On the lengths of divisible codes

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

Kolloquium über Kombinatorik (KolKom) 2018
November 24, 2018
Universität Paderborn

joint work with Sascha Kurz

Linear codes

- finite field $\mathbb{F}_q$ of characteristic p.
- $\mathbb{F}_q$-linear code C: $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.
- n: length of C.
- (Hamming) weight $w(\mathbf{c})$ of $\mathbf{c} \in \mathbb{F}_q^n$:
  $\#$ non-zero positions of $\mathbf{c}$.

Divisible codes

- Introduced by Harold Ward in 1981.
- Linear code C Δ-divisible $:\iff \Delta \mid w(\mathbf{c})$ for all $\mathbf{c} \in C$.
- Only interesting case: Δ power of p.
- In this talk: $\Delta = q^r \qquad (r \in \mathbb{N}_0)$.

Why divisible codes?

- Many good codes are divisible.
- Connection to duality:

  Binary type II self-dual codes are 4-divisible.
  4-divisible binary codes are self-orthogonal.
  Self-orthogonal binary codes are 2-divisible.
  Self-orthogonal ternary codes are 3-divisible.
- Conjecture (Ward 2001):

  C Griesmer code over $\mathbb{F}_q$, $\quad p^r \mid$ minimum distance of C

  $$\implies C \; p^{r+1}/q\text{-divisible.}$$

  True for $q = p$ (Ward 1998), $q = 4$ (Ward 2001)
- Applications in finite geometry, subspace codes, etc.

  In this talk: Upper bounds for partial spreads.

- Divisible code bound (Ward 1992):
  Bound on the dimensions of divisible codes.
- Our Goal:
  Classification of the effective lengths of q^r-divisible codes.

  effective length: $\#$ non-zero coordinates of C.

Projective geometry

- $\mathbb{F}_q$-vector space V of dimension v.
- Subspace lattice of V: projective geometry PG(V)
- 1-subspaces: points, $(v-1)$-subspaces: hyperplanes
-

$$\begin{bmatrix} v \\ k \end{bmatrix}_q := \#(k\text{-subspaces of } V)$$

$$= \begin{cases} \frac{(q^v-1)(q^{v-1}-1)\cdots(q^{v-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} & \text{if } 0 \leq k \leq v; \\ 0 & \text{otherwise.} \end{cases}$$

Linear codes and points

- $\mathbb{F}_q$-linear code C of effective length n $\longleftrightarrow$ multiset $\mathcal{P}$ of n points in $\mathrm{PG}(V)$.
  (read columns of generator matrix as homogeneous coordinates)
- codeword $\mathbf{c}$ of C $\longleftrightarrow$ hyperplane H in $\mathrm{PG}(V)$
- $w(\mathbf{c}) = n - \#(\mathcal{P} \cap H)$.
- C Δ-divisible
  $\iff \#(\mathcal{P} \cap H) \equiv \#\mathcal{P} \pmod{\Delta}$ for all hyperplanes H.
  In this case: Call $\mathcal{P}$ Δ-divisible.
- $\rightsquigarrow$ Classify the sizes of q^r-divisible multisets of points!
  (will be called realizable sizes)

Advantages of geometric setting

- Basis-free approach to coding theory.
- Geometry provides *intuition*.

Lemma

Let $V_1 \subseteq V_2$ $\mathbb{F}_q$-vector spaces and $\mathcal{P}$ multiset of points in V_1.
Then:

$$\mathcal{P}\ q^r\text{-divisible in } V_1 \iff \mathcal{P}\ q^r\text{-divisible in } V_2$$

Lemma

Let U be $\mathbb{F}_q$-vector space of dimension $k \geq 1$.
Let $\mathcal{P}$ be the set of points in U.

Then $\mathcal{P}$ is q^{k-1}-divisible.

Proof.

Choose ambient space $V = U$. For each hyperplane H

$$\#(\mathcal{P} \cap H) = \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q = 1 + q + q^2 + \ldots + q^{k-2}$$

$$\equiv (1 + q + q^2 + \ldots + q^{k-2}) + q^{k-1} = \begin{bmatrix} k \\ 1 \end{bmatrix}_q = \#\mathcal{P} \pmod{q^{k-1}}$$

Lemma

The following sizes are realizable:

$$s(r,i) := q^i \cdot \begin{bmatrix} r-i+1 \\ 1 \end{bmatrix}_q = q^i + q^{i+1} + \ldots + q^r \quad (i \in \{0,\ldots,r\})$$

Proof.

Set of points of a $(r-i+1)$-subspace

is q^{r-i}-divisible of size $\left[\begin{smallmatrix} r-i+1 \\ 1 \end{smallmatrix}\right]_q$.

