Codes from translation schemes on Galois rings of characteristic 4

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

Combinatorics 2012
September 11, 2012
Centro Congressi Hotel Giò, Perugia, Italy

Outline

Preliminaries
- Motivation
- Symmetric translation schemes
- Galois rings

Construction of symmetric 3-class association schemes

Derived combinatorial objects
- Point sets in projective Hjelmslev geometries
- R-linear codes

Outline

Preliminaries
- Motivation
- Symmetric translation schemes
- Galois rings

Construction of symmetric 3-class association schemes

Derived combinatorial objects
- Point sets in projective Hjelmslev geometries
- R-linear codes

Motivation

- Several series of good $\mathbb{Z}_4$-linear codes are based on a Teichmüller point set $\mathfrak{T}$ in projective Hjelmslev geometry. (More general: Galois ring R of char. 4 instead of $\mathbb{Z}_4$)
- Computer search for codes with Johannes Zwanzger: Suggests similar constructions from certain unions of disjoint copies of $\mathfrak{T}$.
- Question: What is the right way to combine copies of $\mathfrak{T}$?
- $\mathfrak{T}$ is two-intersection set. Done by Thomas Honold in 2010, using theory of association schemes. (more precisely: Symmetric translation schemes on group $(R, +)$.)
- Follow his approach to answer the question!

Definition (Symmetric translation scheme)

Given:

- finite Abelian group G,
- partition $\{G_0, \dots, G_n\}$ of G.

Define relations

$$R_i = \{(g,h) \in G \times G \mid g - h \in G_i\}.$$

Then: $\mathcal{A} = \{R_0, \dots, R_n\}$ partition of $G \times G$.

$\mathcal{A}$ called symmetric n-class translation scheme on G, if

- $G_0 = \{0\}$,
  ($\Leftrightarrow$ R_0 is the diagonal of $G \times G$)
- $-G_i = G_i$ for all i,
  ($\Leftrightarrow$ all R_i symmetric)
- For any i, j, k and $(g,h) \in R_k$: Intersection number

  $$p_{ij}^k := \#\{x \in G \mid (g,x) \in R_i \text{ and } (x,g) \in R_j\}$$

  only depends on i, j, k (but not on the choice of g, h).

Example

Symmetric 3-class translation scheme on $G = (\mathbb{Z}_6, +)$.

$$G = \{\{0\}, \{3\}, \{\pm 1\}, \{\pm 2\}\}$$

Then

- $R_0 = \{(0,0), (1,1), (2,2), (3,3), (4,4), (5,5)\}$,
- $R_0 = \{(0,3), (1,4), (2,5), (3,0), (4,1), (5,2)\}$,
- $R_1 = \{(0,1), (1,2), (2,3), (3,4), (4,5), (5,0), \ldots\}$,
- $R_2 = \{(0,2), (1,3), (2,4), (3,5), (4,0), (5,1), \ldots\}$.

$G \times G$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Example

Symmetric 3-class translation scheme on $G = (\mathbb{Z}_6, +)$.

$$G = \{ \{0\}, \{3\}, \{\pm 1\}, \{\pm 2\} \}$$

Then

- $R_0 = \{(0,0),(1,1),(2,2),(3,3),(4,4),(5,5)\}$,
- $R_0 = \{(0,3),(1,4),(2,5),(3,0),(4,1),(5,2)\}$,
- $R_1 = \{(0,1),(1,2),(2,3),(3,4),(4,5),(5,0),\ldots\}$,
- $R_2 = \{(0,2),(1,3),(2,4),(3,5),(4,0),(5,1),\ldots\}$.

$G \times G$	0	1	2	3	4	5
0	0					
1		0				
2			0			
3				0		
4					0	
5						0

Example

Symmetric 3-class translation scheme on $G = (\mathbb{Z}_6, +)$.

$$G = \{ \{0\}, \{3\}, \{\pm 1\}, \{\pm 2\} \}$$

Then

- $R_0 = \{(0,0),(1,1),(2,2),(3,3),(4,4),(5,5)\}$,
- $R_0 = \{(0,3),(1,4),(2,5),(3,0),(4,1),(5,2)\}$,
- $R_1 = \{(0,1),(1,2),(2,3),(3,4),(4,5),(5,0),\ldots\}$,
- $R_2 = \{(0,2),(1,3),(2,4),(3,5),(4,0),(5,1),\ldots\}$.

$G \times G$	0	1	2	3	4	5
0	0			1		
1		0			1	
2			0			1
3	1			0		
4		1			0	
5			1			0

Example

Symmetric 3-class translation scheme on $G = (\mathbb{Z}_6, +)$.

$$G = \{\{0\}, \{3\}, \{\pm 1\}, \{\pm 2\}\}$$

Then

- $R_0 = \{(0,0), (1,1), (2,2), (3,3), (4,4), (5,5)\}$,
- $R_0 = \{(0,3), (1,4), (2,5), (3,0), (4,1), (5,2)\}$,
- $R_1 = \{(0,1), (1,2), (2,3), (3,4), (4,5), (5,0), \ldots\}$,
- $R_2 = \{(0,2), (1,3), (2,4), (3,5), (4,0), (5,1), \ldots\}$.

