On the lengths of divisible codes

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

Oberwolfach Workshop 1912:
Contemporary Coding Theory
March 21, 2019

joint work with Thomas Honold,
Sascha Kurz and Alfred Wassermann

Divisible Codes

Divisible codes

- Introduced by Harold Ward in 1981.
- $\mathbb{F}_q$-linear code C Δ-divisible $:\iff \Delta \mid w(\mathbf{c})$ for all $\mathbf{c} \in C$.
- Only interesting case: Δ power of $p = \mathrm{char}(\mathbb{F}_q)$.
- 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.

- Divisible code bound (Ward 1992):
  Bound on the dimension of a Δ-divisible code.

  If the weights of C are among
  $(b-m+1)\Delta, (b-m+2)\Delta, \ldots, b\Delta$, then

$$\dim(C) \leq \frac{m(v_p(\Delta) + v_p(q)) + v_p(\binom{b}{m})}{v_p(q)}.$$

- Goal: Investigate effective lengths of q^r-divisible codes.
  (will be called realizable)

  effective length: $\#$ non-zero coordinates of C.
- Observation: Set of realizable lengths additively closed.
  (Direct sum of codes!)
- Find small starters.

Lemma

The following lengths are realizable:

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

Proof.

- Simplex code of dimension $r-i+1$:
  Length $\frac{q^{r-i+1}-1}{q-1}$ and constant weight q^{r-i}.
- Take q^i-fold repetition.

□

By additivity:

Lemma

The following lengths are realizable:

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

We will see: That's all!

- The numbers

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

have the property

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

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

suitable base numbers of a positional number system.

- 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 $q = 3$, $r = 3$. $\Longrightarrow$ $S(3) = (40, 39, 36, 27)$.
- $S(3)$-adic expansion of $n = 137$ has the form

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

  with $a_0, a_1, a_2 \in \{0, 1, 2\}$ and $a_3 \in \mathbb{Z}$.
- Modulo 3:

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

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

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

- Modulo 9:

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

- Modulo 27: $\ldots$ $a_2 = 2$ and $a_3 = -2$.

Theorem 1 (MK, S. Kurz)

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.)

- $S(3)$-adic expansion of $n = 137$ is
  $137 = 2 \cdot 40 + 1 \cdot 39 + 2 \cdot 36 + \underbrace{(-2)}_{\textit{leading coeff.}} \cdot 27.$
- Leading coefficient is -2.
- Theorem 1 $\implies$ There is no 27-divisible ternary code of effective length 137.

Proof of Theorem 1 (Idea)

- Let C be q^r-divisible of effective length n.
  Have to show:
  Leading coefficient of $S(r)$-adic expansion of n is ≥ 0.
- Average weight is $\frac{q-1}{q} \cdot n$.
  $\implies \exists$ codeword $\mathbf{c}$ with $w(\mathbf{c}) > \frac{q-1}{q} \cdot n$.
- Lemma: Residual code wrt $\mathbf{c}$ is q^{r-1}-divisible.
  Use induction on r.

Byproduct of proof

For all codewords $\mathbf{c}$:

$$w(\mathbf{c}) \leq q^r \cdot \text{cross sum of } S(r)\text{-adic expansion of } n$$

Application to Partial Spreads

Linear codes and points

- $\mathbb{F}_q$-linear code C of effective length n and dim. k
  $\longleftrightarrow$ multiset $\mathcal{P}$ of n points in $\mathrm{PG}(k-1,q)$.
  (read columns of generator matrix
  as homogeneous coordinates)
- nonzero codeword $\mathbf{c}$ of C
  $\longleftrightarrow$ hyperplane $H = \mathbf{c}^\perp$ 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.

Advantages of geometric setting

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

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 $\#\mathcal{S} = \frac{q^v - q^{k+r}}{q^k - 1} + 2$.

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

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

- Theorem 1: Leading coefficient $q \cdot \left(\begin{bmatrix} r \\ 1 \end{bmatrix}_q - k + 1\right) - 1 \geq 0$.
  $\Longleftrightarrow \quad k \leq \begin{bmatrix} r \\ 1 \end{bmatrix}_q$.

Projective Divisible Codes

Motivation

- $\exists$ partial 3-spread in $\mathbb{F}_2^{11}$ of size 133?
- Hole set $\mathcal{P}$ is 8-divisible multiset of size 52.

  $S(3)$-adic expansion: $52 = 0 \cdot 15 + 0 \cdot 14 + 1 \cdot 12 + 5 \cdot 8$
  no contradiction.
- However, $\mathcal{P}$ is a proper set. Will see: Does not exist!

$$\implies 129 \leq A_2(11, 4) \leq 132.$$

Projective divisible codes

- Sets of points $\longleftrightarrow$ projective linear codes.
- Study effective lengths of projective linear codes.
- As before: Set of realizable lengths additively closed.
- Find small starters.

Lemma

The following lengths are realizable:

$$n_1 = \frac{q^{r+1}-1}{q-1} \quad \text{and} \quad n_2 = q^{r+1}$$

Proof.

