IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 22 November 2022, accepted 3 March 2023, date of publication 6 March 2023, date of current version 13 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3253774

RESEARCH ARTICLE

An Algorithm for Finding Self-Orthogonal and Self-Dual Codes Over Gaussian and Eisenstein Integer Residue Rings via Chinese Remainder Theorem

HAJIME MATSUI
Toyota Technological Institute, Nagoya, Aichi 468-8511, Japan
e-mail: matsui@toyota-ti.ac.jp

ABSTRACT A code over Gaussian or Eisenstein integer residue ring is an additive group of vectors with entries in this integer residue ring which is closed under the action of constant multiplication by the Gaussian or Eisenstein integers. In this paper, we define the dual codes for the codes over the Gaussian and Eisenstein integer residue rings, and consider the construction of the self-dual codes. Because, in the Gaussian and Eisenstein integer rings, the uniqueness of the prime element decomposition holds in the same way as the one-variable polynomial rings over finite fields and the rational integer ring, we provide an efficient construction method for self-dual code generator matrices using that of moduli. As numerical examples, for Gaussian and Eisenstein integer rings, we enumerate and construct the self-dual codes for the actual moduli when the size of the generator matrices is two.

INDEX TERMS Codes over rings, dual codes, error-correcting codes, Euclidean domain.

I. INTRODUCTION

There are various studies on the codes over the rational integer residue rings, summarized in [1]. In [8], the author considers the codes over quotient rings of Euclidean domains and investigates the properties of their generator matrices. On the other hand, in coding theory, the construction and search for various types of self-dual codes have been studied [3]. In [7], for codes over rational integer residue rings $\mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{Z}$, where $\mathbb{Z}$ is the rational integer ring, the author proposes a method for efficiently obtaining a generator matrix for a self-dual code over $\mathbb{Z}/m\mathbb{Z}$ from generator matrices for self-dual codes over $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$, $i = 1, \cdots, t$, according to prime factorization $m = p_1^{e_1} \cdots p_t^{e_t}$. Recently, new applications have been proposed for codes over the Gaussian and Eisenstein integer residue rings in [2], [5], [11], [12], and [13]. It is expected that the construction and search of a class of codes according to the purposes become important for codes over the Gaussian and Eisenstein integer residue rings.

The associate editor coordinating the review of this manuscript and approving it for publication was Zihuai Lin.

In particular, in the Gaussian and Eisenstein integer rings, as in the rational integer ring, the uniqueness of the prime element factorization holds, where a prime element means an element whose quotient ring by the ideal it generates is a finite field, and their ideals are principal [4]. However, until now there has been no known method of constructing a global one from generator matrices of local self-dual codes, such as codes over the rational integer residue rings.

In this paper, we propose a method for efficiently obtaining generator matrices for self-dual codes over the Gaussian and Eisenstein integer residue rings using prime element factorization. From now on, we denote the Gaussian integer ring $\mathbb{Z}\left[\sqrt{-1}\right]$ or Eisenstein integer ring $\mathbb{Z}\left[(-1+\sqrt{-3})/2\right]$ as R. Unlike rational integers, because Gaussian and Eisenstein integers have an involution from complex conjugate, the prime element π of R is classified into two types, i.e., $\pi R = \overline{\pi} R$ or $\gcd(\pi, \overline{\pi}) = 1$, where, for $z \in \mathbb{C}$, $\overline{z}$ means its complex conjugate. Therefore, any $m \in R \setminus \{0\}$ can be decomposed into the product of prime elements uniquely except for the difference of units $R^\times$ as follows (cf. Remark 6), where $p_i, q_j, r_k \in R$ are prime elements, $\epsilon \in R^\times$, and e_i, f_j, g_k are non-negative integers,

$$m = \epsilon \prod_{\gcd(p_i,\overline{p_i})=1} p_i^{e_i} \prod_{q_jR=\overline{q_j}R} q_j^{f_j} \prod_{\gcd(r_k,\overline{r_k})=1} r_k^{g_k}\overline{r_k}^{g_k}.$$

For simplicity, we assume $e_i = 0$, which means that m satisfies $mR = \overline{m}R$ but does not mean that $\epsilon m \in \mathbb{Z}$ for some $\epsilon \in R^\times$, e.g., $1+\sqrt{-1} = -\sqrt{-1}\left(1+\sqrt{-1}\right)$ for $1+\sqrt{-1} \notin R^\times$. Then we show that the self-dual code over R/mR gives those over $R/q_j^{f_j}R$ and over $R/(r_k\overline{r_k})^{g_k}R$ for all j, k, and conversely, the self-dual codes over $R/q_j^{f_j}R$ and over $R/(r_k\overline{r_k})^{g_k}R$ for all j, k give that over R/mR, and these correspondences are inverses of each other. Using these correspondences, we can efficiently construct and search the generator matrices of the self-dual codes over R/mR according to the purposes.

The rest of the paper is organized as follows. In Section II, as preliminaries we summarize facts about the Gaussian and Eisenstein integer rings used in this paper. Subsection II-A summarizes the residue rings of these rings and Subsection II-B summarizes the codes over these residue rings. Section III defines self-orthogonal and self-dual codes and, as their first property, describes the treatment of $p_i^{e_i}$ above with $e_i \neq 0$. Section IV examines how the orthogonality condition of the generator matrices changes with the modulus and its decomposition. If a modulus m satisfies $mR = \overline{m}R$ in Subsection IV-A, if $m = m_1m_2$ with $\gcd(m_1, m_2) = 1$, $m_1R = \overline{m_1}R$, and $m_2R = \overline{m_2}R$ in Subsection IV-B, and if $m = w\overline{w}$ with $\gcd(w, \overline{w}) = 1$ in Subsection IV-C, we derive the properties of each generator matrix. Using these results, we apply the prime element decomposition to self-orthogonal and self-dual codes in Section V. In Section VI, as numerical examples, when the size of the generator matrices is two, the self-dual codes are actually obtained. Subsection VI-A gives examples for Gaussian integer ring and Subsection VI-B for Eisenstein integer ring.

II. PRELIMINARIES

A. GAUSSIAN AND EISENSTEIN INTEGERS

Let $R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$, or $R = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, where $\omega = (-1+\sqrt{-3})/2$. If we denote an element $z = a + bi \in \mathbb{C}$ or $z = a + b\omega \in \mathbb{C}$, then we suppose that $a, b \in \mathbb{R}$ and we denote $\Re(z) = a$ and $\Im(z) = b$. For $m \in R \setminus \{0\}$, let $R/mR = \{f + mR : f \in R\}$ denote the quotient ring by an ideal mR.

For any $w, x, y \in \mathbb{R}$ and $z \in \mathbb{C}$ with $\Re(z) = x$ and $\Im(z) = y$, let $[\![\cdot]\!] : \mathbb{C} \to R$ be an arbitrary function satisfying $[\![f + z]\!] = f + [\![z]\!]$ for all $f \in R$. An example of $[\![\cdot]\!]$ is $[\![z]\!]$ with $\Re([\![z]\!]) = \lfloor x \rfloor$ and $\Im([\![z]\!]) = \lfloor y \rfloor$, where $\lfloor w \rfloor \in \mathbb{Z}$ with $w-1 < \lfloor w \rfloor \leq w$.

Remark 1: Let $f, g, h, k \in R$ and $g \neq 0$.

1) If $f = hg + k$, then $h = [\![f/g]\!]$ if and only if $[\![k/g]\!] = 0$.
2) $(f \bmod g) \in R$ is defined by $(f \bmod g) = f - [\![f/g]\!]g$. Then $(f \bmod g) = (k \bmod g)$ if and only if $(f - k)/g \in R$. The 'if' part is shown by, with $f - k = hg$, $(f \bmod g) = k + hg - [\![(k + hg)/g]\!]g = (k \bmod g)$. We write $f \equiv k \bmod g$ if $(f \bmod g) = (k \bmod g)$. Moreover, we write $g \mid f$ if $f \equiv 0 \bmod g$ and $g \nmid f$ if $f \not\equiv 0 \bmod g$.
3) Two maps $R/gR \to \{k \in R : [\![k/g]\!] = 0\}, f + gR \mapsto (f \bmod g)$, and $\{k \in R : [\![k/g]\!] = 0\} \to R/gR, k \mapsto k + gR$, are inverse each other. Thus R/gR can be identified with $\{k \in R : [\![k/g]\!] = 0\}$.

