A non-free $\mathbb{Z}_4$-linear code of high minimum Lee distance

Johannes Zwanzger

University of Bayreuth

Thurnau
April 12th, 2010

joint work with Michael Kiermaier

Properties of the code

Properties of the code

- Originally found by a heuristic computer search on good linear codes over finite chain rings, for results see:

Properties of the code

- Originally found by a heuristic computer search on good linear codes over finite chain rings, for results see:
  `http://www.mathe2.uni-bayreuth.de/20er/`

Properties of the code

- Originally found by a heuristic computer search on good linear codes over finite chain rings, for results see:
  `http://www.mathe2.uni-bayreuth.de/20er/`
- Gray image has parameters $[58, 2^7, 28]$, exceeding the linear upper bound of $d = 27$.

Properties of the code

- Originally found by a heuristic computer search on good linear codes over finite chain rings, for results see:
  `http://www.mathe2.uni-bayreuth.de/20er/`
- Gray image has parameters $[58, 2^7, 28]$, exceeding the linear upper bound of $d = 27$.
- Improves the known lower bound on the maximal size of binary block codes with $n = 58$ and $d = 28$ by 4 codewords (to our best knowledge).

Properties of the code

- Originally found by a heuristic computer search on good linear codes over finite chain rings, for results see:
  `http://www.mathe2.uni-bayreuth.de/20er/`
- Gray image has parameters $[58, 2^7, 28]$, exceeding the linear upper bound of $d = 27$.
- Improves the known lower bound on the maximal size of binary block codes with $n = 58$ and $d = 28$ by 4 codewords (to our best knowledge).
- Not free as $\mathbb{Z}_4$-module.

$\mathbb{Z}_4$-linear codes

$\mathbb{Z}_4$-linear codes

- C $\mathbb{Z}_4$-linear code of length n $:\Leftrightarrow$ C submodule of $\mathbb{Z}_4^n$

$\mathbb{Z}_4$-linear codes

- C $\mathbb{Z}_4$-linear code of length $n :\Leftrightarrow C$ submodule of $\mathbb{Z}_4^n$
- $\exists$ unique pair of non-negative integers (r_1, r_2) s. t.

$$C \cong \mathbb{Z}_4^{r_1} \oplus 2\mathbb{Z}_4^{r_2}$$

as $\mathbb{Z}_4$-module. (r_1, r_2) is the *shape* of C.

$\mathbb{Z}_4$-linear codes

- C $\mathbb{Z}_4$-linear code of length n :$\Leftrightarrow$ C submodule of $\mathbb{Z}_4^n$
- $\exists$ unique pair of non-negative integers (r_1, r_2) s. t.

$$C \cong \mathbb{Z}_4^{r_1} \oplus 2\mathbb{Z}_4^{r_2}$$

  as $\mathbb{Z}_4$-module. (r_1, r_2) is the *shape* of C.
- C is free as $\mathbb{Z}_4$-module iff $r_2 = 0$.

$\mathbb{Z}_4$-linear codes

- C $\mathbb{Z}_4$-linear code of length n $:\Leftrightarrow$ C submodule of $\mathbb{Z}_4^n$
- $\exists$ unique pair of non-negative integers (r_1, r_2) s. t.

$$C \cong \mathbb{Z}_4^{r_1} \oplus 2\mathbb{Z}_4^{r_2}$$

  as $\mathbb{Z}_4$-module. (r_1, r_2) is the *shape* of C.
- C is free as $\mathbb{Z}_4$-module iff $r_2 = 0$.
- $\mathbb{Z}_4^* = \{1, 3\}$: group of *units* of $\mathbb{Z}_4$.

$\mathbb{Z}_4$-linear codes

- C $\mathbb{Z}_4$-linear code of length n $:\Leftrightarrow$ C submodule of $\mathbb{Z}_4^n$
- $\exists$ unique pair of non-negative integers (r_1, r_2) s. t.

$$C \cong \mathbb{Z}_4^{r_1} \oplus 2\mathbb{Z}_4^{r_2}$$

  as $\mathbb{Z}_4$-module. (r_1, r_2) is the *shape* of C.
- C is free as $\mathbb{Z}_4$-module iff $r_2 = 0$.
- $\mathbb{Z}_4^* = \{1, 3\}$: group of *units* of $\mathbb{Z}_4$.
- $\mathrm{Rad}(\mathbb{Z}_4) = \mathbb{Z}_4 \setminus \mathbb{Z}_4^* = \{0, 2\}$: *radical* of $\mathbb{Z}_4$.

