Construction and Secrecy Gain of Formally Unimodular Lattices in Odd Dimensions

Maiara F. Bollauf, Hsuan-Yin Lin, and Øyvind Ytrehus
Simula UiB, N–5006 Bergen, Norway
Emails: {maiara, lin, oyvindy}@simula.no

2023 IEEE Information Theory Workshop (ITW) | 979-8-3503-0149-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ITW55543.2023.10160234

Abstract—**In contrast to binary codes, odd-length self-dual codes exist over the integers modulo 4. Lately, the use of lattices constructed from codes over $\mathbb{Z}_4$ to guarantee secure communication in a Gaussian wiretap channel was proposed and shown to exceed the performance of lattices from binary codes. This performance is measured regarding the secrecy gain, a criterion that depends on a lattice's volume and theta series. Formally unimodular lattices, i.e., lattices with the same theta series as their dual, have presented promising results with respect to the secrecy gain. While previous contributions in the literature were mainly focused on even-dimensional lattices, this paper addresses the secrecy gain of odd-dimensional formally unimodular lattices obtained from codes over $\mathbb{Z}_4$, together with a novel construction of such codes.**

I. Introduction

The wiretap channel is a communication model proposed by Wyner in [1], where a legit communication between two parties, Alice and Bob, is wiretapped through a secondary channel by an eavesdropper Eve. Based on the relative qualities of the two channels, a coding scheme is designed to ensure that Bob can decode at close to zero error rate while the *equivocation* (i.e., the posterior entropy about the message after observing her channel output) for Eve is maximized.

In particular, results on Gaussian wiretap channel assuming lattice encoding/decoding techniques [2]–[4] have considered mainly two design criteria to evaluate the performance of a given lattice: the secrecy gain [2] and the flatness factor [4]. The former is based on minimizing Eve's success probability of correctly estimating the transmitted message, while the latter concerns the minimization of the mutual information between Eve's channel observation and the message. Despite the different definitions, both criteria rely on optimizing the theta function of a lattice.

Since the theta series of a unimodular lattice is defined through Hecke's theorem [5, Th. 7, p. 187], its respective secrecy gain is completely characterized [3]. Moreover, due to the connection between the weight enumerator of a linear binary code and the theta function of a lattice obtained from the code via Construction A, the secrecy gain of even-dimensional Construction A lattices was also studied [6]. Recently, a generalization of unimodular lattices was introduced, the *formally unimodular lattices*, which are lattices with the same theta series as their dual [7], [8]. Formally unimodular Construction A lattices can outperform the secrecy gain of unimodular lattices.

The secrecy gain of formally unimodular lattices constructed from codes over $\mathbb{Z}_4$ via the so-called Construction A_4 was initially studied in [9], where improvements were shown when considering even-length formally self-dual codes, i.e., codes such that their symmetrized weight enumerator coincides with its dual. This paper extends this idea to lattices constructed from odd-length formally self-dual codes. It appears to be the first work that universally addresses odd-dimensional formally unimodular (which includes unimodular) lattices, which have not been studied extensively in the past literature. More specifically, the contributions of this paper are:

i) An original construction of odd-length codes over $\mathbb{Z}_4$, called *odd extension* codes, and conditions for such codes to be self-dual (see Proposition 2).
ii) We demonstrate that the secrecy gain of odd-dimensional formally unimodular lattices obtained from odd extension codes, denoted by *odd extension lattices*, can be at least *as good as* the best secrecy gain in the preceding even dimension (see Proposition 3). Gains are also observed with respect to previous results for odd-dimensional unimodular lattices.
iii) Upper bounds for the secrecy gain of Type I formally unimodular lattices are recalled on a comparative basis (see Theorem 2).

Given that codes over $\mathbb{Z}_4$ can be entirely characterized (up to equivalence) through their generator matrices according to [10, eq. (2)], we have also done a complete search in some dimensions, which allows us to state the best possible secrecy gain of Construction A_4 formally unimodular lattices obtained from formally self-dual codes in dimension 7.

This paper is organized as follows: Sec. II establishes relevant definitions, Sec. III recalls results on how to calculate the secrecy gain of Construction A_4 lattices, Sec. IV defines and studies properties of the odd extension codes, and Secs. V and VI explore theoretical and numerical results of the secrecy gain of odd extensions lattices. Sec. VII concludes the paper. Due to page limitations, some proofs are omitted and can be found in the extended version [11].

II. Definitions and Preliminaries

A. Notation

We denote by $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ the set of naturals, integers, and reals, respectively. $[i:j] \triangleq \{i, i+1, \dots, j\}$ for $i, j \in \mathbb{Z}$,

This work was supported in part by the Norwegian Research Council through the qsIoT grant, project number 274889.

