Rains' algorithm for classifying self-dual $\mathbb{Z}_4$-codes with given residue

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University
(joint work with Rowena A. L. Betty)

October 14, 2009
Academia Sinica

Definitions and Statement of the Problem

- $\mathbb{Z}_4$: the ring of integers modulo 4,
- $\mathbb{Z}_4^n$: the free module of rank n over $\mathbb{Z}_4$,
- $(x, y) = \sum_{i=1}^{n} x_i y_i$, where $x, y \in \mathbb{Z}_4^n$,
- a submodule $C \subset \mathbb{Z}_4^n$ is called a code of length n over $\mathbb{Z}_4$, or a $\mathbb{Z}_4$-code of length n,
- C is self-dual if $C = C^\perp$, where $C^\perp = \{x \in \mathbb{Z}_4^n \mid (x, y) = 0 \ (\forall y \in C)\}$,
- the residue: $\mathrm{Res}(C) \subset \mathbb{F}_2^n$ (reduction $\mathbb{Z}_4 \to \mathbb{F}_2$ mod 2).

Problem

Given $C_0 \subset \mathbb{F}_2^n$, classify (up to monomial equivalence) self-dual $C \subset \mathbb{Z}_4^n$ with $\mathrm{Res}(C) = C_0$.

Given $C_0 \subset \mathbb{F}_2^n$, classify self-dual $C \subset \mathbb{Z}_4^n$ with $\mathrm{Res}(C) = C_0$.

C: self-dual $\mathbb{Z}_4$-code $\implies C_0 = \mathrm{Res}(C)$: doubly even.

Theorem (Rains, 1999)

Given a doubly even code C_0 of length n, dimension k,

- the set of all self-dual $\mathbb{Z}_4$-codes C with $\mathrm{Res}(C) = C_0$ has a structure as an affine space of dimension $k(k+1)/2$ over $\mathbb{F}_2$,
- the group $\{\pm 1\}^n \rtimes \mathrm{Aut}(C_0)$ acts as an affine transformation group,
- two codes C, C' are equivalent if and only if they are in the same orbit under this group.

The set of all self-dual $\mathbb{Z}_4$-codes C with $\mathrm{Res}(C) = C_0$ has a structure as an affine space of dimension $k(k+1)/2$ over $\mathbb{F}_2$

Naïvely speaking, classifying such C amounts to enumerating $k \times n$ binary matrices M such that

$$\begin{bmatrix} A + 2M \\ 2B \end{bmatrix} \text{ where } A \text{ generates } C_0, \quad \begin{bmatrix} A \\ B \end{bmatrix} \text{ generates } C_0^{\perp},$$

is self-dual. Among the 2^{kn} matrices M, not all of them generate a self-dual code, while some matrices generate the same code as the one generated by some other matrix. This reduces the number

$$2^{kn} \text{ to } 2^{k(k+1)/2}.$$

Given $C_0 \subset \mathbb{F}_2^n$, classify self-dual $C \subset \mathbb{Z}_4^n$ with $\mathrm{Res}(C) = C_0$.

Theorem (Rains, 1999)

Given a doubly even code C_0 of length n, dimension k,

- the set of all self-dual $\mathbb{Z}_4$-codes C with $\mathrm{Res}(C) = C_0$ has a structure as an affine space of dimension $k(k+1)/2$ over $\mathbb{F}_2$, (due to Gaborit, 1996)
- the group $\{\pm 1\}^n \rtimes \mathrm{Aut}(C_0)$ acts as an affine transformation group,
- two codes C, C' are equivalent if and only if they are in the same orbit under this group.

Given $C_0 \subset \mathbb{F}_2^n$, classify self-dual $C \subset \mathbb{Z}_4^n$ with $\mathrm{Res}(C) = C_0$.

Theorem (Rains, 1999)

Given a doubly even code C_0 of length n, dimension k,

- the set of all self-dual $\mathbb{Z}_4$-codes C with $\mathrm{Res}(C) = C_0$ has a structure as an affine space of dimension $k(k+1)/2$ over $\mathbb{F}_2$, (due to Gaborit, 1996)
- the group $\{\pm 1\}^n \rtimes \mathrm{Aut}(C_0)$ acts as an affine transformation group,
- two codes C, C' are equivalent if and only if they are in the same orbit under this group.

The group $\{\pm 1\}^n \rtimes \mathrm{Aut}(C_0)$ acts as an affine transformation group on an affine space of dimension $k(k+1)/2$

Theorem (improved version)

Given a doubly even code C_0 of length n, dimension k,

- the set of all self-dual $\mathbb{Z}_4$-codes C with $\mathrm{Res}(C) = C_0$ has a surjection onto an affine space of dimension at most $k(k+1)/2$ over $\mathbb{F}_2$,
- the group $\mathrm{Aut}(C_0)$ acts as an affine transformation group,
- two codes C, C' are equivalent if and only if their images are in the same orbit under this group.

