Self-dual codes over Galois rings

Whan-Hyuk Choi
崔桓赫

Department of Mathematics
Kangwon National University

5th Sino-Korea International Conference on Coding theory
and Related Topics, Jul 2–6, 2018
Shanghai University

Outline of this talk

In this talk, typically ‘a code’ means a self-dual code over a Galois ring .

1. Review of the classification problem and brief history of classification of codes
2. Galois rings, p-adic and q-adic integer rings and the relations between them.
3. Monomial transformation and automorphism group of codes.
4. The number of codes for mass formula.
5. Classification of codes of length 4 for all odd prime p : free code and non-free code.
6. Improvements : self-dual codes over q-adic integers and codes of length 6. We present some examples.

Classification problem

The general **strategy for the classification problem** is as follows.

1. Calculate the total number of all distinct codes, say N.
2. Choose a code $\mathcal{C}$ as a representative and calculate its automorphism.
3. Count the number of codes in the equivalent class in which $\mathcal{C}$ included.
4. Repeating this step until the total number of codes classified meets the total number of codes N.

Mass formula

Let $N(n)$ be # of all self-dual codes of length n and s be # of equivalent classes. Then we can get the *mass formula* :

$$\sum_{j=1}^{s} \frac{|\mathbb{T}^n|}{|Aut(\mathcal{C}_j)|} = N(n)$$

where $\mathbb{T}^n = \{\sigma\gamma \mid \gamma \in \mathbb{D}^n, \sigma \in S_n\}$ is the group of *monomial transformations*.
Acquiring total number of codes and automorphisms of each class is critical for the classification of self-dual codes.

Classification of self-dual codes over Galois rings

- In 1996, P. Gaborit found mass formula of self-dual codes over $\mathbb{Z}_4$.
- In 2008, K. Nagata et F. Nemenzo and H. Wada found mass formula of self-dual codes over $\mathbb{Z}_{p^s}$ for odd prime p.
- In 2011, K. Nagata et F. Nemenzo and H. Wada found mass formula of self-dual codes over $\mathbb{Z}_{2^s}$ as well.
- In 2011, Y.H. Park classified self-dual codes over $\mathbb{Z}_p$ of length 4.
- In 2017, Park and Choi classified self-dual codes over $\mathbb{Z}_{p^2}$ of length 4.
- We generalized the results on self-dual codes over $GR(p^2, 2)$ of length 4.
- We are now focusing on the classification of free self-dual codes over $GR(p^e, r)$ and q-adic integers of moderate lengths.

Galois rings

Definition (Z.-W. Wan)

A **Galois ring** is defined to be a finite ring with identity 1 such that the set of its zero divisers with 0 added forms a principal ideal $\langle p \rangle$ for some prime number p.

- The ring $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ have the principal ideal $\langle 3 \rangle = \{0, 3, 6\}$. Thus the ring $\mathbb{Z}_9$ is a Galois ring.
- The ring $\mathbb{Z}_{p^e}$ is a Galois ring with p^e elements.
- The finite field $\mathbb{F}_{p^m}$ is trivially a Galois ring with p^m elements.

Construction of a Galois ring

Theorem

Let r be a positive integer and $h(X)$ be a monic basic irreducible polynomial in $\mathbb{Z}_{p^e}[X]$ of degree r that divides $X^{p^r-1}-1$. The polynomial $h(X)$ is chosen so that $\zeta = X + h(X)$ is a primitive (p^r-1)st root of unity. Then a Galois ring of characteristic p^e with $(p^e)^r$ elements, unique up to isomorphism, can be constructed as a ring

$$GR(p^e, r) = \mathbb{Z}_{p^e}[X]/\langle h(X)\rangle \simeq \mathbb{Z}_{p^e}[\zeta].$$

- If $\zeta \in GR(p^e, r)$ is a primitive (p^r-1)st root of unity then the set $\mathcal{T} = \{0, 1, \zeta, \ldots, \zeta^{p^r-2}\}$ is called a **Teichmüller set**.
- Elements of $GR(p^e, r)$ can be uniquely written as a p-adic sum $c_0 + c_1 p + c_2 p^2 + \cdots + c_{e-1} p^{e-1}$ with $c_i \in \mathcal{T}$.
- Elements of $GR(p^e, r)$ can also be written in the ζ-adic expansion $b_0 + b_1\zeta + \cdots + b_{r-1}\zeta^{r-1}$ with $b_i \in \mathbb{Z}_{p^e}$.

Construction of a Galois ring

Example

- In MAGMA $GR(3^3, 3) \simeq \mathbb{Z}_{3^3}[X]/\langle X^3 + 2X + 1\rangle$ and we set $\zeta = X + \langle X^3 + 2X + 1\rangle$ and $GR(3^3, 3) \simeq \mathbb{Z}_{3^3}[\zeta]$.
- Let $\alpha = 15 + 20\zeta + 13\zeta^2 \in GR(3^3, 3) \simeq \mathbb{Z}_{3^3}[\zeta]$ in the ζ-adic expansion. Then α can be represented as a p-adic sum as

$$(2\zeta + \zeta^2) + (2 + \zeta^2)3 + (1 + 2\zeta + \zeta^2)9.$$

- We usually compute elements in $GR(p^e, r)$ with ζ-adic expansion.

$$\begin{aligned} \alpha \cdot \zeta &= 15\zeta + 20\zeta^2 + 13\zeta^3 \\ &= 15\zeta + 20\zeta^2 + 13(25\zeta + 26) \\ &= 14 + 16\zeta + 20\zeta^2 \end{aligned}$$

$h(X)$ of $GR(p^2, 2)$ for each prime $p \leq 61$ used in MAGMA

p	$h(X)$	p	$h(X)$
2	$X^2 + X + 1$	29	$X^2 + 24X + 2$
3	$X^2 + 2X + 2$	31	$X^2 + 29X + 3$
5	$X^2 + 4X + 2$	37	$X^2 + 34X + 2$
7	$X^2 + 6X + 3$	41	$X^2 + 38X + 6$
11	$X^2 + 7X + 2$	43	$X^2 + 42X + 3$
13	$X^2 + 12X + 2$	47	$X^2 + 45X + 5$
17	$X^2 + 16X + 3$	53	$X^2 + 49X + 2$
19	$X^2 + 18X + 2$	59	$X^2 + 58X + 2$
23	$X^2 + 21X + 5$	61	$X^2 + 60X + 2$

Galois ring

- Actually, Z_{p^e} is isomorphic to Galois ring of degree 1, denoted by $GR(p^e, 1)$ and $GF(p^r)$ is isomorphic to $GR(p, r)$.
- The codes over finite chain rings have some good properties.
- Every finite chain ring is a homomorphic image of some polynomial ring $GR(p^e, r)[x]$.
- $GF(p^r)$ can be lifted to $GR(p^e, r)$ and they have some similarities in structure.

