# Enumeration of codes via Hecke rings over a class of Euclidean domains *

松井 一 (Hajime Matsui) †

## Introduction

誤り訂正符号（以下，単に符号と言う）は C.E. Shannon の論文 [3] (1948) に起源を持つとされる．現在では符号は，CD，DVD，デジタル放送，QR コードなど，デジタル情報を扱うありとあらゆるところで用いられている．符号には大きく分けてブロック符号と畳み込み符号に分けられ [1]，畳み込み符号も実用上重要な符号であるが，本発表ではブロック符号のみを扱う．さて，[3] においては，符号は主として存在のみが示されていた．最初の符号は，恐らく $[n = 7, k = 4]$ Hamming 符号であろう（1950 頃）．その後，Golay 符号，BCH 符号，Reed–Solomon 符号と巡回符号が続き，2000 年代に入ってからは，低密度パリティ検査（low-density parity-check, LDPC）符号が，符号の訂正能力の限界である Shannon 限界にほぼ達することが報告された (2006)．

本発表では，符号のある代数的側面について取り上げる．通常，符号と言えば，有限体（実用的には特に標数 2 のもの）上のものを扱うことが多いが，本発表では，3 つのユークリッド整域（有限体上の 1 変数多項式環，有理整数環，ガウス整数環）を扱い，これらのユークリッド整域の剰余環に対する有限直積の部分加群と一致する符号を対象とする．他では見られない特長として，本発表ではある特別な生成行列を定義し，個々の符号に対して一意に定まることを示す．また，ある行列に対しそれが生成行列であるような符号が存在するかという問題に対し，ある種の恒等式（identical equation）が成り立つかどうかによって答えることができることを示す．さらに，Hecke 環を応用することにより，ある種の生成行列の母関数を用いた数え上げおよび列挙ができることを示す．本発表の結果は，あるクラスの符号の構成・分類・数え上げに応用があり，また LDPC 符号の構成も可能である．

## Contents



*第 31 回代数的組合せ論シンポジウム（東北大学，2014 年 6 月 19–20 日）報告集
†豊田工業大学工学部，〒 468 8511 名古屋市天白区久方 2–12 1，E-mail: matsui@toyota-ti.ac.jp

# 1 Background and motivation

- C.E. Shannon [3], "A mathematical theory of communication" (1948)
- Cyclic codes, pseudo-cyclic (PC) codes, low-density parity-check (LDPC) codes, $\cdots$
- Generator and parity-check polynomial matrices of **quasi-cyclic (QC) codes** and their identical equations (Lally–Fitzpatrick [2], 2001)
- Generator and parity-check polynomial matrices of **generalized quasi-cyclic (GQC) codes** and their identical equations (Van–Matsui–Mita [8], 2009), (Matsui [5], 2010)
- (Today) Generator matrices of **generalized pseudo-cyclic (GPC) codes** and their identical equations (Matsui [7], 2014)

$(\mathbb{F}_q[x] \longrightarrow \mathbb{Z})$

- (Today) Generator matrices of **generalized integer codes** and their identical equations (Matsui [6], 2014)

$(\mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{-1}])$

- (Today) Generator matrices of **codes over Gaussian integers** and their identical equations
- (Future works) Application to searching and constructing efficient codes for various classical and/or quantum channels

$q$: a rational prime power, $\mathbb{F}_q$: $q$-element finite field,
$\mathbb{F}_q[x]$: ring of one-variable polynomials over $\mathbb{F}_q$, $\langle d \rangle$: ideal generated by $d$

Cyclic codes: ideals in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$

QC codes: submodules in $(\mathbb{F}_q[x]/\langle x^n - 1 \rangle)^l$

GQC codes: submodules in $\bigoplus_{i=1}^{l} \mathbb{F}_q[x]/\langle x^{n_i} - 1 \rangle$

Pseudo-cyclic (PC) codes: ideals in $\mathbb{F}_q[x]/\langle d \rangle$

Generalized PC (GPC) codes: submodules in $\bigoplus_{i=1}^{l} \mathbb{F}_q[x]/\langle d_i \rangle$

Generalized integer codes: subgroups in $\bigoplus_{i=1}^{l} \mathbb{Z}/\langle d_i \rangle$

Codes over Gaussian integers: submodule in $\bigoplus_{i=1}^{l} \mathbb{Z}[\sqrt{-1}]/\langle d_i \rangle$

