Scattered spaces in Galois geometry

Michel Lavrauw
Università di Padova

The 12th International Conference on Finite Fields and Their Applications - July 13-17, 2015
Scattered spaces

- In topology: A space $W$ is scattered if every non-empty subset $T$ contains a point isolated in $T$. [Cantor 1872]

- In projective geometry: $W$ is scattered w.r.t. a set of subspaces $D$, if $W$ intersects each element of $D$ in at most a point. (Motivated by the theory of blocking sets in projective spaces over finite fields [Ball-Blokhuism-ML 2000])
NOTATION AND TERMINOLOGY

Vector space $\leftrightarrow$ Projective space

$V = V(n, q) \leftrightarrow PG(V) = PG(n-1, q)$

subspace $U \leftrightarrow$ subspace $PG(U)$

$\dim(U) = \dim(PG(U)) + 1$
Scattered spaces in Galois geometry

- $\mathcal{D} = \text{any set of subspaces in } \mathbb{V}(n,q)$.

- A subspace $W$ is scattered w.r.t. $\mathcal{D} \iff \forall R \in \mathcal{D}: \dim(W \cap R) \leq 1$

- In this talk $\mathcal{D}$ will usually be a spread

 Partition of $\mathbb{V}\backslash\{0\}$ by subspaces of constant dimension

Projective space picture: $\mathbb{P}G(n-1,q)$
Let $D$ be a spread of $\text{PG}(n-1,q)$.

$$B(W) := \{ R \in D : \dim(W \cap R) \geq 1 \}$$

If $W$ is scattered and $\dim W = d$ then $|B(W)| = (q^d - 1)/(q-1)$.
Recent work related to scattered spaces

(in alphabetical order)

S. Ball, S. Barwick, A. Blokhuis, B. Csajbók,
G. Donati, N. Durante, W. Jackson, G. Lunardon,
G. Marino, O. Polverino, R. Trombetti,
J. Sheekey, G. Van de Voorde, C. Zanella
Outline

PART I
Basic theory and constructions

PART II
Applications
PART II Applications (a teaser)

1. Translation hyperovals
2. Field reduction and linear set
3. Two-intersection sets
4. Two-weight codes
5. Blocking sets
6. Embeddings of Segre varieties
7. Pseudo-reguli
8. Splashes of subgeometries
9. MRD codes
10. Semifield theory
PART I Basic theory and constructions

References

[1] S. Ball; A. Blokhuis; M. Lavrauw: Linear \( (q+1) \)-fold blocking sets in \( \text{PG}(2,q^4) \). Finite Field Appl. 2000


1.1 First example: Line spread $D$ in $\text{PG}(3, q)$

(a) every line not contained in $D$ is scattered;

(b) no plane is scattered

$\Rightarrow$ scattered space has proj. dim. $\leq 1$
1.2 Second example: plane spread in $\text{PG}(5,q)$

(a) every line not contained in an element of $S$ is scattered;

(b) no solid is scattered, since $|D|=q^3+1$;

(c) does there exist a scattered plane?
Maximal and maximum scattered

Let $U$ be scattered space w.r.t. $D$

- $U$ is called **maximal** scattered if $U$ is not contained in a larger scattered space.
- $U$ is called **maximum** scattered if any scattered space $T$ w.r.t. $D$ has $\dim T \leq \dim U$. 
Theorem 1 If $U$ is maximal scattered w.r.t. a $t$-spread in $V(rt,q)$, then $\dim U \geq (rt-t)/2 + 1$.

Proof If $U$ is scattered, then $\langle U, x \rangle$ is NOT scattered iff $x$ is contained in some $\langle R, U \rangle$ with $R \in B(U)$. Counting all such $x$ gives ($m = \dim U$)

$$(q^{m+t-1}-q^m)(q^{m-1}+q^{m-2}+q^{m-3}+...+q+1)+q^m$$

which should then be compared to the $|V(rt,q)|=q^{rt}$. 

