Canonization of linear Codes over $\mathbb{Z}_4$

Thomas Feulner

University of Bayreuth

April 15, 2010

Linear Codes over $\mathbb{Z}_4$

Linear Code

A (linear) code C is a submodule of $\mathbb{Z}_4^n$.

Type of a Code

It has type (k_0, k_1) if $C \simeq \mathbb{Z}_4^{k_0} \times \mathbb{Z}_2^{k_1}$.

Linear Codes over $\mathbb{Z}_4$

Linear Code

A (linear) code C is a submodule of $\mathbb{Z}_4^n$.

Type of a Code

It has type (k_0, k_1) if $C \simeq \mathbb{Z}_4^{k_0} \times \mathbb{Z}_2^{k_1}$.

Ordered basis matrix

Basis of a Code

Let C be of type (k_0, k_1), $k = k_0 + k_1$. A sequence of generators

$$(g_0, \ldots, g_{k_0-1}, 2g_{k_0}, \ldots, 2g_{k-1})$$

of C is called an *ordered basis* of C.

Set of ordered basis matrices of linear codes of type (k_0, k_1)

$$\mathbb{Z}_4^{(k_0,k_1)\times n} \subseteq \mathbb{Z}_4^{k\times n}$$

Ordered basis matrix

Basis of a Code

Let C be of type (k_0, k_1), $k = k_0 + k_1$. A sequence of generators

$$(g_0, \ldots, g_{k_0-1}, 2g_{k_0}, \ldots, 2g_{k-1})$$

of C is called an *ordered basis* of C.

Set of ordered basis matrices of linear codes of type (k_0, k_1)

$$\mathbb{Z}_4^{(k_0,k_1)\times n} \subseteq \mathbb{Z}_4^{k\times n}$$

Ordered basis matrix

A special subgroup

Let

$$\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \leq \mathrm{GL}_k(\mathbb{Z}_4)$$

denote the subgroup of all block matrices of type

$$\begin{pmatrix} A^{(0,0)} & A^{(0,1)} \\ 2A^{(1,0)} & A^{(1,1)} \end{pmatrix}$$

Set of ordered basis matrices of a given linear code

Let Γ be an ordered basis matrix of C. The orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)\right)\Gamma$$

forms the set of all ordered basis matrices of C.

Ordered basis matrix

A special subgroup

Let

$$\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \leq \mathrm{GL}_k(\mathbb{Z}_4)$$

denote the subgroup of all block matrices of type

$$\begin{pmatrix} A^{(0,0)} & A^{(0,1)} \\ 2A^{(1,0)} & A^{(1,1)} \end{pmatrix}$$

Set of ordered basis matrices of a given linear code

Let Γ be an ordered basis matrix of C. The orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)\right)\Gamma$$

forms the set of all ordered basis matrices of C.

Linear Codes over $\mathbb{Z}_4$

Isometry

Two codes C, C' are equivalent if there is

- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$
- a permutation $\pi \in S_n$

with $(\varphi; \pi)C = C'$.

Isometry in terms of ordered basis matrices

Two ordered basis matrices Γ, Γ' are equivalent if there is

- a matrix $A \in GL_{(k_0,k_1)}(\mathbb{Z}_4)$,
- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$ and
- a permutation $\pi \in S_n$

with $(A, \varphi; \pi)\Gamma = \Gamma'$.

Linear Codes over $\mathbb{Z}_4$

Isometry

Two codes C, C' are equivalent if there is

- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$
- a permutation $\pi \in S_n$

with $(\varphi; \pi)C = C'$.

Isometry in terms of ordered basis matrices

Two ordered basis matrices Γ, Γ' are equivalent if there is

- a matrix $A \in GL_{(k_0, k_1)}(\mathbb{Z}_4)$,
- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$ and
- a permutation $\pi \in S_n$

with $(A, \varphi; \pi)\Gamma = \Gamma'$.

Linear Codes over $\mathbb{Z}_4$

Isometry

Two codes C, C' are equivalent if there is

- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$
- a permutation $\pi \in S_n$

with $(\varphi; \pi)C = C'$.

Isometry in terms of ordered basis matrices

Two ordered basis matrices Γ, Γ‘ are equivalent if there is

- a matrix $A \in \mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)$,
- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$ and
- a permutation $\pi \in S_n$.

with $(A, \varphi; \pi)\Gamma = \Gamma'$.

