New ring-linear codes of high minimum distance

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

2012/11/01
Trends in Coding Theory
Monte Verità

History of ring-linear codes

- 1967: John Robinson, electrical engineer at the University of Iowa: Talk for pupils about coding theory
- Discussed research problem:
  For length 16 and minimum distance 6:
  - Optimum size of a *linear* code is 2^7.
  - For unrestricted block codes:
    Optimum size is in $\{2^7, \dots, 2^8\}$.
- Pupil Alan W. Nordstrom
  Constructed a $(16, 2^8, 6)_2$-code!
  Higher minimum distance than all *linear* codes of equal length and size.
  We say: It is BTL (better than linear)
  $\rightsquigarrow$ Famous *Nordstrom-Robinson code* (1967)

History of ring-linear codes (cont.)

- Generalization of the Nordstrom-Robinson-code:
  - 1968: Infinite series of the Preparata-codes
    1993: All BTL.
  - 1972: Infinite series of the Kerdock-codes
    All BTKL (better than *known* linear), conjecture: BTL.
    (Research Problem 15.4 in MacWilliams, Sloane)
- 1994: All these non-linear codes
  are Gray images of $\mathbb{Z}_4$-linear codes!
- Intensive study of ring-linear codes.
  However: No new $\mathbb{Z}_4$-linear BTL-parameters.
  Only sporadic examples of new BTKL-codes.
- Johannes Zwanzger:
  heuristic search for ring-linear codes.
  2009: First examples of new BTL-parameters over $\mathbb{Z}_4$.

Results

- Four new infinite series of ring-linear codes.
- All codes BTL or BTKL (in the table range).
- Found by analysis of the computer examples.
- „Tool”: Projective Hjelmslev geometry.
- base rings: Galois rings of characteristic 4.
  (Smallest member: $\mathbb{Z}_4$)

Galois rings

- Finite rings, „close" to the finite fields.
- Symbol: $\mathrm{GR}(c, r)$ (characteristic c, rank r).
- From now on: Let $R = \mathrm{GR}(4, r)$ and $q = 2^r$.

ideals of R	size
R	q^2
$\vert$	
$2R$	q
$\vert$	
$\{0\}$	1

- residue class field $R/2R \cong \mathbb{F}_q$.

Linear codes over Galois-rings

Definition

- *R-linear code* C: submodule of the R-module R^n
- n is length of C
- $\#C$ is size of C

Experience

For R-linear codes: Hamming distance not interesting!

Definition (homogeneous weight)

- Idea:
  - $w(0) = 0$.
  - associated ring elements have the same weight.
  - ideals $\neq$ zero ideal: Same average weight $\neq 0$.
- $\rightsquigarrow$ homogeneous weight over R:

$$w_{\mathrm{hom}}(a) = \begin{cases} 0 & \text{if } a = 0 \\ q & \text{if } a \in 2R \setminus \{0\} \\ q-1 & \text{if } a \in R^* \end{cases}$$

Example (Homogeneous weight on $\mathbb{Z}_4 = \mathrm{GR}(2^2, 1)$)

Here $q = 2$.

$$w_{\mathrm{hom}}(0) = 0 \qquad w_{\mathrm{hom}}(1) = 1$$
$$w_{\mathrm{hom}}(2) = 2 \qquad w_{\mathrm{hom}}(3) = 1$$

Better known as the Lee weight w_{Lee}!

Example (Heptacode)

The $\mathbb{Z}_4$-linear Heptacode $\mathcal{H}$ is the row space of

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

Lee weight (=homogeneous weight) of the first row:

$$w_{\mathrm{Lee}}((1,0,0,1,2,3,1)) = 1+0+0+1+2+1+1 = 6.$$

minimum weight $w_{\mathrm{Lee}}(\mathcal{H}) = 6$.

$$\rightsquigarrow \mathcal{H} \text{ is a } (7, 2^6, 6)_{\mathbb{Z}_4}\text{-code.}$$

Connection to traditional coding theory

- Define homogeneous distance $d_{\mathrm{hom}}(\mathbf{c}, \mathbf{c}') = w_{\mathrm{hom}}(\mathbf{c} - \mathbf{c}')$.
- minimum distance $=$ minimum weight.
- $\exists$ distance-preserving embedding

$$\psi : (R^n, d_{\mathrm{hom}}) \to (\mathbb{F}_q^{nq}, d_{\mathrm{Ham}}).$$

  generalized Gray map
- So: R-linear $(n, \#C, d)_R$-code C gives $(qn, \#C, d)_q$-code $\psi(C)$ in the Hamming metric (generally: non-linear).