Lattice of Galois rings

$$
\begin{array}{ccccccc}
\mathbb{F}_{p^{rs}} & \longleftrightarrow & GR(p^2, rs) & \longleftrightarrow & GR(p^3, rs) & \longleftrightarrow \cdots & \longleftrightarrow \quad ?? \\
\vert & & \vert & & \vert & & \vert \\
\mathbb{F}_{p^r} & \longleftrightarrow & GR(p^2, r) & \longleftrightarrow & GR(p^3, r) & \longleftrightarrow \cdots & \longleftrightarrow \quad ? \\
\vert & & \vert & & \vert & & \vert \\
\mathbb{F}_p \simeq \mathbb{Z}_p & \longleftrightarrow & \mathbb{Z}_{p^2} & \longleftrightarrow & \mathbb{Z}_{p^3} & \longleftrightarrow \cdots & \longleftrightarrow \quad \mathbb{Z}_{p^\infty}
\end{array}
$$

p-adic integers

Definition

Fix a prime number p. The p-adic absolute value of a nonzero $r = p^k \frac{a}{b} \in \mathbb{Q}$ with $(a, p) = (b, p) = 1$ is defined by

$$|r|_p = p^{-k}.$$

$|\cdot|_p$ is a legitimate absolute value and it defines a metric on $\mathbb{Q}$. By completing $\mathbb{Q}$ with respect to this metric, we obtain a field of p-adic numbers

$$\mathbb{Q}_p = \{\sum_{i=n_0}^{\infty} a_i p^i \mid \quad 0 \leq a_i < p,\ n_0 \in \mathbb{Z}\} \supset \mathbb{Q}.$$

Its subring

$$\mathcal{O}_p = \{\sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i < p\} = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\}$$

is called the ring of p-adic integers.

Facts

1. The ring of p-adic integers is a pricipal ideal domain.
2. $|\alpha+\beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$ non-archimedian
3. $1+2+2^2+2^3+\cdots = \frac{1}{1-2} = -1$ in $\mathbb{Q}_2$.
4. -1 is a square in $\mathbb{Q}_p$ iff $p \equiv 1 \pmod 4$.
5. $(2121342303\cdots_{(5)})^2 = -1$ in $\mathbb{Q}_5$.
6. $(2+5+2\cdot5^2+5^3+3\cdot5^4+\cdots)(2+5+2\cdot5^2+5^3+3\cdot5^4+\cdots)+1 = 0$

Finite extensions of p-adic numbers

Theorem

For each integer $r \geq 1$, there exists a unique unramified extension $\mathbb{Q}_{p^r}$ of degree r over $\mathbb{Q}_p$. It can be obtained by adjoining to $\mathbb{Q}_p$ a primitive $(p^r - 1)$st root of unity.

- Let $\bar{\zeta}$ be a generator of $\mathbb{F}_{p^r}^*$. Then $\mathbb{F}_{p^r} = \mathbb{F}_p(\bar{\zeta})$.
- Let $\bar{h}(X)$ be a minimal polynomial for $\bar{\zeta}$ over $\mathbb{F}_p$. Lift $\bar{h}(X)$ to any $h(X) \in \mathcal{O}_p$ which is an irreducible polynomial over $\mathcal{O}_p$ and $\mathbb{Q}_p$ of degree r.
- If ζ is a root of $h(X)$, then $\mathbb{Q}_p(\zeta) = \mathbb{Q}_{p^r}$ is an extension of degree r.
- The residue field $\mathbb{K}$ of $\mathbb{Q}_p(\zeta)$ contains a root $\zeta \pmod{p}$ of $\bar{h}(X)$, and $\mathbb{K} = \mathbb{F}_{p^r}$.

q-adic integers

Let $q = p^r$ and the ring of integers of $K = \mathbb{Q}_q$ is denoted by $\mathcal{O}_q$:

$$\mathcal{O}_q = \{a \in \mathbb{Q}_q \mid |a| \leq 1\}.$$

$\mathcal{O}_q$ is the set of all roots in $\mathbb{Q}_{p^r}$ of monic polynomials over $\mathcal{O}_p$. We call $\mathcal{O}_q$ the ring of q-adic integers.

Theorem

$\mathcal{O}_q = \mathcal{O}_p[\zeta]$, where ζ is a primitive $(p^r - 1)$st root of unity.

Its unique maximal ideal is

$$\mathcal{P}_q = p\mathcal{O}_q = \{a \in \mathbb{Q}_{p^r} \mid |a| < 1\}.$$

We have that the residue field of $\mathbb{Q}_{p^r}$ is

$$\mathcal{O}_q/\mathcal{P}_q \simeq \mathbb{F}_q.$$

Hensel's Lemma

Theorem (Hensel's Lemma)

Let $F(X) \in \mathcal{O}_q[X]$. Suppose that there exists an $\alpha_1 \in \mathcal{O}_q$ such that

$$F(\alpha_1) \equiv 0 \pmod{p}, \quad F'(\alpha_1) \not\equiv 0 \pmod{p}$$

Then there exists a unique $\alpha \in \mathcal{O}_{p^r}$ such that $\alpha \equiv \alpha_1 \pmod{p}$ and $F(\alpha) = 0$.

The set of all $(p^r - 1)$st root of unity in $\mathcal{O}_q$ together with 0

$$T_r = \{0, 1, \zeta, \cdots, \zeta^{p^r-2}\}$$

is a complete set of coset representatives for $\mathcal{O}_q/(p)$.v Thus, elements of $\mathcal{O}_q$ can be uniquely written as a formal infinite p-adic sum

$$c_0 + c_1 p + c_2 p^2 + \cdots + c_{e-1} p^{e-1} + \cdots$$

with $c_i \in T_r$.