$\mathbb{Z}_4$-linear codes

- C $\mathbb{Z}_4$-linear code of length n $:\Leftrightarrow$ C submodule of $\mathbb{Z}_4^n$
- $\exists$ unique pair of non-negative integers (r_1, r_2) s. t.

$$C \cong \mathbb{Z}_4^{r_1} \oplus 2\mathbb{Z}_4^{r_2}$$

  as $\mathbb{Z}_4$-module. (r_1, r_2) is the *shape* of C.
- C is free as $\mathbb{Z}_4$-module iff $r_2 = 0$.
- $\mathbb{Z}_4^* = \{1, 3\}$: group of *units* of $\mathbb{Z}_4$.
- $\mathrm{Rad}(\mathbb{Z}_4) = \mathbb{Z}_4 \setminus \mathbb{Z}_4^* = \{0, 2\}$: *radical* of $\mathbb{Z}_4$.
- $S := \{0, 1\}$: set of representatives of $\mathbb{Z}_4/\mathrm{Rad}(\mathbb{Z}_4)$.

$\mathbb{Z}_4$-linear codes cont.

$\mathbb{Z}_4$-linear codes cont.

- $\Gamma \in \mathbb{Z}_4^{(r_1+r_2)\times n}$ *generator matrix* of C $:\Leftrightarrow$ rows of Γ generate C as $\mathbb{Z}_4$-module.

$\mathbb{Z}_4$-linear codes cont.

- $\Gamma \in \mathbb{Z}_4^{(r_1+r_2)\times n}$ *generator matrix* of C $:\Leftrightarrow$ rows of Γ generate C as $\mathbb{Z}_4$-module.
- r_1 rows of Γ contain at least one unit.

$\mathbb{Z}_4$-linear codes cont.

- $\Gamma \in \mathbb{Z}_4^{(r_1+r_2)\times n}$ *generator matrix* of C $:\Leftrightarrow$ rows of Γ generate C as $\mathbb{Z}_4$-module.
- r_1 rows of Γ contain at least one unit.
- r_2 rows have only entries from $\mathrm{Rad}(\mathbb{Z}_4)$ (w.l.o.g. the last r_2 rows).

$\mathbb{Z}_4$-linear codes cont.

- $\Gamma \in \mathbb{Z}_4^{(r_1+r_2)\times n}$ *generator matrix* of C :$\Leftrightarrow$ rows of Γ generate C as $\mathbb{Z}_4$-module.
- r_1 rows of Γ contain at least one unit.
- r_2 rows have only entries from $\mathrm{Rad}(\mathbb{Z}_4)$ (w.l.o.g. the last r_2 rows).
- $C = \{v^t\Gamma : v \in \mathbb{Z}_4^{r_1} \times S^{r_2}\}$.

$\mathbb{Z}_4$-linear codes cont.

- $\Gamma \in \mathbb{Z}_4^{(r_1+r_2)\times n}$ *generator matrix* of C :$\Leftrightarrow$ rows of Γ generate C as $\mathbb{Z}_4$-module.
- r_1 rows of Γ contain at least one unit.
- r_2 rows have only entries from $\mathrm{Rad}(\mathbb{Z}_4)$ (w.l.o.g. the last r_2 rows).
- $C = \{v^t\Gamma : v \in \mathbb{Z}_4^{r_1} \times S^{r_2}\}$.
- v from above is uniquely determined by $c = v^t\Gamma$ and called *information vector* of c.

Lee weight and Lee metric

Lee weight and Lee metric

- $$w_{\mathrm{Lee}} : \mathbb{Z}_4 \to \mathbb{N}, \qquad \begin{cases} 0 & \mapsto 0 \\ 1,3 & \mapsto 1 \\ 2 & \mapsto 2 \end{cases}$$

  is the *Lee weight* on $\mathbb{Z}_4$ and extendable to $\mathbb{Z}_4^n$ by componentwise addition.

Lee weight and Lee metric

- $$w_{\mathrm{Lee}} : \mathbb{Z}_4 \to \mathbb{N}, \quad \begin{cases} 0 & \mapsto 0 \\ 1,3 & \mapsto 1 \\ 2 & \mapsto 2 \end{cases}$$

  is the *Lee weight* on $\mathbb{Z}_4$ and extendable to $\mathbb{Z}_4^n$ by componentwise addition.
- $d_{\mathrm{Lee}}(c, c') := w_{\mathrm{Lee}}(c - c')$, the *Lee metric* on $\mathbb{Z}_4^n$.

