

Four Applications of \mathbb{Z}_4 -codes and their $GR(4, 2)$ analogues

Patrick Solé

Ankara, August 2008

- S P. Solé, “A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties”, Springer Lect. Not. Comp. Sc. 388, 1988.
- HKCSS Hammons, Kumar, Calderbank, Sloane, Solé, “The \mathbb{Z}_4 -linearity of Kerdock Preparata Goethals and related codes” IEEE IT March 94 .
- BSC Bonnetcaze, Solé, Calderbank “Quaternary Construction of Unimodular Lattices” IEEE IT March 95.
- BRS Bonnetcaze, Rains, Solé, “ 3-Colored 5-Designs and \mathbb{Z}_4 -Codes ”, J. Statistical Plan. Inf. 2000.

4 Applications of \mathbb{Z}_4 Codes

- 1988 Quaternary Low Correlation Sequences meeting the Sidelnikov bound (1971)[S] on interference vs length
- 1994 Explication of the formal duality (MacWilliams transform of weight enumerators) of (nonlinear!) Kerdock and Preparata codes (1972) → Award : Best paper in Information Theory for 1994 [HKCSS]
- 1995 A new construction of the Leech lattice (1965) [BCS], the building brick of the Conway sporadic simple groups
- 1999 New 5 – (24, 10, 36) designs supported by the words of the lifted Golay [BRS] (computer find of Harada 96) : proof by invariant theory of weight enumerators

Low Correlation Sequences

Let $\Omega_q = \{z \in \mathbb{C}, z^q = 1\}$

$x, y = 2$ sequences of period T valued in Ω_q . The **periodic correlation** of x and y at time lag l is

$$\theta_{x,y}(l) := \sum_{i=0}^{T-1} x_i^* y_{i+l}$$

Let \mathcal{M} be a family of M such sequences and θ_a (resp. θ_c) the maximum of the modulus of the **autocorrelation** ($x = y \in \mathcal{M}$ and $l \neq 0$) (resp. of the **crosscorrelation** ($x \neq y$)) and $\theta_m = \max(\theta_a, \theta_c)$

Problem : M, T given, find the smallest θ_m

Sidelnikov bounds (1971). For T large, and $M \sim T$:

If $q = 2$ then $\theta_m \geq \sqrt{2T}$

If $q > 2$ then $\theta_m \geq \sqrt{T}$

There is a binary sequence b_j of length $n = 2^m - 1$ with so-called **perfect autocorrelation** :

$$l \neq 0 \Rightarrow \theta_{b,b}(l) = -1$$

Construction : Let h_2 be a monic irreducible primitive $\in \mathbb{F}_2[x]$ and call θ one of its roots. Define $a_j := \text{tr}(\beta\theta^j)$, with β some constant $\in \mathbb{F}_2(\theta)$ and tr the trace from $\mathbb{F}_2(\theta)$ down to \mathbb{F}_2 . Put $b_j := (-1)^{a_j}$.

Generation :

sequence a_j satisfies a linear recurrence with characteristic polynomial h_2

can be implemented with a linear feedback shift register

Quaternary M-Sequences

Let h_4 be any lift of h_2 over $\mathbb{Z}_4[x]$

Eg $h_2(x) = x^2 + x + 1$ and $h_4(x) = x^2 - (x + 1)$

Consider linear recurrence with characteristic recurrence h_4

eg 1011231011... of period $6 = 2(2^2 - 1)$

To avoid period doubling demand h_4 to divide $x^n - 1$

This can be obtained by $h_4(x^2) = h_2(x)h_2(-x)$

Using these recurrences one can show There are $n + 2$ sequences $\in \Omega_4$ with period $n = 2^m - 1$ and $\theta_m \leq 1 + \sqrt{n + 1}$

Lifting Algorithm (odd n)

Input $X^n + 1 = g_2(X)h_2(X)$ over \mathbb{F}_2

Output $X^n - 1 = g_4(X)h_4(X)$ over \mathbb{Z}_4

Algorithm Let $g_2 = E(X) + O(X)$, with E =even part and O =odd part. Then

$$g_4(X^2) = E(X)^2 - O(X)^2$$

Over a suitable extension of \mathbb{Z}_4 the roots of g_2 are of order at most $2n$. The polynomial whose roots are the square of the roots of g_2 is g_4 . \square

