On linear codes associated with the Desarguesian ovoids in $Q^+(7, q)$

Michael Kiermaier

Mathematisches Institut
Universität Bayreuth

Finite Geometries (Irsee 6)
August 30, 2022
Kloster Irsee, Germany

joint work with Tao Feng, Peixian Lin and Kai-Uwe Schmidt

Points and linear codes

- Let $\mathcal{P}$ spanning multiset of n points in $\mathrm{PG}(\mathbb{F}_q^k) \cong \mathrm{PG}(k-1, q)$.
- Write $\mathcal{P} = \{\!\{\langle v_1 \rangle, \ldots, \langle v_n \rangle\}\!\}$.
- Generator matrix $G = (v_1 \cdots v_n) \in \mathbb{F}_q^{k \times n}$ yields $\mathbb{F}_q$-linear $[n, k]_q$-code C.
- C well-defined up to linear equivalence of codes.
- C full-length, i.e. no all-zero position.
- For codeword $c = x^\top G \neq \mathbf{0}$, define hyperplane $H = x^\perp$.
  Then $w_{\mathrm{Ham}}(c) = n - \#\{\!\{P \in \mathcal{P} \mid P \in H\}\!\}$.
  $(= \#$ of points in $\mathcal{P}$ outside of $H)$

Conclusion

- We get correspondence
  Spanning multisets $\mathcal{P}$ of points
  $\longleftrightarrow$ full-length linear codes C.
- Weights of $C \longleftrightarrow$ hyperplane intersections of $\mathcal{P}$.
- Corresponding notions on geometric side: arc, minihyper.
- Strong link between finite geometry and coding theory.
- First (?) published in 1964 in PhD thesis of Burton.

Plan

- Take your favorite point set $\mathcal{P}$.
- Compute the hyperplane intersections.
- Hope for a good code!

Ovoids in $Q^+(7, q)$

- Ovoid in polar space = set of points covering every generator exactly once.
- Kantor (1982): two series of ovoids in $Q^+(7, q)$.
- Unitary ovoid for $q \equiv 0, 2 \mod 3$.
  stabilized by $\mathrm{PGU}(3, q)$.

  Hyperplane intersections determined by Cooperstein (1995) ($q \equiv -1 \mod 6$).
  $\rightsquigarrow [q^3 + 1, 8, q^3 - q^2 - 2q]_q$-code.
- Desarguesian ovoid for q even.
  stabilized by $\mathrm{PGL}(2, q^3)$.

  Goal: Determine its hyperplane intersections.
  $\rightsquigarrow [q^3 + 1, 8, q^3 - q^2 - q]_q$-code.

The Desarguesian ovoid

- Let $V = \mathbb{F}_q \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_q$ vector space over $\mathbb{F}_q$ of dim. 8.
- fix nondegenerate quadratic form on V

$$Q((x,y,z,w)) = xw + \mathrm{Tr}(yz).$$

$\rightsquigarrow$ polar space $Q^+(7,q)$.

- group operation of $\mathrm{PGL}(2,q^3)$ on $\mathrm{PG}(V)$ induced by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet (x\,y\,z\,w)^\top =$$

$$\begin{pmatrix} \mathrm{N}(d)x+\mathrm{N}(c)w+\mathrm{Tr}(cd^{q^2+q}y+dc^{q^2+q}z) \\ bd^{q^2+q}x+ac^{q^2+q}w+ad^{q^2+q}y+bd^{q^2}c^qy^q+bd^qc^{q^2}y^{q^2}+bc^{q^2+q}z+d^qac^{q^2}z^q+d^{q^2}ac^qz^{q^2} \\ db^{q^2+q}x+ca^{q^2+q}w+cb^{q^2+q}y+db^{q^2}a^qy^q+db^qa^{q^2}y^{q^2}+da^{q^2+q}z+b^qca^{q^2}z^q+b^{q^2}ca^qz^{q^2} \\ \mathrm{N}(b)x+\mathrm{N}(a)w+\mathrm{Tr}(ab^{q^2+q}y+ba^{q^2+q}z) \end{pmatrix}$$

- q even: Orbit O of $\langle(1,0,0,0)\rangle$ is Desarguesian ovoid.
  q odd: O complete partial ovoid in $W(7,q)$
  (Cossidente 2011)
- We consider O for all values of q.

