Maximum scattered subspaces and maximum rank distance codes

Bence Csajbók

joint works with

Giuseppe Marino, Olga Polverino,
Corrado Zanella, Ferdinando Zullo

MTA-ELTE Geometric and Algebraic Combinatorics Research Group
ELTE Eötvös Loránd University, Budapest, Hungary
&
University of Campania "Luigi Vanvitelli"
Caserta, Italy

Irsee, 11 September 2017

Scattered subspaces

Let $V = V(r, q^n)$ be an r-dimensional $\mathbb{F}_{q^n}$-space.

Consider V as an rn-dimensional $\mathbb{F}_q$-space, and let $\mathcal{D}$ denote the following Desarguesian spread of n-dimensional $\mathbb{F}_q$-subspaces of V:

$$\mathcal{D} := \{\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} : \mathbf{v} \in V^*\}.$$

Definition (Blokhuis and Lavrauw)

An $\mathbb{F}_q$-subspace U of V is said to be *scattered* (w.r.t. $\mathcal{D}$) if each element of $\mathcal{D}$ meets U in an $\mathbb{F}_q$-subspace of dimension at most one, i.e. for each $\mathbf{v} \in V$ we have

$$\dim_{\mathbb{F}_q}(\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} \cap U) \leqslant 1.$$

For background and generalizations see **Michel Lavrauw:** Scattered spaces in Galois geometry in *Contemporary Developments in Finite Fields and Applications*, World Scientific 2016

Maximum scattered subspaces

Theorem (Blokhuis and Lavrauw 2000)

The rank of a scattered $\mathbb{F}_q$-space of $V(r, q^n)$ is at most $rn/2$.

A scattered $\mathbb{F}_q$-subspace U of V is said to be *maximum scattered* if for each scattered $\mathbb{F}_q$-subspace U' of V, $\dim_{\mathbb{F}_q} U' \leqslant \dim_{\mathbb{F}_q} U$.

Example (Blokhuis and Lavrauw 2000)

If r is even, say $r = 2m$, then

$$\{(x_1, x_1^q, x_2, x_2^q, \ldots, x_m, x_m^q) \colon x_1, x_2, \ldots, x_m \in \mathbb{F}_{q^n}\}$$

is a maximum scattered $\mathbb{F}_q$-subspace of $V(2m, q^n)$

Motivation

- Maximum scattered $\mathbb{F}_q$-subspaces of $V(2, q^n)$ correspond to $\mathbb{F}_q$-linear $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ functions determining maximum number of directions, that is, $(q^n - 1)/(q - 1)$.
- Maximum scattered $\mathbb{F}_q$-subspaces of $V(2, q^n)$ define maximum rank distance codes (Sheekey).
- Maximum scattered $\mathbb{F}_q$-subpsaces of $V(r, q^n)$, rn even define maximum rank distance codes (BCs, Marino, Polverino, Zullo).
- Maximum scattered spaces define two-intersection sets w.r.t. the hyperplanes of the corresponding projective space,
- and hence two-weight codes and strongly regular graphs.
- They can be used to construct translation caps, t-fold blocking sets.

How to construct maximum scattered subspaces?

According to the first example of this talk, there are examples of maximum scattered $\mathbb{F}_q$-subspaces with dimension mn in $V(2m, q^n)$, so the missing cases are when the dimension is odd.

Theorem (Bartoli, Giulietti, Marino, Polverino 2015)

Let U_i be a maximum scattered subspace of $V_i(r_i, q^n)$ for $i = 1, 2$. Then $U_1 \oplus U_2$ is a maximum scattered subspace of $V_1 \oplus V_2$.

It follows that as direct sum of maximum scattered subspaces in 2 and 3-dimensional vector spaces we can construct examples in every dimension.

Maximum scattered subspaces of $V(2, q^n)$

The elements of $\Gamma\mathrm{L}(2, q^n)$ preserve the Desarguesian spread $\mathcal{D}$ and hence the image of a maximum scattered subspace under an element of this group is also a maximum scattered subspace.

Two maximum scattered subspaces are **equivalent** if there is an element of $\Gamma\mathrm{L}(2, q^n)$ mapping one subspace to the other.

Up to equivalence, each n-dimensional $\mathbb{F}_q$-subspace can be written as

$$\{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\},$$

where $f(x)$ is a q-polynomial over $\mathbb{F}_{q^n}$, that is

$$f(x) = \sum_{i=0}^{n-1} a_i x^{q^i},$$

with $a_i \in \mathbb{F}_{q^n}$ for $i = 0, 1, \ldots, n-1$.

The known non-equivalent examples

Example (Blokhuis and Lavrauw 2000)

$\{(x, x^{q^s}) \colon x \in \mathbb{F}_{q^n}\}$, where $\gcd(s, n) = 1$.

Example (For $s = 1$ Lunardon and Polverino 2001, for $s \neq 1$ Sheekey 2016)

$\{(x, x^{q^s} + \delta x^{q^{n-s}}) \colon x \in \mathbb{F}_{q^n}\}$, where $\mathrm{N}_{q^n/q}(\delta) \neq 1$ and $\gcd(s, n) = 1$.