Lattice of Galois rings

For each natural number e,

$$\mathcal{O}_q/(p^e) = \mathcal{O}_p[\zeta]/(p^e) = \mathbb{Z}_{p^e}[\zeta]/(p^e) = GR(p^e, r)$$

We have a projective systems

$$\begin{array}{ccccccc}
\mathbb{F}_{p^{rs}} & \simeq GR(p, rs) & \longleftarrow GR(p^2, rs) & \longleftarrow GR(p^3, rs) & \longleftarrow \cdots & \longleftarrow \mathcal{O}_{p^{rs}} \\
\vert & & \vert & \vert & & \vert \\
\mathbb{F}_{p^r} & \simeq GR(p, r) & \longleftarrow GR(p^2, r) & \longleftarrow GR(p^3, r) & \longleftarrow \cdots & \longleftarrow \mathcal{O}_{p^r} \\
\vert & & \vert & \vert & & \vert \\
\mathbb{F}_p & \simeq \mathbb{Z}_p & \longleftarrow \mathbb{Z}_{p^2} & \longleftarrow \mathbb{Z}_{p^3} & \longleftarrow \cdots & \longleftarrow \mathcal{O}_p
\end{array}$$

Codes over Galois rings

- *A linear code* over Galois ring $GR(p^e, r)$ of length n is a $GR(p^e, r)$-submodule of $GR(p^e, r)^n$
- A code $\mathcal{C}$ over $GR(p^e, r)$ of length n has a generator matrix permutation equivalent to the *standard form*

$$G = \begin{pmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} & \dots & A_{0,e-1} & A_{0e} \\ 0 & pI_{k_1} & pA_{12} & pA_{13} & \dots & pA_{1,e-1} & pA_{1e} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{23} & \dots & p^2 A_{2,e-1} & p^2 A_{2e} \\ . & . & . & . & \dots & . & . \\ 0 & 0 & 0 & 0 & \dots & p^{e-1} I_{k_{e-1}} & p^{e-1} A_{e-1,e} \end{pmatrix},$$

- A code with this matrix is said to be of *type*

$$(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}.$$

- k_0 is called a *free rank* and a code of type 1^k is called a *free code*.

Codes over Galois rings

- The *dual code* $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is

$$\mathcal{C}^{\perp} = \{\mathbf{v} \in GR(p^e, r)^n \mid \mathbf{v} \cdot \mathbf{w} = 0 \text{ for all } \mathbf{w} \in C\}.$$

- A code $\mathcal{C}$ is called *self-orthogonal* if $\mathcal{C} \subset \mathcal{C}^{\perp}$ and *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$.
- A code is called *decomposable* if the code is a direct sum of two or more codes. If a code is not decomposable, it is called *indecomposable*.
- A generator matrix of decomposable code is a block matrix of its subcodes.

$$G_1 \oplus G_2 = \begin{pmatrix} G_1 & O \\ O & G_2 \end{pmatrix}$$

Monomial transformation

- $\mathbb{D}^n$ is a set of diagonal matrices:

$$\mathbb{D}^n = \{\mathrm{diag}(\gamma_1, \gamma_2, \cdots, \gamma_n) \mid \gamma_i \in GR(p^e, r),\ \gamma_i^2 = 1\}.$$

- An element $\sigma \in S_n$ and $\gamma \in \mathbb{D}^n$ acts on $GR(p^e, r)^n$ by $\mathbf{v} = (v_{\sigma(1)}, v_{\sigma(2)}, \cdots, v_{\sigma(n)})\gamma$
- The group of all *monomial transformations* $\mathbb{T}^n$ is defined by

$$\mathbb{T}^n = \{\sigma\gamma \mid \gamma \in \mathbb{D}^n, \sigma \in S_n\}.$$

- Two self-dual codes $\mathcal{C}$ and $\mathcal{C}'$ are called *equivalent* if there exists an element $\tau \in \mathbb{T}^n$ such that $\mathcal{C}\tau = \mathcal{C}'$.

Automorphisms of $\mathcal{C}$

- Aut($\mathcal{C}$) is the group of all automorphisms of $\mathcal{C}$.
- *Permutation parts* of $\mathcal{C}$ is $p(\mathcal{C}) = \{\sigma \mid \sigma\gamma \in \mathrm{Aut}(\mathcal{C})\}$
- *sign parts* of $\mathcal{C}$ is defined by $s(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}) \cap \mathbb{D}$.
- $|s(\mathcal{C})||p(\mathcal{C})| = |Aut(\mathcal{C})|$.
- We denote a automorphism group of $\mathcal{C}$ by

$$|s(\mathcal{C})|.p(\mathcal{C})$$

or we just denote the order as

$$|s(\mathcal{C})|.|p(\mathcal{C})|$$

The number of self-orthogonal codes over $GR(p, r)$

Propostion (V. Pless, 1965)

Let $\sigma_q(n, k)$ be the number of self-orthogonal codes of length n and dimension k over $\mathbb{F}_q$, where $q = p^m$ for some prime p and an integer m. Then:

1. If n is even, q even,

$$\sigma_q(n, k) = \frac{(q^{n-k} - 1)\prod_{i=1}^{k-1}(q^{n-2i} - 1)}{\prod_{i=1}^{k}(q^i - 1)},$$

2. If n is even, q odd,

$$\sigma_q(n, k) = \frac{(q^{n-k} - 1 - \eta((-1)^{n/2})(q^{n/2-k} - q^{n/2}))\prod_{i=1}^{k-1}(q^{n-2i} - 1)}{\prod_{i=1}^{k}(q^i - 1)}.$$

The term $\prod_{i=1}^{k-1}(q^{n-2i} - 1)$ is to be 1 when $k = 1$ and $\sigma_q(n, 0) = 1$

The number of self-orthogonal codes over $GR(p^e, r)$

Next theorem is a generalization of the results on the number of self-dual codes over $\mathbb{Z}_{p^s}$, which are published consecutively by Gaborit (1996), Nagata et al.(2008, 2009), Balmaceda et al. (2008).

Theorem

The number of distinct self-dual codes over a Galois ring $GR(p^2, r)$ for odd prime p is given by

$$N_{p^2,2}(n) = \sum_{0 \le k \le \lfloor n/2 \rfloor} \sigma_{p^r}(n,k)(p^r)^{k(k-1)/2}.$$

Particularly, the number of distinct free self-dual codes over a Galois ring $GR(p^e, r)$ for odd prime p is given by

$$\#_{p^e,r}(n) = \sigma_{p^r}\left(n, \frac{n}{2}\right) p^{(e-1)r\frac{n(n-2)}{8}}.$$

The number of self-orthogonal codes over $GR(p^e, r)$

Sketch of proof

A self-orthogonal code $\mathcal{C}_0$ over $GR(p, r)$ with a generator matrix

$$G_0 = \begin{pmatrix} I_k & A_1 & B_1 \end{pmatrix}$$

is lifted to a self-dual code over $GR(p^2, r)$ with generator matrices

$$G = \begin{pmatrix} I_k & A_1 & B_1 + pB_2 \\ O & pI_{k_1} & pC_1 \end{pmatrix}$$