Example (Heptacode (cont.))

- Gray image of the $(7, 2^6, 6)_{\mathbb{Z}_4}$ Heptacode: $\rightsquigarrow$ binary non-linear $(14, 2^6, 6)_2$-code $\psi(\mathcal{O})$.
- Shortest Gray image which is BTL!
- Related to the $(16, 2^8, 6)_2$ Nordstrom-Robinson code.

Projective Hjelmslev geometry

Let $k \geq 2$.

Definition

Projective Hjelmslev geometry $\mathrm{PHG}(R^k)$:
Lattice of submodules of R^k.

- Points: Free submodules of R^k of rank 1.
- Lines: Free submodules of R^k of rank 2
- hyperplanes: Free submodules of R^k of rank $k-1$.

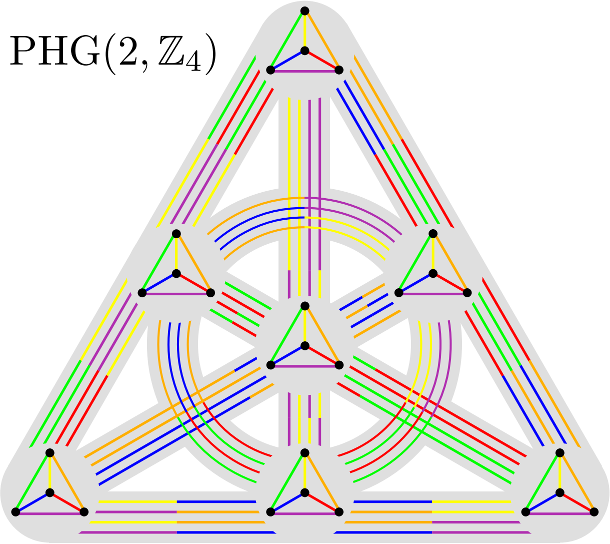
Duality

- The lattice $\mathrm{PHG}(R^k)$ is self-dual.
- Duality interchanges points and hyperplanes.
- $\rightsquigarrow$ construction principle for two series.

Warning

Two different lines may meet in more than one point!

$\mathrm{PHG}(2,\mathbb{Z}_4)$



Connection between codes and geometry

Let $\mathcal{C}$ be an R-linear code of length n, free of rank k.

- $\mathcal{C}$ is the row space of a matrix

$$\mathbf{G} = \begin{pmatrix} | & | & & | \\ \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_n \\ | & | & & | \end{pmatrix} \in R^{k\times n}$$

- If $\mathcal{C}$ fat (projection to each coordinate is onto):
  $\Rightarrow R\mathbf{v}_i$ is a point in $\mathrm{PHG}(R^k)$.
- $\rightsquigarrow$ multiset $\mathfrak{P}$ of points,
  spanning the full geometry
- We get a bijection

$$\begin{array}{c} \text{isomorphism classes of free, fat codes } \mathcal{C} \\ \updownarrow \\ \text{isomorphism classes of multisets } \mathfrak{P} \text{ of points,} \\ \text{spanning the full geometry.} \end{array}$$

Connection between codes and geometry (conn.)

- Bijection:

$$\text{isomorphism classes of free, fat codes } \mathcal{C}$$
$$\updownarrow$$
$$\text{isomorphism classes of multisets } \mathfrak{P} \text{ of points,}$$
$$\text{spanning the full geometry.}$$

$$\begin{array}{rcl} \mathcal{C} & \longrightarrow & \mathrm{pts}(\mathcal{C}) \\ \mathrm{cde}(\mathfrak{P}) & \longleftarrow & \mathfrak{P} \end{array}$$

- Codewords correspond to hyperplanes.
- spectrum of a point set $\mathfrak{P}$:
  information about the position of the points in $\mathfrak{P}$ to the hyperplanes.
- The spectrum of $\mathfrak{P}$
  determines the minimum distance of cde($\mathfrak{P}$)!