Self-dual $\mathbb{Z}_4$-codes C with $\mathrm{Res}(C) = C_0$

Given a doubly even code C_0 of length n, dimension k, with generator matrix A, $C_0^\perp$ is generated by $\begin{bmatrix} A \\ B \end{bmatrix}$, set

- $\mathcal{M} = M_{k\times n}(\mathbb{F}_2)$,
- $V_0 = \{M \in \mathcal{M} \mid MA^T + AM^T = 0\}$,
- W_0: subspace of $\mathcal{M}$ generated by $\{M \in \mathcal{M} \mid MA^T = 0\}$ and $\{AE_{ii} \mid i = 1, \dots, n\}$. Then $W_0 \subset V_0$.

$$V_0/W_0 \ni M \mod W_0 \mapsto \begin{array}{c}\text{eq. class of}\\ \text{code generated by}\end{array} \begin{bmatrix} \tilde{A} + 2M \\ 2B \end{bmatrix}$$

is well-defined. ($\tilde{A}$ will be chosen appropriately)
$\mathrm{Aut}(C_0)$ acts on V_0/W_0 as an affine transformation group, and the orbits are the preimages of equivalence classes.

$\mathrm{Aut}(C_0)$ acts on V_0/W_0

First, take a matrix $\tilde{A}$ over $\mathbb{Z}_4$ such that

$$\tilde{A} \bmod 2 = A \text{ and } \tilde{A}\tilde{A}^T = 0.$$

For each $P \in \mathrm{Aut}(C_0)$, there exists a unique matrix $E_1(P) \in \mathrm{GL}(k, \mathbb{F}_2)$ such that

$$AP = E_1(P)A.$$

Also, there exists a matrix $E_2(P) \in \mathcal{M}$ such that

$$2E_2(P) = E_1(P)^{-1}\tilde{A}P - \tilde{A}.$$

$\mathrm{Aut}(C_0)$ acts on V_0/W_0

Theorem

The group $\mathrm{Aut}(C_0)$ acts on V_0/W_0 by

$$\begin{aligned} P : V_0/W_0 &\ni M \pmod{W_0} \\ &\mapsto E_1(P)^{-1}MP + E_2(P) \pmod{W_0} \in V_0/W_0, \end{aligned}$$

where $P \in \mathrm{Aut}(C_0)$. Moreover, there is a bijection

$$\mathrm{Aut}(C_0)\text{-orbits on } V_0/W_0 \to \begin{array}{c} \text{eq. class of} \\ \text{codes } C \text{ with} \\ \mathrm{Res}(C) = C_0, \end{array}$$

$$M \pmod{W_0} \mapsto \begin{array}{c} \text{eq. class of} \\ \text{codes generated by} \end{array} \begin{bmatrix} \tilde{A} + 2M \\ 2B \end{bmatrix}$$

Practical Implementation

$$\mathsf{Aut}(C_0) \to \mathsf{AGL}(V_0/W_0).$$

Since $\mathsf{AGL}(m, \mathbb{F}_2) \subset \mathsf{GL}(1+m, \mathbb{F}_2)$, we actually construct a linear representation:

$$\mathsf{Aut}(C_0) \to \mathsf{GL}(1 + \dim V_0/W_0, \mathbb{F}_2).$$

A straightforward implementation works provided

$$\dim V_0/W_0 \leq 20 \text{ plus alpha (about).}$$

Enumeration of self-dual $\mathbb{Z}_4$-codes of length 16

- Pless–Leon–Fields (1997): 133 Type II $\mathbb{Z}_4$-codes of length 16,
- Harada–Munemasa (2009): 1372 Type I $\mathbb{Z}_4$-codes of length 16.

Using Rains' algorithm implemented by us, it took about 1 minute to enumerate all the $133 + 1372 = 1505$ self-dual $\mathbb{Z}_4$-codes of length 16, from the set of 146 doubly even codes C_0.

Computing time is roughly proportional to the size of the affine space

$$|V_0/W_0| = 2^{\dim V_0/W_0},$$

and the maximum value of $\dim V_0/W_0$ in the above example is 22.

Toward the classification of extremal Type II codes of length 24

A straightforward computation will not work if one wishes to enumerate self-dual codes of length 24. For example, $C_0 =$ extended Golay code, $|V_0/W_0| = 2^{55}$.
Actually, for Type II codes, it is enough to look at a subspace U_0 of V_0, so that the search space has size

$$|U_0/W_0| = 2^{44}.$$

So we will have a matrix representation

$$M_{24} = \mathrm{Aut}(C_0) \to \mathrm{GL}(45, \mathbb{F}_2).$$

As an estimate:

$$\frac{2^{44}}{|M_{24}|} = 71856.7\ldots$$

but there are only 13 extremal Type II codes C with $\mathrm{Res}(C) =$ extended Golay code.