$i \leq j$. Vectors are *row* vectors and boldfaced, e.g., $\boldsymbol{x}$. The all-zero vector is denoted by $\mathbf{0}$. Matrices and sets are represented by capital sans serif letters and calligraphic uppercase letters, respectively, e.g., X and $\mathcal{X}$. $\mathsf{X}_{k\times n}$ represents a matrix of size $k\times n$, and a square matrix of size n is denoted by X_n. We omit the subscript of a matrix if it is clearly understood from the context. An identity matrix and an all-zero matrix are denoted by I and O, respectively. We denote by, respectively, $w_{\mathrm{H}}(\boldsymbol{x})$ and $w_{\mathrm{Lee}}(\boldsymbol{x})$ the *Hamming* weight and the *Lee* weight of a vector $\boldsymbol{x} \in \mathbb{Z}_m^n$, where $\mathbb{Z}_m = \{0,\ldots,m-1\}$ is the ring of integers modulo m. In this work, m can be 2 or 4. We use the code parameters $[n,M]$ or $[n,M,d_{\mathrm{Lee}}]$ to denote a linear code $\mathscr{C}$ of length n, M codewords, and minimum *Lee distance* $d_{\mathrm{Lee}} \triangleq \min_{\boldsymbol{x},\boldsymbol{y}\in\mathscr{C}} w_{\mathrm{Lee}}(\boldsymbol{x}-\boldsymbol{y})$. $(\cdot)^{\mathsf{T}}$ represents the transpose of its argument and $\langle\cdot,\cdot\rangle$ denotes the inner product between two vectors over $\mathbb{Z}_m$. A generator matrix of a code $\mathscr{C}$ is represented by $\mathsf{G}^{\mathscr{C}}$, while $\mathscr{C}^{\mathsf{G}}$ represents the corresponding linear code generated by G. $\phi_m\colon \mathbb{Z}_m^n \to \mathbb{Z}^n$ is defined as the natural embedding, i.e., $\phi_m(x)$ maps each element $x \in \mathbb{Z}_m$ to the corresponding integer.

B. Basics on Codes and Lattices

In this section, we briefly review well-known concepts related to codes over $\mathbb{Z}_m$, $m \in \{2,4\}$, and their respective lattices. Let $\mathscr{A}$ be an $[n,M]$ code over $\mathbb{Z}_2$. Its *weight enumerator* is

$$W_{\mathscr{A}}(x,y) = \sum_{\boldsymbol{a}\in\mathscr{A}} x^{n-w_{\mathrm{H}}(\boldsymbol{a})} y^{w_{\mathrm{H}}(\boldsymbol{a})}.$$

A $\mathbb{Z}_4$-*linear code* $\mathscr{C}$ of length n is an additive subgroup of $\mathbb{Z}_4^n$. If $\mathscr{C}$ is a $\mathbb{Z}_4$-linear code of length n, then $\mathscr{C}^{\perp} \triangleq \{\boldsymbol{x} \in \mathbb{Z}_4^n\colon \langle\boldsymbol{x},\boldsymbol{y}\rangle = 0, \text{ for all } \boldsymbol{y}\in\mathscr{C}\}$ is the *dual code* of $\mathscr{C}$.

From [12, Prop. 1.1], it is well-known that any $\mathbb{Z}_4$-linear code is *permutation equivalent* to a code $\mathscr{C}$ with a generator matrix G in *standard form*

$$\mathsf{G} = \begin{pmatrix} \mathsf{I}_{k_1} & \mathsf{A}_{k_1\times k_2} & \mathsf{B}_{k_1\times(n-k_1-k_2)} \\ \mathsf{O}_{k_2\times k_1} & 2\mathsf{I}_{k_2} & 2\mathsf{C}_{k_2\times(n-k_1-k_2)} \end{pmatrix}, \qquad (1)$$

where A and C are binary matrices, and B is defined over $\mathbb{Z}_4$. Such a code $\mathscr{C}$ is said to be of *type* $4^{k_1}2^{k_2}$.

The *symmetrized weight enumerator (swe)* of a $\mathbb{Z}_4$-linear code $\mathscr{C}$ is defined as

$$\mathrm{swe}_{\mathscr{C}}(a,b,c) = \sum_{\boldsymbol{c}\in\mathscr{C}} a^{n_0(\boldsymbol{c})} b^{n_1(\boldsymbol{c})+n_3(\boldsymbol{c})} c^{n_2(\boldsymbol{c})},$$

where $n_i(\boldsymbol{c}) \triangleq |\{j\in[1:n]\colon c_j = i\}|$, $i \in \mathbb{Z}_4$.[1] The corresponding MacWilliams identity for $\mathbb{Z}_4$-linear codes is given by [12, Th. 2.3]

$$\begin{aligned}\mathrm{swe}_{\mathscr{C}}&(a,b,c)\\ &= \frac{1}{|\mathscr{C}^{\perp}|}\mathrm{swe}_{\mathscr{C}^{\perp}}(a+2b+c, a-c, a-2b+c).\end{aligned} \qquad (2)$$

We have the following families of codes over $\mathbb{Z}_4$: A code $\mathscr{C}$ is *self-dual* if $\mathscr{C} = \mathscr{C}^{\perp}$. If there is a permutation of coordinates and a (possible) change of signs carried out by a mapping π, such that $\mathscr{C} = \pi(\mathscr{C}^{\perp})$, $\mathscr{C}$ is called *isodual*. If $\mathscr{C}$ and $\mathscr{C}^{\perp}$ have the same symmetrized weight enumerator, i.e., $\mathrm{swe}_{\mathscr{C}}(a,b,c) = \mathrm{swe}_{\mathscr{C}^{\perp}}(a,b,c)$, $\mathscr{C}$ is a *formally self-dual* code.

From (2), the swe of a code belonging to any of these classes satisfies

$$\mathrm{swe}_{\mathscr{C}}(a,b,c) = \frac{1}{|\mathscr{C}|}\mathrm{swe}_{\mathscr{C}}(a+2b+c, a-c, a-2b+c). \quad (3)$$

A (full rank) *lattice* $\Lambda \subset \mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$, which can be viewed as $\Lambda = \{\boldsymbol{\lambda} = \boldsymbol{u}\mathsf{L}_{n\times n}\colon \boldsymbol{u}\in\mathbb{Z}^n\}$, where the n rows of L form a lattice basis in $\mathbb{R}^n$. The *volume* of Λ is $\mathrm{vol}(\Lambda) = |\det(\mathsf{L})|$. If a lattice Λ has generator matrix L, then the lattice $\Lambda^{\star} \subset \mathbb{R}^n$ generated by $\left(\mathsf{L}^{-1}\right)^{\mathsf{T}}$ is called the *dual lattice* of Λ. For lattices, the analogue of the weight enumerator of a code is the *theta series*, defined as follows.

