Relative Projective Group Codes over Chain Rings

Simon Eisenbarth

RWTH Aachen University

19th of July, 2019

Group codes over fields

Let $\mathbb{F}$ be a finite field and $G = \{g_1, \ldots, g_n\}$ be a finite group, then a group code C is an (left/right/two-sided) ideal in the group ring $\mathbb{F}G$.

Dimension of C is the dimension as a vector space.

Berman '67: Reed-Muller Code of order $m - l$ is the l^{th} power of the Jacobson radical in the group algebra $\mathbb{F}_2 C_2^m$

also: cyclic codes are ideals in the group algebra $\mathbb{F}C_n \cong \mathbb{F}[x]/(x^n - 1)$

Berman '67: Reed-Muller Code of order $m - l$ is the l^{th} power of the Jacobson radical in the group algebra $\mathbb{F}_2 C_2^m$

also: cyclic codes are ideals in the group algebra $\mathbb{F} C_n \cong \mathbb{F}[x]/(x^n - 1)$

MacWilliams '69: constructed certain self-dual codes over $\mathbb{F}_2 D_{2n}$, but also remarked that this was by no means a complete classification

MacWilliams '70: generalized properties of cyclic codes to codes over abelian group rings

The map

$$\phi : \mathbb{F}G \to \mathbb{F}^n, \sum_{i=1}^{n} a_i g_i \mapsto (a_1, \ldots, a_n)$$

is an isomorphism, which transfers all relevant properties from a group code $C \leq \mathbb{F}G$ to a classical linear code $\phi(C) \leq \mathbb{F}^n$ with $G \leq \mathrm{Aut}(C)$.

A linear Code C of length n over $\mathbb{F}$ is called group code for G, if there is a bijektion

$$\nu : \{1, \ldots, n\} \to G,$$

such that

$$\left\{ \sum_{i=1}^{n} a_i \nu(i) \mid (a_1, \ldots, a_n) \in C \right\}$$

is an ideal in $\mathbb{F}G$.

Theorem (Bernal, del Río, Simón '09)

Let C be a linear code of length n over $\mathbb{F}$ and let G be a finite group of order n.

i) *C is a left group code for G, iff G is isomorphic to a transitive subgroup of $\mathrm{PAut}(C) = \mathrm{Aut}(C) \cap S_n$.*

ii) *C is a two-sided group code for G, iff G is isomorphic to a transitive subgroup H of S_n, such that $H \cup C_{S_n}(G) \subseteq \mathrm{PAut}(C)$.*

Note: a linear code $C \leq \mathbb{F}^n$ can be a group code for different groups G.

Question: which codes can be realized over "nice" groups (i.e. cyclic, abelian,...)?

Note: a linear code $C \leq \mathbb{F}^n$ can be a group code for different groups G.

Question: which codes can be realized over "nice" groups (i.e. cyclic, abelian,...)?

Theorem (Pillado, González, Markov, Markova, Martinez '18)

Every two-sided group code of dimension ≤ 3 is abelian.

Theorem (Bernal, del Río, Simón, '09)

A group G has an abelian decomposition, if two abelian subgroups A, B of G exists, such that

$$G = AB = \{ab \mid a \in A, b \in B\}.$$

In this case every two-sided group code for G is a group code for an abelian group.

Theorem (Bernal, del Río, Simón, '09)

A group G has an abelian decomposition, if two abelian subgroups A, B of G exists, such that

$$G = AB = \{ab \mid a \in A, b \in B\}.$$

In this case every two-sided group code for G is a group code for an abelian group.

Every group of order < 128, except $\{24, 48, 54, 60, 64, 72, 96, 108, 120\}$, has an abelian decomposition.

$\rightarrow$ every two-sided group code over such a group G is abelian.

Remark

Let G be a group of order < 64, which does not have an abelian decomposition. Then there exists a two-sided ideal in $\mathbb{F}_2 G$ which is not an abelian group code .

Remark

Let G be a group of order < 64, which does not have an abelian decomposition. Then there exists a two-sided ideal in $\mathbb{F}_2 G$ which is not an abelian group code .