Example 1: Let $R = \mathbb{Z}[i]$ and $[\![a + bi]\!] = \lfloor a \rfloor + \lfloor b \rfloor i$. If $g = 4$, then $\{k \in R : [\![k/g]\!] = 0\} = \{a + bi : a, b = 0, 1, 2, 3\}$. If $g = 2 + i$, then $\{k \in R : [\![k/g]\!] = 0\} = \{0, i, 2i, 1 + i, 1 + 2i\}$.

Remark 2 (Cf. [8]): Let $R = \mathbb{Z}[i]$, $f, g \in R$, and $g \neq 0$.

1) For an odd rational prime $p \in \mathbb{Z}$, there exists $a + bi \in R$ with $p = |a + bi|^2 = a^2 + b^2$ if and only if $p \equiv 1 \bmod 4$.
2) $|R/gR| = |g|^2$ by $g = a+bi$, $gR = \mathbb{Z}(a+bi)+\mathbb{Z}(ai-b)$, $\begin{pmatrix} a+bi \\ ai-b \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} 1 \\ i \end{pmatrix}$, and $\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = |g|^2$.
3) For any $w, x, y \in \mathbb{R}$ and $z = x + iy$, define $[\![z]\!] \in R$ by $[\![z]\!] = \lfloor x + 0.5 \rfloor + \lfloor y + 0.5 \rfloor i$. Then $[\![f + z]\!] = f + [\![z]\!]$.
4) If $[\![f/g]\!] = 0$, then $|\Re(f/g)|, |\Im(f/g)| \leq 1/2$ and $|f|^2 \leq |g|^2/2$.

Because of 4 in Remark 2, if we choose $[\![\cdot]\!]$ as 3 in Remark 2, then $\{k \in R : [\![k/g]\!] = 0\}$ is equal not only to the set of representatives of R/gR but also to all remainders of Euclidean division by g, i.e., $\{k \in R : f, h \in R, f = hg + k, |k| < |g|\}$.

Example 2: In Example 1, $k = 3+3i \in \{k \in R : [\![k/4]\!] = 0\}$ and $k = 1 + 2i \in \{k \in R : [\![k/(2 + i)]\!] = 0\}$ do not satisfy $|k| < |4|$ and $|k| < |2 + i|$, respectively. If we adopt $[\![z]\!] = \lfloor x + 0.5 \rfloor + \lfloor y + 0.5 \rfloor i$, then $\{k \in R : [\![k/4]\!] = 0\} = \{a + bi : a, b = -2, -1, 0, 1\}$, $\{k \in R : [\![k/(2 + i)]\!] = 0\} = \{0, \pm 1, \pm i\}$, and all $k \in \{k \in R : [\![k/4]\!] = 0\}$ and $k \in \{k \in R : [\![k/(2 + i)]\!] = 0\}$ satisfy $|k| < |4|$ and $|k| < |2 + i|$, respectively.

Remark 3 (Cf. [8]): Let $R = \mathbb{Z}[\omega]$, $f, g \in R$, and $g \neq 0$.

1) For a rational prime $p \in \mathbb{Z}$, there exists $a + b\omega \in R$ with $p = |a + b\omega|^2 = a^2 - ab + b^2$ if and only if $p \equiv 1 \bmod 3$.
2) $|R/gR| = |g|^2$ by $g = a+b\omega$, $gR = \mathbb{Z}(a+b\omega)+\mathbb{Z}(-b+(a-b)\omega)$, $\begin{pmatrix} a+b\omega \\ -b+(a-b)\omega \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}\begin{pmatrix} 1 \\ \omega \end{pmatrix}$, and $\begin{vmatrix} a & b \\ -b & a-b \end{vmatrix} = |g|^2$.
3) For any $w, x, y \in \mathbb{R}$ and $z = x + y\omega$, define $[\![z]\!] \in R$ by $[\![z]\!] = \lfloor x+0.5 \rfloor + \lfloor y+0.5 \rfloor\omega$. Then $[\![f + z]\!] = f + [\![z]\!]$.
4) If $[\![f/g]\!] = 0$, then $|\Re(f/g)|, |\Im(f/g)| \leq 1/2$ and $|f|^2 \leq 3|g|^2/4$.
5) It is shown in [8] that $[\![z]\!] = \lfloor x \rfloor + \lfloor y \rfloor\omega$ also deduces $|f|^2 < |g|^2$. We adopt $[\![z]\!] = \lfloor x + 0.5 \rfloor + \lfloor y + 0.5 \rfloor\omega$ because of our purpose in Remark 10.

Remark 4 (Chinese Remainder Theorem in R): For $u_1, u_2 \in R$, if there exist $v_1, v_2 \in R$ such that $v_1u_1 + v_2u_2 = 1$, then we denote $\gcd(u_1, u_2) = 1$. If $u_1, u_2, v_1, v_2 \in R$ and $v_1u_1 + v_2u_2 = 1$, then $R/u_1u_2R = v_2u_2(R/u_1R) + v_1u_1(R/u_2R)$ and $(R/u_1u_2R)^\times = v_2u_2(R/u_1R)^\times + v_1u_1(R/u_2R)^\times$, where, e.g., $(R/u_1u_2R)^\times = \{f \in R/u_1u_2R : \gcd(f, u_1u_2) = 1\}$.

B. CODES OVER QUOTIENT RINGS OF R

For a positive $l \in \mathbb{Z}$, let $\mathbb{L} = R^l = \{(c_1, \cdots, c_l) : c_1, \cdots, c_l \in R\}$ and, for $m \in R \setminus \{0\}$, let $\mathbb{L}/m\mathbb{L} = (R/mR)^l = \{(c_1, \cdots, c_l) : c_1, \cdots, c_l \in R/mR\}$.

For a subset $C \subset \mathbb{L}/m\mathbb{L}$, we say that C is a *code over a quotient ring modulo m* of R if and only if C is an R-submodule in $\mathbb{L}/m\mathbb{L}$. If C is a code over a quotient ring modulo m of R, we call $C \subset \mathbb{L}/m\mathbb{L}$ an R-module in short.

For positive $k, l \in \mathbb{Z}$, let $M_{k,l}(R)$ denote a ring of all k-by-l matrices with entries in R and let $M_l(R) = M_{l,l}(R)$. For $G \in M_l(R)$, we say that G is a *generator matrix* of an R-module $C \subset \mathbb{L}/m\mathbb{L}$ if and only if $\mathbb{L}G \supset m\mathbb{L}$ and $C = \mathbb{L}G/m\mathbb{L}$.

Lemma 1: For any $G_1, G_2 \in M_l(R)$, $\mathbb{L}G_1 \subset \mathbb{L}G_2$ if and only if $G_1 = MG_2$ for some $M \in M_l(R)$.

Proof: Let $G_1 = \left(g^{(1)}_{r,s}\right)$. Then

$$\begin{aligned} &\mathbb{L}G_1 \subset \mathbb{L}G_2 \\ &\iff \left(g^{(1)}_{r,1}, \cdots, g^{(1)}_{r,l}\right) = m_r G_2,\ \exists m_r \in R^l,\ 1 \le \forall r \le l \\ &\iff G_1 = MG_2,\ \exists M \in M_l(R). \quad \square \end{aligned}$$

It follows from Lemma 1 that, for $G \in M_l(R)$, G is a generator matrix of some R-module in $\mathbb{L}/m\mathbb{L}$ if and only if $\mathbb{L}G \supset m\mathbb{L}$ if and only if $AG = mI$ for some $A \in M_l(R)$, where $I \in M_l(R)$ is the identity matrix.

Let $R^\times = \{\pm 1, \pm i\}$ if $R = \mathbb{Z}[i]$ and $R^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ if $R = \mathbb{Z}[\omega]$. Let $GL_l(R) = \{\delta \in M_l(R) : \det(\delta) \in R^\times\}$. It follows from Lemma 1 that, for $G_1, G_2 \in M_l(R)$, if $\mathbb{L}G_1 = \mathbb{L}G_2 \supset m\mathbb{L}$, then $G_1 = \delta G_2$ for some $\delta \in GL_l(R)$. Conversely, for $G_1, G_2 \in M_l(R)$, if $G_1 = \delta G_2$ with $\delta \in GL_l(R)$, then $\mathbb{L}G_1 = \mathbb{L}G_2$. It is shown in [8] that, for a generator matrix $G \in M_l(R)$ of an R-module $C = \mathbb{L}G/m\mathbb{L}$, among δG, $\delta \in GL_l(R)$, we can choose $G = (g_{r,s}) \in M_l(R)$ which satisfies the following three conditions.

a. G is upper triangular in the sense that $g_{r,s} = 0$ for all $1 \le s < r \le l$.
b. For all $1 \le r \le l$, $g_{r,r}$ is chosen appropriately among $\{\epsilon g_{r,r} : \epsilon \in R^\times\}$, cf. Remarks 9 and 10.
c. $|g_{r,s}| < |g_{s,s}|$ for all $1 \le r < s \le l$.