Definition 1 (Theta series): Let Λ be a lattice, its *theta series* is given by

$$\Theta_{\Lambda}(z) = \sum_{\boldsymbol{\lambda}\in\Lambda} q^{\|\boldsymbol{\lambda}\|^2},$$

where $q \triangleq e^{i\pi z}$ and $\mathrm{Im}\{z\} > 0$.

Analogously, the spirit of the MacWilliams identity can be captured by the *Jacobi's formula* [5, eq. (19), Ch. 4]

$$\Theta_{\Lambda}(z) = \mathrm{vol}(\Lambda^{\star})\Big(\frac{i}{z}\Big)^{\frac{n}{2}}\Theta_{\Lambda^{\star}}\Big(-\frac{1}{z}\Big).$$

A lattice is said to be *integral* if the inner product of any two lattice vectors is an integer. An integral lattice such that $\Lambda = \Lambda^{\star}$ is called a *unimodular* lattice. A lattice Λ is called *isodual* if it can be obtained from its dual $\Lambda^{\star}$ by (possibly) a rotation or reflection. In [7], a new and broader family was presented, namely, the *formally unimodular lattices*, that consists of lattices having the same theta series as their duals, i.e., $\Theta_{\Lambda}(z) = \Theta_{\Lambda^{\star}}(z)$. We say that a formally unimodular lattice is of *Type I* if it is also integral and is of *Type II* if the inner product of any two lattice vectors is a multiple of 2.

From [8, Prop. 12], a formally unimodular lattice Λ has $\mathrm{vol}(\Lambda) = 1$. Hence, the theta series of a formally unimodular lattice is such that

$$\Theta_{\Lambda}(z) = \Big(\frac{i}{z}\Big)^{\frac{n}{2}}\Theta_{\Lambda}\Big(-\frac{1}{z}\Big).$$

Lattices can be constructed from binary linear codes via the so-called Construction A [5], defined as follows.

Definition 2 (Construction A): Let $\mathscr{A}$ be a binary $[n,M]$ code, then $\Lambda_{\mathrm{A}}(\mathscr{A}) \triangleq \frac{1}{\sqrt{2}}(\phi_2(\mathscr{A}) + 2\mathbb{Z}^n)$ is a lattice.

There is an analogue of Construction A for codes over $\mathbb{Z}_4$, which is called *Construction* A_4.

Definition 3 (Construction A_4 *[13, Ch. 12.5.3]):* If $\mathscr{C}$ is a $\mathbb{Z}_4$-linear code, then $\Lambda_{\mathrm{A}_4}(\mathscr{C}) = \frac{1}{2}(\phi_4(\mathscr{C}) + 4\mathbb{Z}^n)$ is a lattice.

It is known that $\Lambda_{\mathrm{A}_4}(\mathscr{C})$ is a unimodular lattice if and only if the $\mathbb{Z}_4$-linear code $\mathscr{C}$ is a self-dual code [12, Prop. 12.2]. For notational convenience, sometimes the mapping ϕ_m is omitted.

Considering the $\mathbb{Z}_4$-linear code $\mathscr{C}$, the theta series of a Construction A_4 lattice can be expressed as follows.

[1] The exponent of b combines weights 1 and 3 according to the Lee distance definition.

Proposition 1 ([9]): Let $\mathscr{C}$ be a $\mathbb{Z}_4$-linear code with $\mathrm{swe}_{\mathscr{C}}(a,b,c)$, then the theta series of $\Lambda_{\mathrm{A}_4}(\mathscr{C})$ is

$$\Theta_{\Lambda_{\mathrm{A}_4}(\mathscr{C})}(z) = \mathrm{swe}_{\mathscr{C}}(\vartheta_3(4z), {}^{\vartheta_2(z)}/_2, \vartheta_2(4z)).$$

III. Secrecy Gain of Construction A_4 Lattices

The secrecy gain of Construction A_4 lattices was discussed in a former work [9]. We review the main results in this section and start with the definition of *secrecy gain* [3].

Definition 4 (Secrecy function and secrecy gain [3, Defs. 1 and 2]): Let Λ be a lattice with volume $\mathrm{vol}(\Lambda) = \nu^n$. The secrecy function of Λ is defined by

$$\Xi_\Lambda(\tau) \triangleq \frac{\Theta_{\nu\mathbb{Z}^n}(i\tau)}{\Theta_\Lambda(i\tau)},$$

for $\tau \triangleq -iz > 0$. The *(strong) secrecy gain* of a lattice is given by $\xi_\Lambda \triangleq \sup_{\tau>0} \Xi_\Lambda(\tau)$.

The higher the secrecy gain of a lattice, the more secure the lattice wiretap code is [3]. Hence, the objective is to design good lattices to achieve a high secrecy gain. The first family of lattices studied in the literature was unimodular lattices [6], [14], due to the tractability of their theta functions. Also, for unimodular lattices, Belfiore and Solé conjectured that the following holds.

Conjecture 1: [15] The secrecy function of a unimodular lattice attains its maximum at $\tau = 1$.

This result was demonstrated to hold for infinitely many unimodular lattices [16]. Recently, techniques to extend this result to formally unimodular lattices constructed from codes over $\mathbb{Z}_m$ were discussed in [7], [9], together with indications of superior results for the secrecy gain, when compared to unimodular lattices.