Linear Codes over $\mathbb{Z}_4$

Isometry

Two codes C, C' are equivalent if there is

- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$
- a permutation $\pi \in S_n$

with $(\varphi; \pi)C = C'$.

Isometry in terms of ordered basis matrices

Two ordered basis matrices Γ, Γ‘ are equivalent if there is

- a matrix $A \in \mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)$,
- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$ and
- a permutation $\pi \in S_n$.

with $(A, \varphi; \pi)\Gamma = \Gamma'$.

Linear Codes over $\mathbb{Z}_4$

Isometry

Two codes C, C' are equivalent if there is

- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$
- a permutation $\pi \in S_n$

with $(\varphi; \pi)C = C'$.

Isometry in terms of ordered basis matrices

Two ordered basis matrices Γ, Γ‘ are equivalent if there is

- a matrix $A \in \mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)$,
- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$ and
- a permutation $\pi \in S_n$.

with $(A, \varphi; \pi)\Gamma = \Gamma'$.

Linear Codes over $\mathbb{Z}_4$

Isometry

Two codes C, C' are equivalent if there is

- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$
- a permutation $\pi \in S_n$

with $(\varphi; \pi)C = C'$.

Isometry in terms of ordered basis matrices

Two ordered basis matrices Γ, Γ‘ are equivalent if there is

- a matrix $A \in \mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)$,
- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$ and
- a permutation $\pi \in S_n$.

with $(A, \varphi; \pi)\Gamma = \Gamma'$.

Linear Codes over $\mathbb{Z}_4$

Isometry

Two codes C, C' are equivalent if there is

- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$
- a permutation $\pi \in S_n$

with $(\varphi; \pi)C = C'$.

Isometry in terms of ordered basis matrices

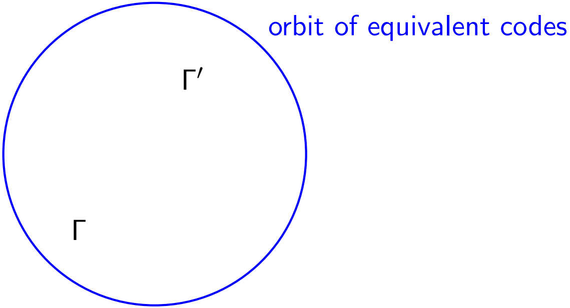
Two ordered basis matrices Γ, Γ' are equivalent if there is

- a matrix $A \in \mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)$,
- a vector of column multiplications $\varphi \in {\mathbb{Z}_4^*}^n$ and
- a permutation $\pi \in S_n$.

with $(A, \varphi; \pi)\Gamma = \Gamma'$.

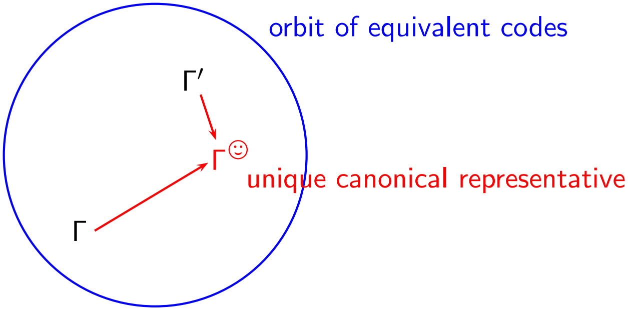
Goal: Canonization

Let $\Gamma, \Gamma' \in \mathbb{Z}_4^{(k_0,k_1)\times n}$ be equivalent ordered basis matrices



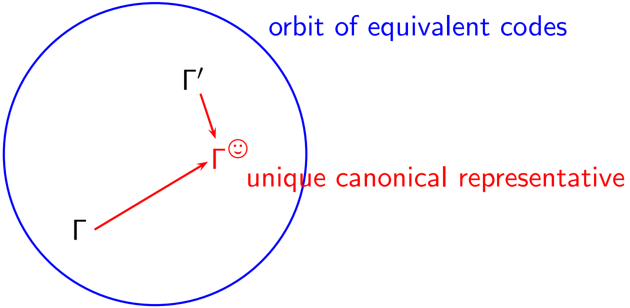
Goal: Canonization

Let $\Gamma, \Gamma' \in \mathbb{Z}_4^{(k_0,k_1)\times n}$ be equivalent ordered basis matrices



