On additive codes over finite fields *

Simeon Ball, Michel Lavrauw, and Tabriz Popatia

Abstract

In this article we prove a Griesmer type bound for additive codes over finite fields. This new bound gives an upper bound on the length of fractional maximum distance separable codes, codes which attain the Singleton bound. We prove that this bound can be obtained in some cases, surpassing the length of the longest known codes in the non-fractional case. We also provide some exhaustive computational results over small fields and dimensions.

1 Introduction

The full version of this work can be found in [1].

Let $\mathbb{F}_q$ denote the finite field with q elements. An *additive code* of length n over $\mathbb{F}_{q^h}$ is a subset C of $\mathbb{F}_{q^h}^n$ with the property that for all $u, v \in C$ the sum $u + v \in C$. It is easy to prove that an additive code is linear over some subfield, which we will assume to be $\mathbb{F}_q$. An additive code is *linear over* $\mathbb{F}_{q^h}$ if $u \in C$ implies $\lambda u \in C$ for all $u \in C$ and all $\lambda \in \mathbb{F}_{q^h}$.

We use the notation $[n, r/h, d]_q^h$ code to denote an additive code of length n over $\mathbb{F}_{q^h}$, of size q^r and minimum distance d. For an additive code C, the minimum distance d is equal to the minimum weight, so this is equivalent to saying that each non-zero vector in C has at least d non-zero coordinates. We will be particularly interested in the case where r/h is not an integer, we will call these codes *fractional codes*, and codes such that $r/h \in \mathbb{N}$ *integral codes*.

2 Griesmer bound for additive codes

The Griesmer bound [4] for linear codes states that, if there is a $[n, k, d]_q$ linear code then

$$n \geqslant \sum_{j=0}^{k-1} \lceil \frac{d}{q^j} \rceil.$$

This bound can be reformulated as $\mathrm{n} \geqslant k + d - m + \sum_{j=1}^{m-1} \lceil \frac{d}{q^j} \rceil$, where we chose $m \leqslant k-1$ such that $q^m < d \leqslant q^{m+1}$, or $m = k$ if $q^k < d$. We prove that a similar but weaker bound holds for additive codes over finite fields,

Theorem 1. *If there is a $[n, r/h, d]_q^h$ additive code then*

$$n \geqslant \lceil r/h \rceil + d - m - 2 + \lceil \frac{d}{f(q,m)} \rceil,$$

where $r = (k-1)h + r_0$, $1 \leqslant r_0 \leqslant h$,

$$f(q,m) = \frac{q^{mh+r_0}(q^h - 1)}{q^{mh+r_0} - 1}$$

*5 April 2024. The first and third author are supported by the Spanish Ministry of Science, Innovation and Universities grant PID2020-113082GB-I00 funded by MICIU/AEI/10.13039/501100011033.

and $0 \leqslant m \leqslant k-2$ *is such that*

$$q^{mh+r_0} < d \leqslant q^{(m+1)h+r_0}$$

or $m = k-2$ *if* $d > q^r$.

We will also show that simply replacing k by $\lceil r/h \rceil$ or $\lfloor r/h \rfloor$ in (2) does not lead to a valid bound for additive codes by constructing additive codes that invalidate these natural generalisations. Furthermore we will show that we can reach the bound given by Theorem 1.

An additive $[n, r/h, d]_q^h$ code is equivalent to the following geometric structure. We define $\mathcal{X}$ to be the set of n subspaces of dimension at most $h-1$ in $\mathrm{PG}(r-1, q)$ with the property that at most $n-d$ of the subspaces are contained in a hyperplane. This representation of additive codes allows us to look at the codes geometrically, which is instrumental in a lot of the proofs and intuitions in this article. This is especially true for constructions of additive codes and classifying their dual code.

3 Singleton bound for additive codes

We will be particularly interested in codes C which meet the Singleton bound

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

for linear codes the Singleton bound can be reformulated as

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

Codes which attain this bound are called maximum distance separable codes, or simply MDS codes. MDS codes are an important class of codes, which are implemented in many applications where we can allow q to be large.

The Griesmer bound gives two important bounds for linear MDS codes. These results are well-known, but we list these as theorems since we will obtain similar bounds for additive MDS codes.

Theorem 2. *If* $k \geqslant 2$ *and there is a* $[n, k, d]_q$ *linear MDS code then* $d \leqslant q$ *and* $n \leqslant q + k - 1$.