Theorem

There are four orbits on $\mathrm{PG}(V)$, with the following properties.

orbit	size	representative v	$\#(v^\perp \cap \mathcal{O})$
$\mathcal{O}$	q^3+1	$\langle(1,0,0,0)\rangle$	1
$\mathcal{O}_2$	$q(q^2+q+1)(q^3+1)$	$\langle(0,0,1,0)\rangle$	q^2+1
$\mathcal{O}_3$	$\frac{1}{2}q^3(q^3+1)(q-1)$	$\langle(1,0,0,1)\rangle$	q^2+q+1
$\mathcal{O}_4$	$\frac{1}{2}q^3(q^3-1)(q+1)$	$\langle(1,0,\alpha,\alpha)\rangle$	q^2-q+1

Where $\alpha \in \mathbb{F}_q$ such that $x^2 - x - \alpha \in \mathbb{F}_q[x]$ is irreducible.

Proof (sketch).

- Enough to compute $\#(v^\perp \cap \mathcal{O})$ for single representative v.
- Use orbit-stabilizer-theorem for $(\#\mathcal{O})$, $\#\mathcal{O}_2$, $\#\mathcal{O}_3$.
- Show that $\mathrm{PG}(V) \setminus (\mathcal{O} \cup \mathcal{O}_2 \cup \mathcal{O}_3)$ is a single orbit.
  (longest part; count solutions of certain equations in $\mathbb{F}_{q^3}$).
- several pages of computations.

Let C_O be the $\mathbb{F}_q$-linear code associated to O.

Corollary

The code C_O has the parameters $[q^3+1, 8, q^3-q^2-q]_q$ and the weight enumerator

weight	multiplicity
0	1
$q(q^2-q-1)$	$\frac{1}{2}q^3(q^3+1)(q-1)^2$
$q^2(q-1)$	$q(q^6-1)$
$q(q^2-q+1)$	$\frac{1}{2}q^3(q^3-1)(q^2-1)$
q^3	$(q^3+1)(q-1)$

Proof.

Correspondence “points $\leftrightarrow$ linear codes”. $\square$

Corollary

The code $C_O^\perp$ has the parameters $[q^3+1, q^3-7, d]_q$ with

$$d = \begin{cases} 9 & \text{if } q = 2; \\ 6 & \text{if } q = 3; \\ 5 & \text{otherwise.} \end{cases}$$

Proof.

Apply MacWilliams to the weight enumerator of C_O. $\square$

Remark

For $q = 2$:

- C_O is the $[9, 8, 2]$ parity check code.
- $C_O^\perp$ is the $[9, 1, 9]$ repetition code.

Question

How good are the codes C_O and $C_O^\perp$?

Interlude: Optimality of linear codes

When should we call a linear code optimal?

First approach: parametric optimality

- Parameters of linear code C usually given as $[n, k, d]$.
- We want: n small, k large, d large.
- parametric optimality: Fix two parameters.
  C optimal $\iff$ third parameter is best possible
- C distance-optimal (d-optimal) $\iff$ $\nexists[n, k, d+1]$-code.
- C dimension-optimal (k-optimal) $\iff$ $\nexists[n, k+1, d]$-code.
- C length-optimal (n-optimal) $\iff$ $\nexists[n-1, k, d]$-code.

Parametric optimality (continued)

- Dependencies among n-, k- and d-optimality?
- Yes!
  C n-optimal $\implies$ C k-optimal <u>and</u> C d-optimal.
  Proof: via shortening / puncturing
- $\implies$
  - n-optimality: interesting!
  - d-optimality and k-optimality: pretty weak.
    Unfortunately: Used a lot in the literature.
- Flaw of concept of parametric optimality:
  Optimality notions depend on chosen basis
  (n, k, d) of the parameter space.

Second approach: wish list

What do we expect of an optimal code?

- "better than others":
  Cannot be constructed in an elementary way
  from other linear codes.
- "building blocks":
  Every realizable parameter set should be constructible
  in an elementary way from optimal codes.

Questions and potential complications

- What should be considered as an elementary construction?
- Conditions might be contradictory (circular dependencies).
- What about computability?

