This document is downloaded from DR-NTU, Nanyang Technological University Library, Singapore.

Title	On LCD Codes and Lattices
Author(s)	Hou, Xiaolu; Oggier, Frédérique
Citation	Hou, X., & Oggier, F. (2016). On LCD Codes and Lattices. 2016 IEEE International Symposium on Information Theory (ISIT), 1501-1505.
Date	2016
URL	http://hdl.handle.net/10220/41415
Rights	© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: http://dx.doi.org/10.1109/ISIT.2016.7541549.

On LCD Codes and Lattices

Xiaolu Hou and Frédérique Oggier
Division of Mathematical Sciences
Nanyang Technological University, Singapore
Email:HO0001LU@e.ntu.edu.sg,frederique@ntu.edu.sg

***Abstract*—LCD (linear complimentary dual) codes are linear codes that trivially intersect their duals. We address the question of an equivalent concept for lattices. We observe basic properties of the intersection of a lattice with its dual, and consider the construction of lattices from LCD codes using Construction A. Lattices obtained from the intersection of a code with its dual via Construction A are further discussed.**

***Index Terms*—Construction A, Lattices, Linear Codes.**

I. Introduction

A linear code is said to have a complementary dual, or to be a linear complementary dual code (LCD) [1], if C meets its dual code $C^\perp$ trivially. Recall that given a linear code C of length n and dimension k, say over the finite field $\mathbb{F}_q$, for q a prime power, $C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n,\ \langle \mathbf{x}, \mathbf{c}\rangle = \sum_i x_i c_i = 0\ \forall \mathbf{c} \in C\}$. For example, the $(3, 2)$ binary parity check code is LCD: a generic codeword $\mathbf{c}$ is of the form $\mathbf{c} = (a_1, a_2, a_1 + a_2)$, $a_1, a_2 \in \mathbb{F}_2$. Its dual $C^\perp$ is the $(3, 1)$ repetition code, and $\langle \mathbf{x}, \mathbf{c}\rangle = 0$ for $\mathbf{x} = (b, b, b)$, $b \in \mathbb{F}_2$. Clearly $C = \{(1, 0, 1), (0, 1, 1), (1, 1, 0), (0, 0, 0)\}$ and $C^\perp = \{(0, 0, 0), (1, 1, 1)\}$ intersect trivially, that is in the whole zero codeword.

LCD codes were introduced by Massey [1], where he proved that asymptotically good LCD codes exist. Furthermore, he showed that LCD codes provide an optimum linear coding solution for the two-user binary adder channel, and he studied the maximum-likelihood decoding problem for LCD codes.

Recently, LCD codes have been proposed to provide counter-measures for side-channel attacks [3]. Constructions of LCD codes over rings have also been provided in [4], together with a linear programming bound on the largest size of an LCD code of given length and minimum distance.

The "continuous" equivalents of linear codes in coding theory are lattices. There are in fact a wealth of connections between linear codes and lattices, in particular via the so-called Constructions A,B,C,D,E [2]. Through these connections, the dual of a linear code is related to that of its corresponding lattice. It is thus natural to wonder how the notion of LCD codes would translate to lattices.

Related works include [5, Method 4], where binary Construction A is considered on the intersection of binary codes, and [6, Section 82F], where a formula that relates the intersection of two lattices is given. It could be applied to intersect a lattice with its dual, though this does not seem to give insight to our computations so far.

We attempt to mimic the definition of LCD codes to lattices and report our basic observations in Section II. It turns out that the notion of intersection between a lattice L and its dual L^* is much less natural than that of a linear code C and its dual $C^\perp$. We identified a lattice L_S that belongs to this intersection. We then compute a few lattices obtained from LCD codes via Construction A in Section III. This as expected yields non-integral lattices, and a few interesting examples are reported. Connections between Construction A applied to the intersection of C and its dual and the lattice L_S are discussed in Section IV. This rises more generally the question of the lattices obtained as preimage of the intersection of a code and its dual via Construction A, which is discussed in Section V. Performance and applications of these lattices are part of future work.