For $G \in M_l(R)$ with $\mathbb{L}G \supset m\mathbb{L}$, we say that G is *reduced* if and only if G satisfies the above three conditions. It is also shown in [8] that, for any R-module $C \subset \mathbb{L}/m\mathbb{L}$, there exists uniquely a reduced generator matrix $G \in M_l(R)$ with $C = \mathbb{L}G/m\mathbb{L}$.

For $m \in R \setminus \{0\}$, let $\{G\}_m = \{G \in M_l(R) : \mathbb{L}G \supset mI$ and G is reduced$\}$, i.e., $\{G\}_m$ is the set of the reduced generator matrices of all R-modules in $\mathbb{L}/m\mathbb{L}$.

Theorem 1 (Cf. [9]): For $m \in R \setminus \left(\{0\} \cup R^\times\right)$, let $m = \epsilon \prod_{x=1}^t m_x$, where $\epsilon \in R^\times$, $m_x \in R \setminus R^\times$, and $\gcd(m_x, m_y) = 1$ for all $1 \le x \ne y \le t$. Then there exists a one-to-one and onto map

$$\alpha : \{G\}_m \to \prod_{x=1}^t \{G_x\}_{m_x},$$

where $\mathbb{L}G + m_x\mathbb{L} = \mathbb{L}G_x$ and $\mathbb{L}G = \bigcap_{x=1}^t \mathbb{L}G_x$. Moreover, if $\alpha(G) = (G_x)_{1 \le x \le t}$, $G = (g_{r,s})$, and $G_x = \left(g^{(x)}_{r,s}\right)$, then $g_{r,r} = \prod_{x=1}^t g^{(x)}_{r,r}$ for all $1 \le r \le l$.

Remark 5: By Theorem 1, an algorithm which computes G from $(G_x)_{1 \le x \le t}$ is extracted as Algorithm 1 in [9]. If we estimate the computational complexity of Algorithm 1 as the total number of operations in R, it is evaluated approximately as $O\left(l^3 t \log |m|\right)$, which is the same order as that of multiplying generator matrices in [8].

For $G = (g_{r,s}) \in M_{k,l}(R)$, let $G^\dagger = (\overline{g_{s,r}}) = \overline{G}^\top$, where $\overline{a + bi} = a - bi \in \mathbb{Z}[i]$ and $\overline{a + b\omega} = a + b\omega^2 \in \mathbb{Z}[\omega]$ are their complex conjugates and, for $G = (g_{r,s}) \in M_{k,l}(R)$, $G^\top = (g_{s,r}) \in M_{l,k}(R)$ is its transposed matrix. We denote

$$\begin{aligned} \widehat{C} &= \left\{a \in \mathbb{L}/m\mathbb{L} : m \,|\, a(b^\dagger),\ \forall b \in C\right\} \\ &= \left\{a \in \mathbb{L}/m\mathbb{L} : m \,|\, a(G^\dagger)\right\}, \end{aligned}$$

where, for $A = (a_{r,s}) \in M_{k,l}(R)$, $m \,|\, A$ means $m \,|\, a_{r,s}$ for all $1 \le r \le k$ and $1 \le s \le l$. Then an R-module $\widehat{C}$ is called the *dual* R-module of C.

Lemma 2 (Cf. [10]): Consider a homomorphism of R-modules

$$\mathbb{L}/m\mathbb{L} \to \mathbb{L}/m\mathbb{L}, \quad a \mapsto a(G^\dagger).$$

Let $\widetilde{C} = (m\mathbb{L} + \mathbb{L}G^\dagger)/m\mathbb{L}$, i.e., the image of this map. Then there exists an exact sequence of R-modules

$$0 \to \widehat{C} \to \mathbb{L}/m\mathbb{L} \to \widetilde{C} \to 0$$

and an equality $|\widehat{C}|\,|\widetilde{C}| = |\mathbb{L}/m\mathbb{L}|$.

Lemma 3 (Cf. [8]): For any $A \in M_l(R)$ with $\det(A) \ne 0$, $|\mathbb{L}/\mathbb{L}A| = |\det(A)|^2$. In particular, if $G \in M_l(R)$ is a generator matrix of an R-module $C \subset \mathbb{L}/m\mathbb{L}$, then $|C| = |\mathbb{L}/m\mathbb{L}|/|\det(G)|^2 = |m|^{2l}/|\det(G)|^2$.

III. SELF-ORTHOGONAL AND SELF-DUAL CODES

We say that an R-module $C = \mathbb{L}G/m\mathbb{L}$ is *self-orthogonal* if and only if $C \subset \widehat{C}$, which is equivalent to $m \mid G(G^\dagger)$. We denote $\{G\}^\dagger_m = \left\{G \in \{G\}_m : m \,|\, G(G^\dagger)\right\}$.

Remark 6: Any $m \in R \setminus \{0\}$ can be decomposed into the product of prime elements uniquely except for the difference of units $R^\times$ as follows, where $p_i, q_j, r_k \in R$ are prime elements, $\epsilon \in R^\times$, and e_i, f_j, g_k are non-negative integers,

$$m = \epsilon \prod_{\gcd(p_i, \overline{p_i})=1} p_i^{e_i} \prod_{q_j R = \overline{q_j} R} q_j^{f_j} \prod_{\gcd(r_k, \overline{r_k})=1} r_k^{g_k} \overline{r_k}^{g_k} \qquad (1)$$

because the prime element π of R is classified into two types, i.e., $\pi R = \overline{\pi} R$ or $\gcd(\pi, \overline{\pi}) = 1$ and m can be factored as follows.

- If $\gcd(\pi, \overline{\pi}) = 1$, $\pi^h \,|\, m$, $\pi^{h+1} \nmid m$, and $\overline{\pi} \nmid m$ for positive $h \in \mathbb{Z}$, then $p_i^{e_i} = \pi^h$.
- If $\pi R = \overline{\pi} R$, $\pi^h \mid m$, and $\pi^{h+1} \nmid m$ for positive $h \in \mathbb{Z}$, then $q_j^{f_j} = \pi^h$.
- If $\gcd(\pi, \overline{\pi}) = 1$, $\pi^h \,|\, m$, $\pi^{h+1} \nmid m$, $\overline{\pi}^h \,|\, m$, $\overline{\pi}^{h+1} \nmid m$ for positive $h \in \mathbb{Z}$, then $r_k^{g_k} = \pi^h$.

- If $\gcd(\pi, \overline{\pi}) = 1$, $\pi^h \mid m$, $\pi^{h+1} \nmid m$, $\overline{\pi}^l \mid m$, $\overline{\pi}^{l+1} \nmid m$ for positive $h, l \in \mathbb{Z}$ with $h < l$, then $r_k^{g_k} = \pi^h$ and $p_i^{e_i} = \overline{\pi}^{l-h}$.

Furthermore, any $m \in R \setminus \{0\}$ satisfy $m = uvw\overline{w}$ for some $u, v, w \in R$ with $vR = \overline{v}R$ and $\gcd(u, \overline{u}) = \gcd(w, \overline{w}) = \gcd(u, vw) = \gcd(v, m/v) = \gcd(w, m/w) = \gcd(\overline{w}, m/\overline{w}) = 1$ by $u = \prod p_i^{e_i}$, $v = \prod q_j^{f_j}$, and $w = \prod r_k^{g_k}$.

Proposition 1: Let $m \in R \setminus \{0\}$ satisfy $m = uvw\overline{w}$ as in Remark 6. Then $\{G\}_m^{\dagger} = \left\{uG' : G' \in \{G'\}_{m/u}^{\dagger}\right\}$. In particular, for $u \in R \setminus \{0\}$ with $\gcd(u, \overline{u}) = 1$, $\{G\}_u^{\dagger} = \{uI\}$.

