Heuristic Construction of Linear Codes over Finite Chain Rings with High Minimum Homogeneous Weight

Johannes Zwanzger

University of Bayreuth

Magdeburg
November 13th, 2009

Motivation

Motivation

- 1967: Nordstrom and Robinson find nonlinear binary $[16, 2^8, 6]$-code (linear: minimum distance ≤ 5)

Motivation

- 1967: Nordstrom and Robinson find nonlinear binary $[16, 2^8, 6]$-code (linear: minimum distance ≤ 5)
- Preparata & Kerdock construct infinite series of such codes including the NR-code.

Motivation

- 1967: Nordstrom and Robinson find nonlinear binary $[16, 2^8, 6]$-code (linear: minimum distance ≤ 5)
- Preparata & Kerdock construct infinite series of such codes including the NR-code.
- Nechaev 1989, Hammons et al. 1994: K. & P.-codes are the Gray image of $\mathbb{Z}_4$-linear codes

Motivation

- 1967: Nordstrom and Robinson find nonlinear binary $[16, 2^8, 6]$-code (linear: minimum distance ≤ 5)
- Preparata & Kerdock construct infinite series of such codes including the NR-code.
- Nechaev 1989, Hammons et al. 1994: K. & P.-codes are the Gray image of $\mathbb{Z}_4$-linear codes

Questions: Are there more examples? What about other rings?

Finite chain rings

Finite chain rings

Definition

A finite chain ring R is a finite ring with unity whose left ideals form a chain $R = I_0 \supsetneq I_1 \cdots \supsetneq I_m = \{0\}$. m is called the *chain length* of R.

Finite chain rings

Definition

A finite chain ring R is a finite ring with unity whose left ideals form a chain $R = I_0 \supsetneq I_1 \cdots \supsetneq I_m = \{0\}$. m is called the *chain length* of R.

- $\exists q : R/I_1 \cong \mathbb{F}_q$.

Finite chain rings

Definition

A finite chain ring R is a finite ring with unity whose left ideals form a chain $R = I_0 \supsetneq I_1 \cdots \supsetneq I_m = \{0\}$. m is called the *chain length* of R.

- $\exists q : R/I_1 \cong \mathbb{F}_q$.
- R, m and q will keep their meaning throughout this talk.

Finite chain rings

Definition

A finite chain ring R is a finite ring with unity whose left ideals form a chain $R = I_0 \supsetneq I_1 \cdots \supsetneq I_m = \{0\}$. m is called the *chain length* of R.

- $\exists q : R/I_1 \cong \mathbb{F}_q$.
- R, m and q will keep their meaning throughout this talk.

Example

$R := \mathbb{Z}_{p^n}$, with p a prime ($m = n$, $q = p$).

Linear codes over finite chain rings

Linear codes over finite chain rings

Linear code over R of length n: submodule of ${}_RR^n$ (row convention).

Linear codes over finite chain rings

Linear code over R of length n: submodule of ${}_R R^n$ (row convention).

Example

Linear codes over finite chain rings

Linear code over R of length n: submodule of ${}_R R^n$ (row convention).

Example

$R := \mathbb{Z}_8 \Rightarrow$

Linear codes over finite chain rings

Linear code over R of length n: submodule of ${}_R R^n$ (row convention).

Example

$R := \mathbb{Z}_8 \Rightarrow I_0 = \mathbb{Z}_8, I_1 = \{0, 2, 4, 6\}, I_2 = \{0, 4\}, I_3 = \{0\}$

Linear codes over finite chain rings

Linear code over R of length n: submodule of ${}_R R^n$ (row convention).

Example

$R := \mathbb{Z}_8 \Rightarrow I_0 = \mathbb{Z}_8, I_1 = \{0, 2, 4, 6\}, I_2 = \{0, 4\}, I_3 = \{0\}$

$$\Gamma = \left(\begin{array}{ccc|cc} 1 & 1 & 0 & 2 & 7 \\ 0 & 2 & 2 & 0 & 6 \\ 0 & 0 & 4 & 4 & 0 \end{array}\right)$$

Linear codes over finite chain rings

Linear code over R of length n: submodule of ${}_R R^n$ (row convention).