Lee weight and Lee metric

- $$w_{\mathrm{Lee}} : \mathbb{Z}_4 \to \mathbb{N}, \quad \begin{cases} 0 & \mapsto 0 \\ 1,3 & \mapsto 1 \\ 2 & \mapsto 2 \end{cases}$$

  is the *Lee weight* on $\mathbb{Z}_4$ and extendable to $\mathbb{Z}_4^n$ by componentwise addition.
- $d_{\mathrm{Lee}}(c, c') := w_{\mathrm{Lee}}(c - c')$, the *Lee metric* on $\mathbb{Z}_4^n$.

Lee weight and Lee metric

- $w_{\mathrm{Lee}} : \mathbb{Z}_4 \to \mathbb{N}, \quad \begin{cases} 0 & \mapsto 0 \\ 1,3 & \mapsto 1 \\ 2 & \mapsto 2 \end{cases}$

  is the *Lee weight* on $\mathbb{Z}_4$ and extendable to $\mathbb{Z}_4^n$ by componentwise addition.
- $d_{\mathrm{Lee}}(c, c') := w_{\mathrm{Lee}}(c - c')$, the *Lee metric* on $\mathbb{Z}_4^n$.
- *Minimum Lee distance* of C:

$$d_{\min}(C) := \min\{d_{\mathrm{Lee}}(c, c') : c \neq c' \in C\}.$$

Lee weight and Lee metric

- $$w_{\mathrm{Lee}} : \mathbb{Z}_4 \to \mathbb{N}, \quad \begin{cases} 0 & \mapsto 0 \\ 1,3 & \mapsto 1 \\ 2 & \mapsto 2 \end{cases}$$

  is the *Lee weight* on $\mathbb{Z}_4$ and extendable to $\mathbb{Z}_4^n$ by componentwise addition.
- $d_{\mathrm{Lee}}(c, c') := w_{\mathrm{Lee}}(c - c')$, the *Lee metric* on $\mathbb{Z}_4^n$.
- *Minimum Lee distance* of C:

  $$d_{\min}(C) := \min\{d_{\mathrm{Lee}}(c, c') : c \neq c' \in C\}.$$
- Due to linearity:

  $$d_{\min}(C) = \min\{w_{\mathrm{Lee}}(c) : 0 \neq c \in C\}.$$

Transformation into a binary code

Transformation into a binary code

- $\gamma : \mathbb{Z}_4 \to \mathbb{F}_2^2, \quad \begin{cases} 0 & \mapsto 00 \\ 1 & \mapsto 01 \\ 2 & \mapsto 11 \\ 3 & \mapsto 10 \end{cases}$

  is an isometry between $(\mathbb{Z}_4, d_{\mathsf{Lee}})$ and $(\mathbb{F}_2^2, d_{\mathsf{Ham}})$, the *Gray map*.

Transformation into a binary code

- $\gamma : \mathbb{Z}_4 \to \mathbb{F}_2^2, \quad \begin{cases} 0 & \mapsto 00 \\ 1 & \mapsto 01 \\ 2 & \mapsto 11 \\ 3 & \mapsto 10 \end{cases}$

  is an isometry between $(\mathbb{Z}_4, d_{\mathrm{Lee}})$ and $(\mathbb{F}_2^2, d_{\mathrm{Ham}})$, the *Gray map*.
- Again, we extend it to $\gamma : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$.

Transformation into a binary code

- $\gamma : \mathbb{Z}_4 \to \mathbb{F}_2^2$, $\begin{cases} 0 & \mapsto 00 \\ 1 & \mapsto 01 \\ 2 & \mapsto 11 \\ 3 & \mapsto 10 \end{cases}$

  is an isometry between $(\mathbb{Z}_4, d_{\mathsf{Lee}})$ and $(\mathbb{F}_2^2, d_{\mathsf{Ham}})$, the *Gray map*.
- Again, we extend it to $\gamma : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$.
- γ transforms any block code $C \subset \mathbb{Z}_4^n$ into a binary code of same size and weights and double length.

Transformation into a binary code

- $\gamma : \mathbb{Z}_4 \to \mathbb{F}_2^2$, $\begin{cases} 0 & \mapsto 00 \\ 1 & \mapsto 01 \\ 2 & \mapsto 11 \\ 3 & \mapsto 10 \end{cases}$

  is an isometry between $(\mathbb{Z}_4, d_{\mathsf{Lee}})$ and $(\mathbb{F}_2^2, d_{\mathsf{Ham}})$, the *Gray map*.
- Again, we extend it to $\gamma : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$.
- γ transforms any block code $C \subset \mathbb{Z}_4^n$ into a binary code of same size and weights and double length.
- $\mathbb{Z}_4$-linearity of C usually does not lead to $\mathbb{F}_2$-linearity of $\gamma(C)$.