Theorem 3. *If* $n \geqslant k + 2$ *and there is a* $[n, k, d]_q$ *linear MDS code then* $k \leqslant q - 1$.

As observed in previous articles, [5, Theorem 10], the Singleton bound can be reformulated for additive codes as

$$k = \lceil r/h \rceil \leqslant n - d + 1,$$

since n and d are always integers. We call codes which attain this bound additive MDS codes. Interestingly, the restrictions from the above theorems do not carry over to additive codes. We will provide a version for these bounds for additive codes and examples which better these bounds.

From Theorem 1 we get the following theorem for additive MDS codes that is the equivalent to Theorem 2.

Theorem 4. *If there is an* $[n, r/h, d]_q^h$ *additive MDS code then*

$$d \leqslant q^h - 1 + \frac{q^h - 1}{q^{r_0} - 1}$$

and

$$n \leqslant k - 2 + q^h + \frac{q^h - 1}{q^{r_0} - 1},$$

where $r = (k-1)h + r_0 > h$ *and* $1 \leqslant r_0 \leqslant h$.

In Theorem 2 we have that $d \leqslant q^h$, so the bound in Theorem 4 is the same when $r_0 = h$ and slightly weaker when $r_0 \neq h$. Furthermore notice a fractional additive MDS code n can be longer than the linear code by a tail of $\frac{q^h-1}{q^{r_0}-1} - 1$. We also have a an equivalent result to Theorem 3 for additive codes given by

Theorem 5. *If there is an $[n, r/h, d]_q^h$ additive MDS code C and $n \geqslant \lceil r/h \rceil + 2$ then*

$$\lceil r/h \rceil \leqslant q^h - 1 + (r_0 - h)\frac{q^h - q^{h-1}}{q^h - 1}.$$

In the next theorem we construct some additive MDS codes which prove that the bound in Theorem 4 is attainable if r_0 divides h and $k = 2$. Observe that Theorem 2 implies that for linear codes with $k = 2$, $n \leqslant q^h + 1$, so the following construction exceeds the bound of linear codes.

Theorem 6. *If r_0 divides h then there is a $[n, 1 + (r_0/h), n - 1]_q^h$ additive MDS code where*

$$n = q^h + \frac{q^h - 1}{q^{r_0} - 1}.$$

A similar construction can be used to prove that the bound in Theorem 4 is also attainable when $k = 3$ and $q = 2$, given by

Theorem 7. *There is a $[2^{h+1}, 2 + 1/h, 2^{h+1} - 2]_2^h$ additive MDS code.*

Although the codes constructed in Theorem 6 and Theorem 7 have very small rate, it is of interest that their length is superior to that of their linear counterparts. In the article [1] we also classify additive MDS codes over small fields and observe, once more, that there are additive MDS codes whose length exceeds linear MDS codes.

In the previous two constructions, we have that k is small. In the following constructions, we look at the other extreme, when d is small.

Theorem 8. *Let π_0 and π_∞ be h dimensional subspace of $\mathbb{F}_q^{2h} = \pi_0 \oplus \pi_\infty$. If there are k r_i-dimensional subspace π_i (with $r_i < h$) such that*

$$\pi_i \cap \pi_j = \{0\}$$

for all distinct $i, j \in \{0, 1 \ldots, k, \infty\}$, and with

$$\sum_{i-1}^{k} r_i = r,$$

then there exists an $[\lceil r/h \rceil] + 2, r/h, 3]_q^h$ additive MDS code.

From Theorem 8 we get the following theorem, which implies that the bound in Theorem 5 is atainable when $r_0 = h - 1$, given by

Theorem 9. *There exists an $[\lceil r/h \rceil] + 2, r/h, 3]_q^h$ additive MDS code for all $\lceil r/h \rceil \leq q^h - 1$*

4 The dual of an additive code

The dual of an additive $[n, r/h, d]_q^h$ code C is defined by

$$C^\perp = \{v \in \mathbb{F}_{q^h}^n \mid \mathrm{tr}_{q^h \mapsto q}(u \cdot v) = 0, \text{ for all } u \in C\},$$

where $\mathrm{tr}_{q^h \mapsto q}$ denotes the trace function from $\mathbb{F}_{q^h}$ to $\mathbb{F}_q$, and $u \cdot v$ denotes the euclidean inner product.