Simplex code of dim. $r+1$ and
1st order Reed-Muller code of dim. $r+2$. □

Question: Are all realizable lengths sum of n_1's and n_2's?

Theorem 2 (T. Honold, MK, S. Kurz)

Length $n \leq rq^{r+1}$ realizable $\iff$ n sum of n_1's and n_2's.

Restriction $n \leq rq^{r+1}$ necessary?

- Yes!
- For $r = 1$, $q^2 + 1$ is realizable (ovoid in $\mathrm{PG}(3, q)$).
- Classification of lengths of projective divisible code apparently quite hard.

Theorem 3 (T. Honold, MK, S. Kurz, A. Wassermann)

(a) The lengths of projective 2-divisible (even) binary codes are

$$3, 4, 5, 6, \dots$$

(b) The lengths of projective 4-divisible (doubly even) binary codes are

$$7, 8,\ 14, 15, 16, 17, \dots$$

(c) The lengths of projective 8-divisible (triply even) binary codes are

$$15, 16,\ 30, 31, 32,\ 45, 46, 47, 48, 49, 50, 51,\ 60, 61, 62, 63, \dots$$

Hardest single case (by far)

Non-existence of 8-divisible code of length 59.

No projective 8-divisible code of length 59

- Let C be such code of smallest possible dimension k, weight enumerator $w(C) = 1 + a_8x^8 + a_{16}x^{16} + \ldots + a_{56}x^{56}$
- Lemma: $a_{56} = a_{48} = 0$
  Residuals would be projective 4-divisible of length 3 and 11
- Lemma: $k \geq 10$: First 4 MacWilliams identities $\rightsquigarrow$

$$a_{16} + a_{40} = -6 - 3a_8 + \frac{1}{128}\#C \qquad (*)$$

$$\implies 0 \leq -6 + \tfrac{1}{128}\#C \implies \#C \geq 768.$$

- Lemma: $k = 10$
  k min. $\implies$ all codim 1 subcodes are non-projective.
  Geometr.: All $2^k - 60$ points outside of $\mathcal{C}$ lie on a secant.
  $\#$secants $\leq \binom{\#\mathcal{C}}{2} = 1711$.
  $\implies 2^k - 60 \leq 1711 \implies k \leq 10$.
- Lemma: $a_8 = 0$ and $a_{16} + a_{40} = 2$
  ($k = 10$ into $(*)$ $\implies a_{16} + a_{40} = 2 - 3a_8$)
- $\ldots \rightsquigarrow$ Lemma: $a_{16} = 0 \rightsquigarrow \ldots \rightsquigarrow$ finally a contradiction.

Further Applications

The Johnson bound for subspace codes

- Most competitive bound for subspace codes:

  Johnson type bound II (Xia, Fu)

$$A_q(v,d;k) \le \left\lfloor \frac{q^v-1}{q^k-1} \cdot A_q(v-1,d;k-1) \right\rfloor$$

- Similar to partial spreads: Improvement via divisible codes.

Example

- Johnson type bound II:

$$A_2(9,6;4) \le \lfloor \frac{2^9-1}{2^4-1} \cdot \underbrace{A_2(8,6;3)}_{=34} \rfloor = 1158$$

- Improvement:

$$A_2(9,6;4) \le 1156$$

The Barth sextic

The Barth sextic

- Record surface: Sextic surface with the maximum possible number of nodes (ordinary double points).
- Its even sets of nodes
  form a binary 8-divisible code C of length 65.
- Via classification: Generator matrix of C is

$$\begin{pmatrix}
11110001110000011010110111101001100011010000000111001101010000111 0\\
11100111100001101000110111000111010000001111010000001000111101010 01\\
11000111001101101011010010100110001101000000111101001010000111110\\
10011110001110100011010100011101001101111010000001000111101010000 1\\
00011100111110101101000110011000111000000011110100101000011110110\\
01111000111010001101011001110100110011101000000010101110101000010 1\\
01110011110010110100011001100011101000000111101001000000111101011 0\\
11100011100100110101101011010011000110100000001110011010100001110 1\\
11001111000111010001101010001110100100111101000000100011110101001 0\\
10001110011111010110100001001100011110000000111101001010000111100 1\\
00111100011101000110101100111010011011110100000000111101010000 10\\
00111001111001011010001100110001110100000011110100101000011110100 1
\end{pmatrix}$$

- $w(C) = 1 + 390x^{24} + 3055x^{32} + 650x^{40}$
- $\#\operatorname{Aut}(C) = 15600, \quad \operatorname{Aut}(C) \cong \mathrm{PSL}(2,25) \rtimes \mathbb{Z}/2\mathbb{Z}$

Open problems

- Effective lengths of general p^s-divisible codes.
  Example 8-divisible over $\mathbb{F}_4$.
- Open cases for lengths of projective linear codes for:
  - Binary 16-divisible
  - Ternary 9-divisible
  - 5-divisible over $\mathbb{F}_5$
- Lengths of divisible codes with
  - restricted dimension and/or
  - restricted point multiplicity
- Classifications.
- Divisible codes of high minimum distance.
- Indecomposable divisible codes.
- q-analog question: divisible rank metric codes.
- ...