Conjecture

Every two-sided group code over a finite group G is abelian, iff G has an abelian decomposition.

Group codes over simple groups

Theorem

Let $\mathbb{F}$ be a finite field, $C \leq \mathbb{F}A_5$ be a two-sided group code and let $A := \mathrm{PAut}(C)$. Then there a two possibilities:

i) $A = S_{60}$, *in particular* $C = \{0\}, C = \mathbb{F}A_5, C = \langle \sum_{g \in A_5} g \rangle$ *or* $C = \langle \sum_{g \in A_5} g \rangle^{\perp}$

ii) C *is not an abelian group code*

Group codes over simple groups

Theorem

Let $\mathbb{F}$ be a finite field, $C \leq \mathbb{F}A_5$ be a two-sided group code and let $A := \mathrm{PAut}(C)$. Then there a two possibilities:

i) *$A = S_{60}$, in particular $C = \{0\}, C = \mathbb{F}A_5, C = \langle \sum_{g \in A_5} g \rangle$ or $C = \langle \sum_{g \in A_5} g \rangle^{\perp}$*

ii) *C is not an abelian group code*

The group A contains A_5^2, in fact all permutations which are induced by the action

$$A_5^2 \times A_5 \to A_5, ((g_1, g_2), g) \mapsto g_1 g g_2^{-1}.$$

Group codes over simple groups

Theorem

Let $\mathbb{F}$ be a finite field, $C \leq \mathbb{F}A_5$ be a two-sided group code and let $A := \mathrm{PAut}(C)$. Then there a two possibilities:

i) *$A = S_{60}$, in particular $C = \{0\}, C = \mathbb{F}A_5, C = \langle \sum_{g \in A_5} g \rangle$ or $C = \langle \sum_{g \in A_5} g \rangle^{\perp}$*

ii) *C is not an abelian group code*

The group A contains A_5^2, in fact all permutations which are induced by the action

$$A_5^2 \times A_5 \to A_5, ((g_1, g_2), g) \mapsto g_1 g g_2^{-1}.$$

This group is primitive, so A is also primitive.

Group codes over simple groups

Theorem

Let $\mathbb{F}$ be a finite field, $C \leq \mathbb{F}A_5$ be a two-sided group code and let $A := \mathrm{PAut}(C)$. Then there a two possibilities:

i) *$A = S_{60}$, in particular $C = \{0\}, C = \mathbb{F}A_5, C = \langle \sum_{g \in A_5} g \rangle$ or $C = \langle \sum_{g \in A_5} g \rangle^{\perp}$*

ii) *C is not an abelian group code*

The group A contains A_5^2, in fact all permutations which are induced by the action

$$A_5^2 \times A_5 \to A_5, ((g_1, g_2), g) \mapsto g_1 g g_2^{-1}.$$

This group is primitive, so A is also primitive.
Using the O'Nan-Scott theorem (classification of all (primitive) maximal subgroups of S_n) one can show that all possible $A \neq S_{60}$ do not contain a transitive, abelian subgroup.

This is still an explicit calculation (done in S_{60} of order $8.3 \cdot 10^{81}$) in GAP:

Is this theorem true for other alternating groups? Can the O'Nan-Scott theorem be used to show such an assertion for other simple groups? Or other interesting families of groups?

Construction D: a chain of (binary) linear codes can be used to construct a $\mathbb{Z}$-lattice with a lower bound on the minumum.

$\rightarrow$ can group codes over chain rings be constructed with chains of group codes over fields?

Group codes over chain rings

Construction D: a chain of (binary) linear codes can be used to construct a $\mathbb{Z}$-lattice with a lower bound on the minumum.

$\rightarrow$ can group codes over chain rings be constructed with chains of group codes over fields?

in other words: how can linear codes be lifted to codes over chain rings, such that a certain subgroup of the (permutation-) automorphism group is preserved?

