(xv_t, xv_{t-1})-minihypers in $\mathrm{PG}(t, q)$

Peter Vandendriessche
(joint work with Ivan Landjev)

June 16, 2012

Linear codes and the Griesmer bound

Definition

A *linear* $[n, k, d]$*-code* C over a finite field $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$, such that every two distinct vectors in C differ in at least d positions.

Definition

The parameters n, k, d are called the *length*, *dimension* and *minimum distance* of C.

Linear codes and the Griesmer bound

A classical problem in coding theory is to find the shortest codes for a given k and d. Several lower bounds exist, one of them is the Griesmer bound.

Theorem (Griesmer, 1960; Solomon and Stiffler, 1965)

For every $[n, k, d]$-code over $\mathbb{F}_q$, one has

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

We are interested in finding and classifying families of Griesmer codes, i.e. codes which attain equality in the Griesmer bound.

Preliminaries

Let $\mathcal{P}$ be the point set of the projective space $\mathrm{PG}(t, q)$.

Definition

A *multiset* is a mapping $\mathfrak{K} : \mathcal{P} \to \mathbb{N}_0$ with its additive extension:

$$\forall \mathcal{Q} \subseteq \mathcal{P} : \mathfrak{K}(\mathcal{Q}) = \sum_{x \in \mathcal{Q}} \mathfrak{K}(x).$$

The *multiplicity* of a point or subset is its image under $\mathfrak{K}$.

Definition

A multiset is *proper* if at least one point has multiplicity 0.

Minihypers

Definition

An (f, m)-*minihyper* in $\mathrm{PG}(t, q)$ is a multiset of total multiplicity f such that the multiplicity of each hyperplane is at least m.

To avoid trivial cases, we will always assume $t \geq 2$ and $f > 0$.

Notation

For each $i \geq 0$, we denote $v_i = \frac{q^i - 1}{q - 1}$, the number of points in an $(i - 1)$-dimensional subspace.

We will study (xv_t, xv_{t-1})-minihypers in $\mathrm{PG}(t, q)$, for $x \in \mathbb{N}$ $(x \leq q)$.

Motivation 1

Theorem (Hamada, 1987)

There exists a bijective correspondence between the set of all non-equivalent $[n, k, d]_q$-codes meeting the Griesmer bound, and the set of $\left(\sum_{i=0}^{k-2} \mu_i v_{i+1}, \sum_{i=0}^{k-2} \mu_i v_i\right)$-minihypers in $\mathrm{PG}(k-1, q)$ with each $\mu_i \leq q-1$.

An interesting class of Griesmer codes arises from the special case $\mu_0 = \mu_1 = \ldots = \mu_{k-3} = 0$ and $\mu_{k-2} \neq 0$: these codes have $q^{k-2}|d$. Hence, we are interested in (xv_t, xv_{t-1})-minihypers in $\mathrm{PG}(t, q)$, where $x = \mu_{m-1} \leq q-1$.

Motivation 2

In PG(t, q), an upper bound on smallest size needed to m-block the hyperplanes is known:

Theorem

Let $\mathfrak{F}$ *be an* (f, m)*-minihyper in* PG(t, q)*. Then* $\frac{f}{m} \geq \frac{v_t}{v_{t-1}}$.

Hence, (xv_t, xv_{t-1})-minihypers in PG(t, q) are the parameterwise optimal minihypers.

Some examples

Some examples of (xv_t, xv_{t-1})-minihypers in $\mathrm{PG}(t, q)$.

Example

- A sum of x hyperplanes in $\mathrm{PG}(t, q)$ is a (xv_t, xv_{t-1})-minihyper.
- In particular, a sum of x lines in $\mathrm{PG}(2, q)$ is a (xv_2, xv_1)-minihyper.
- In particular, the sum of the lines in a dual hyperoval in $\mathrm{PG}(2, q)$, q even, is a $((q+2)v_2, (q+2)v_1)$-minihyper.
- All point multiplicities in the above minihyper are even. Dividing them by 2 yields a $(\frac{q+2}{2}v_2, \frac{q+2}{2}v_1)$-minihyper in $\mathrm{PG}(2, q)$, q even, which cannot be obtained as a sum of lines.

Previous classification results

Several strong results on (xv_t, xv_{t-1})-minihypers in $\mathrm{PG}(t, q)$ are known.

