqslant k \leqslant q-2$ then an arc in $\mathrm{PG}(k-1,q)$ has size at most $q+1$. This would imply that there are no (linear) MDS codes which outperform Reed-Solomon codes. If k is outside this range then we know how large an arc can be and therefore how many errors one can correct with a k-dimensional linear MDS code.

The MDS conjecture was proven for q prime in 2012. I will detail all results since then and before then which prove the MDS conjecture for ranges of k when q is not prime.