To go over $\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_{16}, \dots, \mathbb{Z}_{2^\infty}$ just iterate the above algorithm.
(Cf. Calderbank, Sloane for codes over 2-adics)

The Galois Ring $GR(p^s, m)$ is the unique Galois extension of degree m of \mathbb{Z}_{p^s} (p a prime)

Here $p = s = 2$. Let $R := GR(4, m) = \mathbb{Z}_4[x]/(h_4)$

R is a ring with non units $2R$ and $R/2R = \mathbb{F}_{2^m}$

The so-called **Teichmueller** representatives are

$$\mathcal{T} = \{0, 1, \xi, \dots, \xi^{n-2}\}$$

2-adic expansion of x is $x = a + 2b$ with $a, b \in \mathcal{T}$

Frobenius operator

$$F(a + 2b) := a^2 + 2b^2.$$

Trace operator

$$T := \sum_{j=0}^{m-1} F^j$$

\mathbb{F}_2	\mathbb{Z}_4
h_2	$h_4 \equiv h_2 \pmod{2}$
Galois fields	Galois rings
\mathbb{F}_{2^m}	$GR(4, m)$
$\mathbb{F}_2[x]/(h_2(x))$	$\mathbb{Z}_4[x]/(h_4(x))$
$h_2(\theta) = 0$	$h_4(\xi) = 0$
$tr(\beta\theta^j)$	$Tr(\gamma\xi^j)$

Hamming vs Simplex

Recall that the parity-check matrix for the cyclic $[n, n - m, 3]$ **Hamming code** \mathcal{H}_m is

$$H = [1 | \theta \cdots \theta^{n-1}],$$

where, as usual, \mathbb{F}_{2^m} is identified with \mathbb{F}_2^m by using basis of the extension

Its row \mathbb{F}_2 -span is the **Simplex code** an irreducible cyclic code whose words are periods of the M-sequence of feedback polynomial h_2 .

Note that $h_2(\theta) = 0$, and that h_2^* is a generator for \mathcal{H}_m .

Preparata vs Kerdock

Consider the free \mathbb{Z}_4 -code P_m of length $n + 1 = 2^m$ with parity-check matrix

$$H = [1111 \cdots 101\xi\xi^2 \cdots \xi^{n-1}],$$

where, as has become usual, $GR(4, m)$ is identified with \mathbb{Z}_4^m

Its \mathbb{Z}_4 -dual, K_m say, consists—up to parity check digit and complementation—of the periods of the quaternary M-sequence of feedback polynomial h_4

$\phi(K_m)$ is the **Kerdock code** (for odd $m \geq 3$)

$\phi(P_m)$ is **Preparata-like** (same weight distribution)

Kerdock code was constructed in 1972 and Preparata in 1968 by ad hoc means from Reed Muller codes.

Gray map

To get binary codes from \mathbb{Z}_4 code use the **Gray map** Φ which replaces 0, 1, 2, 3 by 00, 10, 11, 01

(*not* a group morphism!)

Define the **Lee weight** of $x \in \mathbb{Z}_4$ as the Hamming weight of its Gray image $w_L(x) := w_H(\Phi(x))$,

and the **Lee distance** by translation $d_L(x, y) = w_L(x - y)$.

By Galois ring arguments it can be shown that the minimum Lee weight of P_m is 6, and that of K_m is $2^m - 2^{(m-1)/2}$, for odd $m \geq 3$.

This is better than any known linear code with the same length and size!!!

(there is no linear Preparata, Cf. Brouwer-Tolhuizen 1993).

Formal duality

If C is a \mathbb{Z}_4 -code its **Symmetrized Weight Enumerator** is

$$swe := \sum_{c \in C} \prod_{i=0,1,2} x_i^{n_i(c)}$$

where $n_i(c)$ counts the number of coordinates of c of Lee weight i
Then $W_{\Phi(C)}(x, y) = swe_C(x^2, xy, y^2)$.

The McWilliams duality for the swe yields the formula

$$W_{\Phi(C^\perp)}(x, y) = \frac{1}{|C|} W_{\Phi(C)}(x, y)$$

Note that $\Phi(C)$ needs not be linear. Neither Kerdock nor Preparata are linear.