II. Basic Observations

If C is a linear code with dual $C^\perp$, then both are vector subspaces and thus they surely must intersect in $\mathbf{0}$. It turns out that there are codes for which C and $C^\perp$ intersect exactly in $\mathbf{0}$. A lattice and its dual both must contain $\mathbf{0}$ too, however, for lattices whose vectors have rational inner products, and integer inner products in particular, it cannot be that only $\mathbf{0}$ is in the intersection, as we will see next.

Let M be a generator matrix for a lattice L in $\mathbb{R}^n$, with rows $v_1, \ldots, v_n$, meaning that the lattice L is generated as integral linear combinations of $v_1, \ldots, v_n$, and let $G = MM^T$ be the corresponding Gram matrix. Hence

$$L = \{\mathbf{x} = \mathbf{u}M,\ \mathbf{u} \in \mathbb{Z}^n\},$$

and the $i, j-$entry of G is given by $\langle v_i, v_j\rangle = \sum_k v_{ik} v_{jk}$.

Let L^* be the dual lattice of L, that is

$$L^* = \{\mathbf{y} \in \mathbb{R}^n,\ \langle \mathbf{y}, \mathbf{x}\rangle \in \mathbb{Z},\ \forall \mathbf{x} \in L\}.$$

It has generator matrix $(M^T)^{-1} = (M^{-1})^T$.

Lemma 1: If the Gram matrix G of a lattice L has rational entries, then $L \cap L^*$ is a lattice of dimension n. It contains as sublattice the lattice L_S with generator matrix SM, where S is a diagonal matrix with diagonal $s_1, \ldots, s_n$, and s_i is the least common multiple of the denominators of the entries of the ith row of G, $i = 1, \ldots n$.

Proof: Since the entries of G are rational numbers, let s be the least common multiple of all the denominators of the entries of G. Consider the vector

$$w := sv_1 + sv_2 + \cdots + sv_n,$$

for which we have $\langle w, v_i\rangle \in \mathbb{Z}\ \forall i$. This means $w \in L \cap L^*$.

Actually if we let s_i be the least common multiple of the denominators of the entries of row i of G and let $w_i = s_i v_i$, then $\langle w_i, v_j \rangle = s_i \langle v_i, v_j \rangle \in \mathbb{Z}$ and $w_i \in L \cap L^*$. The vectors $\{w_1, \ldots, w_n\}$ are linearly independent over $\mathbb{R}$, and generates a lattice L_S of dimension n, which is a sublattice of $L \cap L^*$, which is therefore also a lattice of dimension n. ∎

When the Gram matrix G has integral coefficients, then the lattice L is integral, which is well known [2] to be equivalent to $L \subseteq L^*$. In the above lemma, this corresponds to S being the identity matrix, in which case $L_S = L$ and $L \cap L^* = L$.

Lemma 2: Consider the lattice L_S of the previous lemma, with generator matrix SM. Then the index of L_S in L is $|\det(S)|$ and the index of L_S in L^* is $|\det(S)\det(G)|$.

Proof: Since the generator matrix of L_S is SM, we have a readily available expression for the basis vectors of L_S as a function of that of L, and thus the index in L is $|\det(S)|$. Then notice that

$$SM = (SMM^T)(M^T)^{-1} = (SG)(M^T)^{-1}$$

thus the index in L^* is $|\det(S)\det(G)|$. ∎

III. Construction A from LCD Codes

We next look at lattices obtained from LCD codes via Construction A. There are several versions of Construction A, we consider one based on number fields [7], which in particular generalizes the standard binary Construction A [2].

Let K be a Galois number field of degree $[K : \mathbb{Q}] = n$ that is totally real, that is, all its embeddings are real. Let $\mathcal{O}_K$ be the ring of integers of K and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$. Then

$$\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f},$$

where $p = \mathfrak{p} \cap \mathbb{Z}$ and f is the inertia degree of p.