Proof. Consider a map $\{G'\}_{m/u}^{\dagger} \to \{G\}_m^{\dagger}$, $G' \mapsto uG'$. For $G' \in \{G'\}_{m/u}^{\dagger}$, because $A'G' = (m/u)I$ for some $A' \in M_l(R)$ and $(m/u) \mid G'(G'^{\dagger})$, $A'uG' = mI$ and $m \mid uG'(uG'^{\dagger})$. Thus $uG' \in \{G\}_m^{\dagger}$. Conversely, for $G \in \{G\}_m^{\dagger}$, because $AG = mI$ for some $A \in M_l(R)$ and $m \mid G(G^{\dagger})$, $m \mid G(G^{\dagger})(A^{\dagger}) = G\overline{m}$ and $u \mid G\overline{u}$. It follows from $\gcd(\overline{u}, u) = 1$ that $u \mid G$. Then $A(G/u) = (m/u)I$ and $(m/u) \mid (G/u)((G/u)^{\dagger})\overline{u}$. It follows from $\gcd(\overline{u}, v\overline{w}) = 1$ that $v\overline{w} \mid (G/u)((G/u)^{\dagger})$, which leads $(m/u) \mid (G/u)((G/u)^{\dagger})$ and $G/u \in \{G'\}_{m/u}^{\dagger}$. □

Example 3: If $l = 1$, $\pi = 2 + i$, and $m = \pi\overline{\pi}^2$, then $m = uvw\overline{w}$ with $u = \overline{\pi}$, $v = 1$, and $w = \pi$. Then $\{G'\}_{m/u} = \{1, \pi, \overline{\pi}, 5\}$ and $\{G'\}_{m/u}^{\dagger} = \{\pi, \overline{\pi}, 5\}$. On the other hand, $\{G\}_m = \{1, \overline{\pi}, \overline{\pi}^2, \pi, \pi\overline{\pi}, \pi\overline{\pi}^2\}$ and $\{G\}_m^{\dagger} = \{\overline{\pi}^2, \pi\overline{\pi}, \pi\overline{\pi}^2\}$. Thus $u\{G'\}_{m/u}^{\dagger} = \{G\}_m^{\dagger}$.

We say that C is *self-dual* if and only if $C = \widehat{C}$. We denote $\{G\}_m^{\ddagger} = \left\{G \in \{G\}_m^{\dagger} : C = \mathbb{L}G/m\mathbb{L} = \widehat{C}\right\}$.

Remark 7: The self-dual version of Proposition 1 does not hold in general. In Example 3, $\{G'\}_{m/u}^{\ddagger} = \{\pi, \overline{\pi}\}$ but $\{G\}_m^{\ddagger} = \{\overline{\pi}^2\}$ because, for $G' = \pi$, $uG' = 5$ and

$$\begin{aligned}\widehat{C} &= \{c \in R/5\overline{\pi}R : 5\overline{\pi} \mid c5 \Leftrightarrow \overline{\pi} \mid c\} \\ &= \overline{\pi}R/5\overline{\pi}R = R/5R \supsetneqq C = R\pi\overline{\pi}/5\overline{\pi}R = \pi R/5R,\end{aligned}$$

for $G' = \overline{\pi}$, $uG' = \overline{\pi}^2$ and

$$\begin{aligned}\widehat{C} &= \{c \in R/5\overline{\pi}R : 5\overline{\pi} \mid c\pi^2 \Leftrightarrow \overline{\pi}^2 \mid c\} \\ &= \overline{\pi}^2R/5\overline{\pi}R = R/\pi R = C = R\overline{\pi}^2/5\overline{\pi}R = R/\pi R,\end{aligned}$$

and, for $G' = 5$, $uG' = \overline{\pi}5$ and

$$\begin{aligned}\widehat{C} &= \{c \in R/5\overline{\pi}R : 5\overline{\pi} \mid c\pi 5 \Leftrightarrow \overline{\pi} \mid c\} \\ &= \overline{\pi}R/5\overline{\pi}R = R/5R \supsetneqq C = R\overline{\pi}5/5\overline{\pi}R = \{0\}.\end{aligned}$$

However, if $\gcd(u, vw\overline{w}) = 1$ in $m = uvw\overline{w}$, then $u\{G'\}_{m/u}^{\ddagger} = \{G\}_m^{\ddagger}$ as shown in Corollary 1.

Lemma 4: Let the assumption be as in Proposition 1. Suppose $\gcd(u, m/u) = 1$. If $G' \in \{G'\}_{m/u}$, then $\widehat{C'} \to \widehat{C}$, $c' \mapsto uc'$, is one to one and onto, where

$$\widehat{C'} = \left\{c' \in \mathbb{L}/(m/u)\mathbb{L} : (m/u) \mid c'(G'^{\dagger})\right\},$$
$$\widehat{C} = \left\{c \in \mathbb{L}/m\mathbb{L} : m \mid c\overline{u}(G'^{\dagger})\right\}.$$

Proof: For $c' \in \widehat{C'}$, $uc' \in u\mathbb{L}/m\mathbb{L} \subset \mathbb{L}/m\mathbb{L}$, $(m/u) \mid c'(G'^{\dagger})$, and $m \mid uc'(G'^{\dagger}) \mid uc'\overline{u}(G'^{\dagger})$ imply $uc' \in \widehat{C}$. Conversely, for $c \in \widehat{C}$, it follows from $m \mid c\overline{u}(G'^{\dagger})$ and $\gcd(\overline{u}, m) = 1$ that $m \mid c(G'^{\dagger})$. Then $m \mid c(G'^{\dagger})(A'^{\dagger}) = cm/u$ implies $u \mid c$. If $c' = c/u$, then $c' \in \mathbb{L}/(m/u)\mathbb{L}$, $m \mid c(G'^{\dagger}) = uc'(G'^{\dagger})$, $(m/u) \mid c'(G'^{\dagger})$, and $c' \in \widehat{C'}$. □

Corollary 1: Let the assumption be as in Proposition 1. Suppose $\gcd(u, m/u) = 1$. Then $\{G\}_m^{\ddagger} = \left\{uG' : G' \in \{G'\}_{m/u}^{\ddagger}\right\}$. In particular, for $u \in R \setminus \{0\}$ with $\gcd(u, \overline{u}) = 1$, $\{G\}_u^{\ddagger} = \{uI\}$.

Proof: For $G' \in \{G'\}_{m/u}^{\ddagger}$, because $C' = \mathbb{L}G'/(m/u)\mathbb{L} \to \mathbb{L}uG'/m\mathbb{L} = C$, $c' \mapsto uc'$, is one to one and onto, it follows from Lemma 4 that $uG' \in \{G\}_m^{\ddagger}$. Conversely, for $G \in \{G\}_m^{\ddagger}$, it follows from Proposition 1 and Lemma 4 that $G/u \in \{G'\}_{m/u}^{\ddagger}$. □

As shown in Proposition 1 and Corollary 1, under certain conditions, $u\{G'\}_{m/u}^{\dagger} = \{G\}_m^{\dagger}$ and $u\{G'\}_{m/u}^{\ddagger} = \{G\}_m^{\ddagger}$. Because the decision of $\{G\}_m^{\dagger}$ and $\{G\}_m^{\ddagger}$ results in the decision of $\{G\}_{m/u}^{\dagger}$ and $\{G\}_{m/u}^{\ddagger}$, from now on we assume $e_i = 0$ in (1), in other words, $mR = \overline{m}R$.

IV. PROPERTIES OF GENERATOR MATRICES

A. THE CASE OF $mR = \overline{m}R$

Assumption 1: In this subsection, we assume that a fixed $m \in R \setminus \{0\}$ is conjugate-invariant, i.e., $\overline{m}R = mR$, if and only if $\overline{m} = \epsilon m$ for some $\epsilon \in R^{\times}$.

Proposition 2: A generator matrix of $\widetilde{C}$ is equal to $G^{\dagger}$, in other words, $\widetilde{C} = \mathbb{L}G^{\dagger}/m\mathbb{L}$. In particular, $\left|\widehat{C}\right| |C| = |\mathbb{L}/m\mathbb{L}|$.

Proof: It follows from $AG = GA = mI$ that $G^{\dagger}A^{\dagger} = A^{\dagger}G^{\dagger} = \overline{m}I = \epsilon mI$. Then $\widetilde{C} = (m\mathbb{L} + \mathbb{L}G^{\dagger})/m\mathbb{L} = \mathbb{L}G^{\dagger}/m\mathbb{L}$. □

Remark 8: If $mR \neq \overline{m}R$, then $\left|\widehat{C}\right| |C| \neq |\mathbb{L}/m\mathbb{L}|$ in general. For example, if $l = 1$ and $G = 2 + i \in \{G\}_{2+i}$, then $\mathbb{L}G/(2+i)\mathbb{L} = \{0\} \subset \mathbb{L}/(2+i)\mathbb{L} = \{0, \pm 1, \pm i\}$. Moreover $\widehat{C} = \{a \in \mathbb{L}/(2+i)\mathbb{L} : (2+i) \mid a(2-i)\} = \{0\}$. Thus $1 = \left|\widehat{C}\right| |C| \neq |\mathbb{L}/m\mathbb{L}| = 5$.

