Additive Codes and Finite Geometries

Tabriz Popatia
Joint work with Simeon Ball and Michel Lavrauw

IRSEE 2025

Table of Contents

Geometry of Additive Codes

Bounds for Additive Codes

Constructions of Additive codes

Additive codes

Definition

A *linear code* of length n, dimension k and distance d over $\mathbb{F}_q$ is a k dimensional linear subspace C of $\mathbb{F}_q^n$ where d is the minimum weight of any non-zero $c \in C$. We denote such a code by $[n, k, d]_q$

Additive codes

Definition

A *linear code* of length n, dimension k and distance d over $\mathbb{F}_q$ is a k dimensional linear subspace C of $\mathbb{F}_q^n$ where d is the minimum weight of any non-zero $c \in C$. We denote such a code by $[n, k, d]_q$

Definition

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 $u + v \in C$.

Additive codes

Definition

A *linear code* of length n, dimension k and distance d over $\mathbb{F}_q$ is a k dimensional linear subspace C of $\mathbb{F}_q^n$ where d is the minimum weight of any non-zero $c \in C$. We denote such a code by $[n, k, d]_q$

Definition

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 $u + v \in C$.

- We use the notation $[n, r/h, d]_q^h$ to denote an additive code of length n over $\mathbb{F}_{q^h}$, of size q^r and minimum distance d, which is linear over $\mathbb{F}_q$.
- Note when $h = 1$ we end up with a linear code.

Geometry of Additive Codes

An $[n, r/h, d]_q^h$ additive code is generated by a $r \times n$ matrix G where each column U is in $\mathbb{F}_{q^h}^r$

$$G = \begin{bmatrix} | & | & & | \\ U_1 & U_2 & \dots & U_n \\ | & | & & | \end{bmatrix}.$$

Geometry of Additive Codes

An $[n, r/h, d]_q^h$ additive code is generated by a $r \times n$ matrix G where each column U is in $\mathbb{F}_{q^h}^r$

$$G = \begin{bmatrix} | & | & & | \\ U_1 & U_2 & \dots & U_n \\ | & | & & | \end{bmatrix}.$$

Let $\{e_1, \dots, e_h\}$ be a basis for $\mathbb{F}_{q^h}$ over $\mathbb{F}_q$, then

$$U_i = \sum_{j=1}^{h} u_j e_j \quad \text{for} \quad u_j \in \mathbb{F}_q^r$$

Geometry of Additive Codes

An $[n, r/h, d]_q^h$ additive code is generated by a $r \times n$ matrix G where each column U is in $\mathbb{F}_{q^h}^r$

$$G = \begin{bmatrix} | & | & & | \\ U_1 & U_2 & \dots & U_n & . \\ | & | & & | \end{bmatrix}$$

Let $\{e_1, \dots, e_h\}$ be a basis for $\mathbb{F}_{q^h}$ over $\mathbb{F}_q$, then

$$U_i = \sum_{j=1}^{h} u_j e_j \quad \text{for} \quad u_j \in \mathbb{F}_q^r$$

Let $\pi_i = \langle u_1 \dots u_h \rangle$ be a subspace of $PG(r-1, q)$ for each U_i and $\mathcal{X}_G = \{\pi_1 \dots \pi_n\}$ be the multiset of subspaces

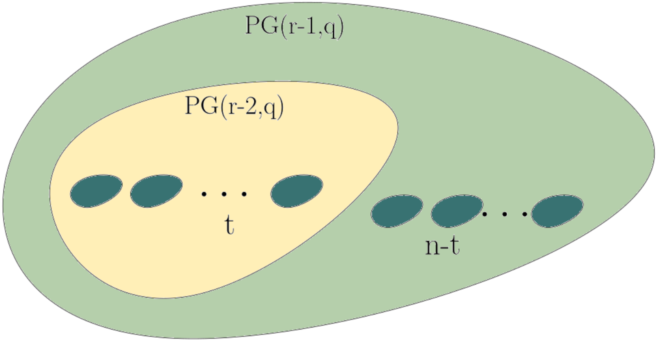
Relationship with Projective Geometries

- There exists a one-to-one relationship between codewords of the additive code and hyperplanes, such that a coordinate c_i of the codeword is 0 if and only if π_i is in the corresponding hyperplane.