Take N a positive integer and consider the map

$$\begin{array}{ccc} \rho : \mathcal{O}_K^N & \to & \mathbb{F}_{p^f}^N \\ (x_1, \ldots, x_N) \mapsto & (x_1 \bmod \mathfrak{p}, \ldots, x_N \bmod \mathfrak{p}). & \end{array}$$

Define b to be the bilinear form

$$b : \mathcal{O}_K^N \times \mathcal{O}_K^N \to \mathbb{R},\ (x, y) \mapsto \tfrac{1}{p} \textstyle\sum_{i=1}^N \mathrm{Tr}\,(x_i y_i).$$

If we take any $C \subseteq \mathbb{F}_{p^f}^N$ a linear code, then the pair $(\rho^{-1}(C), b)$ is a lattice [7][1], which we will denote by Γ_C. The case $K = \mathbb{Q}$ and $p = 2$ is the standard binary Construction A.

It is known for K totally real that if $C \subseteq C^\perp$, then Γ_C is integral [7]. If we further assume $\mathfrak{p}$ is either inert or totally ramified, we have the following converse result.

Proposition 1: If C is not included in $C^\perp$, then Γ_C is not an integral lattice.

Proof: Let $\{\tilde{c_1}, \tilde{c_2}, \ldots, \tilde{c_k}\}$ be a set of $\mathbb{F}_{p^f}-$basis for the linear code C. Let $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_k\}$ be a set of elements in $\mathcal{O}_K^N$ such that $\boldsymbol{c}_i$ is a preimage of $\tilde{c}_i$, $(1 \le i \le k)$. Take $\{v_1, v_2, \ldots, v_n\}$, a $\mathbb{Z}-$basis of $\mathcal{O}_K$. Notice that for $1 \le i \le k,\ 1 \le j \le n$,

$$\rho(v_j \boldsymbol{c}_i) = \rho(v_j)\rho(\boldsymbol{c}_i) = \rho(v_j)\tilde{c}_i.$$

As $\rho(v_j) \in \mathbb{F}_{p^f}$, $\rho(v_j \boldsymbol{c}_i) \in C$, i.e. $v_j \boldsymbol{c}_i \in \Gamma_C$ for all $1 \le i \le k$ and $1 \le j \le n$. Since $C \nsubseteq C^\perp$, take $\boldsymbol{c}_{i_1}, \boldsymbol{c}_{i_2}$ such that $\tilde{c}_{i_1} \cdot \tilde{c}_{i_2} \neq 0$, i.e. $\boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} \notin \mathfrak{p}$. From $\{v_1, \ldots, v_2\}$, take v_{j_0} such that $v_{j_0} \notin \mathfrak{p}$. Suppose

$$b(v_j \boldsymbol{c}_{i_1}, v_{j_0} \boldsymbol{c}_{i_2}) = \frac{1}{p}\mathrm{Tr}\,(v_{j_0} \boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} v_j) \in \mathbb{Z}$$

for all $1 \le j \le n$. As $\{v_j\}_{1 \le j \le n}$ forms a basis for $\mathcal{O}_K$

$$\frac{1}{p}\mathrm{Tr}\,(v_{j_0} \boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} \alpha) \in \mathbb{Z}\ \forall \alpha \in \mathcal{O}_K.$$

Let $\mathcal{D}_K^{-1}$ denote the codifferent of K [12]. Hence

$$\frac{1}{p} v_{j_0} \boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} \in \mathcal{D}_K^{-1} \Longrightarrow v_{j_0} \boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} \in p\mathcal{D}_K^{-1} \cap \mathcal{O}_K = (p) \subseteq \mathfrak{p}.$$

As $v_{j_0} \notin \mathfrak{p}$, we have $\boldsymbol{c}_{i_1} \cdot \boldsymbol{c}_{i_2} \in \mathfrak{p}$ This contradicts with the choice of $\boldsymbol{c}_{i_1}$ and $\boldsymbol{c}_{i_2}$. Thus we must have $b(v_j \boldsymbol{c}_{i_1}, v_{j_0} \boldsymbol{c}_{i_2}) \notin \mathbb{Z}$ for at least one j $(1 \le j \le n)$. As $v_j \boldsymbol{c}_{i_1}, v_{j_0} \boldsymbol{c}_{i_2} \in \Gamma_C$ for all j, we can conclude that the lattice Γ_C is not integral. ∎

We are interested in the intersection between a lattice and its dual, which means here, the intersection of Γ_C and Γ_C^*. When a lattice is integral, some results are known to connect Γ_C^* and $\Gamma_{C^\perp}$. However we are looking at rational lattices here.