The projective Hjelmslev plane

The projective Hjelmslev plane

- $\mathcal{P} :=$ set of all free submodules of $\mathbb{Z}_4^3$ of rank one.

The projective Hjelmslev plane

- $\mathcal{P} :=$ set of all free submodules of $\mathbb{Z}_4^3$ of rank one.
- $\mathcal{L} :=$ set of all free submodules of $\mathbb{Z}_4^3$ of rank two.

The projective Hjelmslev plane

- $\mathcal{P} :=$ set of all free submodules of $\mathbb{Z}_4^3$ of rank one.
- $\mathcal{L} :=$ set of all free submodules of $\mathbb{Z}_4^3$ of rank two.
- Let $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$ the subset relation. The geometry

$$\mathsf{PHG}(2, \mathbb{Z}_4) := (\mathcal{P}, \mathcal{L}, \mathcal{I})$$

is called the *projective Hjelmslev plane*.

The projective Hjelmslev plane

- $\mathcal{P} :=$ set of all free submodules of $\mathbb{Z}_4^3$ of rank one.
- $\mathcal{L} :=$ set of all free submodules of $\mathbb{Z}_4^3$ of rank two.
- Let $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$ the subset relation. The geometry

$$\mathrm{PHG}(2, \mathbb{Z}_4) := (\mathcal{P}, \mathcal{L}, \mathcal{I})$$

  is called the *projective Hjelmslev plane*.
- $p_1, p_2 \in \mathcal{P}$ are *neighbors* $:\Leftrightarrow$ there are two distinct lines incident with p_1 and p_2.

Projective Hjelmslev plane cont.

Projective Hjelmslev plane cont.

- Neighbor relation is equivalence relation,
  $\mathcal{N}$:= set of *neighbor classes*.

Projective Hjelmslev plane cont.

- Neighbor relation is equivalence relation, $\mathcal{N} :=$ set of *neighbor classes*.
- $p \in \mathcal{P}$ and $l \in \mathcal{L}$ are *neighbors* $:\Leftrightarrow$ l contains a neighbor of p.

Projective Hjelmslev plane cont.

- Neighbor relation is equivalence relation, $\mathcal{N}$:= set of *neighbor classes*.
- $p \in \mathcal{P}$ and $l \in \mathcal{L}$ are *neighbors* $:\Leftrightarrow$ l contains a neighbor of p.
- If $p = \mathbb{Z}_4 v$ for $p \in \mathcal{P}$, $v \in \mathbb{Z}_4^3$ is called *coordinate vector* of p.

Projective Hjelmslev plane cont.

- Neighbor relation is equivalence relation, $\mathcal{N}$:= set of *neighbor classes*.
- $p \in \mathcal{P}$ and $l \in \mathcal{L}$ are *neighbors* $:\Leftrightarrow$ l contains a neighbor of p.
- If $p = \mathbb{Z}_4 v$ for $p \in \mathcal{P}$, $v \in \mathbb{Z}_4^3$ is called *coordinate vector* of p.
- For each point exist two different coordinate vectors.

Projective Hjelmslev plane cont.

- Neighbor relation is equivalence relation, $\mathcal{N} :=$ set of *neighbor classes*.
- $p \in \mathcal{P}$ and $l \in \mathcal{L}$ are *neighbors* $:\Leftrightarrow$ l contains a neighbor of p.
- If $p = \mathbb{Z}_4 v$ for $p \in \mathcal{P}$, $v \in \mathbb{Z}_4^3$ is called *coordinate vector* of p.
- For each point exist two different coordinate vectors.
- The *canonical* one has as first unit a symbol 1 and is denoted by $\kappa(p)$.

Projective Hjelmslev plane cont.

Projective Hjelmslev plane cont.

- For vectors $u = (u_1, u_2, u_3)^t, v = (v_1, v_2, v_3)^t \in \mathbb{Z}_4^3$, the *inner product* is

$$\langle u, v \rangle := u_1 v_1 + u_2 v_2 + u_3 v_3.$$

Projective Hjelmslev plane cont.

- For vectors $u = (u_1, u_2, u_3)^t, v = (v_1, v_2, v_3)^t \in \mathbb{Z}_4^3$, the *inner product* is

$$\langle u, v \rangle := u_1 v_1 + u_2 v_2 + u_3 v_3.$$

- The *orthogonal* module of $S \leq \mathbb{Z}_4^3$ is

$$S^\perp := \{u \in \mathbb{Z}_4^3 : \langle u, v \rangle = 0 \text{ for all } v \in S\}.$$

Projective Hjelmslev plane cont.

