On divisible linear codes

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth
Germany

BCC 2021: 28th British Combinatorial Conference
Mini-symposium “Codes and cryptography”
July 8, 2021
Durham University (held online)

Fixed notation

- p prime
- q a power of p
  $\Longrightarrow \operatorname{char} \mathbb{F}_q = p$

Divisible codes

- Introduced by Harold Ward in 1981 [12].
- $\mathbb{F}_q$-linear code C Δ-divisible $:\Longleftrightarrow \Delta \mid w(\mathbf{c})$ for all $\mathbf{c} \in C$.
- Example: extended Golay codes.

  binary: weight enumerator $(0^1 8^{759} 12^{2576} 16^{759} 24^1)$
  $\Longrightarrow$ 4-divisible

  ternary: weight enumerator $(0^1 6^{264} 9^{440} 12^{24})$
  $\Longrightarrow$ 3-divisible

Why divisible codes?

- Many good codes are divisible.
- Connection to duality:
  binary 4-divisible $\implies$ self-orthogonal
  binary self-orthogonal $\implies$ 2-divisible
  ternary self-orthogonal $\implies$ 3-divisible
  quaternary Hermitean self-orthogonal $\implies$ 2-divisible
- generalizes constant-weight codes, two-weight codes.
- Interconnections to other research areas
  like Galois geometries, subspace codes.
- Interesting results and conjectures.

Divisibility of Griesmer-optimal codes

Let C be a $[n,k,d]_q$-code.

- Griesmer bound: $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$
- In case of equality: C Griesmer code
- Theorem (H. Ward 1998 [14]) for q prime:

  C Griesmer code with $q^r \mid d \implies C$ is q^r-divisible.
- Example: C extended ternary $[12,6,6]_3$ Golay code.

  $$\sum_{i=0}^{5} \left\lceil \frac{6}{3^i} \right\rceil = 6+2+1+1+1+1 = 12 \implies C \text{ Griesmer code}$$

  $3 \mid 6 = d$ and indeed, C is 3-divisible.
- Conjecture (H. Ward 2001 [16]), generalization for all q:

  C Griesmer code with $p^r \mid d \implies C$ is p^{r+1}/q-divisible
- Theorem (H. Ward 2001 [16]): Conjecture true for $q = 4$.
- No real progress since 2001.

Initial observations

Zero positions

- zero positions don't affect divisibility $\implies$ can be removed.
- enough to study full-length codes (no zero positions).
- $\#$ non-zero positions = effective length

Restriction on Δ

- Corollary of result of H. Ward 1981 [12, Th. 1]:

  Any full-length Δ-divisible $\mathbb{F}_q$-linear code
  is the repetition of a Δ'-divisible $\mathbb{F}_q$-linear code
  with $\Delta' = \gcd(\Delta, q)$.
- $\Delta' \mid q \implies \Delta'$ is a power of $p = \operatorname{char}(\mathbb{F}_q)$

$\implies$ enough to consider $\Delta = p^a$ $(a \in \mathbb{N})$

Outline

First upper bound on the dimension:

Lemma (Ward 1999 [15, Lem. 6])

Let C be a Δ-divisible linear $[n,k]_q$-code with $\Delta \geq 2$ and $(\Delta, q) \neq (2,2)$.

Then $k \leq \frac{n}{2}$.

Characterization of the extremal cases:

Theorem ("Gleason-Pierce-Ward", Ward 1981 [12, Th. 2])

Let n be even and C a Δ-divisible $[n, \frac{n}{2}]_q$-code.

Then C falls into one of the following cases.

(I) $q = 2$ *and* $\Delta = 2$.

(II) $q = 2$, $\Delta = 4$ *and C is self-dual.*

(III) $q = 3$, $\Delta = 3$ *and C is self-dual.*

(IV) $q = 4$, $\Delta = 2$ *and C is Hermitean self-dual.*

(V) *q arbitrary,* $\Delta = 2$ *and C is the* 2*-fold repetition of* $\mathbb{F}_q^{n/2}$.

Remark

- The Gleason-Pierce-Ward theorem
  generalizes the Gleason-Pierce theorem from the 1960s.
- Roughly speaking:
  For the generalization, self-duality is replaced by divisibility
  (in the requirement on C).
- Bound $k \leq \frac{n}{2}$ is weak for (q, Δ) not listed in the theorem.

  $\rightsquigarrow$ Improvement?

Best known general upper bound on the dimension:

Theorem ("divisible code bound", H. Ward 1992 [13])

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

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

Remark on the proof

- original 1992 proof by character-theoretic and number-theoretic arguments.
- H. Ward 2001 "The divisible code bound revisited" [16]: alternative proof based on divisibility properties of Stirling numbers (of both kind).