We start by noticing connections between Γ_C and $\Gamma_{C^\perp}$.

Lemma 3: Let $C \subseteq \mathbb{F}_{p^f}^N$ be a linear code, then

$$\Gamma_C \cap \Gamma_{C^\perp} = \Gamma_{C \cap C^\perp}.$$

Proof: Take $x \in \mathcal{O}_K^N$, then

$$x \in \Gamma_C \cap \Gamma_{C^\perp} \Longleftrightarrow \rho(x) \in C \text{ and } \rho(x) \in C^\perp.$$

Moreover,

$$\rho(x) \in C \cap C^\perp \Longleftrightarrow x \in \Gamma_{C \cap C^\perp}.$$

∎

Example 1: If we consider the binary Construction A [2] for C the $(3, 2)$ binary parity check code of the introduction, we have for generator matrix M_C and Gram matrix G_C of Γ_C respectively

$$M_C = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix},\ G_C = \begin{bmatrix} 1 & 1/2 & 1 \\ 1/2 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

For $C^\perp$, the $(3, 1)$ repetition code, we have

$$M_{C^\perp} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix},\ G_{C^\perp} = \begin{bmatrix} 3/2 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix}.$$

Finally, since $C \cap C^\perp = \mathbf{0}$, a generator matrix for $\Gamma_{C \cap C^\perp}$ is $\sqrt{2} I_3$ where I_3 is the 3-dimensional identity matrix.

Furthermore, the dual Γ_C^* of Γ_C has Gram matrix

$$\begin{bmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 3/2 \end{bmatrix}.$$

[1]The same holds for K CM, the proof is a slight variation of that for K totally real, where $\mathrm{Tr}\,(x_i \bar{y}_i)$ is used to define b, and $\bar{y}_i$ means the complex conjugate of y_i.

The least common multiple of the denominators of the entries of row i $(1 \leq i \leq 3)$ of G_C are $2, 2, 1$, by Definition of L_S in Lemma 1, the lattice L_S for Γ_C has thus generator matrix

$$\frac{1}{\sqrt{2}}\begin{bmatrix}2&0&0\\0&2&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&0&1\\0&1&1\\0&0&2\end{bmatrix} = \sqrt{2}\begin{bmatrix}1&0&1\\0&1&1\\0&0&1\end{bmatrix}.$$

Notice that $L_S = \Gamma_{C\cap C^\perp}$. This is no coincidence, as we will show in Section IV.

For $K = \mathbb{Q}(\sqrt{5})$, it is known [8] that a generator matrix of Γ_C is given by

$$M_C = \begin{bmatrix} I_K \otimes M & A\tilde{\otimes}M \\ \mathbf{0}_{2N-2k,2k} & I_{N-k} \otimes pM \end{bmatrix}$$

with

$$M = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix},$$

and A such that $(I_k,\ (A \mod p\mathcal{O}_K))$ is a generator matrix of C. Denoting the columns of M (resp. A) by M_i, $i = 1, 2$ (resp. A_i, $i = 1, \ldots, N-k$), we write $A\tilde{\otimes}M = [\sigma_1(A_1) \otimes M_1, \sigma_2(A_1)\otimes M_2, \ldots, \sigma_1(A_{N-k})\otimes M_1, \sigma_2(A_{N-k})\otimes M_2]$, for σ_1, σ_2 the embeddings of $\mathbb{Q}(\sqrt{5})$, applied componentwise.