Proposition 3: A generator matrix of $\widehat{C}$ is equal to $A^{\dagger}$, in other words, $\widehat{C} = \mathbb{L}A^{\dagger}/m\mathbb{L}$.

Proof: It follows from $A^{\dagger}G^{\dagger} = G^{\dagger}A^{\dagger} = \epsilon mI$ that $(m\mathbb{L} + \mathbb{L}A^{\dagger})/m\mathbb{L} = \mathbb{L}A^{\dagger}/m\mathbb{L} \subset \widehat{C}$. On the other hand, it follows from $G^{\dagger}A^{\dagger} = \epsilon mI$ and Proposition 2 that $\left|\mathbb{L}A^{\dagger}/m\mathbb{L}\right| = \left|\det(G^{\dagger})\right|^2 = |\det(G)|^2 = |\mathbb{L}/m\mathbb{L}|/|C| = \left|\widehat{C}\right|$. Thus $\mathbb{L}A^{\dagger}/m\mathbb{L} = \widehat{C}$. □

Proposition 4: Assume that $m = p$ is a rational prime and R/mR is a finite field, which occurs if and only if $p \equiv 3 \bmod 4$ if $R = \mathbb{Z}[i]$ and $p \equiv 2 \bmod 3$ if $R = \mathbb{Z}[\omega]$. If we identify $R/mR = \mathbb{F}_{p^2}$, then, for $f \in R/mR$, $\overline{f} = f^p$. In particular, if m satisfies the assumptions, then $\widehat{C}$ agrees with the Hermitian dual code $C^{\perp_{\mathrm{H}}} = \left\{c \in \left(\mathbb{F}_{p^2}\right)^l : c\left((d^p)^{\top}\right) = 0, \forall d \in C\right\}$ of C as $\mathbb{F}_{p^2}$-linear codes, where $c \in \left(\mathbb{F}_{p^2}\right)^l$ is identified to the vector $c = (c_1, \cdots, c_l) \in \mathbb{L}/m\mathbb{L} = (R/mR)^l$ and $d^p = ((d_1)^p, \cdots, (d_l)^p) \in \left(\mathbb{F}_{p^2}\right)^l$.

Proof: Because $f \mapsto \overline{f}$ belongs to the Galois group of $R/mR = \mathbb{F}_{p^2}$ over $\mathbb{F}_p$ which is generated by $f \mapsto f^p$ and the order of $f \mapsto \overline{f}$ is equal to two, $\overline{f} = f^p$. □

B. THE CASE OF $m = m_1 m_2$, $m_1 R = \overline{m_1} R$, $m_2 R = \overline{m_2} R$, AND $\gcd(m_1, m_2) = 1$

Assumption 2: In this subsection, we assume that a fixed $m \in R \setminus \{0\}$ satisfies $m = m_1 m_2$ for some $m_1, m_2 \in R$ with $m_1 R = \overline{m_1} R$, $m_2 R = \overline{m_2} R$, and $\gcd(m_1, m_2) = 1$.

Proposition 5: Suppose that $G_1 \in \{G_1\}_{m_1}$, $G_2 \in \{G_2\}_{m_2}$, and $G \in \{G\}_m$ satisfy $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$. Then $m \,|\, G(G^\dagger)$ if and only if $m_1 \,|\, G_1(G_1^\dagger)$ and $m_2 \,|\, G_2(G_2^\dagger)$.

Proof: We first show the 'if' part. It follows from $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$ that $G = BG_1 = DG_2$ for some $B, D \in M_l(R)$. Then

$$m_1 \,|\, G(G^\dagger) = (BG_1)((G_1^\dagger)(B^\dagger))$$
$$m_2 \,|\, G(G^\dagger) = (DG_2)((G_2^\dagger)(D^\dagger)).$$

It follows from $\gcd(m_1, m_2) = 1$ that $m \,|\, G(G^\dagger)$.

We next show the 'only if' part. It follows from Theorem 1 that $\mathbb{L}G + m_1\mathbb{L} = \mathbb{L}G_1$, which implies $BG + m_1 D = G_1$ for some $B, D \in M_l(R)$. Then it follows from $m \,|\, G(G^\dagger)$ that

$$m_1 \,|\, G_1(G_1^\dagger) = (BG + m_1 D)((G^\dagger)(B^\dagger) + \overline{m_1}(D^\dagger)). \quad \square$$

C. THE CASE OF $m = w\overline{w}$ AND $\gcd(w, \overline{w}) = 1$

Assumption 3: In this subsection, we assume that a fixed $m \in R \setminus \{0\}$ satisfies $m = w\overline{w}$ for some $w \in R$ with $\gcd(w, \overline{w}) = 1$.

Proposition 6: Suppose that $G_1 \in \{G_1\}_w$, $G_2 \in \{G_2\}_{\overline{w}}$, and $G \in \{G\}_m$ satisfy $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$. Then $m \,|\, G(G^\dagger)$ if and only if $w \,|\, G_1(G_2^\dagger)$.

Proof: We first show the 'if' part. It follows from $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$ that $G = BG_1 = DG_2$ for some $B, D \in M_l(R)$. Then

$$w \,|\, G(G^\dagger) = (BG_1)((G_2^\dagger)(D^\dagger))$$
$$\overline{w} \,|\, G(G^\dagger) = (DG_2)((G_1^\dagger)(B^\dagger)).$$

It follows from $\gcd(w, \overline{w}) = 1$ that $m \,|\, G(G^\dagger)$.

We next show the 'only if' part. It follows from Theorem 1 that $\mathbb{L}G + w\mathbb{L} = \mathbb{L}G_1$, which implies $BG + wD = G_1$ for some $B, D \in M_l(R)$. It follows from Theorem 1 that $\mathbb{L}G + \overline{w}\mathbb{L} = \mathbb{L}G_2$, which implies $EG + \overline{w}F = G_2$ for some $E, F \in M_l(R)$. Then it follows from $m \,|\, G(G^\dagger)$ that

$$w \,|\, G_1(G_2^\dagger) = (BG + wD)((G^\dagger)(E^\dagger) + w(F^\dagger)). \quad \square$$

Corollary 2: Let the assumption be as in Proposition 6. Suppose $G_1(G_2^\dagger) = wM$ for some $M \in M_l(R)$. Then $|\det(M)| = 1$ if and only if $|\det(G)|^2 = |m|^l$.

Proof: It follows from the assumption of Proposition 6 and Theorem 1 that $\det(G_1)\det(G_2) = \det(G)$, and moreover,

$$|\det(M)| = 1 \iff |\det(G_1)| \left|\det(G_2^\dagger)\right| = |w|^l$$
$$\iff |\det(G)| = |w|^l \iff |\det(G)|^2 = |m|^l. \quad \square$$

V. APPLICATION OF PRIME ELEMENT DECOMPOSITION

Theorem 2 (Cf. [9], [10]): For $m \in R \setminus \{0\}$, let $m = \prod_{x=1}^{t} v_x \prod_{y=t+1}^{t+z} w_y \overline{w_y}$, where $v_x, w_y \in R$, $\gcd(v_x, m/v_x) = \gcd(w_y, m/w_y) = \gcd(\overline{w_y}, m/\overline{w_y}) = \gcd(w_y, \overline{w_y}) = 1$, and $v_x R = \overline{v_x} R$ for all $1 \le x \le t$ and $t < y \le t+z$. Then there exists a one-to-one and onto map

$$\beta : \{G\}_m^\dagger \to \prod_{x=1}^{t} \{G_x\}_{v_x}^\dagger \times \prod_{y=t+1}^{t+z} \left\{ \left(G_y^{(1)}, G_y^{(2)}\right) \,\middle|\, \begin{array}{l} G_y^{(1)} \in \{G\}_{w_y}, G_y^{(2)} \in \{G\}_{\overline{w_y}}, \\ G_y^{(1)}\left(G_y^{(2)\dagger}\right) \equiv 0I \bmod w_y \end{array} \right\}, \tag{2}$$

where $\mathbb{L}G + v_x\mathbb{L} = \mathbb{L}G_x$, $\mathbb{L}G + w_y\mathbb{L} = \mathbb{L}G_y^{(1)}$, $\mathbb{L}G + \overline{w_y}\mathbb{L} = \mathbb{L}G_y^{(2)}$, and

$$\mathbb{L}G = \left(\bigcap_{x=1}^{t} \mathbb{L}G_x\right) \cap \left(\bigcap_{y=t+1}^{t+z} \left(\mathbb{L}G_y^{(1)} \cap \mathbb{L}G_y^{(2)}\right)\right).$$