Example

$R := \mathbb{Z}_8 \Rightarrow I_0 = \mathbb{Z}_8, I_1 = \{0, 2, 4, 6\}, I_2 = \{0, 4\}, I_3 = \{0\}$

$$\Gamma = \left(\begin{array}{ccc|cc} 1 & 1 & 0 & 2 & 7 \\ 0 & 2 & 2 & 0 & 6 \\ 0 & 0 & 4 & 4 & 0 \end{array}\right)$$

- C_Γ has *shape* $(3, 2, 1)$.

Linear codes over finite chain rings

Linear code over R of length n: submodule of ${}_R R^n$ (row convention).

Example

$R := \mathbb{Z}_8 \Rightarrow I_0 = \mathbb{Z}_8, I_1 = \{0,2,4,6\}, I_2 = \{0,4\}, I_3 = \{0\}$

$$\Gamma = \left(\begin{array}{ccc|cc} 1 & 1 & 0 & 2 & 7 \\ 0 & 2 & 2 & 0 & 6 \\ 0 & 0 & 4 & 4 & 0 \end{array}\right)$$

- C_Γ has *shape* $(3,2,1)$.
- $R_0 = \mathbb{Z}_8,\ R_1 = \{0,1,2,3\},\ R_2 = \{0,1\} \Rightarrow$

Linear codes over finite chain rings

Linear code over R of length n: submodule of ${}_R R^n$ (row convention).

Example

$R := \mathbb{Z}_8 \Rightarrow I_0 = \mathbb{Z}_8, I_1 = \{0, 2, 4, 6\}, I_2 = \{0, 4\}, I_3 = \{0\}$

$$\Gamma = \left(\begin{array}{ccc|cc} 1 & 1 & 0 & 2 & 7 \\ 0 & 2 & 2 & 0 & 6 \\ 0 & 0 & 4 & 4 & 0 \end{array} \right)$$

- C_Γ has *shape* $(3, 2, 1)$.
- $R_0 = \mathbb{Z}_8,\ R_1 = \{0, 1, 2, 3\},\ R_2 = \{0, 1\} \Rightarrow$
  $C_\Gamma = \{u\Gamma : u \in R_0 \times R_1 \times R_2\}$

The homogeneous weight

The homogeneous weight

Definition

The homogeneous weight

Definition

- *Homogeneous weight:*

$$w : R \to \mathbb{Q}, w(r) = \begin{cases} 0 & r = 0 \\ q & r \in I_{m-1} \setminus \{0\} \\ q-1 & r \in R \setminus I_{m-1} \end{cases}$$

The homogeneous weight

Definition

- *Homogeneous weight:*

$$w : R \to \mathbb{Q}, w(r) = \begin{cases} 0 & r = 0 \\ q & r \in I_{m-1} \setminus \{0\} \\ q - 1 & r \in R \setminus I_{m-1} \end{cases}$$

- $d(r, r') := w(r - r')$ (extend to R^n)

The homogeneous weight

Definition

- *Homogeneous weight:*

$$w : R \to \mathbb{Q}, w(r) = \begin{cases} 0 & r = 0 \\ q & r \in I_{m-1} \setminus \{0\} \\ q-1 & r \in R \setminus I_{m-1} \end{cases}$$

- $d(r, r') := w(r - r')$ (extend to R^n)
- *Minimum homogeneous distance*:
  $d(C) := \min\{d(c, c') : c, c' \in C, c \neq c'\} = \min\{w(c) : c \in C \setminus \{0\}\}$

The homogeneous weight

Definition

- *Homogeneous weight:*

$$w : R \to \mathbb{Q}, w(r) = \begin{cases} 0 & r = 0 \\ q & r \in I_{m-1} \setminus \{0\} \\ q-1 & r \in R \setminus I_{m-1} \end{cases}$$

- $d(r, r') := w(r - r')$ (extend to R^n)
- *Minimum homogeneous distance*:
  $d(C) := \min\{d(c, c') : c, c' \in C, c \neq c'\} = \min\{w(c) : c \in C \setminus \{0\}\}$
- M. Greferath and S. Schmidt, 1999:
  $\exists$ isometry $\Psi : (R, q^{m-2} \cdot d) \to (\mathbb{F}_q^{q^{m-1}}, d_{\mathrm{ham}})$ ("Gray map")