## 2 Definition of codes over some Euclidean domains

$R := \mathbb{Z}$, $\mathbb{F}_q[x]$, or $\mathbb{Z}\left[\sqrt{-1}\right]$ (a class of Euclidean domains)
$R/\langle d_i\rangle$: quotient ring modulo $d_i$, where $d_i \in R$ is nonzero for all $1 \le i \le l$

$$\mathcal{M} := \bigoplus_{i=1}^{l} R/\langle d_i\rangle = \{(a_1, \cdots, a_l) \mid a_i \in R/\langle d_i\rangle\,,\ 1 \le i \le l\}$$

For $a = (a_1, \cdots, a_l), b = (b_1, \cdots, b_l) \in \mathcal{M}$ and $f \in R$, define

$$a - b := (a_1 - b_1, \cdots, a_l - b_l) \in \mathcal{M}, \quad fa := (fa_1, \cdots, fa_l) \in \mathcal{M}.$$

then $a - b \in \mathcal{M}$ and $fa \in \mathcal{M}$. that is. $\mathcal{M}$ is an $R$-module.

**Definition 1** *A* **code** $\mathcal{C} \subset \mathcal{M}$ *is defined by an $R$-submodule.*

From now on, $\mathcal{C}$ indicates a code.

### Natural projection

$$F:\ R^l \longrightarrow \mathcal{M}$$
$$(c_1, \cdots, c_l) \longmapsto (c_1 \bmod d_1, \cdots, c_l \bmod d_l)\,.$$

- If $\mathcal{C} \subset \mathcal{M}$ is a code, then $\mathbb{D} := F^{-1}(\mathcal{C})$ is an $R$-submodule of $R^l$.
- $\mathbb{D} = F^{-1}(\mathcal{C})$ includes polynomial vectors of the form, for $1 \le i \le l$,

$$\Big(\underbrace{0, \cdots, 0}_{i-1},\ d_i,\ \underbrace{0, \cdots, 0}_{l-i}\Big) \ \in F^{-1}\Big((0, \cdots, 0)\Big). \tag{1}$$

  which is considered as another expression of zero codeword $(0, \cdots, 0) \in \mathcal{M}$.
- Conversely, if an $R$-submodule $\mathbb{D} \subset R^l$ includes (1), then $F(\mathbb{D}) =: \mathcal{C} \subset \mathcal{M}$ is a code.
- Thus there is a one-to-one correspondence between

$$\{\ R\text{-submodule } \mathbb{D} \subset R^l \mid \mathbb{D} \text{ includes (1)}\} \longleftrightarrow \{\ R\text{-submodule } \mathcal{C} \subset \mathcal{M}\}.$$

## 3 Generator matrix $G$

**Definition 2** *Let $G \in M_l(R)$ be an $l \times l$ matrix whose rows are in $\mathcal{C}$. Then $G$ is called a* **generator matrix** *of $\mathcal{C}$ if $G$ is of the following form*

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{l,l} \end{pmatrix},$$

*where, for all $1 \le i \le l$, $g_{i,i}$ is nonzero and $g_{i,i} = \min_{|\cdot|}\{c_i \mid (0, \cdots, 0, c_i, \cdots, c_l) \in \mathcal{C},\ c_i \ne 0\}$ and $|\cdot|$ denotes Euclidean function. If $|g_{i,j}| < |g_{j,j}|$ for all $1 \le i < j \le l$. then $G$ is* **reduced.**

- For each code, there uniquely exists the reduced generator matrix if $g_{i,i}$ is appropriately chosen by multiplying $u \in R^\times$.

**Proposition 1 (Necessary and sufficient condition of codewords)**
*For $c = (c_1, \cdots, c_l) \in \mathcal{M}$. we have $c \in \mathcal{C} \iff c = fG$ for some $f = (f_1, \cdots, f_l) \in R^l$.*
*In other words, $F^{-1}(\mathcal{C}) = R^l G$.*

# 4 Identical equation $AG = \mathrm{diag}\,[d_1, \cdots, d_l]$

The $R$-submodules in $R^l$ which come from some $\mathcal{C} \subset \mathcal{M}$ by $F^{-1}$ are characterized by

**Proposition 2 (Identical equation of $G$)** *Let $G = (g_{i,j}) \in M_l(R)$ be an $l \times l$ upper triangular matrix. Then there exists a $\mathcal{C} \subset \mathcal{M}$ with generator matrix $G$ if and only if there exists an $l \times l$ upper triangular matrix $A = (a_{i,j}) \in M_l(R)$ such that*

$$AG = \mathrm{diag}\,[d_1, \cdots, d_l] = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_l \end{pmatrix}. \quad (\ \underline{\text{identical equation}}\ \textit{of}\ G\ )$$

- This proposition describes when $G$ decides a code in $\mathcal{M}$.
- On the other hand, any upper triangular matrix $G \in M_l(R)$ decides at least one code in $\mathcal{M} := (R/fR)^l$ for $f := \det(G)$ (we will see later).