Relationship with Projective Geometries

- There exists a one-to-one relationship between codewords of the additive code and hyperplanes, such that a coordinate c_i of the codeword is 0 if and only if π_i is in the corresponding hyperplane.
- If a hyperplane contains t members of $\mathcal{X}_G = \{\pi_1 \ldots \pi_n\}$ it has weight $n - t$.

Relationship with projective Geometries



Projective Systems

Definition

A *projective* $h-(n,r,d)_q$ *system* is a multiset S of n subspaces of $\mathrm{PG}(r-1,q)$ of dimension at most $h-1$ such that each hyperplane of $\mathrm{PG}(r-1,q)$ contains at most $n-d$ elements of S, and some hyperplane contains exactly $n-d$ elements of S.

Theorem

If C is an additive $[n,r/h,d]_q^h$ code, then $\mathcal{X}(\mathcal{C})$ is a projective $h-(n,r,d)_q$ system, and conversely, each projective $h-(n,r,d)_q$ system defines an additive $[n,r/h,d]_q^h$ code.

Mathon Example

Theorem (Mathon 2003)

There exists a set of 21 *lines* $\mathcal{X}$ *in* $PG(5,3)$ *such that every plane contains* 0 *or* 3 *lines of* $\mathcal{X}$.

Mathon Example

Theorem (Mathon 2003)

There exists a set of 21 lines $\mathcal{X}$ in $PG(5, 3)$ such that every plane contains 0 or 3 lines of $\mathcal{X}$.

Corollary

There exists a $[21, 3, 18]_3^2$ additive code

Griesmer Bound

Theorem (Griesmer 1960)

If there is an $[n,k,d]_q$ *linear code then*

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

Griesmer Bound

Theorem (Griesmer 1960)

If there is an $[n, k, d]_q$ linear code then

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

This bound can be reformulated as follows,

$$n \geqslant k + d - m + \sum_{j=1}^{m-1} \left\lceil \frac{d}{q^j} \right\rceil,$$

where $m \leqslant r - 1$ is such that $q^{k-1} < d \leqslant q^m$.

Additive Griesmer Bound 1.

Theorem (Ball, Lavrauw, P. 2024)

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

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

where $r = (\lceil r/h \rceil - 1)h + r_0$, $1 \leqslant r_0 \leqslant h$,

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

for all m *such that* $0 \leqslant m \leqslant \lceil r/h \rceil - 2$.

Corollary of Bound

Corollary

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

$$n \geqslant \lceil r/h \rceil + d - m + \left\lceil \sum_{j=1}^{m-2} \frac{d}{q^{jh}} \right\rceil ,$$

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

$$q^{(m-2)h+r_0} < d \leqslant q^{(m-1)h+r_0} \leqslant q^r.$$

Additive Griesmer Bound 2.

Theorem (Ball, Lavrauw, P. 2024)

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

$$n \geqslant d + \frac{q-1}{q^h - 1} \sum_{j=1}^{r-h} \lceil \frac{d}{q^j} \rceil.$$

Additive Griesmer Bound 2.

Theorem (Ball, Lavrauw, P. 2024)

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

$$n \geqslant d + \frac{q-1}{q^h-1}\sum_{j=1}^{r-h}\lceil \frac{d}{q^j}\rceil.$$

Theorem

If d *is such that* $q^{(m-2)h+r_0} < d \leqslant q^{(m-1)h+r_0}$, *for some* $m \in \{2, \dots, \lceil r/h \rceil\}$ *and*

$$(\lceil r/h \rceil - m)(q^h - 1) \geqslant (r-h)(q-1) + q^h - q$$

then the first first is better than the second.