$\implies$ q^i-fold repetition

is $(q^i \cdot q^{r-i})$-divisible of size $q^i \cdot \left[\begin{smallmatrix} r-i+1 \\ 1 \end{smallmatrix}\right]_q$. $\square$

Lemma

The following sizes are realizable:

$$n = a_0 s(r,0) + a_1 s(r,1) + \ldots + a_r s(r,r) \quad (a_0, a_1, \ldots, a_r \in \mathbb{N}_0)$$

Proof.

Take unions of the above multisets. $\square$

- The numbers

$$s(r,i) = q^i \cdot \begin{bmatrix} r-i+1 \\ 1 \end{bmatrix}_q = q^i + q^{i+1} + \ldots + q^r \quad (i \in \{0, \ldots, r\})$$

  have the property

$$q^i \mid s(r,i) \qquad \text{but} \qquad q^{i+1} \nmid s(r,i).$$

- $\Longrightarrow$ We can build positional number system upon base numbers

$$S(r) = (s(r,0), s(r,1), \ldots s(r,r))$$

- Each $n \in \mathbb{Z}$ has unique $S(r)$-adic expansion

$$n = a_0 s(r,0) + a_1 s(r,1) + \ldots + a_r s(r,r) \qquad (*)$$

  with $a_0, \ldots, a_{r-1} \in \{0, \ldots, q-1\}$
  and leading coefficient $a_r \in \mathbb{Z}$.
  (Reason: Equation $(*)$ mod $q, q^2, q^3 \ldots$ yields unique $a_0, a_1, a_2, \ldots$)

Example

- Let $q = 3$, $r = 3$. $\implies$ $S(3) = (40, 39, 36, 27)$.
- $S(3)$-adic expansion of $n = 137$?
  Find $a_0, a_1, a_2 \in \{0, 1, 2\}$ and $a_3 \in \mathbb{Z}$ with

$$a_0 \cdot 40 + a_1 \cdot 39 + a_2 \cdot 36 + a_3 \cdot 27 = 137. \qquad (*)$$

- Modulo 3:

$$a_0 \cdot 1 + \underbrace{a_1 \cdot 0 + a_2 \cdot 0 + a_3 \cdot 0}_{=0} \equiv 2 \pmod 3 \implies a_0 = 2$$

- $a_0 = 2$ in $(*)$:

$$a_1 \cdot 39 + a_2 \cdot 36 + a_3 \cdot 27 = \underbrace{137 - 2 \cdot 40}_{=57} \qquad (**)$$

- Modulo 9:

$$a_1 \cdot 3 + a_2 \cdot 0 + a_3 \cdot 0 \equiv 3 \pmod 9 \implies a_1 = 1$$

Example (cont.)

- … Find $a_1, a_2 \in \{0, 1, 2\}$ and $a_3 \in \mathbb{Z}$ with

$$a_1 \cdot 39 + a_2 \cdot 36 + a_3 \cdot 27 = 57. \qquad (**)$$

- $a_1 = 1$ in $(**)$:

$$a_2 \cdot 36 + a_3 \cdot 27 = \underbrace{57 - 1 \cdot 39}_{=18} \qquad (***)$$

- Modulo 27:

$$a_2 \cdot 9 + a_3 \cdot 0 \equiv 18 \pmod{27} \implies a_2 = 2$$

- In $(***)$:

$$a_3 \cdot 27 = \underbrace{18 - 2 \cdot 36}_{=-54} \implies a_3 = -2$$

- $\implies$ $S(3)$-adic expansion of $n = 137$ is

$$137 = 2 \cdot 40 + 1 \cdot 39 + 2 \cdot 36 + (-2) \cdot 27$$

Theorem 1

Let $n \in \mathbb{Z}$ and $r \in \mathbb{N}_0$. Then:

There exists a q^r-divisible $\mathbb{F}_q$-linear code of effective length n

$$\iff$$

The leading coefficient of the $S(r)$-adic expansion of n is ≥ 0.

Example (cont.)

- $q = 3$, $r = 3$
- $S(3)$-adic expansion of $n = 137$ is
  $137 = 2 \cdot 40 + 1 \cdot 39 + 2 \cdot 36 + (-2) \cdot 27$.
- Leading coefficient is -2.
- Theorem 1 $\implies$ There is no 27-divisible ternary code of effective length 137.

Lemma

Let $\mathcal{P}$ be non-empty and q^r-divisible.
Then for all hyperplanes H, $\mathcal{P} \cap H$ is q^{r-1}-divisible.

Proof of Theorem 1 (Idea)

- Let $\mathcal{P}$ be non-empty and q^r-divisible.
  Have to show:
  Leading coefficient of $S(r)$-adic expansion of $\#\mathcal{P}$ is ≥ 0.
- On average, a hyperplane contains

$$\#\mathcal{P} \cdot \frac{1}{q + \frac{1}{\left[{v-1 \atop 1}\right]_q}}$$

  elements of $\mathcal{P}$.
- $\implies$ Exists hyperplane H with $\#(\mathcal{P} \cap H) < \frac{\#\mathcal{P}}{q}$.
- Apply Lemma to this H, use induction on r.