An alternative way of expressing the secrecy gain of Construction A_4 lattices from formally self-dual codes over $\mathbb{Z}_4$ allows a simplified search for its maximum as follows.

Theorem 1 ([9, Th. 2]): Let $\mathscr{C}$ be a formally self-dual code over $\mathbb{Z}_4$. Then

$$\Big[\Xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C})}(\tau)\Big]^{-1} = \frac{\mathrm{swe}_{\mathscr{C}}\big(1+t, \sqrt[4]{1-t^4}, 1-t\big)}{2^n},$$

where $0 < t(\tau) \triangleq {}^{\vartheta_4(i\tau)}/_{\vartheta_3(i\tau)} < 1$. Moreover, define $h_{\mathscr{C}}(t) \triangleq \mathrm{swe}_{\mathscr{C}}\big(1+t, \sqrt[4]{1-t^4}, 1-t\big)$ for $0 < t < 1$. Then, maximizing the secrecy function $\Xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C})}(\tau)$ is equivalent to determining the minimum of $h_{\mathscr{C}}(t)$ on $t \in (0,1)$.

Example 1: Consider a $[7, 2^7]$ code $\mathscr{C}$ over $\mathbb{Z}_4$, with symmetrized weight enumerator given by

$$\begin{aligned}&\mathrm{swe}_{\mathscr{C}}(a,b,c)\\ &\quad= a^7 + a^6c + 3a^5c^2 + 12a^4b^2c + 3a^4c^3 + 12a^3b^2c^2\\ &\qquad + 3a^3c^4 + 24a^2b^4c + 12a^2b^2c^3 + 3a^2c^5\\ &\qquad + 8ab^6 + 24ab^4c^2 + 12ab^2c^4 + ac^6 + 8b^6c + c^7.\end{aligned}$$

Observe that the swe satisfies the MacWilliams identity (2).

If we set $h_{\mathscr{C}}(t) = \mathrm{swe}_{\mathscr{C}}\big(1+t, \sqrt[4]{1-t^4}, 1-t\big)$, then $h'_{\mathscr{C}}(t) = 0$ has a unique solution in the interval $t \in (0,1)$, $t = {}^1/_{\sqrt[4]{2}}$, which is a minimum. Therefore, $\xi_{\Lambda_{\mathrm{A}}(\mathscr{C})} \approx 1.172$. $\Diamond$

IV. Odd Extension Codes

Unlike binary codes, codes over $\mathbb{Z}_4$ admit self-dual (and formally self-dual) codes of odd length. We will use the term *odd extension codes* to describe $\mathbb{Z}_4$ codes generated by

$$\mathsf{G}^{\mathscr{C}_{\mathrm{oext}}} \triangleq \begin{pmatrix} & a_1 & & \\ \mathsf{I}_\eta & \vdots & & \mathsf{B}_\eta \\ & a_\eta & & \\ 0\cdots\cdots 0 & 2 & 2c_1 & 2c_2\cdots\cdots 2c_\eta \end{pmatrix}. \tag{4}$$

It will result in a $[2\eta+1, 4^\eta 2^1]$ $\mathbb{Z}_4$-linear code. The construction is inspired by (1) with $k_1 = \eta$ and $k_2 = 1$, where A and C are chosen to be $\mathsf{A} = \boldsymbol{a}^\mathsf{T} = (a_1, \cdots, a_\eta)^\mathsf{T}$ and $\mathsf{C} = \boldsymbol{c} = (c_1, c_2, \cdots, c_\eta)$, respectively, $a_i, c_i \in \mathbb{Z}_2$, $i \in [\eta]$. Similar construction for odd-length isodual codes over binary rings can be found in [17, Th. 3.8].

The odd extension construction is defined for a general choice of B_η. However, we will mostly consider the case where B_η is a *pure or bordered circulant matrix* [13, Ch. 9.8], i.e.,

$$\mathsf{B}_\eta^{\mathrm{pc}} \triangleq \begin{pmatrix} r_1 & r_2 & r_3 & \cdots & r_\eta \\ r_\eta & r_1 & r_2 & \cdots & r_{\eta-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_2 & r_3 & r_4 & \cdots & r_1 \end{pmatrix} \text{ or} \tag{5}$$

$$\mathsf{B}_\eta^{\mathrm{bc}} \triangleq \begin{pmatrix} \alpha & \beta & \beta & \cdots & \beta \\ \gamma & r_1 & r_2 & \cdots & r_{\eta-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma & r_2 & r_3 & \cdots & r_1 \end{pmatrix}, \tag{6}$$

where $\alpha, \beta, \gamma \in \mathbb{Z}_4$ and $r_i \in \mathbb{Z}_4$, $i \in [\eta]$.

If $\mathscr{C}_{\mathrm{oext}}$ is generated as in (4) using (5) or (6), we call such code an *odd extension code from double circulant code*. Moreover, we know from [10, Eq. (3)] that its dual code is generated by

$$\mathsf{G}^{\mathscr{C}_{\mathrm{oext}}^{\perp}} = \begin{pmatrix} & c_1 & & \\ -\mathsf{B}_\eta^\mathsf{T} - \boldsymbol{c}^\mathsf{T}\boldsymbol{a} & \vdots & & \mathsf{I}_\eta \\ & c_\eta & & \\ 2a_1\cdots\cdots 2a_\eta & 2 & 0 & 0\cdots\cdots 0 \end{pmatrix}.$$

We now give conditions for an odd extension code to be self-dual.