Let R be a commutative, artinian chain ring of length ℓ with maximal ideal $\mathfrak{m} = \langle \pi \rangle$ und residue field $\mathbb{F} := R/\mathfrak{m}$.

R-module isomorphisms ($j = 0, \ldots, \ell - 1$)

$$\alpha_j : \mathfrak{m}^j/\mathfrak{m}^{j+1} \to \mathbb{F}, \pi^j r + \mathfrak{m}^{j+1} \mapsto r + \mathfrak{m}$$

(extend this to RG by abuse of notation)

Definition

A group code $C \leq \mathbb{F}G$ is called (central) projective, if it is generated by some (central) idempotent, i.e. $C = \mathbb{F}Ge$ and $e^2 = e$.

Definition

A group code $C \leq \mathbb{F}G$ is called (central) projective, if it is generated by some (central) idempotent, i.e. $C = \mathbb{F}Ge$ and $e^2 = e$.

If $\text{char}(\mathbb{F}) \nmid |G|$, then $\mathbb{F}G$ is semisimple by the theorem of Maschke, so every group code is projective.

Let $e \in \mathbb{F}G$ be an idempotent. Then there exists an idempotent $\epsilon \in RG$ with

$$\alpha_0(\epsilon) = \epsilon + \mathfrak{m} = e.$$

Let $e \in \mathbb{F}G$ be an idempotent. Then there exists an idempotent $\epsilon \in RG$ with

$$\alpha_0(\epsilon) = \epsilon + \mathfrak{m} = e.$$

Lifting of idempotents in a ring with nilpotent ideal: chose a preimage $\epsilon_0 \in RG$ with $\alpha_0(\epsilon_0) = e$ and define $\epsilon_i = 3\epsilon_{i-1}^2 - 2\epsilon_{i-1}^3$. Then $\epsilon := \epsilon_\ell$ satisfies $\alpha_0(\epsilon) = e$ and $\epsilon^2 = \epsilon$.

Let

$$\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

be a chain of projective group codes over $\mathbb{F}G$ with idempotents $C_i = \mathbb{F}Ge_i$, then $e_i e_j = e_{\min(i,j)}$.

Let

$$\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

be a chain of projective group codes over $\mathbb{F}G$ with idempotents $C_i = \mathbb{F}Ge_i$, then $e_ie_j = e_{\min(i,j)}$.
Let $\epsilon_i \in RG$ be an idempotent such that $\alpha_0(\epsilon_i) = \epsilon_i + \mathfrak{m} = e_i$.

Let

$$\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

be a chain of projective group codes over $\mathbb{F}G$ with idempotents $C_i = \mathbb{F}Ge_i$, then $e_i e_j = e_{\min(i,j)}$.
Let $\epsilon_i \in RG$ be an idempotent such that $\alpha_0(\epsilon_i) = \epsilon_i + \mathfrak{m} = e_i$.
Define

$$\mathcal{C} := RG \cdot \left(\sum_{j=0}^{\ell-1} \pi^j \epsilon_j \right).$$

Define

$$\mathcal{C} := RG \cdot \left(\sum_{j=0}^{\ell-1} \pi^j \epsilon_j \right).$$

Define

$$\mathcal{C} := RG \cdot \left(\sum_{j=0}^{\ell-1} \pi^j \epsilon_j \right).$$

This (left)-ideal is relative projective for the subgroup $\{1\}$ of G (in the sense of homological algebra):

Define

$$\mathcal{C} := RG \cdot \left(\sum_{j=0}^{\ell-1} \pi^j \epsilon_j \right).$$

This (left)-ideal is relative projective for the subgroup $\{1\}$ of G (in the sense of homological algebra): for every short exact sequenz

$$0 \to \mathcal{M} \to \mathcal{N} \stackrel{\varphi}{\to} \mathcal{C} \to 0$$

for which there exists an R-module homomorphism

$$\psi : \mathcal{C} \to \mathcal{N} \text{ with } \varphi \circ \psi = \mathrm{id}_{\mathcal{C}},$$

there exists an RG-module homomorphism with the same property

$\rightarrow$ if the sequence is right split as R-module, it is right split as RG-module

