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

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

1

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





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





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



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

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

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



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

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

$$wt(c) = p + 1$$





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

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

$$wt(c) = p + 1$$

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



weight

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

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

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

wt(c) =
$$p + 1$$

wt(c) = $2p(+1)$
wt(c) = $3p - 3$

weight

weight

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

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



weight

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

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



weight

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

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



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

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

























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



Proposition: $C_1(2, p)^{\perp} \leq \overline{C_1(2, p)}$

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



Proposition: $C_1(2, p)^{\perp} \leq \overline{C_1(2, p)}$

Proof.

→ dim
$$(C_1(2, p^h)) = {\binom{p+1}{2}}^h + 1.$$

→ $(C_1(2, q) \cap C_1(2, q)^{\perp}) \oplus \mathbf{1} = C_1(2, q).$

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



Proposition: $C_1(2, p)^{\perp} \leq C_1(2, p)$

Proof.

$$\dim(C_1(2,p^h)) = {\binom{p+1}{2}}^h + 1.$$

$$(C_1(2,q) \cap C_1(2,q)^{\perp}) \oplus \mathbf{1} = C_1(2,q).$$

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



Proposition: $C_1(2, p)^{\perp} \leq \overline{C_1(2, p)}$

Proof.

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



Proposition

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

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



Proposition

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

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



Proposition

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

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

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



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

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



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

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


Smallest weight code words of $C_{n-1}(n, q)$: generally known.



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

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

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



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

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

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

weight



First result: classification of the third smallest weight

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



First result: classification of the third smallest weight

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



First result: classification of the third smallest weight

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



Proposition

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

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

First result: classification of the third smallest weight

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



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 $C_2(3, q)$, wt(c) small:

First result: classification of the third smallest weight

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



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 $C_2(3, q)$, wt(c) small:

Find a 2-secant.



First result: classification of the third smallest weight

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

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 $C_2(3, q)$, wt(c) small:

- Find a 2-secant.
- Find lots of characterized planes.



First result: classification of the third smallest weight

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

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 $C_2(3, q)$, wt(c) small:

- Find a 2-secant.
- Find lots of characterized planes.



First result: classification of the third smallest weight

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

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 $C_2(3, q)$, wt(c) small:

- Find a 2-secant.
- Find lots of characterized planes.



First result: classification of the third smallest weight

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

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 $C_2(3, q)$, wt(c) small:

- Find a 2-secant.
- Find lots of characterized planes.



First result: classification of the third smallest weight

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

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 $C_2(3, q)$, wt(c) small:

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



First result: classification of the third smallest weight

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



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

First result: classification of the third smallest weight

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

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

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





First result: classification of the third smallest weight

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

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

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





First result: classification of the third smallest weight

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

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.
 - Iots of points!







First result: classification of the third smallest weight

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

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.
 - Iots of points!
- Force all red points into two hyperplanes.







First result: classification of the third smallest weight

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



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

First result: classification of the third smallest weight

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



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

And further ...?

First result: classification of the third smallest weight

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



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

And further ...?

• 'Weird' code word *c* in plane π (for q = p **prime**).



First result: classification of the third smallest weight

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



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

And further ...?

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





First result: classification of the third smallest weight

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



[n - 3]

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

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;
 $wt(c') = 3p^{n-1} - 3p^{n-2}$.

5

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

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



5

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

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



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

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

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

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.

5

wt(c) =
$$3p - 3$$

wt(c) = $3p - 2$
wt(c) = $3p (\pm 1)$
wt(c) =

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

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

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

5

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.

Before Budapest

Proof in $C_2(3, q)$.



Before Budapest

Proof in $C_2(3, q)$.

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



Before Budapest

Proof in $C_2(3, q)$.

(0, 1, 2 || q, q + 1)-secants.

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



[3]

Before Budapest

Proof in $C_2(3, q)$.

(0, 1, 2 || q, q + 1)-secants.

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

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

Before Budapest

Proof in $C_2(3, q)$.

(0, 1, 2 || q, q + 1)-secants.

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

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

After Budapest

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



Before Budapest

Proof in $C_2(3, q)$.

(0, 1, 2 || q, q + 1)-secants.

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

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

After Budapest

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

$$[0, 1, 2 || q, q + 1)$$
-secants.

Before Budapest

Proof in $C_2(3, q)$.

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

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

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

After Budapest

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

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

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



Before Budapest

Proof in $C_2(3, q)$.

(0, 1, 2 || q, q + 1)-secants.

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

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

After Budapest

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

(0, 1, 2 || q, q + 1)-secants.

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

Bound: wt(c) $< 3q^{n-1} - \overline{3\theta}_{n-2}$


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: wt(c) $\leq \frac{5}{2}q^{n-1} - \frac{7}{5}q^{n-2}$



Using *all* information, we can proof all lines are (0, 1, 2, 3 || q - 1, q, q + 1)-secants, for all code words $c \in C_{n-1}(n, q)$, $\operatorname{wt}(c) \leq 4q^{n-1} - \sqrt{10}q^{n-2}\sqrt{q}$.

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

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

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

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

There exists a 3-secant.



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

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

- There exists a 3-secant.
- The planes containing a 3-secant...



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

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

- There exists a 3-secant.
- The planes containing a 3-secant...





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

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

- There exists a 3-secant.
- The planes containing a 3-secant...



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





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

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

- 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.







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







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









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









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









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





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





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





Our result: all small code words are cones

Our result: all small code words are cones

١f:

▶ Prime power q > 17, $q \notin \{25, 27, 31, 32, 49, 121\}$.

Our result: all small code words are cones If:

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

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

Our result: all small code words are cones If:

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

$$\begin{split} \mathrm{wt}(c) &\leq \left(4q - \sqrt{10q} - \frac{39}{2}\right)\theta_{n-2} + \sqrt{10q} - \frac{3}{2}\\ \mathrm{wt}(c) &\leq 4\left(q - \sqrt{q} - 4\right)\theta_{n-2} \text{ [simplified]} \end{split}$$

Our result: all small code words are cones If:

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

$$\begin{split} \mathrm{wt}(c) &\leq \left(4q - \sqrt{10q} - \frac{39}{2}\right)\theta_{n-2} + \sqrt{10q} - \frac{3}{2}\\ \mathrm{wt}(c) &\leq 4\left(q - \sqrt{q} - 4\right)\theta_{n-2} \text{ [simplified]} \end{split}$$

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

Our result: all small code words are cones If:

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

$$\begin{split} \mathrm{wt}(c) &\leq \left(4q - \sqrt{10q} - \frac{39}{2}\right)\theta_{n-2} + \sqrt{10q} - \frac{39}{2}\\ \mathrm{wt}(c) &\leq 4\left(q - \sqrt{q} - 4\right)\theta_{n-2} \text{ [simplified]} \end{split}$$

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



Szőnyi & Weiner: the plane ($q = p^h$, $h \ge 2$, 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 $\lceil \frac{\operatorname{wt}(c)}{q+1} \rceil$ lines.

Szőnyi & Weiner: the plane ($q = p^h$, $h \ge 2$, 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 $\lceil \frac{\operatorname{wt}(c)}{q+1} \rceil$ lines.

Our result: further classification ($q = p^h$, $h \ge 2$, 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 $\left\lceil \frac{wt(c)}{\theta_{n-1}} \right\rceil$ hyperplanes.



Fin.

Thank you for your attention. Are there any **questions?**



Fin. ite geometry is awesome!

Thank you for your attention. Are there any **questions**?