Example

Dimension k of 8-divisible binary codes of length $n = 48$?

- non-zero weights are in $\{8, 16, 24, 32, 40, 48\}$, so $b = m = 6$.

  divisible code bound: $k \leq \frac{6\cdot(3+1)+0}{1} = 24$.

  $\rightsquigarrow$ no improvement of $k \leq \frac{n}{2}$
- little trick: Assume that C does not contain the all-1 word.

  non-zero weights are in $\{8, 16, 24, 32, 40\}$, so $b = m = 5$.

  divisible code bound: $k \leq \frac{5\cdot(3+1)+0}{1} = 20$.

  If C contains the all-1 word,
  C has a subcode of the above type of codimension 1.

  Altogether, $k \leq 20 + 1 = 21$.
- Classification of K. Betsumiya and A. Munemasa 2012 [1]: sharp bound is $k \leq 15$.

Research problem

- H. Well, H. Ward 2001 [16]:
  "The divisible code bound can be disappointingly weak [...]"
- still: best known general bound on the dimension.
- Improve the divisible code bound!

Outline

The effective length

- Goal: Characterize the effective lengths of q^r-divisible codes.
  (will be called realizable)
- Observation: Set of realizable lengths additively closed.
  (Direct sum of codes!)
- First step: Find small starters.

Lemma

The following lengths are realizable:

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

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.

$\square$

By additivity:

Lemma

The following lengths are realizable:

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

We will see: That's all!

- The numbers

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

have the property

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

$$\Longrightarrow \qquad S_q(r) = (s_q(r,0), s_q(r,1), \ldots s_q(r,r))$$

suitable base numbers of a positional number system.

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

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

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 $a_0, a_1, a_2, \ldots$)

Theorem 1 (MK, S. Kurz 2020 [6, Th. 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

$$\Longleftrightarrow$$

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

Example

- $q = 3$, $r = 3 \quad \rightsquigarrow \quad S_q(3) = (40, 39, 36, 27)$.
- $S_q(3)$-adic expansion of $n = 137$ is
  $137 = 2 \cdot 40 + 1 \cdot 39 + 2 \cdot 36 + \underbrace{(-2)}_{\substack{\textit{leading}\\ \textit{coeff.}}} \cdot 27$.
- Theorem 1 $\Longrightarrow$
  No ternary 27-divisible code of effective length 137.

Research problem

- Theorem 1 only covers $\Delta = q^a$ with $a \in \mathbb{N}$.
- Example: 8-divisible over $\mathbb{F}_4$ not covered.
- Find generalization for $\Delta = p^a$ with $p = \mathrm{char}(\mathbb{F}_q)$, $a \in \mathbb{N}$.

Outline

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 $\mathrm{PG}(V)$ 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 [11]:
  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 [2]:
  $$A_q(v,k) \geq \frac{q^v - q^{k+r}}{q^k - 1} + 1 \qquad (*)$$
  Bound sharp for $r = 1$.
- 1979 Drake, Freeman [3]: Better upper bound on $A_q(v,k)$.
- 2010 El-Zanati, Jordon, Seelinger, Sissokho, Spence [18]:
  Computer construction for $A_2(8,3) = 34$.
  Settles all cases with $q = 2$, $r = 2$, $k = 3$ recursively.
  Here, bound $(*)$ is not sharp!
- 2017 Kurz [8]: Bound $(*)$ sharp for $q = 2$, $r = 2$, $k \geq 4$.
- 2017 Năstase, Sissokho [9]: $(*)$ 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 $\#\mathcal{S} = \frac{q^v - q^{k+r}}{q^k - 1} + 2$.

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

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

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

Outline

The Johnson bound for subspace codes

- Most competitive bound for subspace codes:

  Johnson type bound II (Xia, Fu 2009) [17]

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

- 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 [6]:

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

Outline

Motivation

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

  $S_2(3)$-adic expansion:

  $$52 = 0 \cdot 15 + 0 \cdot 14 + 1 \cdot 12 + 5 \cdot 8$$

  $\rightsquigarrow$ no contradiction.
- However, $\mathcal{P}$ is a set (not only a multiset).
- Geometrically:

  sets of points $\longleftrightarrow$ projective linear codes.
- Will see: $\nexists$ projective 8-divisible code of length 52.

  $\implies$ $\nexists$ 3-spread in $\mathbb{F}_2^{11}$ of size 133.