Then, C_1 is determined completely by G_0 and B_2 is chosen among $(p^r)^{k(k-1)/2}$

Possible length of self-dual codes over $GR(p^e, r)$

Theorem (S.T. Dougherty et al., 2009)

1. *If e is even, then there exist self-dual codes over $GR(p^e, r)$ for all lengths.*
2. *If e is odd and the residue field $GF(p^r)$ has characteristic 1 (mod 4), then there exist self-dual codes over $GR(p^e, r)$ for all even lengths.*
3. *If e is odd and the residue field $GF(p^r)$ has characteristic 3 (mod 4), then there exist self-dual codes over $GR(p^e, r)$ for all even lengths a multiple of 4.*

Free self-dual codes over $GR(p^e, r)$ of length 4

Theorem

Let $p \neq 2, 3$ and A_4 be the alternating subgroup of S_4. Then the free self-dual code $\mathcal{C}$ with generator matrix (denoted by (a, b))

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix}$$

over $GR(p^e, r)$ is one of the following four classes :

Class	(a, b)	$\mathrm{Aut}(\mathcal{C})$
(i)	$a^2 + 1 = 0,\ b = 0$	$4.\langle(13), (1234)\rangle$
(ii)	$a^6 = 1,\ a \neq \pm 1$	$2.A_4$
(iii)	$a = 1,\ b^2 + 2 = 0$	$2.\langle(13), (1234)\rangle$
(iv)	*else*	$2.\langle(12)(34), (13)(24)\rangle$

Codes from classes (i), (ii), (iii) are unique, up to equivalence.

Self-dual codes over $GR(p^e, r)$ of type $1^2 p^0$

Theorem

Let N_1, N_2, N_3, N_4 be the number of class (i), (ii), (iii), (iv) self-dual codes over $GR(p^e, r)$ of length 4 and rank 2, respectively.

$p^r \pmod{24}$	N_1	N_2	N_3	N_4
1	1	1	1	$\frac{p^{er}+p^{er-r}-26}{24}$
5	1	0	0	$\frac{p^{er}+p^{er-r}-6}{24}$
7	0	1	0	$\frac{p^{er}+p^{er-r}-8}{24}$
11	0	0	1	$\frac{p^{er}+p^{er-r}-12}{24}$
13	1	1	0	$\frac{p^{er}+p^{er-r}-14}{24}$
17	1	0	1	$\frac{p^{er}+p^{er-r}-18}{24}$
19	0	1	1	$\frac{p^{er}+p^{er-r}-20}{24}$
23	0	0	0	$\frac{p^{er}+p^{er-r}}{24}$

Self-dual codes over $GR(p^e, r)$ of type $1^2 p^0$

Sketch of proof

Compute solutions of each polynomial over $GR(p, 1)[x]$; $x^2 + 1 = 0$,$x^6 = 1$ and $x^2 + 2 = 0$. Then by Hensel's lemma, we get the solutions of each polynomial over $GR(p^e, r)[x]$. Checking the mass formula, we obtain the number of inequivalent codes of each class.

For example, we checked that

- $5^3 \equiv 5 \pmod{24}$. Thus over $GR(5^2, 3)$ there are unique code of class (i) and $(5^6 + 5^3 - 6)/24 = 656$ codes of class (iv).
- $7^4 \equiv 1 \pmod{24}$. thus over $GR(7, 4)$ there are unique codes of class (i),(ii),(iii) and $(7^4 + 7^0 - 26)/24 = 99$ codes of class (iv).
- $7^3 \equiv 7 \pmod{24}$. Thus over $GR(7^2, 3)$ there are unique code of class (ii) and $(7^6 + 7^3 - 8)/24 = 4916$ codes of class (iv).

Self-dual codes over $GR(p, 1)$

p	(i)	(ii)	(iii)	(iv)
5	$(2, 0)$			
7		$(2, 3)$		
11			$(1, 3)$	
13	$(5, 0)$	$(3, 4)$		
17	$(4, 0)$		$(1, 7)$	
19		$(7, 8)$	$(1, 6)$	
23				$(2, 8)$
29	$(12, 0)$			$(2, 13)$
31		$(5, 6)$		$(4, 13)$
37	$(6, 0)$	$(10, 11)$		$(3, 8)$
41	$(9, 0)$		$(1, 11)$	$(2, 6)$
43		$(6, 7)$	$(1, 16)$	$(2, 9)$
47				$(2, 18), (3, 15)$
53	$(23, 0)$			$(3, 19), (4, 6)$
59			$(1, 23)$	$(3, 7), (6, 9)$

Free self-dual codes over $GR(p^2, 1)$

p	(i)	(ii)	(iii)	(iv)
3			$(1, 4)$	
5	$(7, 0)$			$(7, 5)$
7		$(18, 19)$		$(2, 17), (4, 9)$
11			$(1, 19)$	5 codes
13	$(70, 0)$	$(22, 23)$		7 codes
17	$(38, 0)$		$(1, 24)$	12 codes
19		$(68, 69)$	$(1, 63)$	15 codes
23				23 codes
29	$(41, 0)$			36 codes
31		$(439, 440)$		41 codes
37	$(117, 0)$	$(581, 582)$		58 codes
41	$(378, 0)$		$(1, 71)$	71 codes

Table: Self-dual codes over $GR(p^2, 1)$ of type $1^2 p^0$.

Self-dual codes over $GR(p,2)$ of length 4

p	(i)	(ii)	(iii)	(iv)
5	$(2,0)$	$(2\zeta+1, 2\zeta+2)$	$(1, 2\zeta+4)$	
7	$(\zeta+3, 0)$	$(2,3)$	$(1, 3\zeta+2)$	1 code
11	$(4\zeta+3, 0)$	$(\zeta+3, \zeta+4)$	$(1,3)$	4 codes
13	$(5,0)$	$(3,4)$	$(1, 4\zeta+11)$	6 codes
17	$(4,0)$	$(5\zeta+14, 5\zeta+15)$	$(1,7)$	11 codes
19	$(5\zeta+7, 0)$	$(7,8)$	$(1,6)$	14 codes
23	$(11\zeta+12, 0)$	$(4\zeta+7, 4\zeta+8)$	$(1, 9\zeta+14)$	21 codes
29	$(12,0)$	$(14\zeta+8, 14\zeta+9)$	$(1, 7\zeta+26)$	34 codes
31	$(4\zeta+27, 0)$	$(5,6)$	$(1, \zeta+30)$	39 codes
37	$(6,0)$	$(10,11)$	$(1, 6\zeta+25)$	56 codes
41	$(9,0)$	$(19\zeta+12, 19\zeta+13)$	$(1,11)$	69 codes
43	$(4\zeta+41, 0)$	$(6,7)$	$(1,16)$	76 codes
47	$(23\zeta+24, 0)$	$(3\zeta+20, 3\zeta+21)$	$(1, 20\zeta+27)$	91 codes
53	$(23,0)$	$(24\zeta+31, 24\zeta+32)$	$(1, 23\zeta+7)$	116 codes
59	$(3\zeta+28, 0)$	$(13\zeta+52, 13\zeta+53)$	$(1,23)$	144 codes