\(\square\)
Suppose $U$ in $V(6,q)$ is maximal scattered. Then

(a) $\dim U \geq 2$

(b) $\dim U < 4$

(c) Theorem 1 ($r=2, t=3$) $\Rightarrow \dim U \geq 3/2+1 \Rightarrow \dim U \geq 3$

(a), (b), (c) $\Rightarrow \text{PG}(U)$ is plane in $\text{PG}(5,q)$

NOTE: maximum $\approx$ maximal in this case
1.4 Upper bound on scattered spaces

**Theorem 2** If $U$ is scattered w.r.t. a $t$-spread in $V(rt,q)$, then $\dim U \leq rt-t$.

**REMARK:** The bound from Theorem 2 is sharp $\Rightarrow$ “scattering spreads”
1.5 Changing the problem: “scatteringspreads”

Given a subspace $U$, can we find a spread $S$, such that $U$ is scattered w.r.t. $S$?

**Theorem 3** If $\dim U \leq rt-t$, then there exists a spread $S$ such that $U$ is scattered w.r.t. $S$.

**Theorem 3** $\Rightarrow$ bound from Theorem 2 is sharp.
1.6 Desarguesian spreads

Spread $S \to \mathcal{S}(S)$ design with parallelism

$S$ is a **Desarguesian spread** if $\mathcal{S}(S)$ is a Desarguesian affine space

$D_{r,t,q} = \text{Desarguesian } t\text{-spread in } V(rt,q)$
1.6 Desarguesian spreads

**Theorem 4** If $U$ is scattered w.r.t. $D_{r,t,q}$ then $\dim U \leq rt/2$.

**Corollary 5** A maximal scattered space $U$ w.r.t. $D_{r,t,q}$ satisfies $(rt-t)/2 + 1 \leq \dim U \leq rt/2$.

**Corollary 6** If $t=2$, then a maximal scattered space w.r.t. $D_{r,t,q}$ is maximum scattered and has $\dim = r$. 
1.6 Desarguesian spreads

**Theorem 7** If $r$ is even, then the upper bound $rt/2$ is sharp.

Lower bound for a maximum scattered space:

**Theorem 8** The dimension of a maximum scattered space w.r.t. $D_{r,t,q}$ is $2r'k$ where $r'|r$, $(r',t)=1$, and $r'k$ is maximal such that

$$k < (rt-t+3)/2$$

for $q=2$ and $r'=1$

and

$$r'k < (rt-t+r'+3)/2$$

otherwise.
1.7. Many open problems!

1. Determine the exact dimension for maximum scattered spaces w.r.t. $D_{r,t,q}$ (for $r$ odd).

2. What is the minimum dimension of maximal scattered spaces w.r.t. $D_{r,t,q}$?

3. What is the dimension of the second largest maximal scattered spaces w.r.t. $D_{r,t,q}$?

4. Can we determine the spectrum of maximal scattered spaces w.r.t. $D_{r,t,q}$?

5. Constructions! (geometric, polynomial method, tensor products, ...)
PART II Applications

1. Translation hyperovals
2. Field reduction and linear sets
3. Two-intersection sets
4. Two-weight codes
5. Blocking sets
6. Embeddings of Segre varieties
7. Pseudo-reguli
8. Splashes of subgeometries
9. MRD codes
10. Semifield theory
1. Translation hyperovals

Scattered t-space in $V(2t,2)$ w.r.t t-spread $S \leftrightarrow$ translation hyperoval in the projective plane $ABB(S)$ (André-Bruck-Bose)

[Denniston 1979], [O’Keefe-Pascasio-Penttila 1992], [Jha-Johnson 1992], [Cherowitzo 2010]
2. Field reduction and linear sets

Field reduction map $F_{r,t,q} : V(r,q^t) \rightarrow V(rt,q)$

- $D_{r,t,q} = \{F_{r,t,q}(v) : v \in V \setminus \{0\}\}$ is a Desarg. t-spread

- If $U \subseteq V(rt,q)$ then $B(U) \subseteq PG(r-1,q^t)$

- $B(U)$ is called an $F_q$-linear set

- $\dim U = \text{rank}$ of the linear set $B(U)$

**Proposition 9** An $F_q$-linear set $B(U)$ in $PG(r-1,q^t)$ has maximal size (w.r.t. to its rank) iff $U$ is scattered w.r.t. $D_{r,t,q}$

(more on this by B. Csajbók this afternoon)
3. Two-intersection sets

W.r.t. hyperplanes in $\text{PG}(r-1,q^t)$:

- **Type 1**: if $t=2u$, union of $\text{PG}(r-1,q^u)$'s
- **Type 2**: if $r=2s$, then union of $(s-1)$-dim subspaces

**Theorem 10** [Blokhuis-ML 2000] If $U$ is scattered w.r.t. $D_{r,t,q}$ of dim $rt/2$ then $B(U)$ is a two-intersection set w.r.t. hyperplanes in $\text{PG}(r-1,q^t)$, projectively inequivalent to the sets of type 1, 2.

two-intersection sets “of scattered type”
4. Two-weight codes

Each two-intersection set gives a two-weight code.