Goal: Canonization

Let $\Gamma, \Gamma' \in \mathbb{Z}_4^{(k_0,k_1)\times n}$ be equivalent ordered basis matrices

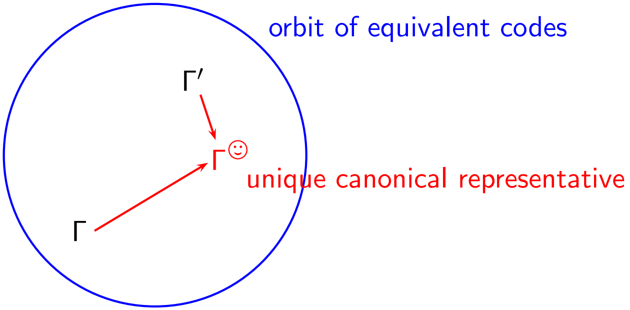


Possible approach to define $\Gamma^{☺}$:

Take the smallest ordered basis matrix

Goal: Canonization

Let $\Gamma, \Gamma' \in \mathbb{Z}_4^{(k_0,k_1)\times n}$ be equivalent ordered basis matrices

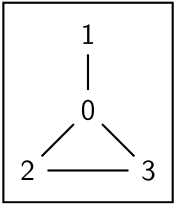


Possible approach to define $\Gamma^{☺}$:

Take the smallest ordered basis matrix

Our definition of "small" is done via the definition of a fast canonization algorithm.

The partition and refinement idea



There is a well-known, very fast canonization algorithm for graphs:

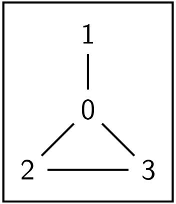
nauty (B. McKay)

based on

Partition & Refinement

The Refinement step

Calculate properties of the vertices, invariant under relabeling!

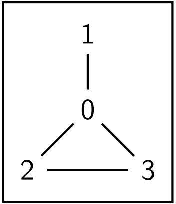


Calculate the degree of the vertices

i	0	1	2	3
degree(i)	3	1	2	2

The Refinement step

Calculate properties of the vertices, invariant under relabeling!



Calculate the degree of the vertices

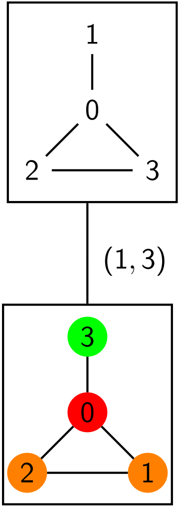
i	0	1	2	3
degree(i)	3	1	2	2

Sort in descending order

i	0	3	2	1
degree(i)	3	2	2	1

The Refinement step

Calculate properties of the vertices, invariant under relabeling!



Calculate the degree of the vertices

i	0	1	2	3
degree(i)	3	1	2	2

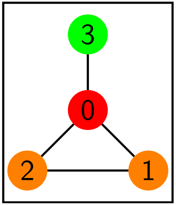
Sort in descending order

i	0	3	2	1
degree(i)	3	2	2	1

Relabel the vertices

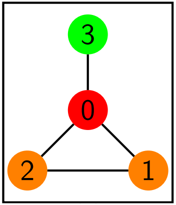
i	0	1	2	3
degree(i)	3	2	2	1

The Partition step



Do a backtracking procedure.

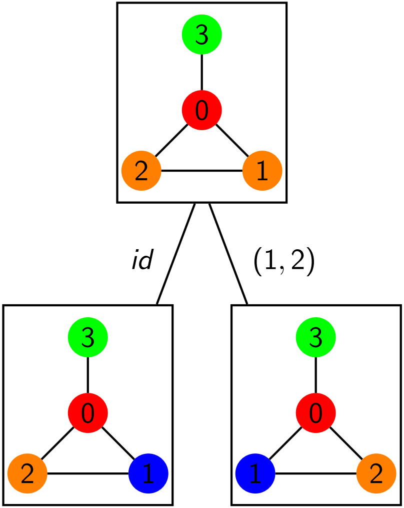
The Partition step



Do a backtracking procedure.

Choose a block of vertices which have the same color.