## The cardinality of $\mathcal{C}$

Consider the following composition map

$$\begin{gathered} R^l \xrightarrow{\times G} R^l \xrightarrow{F(\cdot)} \mathcal{M} \\ (c_1, \cdots, c_l) \longmapsto (c_1 \bmod d_1, \cdots, c_l \bmod d_l)\, G. \end{gathered}$$

Then, the kernel of this composition map is equal to $R^l A$ because

$$\begin{aligned} F((c_1, \cdots, c_l)\, G) = 0 &\iff (c_1, \cdots, c_l)\, G \in R^l \mathrm{diag}\,[d_1, \cdots, d_l] \\ &\iff (c_1, \cdots, c_l)\, G \in R^l AG \\ &\iff (c_1, \cdots, c_l) \in R^l A. \end{aligned}$$

Hence $R^l/R^l A = \mathcal{C}$. On the other hand, $\left|R^l/R^l A\right| = \begin{cases} q^{\deg \det(A)} & R = \mathbb{F}_q[x] \\ |\det(A)| & R = \mathbb{Z} \text{ or } \mathbb{Z}\left[\sqrt{-1}\right] \end{cases}$ follows from elementary divisor theory. If $A = (a_{i,j}) \Longrightarrow \det(A) = \prod_{i=1}^{l} a_{i,i} = \prod_{i=1}^{l} d_i/g_{i,i}$ because $a_{i,i} g_{i,i} = d_i$. Thus we have

$$|\mathcal{C}| = \begin{cases} q^{n - \deg \det(G)} = |\mathcal{M}|/q^{\deg \det(G)} \\ |\mathcal{M}|/|\det(G)|, \end{cases} \qquad R = \mathbb{F}_q[x] \Rightarrow \dim_{\mathbb{F}_q} \mathcal{C} = n - \deg \det(G).$$

# 5 Basics of Hecke rings

$H(\Gamma,\Delta) := \left\{ \sum_{\alpha\in\Delta}^{\text{finite}} c_\alpha \Gamma\alpha\Gamma \;\middle|\; c_\alpha \in \mathbb{Z} \right\}$, $\Gamma := SL_l(R)$, $\Delta := \{\alpha \in M_l(R) \mid \det(\alpha) \neq 0\}$.
$H(\Gamma,\Delta)$ is called a **Hecke ring** [4] with respect to $\Gamma$ *and* $\Delta$ with a commutative multiplication.

- $\Gamma\alpha\Gamma = \Gamma \mathrm{diag}[b_1,\cdots,b_l]\Gamma$ for unique $b_1 | b_2 | \cdots | b_l \in R$ (elementary divisors); thus we may assume $\alpha = \mathrm{diag}[b_1,\cdots,b_l]$; then we denote $T(b_1,\cdots,b_l) := \Gamma\alpha\Gamma$.
- $T(b_1,\cdots,b_l) = \biguplus_{k=1}^{d} \Gamma\alpha_k$ with $d = [\Gamma : \Gamma \cap \alpha_k^{-1}\Gamma\alpha_k] < \infty$
- $\{\Gamma\alpha_k\}_{1\le k\le d} \longleftrightarrow \left\{ \text{lattice } \mathbb{D} \subset R^l \;\middle|\; R^l/\mathbb{D} = \bigoplus_{i=1}^{l} R/\langle b_i\rangle \right\}$ by $\Gamma\alpha_k \mapsto \mathbb{D} := R^l\alpha_k$

Thus we define $\mathrm{ind}\,(T(b_1,\cdots,b_l)) := d$ and $\mathrm{ind}\,(\sum_\alpha c_\alpha \Gamma\alpha\Gamma) := \sum_\alpha c_\alpha \mathrm{ind}\,(\Gamma\alpha\Gamma)$.

$$\alpha = \mathrm{diag}[b_1,\cdots,b_l] \implies \mathrm{ind}\,(\Gamma\alpha\Gamma) = \#\left\{ \mathbb{D} \subset R^l \;\middle|\; R^l/\mathbb{D} = \bigoplus_{i=1}^{l} R/\langle b_i\rangle \right\}$$

It is shown that ind$(\cdot)$ (deg$(\cdot)$ in Shimura's book) is a ring homomorphism of $H(\Gamma,\Delta)$.