Proposition 2: Consider an odd extension code $\mathscr{C}_{\mathrm{oext}}$ generated by $\mathsf{G}^{\mathscr{C}_{\mathrm{oext}}}$ as in (4). Then, $\mathscr{C}_{\mathrm{oext}}$ is self-dual if and only if the following conditions hold

i) $\boldsymbol{a}^\mathsf{T}\boldsymbol{a} + \mathsf{B}\mathsf{B}^\mathsf{T} \equiv 3\mathsf{I}_\eta \pmod 4$,
ii) $2\boldsymbol{a} + 2\boldsymbol{c}\mathsf{B}^\mathsf{T} \equiv \boldsymbol{0} \pmod 4$.

Proof: Since $\mathscr{C}_{\mathrm{oext}}$ is self-dual if and only if $\mathsf{G}^{\mathscr{C}_{\mathrm{oext}}}\big(\mathsf{G}^{\mathscr{C}}_{\mathrm{oext}}\big)^\mathsf{T} = \mathsf{O}_{\eta+1}$, we have

$$\begin{pmatrix} \mathsf{I}_\eta & \boldsymbol{a}^\mathsf{T} & \mathsf{B}_\eta \\ \boldsymbol{0} & 2 & 2\boldsymbol{c} \end{pmatrix} \begin{pmatrix} \mathsf{I}_\eta & \boldsymbol{0}^\mathsf{T} \\ \boldsymbol{a} & 2 \\ \mathsf{B}_\eta^\mathsf{T} & \boldsymbol{c}^\mathsf{T} \end{pmatrix} = \mathsf{O}_{\eta+1}$$

by using $\mathsf{G}^{\mathscr{C}_{\mathrm{oext}}}$ as in (4). Thus, this gives that $\mathsf{I} + \boldsymbol{a}^\mathsf{T}\boldsymbol{a} + \mathsf{B}\mathsf{B}^\mathsf{T} = \mathsf{O}_\eta$ and $2\boldsymbol{a} + 2\boldsymbol{c}\mathsf{B}^\mathsf{T} \equiv \boldsymbol{0} \pmod 4$, which leads to conditions i) and ii) stated in the proposition. ■

Example 2: Consider a $[13, 2^{13}]$ formally self-dual code $\mathscr{C}_{\mathrm{oext}}$ over $\mathbb{Z}_4$ generated as in (4), where

$$\mathsf{B}^{\mathsf{pc}} = \begin{pmatrix} 0 & 2 & 1 & 2 & 2 & 2 \\ 2 & 0 & 2 & 1 & 2 & 2 \\ 2 & 2 & 0 & 2 & 1 & 2 \\ 2 & 2 & 2 & 0 & 2 & 1 \\ 1 & 2 & 2 & 2 & 0 & 2 \\ 2 & 1 & 2 & 2 & 2 & 0 \end{pmatrix}$$

is a pure double circulant matrix, $\boldsymbol{c} = (0, 0, 0, 0, 1, 1)$ and $\boldsymbol{a} = (0, 0, 1, 1, 0, 0)$. Since

$$\boldsymbol{a}^{\mathsf{T}}\boldsymbol{a} + \mathsf{B}\mathsf{B}^{\mathsf{T}} = \begin{pmatrix} 1 & 0 & 2 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 & 0 & 1 \end{pmatrix} \neq 3\mathsf{I}_6,$$

this implies that $\mathscr{C}_{\mathrm{oext}}$ is not self-dual. ♢

Example 3: The $[9, 2^9]$ odd extension code generated by

$$\mathsf{G}^{\mathscr{C}_{\mathrm{oext}}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 0 & 0 & 1 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \end{pmatrix}$$

satisfies the conditions of Proposition 2 and it is self-dual. ♢

V. Secrecy Gain of Odd Extension Lattices

Lattices constructed via Construction A_4 from odd extension codes will be called *odd extension lattices*. This section explores the secrecy gain of odd extension formally unimodular lattices. The first property we highlight is that the symmetrized weight enumerator of $\mathscr{C}_{\mathrm{oext}}$ can be obtained from the one of $\mathscr{C}$, generated by $G_{\mathscr{C}} = (\mathsf{I}_\eta \ \mathsf{B}_\eta)$. As a consequence, their secrecy gains coincide.

Proposition 3: Let $\mathscr{C}$ be a $[2\eta, M]$ code over $\mathbb{Z}_4$ with generator matrix $\mathsf{G}^{\mathscr{C}} = (\mathsf{I} \ \ \mathsf{B})$, $\eta \in \mathbb{N}$. Consider a $[2\eta+1, 2M]$ odd extension code $\mathscr{C}_{\mathrm{oext}}$ with the generator matrix

$$\mathsf{G}^{\mathscr{C}_{\mathrm{oext}}} = \begin{pmatrix} \mathsf{I}_\eta & \mathbf{0}^{\mathsf{T}} & \mathsf{B}_\eta \\ \mathbf{0} & 2 & \mathbf{0} \end{pmatrix}.$$

Then, $\mathrm{swe}_{\mathscr{C}_{\mathrm{oext}}}(a, b, c) = \mathrm{swe}_{\mathscr{C}}(a, b, c) \cdot (a + c)$ and $\Xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C})}(\tau) = \Xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_{\mathrm{oext}})}(\tau)$.