Table: Self-dual codes of length 4 over $GR(p,2)$

Free self-dual codes over $GR(2,2)$ and $GR(4,2)$

- There exist two inequivalent self-dual codes over $GR(2,2)$
  $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} : \langle (13), (1234) \rangle,$
  $\begin{pmatrix} 1 & 0 & \zeta & 1+\zeta \\ 0 & 1 & 1+\zeta & \zeta \end{pmatrix} : A_4.$
- There exist 2 inequivalent free codes over $GR(4,2)$,
  $\begin{pmatrix} 1 & 0 & \zeta & \zeta+1 \\ 0 & 1 & 3\zeta+3 & \zeta \end{pmatrix} : 2.A_4,$
  $\begin{pmatrix} 1 & 0 & \zeta & \zeta+1 \\ 0 & 1 & 3\zeta+1 & \zeta \end{pmatrix} : 2.\langle (12)(34), (14)(23) \rangle.$
- $h(X) = X^2 + X + 1 \in \mathbb{Z}_{2^e}[X]$.

Free self-dual codes over $GR(3,2)$ and $GR(3^2,2)$

- There exist two inequivalent self-dual codes over $GR(3,2)$
  $\begin{pmatrix} 1 & 0 & 1+\zeta & 0 \\ 0 & 1 & 0 & 1+\zeta \end{pmatrix}$: $4.\langle(13),(1234)\rangle$,
  $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix}$: $2.S_4$.
- There exist 5 inequivalent free codes over $GR(9,2)$,
  $\begin{pmatrix} 1 & 0 & 1+\zeta & 0 \\ 0 & 1 & 0 & 1+\zeta \end{pmatrix}$ of class (i) since $(1+\zeta)^2+1=0$,
  $\begin{pmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 5 & 1 \end{pmatrix}$ of class(iii) since $4^2+2=0$
  $(1+\zeta,3\zeta),(1+\zeta,3),(3\zeta+1,6\zeta+4)$ of class (iv).
- $h(X)=X^2+2X+2\in\mathbb{Z}_{3^e}[X]$.

Free Self-dual codes over $GR(p^2, 2)$

p	(i)	(ii)	(iii)	(iv)
3	$(1+\zeta, 0)$		$(1, 4)$	3
5	$(7, 0)$	$(6+22\zeta, 7+22\zeta)$	$(5\zeta, 7)$	26
7	$(29\zeta+38, 0)$	$(30, 31)$	$(1, 45\zeta+37)$	101
11	$(92\zeta+80, 0)$	$(89\zeta+69, 89\zeta+70)$	$(1, 19)$	614
13	$(70, 0)$	$(146, 147)$	$(1, 43\zeta+89)$	1196
17	$(38, 0)$	$(226\zeta+218, 226\zeta+219)$	$(1, 24)$	3491
19	$(252\zeta+102, 0)$	$(68, 69)$	$(1, 63)$	5444
23	$(34\zeta+357, 0)$	$(441\zeta+398, 441\zeta+399)$	$(1, 515\zeta+382)$	11681

Table: Self-dual codes of freerank 2 and length 4 over $GR(p^2, 2)$

Types of self-dual codes over $GR(p^2, r)$ of length 4

1. Type of $1^0 p^4$ (Trivial code).

$$pI_4 : 16.S_4$$

2. Type of $1^2 p^0$ (Free code).

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix}$$

3. Type of $1^1 p^2$.

$$\begin{pmatrix} 1 & a & b & c \\ 0 & p & 0 & -\frac{a}{c}p \\ 0 & 0 & p & -\frac{b}{c}p \end{pmatrix}$$

Note that there are more types of codes over $GR(p^e, r)$ as e and n grows.

Mass formula of self-dual codes over $GR(p^2, 1)$ of length 4

$$\begin{aligned} N_{p^2,1}(4) &= \sigma_p(4,0)p^0 + \sigma_p(4,1)p^0 + \sigma_p(4,2)p^1 \\ &= 1 + (p+1)^2 + 2(p+1)p \\ &= 3p^2 + 4p + 2 \\ &= \sum_{\mathcal{C}} \frac{2^4 \times 4!}{|\operatorname{Aut}(\mathcal{C})|} \end{aligned}$$

- # of the trivial self-dual code pI_4 : $\sigma_p(4,0)p^0 = 1$
- # of the self-dual codes of type $1^1 p^2$: $\sigma_p(4,1)p^0 = (p+1)^2$
- # of the self-dual codes of type 1^2 : $\sigma_p(4,2)p^0 = 2(p+1)p$

Self-dual codes over $GR(p^2, r)$ of free rank 1

Lemma (Park and Choi, 2017)

Let p be a odd prime. Then a self-dual code C over $GR(p^2, r)$ of free rank 1 of length n has a generator matrix in the standard form ;

$$\begin{pmatrix} 1 = a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n + pb_1 \\ 0 & p & 0 & \cdots & 0 & pb_2 \\ 0 & 0 & p & \cdots & 0 & pb_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & p & pb_{n-1} \end{pmatrix} \tag{1}$$

where a_i's, b_j's are in $\mathcal{T}$ and

1. *$a_n + pb_1$ is a unit in $GR(p^2, r)$,*
2. *$b_k = -a_k a_n^{-1}$ for $k \geq 2$.*

$(1, a_2, a_3, \cdots, a_n) \in GR(p, r)^n$ of rank 1 determines the self-dual codes over $GR(p^2, r)$ of free rank 1.

Self-dual codes over $GR(p^2, r)$ of free rank 1

Corollary

There is an one-to-one correspondence upto equivalence between the set of self-dual codes over $GR(p^2, r)$ of free rank 1 and the set of self-orthogonal codes over $GR(p, r)$ of rank 1.