## Multiplication in Hecke rings

There exists finite decomposition $\Gamma\alpha\Gamma\beta\Gamma = \biguplus_\xi \Gamma\xi\Gamma$ because

$$\Gamma\alpha\Gamma = \biguplus_i \Gamma\alpha_i, \quad \Gamma\beta\Gamma = \biguplus_j \Gamma\beta_j \implies \Gamma\alpha\Gamma\beta\Gamma = \bigcup_j \Gamma\alpha\Gamma\beta_j = \bigcup_{i,j} \Gamma\alpha_i\beta_j.$$

Then, we define

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \sum_\xi m_\xi(\alpha,\beta)\,\Gamma\xi\Gamma \in H(\Gamma,\Delta)$$

where

$$m_\xi(\alpha,\beta) := \#\{(i,j) \mid \Gamma\alpha_i\beta_j = \Gamma\xi\}.$$

$\{m_\xi(\alpha,\beta)\}$ does not depend on the choices of $\{\alpha_i\}$, $\{\beta_j\}$, and $\{\xi\}$.

There is another formula $\mathrm{ind}\,(\Gamma\xi\Gamma)\, m_\xi(\alpha,\beta) = \#\{(i,j) \mid \Gamma\alpha_i\beta_j\Gamma = \Gamma\xi\Gamma\}$.

$$\mathrm{ind}\,(\Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma) = \sum_\xi \mathrm{ind}\,(\Gamma\xi\Gamma)\, m_\xi(\alpha,\beta) = \#\{\text{all } (i,j)\} = \mathrm{ind}\,(\Gamma\alpha\Gamma)\cdot\mathrm{ind}\,(\Gamma\beta\Gamma)$$

# 6 Connection of Hecke rings with our codes

Let $\mathcal{M} = (R/fR)^l = R^l/fR^l$.

For nonzero $f \in R$, define $T(f) := \sum_{\alpha\in\Delta,\,\det(\alpha)=f} \Gamma\alpha\Gamma \in H(\Gamma,\Delta)$.

$$\begin{aligned}\mathrm{ind}\,(T(f)) &= \#\left\{ \mathbb{D} \subset R^l \;\middle|\; R^l/\mathbb{D} = \bigoplus_{i=1}^{l} R/b_iR,\ \prod_{i=1}^{l} b_i = f \right\} \\ &= \#\left\{ \mathcal{C} \subset \mathcal{M} \;\middle|\; \mathcal{M}/\mathcal{C} = \bigoplus_{i=1}^{l} R/b_iR,\ \prod_{i=1}^{l} b_i = f \right\}. \end{aligned} \tag{2}$$

- $\mathbb{D} \mapsto \mathcal{C} = F(\mathbb{D}) = \mathbb{D}/fR^l$ and $\mathcal{C} \mapsto \mathbb{D} = F^{-1}(\mathcal{C})$ are inverse.
- If $\mathbb{D} \subset R^l$ with $R^l/\mathbb{D} = \bigoplus_{i=1}^{l} R/b_i R$ and $\prod_{i=1}^{l} b_i = f$, then we have $\mathbb{D} \supset fR^l$.
- The condition of (2) $\Longleftrightarrow \det(G) = f$ because

$$\mathcal{C} = R^l/R^l A = R^l G/fR^l \quad \text{and} \quad \mathcal{M}/\mathcal{C} = R^l/R^l G.$$

$$R = \mathbb{Z} \Rightarrow \operatorname{ind}(T(f)) = \#\left\{\mathbb{D} \subset \mathbb{Z}^l \mid \left|\mathbb{Z}^l/\mathbb{D}\right| = |f|\right\} = \#\left\{\mathcal{C} \subset \mathcal{M} \mid |\mathcal{M}/\mathcal{C}| = |f|\right\}$$