Theorem

Let $\mathcal{C} \leq RG$ be a relative projective group code. Then there exist primitive, orthogonal idempotents $\epsilon_i \in RG$ and $a_i \in \mathbb{N}_0$ such that

$$\mathcal{C} = \bigoplus_{i=1}^{s} \pi^{a_i} RG \epsilon_i.$$

Let $\mathcal{C} = \bigoplus_{i=1}^{s} \pi^{a_i} RG\epsilon_i$ be a relative projective group ring code.
For $0 \leq j \leq \ell - 1$ define

$$C_j := \alpha_j \left(\frac{\mathcal{C} \cap \mathfrak{m}^j}{\mathcal{C} \cap \mathfrak{m}^{j+1}} \right).$$

Let $\mathcal{C} = \bigoplus_{i=1}^{s} \pi^{a_i} RG\epsilon_i$ be a relative projective group ring code. For $0 \leq j \leq \ell - 1$ define

$$C_j := \alpha_j \left(\frac{\mathcal{C} \cap \mathfrak{m}^j}{\mathcal{C} \cap \mathfrak{m}^{j+1}} \right).$$

This code is projective because

$$\alpha_j \left(\frac{\mathcal{C} \cap \mathfrak{m}^j}{\mathcal{C} \cap \mathfrak{m}^{j+1}} \right) = \mathbb{F}G \cdot \underbrace{\sum_{a_i \leq j} \alpha_0(\epsilon_i)}_{=: e_j}$$

and

$$\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

is a chain of projective group ring codes over $\mathbb{F}$.

We get the following maps:

$$\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

We get the following maps:

$$\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

$$\downarrow$$

$$\mathcal{C} = RG\left(\sum_{j=0}^{\ell-1} \pi^j \epsilon_j\right)$$

We get the following maps:

$$\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

$$\downarrow$$

$$\mathcal{C} = RG\left(\sum_{j=0}^{\ell-1} \pi^j \epsilon_j\right)$$

$$\downarrow$$

$$C_j = \alpha_j\left(\frac{\mathcal{C} \cap \mathfrak{m}^j}{\mathcal{C} \cap \mathfrak{m}^{j+1}}\right),\ j = 0, \ldots, \ell - 1$$

In summary, we get the following tongue twister:

Theorem

Relative projective group ring codes over chain rings are in bijection to chains of projective group ring codes.

Duality

Let $\mathcal{C} \leq RG$ be a relative projective group ring code with $\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$. Then the „dual chain“ is given by

$$\mathcal{C}_\star^\perp : C_{\ell-1}^\perp \leq \cdots \leq C_0^\perp .$$

Duality

Let $\mathcal{C} \leq RG$ be a relative projective group ring code with $\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$. Then the „dual chain" is given by

$$\mathcal{C}_\star^\perp : C_{\ell-1}^\perp \leq \cdots \leq C_0^\perp .$$

Remark

If ℓ is even, a self-dual relative projective group code always exists, for example

$$\mathcal{C}_\star = \underbrace{\{0\} \leq \cdots \leq \{0\}}_{\ell/2} \leq \underbrace{\mathbb{F}G \leq \cdots \leq \mathbb{F}G}_{\ell/2} .$$

For ℓ odd, the code $C_{\frac{l-1}{2}}$ over $\mathbb{F}G$ has to be self-dual, but such a code can never be generated by an idempotent (Willems 2002)
$\rightarrow$ a self-dual relative projective code over RG exists iff the length of R is even

The minimum distance

Hamming weight:

$$w_H(c) := |\{c_i \mid c_i \neq 0\}|, c = \sum_{i=1}^{n} c_i g_i \in \mathcal{C} \leq RG$$

Hamming distance:

$$d_H(\mathcal{C}) := \min\{w_H(c) \mid 0 \neq c \in \mathcal{C}\}$$

The minimum distance

Hamming weight:

$$w_H(c) := |\{c_i \mid c_i \neq 0\}|, c = \sum_{i=1}^{n} c_i g_i \in \mathcal{C} \leq RG$$

