Colloquium Coding Theory and Cryptography

Small weight code words

in the code of points and hyperplanes in $PG(n, q)$

Lins Denaux

Joint work with S. Adriaensen, L. Storme and Zs. Weiner

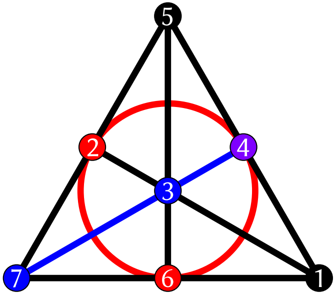
GHENT UNIVERSITY

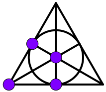
1 Preliminaries

The code $C_{n-1}(n, q)$

Vector space over $\mathbb{F}_p$ spanned by the rows of the incidence matrix of hyperplanes and points in $PG(n, q)$. Vectors = '**code words**'.

$$\text{hyperplanes}\left\{\overbrace{\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}}^{\text{points}}\right.$$



red + blue = $(0\ 1\ 1\ 0\ 0\ 1\ 1)$ = 

Known results in the plane: $C_1(2, q)$

Small weight code words ≈ **few** hyperplanes (= lines)?

The case $q = p$ prime (Szőnyi & Weiner):

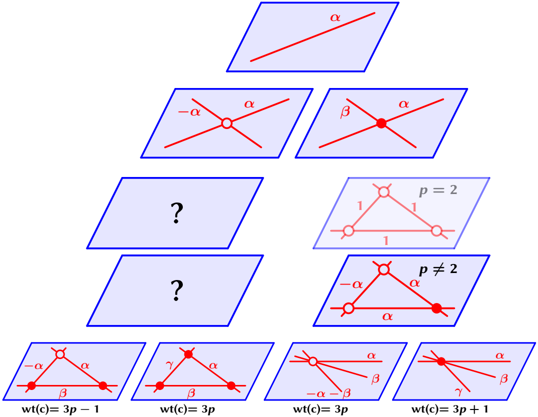
$\mathrm{wt}(c) = p + 1$

$\mathrm{wt}(c) = 2p\,(+1)$

$\mathrm{wt}(c) = 3p - 3$

$\mathrm{wt}(c) = 3p - 2$

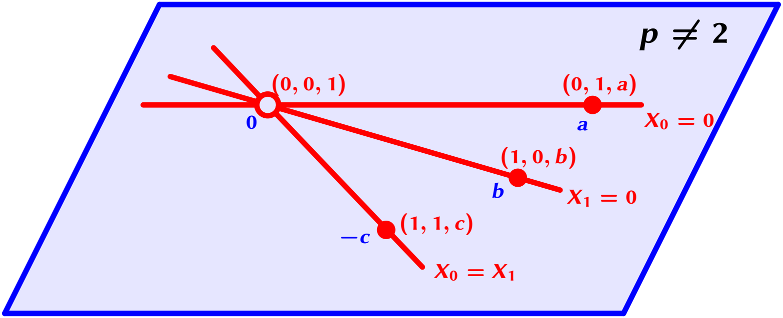
$\mathrm{wt}(c) = 3p\,(\pm 1)$



------------ $\mathrm{wt}(c) \leqslant \max\{3p + 1, 4p - 22\}$ ------------

2 Known results in the plane: $C_1(2, q)$

An 'odd' code word for $q = p$ prime (Bagchi; De Boeck & Vandendriessche):



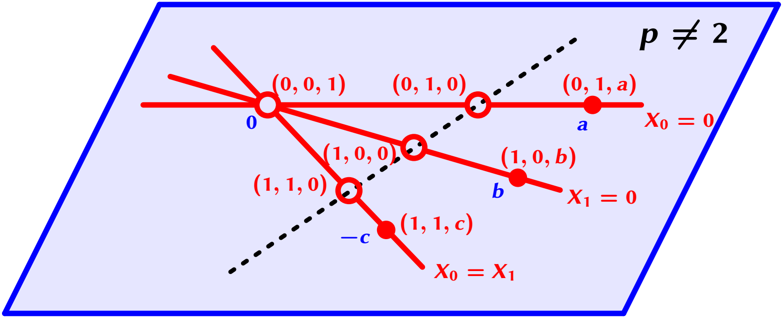
Proposition: $C_1(2, p)^\perp \leqslant C_1(2, p)$

Proof.