Proof: Define β as α which is paired the factors of $\{G_x\}_{m_x}$ for $m_x = w_y, \overline{w_y}$ in Theorem 1 if they are included. Then it follows from Propositions 5,6 that the images of β and β^{-1} are included in both sides of (2), respectively. □

For $m \in R \setminus \{0\}$ with $mR = \overline{m}R$ and self-orthogonal C, because $|C| \le \left|\widehat{C}\right|$ and $|C|^2 \le |\mathbb{L}/m\mathbb{L}|$ by Proposition 2, C is self-dual if and only if $|C|^2 = |\mathbb{L}/m\mathbb{L}|$, which is equivalent to $|\det(G)|^2 = |m|^l$ by Lemma 3. Thus, if $mR = \overline{m}R$, $\{G\}_m^\ddagger = \left\{G \in \{G\}_m^\dagger : |\det(G)|^2 = |m|^l\right\}$.

Corollary 3 (Cf. [9], [10]): Let the assumption be as in Theorem 2. Then there exists a one-to-one and onto map $\gamma : \{G\}_m^\ddagger \to \prod_{x=1}^{t} \{G_x\}_{v_x}^\ddagger \prod_{y=t+1}^{t+z} \{G_y\}_{w_y}$, where $\mathbb{L}G + v_x\mathbb{L} = \mathbb{L}G_x$, $\mathbb{L}G + w_y\mathbb{L} = \mathbb{L}G_y$, $A_y G_y = w_y I$, and $\mathbb{L}G = \left(\bigcap_{x=1}^{t} \mathbb{L}G_x\right) \cap \left(\bigcap_{y=t+1}^{t+z} \left(\mathbb{L}G_y \cap \mathbb{L}A_y^\dagger\right)\right)$.

Proof: If $G_y^{(1)}\left(G_y^{(2)\dagger}\right) = wM$ for some $M \in M_l(R)$ with $|\det(M)| = 1$, then it follows from $G_y^{(1)} A_y^{(1)} = wI$ that $G_y^{(2)} = M^\dagger \left(A_y^{(1)\dagger}\right)$, which implies that, for any $G_y^{(1)} \in \{G_y\}_w$, $G_y^{(2)}$ is uniquely determined. Conversely, it similarly follows from $G_y^{(2)}\left(G_y^{(1)\dagger}\right) = \overline{w}M^\dagger$ that, for any $G_y^{(2)} \in \{G_y\}_{\overline{w}}$, $G_y^{(1)}$ is uniquely determined. Thus, if β is restricted to $\{G\}_m^\ddagger$, then $\left(G_y^{(1)}, G_y^{(2)}\right) = \left(G_y^{(1)}, M^\dagger\left(A_y^{(1)\dagger}\right)\right)$, $\mathbb{L}G_y^{(1)} \cap \mathbb{L}G_y^{(2)} = \mathbb{L}G_y^{(1)} \cap \mathbb{L}A_y^{(1)\dagger}$, and β can be identified with γ. □

VI. EXAMPLES

A. THE CASE OF $R = \mathbb{Z}[i]$

Remark 9 (Cf. b of the Definition of Reduced G): The simplest method to decide $\epsilon \in R^\times$ of $\epsilon g_{r,r}$ uniquely in the reduced generator matrix $G = (g_{r,s})$ is to be $\Re(\epsilon g_{r,r}) > 0$ and $\Im(\epsilon g_{r,r}) \ge 0$, which is not preserved, however, by multiplication, e.g., $(1+2i)(2+3i) = -4+7i$. A congruence equation $\epsilon g_{r,r} \equiv 1 \bmod t$ is often used for appropriate $t \in R$ to decide $\epsilon \in R^\times$. In [4], $t = (1+i)^3$ is adopted.

In this subsection, we adopt $t = 2 + i$ to treat it similarly in $\mathbb{Z}[\omega]$. Because $\{k \in R : [\![k/(2+i)]\!] = 0\} = \{0, \pm 1, \pm i\} = \{0\} \cup R^\times$, it is shown that, for $g \in R$ with $(2 + i) \nmid g$, there exists a unique $\epsilon \in R^\times$ such that $\epsilon g \equiv 1 \bmod (2 + i)$, and for $g = \varepsilon(2 + i)^e$ with $\varepsilon \in R^\times$, we choose $\varepsilon^{-1} g = (2 + i)^e$. By the unique factorization in R, for $g \in R \setminus \{0\}$, there exists a unique ϵ such that $\epsilon g = (2 + i)^{e_0} g_1^{e_1} \cdots g_a^{e_a}$ with positive $e_0, \cdots, e_a \in \mathbb{Z}$, where, for $1 \le b \le a$, $g_b \equiv 1 \bmod (2 + i)$ and $R/g_b R$ is a finite field. For example, $1+2i \equiv -i$, $2+3i \equiv 1 \bmod (2+i)$ and $i(1+2i)(2+3i) = -7-4i \equiv 1 \bmod (2+i)$.

Example 4: We determine the self-dual R-modules in $\mathbb{L}/3\mathbb{L}$ for $l = 2$. If $C = \mathbb{L}G_1/3\mathbb{L}$ is self-dual, then $|\det(G_1)| = 3$. Thus $G_1 = \begin{pmatrix} -3i & 0 \\ 0 & 1 \end{pmatrix}$ or $G_1 = \begin{pmatrix} 1 & g \\ 0 & -3i \end{pmatrix}$ for some $g \in R$, but $\begin{pmatrix} -3i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -3i & 0 \\ 0 & 1 \end{pmatrix}^\dagger \not\equiv 0I \bmod 3$. On the other hand,

$$G_1 G_1^\dagger = \begin{pmatrix} 1 & g \\ 0 & -3i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \overline{g} & 3i \end{pmatrix} = \begin{pmatrix} 1+|g|^2 & 3ig \\ -3i\overline{g} & 9 \end{pmatrix} \equiv 0I \bmod 3$$

if and only if $|g|^2 \equiv 2 \bmod 3$. If we choose $R/3R = \{g_1 + g_2 i : g_1, g_2 = 0, \pm 1\}$ by 3 of Remark 1, $|g|^2 \equiv 2 \bmod 3$ if and only if $g = \pm 1 \pm i$ and $\pm 1 \mp i$. Thus there exist four self-dual R-modules $\mathbb{L}G_1/3\mathbb{L}$ with

$$A_1 G_1 = \begin{pmatrix} 3 & \pm 1 \mp i \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & \pm 1 \pm i \\ 0 & -3i \end{pmatrix} = \begin{pmatrix} 3 & \mp 1 \mp i \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & \pm 1 \mp i \\ 0 & -3i \end{pmatrix} = 3I.$$

Example 5: We determine the self-dual R-modules in $\mathbb{L}/5\mathbb{L}$ for $l = 2$. Because $5 = (2 + i)(2 - i)$ with $-(2 + i) + (1 + i)(2 - i) = 1$, we have to determine first all R-modules in $\mathbb{L}/(2 + i)\mathbb{L}$ and second the self-dual ones in $\mathbb{L}/5\mathbb{L}$ by Corollary 3. If we choose $R/(2 + i)R = \{0, \pm 1, \pm i\}$ by 3 of Remark 1, all R-modules in $\mathbb{L}/(2 + i)\mathbb{L}$ are $\mathbb{L}G_0/(2 + i)\mathbb{L}$ with

$$\begin{aligned} A_0 G_0 &= \begin{pmatrix} 1 & 0 \\ 0 & 2+i \end{pmatrix} \begin{pmatrix} 2+i & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2+i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2+i \end{pmatrix} \\ &= \begin{pmatrix} 2+i & 0 \\ 0 & 2+i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2+i & 0 \\ 0 & 2+i \end{pmatrix} \\ &= \begin{pmatrix} 2+i & \mp 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \pm 1 \\ 0 & 2+i \end{pmatrix} = \begin{pmatrix} 2+i & \mp i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \pm i \\ 0 & 2+i \end{pmatrix} \\ &= (2+i)I. \end{aligned}$$

Consider $G_0 = \begin{pmatrix} 2+i & 0 \\ 0 & 1 \end{pmatrix}$. Then $A_0^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & 2-i \end{pmatrix}$ and $\mathbb{L}G_2 = \mathbb{L}G_0 \cap \mathbb{L}A_0^\dagger$ with $G_2 = \begin{pmatrix} 2+i & 0 \\ 0 & -2+i \end{pmatrix}$. Similarly, if we consider $G_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2+i \end{pmatrix}$, then $G_2 = \begin{pmatrix} -2+i & 0 \\ 0 & 2+i \end{pmatrix}$. If $G_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then $G_2 = \begin{pmatrix} -2+i & 0 \\ 0 & -2+i \end{pmatrix}$. If $G_0 = \begin{pmatrix} 2+i & 0 \\ 0 & 2+i \end{pmatrix}$, then $G_2 = \begin{pmatrix} 2+i & 0 \\ 0 & 2+i \end{pmatrix}$.