**Theorem 11** [Blokhuis-ML 2000] A scattered space of dimension \( m=rt/2 \) w.r.t. \( D_{r,t,q} \) gives rise to a linear \([((q^m-1)/(q-1)),r]\)-code with weights

\[
q^{m-t}(q^t-1)/(q-1) \text{ and } q^{m-t+1}(q^{t-1}-1)/(q-1).
\]

It follows from Theorem 10 that scattered two-weight codes are inequivalent to the ones arising from sets of type 1 and 2.
5. Blocking sets

[Blokhuis, Storme and Szönyi 1999] showed that an \( s \)-fold blocking set in \( \text{PG}(2,q^4) \) of size \( s(q^4+1)+c \) with \( s \) and \( c \) small enough contains the union of \( s \) disjoint Baer subplanes.

In [Ball-Blokhuis-ML 2000] a scattered linear set of rank 6 is constructed, which gives a \((q+1)\)-fold blocking set of size \((q+1)(q^4+q^2+1)\) in \( \text{PG}(2,q^4) \) \( (r=3,t=4) \) which is not the union of Baer subplanes.
5. Blocking sets

**Theorem 12** [Blokhuis-ML 2000] A scattered subspace $W$ of dimension $m$ w.r.t. $D_{r,t,q}$ induces a $(\mu_{k-1}(q))$-fold blocking set $B(W)$ w.r.t. $((rt-m+k)/t-1)$-dimensional subspaces in $PG(r-1,q^t)$, of size $\mu_{m-1}(q)$ where $1 \leq k \leq m$ and $t \mid m-k$.

Previous result [Ball-Blokhuis-ML 2000] for $m=6$, $r=3$, $t=4$, $k=2$:

$\mu_{k-1}(q) = \mu_1(q) = q+1$

$((rt-m+k)/t-1) = (12-6+2)/4-1 = 1$

$PG(r-1,q^t) = PG(2,q^4)$
6. Embeddings of Segre varieties

**Theorem 13** [ML-Sheekey-Zanella 2014]

If $U$ is a maximum scattered subspace w.r.t. $D_{2,t,q}$ then $B(U)$ (in $\text{PG}(2t-1,q)$) is a minimum embedding of the Segre variety $S_{t,t}(q)$.

(natural embedding is in $\text{PG}(t^2-1,q)$)

This minimum embedding turns out to be quite an interesting hypersurface.
7. Pseudo-regulus

Generalizes the concept of a regulus in $\text{PG}(3, q)$

- [Freeman 1980] $\text{PG}(3, q^2)$: $rt/2 = 4$
- [Marino et al. 2007] $\text{PG}(3, q^3)$: $rt/2 = 6$
- [ML-Van de Voorde 2013] $\text{PG}(2n-1, q^3)$: $rt/2 = 3n$
- [Lunardon et al. 2014] $\text{PG}(2n-1, q^t)$: $rt/2 = nt$
8. Splashes of subgeometries

8. Splashes of subgeometries

\[ S(T, L_\infty) \]

\[ T = \text{PG}(2, q) \]

\[ \text{Barwick-Jackson 2014, 201*] PG}(2, q^3) \]

\[ \text{ML-Zanella 2015] PG}(r-1, q^t) \] + characterisation of scattered splashes
9. MRD codes

(see talk by J. Sheekey on Friday)

Scattered space of dimension $n$ in $V(2n,q)$ $\rightarrow$ MRD code of dimension $2n$ over $GF(q)$, and minimum distance $n-1$.