- $\dim(C_1(2, p^h)) = \binom{p+1}{2}^h + 1.$
- $(C_1(2, q) \cap C_1(2, q)^\perp) \oplus \mathbf{1} = C_1(2, q).$ □

2 Known results in the plane: $C_1(2, q)$

An ‘odd’ code word for $q = p$ prime (Bagchi; De Boeck & Vandendriessche):

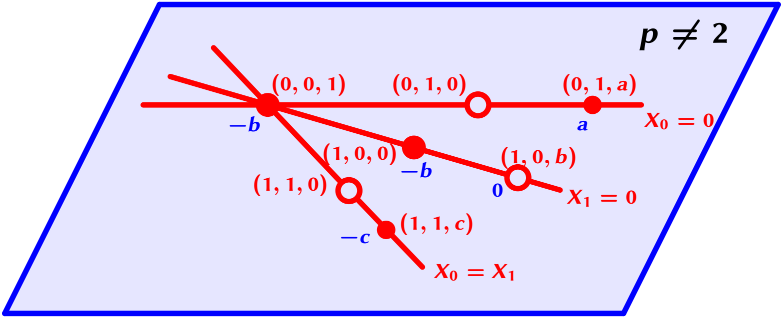


Proposition

- $\mathbf{wt(c) = 3p - 3}$, every $(2/3)$-secant $\rightarrow \alpha + \beta\,(+\gamma) = 0$.

2 Known results in the plane: $C_1(2, q)$

An ‘odd’ code word for $q = p$ prime (Bagchi; De Boeck & Vandendriessche):



Proposition

- $\mathbf{wt}(c) = 3p - 3$, every $(2/3)$-secant $\to \alpha + \beta\,(+\gamma) = 0$.
- $\mathbf{wt}(c) = 3p - 2$, every $(2/3)$-secant $\to \alpha + \beta\,(+\gamma) \neq 0$.

2 Known results in the plane: $C_1(2, q)$

Small weight code words ≈ **few** hyperplanes (= lines)?

The case $q = p$ prime (Szőnyi & Weiner):

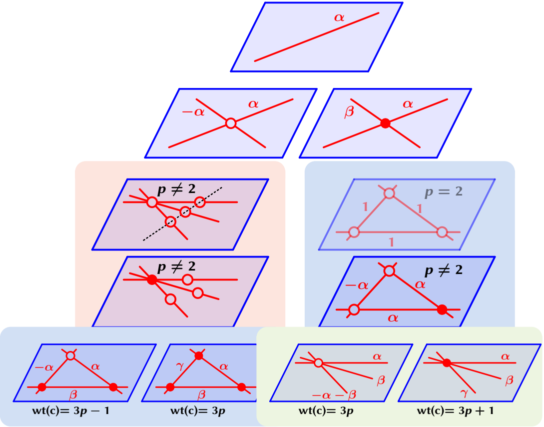
wt(c) $= p + 1$

wt(c) $= 2p\,(+1)$

wt(c) $= 3p - 3$

wt(c) $= 3p - 2$

wt(c) $= 3p\,(\pm 1)$



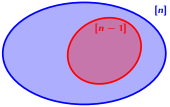
- - - - - - - - - - - - wt(c) $\leqslant \max\{3p + 1, 4p - 22\}$ - - - - - - - - - - - -

3 Known results in general: $C_{n-1}(n, q)$

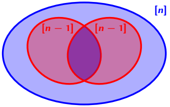
Smallest weight code words of $C_{n-1}(n, q)$: **generally known**.
Second smallest weight:
recently characterized (Polverino & Zullo).

weight ↓

$$\mathrm{wt}(c) = q^{n-1} + \cdots + q + 1$$

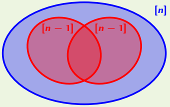


$$\mathrm{wt}(c) = 2q^{n-1}$$



First result: classification of the third smallest weight

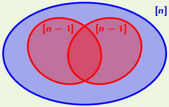
$$\mathrm{wt}(c) = 2q^{n-1} + \cdots + q + 1$$



Proof of third smallest weight: first approach

First result: classification of the third smallest weight

$$\mathbf{wt(c)} = 2q^{n-1} + \cdots + q + 1$$



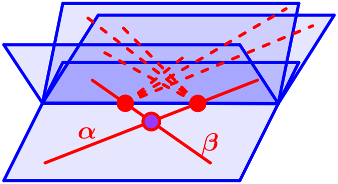
Proposition

For every k-space $\kappa \subseteq PG(n, q)$ and code word $c \in C_{n-1}(n, q)$:

$$c_{|\kappa} \in C_{k-1}(k, q).$$

The case $C_2(3, q)$, $\mathrm{wt}(c)$ small:

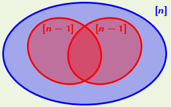
- Find a 2-secant.
- Find lots of characterized planes.
- Force the red lines to be coplanar.