- For vectors $u = (u_1, u_2, u_3)^t, v = (v_1, v_2, v_3)^t \in \mathbb{Z}_4^3$, the *inner product* is

$$\langle u, v \rangle := u_1 v_1 + u_2 v_2 + u_3 v_3.$$

- The *orthogonal* module of $S \leq \mathbb{Z}_4^3$ is

$$S^\perp := \{u \in \mathbb{Z}_4^3 : \langle u, v \rangle = 0 \text{ for all } v \in S\}.$$

- The orthogonal of a point is a line and vice versa: $\mathcal{L} = \{p^\perp : p \in \mathcal{P}\}$ and $\mathcal{P} = \{l^\perp : l \in \mathcal{L}\}$.

Projective Hjelmslev plane cont.

- For vectors $u = (u_1, u_2, u_3)^t, v = (v_1, v_2, v_3)^t \in \mathbb{Z}_4^3$, the *inner product* is

$$\langle u, v \rangle := u_1 v_1 + u_2 v_2 + u_3 v_3.$$

- The *orthogonal* module of $S \leq \mathbb{Z}_4^3$ is

$$S^\perp := \{u \in \mathbb{Z}_4^3 : \langle u, v \rangle = 0 \text{ for all } v \in S\}.$$

- The orthogonal of a point is a line and vice versa: $\mathcal{L} = \{p^\perp : p \in \mathcal{P}\}$ and $\mathcal{P} = \{l^\perp : l \in \mathcal{L}\}$.
- For $p \in \mathcal{P}$, $l \in \mathcal{L}$: ${p^\perp}^\perp = p$, ${l^\perp}^\perp = l$.

Projective Hjelmslev plane cont.

Projective Hjelmslev plane cont.

- Let $l = p^{\perp}$ and v a coordinate vector of p. Then v is also called a *coordinate vector* of l.

Projective Hjelmslev plane cont.

- Let $l = p^\perp$ and v a coordinate vector of p. Then v is also called a *coordinate vector* of l.
- Let $p_1 = \mathbb{Z}_4 v_1$, $p_2 = \mathbb{Z}_4 v_2$ and $l = (\mathbb{Z}_4 u)^\perp$.

Projective Hjelmslev plane cont.

- Let $l = p^\perp$ and v a coordinate vector of p. Then v is also called a *coordinate vector* of l.
- Let $p_1 = \mathbb{Z}_4 v_1$, $p_2 = \mathbb{Z}_4 v_2$ and $l = (\mathbb{Z}_4 u)^\perp$.

  p_1 and p_2 are neighbors $\Leftrightarrow 2(v_1 - v_2) = 0$.

Projective Hjelmslev plane cont.

- Let $l = p^\perp$ and v a coordinate vector of p. Then v is also called a *coordinate vector* of l.
- Let $p_1 = \mathbb{Z}_4 v_1,\ p_2 = \mathbb{Z}_4 v_2$ and $l = (\mathbb{Z}_4 u)^\perp$.

  p_1 and p_2 are neighbors $\Leftrightarrow 2(v_1 - v_2) = 0$.
  p_i is incident with $l \Leftrightarrow \langle u, v_i \rangle = 0$.

Projective Hjelmslev plane cont.

- Let $l = p^\perp$ and v a coordinate vector of p. Then v is also called a *coordinate vector* of l.
- Let $p_1 = \mathbb{Z}_4 v_1,\ p_2 = \mathbb{Z}_4 v_2$ and $l = (\mathbb{Z}_4 u)^\perp$.

  p_1 and p_2 are neighbors $\Leftrightarrow 2(v_1 - v_2) = 0$.
  p_i is incident with $l \Leftrightarrow \langle u, v_i \rangle = 0$.
  p_i and l are neighbors $\Leftrightarrow \langle u, v_i \rangle \in \mathrm{Rad}(\mathbb{Z}_4)$.

Some numbers

Some numbers

- $|\mathcal{P}| = |\mathcal{L}| = 28.$

Some numbers

- $|\mathcal{P}| = |\mathcal{L}| = 28$.
- Each line contains 6 points, any point is incident with 6 lines.

Some numbers

- $|\mathcal{P}| = |\mathcal{L}| = 28$.
- Each line contains 6 points, any point is incident with 6 lines.
- $\#\mathcal{N} = 7$.

Some numbers

- $|\mathcal{P}| = |\mathcal{L}| = 28$.
- Each line contains 6 points, any point is incident with 6 lines.
- $\#\mathcal{N} = 7$.
- Each neighbor class consists of 4 points.