$G \times G$	0	1	2	3	4	5
0	0	2		1		2
1	2	0	2		1	
2		2	0	2		1
3	1		2	0	2	
4		1		2	0	2
5	2		1		2	0

Example

Symmetric 3-class translation scheme on $G = (\mathbb{Z}_6, +)$.

$$G = \{ \{0\}, \{3\}, \{\pm 1\}, \{\pm 2\} \}$$

Then

- $R_0 = \{(0,0),(1,1),(2,2),(3,3),(4,4),(5,5)\}$,
- $R_0 = \{(0,3),(1,4),(2,5),(3,0),(4,1),(5,2)\}$,
- $R_1 = \{(0,1),(1,2),(2,3),(3,4),(4,5),(5,0),\ldots\}$,
- $R_2 = \{(0,2),(1,3),(2,4),(3,5),(4,0),(5,1),\ldots\}$.

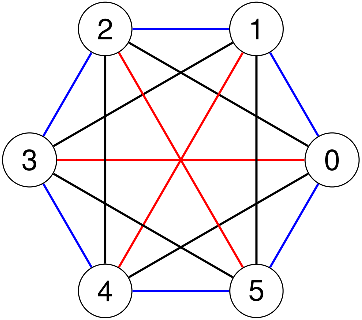
$G \times G$	0	1	2	3	4	5
0	0	2	3	1	3	2
1	2	0	2	3	1	3
2	3	2	0	2	3	1
3	1	3	2	0	2	3
4	3	1	3	2	0	2
5	2	3	1	3	2	0

Example (continued)

Visualization as colored complete graph:

$G \times G$	0	1	2	3	4	5
0	0	2	3	1	3	2
1	2	0	2	3	1	3
2	3	2	0	2	3	1
3	1	3	2	0	2	3
4	3	1	3	2	0	2
5	2	3	1	3	2	0

$\rightsquigarrow$



$$p^{1}_{2\,3} = 2$$

$$p^{2}_{2\,2} = 0$$

$$p^{0}_{3\,3} = 2$$

Aim for this talk

Find symmetric 3-class translation schemes on

$$G = (\mathbb{Z}_4 \times \ldots \times \mathbb{Z}_4, \quad +)$$

Idea

- Take finite ring R with $(R, +) \cong G$.
- For construction: Make use of ring multiplication!

Choice for the ring R

Galois rings of characteristic 4.

Definition (Galois ring)

Given:

- Prime power $q = p^r$.
- m positive integer.
- $f \in \mathbb{Z}_{p^m}[X]$ monic, $\deg(f) = r$, image $\bar{f} \in \mathbb{Z}_p[X]$ irreducible.

Galois ring $GR(p^m, r) := \mathbb{Z}_{p^m}[X]/(f)$

Remarks

- p^m is the characteristic.
- r is the degree.
- Up to ring-isomorphism: Independent of the choice of f.
- Order: p^{mr}.

Example

- $\mathrm{GR}(p, r) \cong \mathbb{F}_{p^r}$
- $\mathrm{GR}(p^m, 1) \cong \mathbb{Z}_{p^m}$
- Smallest ”proper” Galois ring: $\mathrm{GR}(4, 2)$ or order 16.

Fact

R^* has a unique subgroup T of order $q-1$ (Teichmüller group).
T is cyclic.

Example

Look at $R = \mathbb{Z}_{25} = \mathrm{GR}(5^2, 1)$.
Then $q = 5$. Its Teichmüller group is

$$T = \langle 7 \rangle = \{\pm 1, \pm 7\} < R^*,$$

a cyclic group of order 4.

From now on

$R = \mathrm{GR}(4, r)$ Galois ring of characteristic 4 (i.e. $p = m = 2$).
Smallest case: $R = \mathrm{GR}(4, 1) = \mathbb{Z}_4$.

Lattice of ideals

$$\begin{array}{c} R \\ | \\ 2R \\ | \\ \{0\} \end{array}$$

$2R$ is maximum ideal.
Residue field $R/2R \cong \mathbb{F}_q$ with $q = 2^r$.

Outline

Preliminaries
Motivation
Symmetric translation schemes
Galois rings

Construction of symmetric 3-class association schemes

Derived combinatorial objects
Point sets in projective Hjelmslev geometries
R-linear codes

For $T \leq \Sigma < R^*$ consider partition of $\mathrm{GR}(4, r)$

$$\{\{0\}, \quad 2\Sigma \setminus \{0\}, \quad \Sigma, \quad R^* \setminus \Sigma\}$$

Question

Which Σ induce 3-class translation scheme on $(\mathrm{GR}(4, r), +)$?