Next, consider $G_0 = \begin{pmatrix} 1 & \pm 1 \\ 0 & 2+i \end{pmatrix}$. Then $A_0^\dagger = \begin{pmatrix} 2-i & 0 \\ \mp 1 & 1 \end{pmatrix} = \begin{pmatrix} 2-i & \mp 1 \\ \mp 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \mp 1 \\ 0 & -2+i \end{pmatrix}$. If $\mathbb{L}G_2 = \mathbb{L}G_0 \cap \mathbb{L}A_0^\dagger$, i.e.,

$$\begin{pmatrix} 1 & g \\ 0 & -5 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & -2+i \end{pmatrix} \begin{pmatrix} 1 & \pm 1 \\ 0 & 2+i \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 2+i \end{pmatrix} \begin{pmatrix} 1 & \mp 1 \\ 0 & -2+i \end{pmatrix},$$

then $g = \pm 1 + a(2 + i) = \mp 1 + b(-2 + i)$, i.e., $\pm 2i = \pm 1 + (\pm i)(2+i) = \mp 1 + (\mp i)(-2+i)$. Thus $G_2 = \begin{pmatrix} 1 & \pm 2i \\ 0 & -5 \end{pmatrix}$.

Finally, consider $G_0 = \begin{pmatrix} 1 & \pm i \\ 0 & 2+i \end{pmatrix}$. Then $A_0^\dagger = \begin{pmatrix} 2-i & 0 \\ \pm i & 1 \end{pmatrix} = \begin{pmatrix} 2-i & \mp i \\ \pm i & 0 \end{pmatrix} \begin{pmatrix} 1 & \mp i \\ 0 & -2+i \end{pmatrix}$. If $\mathbb{L}G_2 = \mathbb{L}G_0 \cap \mathbb{L}A_0^\dagger$, i.e.,

$$\begin{pmatrix} 1 & g \\ 0 & -5 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & -2+i \end{pmatrix} \begin{pmatrix} 1 & \pm i \\ 0 & 2+i \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 2+i \end{pmatrix} \begin{pmatrix} 1 & \mp i \\ 0 & -2+i \end{pmatrix},$$

then $g = \pm i + a(2 + i) = \mp i + b(-2 + i)$, i.e., $\mp 2 = \pm i + (\mp 1)(2+i) = \mp i + (\pm 1)(-2+i)$. Thus $G_2 = \begin{pmatrix} 1 & \mp 2 \\ 0 & -5 \end{pmatrix}$. Thus there exist eight self-dual R-modules $\mathbb{L}G_2/5\mathbb{L}$ with

$$\begin{aligned} A_2 G_2 &= \begin{pmatrix} \pm 2-i & 0 \\ 0 & \mp 2-i \end{pmatrix} \begin{pmatrix} \pm 2+i & 0 \\ 0 & \mp 2+i \end{pmatrix} \\ &= \begin{pmatrix} \pm 2-i & 0 \\ 0 & \pm 2-i \end{pmatrix} \begin{pmatrix} \pm 2+i & 0 \\ 0 & \pm 2+i \end{pmatrix} \\ &= \begin{pmatrix} 5 & \pm 2i \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & \pm 2i \\ 0 & -5 \end{pmatrix} = \begin{pmatrix} 5 & \pm 2 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & \pm 2 \\ 0 & -5 \end{pmatrix} = 5I. \end{aligned}$$

Example 6: Because $15 = 3(2 + i)(2 - 1)$, all self-dual R-modules $\mathbb{L}G/15\mathbb{L}$ are derived from self-dual R-modules $\mathbb{L}G_1/3\mathbb{L}$ and $\mathbb{L}G_2/5\mathbb{L}$ by $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$. We compute G with $G_1 = \begin{pmatrix} 1 & 1+i \\ 0 & -3i \end{pmatrix}$ and $G_2 = \begin{pmatrix} 1 & 2 \\ 0 & -5 \end{pmatrix}$. If $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$, i.e.,

$$\begin{pmatrix} 1 & g \\ 0 & 15i \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & -5 \end{pmatrix} \begin{pmatrix} 1 & 1+i \\ 0 & -3i \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & -3i \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & -5 \end{pmatrix},$$

then $g = 1+i-a3i = 2-b5$, i.e., $7-5i = 1+i-(2+2i)3i = 2-(-1+i)5$. Thus $G = \begin{pmatrix} 1 & 7-5i \\ 0 & 15i \end{pmatrix}$ and

$$AG = \begin{pmatrix} 15 & 5+7i \\ 0 & -i \end{pmatrix} \begin{pmatrix} 1 & 7-5i \\ 0 & 15i \end{pmatrix} = 15I.$$

B. THE CASE OF $R = \mathbb{Z}[\omega]$

Remark 10 (Cf. b of the Definition of Reduced G): In [4], a congruence equation $\epsilon g \equiv 2 \bmod 3$ is used to decide $\epsilon \in R^\times$ of ϵg uniquely for $g \in R$ with $\gcd(g, 3) = 1$.

In this subsection, if $\gcd(g_{r,r}, 3+\omega) = 1$, we adopt $\epsilon g_{r,r} \equiv 1 \bmod (3+\omega)$ to decide $\epsilon \in R^\times$ of $\epsilon g_{r,r}$ uniquely in the reduced generator matrix $G = (g_{r,s})$. Because $\{k \in R : [\![k/(3+\omega)]\!] = 0\} = \{0, \pm 1, \pm\omega, \pm(1+\omega)\} = \{0\} \cup R^\times$, it is shown that, for $g \in R$ with $(3+\omega) \nmid g$, there exists a unique $\epsilon \in R^\times$ such that $\epsilon g \equiv 1 \bmod (3+\omega)$, and for $g = \varepsilon(3+\omega)^e$ with $\varepsilon \in R^\times$, we choose $\varepsilon^{-1} g = (3+\omega)^e$. By the unique factorization in R, for $g \in R \setminus \{0\}$, there exists a unique ϵ such that $\epsilon g = (3+\omega)^{e_0} g_1^{e_1} \cdots g_a^{e_a}$ with positive $e_0, \cdots, e_a \in \mathbb{Z}$, where, for $1 \le b \le a$, $g_b \equiv 1 \bmod (3+\omega)$ and $R/g_b R$ is a finite field.

Example 7: We determine the self-dual R-modules in $\mathbb{L}/2\mathbb{L}$ for $l = 2$. If $C = \mathbb{L}G_1/2\mathbb{L}$ is self-dual, then $|\det(G_1)| = 2$. Thus $G_1 = \begin{pmatrix} 2\omega & 0 \\ 0 & 1 \end{pmatrix}$ or $G_1 = \begin{pmatrix} 1 & g \\ 0 & 2\omega \end{pmatrix}$ for some $g \in R$, but $\begin{pmatrix} 2\omega & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2\omega & 0 \\ 0 & 1 \end{pmatrix}^\dagger \not\equiv 0I \bmod 2$. On the other hand,

$$G_1 G_1^\dagger = \begin{pmatrix} 1 & g \\ 0 & 2\omega \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \overline{g} & 2\omega^2 \end{pmatrix} = \begin{pmatrix} 1+|g|^2 & 2\omega^2 g \\ 2\omega\overline{g} & 4 \end{pmatrix} \equiv 0I \bmod 2$$

if and only if $|g|^2 \equiv 1 \bmod 2$. If we choose $R/(2\omega)R = \{0, -\omega, 1, 1+\omega\}$ by 3 of Remark 1, $|g|^2 \equiv 1 \bmod 2$ if and only if $g = -\omega, 1, 1+\omega$. Thus there exist three self-dual R-modules $\mathbb{L}G_1/2\mathbb{L}$ with

$$A_1 G_1 = \begin{pmatrix} 2 & 1+\omega \\ 0 & \omega^2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 2\omega \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & \omega^2 \end{pmatrix} \begin{pmatrix} 1 & -\omega \\ 0 & 2\omega \end{pmatrix} = \begin{pmatrix} 2 & \omega \\ 0 & \omega^2 \end{pmatrix} \begin{pmatrix} 1 & 1+\omega \\ 0 & 2\omega \end{pmatrix} = 2I.$$