## Calculation of $\operatorname{ind}(T(N))$ by generating function

- For nonzero $f, g \in R$, $\gcd(f, g) = 1 \Longrightarrow T(fg) = T(f)T(g)$ Thus we can compute $\operatorname{ind}(T(N))$ by calculating $\operatorname{ind}(T(p^e))$ for prime power $p^e \mid N$.
- Irreducible factor power $\pi^e \mid f \Longrightarrow T(\pi^e) = \sum_{\substack{0 \le d_1 \le \cdots \le d_l \\ d_1 + \cdots + d_l = e}} T(\pi^{d_1}, \cdots, \pi^{d_l})$

$T(p^e)$ and $\operatorname{ind}(T(p^e))$ have generating function

$$\sum_{e=0}^{\infty} T(\pi^e) X^e = \left[\sum_{k=0}^{l} (-1)^k r^{k(k-1)/2} T_k^{(l)} X^k\right]^{-1},$$

where $T_k^{(l)} := T(\overbrace{1, \cdots, 1}^{l-k}, \overbrace{\pi, \cdots, \pi}^{k})$ and

$$r := |R/\pi R| = \begin{cases} q^{\deg \pi} & R = \mathbb{F}_q[x] \\ |\pi| & R = \mathbb{Z} \text{ or } \mathbb{Z}\left[\sqrt{-1}\right]. \end{cases}$$

and $\operatorname{ind}(T(p^e))$ can be computed by

$$\sum_{e=0}^{\infty} \operatorname{ind}(T(\pi^e)) X^e = \left[\sum_{k=0}^{l} (-1)^k r^{k(k-1)/2} \operatorname{ind}\left(T_k^{(l)}\right) X^k\right]^{-1}$$

$$= \frac{1}{(1-X)(1-rX)\cdots(1-r^{l-1}X)} = \sum_{e=0}^{\infty} \left\{ \sum_{\substack{0 \le d_1, d_2, \cdots, d_l \\ d_1 + d_2 + \cdots + d_l = e}} r^{d_2} \cdots r^{(l-1)d_l} \right\} X^e.$$

Thus, all reduced $G$ with $\det(G) = \pi^e$ of $\mathcal{C} \subset (R/\pi^e R)^l$ are

$$\begin{pmatrix} \pi^{d_1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & \pi^{d_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & g_{l-1,l} \\ 0 & \cdots & 0 & \pi^{d_l} \end{pmatrix}, \quad \text{where} \begin{cases} d_1 + \cdots + d_l = e \text{ and } |g_{i,j}| < \left|\pi^{d_j}\right| \\ \text{for all } i < j. \end{cases}$$

because the number of these matrices agrees with $\operatorname{ind}(T(p^e))$.

Summarizing $f = \pi_1^{e_1} \cdots \pi_b^{e_b} \Longrightarrow T(f) = T(\pi_1^{e_1}) \cdots T(\pi_b^{e_b}) \Longrightarrow$
By the multiplication, all $G$ of $\mathcal{C} \subset (R/fR)^l$ with $\deg(G) = f$ are obtained. Note that the multiplication of two reduced generator matrices is not reduced in general, e.g.,

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ 0 & 6 \end{pmatrix}.$$

# 7 Examples

## (a) Generalized integer codes [6]

**Example 1** $l = 1$, $d_1 = 6$, $F : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \supset \mathcal{C} = g\mathbb{Z}/6\mathbb{Z}$ with $g = 1, 2, 3, 6$. (subgroup in $\mathbb{Z}$) $= m\mathbb{Z}$, but $F^{-1}(g\mathbb{Z}/6\mathbb{Z}) = g\mathbb{Z}$. (The identical equation $Ag = 6$)

**Example 2** Consider a subset $\mathcal{C}_1$ of $\mathcal{M} := \mathbb{Z}/10\mathbb{Z} \bigoplus \mathbb{Z}/12\mathbb{Z}$

$$\mathcal{C}_1 := \Big\{(0,0),\ (0,4),\ (0,8),\ (5,2),\ (5,6),\ (5,10)\Big\}.$$

Because $\mathcal{C}_1$ forms a subgroup, $\mathcal{C}_1$ is a generalized integer code. Note that $\mathcal{C}_1 = f_1(5,2) + f_2(0,4)$ with $f_1 \in \{0,1\}$ and $f_2 \in \{0,1,2\}$. The generator matrix of $\mathcal{C}_1$ is equal to $G_1 := \begin{pmatrix} 5 & 2 \\ 0 & 4 \end{pmatrix}$. The identical equation of $G_1$ is equal to $\begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 5 & 2 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 10 & 0 \\ 0 & 12 \end{pmatrix}$.