$\rightarrow U_f: (x, f(x))$ and $D_a: (x, ax)$ \hspace{1cm} (x in $GF(q^n)$)

$\rightarrow U_f \cap D_a: f(x) = ax \iff (f-a)(x) = 0$

$\rightarrow U_f$ scattered $\Rightarrow \ker(f-a) \leq 1$ for all $0 \neq a$ in $GF(q^n)$

$\rightarrow \text{rank}(a+bf) \geq n-1$, for all $a,b$ in $GF(q^n)$, $(a,b) \neq (0,0)$

$\rightarrow C_f = <1, f>$ is an MRD code
10. Semifield theory

Finite non-associative division algebras: same axioms as for a finite field, but we do NOT assume commutativity and associativity for multiplication.

First studied by L. E. Dickson (1906)

Example: Generalized Twisted Fields (GTF) (Albert 1960)

\[(\text{GF}(q^n),+,\cdot): \ x\cdot y = xy - cx^ay^b\]

where \(\text{Fix}(a)=\text{Fix}(b)=F_q\), and \(N(c)\neq 1\)
A recent construction

[Dempwolff 2013]: translation planes and semifields from Dembowski-Ostrom polynomials

\[ S(F_1, F_2) = (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, +, \ast), \text{ whose multiplication is given by} \]

\[ (u, v) \ast (x, y) = (u, v) \begin{pmatrix} x & y \\ F_1(y) & \xi F_2(x) \end{pmatrix}, \quad (*) \]

A) \( F_1(x) = F_2(x) = A_{a,r}(x) = x^{q^r} - ax^{q^r} \) such that \( \gcd(n, r) = 1 \) and \( a \) is an element of \( \mathbb{F}_{q^n}^* \) with \( N_q(a) \neq 1 \), where \( N_q : \mathbb{F}_{q^n} \to \mathbb{F}_q \) denotes the norm function from \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \);

B) \( F_1(x) = F_2(x) = B_{b,r}(x) = 2H_{b,r}^{-1}(x) - x \) such that \( H_{b,r}(x) = x - bx^{q^r}, \gcd(n, r) = 1 \) and \( b \in \mathbb{F}_{q^n}^* \) with \( N_q(b) \neq \pm 1 \);

AB) \( F_i(x) = A_{b^2,r}(x), F_j(x) = B_{b,-r}(x), \{i, j\} = \{1, 2\} \) such that \( \gcd(n, r) = 1 \) and \( N_q(b) \neq \pm 1 \).
Scattered linear sets and semifields

- Semifield $\mathcal{S}$, l-dim over $N_l(\mathcal{S})$, $l$s-dimensional over its center $Z(\mathcal{S})=GF(q)$

$\implies$ linear set $R(\mathcal{S})$ of rank $l$s, disjoint from $\Omega(S_{l,l}(q^s))$

$\implies$ isotopism class $[\mathcal{S}] \leftrightarrow$ orbit of $H=H(S_{l,l}(q^s))$

[ML 2011]

$\implies$ $\mathcal{S}$ is a scattered semifield $\iff R(\mathcal{S})$ is scattered
Scattered linear sets and semifields

\[(u,v)*(x,y) = (ux + vF_1(y), uy + v\mu F_2(x)) \quad (\mu \text{ a nonsquare in } GF(q))\]

A) \[F_1(x) = F_2(x) = A_{a,r}(x) = x^{q} - ax^{-r}\] such that \(gcd(n, r) = 1\) and \(a\) is an element of \(\mathbb{F}_{q^n}^*\) with \(N_q(a) \neq 1\), where \(N_q : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q\) denotes the norm function from \(\mathbb{F}_{q^n}\) over \(\mathbb{F}_q\);

B) \[F_1(x) = F_2(x) = B_{b,r}(x) = 2H_{b,r}^{-1}(x) - x\] such that \(H_{b,r}(x) = x - bx^{q^r}\), \(gcd(n, r) = 1\) and \(b \in \mathbb{F}_{q^n}^*\) with \(N_q(b) \neq \pm 1\);

AB) \(F_i(x) = A_{b^2,i,r}(x), \ F_j(x) = B_{b,-r}(x), \ {i, j} = \{1, 2\}\) such that \(gcd(n, r) = 1\) and \(N_q(b) \neq \pm 1\).

Theorem 14 [ML-Marino-Polverino-Trombetti 2014, 2015]

A) contains new\(^*\) semifields

B) always isotopic to GTF: \(x*y = xy - cx^ay^b\)

AB) contains new\(^*\) semifields

*including Knuth operations and extension
Thank you for your attention!