Corollary

Let $\mathcal{C}$ be a self-dual code $GR(p^2, r)$ of free rank 1 and $Res(\mathcal{C})$ the residue code of $\mathcal{C}$. Then, $Aut(\mathcal{C}) = Aut(Res(\mathcal{C}))$.

Self-dual codes over $GR(p^2, r)$ of free rank 1

Theorem (Park and Choi, 2017)

Let C be a code over $GR(p, r)$ of rank 1 of length 4 with generator matrix $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}$ and $(ij), (ijk)$ be elements in S_4 and $\omega \in GR(p, r)$ such that $\omega^6 = 1, \omega \neq \pm 1$.

1. *If $a_i^2 = a_j^2$, then $(ij) \in p(C)$.*
2. *If $(ij) \in p(C)$ and $a_i^2 \neq a_j^2$, then $a_i^2 = -a_j^2$ and all the other elements except a_i and a_j are zero.*
3. *If $(ijk) \in p(C)$ and $\langle (ijk), (ij) \rangle \not\subseteq p(C)$, then $a_j^2 = \omega^2 a_i^2$, $a_k^2 = \omega^4 a_i^2$ and the other element except a_i, a_j and a_k is zero.*
4. *If p is odd and the number of a_i's which are zero is m, then $|s(C)| = 2^{1+m}$.*

Self-dual codes over $GR(p^2, 1)$ of type $1^1 p^2$

Theorem (Park and Choi, 2017)

Let $p \neq 2, 3$. Then self-dual codes (a, b, c) of rank 3 is equivalent to one of the following inequivalent codes :

Class	(a, b, c)	$\mathrm{Aut}((a, b, c))$
(i)	$a = b = 0$	$8.\langle(14), (23)\rangle$
(ii)	$b = 0$, $a^6 \equiv 1$ *and* $a^2 \neq 1, c^2 \neq 1$	$4.\langle(124)\rangle$
(iii)	$a^2 = 1, b = 0$	$4.\langle(12)\rangle$
(iv)	$b = 0, a \neq 0, a^3 \neq \pm 1, c^3 \neq \pm 1, a^2 \neq c^2$	$4.\langle(1)\rangle$
(v)	$a^2 \equiv 1 \neq b^2 \equiv c^2$	$2.\langle(1324), (12)\rangle$
(vi)	$a^2 \equiv b^2 \equiv 1$	$2.S_3$
(vii)	$a^2 \equiv 1, b^2 \neq \pm 1, c^2 \neq \pm 1$	$2.S_2$
(viii)	$a^2 \equiv -1, b^2 \neq \pm 1$ *and* $b^4 \neq -1$	$2.\langle(1), (14)(23)\rangle$
(ix)	$a^2 \equiv -1, b^2 \neq \pm 1$ *and* $b^4 \equiv -1$	$2.\langle(1243)\rangle$
(x)	$1, a^2, b^2, c^2$ *are distinct,* $a^2, b^2, c^2 \neq -1$	$2.\langle(1)\rangle$

Self-dual codes over $GR(p^2, 1)$ of type $1^1 p^2$

Theorem (Park and Choi, 2017)

For $p \neq 2, 3$, let $N_1, N_2, \cdots, N_{10}$ be the number of class (i), (ii), $\cdots$, (x) self-dual codes over $GR(p^2, 1)$, respectively. These numbers are determined as follows.

$p(24)$	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
1	1	1	1	$\frac{p-25}{24}$	1	1	$\frac{p-17}{8}$	$\frac{p-9}{8}$	1	$\frac{(p+1)^2-28p+216}{192}$
5	1	0	0	$\frac{p-5}{24}$	1	0	$\frac{p-5}{8}$	$\frac{p-5}{8}$	0	$\frac{(p+1)^2-28p+104}{192}$
7	0	1	0	$\frac{p-7}{24}$	0	1	$\frac{p-7}{8}$	0	0	$\frac{(p+1)^2-16p+48}{192}$
11	0	0	1	$\frac{p-11}{24}$	0	0	$\frac{p-3}{8}$	0	0	$\frac{(p+1)^2-16p+32}{192}$
13	1	1	0	$\frac{p-13}{24}$	1	1	$\frac{p-13}{8}$	$\frac{p-5}{8}$	0	$\frac{(p+1)^2-28p+168}{192}$
17	1	0	1	$\frac{p-17}{24}$	1	0	$\frac{p-9}{8}$	$\frac{p-9}{8}$	1	$\frac{(p+1)^2-28p+152}{192}$
19	0	1	1	$\frac{p-19}{24}$	0	1	$\frac{p-11}{8}$	0	0	$\frac{(p+1)^2-16p+96}{192}$
23	0	0	0	$\frac{p+1}{24}$	0	0	$\frac{p+1}{8}$	0	0	$\frac{(p+1)^2-16p-16}{192}$

Self-dual codes over $GR(p^2, 1)$ of type $1^1 p^2$

- There exists unique self-dual code over $GR(4, 1)$ of type $1^1 p^2$.
  $(1, 1, 1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}$
  with automorphism S_4. (a.k.a. the Klemm code)
- There exists unique self-dual code over $GR(9, 1)$ of type $1^1 p^2$.
  $(1, 0, 4) = \begin{pmatrix} 1 & 1 & 0 & 4 \\ 0 & 3 & 0 & 6 \\ 0 & 0 & 3 & 0 \end{pmatrix}$
  with automorphism $4.\langle (12), (124) \rangle$

Self-dual codes over $GR(p^2, 1)$ of type $1^1 p^2$

p^2	(i)	(ii)	(iii)	(iv)	(v)
5^2	$(0, 0, 7)$				$(1, 2, 12)$
7^2		$(2, 0, 17)$			
11^2			$(1, 0, 19)$		
13^2	$(0, 0, 70)$	$(3, 0, 43)$			$(1, 5, 34)$
17^2	$(0, 0, 38)$		$(1, 0, 24)$		$(1, 4, 72)$
19^2		$(7, 0, 46)$	$(1, 0, 63)$		
23^2				$(2, 0, 169)$	
29^2	$(0, 0, 41)$			$(2, 0, 71)$	$(1, 12, 70)$
31^2		$(5, 0, 161)$		$(4, 0, 142)$	
37^2	$(0, 0, 117)$	$(10, 0, 248)$		$(3, 0, 510)$	$(1, 6, 228)$