Theorem (Hill and Ward, 2007; Herdt, 2008)

Let $\mathfrak{F}$ be an (xv_t, xv_{t-1})-minihyper in $\mathrm{PG}(t, q)$, with $x \leq q - p^f$ for some nonnegative integer f. Then $\mathfrak{F}(\pi) \equiv xv_{t-1} \pmod{p^{f+1}q^{t-2}}$ for every hyperplane π in $\mathrm{PG}(t, q)$.

Corollary

If $x \leq q - \frac{q}{p}$, the minihyper consists of a sum of x hyperplanes.

A linear algebraic point of view

Definition

The *characteristic vector* of a multiset $\mathfrak{K}$ of $\mathrm{PG}(t, q)$ is the vector

$$w = (\mathfrak{K}(P))_{P \in \mathcal{P}} \in \mathbb{N}_0^{\mathcal{P}} \subset \mathbb{Q}^{\mathcal{P}}.$$

Clearly, every such vector uniquely corresponds to a multiset in $\mathrm{PG}(t, q)$. Often, we will identify multisets with their characteristic vectors.

Remark

Addition and scalar multiplication on multisets are defined by the corresponding operations on these vectors.

Why linear algebra?

Not all (xv_2, xv_1)-minihypers in $\mathrm{PG}(2,q)$ with $x < q$ are a sum of lines. However, the following holds.

Theorem (Landjev and Storme, 2009)

Let $\mathfrak{F}$ be an (xv_2, xv_1)-minihyper in $\mathrm{PG}(2,q)$ and let $\mathcal{L}$ be the lines of $\mathrm{PG}(2,q)$. Then exist nonnegative rational coefficients $(r_\ell)_{\ell\in\mathcal{L}}$ such that $\mathfrak{F} = \sum_{\ell\in\mathcal{L}} r_\ell \chi_\ell$.

This brings up a natural question: which (multi)sets in $\mathrm{PG}(t,q)$ can be written as a nonnegative rational sum of hyperplanes?

A useful characterisation

We have been able to solve this problem:

Theorem

Let $\mathcal{H}$ be the set of hyperplanes of $\mathrm{PG}(t, q)$, let $\mathfrak{K}$ be an arbitrary multiset in $\mathrm{PG}(t, q)$ and let w be its characteristic vector. Then:

- *w can be written uniquely as a rational sum of hyperplanes: $w = \sum_{H \in \mathcal{H}} r_H \chi_H$;*
- *$r_H \geq 0$ for each $H \in \mathcal{H}$ if and only if w is an (f, m)-minihyper with $m \geq \frac{v_{t-1}}{v_t} f$;*
- *if the multiset is proper, $r_H \geq 0$ for each $H \in \mathcal{H}$ if and only if $\mathfrak{K}$ is an (xv_t, xv_{t-1})-minihyper for some x.*

Whenever we write r_H, we mean the unique rational coefficients of the minihyper.

On the rational denominator

First we make an additional remark: all denominators divide q^{t-1}.

Theorem

For any proper (xv_t, xv_{t-1})-minihyper $\mathfrak{F} = \sum_{H \in \mathcal{H}} r_H \chi_H$ in $\mathrm{PG}(t,q)$, the smallest positive integer c for which $cr_H \in \mathbb{N}_0$ for all $H \in \mathcal{H}$, is a power of p, and a divisor of q^{t-1}.

Corollary

$c = 1$ if and only if the minihyper is a sum of hyperplanes.

Whenever we write c, we mean the number from the above theorem.

An improvement to the congruence result & lower bound

Theorem

Let $\mathfrak{F}$ be a proper (xv_t, xv_{t-1})-minihyper in $\mathrm{PG}(t, q)$. Then $\mathfrak{F}(H) \equiv xv_{t-1} \pmod{\frac{q^{t-1}}{c}}$ for every hyperplane H in $\mathrm{PG}(t, q)$.

When $x \leq q - p^{f+1}$, it can be shown that $\mathfrak{F}$ is proper, and that the term p^{f+1} divides $\frac{q}{c}$, which makes this result stronger than the result from [Hill and Ward, 2007; Herdt, 2008].

Corollary

Let $\mathfrak{F}$ be an (xv_t, xv_{t-1})-minihyper in $\mathrm{PG}(t, q)$ with $x < q$. Then $x > q - \frac{q}{c}$ or, equivalently, $c < \frac{q}{q-x}$.

For $x \leq q - \frac{q}{p}$, this yields $c < p$ and hence $c = 1$. Hence, this bound generalizes the previous bound.