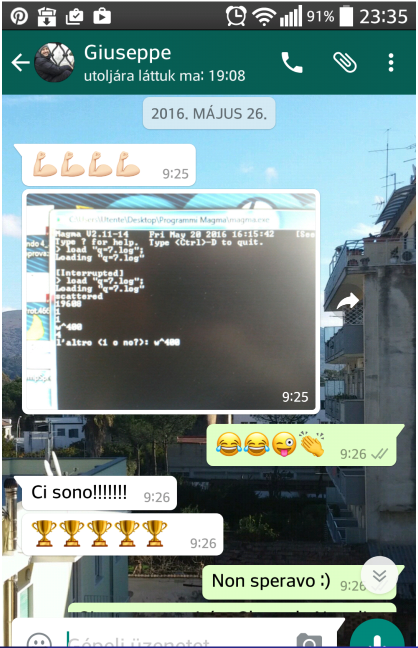
Theorem (Lavrauw and Van de Voorde 2010)

In $V(2, q^3)$ the only example is the Blokhuis–Lavrauw construction.

Theorem (BCs and Zanella 2017)

In $V(2, q^4)$ the only examples are the Blokhuis–Lavrauw and the Lunardon–Polverino constructions.

Are there further examples in $V(2, q^n)$, $n \geqslant 5$?


91%
23:35
Giuseppe
utoljára láttuk ma: 19:08
2016. MÁJUS 26.
9:25
C:\Users\Utente\Desktop\Programmi Magma\magma.exe
Magma V2.11-14 Fri May 20 2016 16:15:42
Type ? for help. Type <Ctrl>-D to quit.
> load "q=7.log";
Loading "q=7.log"
[Interrupted]
> load "q=7.log";
Loading "q=7.log"
scattered
19600
1
1
w^400
4
l'altro (1 o no?): w^400
9:25
9:26
Ci sono!!!!!!!
9:26
9:26
Non speravo :)
9:26

Recent constructions over $\mathbb{F}_{q^6}$ and $\mathbb{F}_{q^8}$

Example (BCs, Marino, Polverino and Zanella 2017)

For $q > 2$ there exists $\delta \in \mathbb{F}^*_{q^6}$ such that

$$\{(x, \delta x^q + x^{q^4}) \colon x \in \mathbb{F}_{q^6}\}$$

is a new maximum scattered $\mathbb{F}_q$-subspace of $V(2, q^6)$.
For example when $q \equiv 1 \pmod 4$, then take $\delta \in \mathbb{F}_{q^2}$ such that $\mathrm{N}_{q^2/q}(\delta) = -1$.

Example (BCs, Marino, Polverino and Zanella 2017)

Let q be odd, then

$$\{(x, \delta x^q + x^{q^5}) \colon x \in \mathbb{F}_{q^8}\}$$

is a new maximum scattered $\mathbb{F}_q$-subspace of $V(2, q^8)$ for each $\delta \in \mathbb{F}_{q^2}$ with $\delta^2 = -1$.

Consider in general the following $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$:

$$U = \{(x, \delta x^{q^s} + x^{q^{s+n}}) \colon x \in \mathbb{F}_{q^{2n}}\},$$

where $\gcd(s, n) = 1$ and $\mathrm{N}_{q^{2n}/q^n}(\delta) \neq 1$.

- If we consider $\mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ as a 4-dimensional $\mathbb{F}_{q^n}$-space, then U is always maximum scattered, that is, the one-dimensional $\mathbb{F}_{q^n}$-spaces meet U in $\mathbb{F}_q$-subspaces of dimension at most one.
- It defines a linear set of pseudoregulus type in $\mathrm{PG}(3, q^n)$. Using the known properties of this linear set we can prove that each one-dimensional $\mathbb{F}_{q^{2n}}$-space meets U in an $\mathbb{F}_q$-subspace of dimension at most two.
- With further restrictions on δ and putting $n = 3, 4$ we obtain the previous two examples, where the one-dimensional $\mathbb{F}_{q^{2n}}$-spaces meet U in $\mathbb{F}_q$-subspaces of dimension at most one.

Constructions in $V(3, q^{2t})$

- In order to find maximum scattered subspaces of $V(r, q^n)$ of rank $rn/2$ when r is odd and $n = 2t$ is even, we need
- maximum scattered subspaces of rank $3t$ in $V(3, q^{2t})$.
- **Bartoli, Giulietti, Marino, Polverino (2016)** found maximum scattered spaces for various infinite families of the parameters q and t. For certain parameters there are constructions also due to **Ball, Blokhuis, Lavrauw (2000)**.
- We generalized the construction of Bartoli, Giulietti, Marino, Polverino (2016) and gave a construction which works for every parameter.

Theorem (BCs, Marino, Polverino and Zullo 2017)

In $V(r, q^n)$, rn even, there exist maximum scattered $\mathbb{F}_q$-subspaces of dimension $rn/2$.