**Example 3** If $l = 4$ and $\mathcal{M} = (\mathbb{Z}/20\mathbb{Z})^4$, then an example of identical equations is shown by

$$\begin{pmatrix} 20 & -16 & -11 & 23 \\ 0 & 4 & -1 & -3 \\ 0 & 0 & 5 & -4 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 4 & 3 & 1 \\ 0 & 5 & 1 & 19 \\ 0 & 0 & 4 & 16 \\ 0 & 0 & 0 & 20 \end{pmatrix} = \begin{pmatrix} 20 & 0 & 0 & 0 \\ 0 & 20 & 0 & 0 \\ 0 & 0 & 20 & 0 \\ 0 & 0 & 0 & 20 \end{pmatrix}.$$

**Example 4** In the case of $l = 3$ and $p = 2$, $\mathrm{ind}\,(T(2^e))$ is computed by

$$\sum_{e=0}^{\infty} \mathrm{ind}\,(T(2^e))\,X^e = \frac{1}{1 - 7X + 14X^2 - 8X^3} = 1 + 7X + 35X^2 + 155X^3 + 651X^4 + \cdots.$$

For example, we have $\mathrm{ind}\,(T(2^2)) = 35$. On the other hand, because we have $T(2^2) = T(1,2,2) + T(1,1,4)$, all reduced generator matrices are

$$\begin{pmatrix} 1 & * & * \\ & 2 & * \\ & & 2 \end{pmatrix}\ \langle 8\rangle \qquad \begin{pmatrix} 1 & 0 & * \\ & 1 & * \\ & & 4 \end{pmatrix}\ \langle 16\rangle$$

$$\begin{pmatrix} 2 & 0 & * \\ & 1 & * \\ & & 2 \end{pmatrix}\ \langle 4\rangle \qquad \begin{pmatrix} 1 & * & 0 \\ & 4 & 0 \\ & & 1 \end{pmatrix}\ \langle 4\rangle$$

$$\begin{pmatrix} 2 & * & 0 \\ & 2 & 0 \\ & & 1 \end{pmatrix}\ \langle 2\rangle \qquad \begin{pmatrix} 4 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}\ \langle 1\rangle.$$

where $\langle\cdot\rangle$ indicates the number of generator matrices of that type. Thus we can list all 35 generator matrices of $\mathcal{C} \subset (\mathbb{Z}/4\mathbb{Z})^3$ with $|\mathcal{C}| = 4^2$.

## (b) Codes over Gaussian integers

**Example 5** Let $R := \mathbb{Z}\left[\sqrt{-1}\right]$. $l = 1$, $d_1 = 5$, $F : R \to R/5R \supset \mathcal{C} = gR/5R$ with $g = 1, -1 \pm 2\sqrt{-1}, 5$. (submodule in $R$) $= \alpha R$, but $F^{-1}(gR/5R) = gR$ for $g = 1, -1 \pm 2\sqrt{-1}, 5$ (The identical equation $Ag = 5$)

**Example 6** Let $R := \mathbb{Z}\left[\sqrt{-1}\right]$. Consider

$$C_2 := \left\{ \begin{array}{l} (4+2\sqrt{-1}, 2+1\sqrt{-1}), \\ (3+4\sqrt{-1}, 4+2\sqrt{-1}), \\ (2+1\sqrt{-1}, 1+3\sqrt{-1}), \\ (1+3\sqrt{-1}, 3+4\sqrt{-1}), \\ (0,0) \end{array} \right\} \subset \mathcal{M} = (R/5R)^2.$$

Because $C_2$ forms an $R$-submodule, $C_2$ is a code over Gaussian integers. We note that the generator matrix of $C_2$ is equal to

$$G_2 := \begin{pmatrix} -1+2\sqrt{-1} & 2+\sqrt{-1} \\ 0 & 5 \end{pmatrix}.$$

The identical equation of $G_2$ is equal to

$$\begin{pmatrix} -1-2\sqrt{-1} & \sqrt{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1+2\sqrt{-1} & 2+\sqrt{-1} \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}.$$

**Example 7** In case of $R := \mathbb{Z}\left[\sqrt{-1}\right]$ and $l = 3$, $\mathrm{ind}\left(T\left(\pi^e\right)\right)$ with $\pi = -1+2\sqrt{-1}$ is computed by

$$\sum_{e=0}^{\infty} \mathrm{ind}\left(T\left(\pi^e\right)\right) X^e = \frac{1}{1 - 31X + 155X^2 - 125X^3} = 1 + 31x + 806X^2 + 20306X^3 + \cdots.$$