Compromise

- We consider the following "local" elementary constructions:
  - Extend by a zero position: $[n, k, d] \rightsquigarrow [n+1, k, d]$.
  - Shorten: $[n, k, d] \rightsquigarrow [n-1, k-1, d]$.
  - Puncture: $[n, k, d] \rightsquigarrow [n-1, k, d-1]$.
- "better than others"-property yields
  the following notions of optimality for $[n, k, d]$ code C.
  - Again: C length-optimal (n-opt.) $\iff$ $\nexists [n-1, k, d]$-code.
  - C shortening-optimal (S-opt.) $\iff$ $\nexists [n+1, k+1, d]$-code.
  - C puncturing-optimal (P-opt.) $\iff$ $\nexists [n+1, k, d+1]$-code.
  - C strongly optimal $\iff$ n-opt. <u>and</u> S-opt. <u>and</u> P-opt.

  (Dodunekov, Simonis 2000)

Remarks

- n-, S- and P-optimality are independent properties.
- strongly regular codes satisfy “building block”-property for all codes C except border cases.
  (repetition & parity-check codes, full/empty space)
- n-, S- and P-optimality are parametric optimality wrt representation of parameters as $[s, k, d]$, where $s = n - k - d + 1 \geq 0$ is Singleton defect of C.

Conclusion

- d- and k-optimality are weak concepts of optimality. Forget about them!
- Instead: Think in terms of n-, S- and P-optimality.

Back to the codes C_O and $C_O^\perp \dots$

Theorem

All codes C_O and all codes $C_O^\perp$ are n-optimal.

Proof.

- For $C_O^\perp$: sphere packing bound.
- For C_O: linear programming bound ...

$\square$

Proof (n-optimaliy of C_O via LP-bound).

- Assume there exists $[n,k,d]_q = [q^3, 8, q^3 - q^2 - q]_q$ code.
- Let $f(x) = (x - z_1)(x - z_2)(x - z_3)(x - n)$ where

  $$z_1 = q^3 - q^2 - q, \quad z_2 = q^3 - q^2 + q - 2, \quad z_3 = q^3 - q^2 + q - 1.$$

- Then $f(i) \leq 0$ for all $i \in \{d, d+1, \ldots, n\}$.
- Krawchouk expansion of f is $f(x) = \sum_{i=0}^{4} f_i K_i(x)$ where

  $$\begin{aligned} K_i &= i\text{th Krawchouk polynomial} \\ f_0 &= 2/q \cdot (q-1)(q^4 - 2q^3 - q^2 + 3), \\ f_1 &= 2/q^4 \cdot (q-1)(q^6 + q^5 - 10q^3 + 3q + 12), \\ f_2 &= 2/q^4 \cdot (q^5 + 5q^4 - 9q^3 - 6q^2 - 18q + 36), \\ f_3 &= 6/q^4 \cdot (q^3 + q^2 + 3q - 12), \\ f_4 &= 24/q^4. \end{aligned}$$

- For $q \geq 3$: $f_i \geq 0$.
- LP-bound $\implies \#C \leq f(0)/f_0 < q^8$. Contradiction.

Parameters for small q

C_O	$[n, k, d]$	n-opt	S-opt	P-opt	strongly opt
$q = 2$	$[9, 8, 2]$	yes	(no)	yes	(no)
$q = 3$	$[28, 8, 15]$	yes	yes	yes	yes
$q = 4$	$[65, 8, 44]$	yes	yes	yes	yes
$q = 5$	$[126, 8, 95]$	yes	yes	?	?

$C_O^{\perp}$	$[n, k, d]$	n-opt	S-opt	P-opt	strongly opt
$q = 2$	$[9, 1, 9]$	yes	yes	(no)	(no)
$q = 3$	$[28, 20, 6]$	yes	?	yes	?
$q = 4$	$[65, 57, 5]$	yes	no	?	no
$q = 5$	$[126, 118, 5]$	yes	?	?	?

Optimistic conjecture

The codes C_O are strongly optimal for all $q \geq 3$.

Thank you!

Slides will be uploaded at
https://mathe2.uni-bayreuth.de/michaelk/