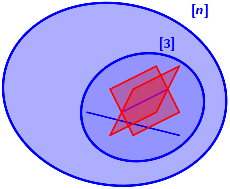
4 Proof of third smallest weight: first approach

First result: classification of the third smallest weight

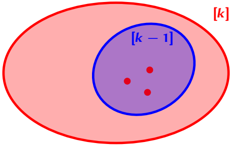
$$\mathbf{wt(c)} = 2q^{n-1} + \cdots + q + 1$$



The case $C_{n-1}(n, q)$, $wt(c)$ small:



- Each line intersects in 0, 1, 2, q or $q + 1$ points.

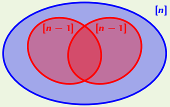


- Non-characterized spaces: contains affine part.
  - lots of points!
- Force all red points into two hyperplanes.

5 A quiet moment to think things through

First result: classification of the third smallest weight

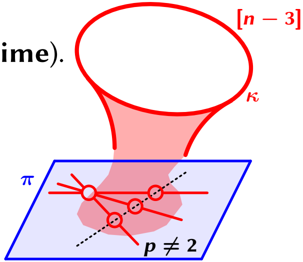
$$\mathbf{wt(c)} = 2q^{n-1} + \cdots + q + 1$$



for all c with $2q^{n-1} < wt(c) \leqslant \frac{5}{2}q^{n-1} - \frac{7}{5}q^{n-2}$.

And further...?

- 'Weird' code word c in plane π (for $q = p$ **prime**).
- Chose a disjoint $(n-3)$-space κ.



If $c = \sum_i \alpha_i l_i$, then $c' := \sum_i \alpha_i \langle l_i, \kappa \rangle$ is a linear combination of hyperplanes;
$\boldsymbol{wt(c') = 3p^{n-1} - 3p^{n-2}}$.

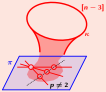
A quiet moment to think things through

Small weight code words ≈ **few** hyperplanes (= lines)?

The case $q = p$ prime (Szőnyi & Weiner):

Conjecture ($q = p$ prime, $p \geqslant 7$)

Code words up to weight $3p^{n-1} + p^{n-2} + \cdots + p + 1$
$\sim$ linear combinations of at most three hyperplanes
or a generalization of the 'weird' code word right.

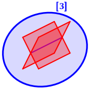


We can likely do better.

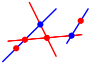
6 The Budapest effect

Before Budapest

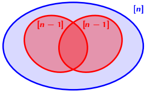
Proof in $C_2(3, q)$.



$(0, 1, 2 \parallel q, q+1)$-secants.



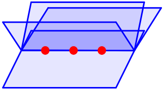
Proof in $C_{n-1}(n, q)$.



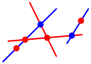
Bound: $\mathrm{wt}(c) \leqslant \mathbf{\frac{5}{2}} q^{n-1} - \frac{7}{5} q^{n-2}$

After Budapest

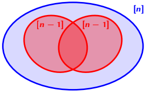
$(\geqslant \lfloor\sqrt{10q}\rfloor)$-secants.



$(0, 1, 2 \parallel q, q+1)$-secants.



Proof in $C_{n-1}(n, q)$.



Bound: $\mathrm{wt}(c) < \mathbf{3} q^{n-1} - 3\theta_{n-2}$

Using *all* information, we can proof all lines are

$$(0, 1, 2, \mathbf{3} \parallel \boldsymbol{q-1}, q, q+1)\text{-secants},$$

for all code words $c \in C_{n-1}(n, q)$,

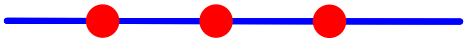
$$\mathrm{wt}(c) \lesssim \boldsymbol{4q^{n-1} - \sqrt{10}q^{n-2}\sqrt{q}}.$$

7 The smallest weight code words of $C_2(3, p)$

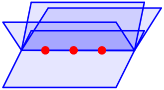
To simplify things, we consider a code word $\boldsymbol{c} \in \boldsymbol{C_2(3, p)}$, with

$$2p^2 + p + 1 < \mathrm{wt}(c) \leqslant 4p^2 - \sqrt{10}p\sqrt{p} - \frac{31}{2}p - 21$$

- There exists a 3-secant.