  $\implies$ $129 \leq A_2(11, 4) \leq 132$ (best known bounds of today)

Projective divisible 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. $r+2$. $\square$

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 2020) [4, Th. 13] & [5])

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

$$3, 4, 5, 6, \ldots$$

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

$$7, 8, \quad 14, 15, 16, 17, \ldots$$

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

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

Hardest single case (by far)

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

Research problem

Undecided effective lengths exist for:

- $q = 2$, $\Delta = 16$.
- $q = 3$, $\Delta = 9$.
- $q = 5$, $\Delta = 5$.
- $\ldots$

Outline

Theorem 4 (MK, S. Kurz, submitted [7])

Let C be full-length Δ-divisible code spanned by codewords of weight Δ.
Then C is isomorphic to the direct sum of repeated codes of the following form:

- q-ary simplex code.
- Only $q = 2$: binary first order Reed-Muller code.
- Only $q = 2$: binary parity check code.

Remarks

- Generalizes Thm. 6.5 in [10] (Pless and Sloane 1975) on self-orthogonal binary codes spanned by weight-4-words.
- Motive of the generalization (again):
  Replace orthogonality by divisibility.
- Application:
  Classification of more general Δ-divisible codes by looking at the subcode spanned by weight-Δ-words.

Thank you!

Slides can be found at
https://www.mathe2.uni-bayreuth.de/michaelk/

[1] K. Betsumiya and A. Munemasa. “On triply even binary codes”. In: *J. London Math. Soc. (2)* 68.1 (Aug. 2012), pp. 1–16.

[2] A. Beutelspacher. “Partial spreads in finite projective spaces and partial designs”. In: *Math. Z.* 145.3 (1975), pp. 211–229.

[3] D. A. Drake and J. W. Freeman. “Partial t-spreads and group constructible (s, r, μ)-nets”. In: *J. Geom.* 13.2 (1979), pp. 210–216.

[4] T. Honold, M. Kiermaier, and S. Kurz. “Partial spreads and vector space partitions”. In: *Network Coding and Subspace Designs*. Ed. by M. Greferath, M. O. Pavčević, N. Silberstein, and M. Á. Vázquez-Castro. Signals Commun. Technol. Cham: Springer, 2018, pp. 131–170. ISBN: 978-3-319-70292-6.

[5] T. Honold, M. Kiermaier, S. Kurz, and A. Wassermann. “The lengths of projective triply-even binary codes”. In: *IEEE Trans. Inf. Theory* 66.5 (May 2020), pp. 2713–2716.

[6] M. Kiermaier and S. Kurz. “On the lengths of divisible codes”. In: *IEEE Trans. Inf. Theory* 66.7 (July 2020), pp. 4051–4060.

[7] M. Kiermaier and S. Kurz. *Classification of Δ-divisible linear codes spanned by codewords of weight Δ*. Jan. 18, 2021. arXiv: `2011.05872`.

[8] S. Kurz. “Improved upper bounds for partial spreads”. In: *Des. Codes Cryptogr.* 85.1 (Oct. 2017), pp. 97–106.

[9] E. Năstase and P. Sissokho. “The maximum size of a partial spread in a finite projective space”. In: *J. Combin. Theory Ser. A* 152 (Nov. 2017), pp. 353–362.

[10] V. Pless and N. J. A. Sloane. “On the classification and enumeration of self-dual codes”. In: *J. Combin. Theory Ser. A* 18.3 (May 1975), pp. 313–335.

[11] B. Segre. "Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane". In: *Ann. Mat. Pura Appl. (4)* 64.1 (Dec. 1964), pp. 1–76.

[12] H. N. Ward. "Divisible codes". In: *Arch. Math.* 36.6 (Dec. 1981), pp. 485–494.

[13] H. N. Ward. "A bound for divisible codes". In: *IEEE Trans. Inf. Theory* 38.1 (Jan. 1992), pp. 191–194.

[14] H. N. Ward. "Divisibility of codes meeting the Griesmer bound". In: *J. Combin. Theory Ser. A* 83.1 (July 1998), pp. 79–93.

[15] H. N. Ward. "An introduction to divisible codes". In: *Des. Codes Cryptogr.* 17.1–3 (Sept. 1999), pp. 73–79.

[16] H. N. Ward. "The divisible code bound revisited". In: *J. Combin. Theory Ser. A* 94.1 (Apr. 2001), pp. 34–50.

[17] S.-T. Xia and F.-W. Fu. "Johnson type bounds on constant dimension codes". In: *Des. Codes Cryptogr.* 50.2 (Feb. 2009), pp. 163–172.

[18] S. El-Zanati, O. Heden, G. Seelinger, P. Sissokho, L. Spence, and C. Vanden Eynden. "Partitions of the 8-dimensional vector space over $\mathrm{GF}(2)$". In: *J. Combin. Des.* 18.6 (Nov. 2010), pp. 462–474.