The Partition step

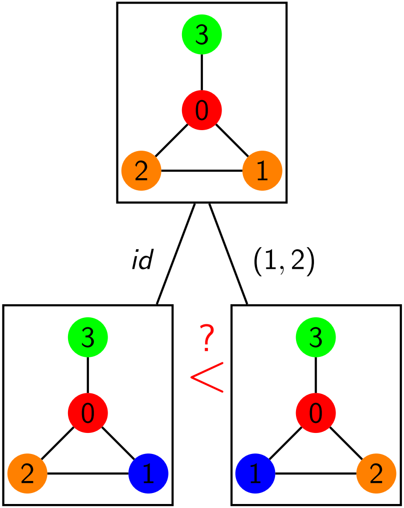


Do a backtracking procedure.

Choose a block of vertices which have the same color.

Investigate all possibilities to color one vertex in this block with a new color and to give it the smallest label.

The Partition step



Do a backtracking procedure.

The comparison of the leaf nodes yields "=":

- $(1, 3)$ and $(1, 2)(1, 3)$ map the graph to its canonical representative
- $(1, 3)^{-1}(1, 2)(1, 3)$ is the only automorphism

Comparison: Graphs and linear Codes

	Graphs	linear Codes
Group Action	$S_n \backslash\backslash 2^{\binom{n}{2}}$	$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times ({\mathbb{Z}_4^*}^n \rtimes S_n)\right) \backslash\backslash \mathbb{Z}_4^{(k_0,k_1)\times n}$

Comparison: Graphs and linear Codes

	Graphs	linear Codes
Group Action	$S_n \backslash\backslash 2^{\binom{n}{2}}$	$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times (\mathbb{Z}_4^{*n} \rtimes S_n)\right) \backslash\backslash \mathbb{Z}_4^{(k_0,k_1)\times n}$ replace by $S_n \backslash\backslash \left(\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times \mathbb{Z}_4^{*n}\right) \backslash\backslash \mathbb{Z}_4^{(k_0,k_1)\times n} \right)$

Leon's algorithm for linear codes over finite fields

Interpret the group

$$\left(\mathbb{F}_q^*\right)^n \rtimes S_n$$

as subgroup of

$$S_{n(q-1)^n}$$

Comparison: Graphs and linear Codes

	Graphs	linear Codes
Group Action	$S_n \backslash\backslash 2^{\binom{n}{2}}$	$S_n \backslash\backslash \left(\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n \right) \backslash\backslash \mathbb{Z}_4^{(k_0,k_1)\times n} \right)$

Comparison: Graphs and linear Codes

	Graphs	linear Codes
Group Action	$S_n \backslash\backslash 2^{\binom{n}{2}}$	$S_n \backslash\backslash \left(\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n \right) \backslash\backslash \mathbb{Z}_4^{(k_0,k_1)\times n} \right)$
Refinement	$f : 2^{\binom{n}{2}} \to X^n$ G-homomorphism for some appropriate $G \leq S_n$	

Homomorphism of group actions

Let G act on X, Y.
$f : X \to Y$ is a G-homomorphism if

$$f(gx) = gf(x),\ \forall\ x \in X, g \in G$$

Comparison: Graphs and linear Codes

	Graphs	linear Codes
Group Action	$S_n \wr 2^{\binom{n}{2}}$	$S_n \wr \left(\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times \mathbb{Z}_4^{*\,n} \right) \wr \mathbb{Z}_4^{(k_0,k_1)\times n} \right)$
Refinement	$f : 2^{\binom{n}{2}} \to X^n$ G-homomorphism for some appropriate $G \leq S_n$	$f : \left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times \mathbb{Z}_4^{*\,n} \right) \wr \mathbb{Z}_4^{(k_0,k_1)\times n} \to X^n$ G-homomorphism for some appropriate $G \leq S_n$

Homomorphism of group actions

Let G act on X, Y.
$f : X \to Y$ is a G-homomorphism if

$$f(gx) = gf(x), \ \forall\, x \in X, g \in G$$

Example: A refinement procedure for linear codes

Let

- $\Gamma \in \mathbb{Z}_4^{(k_0,k_1)\times n}$ be an ordered basis matrix, which generates a linear code C
- $C_i \leq {\mathbb{Z}_4}^n$ denote the punctured code of C in $i \in \{0,\ldots,n-1\}$
- $\mathrm{swe}(C) \in \mathbb{Z}[X_0, X_1, X_2]$ be the symmetrized weight enumerator of C (or any other invariant for equivalent codes)