Proof: Observe that a codeword $\boldsymbol{v}_{\mathrm{oext}} \in \mathscr{C}_{\mathrm{oext}}$ can be expressed as

$$\begin{aligned} \boldsymbol{v}_{\mathrm{oext}} &= (u_1, \ldots, u_\eta, u_{\eta+1})\mathsf{G}_{\mathscr{C}_{\mathrm{oext}}} \\ &= \left(u_1, \ldots, u_\eta, 2u_{\eta+1}, \sum_{i=1}^{\eta} b_{i,1}u_i, \cdots, \sum_{i=1}^{\eta} b_{i,\eta}u_i\right), \end{aligned}$$

where $(u_1, \ldots, u_\eta, u_{\eta+1}) \in \mathbb{Z}_4^\eta \times \mathbb{Z}_2$ is a message vector.

For convenience, denote by $\boldsymbol{v}_{\mathrm{oext}} \triangleq [\boldsymbol{u}, 2u_{\eta+1}, \boldsymbol{w}]$ and $\boldsymbol{v} \triangleq \boldsymbol{u}\mathsf{G}^{\mathscr{C}} = [\boldsymbol{u}, \boldsymbol{w}]$. Then, we have

$$\begin{aligned} &\mathrm{swe}_{\mathscr{C}_{\mathrm{oext}}}(a, b, c) \\ &\quad= \sum_{[\boldsymbol{u}, 2u_{2\eta+1}, \boldsymbol{w}] \in \mathscr{C}_{\mathrm{oext}}} a^{n_0(\boldsymbol{v}_{\mathrm{oext}})} b^{n_1(\boldsymbol{v}_{\mathrm{oext}}) + n_3(\boldsymbol{v}_{\mathrm{oext}})} c^{n_2(\boldsymbol{v}_{\mathrm{oext}})} \\ &\quad\overset{(a)}{=} \sum_{[\boldsymbol{u}, 0, \boldsymbol{w}] \in \mathscr{C}_{\mathrm{oext}}} a^{n_0(\boldsymbol{v}_{\mathrm{oext}})} b^{n_1(\boldsymbol{v}_{\mathrm{oext}}) + n_3(\boldsymbol{v}_{\mathrm{oext}})} c^{n_2(\boldsymbol{v}_{\mathrm{oext}})} \\ &\qquad+ \sum_{[\boldsymbol{u}, 2, \boldsymbol{w}] \in \mathscr{C}_{\mathrm{oext}}} a^{n_0(\boldsymbol{v}_{\mathrm{oext}})} b^{n_1(\boldsymbol{v}_{\mathrm{oext}}) + n_3(\boldsymbol{v}_{\mathrm{oext}})} c^{n_2(\boldsymbol{v}_{\mathrm{oext}})} \\ &\quad= \sum_{[\boldsymbol{u}, \boldsymbol{w}] \in \mathscr{C}} a^{n_0(\boldsymbol{v})+1} b^{n_1(\boldsymbol{v}) + n_3(\boldsymbol{v})} c^{n_2(\boldsymbol{v})} \\ &\qquad+ \sum_{[\boldsymbol{u}, \boldsymbol{w}] \in \mathscr{C}} a^{n_0(\boldsymbol{v})} b^{n_1(\boldsymbol{v}) + n_3(\boldsymbol{v})} c^{n_2(\boldsymbol{v})+1} \\ &\quad= \mathrm{swe}_{\mathscr{C}}(a, b, c) \cdot (a + c), \end{aligned} \tag{7}$$

where (a) holds since $u_{\eta+1} \in \mathbb{Z}_2$.

Next, using Theorem 1 and (7), we have

$$\begin{aligned} \Xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_{\mathrm{oext}})}(\tau) &= \frac{2^{2\eta+1}}{\mathrm{swe}_{\mathscr{C}_{\mathrm{oext}}}\big(1+t, \sqrt[4]{1-t^4}, 1-t\big)} \\ &= \frac{2^{2\eta+1}}{\mathrm{swe}_{\mathscr{C}}\big(1+t, \sqrt[4]{1-t^4}, 1-t\big) \cdot (1+t+1-t)} \\ &= \frac{2^{2\eta}}{\mathrm{swe}_{\mathscr{C}}\big(1+t, \sqrt[4]{1-t^4}, 1-t\big)} = \Xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C})}(\tau). \end{aligned}$$

■

The next example points out that the swe's between $\mathscr{C}_{\mathrm{oext}}$ and $\mathscr{C}$ can be different.

Example 4: Consider a $[12, 2^{12}]$ code $\mathscr{C}_{\mathrm{pdc}}$ with generator matrix $\mathsf{G} = \begin{pmatrix}\mathsf{I}_\eta & \mathsf{B}_\eta^{\mathsf{pc}}\end{pmatrix}$, where

$$\mathsf{B}_\eta^{\mathsf{pc}} = \begin{pmatrix} 0 & 2 & 1 & 2 & 2 & 2 \\ 2 & 0 & 2 & 1 & 2 & 2 \\ 2 & 2 & 0 & 2 & 1 & 2 \\ 2 & 2 & 2 & 0 & 2 & 1 \\ 1 & 2 & 2 & 2 & 0 & 2 \\ 2 & 1 & 2 & 2 & 2 & 0 \end{pmatrix}.$$

Observe that $\xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_{\mathrm{pdc}})} \approx 1.657$. If we now consider the $[13, 2^{13}]$ code $\mathscr{C}_{\mathrm{oext}}$ generated as in (4), with $\mathsf{B}_\eta = \mathsf{B}_\eta^{\mathsf{pc}}$, $\boldsymbol{a} = (0, 0, 1, 1, 0, 0)$ and $\boldsymbol{c} = (0, 0, 0, 0, 1, 1)$, we would get $\mathrm{swe}_{\mathscr{C}_{\mathrm{oext}}}(a, b, c) \neq \mathrm{swe}_{\mathscr{C}_{\mathrm{pdc}}}(a, b, c) \cdot (a + c)$. However, one can see that $\xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_{\mathrm{oext}})} \approx 1.704 > \xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C}_{\mathrm{pdc}})}$. ♢

Proposition 3 points out that every secrecy gain in a particular even dimension 2η can also be achieved by a respective odd extension code in dimension $2\eta + 1$. On the other hand, Example 4 shows that there are cases when the swe's differ, which could lead to improvements. The remaining question is whether the secrecy gain could be improved concerning odd unimodular lattices [6] and/or with respect to the preceding even dimension. The answer is positive; more details will be explored in the next section.