Some numbers

- $|\mathcal{P}| = |\mathcal{L}| = 28$.
- Each line contains 6 points, any point is incident with 6 lines.
- $\#\mathcal{N} = 7$.
- Each neighbor class consists of 4 points.
- Any line intersects 3 different neighbor classes, each in 2 points.

Hyperovals

Hyperovals

- $\mathcal{O} \subset \mathcal{P}$ is called a *hyperoval* in $\mathrm{PHG}(2, \mathbb{Z}_4)$ iff:

Hyperovals

- $\mathcal{O} \subset \mathcal{P}$ is called a *hyperoval* in $\mathrm{PHG}(2, \mathbb{Z}_4)$ iff:
  - $\#\mathcal{O} = 7$.

Hyperovals

- $\mathcal{O} \subset \mathcal{P}$ is called a *hyperoval* in $\mathrm{PHG}(2, \mathbb{Z}_4)$ iff:
  - $\#\mathcal{O} = 7$.
  - Each line intersects $\mathcal{O}$ in at most two points.

Hyperovals

- $\mathcal{O} \subset \mathcal{P}$ is called a *hyperoval* in $\mathrm{PHG}(2, \mathbb{Z}_4)$ iff:
  - $\#\mathcal{O} = 7$.
  - Each line intersects $\mathcal{O}$ in at most two points.
- Such hyperovals exist!

Hyperovals

- $\mathcal{O} \subset \mathcal{P}$ is called a *hyperoval* in $\mathrm{PHG}(2, \mathbb{Z}_4)$ iff:
  - $\#\mathcal{O} = 7$.
  - Each line intersects $\mathcal{O}$ in at most two points.
- Such hyperovals exist!

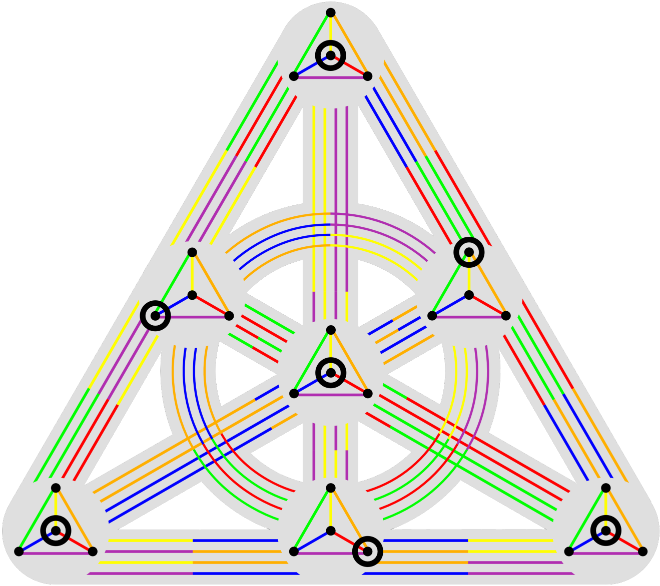
Lemma

Let $\mathcal{O}$ be a hyperoval in $\mathrm{PHG}(2, \mathbb{Z}_4)$. Then:

- *Each line meets $\mathcal{O}$ in zero or two points. This happens for 7 and 21 lines, respectively.*
- *From each neighbor class there is exactly one point in $\mathcal{O}$.*

Maybe a picture says more than 8 slides...

Maybe a picture says more than 8 slides...



Construction of the new code

Construction of the new code

- Let $\mathcal{O}$ be a hyperoval in $\mathrm{PHG}(2, \mathbb{Z}_4)$ and

$$\mu : \mathcal{P} \to \mathrm{Rad}(\mathbb{Z}_4), \quad p \mapsto \begin{cases} 0 & \text{if } p \in \mathcal{O} \\ 2 & \text{otherwise} \end{cases}$$

Construction of the new code

- Let $\mathcal{O}$ be a hyperoval in $\mathrm{PHG}(2, \mathbb{Z}_4)$ and

$$\mu : \mathcal{P} \to \mathrm{Rad}(\mathbb{Z}_4), \quad p \mapsto \begin{cases} 0 & \text{if } p \in \mathcal{O} \\ 2 & \text{otherwise} \end{cases}$$

- For a point $p \in \mathcal{P}$ we define a vector

$$v_p = \begin{pmatrix} \kappa(p) \\ \mu(p) \end{pmatrix} \in \mathbb{Z}_4^3 \times \mathrm{Rad}(\mathbb{Z}_4).$$

Construction cont.

Construction cont.