Still, they are formal duals of each other, a fact known since 1972!
Bill Kantor wrote in 1983 that this was "merely a coincidence" !

Let (v_1, \dots, v_n) be a basis of \mathbf{R}^n

A **Lattice** Λ is defined as

$$\Lambda := \left\{ \sum_{i=1}^n \lambda_i v_i \mid \lambda_i \in \mathbb{Z} \right\}$$

Its main measurements are
fundamental parallelotope, fundamental volume, packing radius ρ ,
covering radius R .

The **dual** Λ^* of a lattice Λ is

$$\Lambda^* := \{y \in \mathbf{R}^n \mid \forall x \in \Lambda \ x \cdot y \in \mathbb{Z}\}$$

A lattice is **unimodular** if it is equal to its dual.

Construction A

Given an additive code C of length n over \mathbb{Z}_m **construction A** builds a lattice $A(C)$ by the rule

$$\sqrt{m}A(C) = C + m\mathbb{Z}^n$$

$\sqrt{m}A(C)$ is the inverse image of reduction mod m in \mathbb{Z}^n

The **fundamental volume** is $m^{n/2}/|C|$

The **packing radius** is determined by the minimum Hamming distance ($m = 2$)

or the minimum Euclidean distance ($m = 4$)

$A(C)$ is **unimodular** iff C is self-dual

$A(C)$ is **even** iff the euclidean weights of C are multiples of $2m$

Binary Cyclic Codes

To construct all binary cyclic codes of length n we need to factorize $X^n + 1$ over $GF(2)$. Two famous **quadratic residue codes** are

- the $[7, 4, 3]$ Hamming code

$$X^7 + 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

- the $[23, 12, 7]$ Golay code

$$X^{23} + 1 = (X + 1)$$

$$(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)$$

$$(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)$$

Adding an overall parity-check we obtain two **Type II** binary codes : self-dual and with weights multiple of 4.

The $[24, 12, 8]$ is invariant under the **Mathieu group** M_{24} .

Quaternary cyclic codes

To construct all quaternary cyclic codes of length n we need to factorize $X^n - 1$ over \mathbb{Z}_4 . Two interesting **lifted** quadratic residue codes are

- above the $[7, 4, 3]$ Hamming code

$$X^7 - 1 = (X - 1)(X^3 + 2X^2 + X + 3) \\ (X^3 + 3X^2 + 2X + 3)$$

- above the $[23, 12, 7]$ Golay code

$$X^{23} - 1 = (X - 1) \\ (X^{11} + 2X^{10} + 3X^9 + 3X^7 + 3X^6 + 3X^5 + 2X^4 + X + 3) \\ (X^{11} + 3X^{10} + 2X^7 + X^6 + X^5 + X^4 + X^2 + 2X + 3)$$

Adding an overall parity-check we obtain two **Type II** \mathbb{Z}_4 -codes : self-dual and with Euclidean weights multiple of 8.

The $[24, 12, 12]$ is only invariant (by monomial action) under $PSL(2, 23)$.

Applications :

Adding an overall parity-check we obtain two extended cyclic codes the **octacode** and the **lifted Golay** both self-dual and with Euclidean weights multiple of 8.

- Gray mapping of octacode gives the $(16, 2^8, 6)$ Nordstrom-Robinson code [HKCSS]. The lifted Golay gives a non-linear f.s.d. $(48, 2^{24}, 12)$. [BSC]
- Construction $A \bmod 4$ yields respectively the E_8 and the Leech lattices, two integral unimodular even lattices [BSC]. The Leech lattice is famous as a tool for constructing four sporadic finite simple groups. This is "the simplest construction of the Leech lattice known to date" wrote Conway and Sloane in *Sphere packings, Lattices and groups*.

In 1996 Masaaki Harada discovered by computer new 5-designs e.g $5 - (24, 10, 36)$ in the words of given Lee composition of the lifted Golay.

Their existence *cannot* be explained by transitivity. ($PSL(2, 23)$ is only 3-homogeneous).

There was no analogue of Assmus-Mattson then (See David Masson 2003 and Kenichiro Tanabe 2003 since).

Develop a notion of **colored designs** and use invariant theory of split weight enumerators to show their existence.