VI. Secrecy-Good Odd Dimensional Lattices

An upper bound on the secrecy gain of Type I formally unimodular lattices is presented, both for even or odd dimensions. The derivation is similar to the one in [14, Section IV]. However, our approach is based on the technique in our prior work that is sufficient to prove the Belfiore and Solé conjecture for Construction A formally unimodular packings obtained from formally self-dual codes [8]. See the complete proof of [11, Lemma 36].

Theorem 2: For any n-dimensional Type I formally unimodular lattice Λ that satisfies the Belfiore and Solé's conjecture (Conjecture 1) with $2 \leq n \leq 40$, the secrecy gain is upper bounded by

$$\xi_\Lambda \leq \frac{1}{\boldsymbol{\omega}\mathsf{S}^{-1}\boldsymbol{e}_1^\mathsf{T}},$$

where $\boldsymbol{\omega} = \bigl(1, {}^3\!/\!{}_4, \ldots, ({}^3\!/\!{}_4)^\ell\bigr)$, S is an $(\ell{+}1)$ by $(\ell{+}1)$ matrix whose $(s+1)$-th column contains the first $\ell + 1$ coefficients of the power series of $\vartheta_3^{n-8s}(z)\Theta_{\mathbb{E}_8}(z)^s$ for $s \in [0:\ell]$, $\boldsymbol{e}_{s+1}$ is the vector with a 1 in the $(s+1)$-th coordinate and zeros elsewhere, $\mathbb{E}_8$ is the Gosset lattice of dimension 8, and $\ell \triangleq \lfloor {}^n\!/\!{}_8 \rfloor$. Note that

$$\begin{aligned}\Theta_{\mathbb{E}_8}(z) &= \vartheta_3(z)^8 - \vartheta_3^4(z)\vartheta_4^4(z) + \vartheta_4^8(z)\\ &= 1 + 240q^2 + 2160q^4 + 6720q^6 + \cdots.\end{aligned}$$

We present results of the secrecy gain of odd-dimensional formally unimodular Construction A_4 lattices in Table I. In the table, *opdc* refers to an odd extension code, where $\mathsf{B}_\eta^{\text{pc}}$ is a pure circulant matrix as in (5), *obdc* refers to an odd extension code, where $\mathsf{B}_\eta^{\text{bc}}$ is a bordered circulant matrix as in (6).

Values highlighted values are the ones outperforming previously known results in the literature [6]. The upper bound refers to Theorem 2, which concerns only Type I formally unimodular lattices. We remark that since not every formally unimodular lattice is Type I (and neither Type II), it is possible to obtain a good secrecy gain of a formally unimodular lattice that exceeds the upper bound on the secrecy gain of Type I formally unimodular lattices. We can notice that this upper bound is exceeded in dimensions 7, 13, and 15.

Following the notation of (4)–(6), for each dimension, we are going to specify the vectors $\boldsymbol{a}, \boldsymbol{c} \in \mathbb{Z}_2^\eta$, the circulant vector $\boldsymbol{r} = (r_1, \ldots, r_\eta)$ (or $(r_1, \ldots, r_{\eta-1})$) that generates $\mathsf{B}_\eta^{\text{pc}}$ (or $\mathsf{B}_\eta^{\text{bc}}$), and the values of α, β, γ (if applicable) that yield to the respective secrecy gain. For example, in length 7, the vectors $\boldsymbol{a} = \boldsymbol{c} = (0, 0, 0)$, $\boldsymbol{r} = (2, 1, 0)$ indicates the generator matrix

$$\mathsf{G}^{\mathscr{C}_{\text{oext}}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 2 & 1\\ 0 & 0 & 1 & 0 & 1 & 0 & 2\\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \end{pmatrix},$$

which is the generator matrix of the code with swe presented in Example 1. Moreover, we can observe that this $[7, 2^7]$ code is an application of Proposition 3, i.e., an odd extension of a $[6, 2^6]$ code generated by

$$\mathsf{G}^{\mathscr{C}} = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 0\\ 0 & 1 & 0 & 0 & 2 & 1\\ 0 & 0 & 1 & 1 & 0 & 2 \end{pmatrix}.$$

Our code search revealed that this is the highest secrecy gain for Construction A_4 lattices obtained from all the possible $\mathbb{Z}_4$-linear formally self-dual codes of length 7 generated by the standard form as in (1).