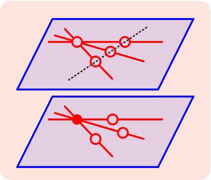
- The planes containing a 3-secant...

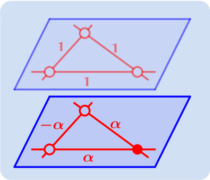


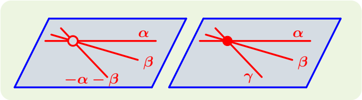
⋆ ... are all characterized.

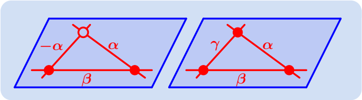
⋆ ... are all of the *same* green type, ***or***...

⋆ ... can be divided into two types: a green type and another type.



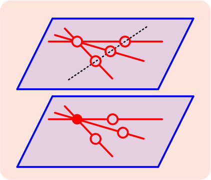


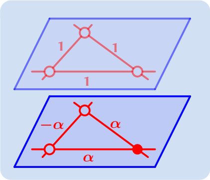


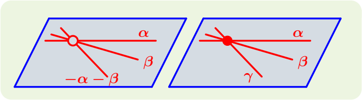


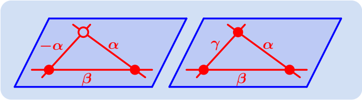
7 The smallest weight code words of $C_2(3, p)$

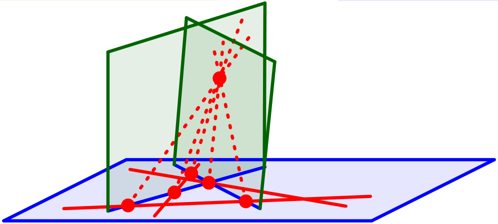
- ⋆ … are all characterized.
- ⋆ … are all of the *same* green type, ***or***…
- ⋆ … can be divided into two types:
  a green type and another type.











Results & further research

Our result: all small code words are cones

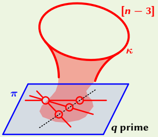
If:

- Prime power $q > 17$, $q \notin \{25, 27, 31, 32, 49, 121\}$.
- Code word $c \in C_{n-1}(n, q)$,

$$\mathrm{wt}(c) \leqslant \left(4q - \sqrt{10q} - \frac{39}{2}\right)\theta_{n-2} + \sqrt{10q} - \frac{3}{2}$$

$$\mathrm{wt}(c) \leqslant 4\left(q - \sqrt{q} - 4\right)\theta_{n-2} \text{ [simplified]}$$

Then $\mathrm{supp}(c)$ correspond to a cone with a $(n-3)$-dimensional vertex and a characterized plane as base.



Results & further research

Szőnyi & Weiner: the plane ($q = p^h$, $h \geqslant 2$, $q > 27$)

Code words of weight lower than $\frac{(p-1)(p-4)(p^2+1)}{2p-1}$, when $h = 2$,

$(\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$, when $h > 2$,

correspond to linear combinations of exactly $\left\lceil\frac{\mathrm{wt}(c)}{q+1}\right\rceil$ lines.

Our result: further classification ($q = p^h$, $h \geqslant 2$, $q > 27$)

Code words up to weight $\left(\left\lfloor\frac{1}{2^{n-1}}\sqrt{q}\right\rfloor - \frac{9}{4}\right)\theta_{n-1}$, when $h = 2$,

$\left(\left\lfloor\frac{1}{2^{n-2}}\sqrt{q}\right\rfloor - 1\right)\theta_{n-1}$, when $h > 2$,

correspond to linear combinations of exactly $\left\lceil\frac{\mathrm{wt}(c)}{\theta_{n-1}}\right\rceil$ hyperplanes.

Fin.[ite geometry is awesome!]

Thank you for your attention. Are there any
questions?