Example (Simplex-code)

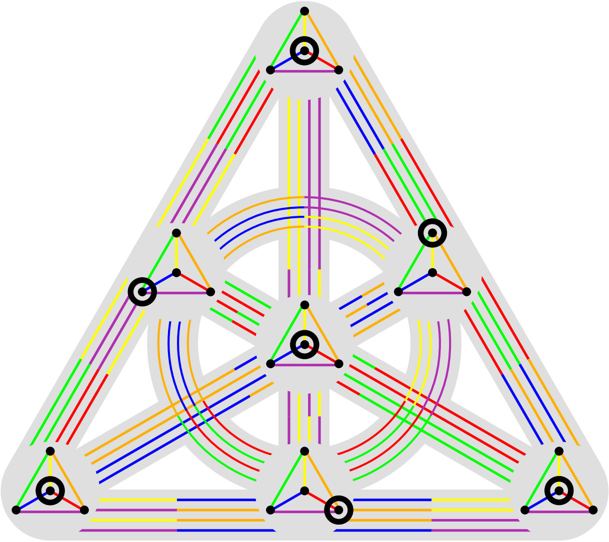
- Chose $\mathfrak{P}$ as the complete point set of PHG(R^k).
- As a linear code: Gray image of cde($\mathfrak{P}$) would be optimal.
- However not BTL, since these optimum linear codes do exist.

Example (Heptacode (cont.))

Look again at the Heptacode $\mathcal{H}$:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

Yields 7 points pts($\mathcal{H}$) in PHG($\mathbb{Z}_4^3$).



Teichmüller codes

- Consider ring extension

$$R = \mathrm{GR}(4, r) \quad \overset{k}{\subset} \quad \mathrm{GR}(4, rk) =: S.$$

- S^* has a unique subgroup of order $q^k - 1$
  (Teichmüller group T, cyclic, $q = 2^r$)
  Teichmüller group t of R^*: order $q - 1$ and $t < T$.
- Consider elements of S as vectors $\mathbf{v} \in R^k$.
  Units in S^* give points $R\mathbf{v}$ in $\mathrm{PHG}(R^k)$.
- coset representatives of T/t yield
  Teichmüller point set $\mathfrak{T}_{q,k}$.
- T. Honold 2010: For k odd:
  $\mathfrak{T}_{q,k}$ is two-intersection.
  (only two intersection numbers with the hyperplanes.)
- Teichmüller codes $\mathcal{T}_{q,k} = \mathrm{cde}(\mathfrak{T}_{q,k})$
  have very good parameters!

Generalization of the Teichmüller codes

- Instead of T: Take supergroups Σ of T!
- Which groups Σ yield 2-intersection sets?
- By the structure of S^* (Raghavendran 1969):

$$T \leq \Sigma < S^* \quad \stackrel{\text{bij.}}{\longleftrightarrow} \quad \mathbb{F}_2\text{-subspaces } \mathbb{F}_q \leq U_\Sigma < \mathbb{F}_{q^k}.$$

- trace form $B : \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \to \mathbb{F}_2$, $(a, b) \mapsto \mathrm{Tr}_{\mathbb{F}_2}(ab)$
  is a symmetric bilinear form on the $\mathbb{F}_2$-vector space $\mathbb{F}_{q^k}$.

Theorem

Σ *induces a two-intersection set in* $\mathrm{PHG}(R^k)$ *if and only if*

1. $B|_{U_\Sigma \times U_\Sigma}$ *is non-degenerate or*
2. $B|_{U_\Sigma^\perp \times U_\Sigma^\perp}$ *is alternate.*
   (i.e. $U_\Sigma^\perp$ *is totally isotropic.)*

Theorem (restated)

Σ induces a two-intersection set in $\mathrm{PHG}(R^k)$ *if and only if*

1. $B|_{U_\Sigma \times U_\Sigma}$ *is non-degenerate or*
2. $B|_{U_\Sigma^\perp \times U_\Sigma^\perp}$ *is alternate.*
   (i.e. $U_\Sigma^\perp$ is totally isotropic.)