Colored designs

A **colored design** D is a triple of sets (P, B, C) of "points", "blocks", and "colors" along with a "palette"

$$\rho : (P, B) \longrightarrow C$$

Block b uses color s at point p if $\rho(p, b) = s$.

D is a **strong** colored t -design iff $\forall c \in C^t$ there is a constant λ such that $\forall \pi \in P^t$ there are λ blocks using the prescribed colors at the prescribed points.

If order of points and colors does not matter replace strong by **weak** in the above.

Motivation usual (i.e. bicolore) designs are obtained by bleaching ie equating $|C| - 1$ colors.

Split weight enumerators

Let C be a \mathbb{Z}_4 -code of length n and $T \subseteq [n]$ a subset of coordinate places.

Define the **Lee composition** of $c \in \mathbb{Z}_4^n$ on T as (m_0, m_1, m_2) where m_i counts the number of $j \in T$ such that $c_j = i$ and the Lee composition out of T as the number of $j \in [n] \setminus T$ such that $c_j = i$. Define the **split weight enumerator** $J_{C,T}$ (called **Jacobi polynomial** by Michio Ozeki) as

$$J_{C,T} = \sum_{c \in C} \prod_{i=0,1,2} x_i^{m_i} y_i^{n_i}$$

If we can prove that $J_{C,T}$ does **not** depend on T for $|T| = t$ then the codewords of C of given Lee composition (on $[n]$) hold a weak **tricolore** t -design.

Define the **Aronhold differential operator**

$$A := \sum_{i=0,1,2} x_i \partial / \partial y_i$$

Call a \mathbb{Z}_4 -code colorwise **t -homogeneous** if the codewords of given Lee composition hold a t -design.

For such a code $\forall T, |T| = t$, we have

$$J_{C,T} = \frac{1}{\binom{n}{t}} A^t \text{swec}$$

Four applications of $GR(4, 2)$

The Galois ring $GR(4, 2)$ of order 16 and characteristic 4 shares, as a coding alphabet, properties of both the ring \mathbb{Z}_4 and the field \mathbb{F}_4 . Consider **four applications**

- self-dual \mathbb{Z}_4 -codes of length $2n$ by projection on a **Trace Orthogonal Basis**
- **Quasi-Cyclic** self-dual \mathbb{Z}_4 -codes of length $3n$ by the cubic construction
- **Modular Lattices** of dimension $2n$ by Construction A
- formally self-dual \mathbb{F}_4 -codes of length $2n$ by Gray map

Type II codes over $GR(4, 2)$

A code over $GR(4, 2)$ is **Euclidean self-dual** iff it is equal to its dual for the Euclidean scalar product

$$\sum_i x_i y_i$$

Let \tilde{x} denote an arbitrary lift from $GR(4, 2)$ into $GR(8, 2)$. According to Choie-Betsumiya an Euclidean self-dual code is **Type II** iff each one of its codewords c satisfies

$$\sum_{i=1}^n \tilde{c}_i^2 = 0.$$

A TOB of $GR(4, 2)$ over \mathbb{Z}_4

Write $GR(4, 2) = \mathbb{Z}_4[\alpha]$, with $\alpha^2 + \alpha + 1 = 0$.

Let $\gamma = \alpha$ and $\delta = \alpha^2 + 2\alpha = \alpha + 3$.

Observe that reduction modulo 2 yields a TOB of \mathbb{F}_4 over \mathbb{F}_2 .

Define a bijective map ν say which maps $c\gamma + d\delta \in R$ onto $(c, d) \in \mathbb{Z}_4^2$.

A result special to $GR(4, 2)$ is

If $C \subseteq R^n$ is a **euclidean self-dual code** then $\nu(C)$ is a **self-dual \mathbb{Z}_4 code**.

Furthermore $\nu(C)$ is **Type II** iff C is.

Example : Augmented QR code in length 19 over $GR(4, 2)$ yields after Construction A4 an extremal Type I lattice in dimension 38

Cubic Construction of \mathbb{Z}_4 codes

A code C over \mathbb{Z}_4 of length 3ℓ is ℓ -quasi-cyclic if it is invariant under the power ℓ of the shift.

