# ADDITIVE MDS CODES

SIMEON BALL AND SAM ADRIAENSEN

Abstract. We prove that an additive code over a finite field which has a few projections which are equivalent to a linear code is itself equivalent to a linear code, providing the code is not too short.

## 1. MDS codes

Let $A$ be a finite set and let $n$ and $k$ be positive integers. A *code* $C$ of *minimum distance* $d$ is a subset of $A^n$ in which any two elements of $C$ differ in at least $d$ coordinates. Fixing any $d-1$ coordinates, it follows that any two codewords cannot agree on the remaining $n-d+1$ coordinates. Thus, we arrive at the *Singleton bound*

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

A *maximum distance separable (MDS) code* $C$ is a subset of $A^n$ of size $|A|^{n-d+1}$. If there is no restriction on the size of $A$ then MDS codes are the best performing codes when we apply nearest neighbour decoding. They have the property that a codeword can be recovered from any $k = n - d + 1$ coordinates, which makes them very useful, for example, in distributed storage systems. Assuming that $|C| = |A|^k$, the Singleton bound can be rewritten as

$$n \geqslant k + d - 1.$$

The ubiquitous example of an MDS code is the Reed-Solomon code. The Reed-Solomon code is an example of a linear code in which the alphabet is a finite field $\mathbb{F}_q$ and $C$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$. The Reed-Solomon code has length $n = q + 1$ which can be extended to a code of length $q+2$ in the case that $k \in \{3, q-1\}$ and $q$ is even. Its codewords are the evaluation of polynomials of degree at most $k-1$. To give a more precise definition, suppose $\mathbb{F}_q = \{a_1, \ldots, a_q\}$. The Reed-Solomon code is

$$C = \{(f(a_1), \ldots, f(a_q), c_f) \mid f \in \mathbb{F}_q[X], \quad \deg f \leqslant k-1\},$$

where $c_f$ is the coefficient of $X^{k-1}$ in $f$.

There are no known MDS codes which are better than the Reed-Solomon code and it is generally assumed that there are none. The *MDS conjecture* reflects this and states that for an $(n, q^k, d)_q$ MDS code where $d \geqslant 3$, the length $n$ satisfies $n \leqslant q + 1$, unless $k \in \{3, q-1\}$ and $q = 2^h$ in which case $n \leqslant q + 2$.

The MDS conjecture has been verified for linear codes when $q$ is prime [2]. It is also known to hold for linear codes when $q$ is square and $k \leqslant c\sqrt{q}$, where the constant $c$ depends

*Date*: 16 June 2022.

The author has been partially supported by PID2020-113082GB-I00 financed by MCIN / AEI / 10.13039/501100011033, the Spanish Ministry of Science and Innovation.

The talk at the 8IMM 2022 has been given by the first author.

on whether $q$ is odd or even. And for $q$ non-square and $k \leqslant c'\sqrt{pq}$, where again the constant $c'$ depends on whether $q$ is an odd power of an even or odd prime. See [3] for a recent survey. It is also known to hold for all MDS codes over alphabets of size at most 8, see [5].

## 2. Additive MDS codes

Here, we will be interested in additive codes over $\mathbb{F}_q$. It seems reasonable that relaxing linear to additive might allow one to find counter-examples to the MDS conjecture. However, this has not been the case thus far.

Since additive are always linear over some subfield, we fix this subfield as $\mathbb{F}_q$ and consider the code over $\mathbb{F}_{q^h}$. In [4] it was confirmed that the MDS conjecture is true for additive MDS codes over $\mathbb{F}_9$ and $\mathbb{F}_{16}$, where in the last case linearity over $\mathbb{F}_4$ is assumed.

Let us denote by an $[n,k]_{q^h}$ MDS code any $(n, q^k, n-k+1)_{q^h}$ additive MDS code which is linear over $\mathbb{F}_q$. Recall that the projection of a code $C$ on the $i$-th coordinate is the code obtained from $C$ taking those codewords with a zero in the $i$-th coordinate. The projection of a $[n,k]_{q^h}$ MDS code is a $[n-1,k-1]_{q^h}$ MDS code.

The following theorem from [1] is a strengthening of a similar theorem used in [4] and will be the main focus of the talk.

**Theorem 2.1.** *Let $C$ be an $[n,k]_{q^h}$ MDS code. Suppose one of the following holds.*

(1) *$k = 3$, $h \in \{2,3\}$, $n > \max\{q^{h-1}, hq-1\} + 3$ and $C$ has three coordinate positions from which its projection is equivalent to a linear code.*
(2) *$k > 3$, $n > q^{h-1}+k$ and there are disjoint subsets $A$ and $B$ of the coordinate positions of $C$ such that $|A| + |B| \leq k-2$, and the projections from $A$ and $B$ are equivalent to linear codes.*

*Then $C$ itself is equivalent to a linear code.*

Note that in the above an additive code $C$ is equivalent to a linear code if there are linearised maps

$$\sigma_i : x \mapsto \sum_{i=0}^{h-1} c_{ij} x^{q^i}$$

such that

$$\{(\sigma_1(u_1), \ldots, \sigma_n(u_n)) \mid (u_1, \ldots, u_n) \in C\}$$

is linear over $\mathbb{F}_{q^h}$.

## References

[1] S. Adriaensen and S. Ball, On additive MDS codes with linear projections, preprint.
[2] S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis, *J. Eur. Math. Soc.*, **14** (2012) 733–748.
[3] S. Ball and M. Lavrauw, Arcs in finite projective spaces, *EMS Surv. Math. Sci.*, **6** (2019) 133–172.
[4] S. Ball, G, Gamboa and M. Lavrauw, On additive MDS codes over small fields, *Adv. Math. Commun.*, to appear.
[5] J. I. Kokkala and P. R. J. Östergård, Further results on the classification of MDS codes, *Adv. Math. Commun.*, **10** (2016) 489–498.

Simeon Ball Universitat Politècnica Catalunya
*Email address*: simeon.michael.ball@upc.edu

Sam Adriaensen Vrije Universiteit Brussel
*Email address*: Sam.Adriaensen@vub.be