Example 2: Consider $K = \mathbb{Q}(\sqrt{5})$. Take $p = 2$, a prime that is inert in K. Consider the linear code with generator matrix $(1\ \omega)$, where $\mathbb{F}_4 = \mathbb{F}_2(\omega)$. Then Γ_C has generator matrix

$$\begin{aligned} M_C &= \begin{bmatrix} 1\otimes M & \frac{1+\sqrt{5}}{2}\otimes M_1 & \frac{1-\sqrt{5}}{2}\otimes M_2 \\ 0 & & 2\otimes M \end{bmatrix} \\ &= \frac{1}{2\sqrt{2}}\begin{bmatrix} 2 & 2 & 1+\sqrt{5} & 1-\sqrt{5} \\ 1+\sqrt{5} & 1-\sqrt{5} & 3+\sqrt{5} & 3-\sqrt{5} \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 2+2\sqrt{5} & 2-2\sqrt{5} \end{bmatrix} \end{aligned}$$

and Gram matrix

$$G_C = \begin{bmatrix} 5/2 & 5/2 & 1 & 3 \\ 5/2 & 5 & 3 & 4 \\ 1 & 3 & 4 & 2 \\ 3 & 4 & 2 & 6 \end{bmatrix}$$

We get a lattice with minimum $5/2$, kissing number 8 and determinant 25. The dual lattice has minimum $\frac{1}{2}$ and kissing number 8 with determinant $\frac{1}{25}$.

Using $\mathbb{Q}(\sqrt{5})$ and $p = 2$, other lattices can be found as listed in Table I.

A	$\min(\Gamma_C)$	$K(\Gamma_C)$	$\det(\Gamma_C)$
$\begin{bmatrix}1+w & w\\ 1 & 1+w\end{bmatrix}$	5/2	8	5^4
$\begin{bmatrix}1+w & 0\\ 0 & 1+w\end{bmatrix}$	5/2	16	5^4
$\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$	2	4	5^4
$\begin{bmatrix}1 & 1 & 0\\ 1 & 1 & 0\\ 1 & 0 & 1\end{bmatrix}$	2	4	5^6

TABLE I
EXAMPLES OF LATTICES Γ_C, OBTAINED FROM $\mathbb{Q}(\sqrt{5})$, $p = 2$, C WITH GENERATOR MATRIX $(I_k,\ A)$ OVER $\mathbb{F}_4 = \mathbb{F}_2(w)$, AND THEIR MINIMUM $\min(\Gamma_C)$, KISSING NUMBER $K(\Gamma_C)$ AND DETERMINANT $\det(\Gamma_C)$.

IV. THE LATTICE $\Gamma_{C\cap C^\perp}$

We now focus on the case where p a prime inert in K.

Let $\sigma_1, \ldots, \sigma_n$ be the n real embeddings of K, $\{v_1, \ldots, v_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, and set

$$M = \begin{bmatrix} \sigma_1(v_1) & \sigma_2(v_1) & \ldots & \sigma_n(v_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(v_n) & \sigma_2(v_n) & \ldots & \sigma_n(v_n) \end{bmatrix}. \quad (1)$$

Proposition 2: A generator matrix for Γ_C is given by

$$M_C = \frac{1}{\sqrt{p}}\begin{bmatrix} I_k \otimes M & A\widetilde{\otimes}M \\ \mathbf{0}_{nN-nk,nk} & pI_{N-k}\otimes M \end{bmatrix},$$

where M was defined in (1). A is a matrix such that $(I_k\ \ (A \mod \mathfrak{p}))$ is a generator matrix of C. Denote the columns of M, A by $M_i (i = 1, 2, \ldots, n)$, $A_j (j = 1, 2, \ldots, N-k)$, then

$$\begin{aligned} A\widetilde{\otimes}M := [&\sigma_1(A_1)\otimes M_1, \ldots, \sigma_n(A_1)\otimes M_n, \\ &\ldots, \sigma_n(A_{N-k})\otimes M_1, \sigma_n(A_{N-k})\otimes M_n], \end{aligned}$$

here σ_is are applied componentwise.