Example: A refinement procedure for linear codes

Let

- $\Gamma \in \mathbb{Z}_4^{(k_0,k_1)\times n}$ be an ordered basis matrix, which generates a linear code C
- $C_i \leq \mathbb{Z}_4{}^n$ denote the punctured code of C in $i \in \{0, \ldots, n-1\}$
- $\mathrm{swe}(C) \in \mathbb{Z}[X_0, X_1, X_2]$ be the symmetrized weight enumerator of C (or any other invariant for equivalent codes)

Example: A refinement procedure for linear codes

Let

- $\Gamma \in \mathbb{Z}_4^{(k_0,k_1)\times n}$ be an ordered basis matrix, which generates a linear code C
- $C_i \leq \mathbb{Z}_4{}^n$ denote the punctured code of C in $i \in \{0, \ldots, n-1\}$
- $\mathrm{swe}(C) \in \mathbb{Z}[X_0, X_1, X_2]$ be the symmetrized weight enumerator of C (or any other invariant for equivalent codes)

Example: A refinement procedure for linear codes

Let

- $\Gamma \in \mathbb{Z}_4^{(k_0,k_1)\times n}$ be an ordered basis matrix, which generates a linear code C
- $C_i \leq \mathbb{Z}_4{}^n$ denote the punctured code of C in $i \in \{0, \dots, n-1\}$
- $\mathrm{swe}(C) \in \mathbb{Z}[X_0, X_1, X_2]$ be the symmetrized weight enumerator of C (or any other invariant for equivalent codes)

The function

$$f : \left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times \mathbb{Z}_4^{*\,n}\right) \backslash\!\backslash \mathbb{Z}_4^{(k_0,k_1)\times n} \to (\mathbb{Z}[X_0, X_1, X_2])^n$$
$$\Gamma \mapsto (\mathrm{swe}(C_0), \dots, \mathrm{swe}(C_{n-1}))$$

is an S_n-homomorphism.

Example

Code C generated by $\begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

swe(C_0)	$X_0^4 + 2X_0^3X_2 + 4X_0^2X_1^2 + 4X_0^2X_1X_2 + X_0^2X_2^2 + 4X_0X_1X_2^2$
swe(C_1)	$X_0^4 + 2X_0^3X_1 + 2X_0^3X_2 + 4X_0^2X_1X_2 + X_0^2X_2^2 + 4X_0X_1^2X_2 + 2X_0X_1X_2^2$
swe(C_2)	$X_0^4 + 2X_0^3X_1 + 2X_0^3X_2 + 4X_0^2X_1X_2 + X_0^2X_2^2 + 4X_0X_1^2X_2 + 2X_0X_1X_2^2$
swe(C_3)	$X_0^4 + 6X_0^2X_1^2 + 3X_0^2X_2^2 + 6X_0X_1^2X_2$

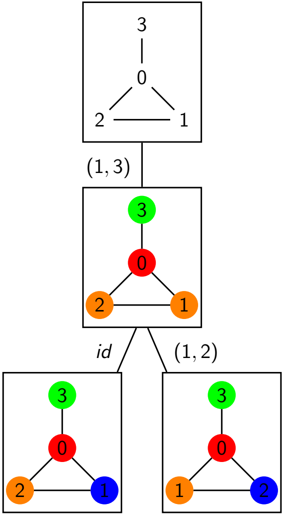
Example

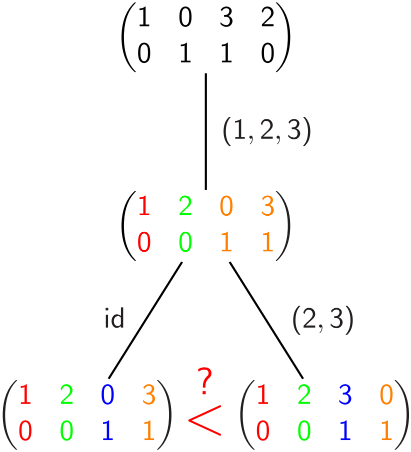
Code C generated by $\begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

swe(C_0)	$X_0^4 + 2X_0^3X_2 + 4X_0^2X_1^2 + 4X_0^2X_1X_2 + X_0^2X_2^2 + 4X_0X_1X_2^2$
swe(C_1)	$X_0^4 + 2X_0^3X_1 + 2X_0^3X_2 + 4X_0^2X_1X_2 + X_0^2X_2^2 + 4X_0X_1^2X_2 + 2X_0X_1X_2^2$
swe(C_2)	$X_0^4 + 2X_0^3X_1 + 2X_0^3X_2 + 4X_0^2X_1X_2 + X_0^2X_2^2 + 4X_0X_1^2X_2 + 2X_0X_1X_2^2$
swe(C_3)	$X_0^4 + 6X_0^2X_1^2 + 3X_0^2X_2^2 + 6X_0X_1^2X_2$