Hamming distance:

$$d_H(\mathcal{C}) := \min\{w_H(c) \mid 0 \neq c \in \mathcal{C}\}$$

Theorem

Let $\mathcal{C} \leq RG$ be a relative projective group code with $\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$. Then

$$d_H(\mathcal{C}) = d_H(C_{\ell-1}).$$

Special case $R = \mathbb{Z}/p^l\mathbb{Z}$:
Euclidian weight:

$$w_E(c) := \min\left\{\sum_{i=1}^{n} a_i^2 \mid a_i \in \mathbb{Z}, a_i + p^l\mathbb{Z} = c_i\right\}$$

Euclidian distance:

$$d_E(\mathcal{C}) = \min\{w_E(c) \mid 0 \neq c \in \mathcal{C}\}.$$

Special case $R = \mathbb{Z}/p^l\mathbb{Z}$:
Euclidian weight:

$$w_E(c) := \min\left\{\sum_{i=1}^{n} a_i^2 \mid a_i \in \mathbb{Z}, a_i + p^l\mathbb{Z} = c_i\right\}$$

Euclidian distance:

$$d_E(\mathcal{C}) = \min\{w_E(c) \mid 0 \neq c \in \mathcal{C}\}.$$

Theorem

Let $\mathcal{C} \leq (\mathbb{Z}/p^l\mathbb{Z})G$ be a relative projective group code with $\mathcal{C}_\star : C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$. If there exists a $\gamma > 0$, such that $d_E(C_j) \geq \frac{\gamma}{p^{2l}}$, then $d_E(\mathcal{C}) \geq \gamma$.

(similar to construction D)

Example: Dihedral groups

$n = 2^l m$, m odd:

Let

$$x^m - 1 = (x-1) \cdot f_1 \dots f_{m_1} \cdot g_1 g_1^* \dots g_{m_2} g_{m_2}^*,$$

where the f_i are self-conjugate with conjugation $^* : \zeta_m \mapsto \zeta_m^{-1}$.
Then $\mathbb{F}_2 D_{2n}$ has the central, primitive, orthogonal idempotents $\{e_0, \dots, e_{m_1+m_2}\}$ and

$$\mathbb{F}_2 D_{2n} \cdot e_i / \mathfrak{J}_i \cong \begin{cases} \mathbb{F}_2 C_2 & i = 0 \\ \mathbb{E}_i^{2\times 2} & i \geq 1,\ [\mathbb{E} : \mathbb{F}] = \deg(f_i)/2 \ \text{ resp. } \deg(g_i) \end{cases}$$

The idempotents in $\mathbb{F}_2 C_2$ are 0 and 1, the idempotents in $\mathbb{E}_i^{2\times 2}$ are conjugated to

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The idempotents in $\mathbb{F}_2 C_2$ are 0 and 1, the idempotents in $\mathbb{E}_i^{2\times 2}$ are conjugated to

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$\rightarrow$ the idempotents of $\mathbb{F}_2 D_{2n} \cdot e_i / \mathfrak{J}_i$ can be lifted to idempotents of $\mathbb{F} D_{2n} \cdot e_i$, also suitable chains of projective, dihedral group codes can be easily constructed

The idempotents in $\mathbb{F}_2 C_2$ are 0 and 1, the idempotents in $\mathbb{E}_i^{2\times 2}$ are conjugated to

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$\rightarrow$ the idempotents of $\mathbb{F}_2 D_{2n} \cdot e_i / \mathfrak{J}_i$ can be lifted to idempotents of $\mathbb{F} D_{2n} \cdot e_i$, also suitable chains of projective, dihedral group codes can be easily constructed

$\rightarrow$ the (self-dual) codes in $(\mathbb{Z}/4\,\mathbb{Z})D_{2n}$ (for $n \leq 20$) aren't particular interesting, usually in modular representation theory, non-projective group codes are „better" than projective ones (higher minimum distance etc.)