Notes on the proof

- Adaption of the proof by T. Honold.
- Representation of S as truncated Witt vectors.
- Use theory of association schemes.
- Use properties of the trace form on U_Σ.

Generated codes

- For good codes: Case 1.
- In which dimension exist suitable subspaces U_Σ?

Lemma

There is an $\mathbb{F}_2$-subspace U of $\mathbb{F}_{q^k}$ with $\dim(U) = s + r$, $\mathbb{F}_q \leq U$ and $B|_{U\times U}$ non-degenerate, if and only if

$$s \in \begin{cases} \{0, 2, 4, \ldots, (k-1)r\} & \text{for } k \text{ odd,} \\ \{r, r+2, r+4, \ldots, (k-1)r\} & \text{for } k \text{ even.} \end{cases}$$

Idea of the proof

- $\mathbb{F}_q \leq U \leq \mathbb{F}_{q^k} \quad \iff \quad U^\perp \leq \mathbb{F}_q^\perp$
- Use classification of bilinear forms over $\mathbb{F}_2$ (A. A. Albert 1938).

Definition

- Generated point set: $\mathfrak{T}_{q,k,s}$
- $\mathcal{T}_{q,k,s} = \mathrm{cde}(\mathfrak{T}_{q,k,s})$

For k odd: $\mathcal{T}_{q,k,0} = \mathcal{T}_{q,k}$.

Theorem

The Gray image of $\mathcal{T}_{q,k,s}$ has the parameters

$$\left(2^s q \cdot \frac{q^k - 1}{q - 1}, \quad q^{2k}, \quad 2^s q^k - 2^{s/2} q^{\frac{k-1}{2}}\right)_q.$$

Idea of the proof

Two intersection numbers of $\mathfrak{T}_{q,k,s}$

$\rightsquigarrow$ spec($\mathfrak{T}_{q,k,s}$)

$\rightsquigarrow$ Minimum distance of $\mathcal{T}_{q,k,s}$.

Comment

Algorithm of T. Feulner:
Isomorphism Type of $\mathcal{T}_{q,k,s}$
generally depends on the choice of U_Σ.

Example

- $\mathcal{T}_{2,3,0}$ is the Heptacode, so BTL.
- Gray image of $\mathcal{T}_{2,4,1}$ has the BTL parameters

$$(60, 2^8, 28)_2$$

  (Same parameters as a doubly shortened Kerdock code.)
- Gray image of $\mathcal{T}_{2,5,2}$ has the BTKL parameters

$$(248, 2^{10}, 120)_2$$

  unknown!

Overview

Constructed Series

- Generalized Teichmüller codes $\mathcal{T}_{q,k,s}$.
- Dualized generalized Teichmüller codes $\mathcal{T}^*_{q,k,s}$.
- Dualized Kerdock codes $\hat{\mathcal{K}}^*_{k+1}$.
- Augmented Simplex codes $\hat{\mathcal{S}}_{q,k}$.

Examples

Code	Gray image	Status	Comment
$\mathcal{T}_{2,5,2}$	$(248, 2^{10}, 120)_2$	BTKL	new
$\mathcal{T}_{4,3,0}$	$(84, 4^6, 60)_4$	BTKL	Hemme, Honold, Landjev 2000
$\mathcal{T}^*_{2,5,0}$	$(372, 2^{10}, 184)_2$	**BTL**	K., Zwanzger 2011
$\mathcal{T}^*_{4,3,0}$	$(504, 4^6, 376)_4$	BTKL	K., Kohnert 2007
$\hat{\mathcal{K}}^*_{3+1}$	$(114, 2^8, 56)_2$	**BTL**	Zwanzger 2009
$\hat{\mathcal{S}}_{2,3}$	$(58, 2^7, 28)_2$	**BTL**	Zwanzger 2009
$\hat{\mathcal{S}}_{2,4}$	$(244, 2^9, 120)_2$	BTKL	K., Zwanzger 2011