Suppose swe(C_0) $>$ swe(C_3) $>$ swe(C_1) $=$ swe(C_2)

Example


3
0
2
1
(1, 3)
3
0
2
1
id
(1, 2)
3
0
2
1
3
0
1
2


1 0 3 2
0 1 1 0
(1, 2, 3)
1 2 0 3
0 0 1 1
id
(2, 3)
1 2 0 3
0 0 1 1
?
<
1 2 3 0
0 0 1 1

Problem

Remember that the nodes of this tree represents orbits:

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

is a synonym for the orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n\right) \Gamma$$

Problem

Remember that the nodes of this tree represents orbits:

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

is a synonym for the orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n\right) \Gamma$$

Example continued

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

Problem

Remember that the nodes of this tree represents orbits:

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

is a synonym for the orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n\right) \Gamma$$

Example continued

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

Problem

Remember that the nodes of this tree represents orbits:

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

is a synonym for the orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n\right) \Gamma$$

Example continued

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

Problem

Remember that the nodes of this tree represents orbits:

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

is a synonym for the orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n\right) \Gamma$$

Example continued

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

Problem

Remember that the nodes of this tree represents orbits:

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

is a synonym for the orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n\right) \Gamma$$

Example continued

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

Problem

Remember that the nodes of this tree represents orbits:

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

is a synonym for the orbit

$$\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n\right) \Gamma$$

Solution:

A fast canonization algorithm for the calculation of orbit representatives in $\left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n\right) \Gamma$

Modifications of the group action

A common stabilizer

The group $\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)$ does not act faithfully (for $k_1 > 0$). There is a common stabilizer

$$\mathcal{N} := I_k + \left\{ \begin{pmatrix} 0 & 2B \end{pmatrix} \,\middle|\, B \in \mathbb{Z}_4^{k \times k_1} \right\}$$

Replacement of the group

Instead of $\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n$ use

$$\mathcal{G} := \left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)/\mathcal{N}\right) \times {\mathbb{Z}_4^*}^n$$

Modifications of the group action

A common stabilizer

The group $\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)$ does not act faithfully (for $k_1 > 0$). There is a common stabilizer

$$\mathcal{N} := I_k + \left\{ \begin{pmatrix} 0 & 2B \end{pmatrix} \middle| B \in \mathbb{Z}_4^{k \times k_1} \right\}$$

Replacement of the group

Instead of $\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4) \times {\mathbb{Z}_4^*}^n$ use

$$\mathcal{G} := \left(\mathrm{GL}_{(k_0,k_1)}(\mathbb{Z}_4)/\mathcal{N}\right) \times {\mathbb{Z}_4^*}^n$$

Modifications of the nodes of the backtrack tree

Let $(b_0, \ldots, b_{n-1})$ be the ordering of $\{0, \ldots, n-1\}$ in which the columns are fixed during the backtracking procedure.

i-semicanonical representatives

Represent the nodes $\pi\Gamma$ on level i by another orbit representative $\Gamma^{(i,\pi)}$ with:

$$\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)}) \leq \Pi_{(b_0,\ldots,b_{i-1})}(\widetilde{\Gamma}), \forall \widetilde{\Gamma} \in \mathcal{G}(\pi\Gamma)$$

Conclusion:

We only need a procedure to calculate $\Gamma^{(i+1,\pi)}$ or equivalently we must determine the stabilizer of $\Gamma^{(i,\pi)}$.

Modifications of the nodes of the backtrack tree

Let $(b_0, \ldots, b_{n-1})$ be the ordering of $\{0, \ldots, n-1\}$ in which the columns are fixed during the backtracking procedure.

i-semicanonical representatives

Represent the nodes $\pi\Gamma$ on level i by another orbit representative $\Gamma^{(i,\pi)}$ with:

$$\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)}) \leq \Pi_{(b_0,\ldots,b_{i-1})}(\widetilde{\Gamma}), \forall \widetilde{\Gamma} \in \mathcal{G}(\pi\Gamma)$$

Conclusion:

We only need a procedure to calculate $\Gamma^{(i+1,\pi)}$ or equivalently we must determine the stabilizer of $\Gamma^{(i,\pi)}$.