Example 8: We determine the self-dual R-modules in $\mathbb{L}/3\mathbb{L}$ for $l = 2$. Note that $R/3R$ is not a field because $(-2-\omega)^2 = 3(1+\omega)$. All R-modules $C \subset \mathbb{L}/3\mathbb{L}$ with $|C|^2 = |\mathbb{L}/3\mathbb{L}|$ are $\mathbb{L}G_2/3\mathbb{L}$ for

$$A_2 G_2 = \begin{pmatrix} -\omega & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 3(1+\omega) & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1+\omega & f\omega \\ 0 & -1+\omega \end{pmatrix} \begin{pmatrix} -2-\omega & f \\ 0 & -2-\omega \end{pmatrix} = \begin{pmatrix} 3 & g\omega \\ 0 & -\omega \end{pmatrix} \begin{pmatrix} 1 & g \\ 0 & 3(1+\omega) \end{pmatrix} = 3I,$$

where $f \in R/(-2-\omega)R$ and $g \in R/(3(1+\omega))R$. Consider $G_2 = \begin{pmatrix} 3(1+\omega) & 0 \\ 0 & 1 \end{pmatrix}$. Because

$$\begin{pmatrix} 3(1+\omega) & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3(1+\omega) & 0 \\ 0 & 1 \end{pmatrix}^\dagger \not\equiv 0I \bmod 3,$$

$\mathbb{L}G_2/3\mathbb{L}$ is not self-dual.

Next, consider $G_2 = \begin{pmatrix} -2-\omega & f \\ 0 & -2-\omega \end{pmatrix}$. If

$$G_2 G_2^\dagger = \begin{pmatrix} -2-\omega & f \\ 0 & -2-\omega \end{pmatrix} \begin{pmatrix} \overline{-2-\omega} & 0 \\ \overline{f} & \overline{-2-\omega} \end{pmatrix} = \begin{pmatrix} 3+|f|^2 & f\overline{(-2-\omega)} \\ \overline{f}(-2-\omega) & 3 \end{pmatrix} \equiv 0I \bmod 3,$$

then $f\overline{(-2-\omega)} \equiv 0 \bmod 3$ and $f = 0$.

Finally, consider $G_2 = \begin{pmatrix} 1 & g \\ 0 & 3(1+\omega) \end{pmatrix}$. If

$$G_2 G_2^\dagger = \begin{pmatrix} 1 & g \\ 0 & 3(1+\omega) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \overline{g} & 3\overline{(1+\omega)} \end{pmatrix} = \begin{pmatrix} 1+|g|^2 & g3\overline{(1+\omega)} \\ \overline{g}3(1+\omega) & 9 \end{pmatrix} \equiv 0I \bmod 3$$

and we choose $R/3(1+\omega)R = \{0, \pm 1, \pm\omega, \pm(1+\omega), \pm(2+\omega)\}$ by 3 of Remark 1, then there is no such g with $|g|^2 \equiv 2 \bmod 3$.

Thus there exist one self-dual R-module $\mathbb{L}G_2/3\mathbb{L}$ with

$$A_2 G_2 = \begin{pmatrix} -1+\omega & 0 \\ 0 & -1+\omega \end{pmatrix} \begin{pmatrix} -2-\omega & 0 \\ 0 & -2-\omega \end{pmatrix} = 3I.$$

Example 9: All self-dual R-modules $\mathbb{L}G/6\mathbb{L}$ are derived from self-dual R-modules $\mathbb{L}G_1/2\mathbb{L}$ and $\mathbb{L}G_2/3\mathbb{L}$ by $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$. We compute G with $G_1 = \begin{pmatrix} 1 & 1+\omega \\ 0 & 2\omega \end{pmatrix}$ and $G_2 = \begin{pmatrix} -2-\omega & 0 \\ 0 & -2-\omega \end{pmatrix}$. If $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$, then

$$G = G_1 G_2 = \begin{pmatrix} -2-\omega & -1-2\omega \\ 0 & 2-2\omega \end{pmatrix},$$

$$AG = \begin{pmatrix} -2+2\omega & -1-2\omega \\ 0 & 2+\omega \end{pmatrix} \begin{pmatrix} -2-\omega & -1-2\omega \\ 0 & 2-2\omega \end{pmatrix} = 6I.$$

VII. CONCLUSION

In this paper, for codes over the residue ring with modulo $m \in R$ of Gaussian or Eisenstein integer ring R, we have proposed a method of constructing self-orthogonal and self-dual codes from codes modulo powers of prime elements appearing in the prime-element decomposition of m. In particular, in Proposition 4, we have shown that, if $R/mR = \mathbb{F}_{p^2}$, the dual code $\widehat{C} \subset \mathbb{L}/m\mathbb{L}$ corresponds to the Hermitian dual code over $\mathbb{F}_{p^2}$. Thus Corollary 3 is an analogue of [6, Theorem 4.2] and [10, Propositions 3,4] for quasi-cyclic codes over $\mathbb{F}_q$ in the sense that the conjugation in R corresponds to reciprocal polynomials in $\mathbb{F}_q[x]$, and Theorem 2 can be said to be its generalization to self-orthogonal codes. As future works, concerning recent applications using codes over the residue rings of Gaussian and Eisenstein integers, we should specifically find useful codes of this types with high error correction capability according to the communication channels.

REFERENCES

[1] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic cyclic codes," *Des., Codes Cryptogr.*, vol. 6, no. 1, pp. 21–35, Jul. 1995.

[2] C. Camarero and C. Martínez, "Quasi-perfect Lee codes of radius 2 and arbitrarily large dimension," *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1183–1192, Mar. 2016.

[3] W. Cary Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Their Appl.*, vol. 11, no. 3, pp. 451–490, Aug. 2005.

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. Berlin, Germany: Springer: 1990.

[5] J.-L. Kim and J. Park, "Steganography from perfect codes on Cayley graphs over Gaussian integers, Eisenstein–Jacobi integers and Lipschitz integers," *Des., Codes Cryptogr.*, vol. 90, pp. 2967–2989, Dec. 2022.

[6] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: Finite fields," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2751–2760, Nov. 2001.

[7] H. Matsui, "On generator matrices and parity check matrices of generalized integer codes," *Des., Codes Cryptogr.*, vol. 74, no. 3, pp. 681–701, Mar. 2015.

[8] H. Matsui, "Multiplicative structure and Hecke rings of generator matrices for codes over quotient rings of Euclidean domains," *Mathematics*, vol. 5, no. 4, p. 82, Dec. 2017, doi: 10.3390/math5040082.

[9] H. Matsui, "A modulus factorization algorithm for self-orthogonal and self-dual integer codes," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 101, no. 11, pp. 1952–1956, 2018.

[10] H. Matsui, "A modulus factorization algorithm for self-orthogonal and self-dual quasi-cyclic codes via polynomial matrices," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 104, no. 11, pp. 1649–1653, 2021.

[11] H. Morita, M. Fujisawa, and S. Sakata, "Two-dimensional Lee-error-correcting codes on hexagonal signal constellations," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Kanazawa, Japan, Oct. 2021, pp. 1–6, doi: 10.1109/ITW48936.2021.9611434.

[12] H. Morita, M. Fujisawa, and S. Sakata, "Error-correcting codes in the two-dimensional lee metric on square and hexagonal signal constellations," *TechRxiv*, Sep. 2022, doi: 10.36227/techrxiv.21173695.v1.

[13] E. Yildiz, "On bounds for quantum error correcting codes over EJ-integers," *Electron. Notes Discrete Math.*, vol. 70, pp. 89–94, Dec. 2018.

HAJIME MATSUI received the Ph.D. degree from the Graduate School of Mathematics, Nagoya University, Japan, in 1999. He was a Postdoctoral Fellow and a Research Associate with the Toyota Technological Institute, Japan, from 1999 to 2002 and from 2002 to 2006, respectively, where he has been an Associate Professor, since 2006. His research interests include number theory, error-correcting codes, and computer science. He received the Best Paper Award from IEICE, in 2017 and 2022.