Table: Cases 1 to 5 of self-dual codes of type $1^1 p^2$ over $GR(p^2, 1)$

Self-dual codes over $GR(p^2, 1)$ of type $1^1 p^2$

p^2	(vi)	(vii)	$(viii)$	(ix)	(x)
7^2	$(1, 1, 12)$				
11^2		$(1, 2, 29)$			
13^2	$(1, 1, 45)$		$(5, 6, 48)$		
17^2		$(1, 6, 110)$	$(4, 5, 139)$	$(4, 8, 53)$	
19^2	$(1, 1, 137)$	$(1, 5, 50)$			$(2, 3, 104)$
23^2		$(1, 3, 239)$ $(1, 6, 56)$ $(1, 7, 100)$			$(2, 4, 212)$
29^2		$(1, 2, 136)$ $(1, 6, 181)$ $(1, 11, 333)$	$(12, 13, 47)$ $(12, 14, 325)$ $(12, 19, 149)$		$(3, 5, 96)$
31^2	$(1, 1, 82)$	$(1, 2, 98)$ $(1, 3, 446)$ $(1, 9, 107)$			$(2, 44, 234)$ $(2, 9, 289)$ $(3, 8, 53)$
37^2	$(1, 1, 206)$	$(1, 3, 64)$ $(1, 5, 618)$ $(1, 9, 425)$	$(6, 7, 143)$ $(6, 8, 248)$ $(6, 9, 609)$ $(6, 12, 298)$		$(2, 5, 231)$ $(2, 13, 97)$ $(3, 4, 495)$

Table: Case 5 to 10 of self-dual codes of type $1^1 p^2$ over $GR(p^2, 1)$

Self-dual codes over $GR(p^2, 2)$ of type $1^2 p^0$

$$\begin{aligned} N_{p^2,2}(4) &= \sigma_{p^2}(4,0)p^0 + \sigma_{p^2}(4,1)p^0 + \sigma_{p^2}(4,2)(p^2)^1 \\ &= 1 + (p^2+1)^2 + 2(p^2+1)p^2 \\ &= 3p^4 + 4p^2 + 2 \end{aligned}$$

- For example, $3 \cdot 23^4 + 4 \cdot 23^2 + 2 = 841,641$ self-dual codes over $GR(23^2, 2)$ exist.
- A self-dual code over $GR(23^2, 2)$ has $23^8 = 78,310,985,281$ codewords.
- We show that there are $13,228$ equivalent classes.

Self-dual codes over $GR(p^2, 2)$ of type $1^1 p^2$

Theorem

For $p \neq 2, 3$, let $N_1, N_2, \cdots, N_{10}$ be the number of class (i), (ii), $\cdots$, (x) self-dual codes over $GR(p^2, 2)$, respectively. These numbers are determined as follows.

Class	N_4	N_7	N_8	N_{10}
#	$\frac{p^2-25}{24}$	$\frac{p^2-17}{8}$	$\frac{p^2-9}{8}$	$\frac{(p^2+1)^2-28p^2+216}{192}$

and $N_1 = N_2 = N_3 = N_5 = N_6 = N_9 = 1$

Self-dual codes over $GR(p^2, 2)$ of type $1^1 p^2$

Note that there exist two self-dual code over $GR(4, 2)$ of type $1^1 p^2$.

$$(1, 1, 1) : 8.S_4,$$

$$(1, 1, 1 + 2\zeta) : 8.S_4,$$

and there exist four self-dual code over $GR(9, 2)$ of type $1^1 p^2$.

$$(1, 0, 4) : 4.B_6,$$

$$(0, 0, \zeta + 1) : 8.B'_4,$$

$$(1, \zeta + 1, \zeta + 1) : 2.B'_8,$$

$$(\zeta, \zeta + 1, \zeta + 2) : 2.B_2.$$

Self-dual codes over $GR(p^2, 2)$ of type $1^1 p^2$

p^2	(v)	(vi)	(vii)	(viii)
5^2	$(1, 2, 12)$	$(1, 1, 6\zeta + 12)$	$(1, 2\zeta, 2\zeta + 3)$	$(2, \zeta, 2\zeta), (2, \zeta + 1, 2\zeta + 2)$
7^2	$(1, \zeta + 3, 8\zeta + 24)$	$(1, 1, 37)$	$(1, 3, 23\zeta + 20)$ $(1, \zeta + 2, 30\zeta + 10)$ $(1, \zeta + 4, 30\zeta + 23)$ $(1, 3\zeta + 1, 24\zeta + 24)$	$(2, \zeta + 3, 23\zeta + 20)$ $(\zeta, \zeta + 3, 17\zeta + 31)$ $(\zeta + 1, \zeta + 3, 30\zeta + 28)$ $(\zeta + 2, \zeta + 3, 43\zeta + 39)$ $(\zeta + 3, 2\zeta + 2, 45\zeta + 35)$
11^2	$(1, 4\zeta + 3, 59\zeta + 36)$	$(1, 1, 57\zeta + 18)$	13 codes	14 codes
13^2	$(1, 5, 135)$	$(1, 1, 45)$	19 codes	20 codes
17^2	$(1, 4, 72)$	$(1, 1, 126\zeta + 141)$	34 codes	35 codes
19^2	$(1, 11\zeta + 12, 57\zeta + 173)$	$(1, 1, 137)$	43 codes	44 codes
23^2	$(1, 11\zeta + 12, 57\zeta + 173)$	$(1, 1, 353\zeta + 268)$	64 codes	65 codes

Table: Self-dual codes of type $1^1 p^2$ over $GR(p^2, 2)(p < 29)$

Self-dual codes over p-adic numbers of length 4

The preivous results can be extended for the self-dual codes over p-adic integer rings Z_{p^∞} and, hopefully, over q-adic integer rings.

Theorem (Dougherty and Park, 2006)

If $\mathcal{C}$ is a self-dual code of length n over $\mathbb{Z}_{p^\infty}$ then C has type $1^{\frac{n}{2}}$.

With this theorem and Helsel's lemma, we can see that there exist four classes of self-dual codes over $\mathbb{Z}_{p^\infty}$ of length 4 as same as the case over $\mathbb{Z}_p$. Especially, there are infinitely many inequivalent codes of class (iv).

Examples of self-dual codes over $\mathbb{Z}_{p^\infty}$

- Over $\mathbb{Z}_{3^\infty}$ there exists a unique self-dual codes of class (iii)

$$\begin{pmatrix} 1 & 0 & 1 & b \\ 0 & 1 & -b & 1 \end{pmatrix}$$

where $b^2 + 2 = 0$.
$b = 112212\cdots_{(3)} = 1 + 1\cdot 3 + 2\cdot 3^2 + 2\cdot 3^5 + 1\cdot 3^7 + 2\cdot 3^{11} + \cdots$

- Over $\mathbb{Z}_{7^\infty}$ there exists a unique self-dual code of class (ii)

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix}$$

where $a^2 + b^2 + 1 = 0$, $a^6 = 1$ and $a^2 \neq 1$.