Description by $\mathbb{F}_2$-vector spaces

By structure of R^* (Raghavendran 1969):

$$T \leq \Sigma \leq R^* \quad \stackrel{1-\mathrm{to}-1}{\longleftrightarrow} \quad \mathbb{F}_2\text{-subspaces } U_\Sigma \leq \mathbb{F}_q.$$

Conditions

- We need $-\Sigma_U = \Sigma_U$.
  Corresponds to: $\mathbb{F}_2 \leq U$.
- Critical point: Intersection number p_{22}^3.

Look at trace form

$$B(x,y) : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_2, \quad (x,y) \mapsto \mathrm{Tr}_{\mathbb{F}_2}(xy).$$

B is nondegenerate symmetric bilinear form on $\mathbb{F}_q$ (as $\mathbb{F}_2$-vector space).

Definition

Let U be a $\mathbb{F}_2$-subspace of $\mathbb{F}_q$.
Restriction $B|_{U\times U}$ is bilinear form on U.
Call U

- Type I, if $B|_{U\times U}$ is nondegenerate.
- Type II, if $B|_{U^\perp \times U^\perp}$ is alternating.
  (That is, $U^\perp$ is totally isotropic)

Theorem

Σ_U induces symm. 3-class transl. scheme on $(\mathrm{GR}(4,r),+)$ *iff*

- $\mathbb{F}_2 \leq U < \mathbb{F}_q$ *and*
- *U is of type I or II.*

Theorem (restated)

Σ_U induces symm. 3-class transl. scheme on $(\mathrm{GR}(4, r), +)$ iff

- $\mathbb{F}_2 \leq U < \mathbb{F}_q$ and
- U is of type I or II.

Idea of proof

Thomas Honold (2010): Proof for particular group Σ.
Follow this proof.
For p^3_{22}, extra work is needed.
Use properties of the trace form and type I/II property of U.

Theorem (restated)

Σ_U induces symm. 3-class transl. scheme on $(\mathrm{GR}(4,r),+)$ iff

- $\mathbb{F}_2 \leq U < \mathbb{F}_q$ and
- U is of type I or II.

Theorem

There exists $\mathbb{F}_2$-subspace U of $\mathbb{F}_q$ with $\mathbb{F}_2 \leq U$ and $\dim(U) = \sigma$

- *of type I, iff*
$$\sigma \in \begin{cases} \{1,3,5,\dots,r\} & \text{if } r \text{ odd,} \\ \{2,4,6,\dots,r\} & \text{if } r \text{ even.} \end{cases}$$
- *of type II, iff*
$$\sigma \in \{\lceil r/2 \rceil, \quad \lceil r/2 \rceil + 1, \quad \lceil r/2 \rceil + 2, \quad \dots, \quad r\}.$$

Idea of proof

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

Comparison with literature

- Type II: Translation schemes already known. (as fusions of amorphous association schemes by Ito, Munemasa, Yamada (1991)).
- Type I: Only known for
  - $\sigma \in \{1, 2\}$ (Ma 2007).
  - $\sigma \mid r$ and r/σ odd (Honold 2010).

Outline

Preliminaries
- Motivation
- Symmetric translation schemes
- Galois rings

Construction of symmetric 3-class association schemes

Derived combinatorial objects
- Point sets in projective Hjelmslev geometries
- *R*-linear codes

Point sets in projective Hjelmslev geometries

- Schemes of type I and II:
  $\rightsquigarrow$ 2-intersection sets in projective Hjelmslev geometries.
- In type I case:
  Series of large u-arcs $\mathfrak{T}_{2^r,k,s}$ in $\mathrm{PHG}(\mathrm{GR}(4,r)^k)$, generalizing
  - Teichmüller point sets (k odd, $s=0$)
  - containing the hyperovals ($k=3$, $s=0$),

  Examples of arcs of maximal possible size:
  - $\mathfrak{T}_{4,3,2}$ is $(84,6)$-arc in $\mathrm{PHG}(\mathrm{GR}(4,2)^3)$ (already known).
  - $\mathfrak{T}_{2,4,2}$ is $(30,8)$-arc in $\mathrm{PHG}(\mathbb{Z}_4^4)$ (new!)

R-linear codes

- From Type II schemes:
  Infinite series $\mathcal{U}_{2^r,k,s}$ of GR$(4, r)$-linear two-weight codes.
- From Type I schemes:
  Infinite series $\mathcal{T}_{2^r,k,s}$ of GR$(4, r)$-linear codes
  of high minimum distance.
  Generalization of Teichmüller codes (special case $s = 0$).
- Codes in $\mathcal{T}_{2^r,k,s}$ have very high minimum distance:
  Gray image of any code $\mathcal{T}_{2^r,k,s}$
  is better than all known comparable $\mathbb{F}_{2^r}$-linear codes.
- Example: Gray image of $\mathcal{T}_{2,5,2}$ is new nonlinear binary $(248, 2^{10}, 120)_2$-code.
  Best known *linear* binary $[248, 10]$-code has minimum distance only 119.
- Generalization of two further series
  of high-distance R-linear codes.