Lemma

Let $\mathcal{P} = \{p_0, \ldots, p_{27}\}$, $\Gamma := (v_{p_0}, \ldots, v_{p_{27}}) \in \mathbb{Z}_4^{(3+1)\times 28}$ *and* C *the code generated by* Γ. *Then:*

$$\mathrm{Lee}_C = 1 + 49X^{26} + 56X^{28} + 7X^{32} + 14X^{34} + X^{42}$$

and the subcode $(\mathbb{Z}_4^3 \times \{0\})\Gamma$ *contains exactly the codewords of Lee weight* 0, 28 *and* 32.

Main result:

Main result:

Corollary

Let $\delta := (0\ 0\ 0\ 2)^t \in \mathbb{Z}_4^4$ *and* $\hat{\Gamma} := (\Gamma|\delta) \in \mathbb{Z}_4^{(3+1)\times 29}$*. For the code* $\hat{C}$ *generated by* $\hat{\Gamma}$ *holds*

$$\mathrm{Lee}_{\hat{C}} = 1 + 105X^{28} + 7X^{32} + 14X^{36} + X^{44}.$$

Main result:

Corollary

Let $\delta := (0\ 0\ 0\ 2)^t \in \mathbb{Z}_4^4$ *and* $\hat{\Gamma} := (\Gamma|\delta) \in \mathbb{Z}_4^{(3+1)\times 29}$. *For the code* $\hat{C}$ *generated by* $\hat{\Gamma}$ *holds*

$$\mathrm{Lee}_{\hat{C}} = 1 + 105X^{28} + 7X^{32} + 14X^{36} + X^{44}.$$

Remark

Claim does not depend on $\mathcal{O}$ *and* $\kappa(-)$. *For example,*

$$\hat{\Gamma} := \begin{pmatrix} 0022\ 0022\ 1111\ 1111\ 0022\ 1111\ 1111\ 0 \\ 0202\ 1111\ 0022\ 1133\ 1111\ 0022\ 1133\ 0 \\ 1111\ 0202\ 0202\ 1313\ 1313\ 1313\ 0202\ 0 \\ 0222\ 0222\ 0222\ 2022\ 2202\ 2202\ 2220\ 2 \end{pmatrix}$$

Proof of the lemma

Proof of the lemma

Any $c \in C$ can uniquely be written as $c = (u^t, s)^t \Gamma$. We distinguish a few cases for u and s:

Proof of the lemma

Any $c \in C$ can uniquely be written as $c = (u^t, s)^t \Gamma$. We distinguish a few cases for u and s:

1. $s = 0$:

Proof of the lemma

Any $c \in C$ can uniquely be written as $c = (u^t, s)^t \Gamma$. We distinguish a few cases for u and s:

1. $s = 0$:

- If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$:

$\langle u, \kappa(p_i) \rangle$	0	2	1 or 3
#	6 times	6 times	16 times

Proof of the lemma

Any $c \in C$ can uniquely be written as $c = (u^t, s)^t \Gamma$. We distinguish a few cases for u and s:

1. $s = 0$:

- If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$:

$\langle u, \kappa(p_i) \rangle$	0	2	1 or 3
#	6 times	6 times	16 times

$\rightsquigarrow$ 56 codewords of Lee weight $6 \cdot 2 + 16 \cdot 1 = 28$.

Proof of the lemma

Any $c \in C$ can uniquely be written as $c = (u^t, s)^t \Gamma$. We distinguish a few cases for u and s:

1. $s = 0$:

- If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$:

$\langle u, \kappa(p_i) \rangle$	0	2	1 or 3
#	6 times	6 times	16 times

  $\rightsquigarrow$ 56 codewords of Lee weight $6 \cdot 2 + 16 \cdot 1 = 28$.

- If $2u = 0$: $u = 0$ yields the zero codeword. Otherwise, choose u' with $u = 2u'$. Use $\langle u, p_i \rangle = 2\langle u', p_i \rangle$ and the table above.

Proof of the lemma

Any $c \in C$ can uniquely be written as $c = (u^t, s)^t \Gamma$. We distinguish a few cases for u and s:

1. $s = 0$:

- If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$:

$\langle u, \kappa(p_i) \rangle$	0	2	1 or 3
#	6 times	6 times	16 times

  $\rightsquigarrow$ 56 codewords of Lee weight $6 \cdot 2 + 16 \cdot 1 = 28$.
- If $2u = 0$: $u = 0$ yields the zero codeword. Otherwise, choose u' with $u = 2u'$. Use $\langle u, p_i \rangle = 2\langle u', p_i \rangle$ and the table above.
  $\rightsquigarrow$ 7 codewords of Lee weight $16 \cdot 2 = 32$ and one of weight zero.

Proof cont.

Proof cont.

2. $s = 1$:

Proof cont.