MRD-codes

Consider the set of $m \times n$ matrices $\mathbb{F}_q^{m \times n}$ over $\mathbb{F}_q$ with distance function

$$d(A, B) = rk\,(A - B)$$

for $A, B \in \mathbb{F}_q^{m \times n}$.
A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ is called a rank distance code.
The **minimum distance** of $\mathcal{C}$ is

$$d(C) = \min_{A,B \in \mathcal{C},\ A \neq B} \{d(A, B)\}.$$

For an $m \times n$ rank metric code $\mathcal{C}$ with minimum distance d the Singleton like bound, proved by **Delsarte** and later by **Gabidulin** is

$$\#\mathcal{C} \leqslant q^{\max\{m,n\}(\min\{m,n\}-d+1)}. \tag{1}$$

If this bound is achieved, then $\mathcal{C}$ is called a **maximum rank distance code (MRD-code)**.

The parameters of an $m \times n$ MRD-code over $\mathbb{F}_q$ with minimum distance d and dimension t over $\mathbb{F}_q$ are: $[m \times n, t, d]$.

Lately, such codes have been studied intensively since they define subspace codes, which are used in random network coding.

After fixing basis in $V(n,q)$ and $V(m,q)$, $m \times n$ matrices over $\mathbb{F}_q$ can also be viewed as $\mathbb{F}_q$-linear maps from $V(n,q)$ to $V(m,q)$.

Theorem (Sheekey 2015)

Let $\{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\}$ be a maximum scattered $\mathbb{F}_q$-space of $V(2,q^n)$. Then the following set of $\mathbb{F}_q$-linear $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ maps:

$$\{x \mapsto ax + bf(x) \colon a, b \in \mathbb{F}_{q^n}\}$$

is an MRD-code with parameters $[n \times n, 2n, n-1]_{\mathbb{F}_q}$.

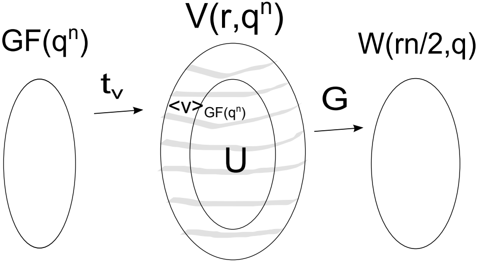
Theorem (BCs, Marino, Polverino, Zullo 2017):
Let U be a maximum scattered $\mathbb{F}_q$-subspace of $V = V(r, q^n)$, rn even.
For every $\mathbf{v} \in V$ let $t_{\mathbf{v}}$ denote the $\mathbb{F}_{q^n} \to V$ map:

$$x \in \mathbb{F}_{q^n} \mapsto x\mathbf{v} \in V.$$

Let W be an $\mathbb{F}_q$-space of dimension $rn/2$ and let G be any $\mathbb{F}_q$-linear $V \to W$ function such that $\ker G = U$. Then the set of $\mathbb{F}_{q^n} \to W$ maps

$$\{G \circ t_{\mathbf{v}} : \mathbf{v} \in V\}$$

is an MRD-code with parameters $[rn/2 \times n, rn, n-1]_{\mathbb{F}_q}$.



- Choosing a different $V \to W$ map G' with kernel U yields an equivalent MRD-code.
- What hapens when $r = 2$?
  Let $U = \{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\}$, $W = \mathbb{F}_{q^n}$ and define G as

$$(a, b) \in V(2, q^n) \mapsto f(a) - b,$$

  clearly it has U as kernel and the obtained MRD-code is

$$\{x \in \mathbb{F}_{q^n} \mapsto G(xa, xb) = f(xa) - xb \colon a, b \in \mathbb{F}_{q^n}\}.$$

  This is the the adjoint of the code obtained from the maximum scattered subspace $U = \{(x, \hat{f}(x)) \colon x \in \mathbb{F}_{q^n}\}$ by Sheekey's contruction. (Where $\hat{f}(x) = \sum_{i=0}^{n-1} a_{n-i}^{q^i} x^{q^i}$ is the adjoint of $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ w.r.t. the bilinear form $\langle x, y \rangle = \mathrm{Tr}_{q^n/q}(xy)$.)

The left-idealiser of an $n \times n$ MRD code $\mathcal{C}$ is

$$\{A \in \mathbb{F}_q^{n\times n} \colon AC \in \mathcal{C} \text{ for each } C \in \mathcal{C}\}.$$

Equivalent codes have isomorphic left-idealisers and this allowed us to prove the following.

Theorem (BCs, Marino, Polverino, Zanella 2017)

The MRD-codes with parameters $[6 \times 6, 12, 5]_{\mathbb{F}_q}$ *and* $[8 \times 8, 16, 7]_{\mathbb{F}_q}$ *which arise from the new maximum scattered subspaces*

$$\{(x, \delta x^q + x^{q^4}) \colon x \in \mathbb{F}_{q^6}\}$$

and

$$\{(x, \delta x^q + x^{q^5}) \colon x \in \mathbb{F}_{q^8}\}$$

are not equivalent to the known MRD-codes.

THANK YOU FOR YOUR ATTENTION