For example, we have $\mathrm{ind}\left(T(\pi^2)\right) = 806$. On the other hand, because we have $T(\pi^2) = T(1, \pi, \pi) + T(1, 1, \pi^2)$, all reduced generator matrices are

$$\begin{array}{cc} \begin{pmatrix} 1 & * & * \\ & \pi & * \\ & & \pi \end{pmatrix} \langle 5^3 \rangle & \begin{pmatrix} 1 & 0 & * \\ & 1 & * \\ & & \pi^2 \end{pmatrix} \langle 25^2 \rangle \\ \begin{pmatrix} \pi & 0 & * \\ & 1 & * \\ & & \pi \end{pmatrix} \langle 5^2 \rangle & \begin{pmatrix} 1 & * & 0 \\ & \pi^2 & 0 \\ & & 1 \end{pmatrix} \langle 25 \rangle \\ \begin{pmatrix} \pi & * & 0 \\ & \pi & 0 \\ & & 1 \end{pmatrix} \langle 5 \rangle & \begin{pmatrix} \pi^2 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \langle 1 \rangle. \end{array}$$

where $\langle \cdot \rangle$ indicates the number of reduced generator matrices of each type. Thus, we can list all 806 reduced $G$ for $\mathcal{C} \subset (R/\pi^2 R)^3$ with $|\mathcal{C}| = |\pi|^4 = 5^4$.

## (c) Generalized pseudo-cyclic (GPC) codes [7]

**Example 8** Let $R = \mathbb{F}_q[x]$.
In case of $l = 3$ and $q = 2$, we set $d_1 = d_2 = d_3 = (1 + x + x^3)^2 = 1 + x^2 + x^6$. Consider

$$A = \begin{pmatrix} 1+x^2+x^6 & 1+x^4+x^5 & x^2+x^3+x^4+x^5 \\ 0 & 1+x+x^3 & x+x^2 \\ 0 & 0 & 1 \end{pmatrix}, \quad G = \begin{pmatrix} 1 & 1+x+x^2 & x+x^2+x^3+x^5 \\ 0 & 1+x+x^3 & x+x^3+x^4+x^5 \\ 0 & 0 & 1+x^2+x^6 \end{pmatrix}.$$

Then, we have

$$AG = \mathrm{diag}\left[1 + x^2 + x^6, 1 + x^2 + x^6, 1 + x^2 + x^6\right].$$

Let $\mathcal{C}$ be the GPC code defined by $G$. Then, $\mathcal{C} \subset \mathcal{M}$ with $|\mathcal{M}| = 2^{18}$ and $|\mathcal{C}| = 2^9$.
A binary generator matrix $\tilde{G}$ of $\mathcal{C}$ can be derived from $G$:

$$\tilde{G} = \left(\begin{array}{c|c|c} 100000 & 111000 & 011101 \\ 010000 & 011100 & 100110 \\ 001000 & 001110 & 010011 \\ 000100 & 000111 & 100001 \\ 000010 & 101011 & 111000 \\ 000001 & 111101 & 011100 \\ \hline 000000 & 110100 & 010111 \\ 000000 & 011010 & 100011 \\ 000000 & 001101 & 111001 \end{array}\right).$$

**Example 9** In the case of $l = 3$ and $q = 2$, $\mathrm{ind}\,(T(\pi^c))$ with $\pi = x^2 + x + 1$ is computed by

$$\sum_{c=0}^{\infty} \mathrm{ind}\,(T(\pi^c))\, X^c = \frac{1}{1 - 21X + 84X^2 - 64X^3} = 1 + 21X + 357X^2 + 5797X^3 + \cdots.$$

For example, we have $\mathrm{ind}\,(T(\pi^2)) = 357$. On the other hand, because we have $T(\pi^2) = T(1, \pi, \pi) + T(1, 1, \pi^2)$, all reduced generator matrices are

$$\begin{pmatrix} 1 & * & * \\ & \pi & * \\ & & \pi \end{pmatrix} \langle 4^3 \rangle \qquad \begin{pmatrix} 1 & 0 & * \\ & 1 & * \\ & & \pi^2 \end{pmatrix} \langle 16^2 \rangle$$