2. $s = 1$:
   - If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$.

Proof cont.

2. $s = 1$:
   - If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$.
     - If $l \cap \mathcal{O} = \emptyset$:

$\langle u, \kappa(p_i) \rangle$	0		2		1 or 3	
$\mu(p_i)$	0	2	0	2	0	2
$\#$	$0\times$	$6\times$	$3\times$	$3\times$	$4\times$	$12\times$

Proof cont.

2. $s = 1$:
   - If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$.
     - If $l \cap \mathcal{O} = \emptyset$:

$\langle u, \kappa(p_i) \rangle$	0		2		1 or 3	
$\mu(p_i)$	0	2	0	2	0	2
#	$0\times$	$6\times$	$3\times$	$3\times$	$4\times$	$12\times$

$\rightsquigarrow$ 14 codewords of Lee weight $9 \cdot 2 + 16 \cdot 1 = 34$.

Proof cont.

2. $s = 1$:

- If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$.
  - If $l \cap \mathcal{O} = \emptyset$:

$\langle u, \kappa(p_i)\rangle$	0		2		1 or 3	
$\mu(p_i)$	0	2	0	2	0	2
#	$0\times$	$6\times$	$3\times$	$3\times$	$4\times$	$12\times$

$\rightsquigarrow$ 14 codewords of Lee weight $9 \cdot 2 + 16 \cdot 1 = 34$.

  - If $\#(l \cap \mathcal{O}) = 2$:

$\langle u, \kappa(p_i)\rangle$	0		2		1 or 3	
$\mu(p_i)$	0	2	0	2	0	2
#	$2\times$	$4\times$	$1\times$	$5\times$	$4\times$	$12\times$

Proof cont.

2. $s = 1$:
   - If $2u \neq 0$, consider $l := \mathbb{Z}_4 u^\perp \in \mathrm{PHG}(2, \mathbb{Z}_4)$.
     - If $l \cap \mathcal{O} = \emptyset$:

$\langle u, \kappa(p_i) \rangle$	0		2		1 or 3	
$\mu(p_i)$	0	2	0	2	0	2
#	0×	6×	3×	3×	4×	12×

$\rightsquigarrow$ 14 codewords of Lee weight $9 \cdot 2 + 16 \cdot 1 = 34$.

     - If $\#(l \cap \mathcal{O}) = 2$:

$\langle u, \kappa(p_i) \rangle$	0		2		1 or 3	
$\mu(p_i)$	0	2	0	2	0	2
#	2×	4×	1×	5×	4×	12×

$\rightsquigarrow$ 42 codewords of Lee weight $5 \cdot 2 + 16 \cdot 1 = 26$.

Proof cont.

Proof cont.

Continuation for $s = 1$:

Proof cont.

Continuation for $s = 1$:

- If $2u = 0$: $u = 0$ yields the last row of Γ. Otherwise:

$\langle u, \kappa(p_i) \rangle$	0		2	
$\mu(p_i)$	0	2	0	2
$\#$	$3\times$	$9\times$	$4\times$	$12\times$

Proof cont.

Continuation for $s = 1$:

- If $2u = 0$: $u = 0$ yields the last row of Γ. Otherwise:

$\langle u, \kappa(p_i)\rangle$	0		2	
$\mu(p_i)$	0	2	0	2
#	$3\times$	$9\times$	$4\times$	$12\times$

$\rightsquigarrow$ 7 codewords of Lee weight $13 \cdot 2 = 26$ and one of weight 42.

Proof cont.

Continuation for $s = 1$:

- If $2u = 0$: $u = 0$ yields the last row of Γ. Otherwise:

$\langle u, \kappa(p_i)\rangle$	0		2	
$\mu(p_i)$	0	2	0	2
$\#$	$3\times$	$9\times$	$4\times$	$12\times$

$\rightsquigarrow$ 7 codewords of Lee weight $13 \cdot 2 = 26$ and one of weight 42.

$\square$

Questions to the audience

Questions to the audience

- Are there more examples of **non-free** $\mathbb{Z}_4$-linear codes where the minimum distance of the Gray image exceeds the linear upper bound?

Questions to the audience

- Are there more examples of **non-free** $\mathbb{Z}_4$-linear codes where the minimum distance of the Gray image exceeds the linear upper bound?
- Is $A(58, 28) \geq 128$ for binary block codes already known?

Questions to the audience

- Are there more examples of **non-free** $\mathbb{Z}_4$-linear codes where the minimum distance of the Gray image exceeds the linear upper bound?
- Is $A(58, 28) \geq 128$ for binary block codes already known?

Thanks for your attention!