Self-dual codes over $\mathbb{Z}_{73^\infty}$ of length 4

$p = 73$ is the smallest prime which gives examples of self-dual codes over $\mathbb{Z}_{p^\infty}$ in all classified classes.

- Unique free code of Class (i)

  $a = (27, 62, 28, 56, 58, 52, 51, 21, 11, 56, 39, 27, 47, 1, 67, 3, 68, 25, \dots)$
  $b = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \dots)$

- Unique free code of Class (ii)

  $a = (8, 30, 54, 57, 49, 56, 69, 62, 19, 51, 66, 22, 51, 18, 2, 40, 14, 48, \dots)$
  $b = (9, 30, 54, 57, 49, 56, 69, 62, 19, 51, 66, 22, 51, 18, 2, 40, 14, 48, \dots)$

- Unique free code of Class (iii)

  $a = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \dots)$
  $b = (12, 6, 41, 58, 55, 49, 36, 27, 5, 35, 34, 70, 30, 27, 13, 39, 25, 63, \dots)$

- One of infinitely many free codes of Class (iv)

  $a = (17, 60, 35, 42, 26, 40, 66, 52, 39, 29, 60, 45, 29, 37, 4, 7, 29, 23, \dots)$
  $b = (32, 34, 2, 9, 29, 16, 42, 56, 67, 27, 33, 58, 38, 22, 69, 47, 47, 12, \dots)$

Here a p-adic integer $\sum_{i=0}^{\infty} a_i p^i$ is expressed as an infinite sequence (a_i).

Free self-dual codes of length 6 - decomposable cases

Decomposable free self-dual codes $\mathcal{C}$ of length 6 with generator matrix (denoted by $\mathscr{D}(a, b, c)$)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & 0 & b & c & 0 \\ 0 & 0 & 1 & -c & b & 0 \end{pmatrix}$$

over $GR(p, 1)$ is one of the following four classes :

Class	$\mathscr{D}(a, b, c)$	$\lvert s(\mathcal{C})\rvert.\lvert p(\mathcal{C})\rvert$
(i)	$a^2 + 1 = 0,\ c^2 + 1 = 0, b = 0$	8.48
(ii)	$a^2 + 1 = 0, b^6 = 1, b^2 \neq 1$	4.24
(iii)	$a^2 + 1 = 0, b = 1, c^2 + 2 = 0$	4.16
(iv)	else	4.8

Codes from classes (i), (ii), (iii) are unique, up to equivalence.

Free self-dual codes of length 6 - decomposable cases

The number of class (i), (ii), (iii), (iv) decomposable free self-dual codes $\mathcal{C}$ over $GR(p^e, r)$ of length 6

$p^r \pmod{24}$	N_1	N_2	N_3	N_4
1	1	1	1	$\frac{p^{er}+p^{er-r}-26}{24}$
5	1	0	0	$\frac{p^{er}+p^{er-r}-6}{24}$
13	1	1	0	$\frac{p^{er}+p^{er-r}-14}{24}$
17	1	0	1	$\frac{p^{er}+p^{er-r}-18}{24}$

Free self-dual codes of length 6 -Indecomposable cases

Propostion

Let

$$G = (I_n \quad A)$$

be a standard generator matrix of a self-dual code over $GR(p, r)$ of length 6. Then, G is decomposable iff A has at least two zero elements.

Sketch of proof

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & 0 & b & c & d \\ 0 & 0 & 1 & e & f & g \end{pmatrix} \Rightarrow 1 + a^2 = 0, ad = ag = 0 \text{ Thus, } d = g = 0.$$

Similarly, we can check all cases and 'only if' part is clear.

Thus indecomposable code has at most 1 zero in A. Indecomposable codes of length 6 with no zero in A are all MDS.

Free self-dual codes of length 6

Propostion

Let $\mathcal{C}$ be a self-dual code over $GR(p, r)$ with

$$\begin{pmatrix} 1 & 0 & 0 & 0 & b & c \\ 0 & 1 & 0 & b & -c^2 i & bci \\ 0 & 0 & 1 & c & bci & -b^2 i \end{pmatrix}$$

where $i^2 + 1 = 0$. Then, $(13)(24)(36) \in \mathrm{Aut}(\mathcal{C})$.
If $b = 1$, then there is unique $\mathcal{C}$ with $|\mathrm{Aut}(\mathcal{C})| = 2.8$ for $p \equiv 1, 17 \pmod{24}$.

For example, over $GR(89, 1)$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 40 \\ 0 & 1 & 0 & 1 & 21 & 64 \\ 0 & 0 & 1 & 40 & 64 & 34 \end{pmatrix}$$

and over $GR(97, 1)$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 17 \\ 0 & 1 & 0 & 1 & 44 & 83 \\ 0 & 0 & 1 & 17 & 83 & 75 \end{pmatrix}$$

Free self-dual codes of length 6

Propostion

Let $\mathcal{C}$ be a self-dual code over $GR(p, r)$ with

$$\begin{pmatrix} 1 & 0 & 0 & 1 & i & i \\ 0 & 1 & 0 & i & a & -a-1 \\ 0 & 0 & 1 & i & -a-1 & a \end{pmatrix}$$

Then, $|\mathrm{Aut}(\mathcal{C})| = 2.24$.

For example, over $GR(89, 1)$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 34 & 34 \\ 0 & 1 & 0 & 34 & 27 & 61 \\ 0 & 0 & 1 & 34 & 61 & 27 \end{pmatrix}$$

and over $GR(97, 1)$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 22 & 22 \\ 0 & 1 & 0 & 22 & 37 & 59 \\ 0 & 0 & 1 & 22 & 59 & 37 \end{pmatrix}$$

Rigid codes

If a codes has a trivial automorphism group, it is called a rigid code. $p = 53$ is the smallest prime which gives examples of rigid code over $GR(p, r)$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 19 \\ 0 & 1 & 0 & 4 & 25 & 10 \\ 0 & 0 & 1 & 6 & 1 & 11 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 10 \\ 0 & 1 & 0 & 12 & 36 & 34 \\ 0 & 0 & 1 & 15 & 17 & 11 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 8 & 26 \\ 0 & 1 & 0 & 16 & 5 & 6 \\ 0 & 0 & 1 & 22 & 49 & 33 \end{pmatrix}$$

Thank you!