Additive MDS codes

Theorem (Singleton Bound)

For an $[n, k, d]_q$ *linear code* $k \leq n - d + 1$

Theorem (Huffman 2013)

If there is an $[n, r/h, d]_q^h$ *additive code then the Singleton bound can be reformulated as* $\lceil r/h \rceil \leqslant n - d + 1.$

A code is called maximum distance sepearable (MDS) when it meets the bound.

Additive MDS Bound

Theorem (Griesmer)

If there exists a $[n, k, d]_{q^h}$ *linear MDS code then* $n \leqslant k - 1 + q^h$

Additive MDS Bound

Theorem (Griesmer)

If there exists a $[n, k, d]_{q^h}$ *linear MDS code then* $n \leqslant k - 1 + q^h$

Theorem (Ball, Lavrauw, P. 2024)

If there exists an $[n, r/h, d]_q^h$ *additive MDS code then*

$$n \leqslant \lceil r/h \rceil - 2 + q^h + \frac{q^h - 1}{q^{r_0} - 1},$$

where $r = (\lceil r/h \rceil - 1)h + r_0$, $1 \leqslant r_0 \leqslant h$,

Constructions of additive MDS codes

Example (Ball, Lavrauw, P 2024)

1. If r_0 divides h then there is a $[n, 1+(r_0/h), n-1]_{q^{r_0}}^{h/r_0}$ additive MDS code where

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

2. There is a $[2^{h+1}, 2+(1/h), d]_2^h$ additive MDS code.

3. There are 6 inequivalent $[12, 2.5, 10]_3^2$ additive MDS codes.

Construction of additive Codes from Linear codes

Theorem (Ball, P. 2025)

If there is a linear $[n, k, d]_q$ code then there is a $[n, k/h, d_{\mathrm{add}}]_q^h$ additive code where

$$d_{\mathrm{add}} \geqslant \sum_{j=0}^{h-1} \lceil \frac{d}{q^j} \rceil.$$

- A generalization of a theorem by Guan et al.

[1] C. Guan, R. Li, Y.Liu and Z. Ma
Some quaternary additive codes outperform linear counterparts
IEEE Transactions on Information Theory, vol. 69, no. 11, pp. 7122-7131, Nov. 2023.

New Construction of additive codes

Theorem (Ball, P. 2025)

If $h \leqslant s$ *and* $t \geqslant 2$ *then there is a* $[q^{st}-1, \frac{st+s+1}{h}, d]_q^h$ *additive code where*

$$d \geqslant q^{st} - 1 - \frac{q^{st}-1}{q^s-1} q^{s-h}.$$

New Construction of additive codes

Theorem (Ball, P. 2025)

If $h \leqslant s$ *and* $t \geqslant 2$ *then there is a* $[q^{st}-1, \frac{st+s+1}{h}, d]_q^h$ *additive code where*

$$d \geqslant q^{st} - 1 - \frac{q^{st}-1}{q^s-1} q^{s-h}.$$

- The above theorem reaches the additive griesmer bound when $t = 2$ and $s = h$.
- The code gives a $[63, 5, 45]_2^2$ code, which performs better than any known linear codes.

Integral additive codes that outperform linear codes

- There exists a $[21, 3, 18]_3^2$ additive code (Mathon et al. 2003)
- Six examples for $q = 2$ and $h = 2$ (Guan et al. 2023)
- Examples for the following parameters when n is sufficiently large $[n, 4, d]_2^2$, $[n, 3, d]_3^2$, $[n, 3, d]_2^3$, $[n, 3, d]_4^2$, $[n, 5, d]_2^2$, and $[n, 3, d]_5^2$ (Kurz 2024)

Generalized Maximal Arc

Definition

A maximal arc $\mathcal{X}$ of degree t in $PG(2, q)$ is a set of points such that every line is incident to 0 or t points.

Definition

A generalized maximal arc of degree t is a set $\mathcal{X}$ of $h-1$ dimensional subspaces in $PG(kh-1, q)$ such that every hyperplane contains 0 or t members of $\mathcal{X}$.

Corollary

A generalized maximal arc of degree t over $PG(kh-1, q)$ is equivalent to a $[n, k, n-t]_q^h$ additive two weight code.