On (in)decomposability

Definition

An (xv_t, xv_{t-1})-minihyper is (in)decomposable if it is (not) the sum of two nonempty minihypers $(x_1 v_t, x_1 v_{t-1})$ and $(x_2 v_t, x_2 v_{t-1})$. It is hyperplane-(in)decomposable if this can(not) be done with $x_2 = 1$.

Remark

- When $x < 2(q - \frac{q}{p} + 1)$, both concepts are equivalent.
- The size of the largest hyperplane-indecomposable (xv_t, xv_{t-1})-minihyper is $q^t - q$, the size of the second largest is $q^t - 2q + q/p - 1$. This generalizes earlier results by [Landjev and Storme, 2009].
- The size of the largest indecomposable (xv_t, xv_{t-1}) minihyper in $\mathrm{PG}(t, q)$ is not known.

A new correspondence result

Let $\mathbb{Z}_n$ be the ring of integers mod n and let $\mathcal{F}_c$ be the set of hyperplane-indecomposable minihypers in $\mathrm{PG}(t, q)$ with rational denominator c.

Definition

For a given integer n, the linear code $C_n^\perp(t, q)$ is the set of mappings $\mathcal{H} \to \mathbb{Z}_n$, with the additional property that for each point u, $\sum_{H \ni u} r_H$ is an integer.

Theorem

Each minihyper in $\mathcal{F}_c$ corresponds uniquely to a codeword in $C_c^\perp(t, q)$. This yields a natural bijective correspondence between $\mathcal{F}_c$ and the projective space code over the ring $\mathbb{Z}_c$.

A new construction technique

This correspondence yields several new construction techniques.

Lemma (Ball's construction)

Let B be a set of points in $\mathrm{PG}(t,q)$ and let e be the largest nonnegative integer such that B meets each hyperplane in 0 modulo p^e points. Then there exists an $\left(\frac{|B|}{p^e}v_t, \frac{|B|}{p^e}v_{t-1}\right)$-minihyper in $\mathrm{PG}(t,q)$ with $c = p^e$.

Lemma

Let A and B be sets of points in $\mathrm{PG}(t,q)$ and let e be the largest nonnegative integer such that A and B both meet each hyperplane in 1 modulo p^e points. Then there exists an (xv_t, xv_{t-1})-minihyper $\mathfrak{F}$ in $\mathrm{PG}(t,q)$ with $c = p^e$ and $x = |B \setminus A| + \lambda\frac{|A|-|B|}{p^e}$, for any $\lambda \in \{1, 2, \ldots, p^e - 1\}$.

A new construction

Example

Let $q = p^h$ and let e be a divisor of h. Let π be a plane in $\mathrm{PG}(t,q)$, let μ be the line $X_0 = 0$ and let

$$B = \{(1, z, z^{p^e}) | z \in \mathbb{F}_q\} \cup \{(0, z, z^{p^e}) | z \in \mathbb{F}_q^*\}$$

be a Rédei-type blocking set in π. Then applying the previous lemma to B and μ, one obtains an (xv_t, xv_{t-1})-minihyper in $\mathrm{PG}(t,q)$, with $x = q - \frac{q}{p^e} + 1 = q - \frac{q}{c} + 1$.

This shows the sharpness of our lower bound $x \geq q - \frac{q}{p^e} + 1$ when $e|h$. Previously, such minihypers were only known for $p = 2$. If $p \neq 2$ and $e \nmid h$, this sharpness is an open problem.

A surprisingly related conjecture

Definition

Let $d_S(C) = \min_{c \in C^*} \sum_{H \in \mathcal{H}} c_H$ with $c \in \{0, 1, \ldots, c-1\}^{\mathcal{H}}$.

Corollary

$d_S(C_p^\perp(2, q)) = (q - \frac{q}{p} + 1)p$, *i.e. every proper line-indecomposable (xv_2, xv_1)-minihyper with $c = p$ in* $\mathrm{PG}(2, q)$, *is a sum of at least $(q - \frac{q}{p} + 1)p$ lines (with coefficient $\frac{1}{p}$).*

Conjecture

$d_H(C_p^\perp(t, q)) = 2q - \frac{q-p}{p-1}$, i.e. ... sum of at least $2q - \frac{q-p}{p-1}$ different lines (with coefficient a multiple of $\frac{1}{p}$).

Moreover, the d_S-smallest and d_H-smallest known code words coincide.

Thank you for your attention!