System of Diophantine inequalities

System of Diophantine inequalities

Theorem

Searching a linear $(n, \lambda, \geq \delta, R)$-code

$$\Updownarrow$$

Solving the system:

$$\begin{aligned} Mx &\geq \begin{pmatrix} \delta \\ \vdots \\ \delta \end{pmatrix} \\ \mathbb{1}^T x &= n \end{aligned}$$

$$(M \in \mathbb{N}_0^{t \times t}, x \in \mathbb{N}_0^t)$$

Example

Example

$R := \mathbb{Z}_4, \lambda := (2, 1, 1).$

			1	1	1	1	2	2	2	2	0	0	0
			0	0	2	2	0	0	2	2	2	2	0
			0	2	2	0	0	2	2	0	0	2	2
1	1	0	1	1	1	1	2	2	2	2	0	0	0
1	0	1	1	1	1	1	2	0	0	2	0	2	2
1	1	1	1	1	1	1	2	0	2	0	2	0	2
1	1	0	1	1	1	1	2	2	0	0	2	2	0
2	0	0	2	2	2	2	0	0	0	0	0	0	0
2	0	1	2	0	0	2	0	2	2	0	0	2	2
2	1	1	2	0	2	0	0	2	0	2	2	0	2
2	1	0	2	2	0	0	0	0	2	2	2	2	0
0	1	0	0	0	2	2	0	0	2	2	2	2	0
0	1	1	0	2	0	2	0	2	0	2	2	0	2
0	0	1	0	2	2	0	0	2	2	0	0	2	2

Heuristic algorithm

Heuristic algorithm

- Define heuristic evaluation function $\text{eval} : \mathbb{N}_0^t \to \mathbb{R}$.

Heuristic algorithm

- Define heuristic evaluation function $\mathrm{eval} : \mathbb{N}_0^t \to \mathbb{R}$.
- Construct $x_0 \le x_1 \le x_2 \cdots \le x_n$ in $\mathbb{N}_0^t$ with

Heuristic algorithm

- Define heuristic evaluation function $\mathrm{eval} : \mathbb{N}_0^t \to \mathbb{R}$.
- Construct $x_0 \leq x_1 \leq x_2 \cdots \leq x_n$ in $\mathbb{N}_0^t$ with
  - $x_0 = 0$

Heuristic algorithm

- Define heuristic evaluation function $\text{eval} : \mathbb{N}_0^t \to \mathbb{R}$.
- Construct $x_0 \leq x_1 \leq x_2 \cdots \leq x_n$ in $\mathbb{N}_0^t$ with
  - $x_0 = 0$
  - $x_{i+1} = x_i + e_{s_i}$

Heuristic algorithm

- Define heuristic evaluation function $\mathrm{eval} : \mathbb{N}_0^t \to \mathbb{R}$.
- Construct $x_0 \leq x_1 \leq x_2 \cdots \leq x_n$ in $\mathbb{N}_0^t$ with
  - $x_0 = 0$
  - $x_{i+1} = x_i + e_{s_i}$
  - s_i chosen s. t. $\mathrm{eval}(x_i + e_{s_i})$ is maximized ("greedy")

Heuristic algorithm

- Define heuristic evaluation function $\text{eval} : \mathbb{N}_0^t \to \mathbb{R}$.
- Construct $x_0 \leq x_1 \leq x_2 \cdots \leq x_n$ in $\mathbb{N}_0^t$ with
  - $x_0 = 0$
  - $x_{i+1} = x_i + e_{s_i}$
  - s_i chosen s. t. $\text{eval}(x_i + e_{s_i})$ is maximized ("greedy")
- If x_n is a solution $\to$ terminate; otherwise: backtracking.

Evaluation function

Evaluation function

- Idea:

$$\mathrm{eval}(x) \overset{!}{\approx} \epsilon(x) := \frac{|\{y \geq x : \|y\|_1 = n,\ My \geq \delta \cdot \mathbb{1}\}|}{|\{y \geq x : \|y\|_1 = n\}|}$$

Evaluation function

- Idea:

$$\mathrm{eval}(x) \stackrel{!}{\approx} \epsilon(x) := \frac{|\{y \geq x : \|y\|_1 = n,\ My \geq \delta \cdot \mathbb{1}\}|}{|\{y \geq x : \|y\|_1 = n\}|}$$

- Consider inequalities $M_{i,*}y \geq \delta$ separately:

Evaluation function

- Idea:

$$\mathrm{eval}(x) \overset{!}{\approx} \epsilon(x) := \frac{|\{y \geq x : \|y\|_1 = n,\ My \geq \delta \cdot \mathbb{1}\}|}{|\{y \geq x : \|y\|_1 = n\}|}$$