TABLE I
Secrecy gain of Odd Extension Construction A_4 lattices

$[2\eta + 1, M, d_{\text{Lee}}]$	Reference	$\xi_{\Lambda_{\mathrm{A}_4}(\mathscr{C})}$	Best-known [6]	Upper bound (Type I)
$[7, 2^7, 2]$	opdc	$\mathbf{1.172}$	–	1
$[9, 2^9, 2]$	obdc	$\mathbf{1.333}$	–	1.391
$[11, 2^{11}, 4]$	opdc	$\mathbf{1.512}$	–	1.524
$[13, 2^{13}, 4]$	opdc, Ex. 4	$\mathbf{1.704}$	–	1.684
$[15, 2^{15}, 6]$	obdc	$\mathbf{1.972}$	1.882	1.882
$[17, 2^{17}, 4]$	opdc	$\mathbf{2.203}$	2.133	2.387
$[19, 2^{19}, 4]$	obdc	$\mathbf{2.641}$	2.462	2.709
$[21, 2^{21}, 6]$	[18, App. A]	2.909	2.909	3.094
$[23, 2^{23}, 10]$	[18, App. A]	3.556	3.556	3.556
$[31, 2^{31}, 6]$	[18, App. A]	6.564	–	6.774

In summary, the parameters for the generator matrices of the codes in Table I are, respectively:

Length 9**:** $\alpha = 2$, $\beta = \gamma = 1$, $\boldsymbol{r} = (1, 2, 3)$, $\boldsymbol{a} = \boldsymbol{c} = (0, 0, 0, 0)$.

Length 11**:** $\boldsymbol{r} = (3, 1, 1, 1, 1)$, $\boldsymbol{a} = \boldsymbol{c} = (0, 1, 1, 1, 1)$.

Length 13**:** $\boldsymbol{r} = (0, 2, 1, 2, 2, 2)$, $\boldsymbol{a} = (0, 0, 1, 1, 0, 0)$, $\boldsymbol{c} = (0, 0, 0, 0, 1, 1)$.

Length 15**:** $\alpha = \beta = \gamma = 1$, $\boldsymbol{r} = (0, 0, 1, 2, 1, 3)$, $\boldsymbol{a} = \boldsymbol{c} = (0, 1, 1, 1, 1, 1, 1)$.

Length 17**:** $\boldsymbol{r} = (0, 0, 0, 1, 2, 0, 0, 2)$, $\boldsymbol{a} = (0, 0, 0, 0, 0, 0, 1, 1)$, $\boldsymbol{c} = (0, 1, 1, 0, 0, 0, 0, 0)$.

Length 19**:** $\alpha = \beta = 1$, $\gamma = 2$, $\boldsymbol{r} = (0, 0, 0, 0, 1, 0, 2, 2)$, $\boldsymbol{a} = (0, 1, 1, 1, 1, 1, 1, 1, 1)$, $\boldsymbol{c} = (1, 1, 1, 1, 1, 1, 1, 1, 1)$.

We remark that there might be equivalent codes to the ones presented here that would result in the same secrecy gain.

VII. Conclusion

We proposed odd extension codes over $\mathbb{Z}_4$ and studied the secrecy gain of their respective odd extension lattices, aiming to maximize the security against a potential eavesdropper in a Gaussian wiretap channel. Cases, where odd extension formally unimodular lattices outperform previous results in the literature (in terms of unimodular lattices or upper bounds for Type I formally unimodular lattices), were highlighted.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] J.-C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," in *Proc. IEEE Int. Symp. Inf. Theory Appl. (ISITA)*, Taichung, Taiwan, Oct. 17–20, 2010.

[3] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5690–5708, Oct. 2016.

[4] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehle, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY, USA: Springer, 1999.

[6] F. Lin and F. Oggier, "A classification of unimodular lattice wiretap codes in small dimensions," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3295–3303, Jun. 2013.

[7] M. F. Bollauf, H.-Y. Lin, and Ø. Ytrehus, "The secrecy gain of formally unimodular lattices on the Gaussian wiretap channel," in *Proc. Int. Zurich Sem. Inf. Commun. (IZS)*, Zurich, Switzerland, Mar. 2–4, 2022, pp. 69–73.

[8] ——, "Formally unimodular packings for the Gaussian wiretap channel," Jun. 2022, arXiv:2206.14171v1 [cs.IT].

[9] ——, "On the secrecy gain of formally unimodular Construction A_4 lattices," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Espoo, Finland, Jun. 26–Jul. 1, 2022, pp. 3226–3231.

[10] J. H. Conway and N. J. A. Sloane, "Self-dual codes over the integers modulo 4," *J. Combinatorial Theory, Ser. A*, vol. 62, no. 1, pp. 30–45, Jan. 1993.

[11] M. F. Bollauf, H.-Y. Lin, and Ø. Ytrehus, "Secrecy gain of formally unimodular lattices from codes over the integers modulo 4," Mar. 2023, arXiv:2303.08083v2 [cs.IT].

[12] Z.-X. Wan, *Quaternary Codes*. World Scientific, Nov. 1997.

[13] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge University Press, 2003.

[14] F. Lin and F. Oggier, "Gaussian wiretap lattice codes from binary self-dual codes," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Lausanne, Switzerland, Sep. 3–7, 2012.

[15] J.-C. Belfiore and P. Solé, "Unimodular lattices for the Gaussian wiretap channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Dublin, Ireland, Aug. 30 – Sep. 3, 2010.

[16] J. Pinchak, "Wiretap codes: Families of lattices satisfying the Belfiore-Solé secrecy function conjecture," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, Jul. 7–12, 2013, pp. 2617–2620.

[17] S. Karadeniz, S. T. Dougherty, and B. Yildiz, "Constructing formally self-dual codes over R_k," *Discrete Appl. Math.*, vol. 167, pp. 188–196, Apr. 2014.

[18] V. Pless, P. Solé, and Z. Qian, "Cyclic self-dual $\mathbb{Z}_4$-codes," *Finite Fields Their App.*, vol. 3, no. 1, pp. 48–69, Jan. 1997.