On the MDS conjecture

Jan De Beule

Vrije Universiteit Brussel

Let C be a q-ary code of length n and minimum distance d. The Singleton bound states that $|C| \leq q^{n-d+1}$. Codes reaching the Singleton bound are called *Maximum Distance Separable codes* (MDS codes). Given an alphabet of size q and a minimum distance d, a natural question is whether there is a bound on the length of an MDS code. We will restrict to linear MDS codes, then C is a k-dimensional subspace of the n-dimensional vector space over $\mathbb{F}_q$, the finite field of order q. The following conjecture is known as the (linear) MDS conjecture.

> Let C be a linear $[n, k, d]$ code over the finite field $\mathbb{F}_q$ satisfying the Singleton bound. Then $n \leq q + 1$, unless q is even and $k = 3$ or $k = q - 1$, in which case $n \leq q + 2$.

Let $V(r, q)$ be an r-dimensional vector space over $\mathbb{F}_q$, then an *arc* of $V(r, q)$ is a set S of vectors with the property that every subset of size r of S is a base of $V(r, q)$. Arcs of vector spaces are equivalent with MDS codes, and the size of the arc equals the length of the code.

The first part of the talk will be devoted to explain the state of the art of the MDS conjecture. Old and recent results will be discussed, as well as the techniques that were used to prove the following theorems. Let p be prime.

THEOREM. **(S. Ball [2])** *An arc of $V(k, q)$, $q = p^h$, has size at most $q + k + 1 - \min(k, p)$, where $k \leq q$.*

THEOREM. **(S. Ball and J. De Beule [4])** *An arc of $V(k, q)$, $q = p^h$ non-prime and $2 < k \leq 2p - 2$, has size at most $q + 1$.*

In vector spaces of dimension at least three, there are very few examples known of arcs reaching the conjectured largest possible size. Among them are *normal rational curves*, which are equivalent with Reed-Solomon codes. Besides the progress towards the MDS conjecture, the work of S. Ball in [2] also contains the following classification result.

THEOREM. **(S. Ball [2])** *If $p \geq k \geq 3$, then an arc of $V(k, q)$, $q = p^h$, of size $q + 1$ is equivalent to a normal rational curve.*

As described in [2], a corollary of the previous theorem for linear codes is the following statement.

COROLLARY. *If $p \geq k \geq 3$, then a linear MDS code of length $q+1$ over the finite field $\mathbb{F}_q$, $q = p^h$, is a Reed-Solomon code.*

In the second part of the talk, we will briefly discuss some examples of arcs of largest possible size in vector spaces, and explain the ideas and techniques from [2] that have led to the classification result mentioned above.

The third part of the talk will be devoted to some recent results found in [1], [3] and [5]. In [1], the connection between arcs of vector spaces and inclusion matrices is described. In [3] and [5], this leads to extension results of arcs. A particular example of such a result is the following.

THEOREM. **(S. Ball and J. De Beule [5])** *Suppose that q is odd and that G is an arc of $V(k,q)$ of size $3k-6$. Suppose that E is a subset of G of size $2k-3$ and that G projects to a subset of a conic from every $(k-3)$-subset of E. Then G cannot be extended to an arc of size $q+2$.*

References

[1] Simeon Ball. Extending small arcs to large arcs. http://arxiv.org/abs/1603.05795.

[2] Simeon Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *J. Eur. Math. Soc. (JEMS)*, 14(3):733–748, 2012.

[3] Simeon Ball. On arcs and quadrics. In Sylvain Duquesne and Svetla Petkova-Nikova, editors, *Arithmetic of Finite Fields*, number 10064 in LNCS, pages 95–104. 6th International Workshop, WAIFI 2016, Springer, 2017.

[4] Simeon Ball and Jan De Beule. On sets of vectors of a finite vector space in which every subset of basis size is a basis II. *Des. Codes Cryptogr.*, 65(1-2):5–14, 2012.

[5] Simeon Ball and Jan De Beule. On subsets of the normal rational curve. *IEEE Trans. Inform. Theory*, 63(6):3658–3662, 2017.

Vrije Universiteit Brussel, Department of Mathematics, Pleinlaan 2, B–1050 Brussel

jan@debeule.eu