Definition

- Let V be $\mathbb{F}_q$ vector space of dimension v.
- Let $\mathcal{S}$ be a set of k-subspaces of V.
- $\mathcal{S}$ is partial $(k-1)$-spread
  if each point in V is covered by at most 1 element of $\mathcal{S}$.

Research Problem

Find maximum possible size $A_q(v, k)$ of partial spread.

History

Write $v = tk + r$, $r \in \{0, \ldots, k-1\}$, $t \geq 2$.

- 1964 Segre:
  All points can be covered $\iff k \mid v$ (settles $r = 0$).
  In this case, $\mathcal{S}$ spread, $A_q(v,k) = \frac{q^v-1}{q^k-1}$.
- 1975 Beutelspacher:
  $$A_q(v,k) \geq \frac{q^v - q^{k+r}}{q^k - 1} + 1 \qquad (*)$$
  Bound sharp for $r = 1$.
- 1979 Drake, Freeman: Improved upper bound on $A_q(v,k)$.
- 2010 El-Zanati, Jordon, Seelinger, Sissokho, Spence:
  Computer construction for $A_2(8,3) = 34$.
  Settles all cases with $q = 2$, $r = 2$, $k = 3$ recursively.
  Here, bound $(*)$ is not sharp!
- 2016 Kurz: Bound $(*)$ sharp for $q = 2$, $r = 2$, $k \geq 4$.
- 2017 Năstase, Sissokho: $(*)$ sharp whenever $k > \begin{bmatrix} r \\ 1 \end{bmatrix}_q$.

Năstase and Sissokho as a corollary from Theorem 1

- Let $\mathcal{S}$ be partial $(k-1)$-spread.
- Set $\mathcal{P}$ of holes (points not covered by $\mathcal{S}$) is q^{k-1}-divisible!
- Assume $\#\mathcal{S} = \frac{q^v - q^{k+r}}{q^k - 1} + 2$.

$$\implies \#\mathcal{P} = \begin{bmatrix} k+r \\ 1 \end{bmatrix}_q - 2\begin{bmatrix} k \\ 1 \end{bmatrix}_q$$

$$S(k-1)\text{-adic ex.} = \sum_{i=0}^{k-2} (q-1)s(k-1,i) + \left(q \cdot \left(\begin{bmatrix} r \\ 1 \end{bmatrix}_q - k + 1 \right) - 1 \right) s(k-1,k-1)$$

- Theorem 1: Leading coefficient $q \cdot \left(\begin{bmatrix} r \\ 1 \end{bmatrix}_q - k + 1 \right) - 1 \geq 0$.
  $\iff k \leq \begin{bmatrix} r \\ 1 \end{bmatrix}_q$.
- $\rightsquigarrow$ 2017 result of Năstase and Sissokho follows as corollary from Theorem 1!.

Projective divisible codes

- For partial spreads: $\mathcal{P}$ is a proper set (not only a multiset). Can we make use of this extra information?
- Sets of points $\longleftrightarrow$ projective linear codes.
- Classification of the lengths of projective q^r-divisible linear codes apparently much harder.

Theorem 2

There exists a projective binary 8-divisible of length n

$$\iff \quad n \notin \{1,2,3,4,5,6,7,\mathbf{8},9,10,11,\mathbf{12},13,\mathbf{14}\}$$
$$\cup \{17,18,19,\mathbf{20},21,\mathbf{22},\mathbf{23},\mathbf{24},25,\mathbf{26},\mathbf{27},\mathbf{28},\mathbf{29}\}$$
$$\cup \{33,\mathbf{34},\mathbf{35},\mathbf{36},\mathbf{37},\mathbf{38},\mathbf{39},\mathbf{40},\mathbf{41},\mathbf{42},\mathbf{43},\mathbf{44}\}$$
$$\cup \{\mathbf{52},\mathbf{53},\mathbf{54},\mathbf{55},\mathbf{56},\mathbf{57},\mathbf{58},\mathbf{59}\}$$

No projective 8-divisible code of length 52

- Use first 4 MacWilliams-identities.
- Would be the size of the hole set
  of a partial 3-spread in $\mathbb{F}_2^{11}$ of size 133.
  $$\Longrightarrow \; 129 \le A_2(11,4) \le 132.$$

No projective 8-divisible code of length 59

- Hardest single case.
- Cannot have weights 56 and 48
  (residuals would be proj. 4-divisible of length 3 and 11)
- If it has weight 40:
  Residual is projective 4-divisible of length 19.
  3 isomorphism types.
  - 2 excluded by theoretical argument.
  - 1 excluded computationally.
- Otherwise, must have weight 32.
  Excluded computationally.