- Consider inequalities $M_{i,*}y \geq \delta$ separately:

$$\epsilon_i(x) := \frac{|\{y \geq x : \|y\|_1 = n,\ M_{i,*}y \geq \delta\}|}{|\{y \geq x : \|x\|_1 = n\}|}$$

Evaluation function

- Idea:

$$\mathrm{eval}(x) \stackrel{!}{\approx} \epsilon(x) := \frac{|\{y \geq x : \|y\|_1 = n,\ My \geq \delta \cdot \mathbb{1}\}|}{|\{y \geq x : \|y\|_1 = n\}|}$$

- Consider inequalities $M_{i,*}y \geq \delta$ separately:

$$\epsilon_i(x) := \frac{|\{y \geq x : \|y\|_1 = n,\ M_{i,*}y \geq \delta\}|}{|\{y \geq x : \|x\|_1 = n\}|}$$

- Assuming "stochastic independence" $\Rightarrow$

$$\epsilon(x) \approx \prod_{i=0}^{t-1} \epsilon_i(x) =: \mathrm{eval}(x)$$

Computation of ϵ_i

Computation of ϵ_i

- $\epsilon_i(x)$ only depends from $\|x\|_1$ and $M_{i,*}x$.

Computation of ϵ_i

- $\epsilon_i(x)$ only depends from $\|x\|_1$ and $M_{i,*}x$.
- Derive lookup table from coefficients of

$$p_i(y,z) = \prod_{s:a_i^s>0} \left(\sum_{j=0}^{n} y^{sj} z^j \binom{j + a_i^s - 1}{j} \right)$$

($a_i^s :=$ multiplicity of weight s in $M_{i,*}$)

Computation of ϵ_i

- $\epsilon_i(x)$ only depends from $\|x\|_1$ and $M_{i,*}x$.
- Derive lookup table from coefficients of

$$p_i(y,z) = \prod_{s:a_i^s>0} \left(\sum_{j=0}^{n} y^{sj} z^j \binom{j + a_i^s - 1}{j} \right)$$

($a_i^s :=$ multiplicity of weight s in $M_{i,*}$)

- Using reductions: $\leq (\delta+2)(n+1)^2$ multiplications.

Results

Results

- Codes of high minimum distance for more than 300 pairs (R, λ) $(n \leq 100)$ were constructed.

Results

- Codes of high minimum distance for more than 300 pairs (R, λ) $(n \leq 100)$ were constructed.
- For $char(R) = p$ many of them are provably optimal.

Results

- Codes of high minimum distance for more than 300 pairs (R, λ) $(n \leq 100)$ were constructed.
- For $char(R) = p$ many of them are provably optimal.
- Two new $\mathbb{Z}_4$-linear codes whose Gray image beats the corresponding upper binary linear bound were found:

Results

- Codes of high minimum distance for more than 300 pairs (R, λ) $(n \leq 100)$ were constructed.
- For $char(R) = p$ many of them are provably optimal.
- Two new $\mathbb{Z}_4$-linear codes whose Gray image beats the corresponding upper binary linear bound were found:
  - $\lambda = (2, 2, 2, 1)$, $n = 29$, $d(C) = 28$
  - $\lambda = (2, 2, 2, 2)$, $n = 57$, $d(C) = 56$

Results

- Codes of high minimum distance for more than 300 pairs (R, λ) $(n \leq 100)$ were constructed.
- For $char(R) = p$ many of them are provably optimal.
- Two new $\mathbb{Z}_4$-linear codes whose Gray image beats the corresponding upper binary linear bound were found:
  - $\lambda = (2, 2, 2, 1)$, $n = 29$, $d(C) = 28$
  - $\lambda = (2, 2, 2, 2)$, $n = 57$, $d(C) = 56$
- All results: `http://www.mathe2.uni-bayreuth.de/20er/`

Results

- Codes of high minimum distance for more than 300 pairs (R, λ) $(n \leq 100)$ were constructed.
- For $char(R) = p$ many of them are provably optimal.
- Two new $\mathbb{Z}_4$-linear codes whose Gray image beats the corresponding upper binary linear bound were found:
  - $\lambda = (2, 2, 2, 1)$, $n = 29$, $d(C) = 28$
  - $\lambda = (2, 2, 2, 2)$, $n = 57$, $d(C) = 56$
- All results: `http://www.mathe2.uni-bayreuth.de/20er/`

Thanks for your attention!