The inner group action

With the right choice of $(b_0, \dots, b_{i-1})$ we can guarantee

$$\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)}) =$$

$$\begin{pmatrix} \gamma_0 & * & \dots & * & * & & & & & & \\ 0 & \dots & 0 & \gamma_1 & * & \dots & * & & & & \\ & & & & & & & \ddots & & & \\ & & & & & & & & \gamma_{s-1} & * & \dots & * \\ 0 & & & & & \dots & & & & & 0 \end{pmatrix}$$

to be in *reduced row echelon form*:

- Pivot Elements in $\{1, 2\}$
- $\gamma_i = 2$ implies a row that is a multiple of 2
- the entries above the pivot elements are reduced modulo γ_i
- $\gamma_i = 2 \iff i \geq k_0$

The inner group action

With the right choice of $(b_0, \ldots, b_{i-1})$ we can guarantee

$$\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)}) =$$

$$\begin{pmatrix} \gamma_0 & * & \ldots & * & * & & & & & \\ 0 & \ldots & 0 & \gamma_1 & * & \ldots & * & & & \\ & & & & & & \ddots & & & \\ & & & & & & & \gamma_{s-1} & * & \ldots & * \\ 0 & & & & & \ldots & & & & & 0 \end{pmatrix}$$

to be in *reduced row echelon form*:

- Pivot Elements in $\{1, 2\}$
- $\gamma_i = 2$ implies a row that is a multiple of 2
- the entries above the pivot elements are reduced modulo γ_i
- $\gamma_i = 2 \iff i \geq k_0$

The inner group action

With the right choice of $(b_0, \dots, b_{i-1})$ we can guarantee

$$\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)}) =$$

$$\begin{pmatrix}
\gamma_0 & * & \dots & * & * & & & & & \\
0 & \dots & 0 & \gamma_1 & * & \dots & * & & & \\
 & & & & & & & \ddots & & \\
 & & & & & & & \gamma_{s-1} & * & \dots & * \\
0 & & & & & \dots & & & & & 0
\end{pmatrix}$$

to be in *reduced row echelon form*:

- Pivot Elements in $\{1, 2\}$
- $\gamma_i = 2$ implies a row that is a multiple of 2
- the entries above the pivot elements are reduced modulo γ_i
- $\gamma_i = 2 \iff i \geq k_0$

The inner group action

With the right choice of $(b_0, \ldots, b_{i-1})$ we can guarantee

$$\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)}) =$$

$$\begin{pmatrix} \gamma_0 & * & \ldots & * & * & & & & & \\ 0 & \ldots & 0 & \gamma_1 & * & \ldots & * & & & \\ & & & & & & \ddots & & & \\ & & & & & & & \gamma_{s-1} & * & \ldots & * \\ 0 & & & & \ldots & & & & & & 0 \end{pmatrix}$$

to be in *reduced row echelon form*:

- Pivot Elements in $\{1, 2\}$
- $\gamma_i = 2$ implies a row that is a multiple of 2
- the entries above the pivot elements are reduced modulo γ_i
- $\gamma_i = 2 \iff i \geq k_0$

The main observation

Let $(\overline{k}_0, \overline{k}_1)$ be the type of $\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)})$.
With the right choice of $(b_0, \dots, b_{i-1})$ we can guarantee, that

$$\left(\mathcal{G}_{(k_0,k_1)\times i}\right)_{\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)})}$$

is generated by

1. $\left(\begin{pmatrix} I_{\overline{k}} & B \\ & C \end{pmatrix}, 1^n\right), \overline{k} = \overline{k}_0 + \overline{k}_1$
2. $\left(\begin{pmatrix} A & 0 \\ & I_{k-\overline{k}} \end{pmatrix}, \varphi\right)$ with $(A, \varphi) \in \left(\mathcal{G}_{(\overline{k}_0,\overline{k}_1)\times i}\right)_{\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)})}$

The main observation

Let $(\overline{k}_0, \overline{k}_1)$ be the type of $\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)})$.
With the right choice of $(b_0, \ldots, b_{i-1})$ we can guarantee, that

$$\left(\mathcal{G}_{(k_0,k_1)\times i}\right)_{\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)})}$$

is generated by

1. $\left(\begin{pmatrix} I_{\overline{k}} & B \\ & C \end{pmatrix}, 1^n\right), \overline{k} = \overline{k}_0 + \overline{k}_1$
2. $\left(\begin{pmatrix} A & 0 \\ & I_{k-\overline{k}} \end{pmatrix}, \varphi\right)$ with $(A, \varphi) \in \left(\mathcal{G}_{(\overline{k}_0,\overline{k}_1)\times i}\right)_{\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)})}$