$$\begin{pmatrix} \pi & 0 & * \\ & 1 & * \\ & & \pi \end{pmatrix} \langle 4^2 \rangle \qquad \begin{pmatrix} 1 & * & 0 \\ & \pi^2 & 0 \\ & & 1 \end{pmatrix} \langle 16 \rangle$$

$$\begin{pmatrix} \pi & * & 0 \\ & \pi & 0 \\ & & 1 \end{pmatrix} \langle 4 \rangle \qquad \begin{pmatrix} \pi^2 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \langle 1 \rangle,$$

where $\langle \cdot \rangle$ indicates the number of reduced generator matrices of each type. Thus, we can list all 357 reduced $G$ for $\mathcal{C} \subset (R/\pi^2 R)^3$ with $|\mathcal{C}| = (2^2)^4 = 2^8$.

**Example 10 (A zeta function)** From the above argument, we can extract some properties of a certain zeta function.

$$X := q^{-s \deg \pi} \implies \sum_{c=0}^{\infty} \frac{\mathrm{ind}\,(T(\pi^c))}{q^{s \deg \pi^c}} = \prod_{i=0}^{l-1} \left(1 - \frac{1}{q^{(s-i)\deg \pi}}\right)^{-1}.$$

Take $\prod_\pi$ of both sides, where $\pi$ runs over all monic irreducible polynomials in $R$. As for the left hand side, it follows from the commutativity that

$$(\textstyle\prod_\pi \text{ of left-hand side}) = \displaystyle\prod_{\pi} \sum_{c=0}^{\infty} \frac{\mathrm{ind}\,(T(\pi^c))}{q^{s \deg \pi^c}} = \sum_{f:\,\text{monic}} \frac{\mathrm{ind}\,(T(f))}{q^{s \deg f}},$$

where $f$ runs over all monic polynomials in $R$. As for the right hand side, we have, for $0 \le i \le l - 1$,

$$\prod_{\pi} \left(1 - \frac{1}{q^{(s-i)\deg \pi}}\right)^{-1} = \prod_{\pi} \sum_{c=0}^{\infty} \frac{1}{q^{(s-i)\deg \pi^c}} = \sum_{f} \frac{1}{q^{(s-i)\deg f}} = \sum_{m=0}^{\infty} \frac{q^m}{q^{(s-i)m}} = \left(1 - \frac{1}{q^{s-i-1}}\right)^{-1}.$$

Thus, we obtain a rational-function expression of the zeta function

$$\sum_{f} \frac{\mathrm{ind}\,(T(f))}{q^{s \deg f}} = \prod_{i=1}^{l} \left(1 - \frac{1}{q^{s-i}}\right)^{-1}.$$

# 8 Conclusion and future work

- We have found various useful properties on codes over a class of Euclidean domains:
  - Generator matrices
  - Identical equations of generator matrices
  - Application of Hecke rings.
- Future work will focus on developing the enumeration of efficient codes.
- Another area of research will involve establishing the theory of parity-check matrices of these codes.

# References


[1] J. Justesen, T. Hoholdt, *A Course In Error-Correcting Codes*, European Mathematical Society, 2004.
(ユステセン，ホーホルト（共著），阪田省二郎，栗原正純，松井一，藤沢匡哉（共訳），誤り訂正符号入門，森北出版，2005.)

[2] K. Lally, P. Fitzpatrick, "Algebraic structure of quasi-cyclic codes," *Discrete Applied Mathematics*, vol.111, no.1–2, pp.157–175, Jul. 2001.

[3] C.E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol.27, no.3, pp.379–423 and 623–656, Jul. and Oct. 1948.

[4] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten, Publishers, and Princeton University Press, 1971.

[5] H. Matsui, "On polynomial generator matrices of generalized quasi-cyclic codes," *6th Asia-Europe Workshop on Information Theory*, Ishigaki Island, Okinawa, Japan, Oct. 22–24, 2010.

[6] H. Matsui, "On generator matrices and parity check matrices of generalized integer codes," to appear in *Designs, Codes and Cryptography*, DOI 10.1007/s10623-013-9883-7

[7] H. Matsui, "On generator polynomial matrices of generalized pseudo-cyclic codes," to appear in *International Symposium on Information Theory and Its Applications (ISITA2014)*, Melbourne, Australia, Oct. 26–29, 2014.

[8] V.T. Van, H. Matsui, S. Mita, "Computation of Gröbner basis for systematic encoding of generalized quasi-cyclic codes," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol.E92-A, no.9, pp.2345–2359, Sep. 2009.