By results of Ling-S., every such code can be written as

$$C = \{(x + \text{Tr}(y)|x + \text{Tr}(\alpha^2 y)|x + \text{Tr}(\alpha y)) \mid \mathbf{x} \in C_1, y \in C_2\}$$

where C_1 is a code over \mathbb{Z}_4 of length ℓ
and C_2 is a code of length ℓ over $GR(4, 2)$.

Furthermore, if both C_1 and C_2 are self-dual so is C . In that case C is Type II iff C_1 is.

\Rightarrow Good codes in lengths 30 and 42 yielding optimal and extremal unimodular lattices in dimensions 30 and 42

Hermitian Self dual Codes

There is a **conjugation** on $GR(4, 2)$ induced by **complex conjugation**.

Let $z = t + \alpha t'$ be a generic $z \in GR(4, 2)$ with $t, t' \in \mathbb{Z}_4$. We shall denote by \bar{z} the **conjugate** of z and define it as

$$\bar{z} = t + t'\alpha^2 = t - t' - \alpha t'.$$

A code is **Hermitian self-dual** if it is equal to its dual w.r.t. the form

$$x \cdot y = \sum_i x_i \bar{y}_i$$

Hermitian Weight

Let T denote the **Teichmüller** representatives of the cosets of $2GR(4, 2)$ into $GR(4, 2)$.

$$T = \{0, 1, \alpha, \alpha^2\}.$$

For convenience let $T^* = T \setminus 0$. Define

$$T_0 = \{0\}, T_1 = \pm T^*, T_2 = 2T_1, T_3 = (\alpha - 1)T_1.$$

The **hermitian weight** $w_3(\cdot)$ is defined as $w_3(x) = 1, 4, 9$ if $x \in T_1, T_2, T_3$ respectively, and zero otherwise.

It is instrumental in computing the **norm** of the lattice constructed from the code, as shown next.

Eisenstein lattices

Let A_2 denote the hexagonal lattice scaled to have norm 2.

Let ρ be a **complex third root of unity** $\rho = \exp(2\pi\sqrt{-1}/3)$

In other words $A_2 = \sqrt{2}E$ where $E := \mathbb{Z}[\rho]$ stands for the ring of **Eisenstein integers**. To every $GR(4, 2)$ -code we attach an E -lattice

Define construction A_3 as

$$A_3(C) = \frac{1}{\sqrt{2}}(C + 4A_2^n).$$

In particular such lattices are **3-modular**: isometric (as quadratic forms) to three times their dual.

If C is an **hermitian self-dual** R -code of length n then the real image of $A_3(C)$ is a 3-modular \mathbb{Z} -lattice of dimension $2n$ and of norm

$$\min(8, w_3(C)/2).$$

A Gray Map over $GR(4, 2)$

We consider the following "Gray map" ϕ

$$z = A + 2B \mapsto (b, a + b)$$

from $GR(4, 2)$ into \mathbb{F}_4^2 . Here $A, B \in T$ and a, b are their images under reduction modulo 2. The Hamming weight of $\phi(x)$ is constant on $x \in T_i$ of respective value 0, 1, 2, 2. Unfortunately this Gray map, unlike the one from \mathbb{Z}_4 , is **not** an isometry.

The Hamming weight enumerator of $\phi(C)$ can therefore be easily obtained from its swe : $W_{\phi(C)}(x, y) = swe_C(x^2, xy, y^2, y^2)$. For convenience one can define a super symmetrized weight enumerator

$$sswe_C(X, Y, Z) := swe_C(X, Y, Z, Z).$$

With this notation

$$W_{\phi(C)}(x, y) = sswe_C(x^2, xy, y^2).$$

Note that the codes obtained on \mathbb{F}_4 are non-linear in general.

Formally Self Dual quaternary codes

If C is either hermitian or euclidean self-dual then $\phi(C)$ is formally self-dual for the Hamming weight enumerator.

n	R-code	sd	\rightarrow	$2n$	F4-code	num	d
6	$P_3(\omega, 3\omega + 1, 3\omega + 1)$	H		12	C_{12}	4^6	6
8	$XQ_7(1, 1 + 2\omega, 1 + 3\omega)$	H		16	C_{16}	4^8	6
12	$XQ_{11}(0, 1 + 2\omega, 1 + 3\omega)$	E		24	C_{24}	4^{12}	9

TAB.: Non-linear \mathbb{F}_4 codes