The main observation

But:

- $$\left(\mathcal{G}_{(\overline{k}_0,\overline{k}_1)\times i}\right)_{\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)})} \leq \mathbb{Z}_2^{\overline{k}_0+\overline{k}_0\overline{k}_1}$$

  is an *elementary abelian 2-group*:

  $$\begin{pmatrix} D & A \\ 0 & I_{\overline{k}_1} \end{pmatrix} \begin{pmatrix} E & B \\ 0 & I_{\overline{k}_1} \end{pmatrix} \mathcal{N} = \begin{pmatrix} DE & A+B \\ 0 & I_{\overline{k}_1} \end{pmatrix} \mathcal{N}$$

- It has at most $\overline{k}$ generators

Allows the implementation of a fast inner minimization algorithm!

The main observation

But:

- $$\left(\mathcal{G}_{(\overline{k}_0,\overline{k}_1)\times i}\right)_{\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)})} \leq \mathbb{Z}_2^{\overline{k}_0+\overline{k}_0\overline{k}_1}$$

  is an *elementary abelian 2-group*:

  $$\begin{pmatrix} D & A \\ 0 & I_{\overline{k}_1} \end{pmatrix} \begin{pmatrix} E & B \\ 0 & I_{\overline{k}_1} \end{pmatrix} \mathcal{N} = \begin{pmatrix} DE & A+B \\ 0 & I_{\overline{k}_1} \end{pmatrix} \mathcal{N}$$

- It has at most $\overline{k}$ generators

Allows the implementation of a fast inner minimization algorithm!

The main observation

But:

- $$\left(\mathcal{G}_{(\overline{k}_0,\overline{k}_1)\times i}\right)_{\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)})} \leq \mathbb{Z}_2^{\overline{k}_0+\overline{k}_0\overline{k}_1}$$

  is an *elementary abelian 2-group*:

  $$\begin{pmatrix} D & A \\ 0 & I_{\overline{k}_1} \end{pmatrix} \begin{pmatrix} E & B \\ 0 & I_{\overline{k}_1} \end{pmatrix} \mathcal{N} = \begin{pmatrix} DE & A+B \\ 0 & I_{\overline{k}_1} \end{pmatrix} \mathcal{N}$$

- It has at most $\overline{k}$ generators

Allows the implementation of a fast inner minimization algorithm!

The main observation

But:

- $$\left(\mathcal{G}_{(\overline{k}_0,\overline{k}_1)\times i}\right)_{\Pi_{(b_0,\ldots,b_{i-1})}(\Gamma^{(i,\pi)})} \leq \mathbb{Z}_2^{\overline{k}_0+\overline{k}_0\overline{k}_1}$$

  is an *elementary abelian 2-group*:

  $$\begin{pmatrix} D & A \\ 0 & I_{\overline{k}_1} \end{pmatrix}\begin{pmatrix} E & B \\ 0 & I_{\overline{k}_1} \end{pmatrix}\mathcal{N} = \begin{pmatrix} DE & A+B \\ 0 & I_{\overline{k}_1} \end{pmatrix}\mathcal{N}$$

- It has at most $\overline{k}$ generators

Allows the implementation of a fast inner minimization algorithm!

Codes over finite fields and free $\mathbb{Z}_4$-linear codes

$$\mathcal{G} = GL_k(R) \times {R^*}^n$$

$\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)})$ defines some unique partition $(p_0, \dots, p_{l-1})$ of $\{0, \dots, s-1\}$ such that

$$\left(\mathcal{G}_{(s,0)}\right)_{\Pi_{(b_0,\dots,b_{i-1})}(\Gamma^{(i,\pi)})}$$

is generated by

$$\left(\begin{pmatrix} d_0 & & \\ & \ddots & \\ & & d_{s-1} \end{pmatrix}, \varphi \right), \text{ with}$$

$$d_a = \mu \iff a \in p_j$$

$$\varphi_b = \mu^{-1} \iff \text{supp}^*(\Gamma_b) \subset p_j$$