Since an $\mathbb{F}_q$-basis for C defines r equations for the $\mathbb{F}_q$-subspace $C^\perp$, the dual code is an additive $[n, n-r/h, d^\perp]_q^h$ code. Note that as an $\mathbb{F}_q$-vector space the vector space $\mathbb{F}_{q^h}^n$ has dimension hn implying that $|C^\perp| = q^{nh-r}$.

Recall that in Section 2, we defined a set of subspaces $\mathcal{X}$ of $PG(r-1,q)$ from an additive code of size q^r. We say an additive code is *full* if all the elements of $\mathcal{X}$ are of rank h, i.e. projective $(h-1)$-dimensional subspaces of $PG(r-1,q)$ (and *non-full* otherwise). We can always extend the subspaces of $\mathcal{X}$ so that they have rank r. This can be done arbitrarily without the minimum distance decreasing. Thus, a non-full additive $[n, r/h, d]_q^h$ code C can always be converted in a full additive $[n, r/h, \geqslant d]_q^h$ code. Using the concept of full and non-full additive codes we get the following results.

Theorem 10. *C is a non-full additive $[n, r/h, d]_q^h$ code if and only if $C^\perp$ is an additive $[n, n-r/h, 1]_q^h$ code.*

Theorem 11. *C is a full additive $[n, r/h, d]_q^h$ code with $d \geqslant 2$ if and only if $C^\perp$ is a full additive $[n, r/h, d^\perp]_q^h$ code with $d^\perp \geqslant 2$.*

Theorem 12. *A fractional sub-code of a linear code C is non-full.*

For linear codes we have that that the dual of an MDS code is also MDS. For additive codes the following result from [3, Theorem 4.3] (see also [6, Theorem 3.3]) classifies a group of additive MDS codes with a dual that is also MDS.

Theorem 13. *The dual of an integral additive MDS code is an additive MDS code.*

In the fractional case, as pointed out in [6, Example 3.1] the dual of a fractional MDS code is not necessarily MDS. Here, we give a precise condition on when the dual of a fracitonal MDS code is also MDS,

Let J be a subset of $\{1, \ldots, n\}$. The *projection* of an additive code C at J is

$$C/J = \{u \in C \mid u_j = 0, \text{ for all } j \in J\}.$$

Geometrically, the code C/J can be obtained from the set $\mathcal{X}$ in the following way. Let $\mathcal{X}_J$ be the set of subspaces corresponding to the coordinates of J. By projecting from the subspace Σ spanned by X_J, we obtain a set of $n - |J|$ subspaces $\mathcal{X}/J$ which are the subspaces of $\mathcal{X} \setminus \mathcal{X}_J$ projected from Σ. Note that the operation of projection of a code is also known as shortening a code.

We say a projection is *non-obliterating* if the dimension of C/J is at least h, i.e. $|C/J| \geqslant q^h$. Note that an obliterating projection always yields a non-full additive code.

Theorem 14. *Let C be an additive MDS code. The dual code $C^\perp$ is an additive full MDS code if and only if every non-obliterating projection of C is full.*

We can now improve on our bound for n in the case that the MDS code is non-full.

Theorem 15. *If there is a non-full $[n, r/h, d]_q^h$ additive MDS code then*

$$n \leqslant q^h + k - 1 + \frac{q^h - q^{r_0+1}}{q^{r_0} - 1},$$

where $r = (k-1)h + r_0 > h$ and $1 \leqslant r_0 \leqslant h$.

References

[1] S. Ball, M. Lavrauw, and T. Popatia, On additive codes over finite fields, preprint (2024).

[2] S. Ball and M. Lavrauw, Arcs in finite projective spaces, EMS Surveys in Mathematical Science, 6 (2019) 133–172.

[3] S. Ball, G. Gamboa and M. Lavrauw, On additive MDS codes over small fields, *Adv. Math. Commun.*, **17** (2023) 828–844.

[4] J. H. Griesmer, A bound for error-correcting codes, *IBM Journal of Res. and Dev.*, **4** (1960) 532–542.

[5] W. Cary Huffman, On the theory of $\mathbb{F}_q$ linear $\mathbb{F}_{q^t}$-codes, *Adv. Math. Commun.*, **7** (2013) 349–878.

[6] M.Yadav and A. Sharma, Some new classes of additive MDS and almost MDS codes over finite fields, *Finite Fields Appl.* **95** (2024) 102394.