Proposition 3: The Gram matrix for Γ_C is given by

$$G_C = \begin{bmatrix} \frac{1}{p}\mathrm{Tr}\left((I + AA^T)\otimes M_1M_1^T\right) & \mathrm{Tr}\left(A\otimes M_1M_1^T\right) \\ \mathrm{Tr}\left(A\otimes M_1M_1^T\right)^T & I_{N-k}\otimes pMM^T \end{bmatrix}. \quad (2)$$

The proofs for both propositions follow the same argument as in [8]. It includes as particular case when K is a real quadratic field used in the above section.

We have

Proposition 4: $\Gamma_C \cap \Gamma_C^* = \Gamma_{C\cap C^\perp}$ and $|\Gamma_C/\Gamma_{C\cap C^\perp}| = p^{nk}$.

Proof: Firstly, if we take any $y \in \Gamma_{C^\perp}$ and $x \in \Gamma_C$, then $\rho(y) \in C^\perp$, $\rho(x) \in C$. We have

$$\rho(y\cdot x) = \rho(y)\cdot\rho(x) = 0 \Longrightarrow y\cdot x \in (p).$$

and hence $\mathrm{Tr}(y\cdot x) \in p\mathbb{Z}$, and

$$b(y,x) = \frac{1}{p}\sum_{i=1}^{N}\mathrm{Tr}(y_ix_i) = \frac{1}{p}\mathrm{Tr}(y\cdot x) \in \mathbb{Z}.$$

We just proved $\Gamma_{C^\perp} \subseteq \Gamma_C^*$. By Lemma 3, we have $\Gamma_{C\cap C^\perp} \subseteq \Gamma_C \cap \Gamma_C^*$. Hence $\Gamma_C \cap \Gamma_C^* \neq \Gamma_{C\cap C^\perp}$ iff there exists Γ' such that $\Gamma_C \cap \Gamma_C^* \supset \Gamma' \supsetneq \Gamma_{C\cap C^\perp}$. Let Δ be the discriminant of the number field K. From the generator matrices, we can tell that for a linear code C_0 of dimension k_0, the lattice Γ_{C_0} has volume $vol(\Gamma_{C_0}) = \Delta^{\frac{N}{2}}p^{n(N-k)-\frac{nN}{2}}$. Then the quotient group $\Gamma_{C^\perp}/\Gamma_{C\cap C^\perp}$ has order [2] $vol(\Gamma_{C\cap C^\perp})/vol(\Gamma_{C^\perp}) = p^{nN-nk}$ and $\Gamma_C^*/\Gamma_{C\cap C^\perp}$ has order $\Delta^N p^{nN-nk}$. As p is inert, we have $p \nmid \Delta$. Thus $\Gamma_{C^\perp}/\Gamma_{C\cap C^\perp}$ is the unique Sylow $p-$subgroup of $\Gamma_C^*/\Gamma_{C\cap C^\perp}$ [10]. Then $\Gamma'/\Gamma_{C\cap C^\perp}$, as a $p-$subgroup of $\Gamma_C^*/\Gamma_{C\cap C^\perp}$, is contained in $\Gamma_{C^\perp}/\Gamma_{C\cap C^\perp}$ [10], which then implies $\Gamma' \subset \Gamma_C$, a contradiction with our assumption that $\Gamma_{C\cap C^\perp} \subsetneq \Gamma'$. ∎

Let L_S be the lattice as defined in Section II for Γ_C, then

Proposition 5: $L_S = \Gamma_{C\cap C^\perp}$.

Proof: We know that $L_S \subseteq \Gamma_{C\cap C^\perp} \subseteq \Gamma_C$. It is enough to prove that

$$|\Gamma_C/\Gamma_{C\cap C^\perp}| = |\Gamma_C/L_S|.$$

We just proved $|\Gamma_C/\Gamma_{C\cap C^\perp}| = p^{nk}$. If we examine G_C, as all entries in A, I, M are elements from $\mathcal{O}_K$, thus all the entries of $\mathrm{Tr}\left(A \otimes M_1 M_1^T\right)$, $\mathrm{Tr}\left(A \otimes M_1 M_1^T\right)^T$ and $I_{N-k} \otimes pMM^T$ are integers.

Also, the entries of $\mathrm{Tr}\left((I + AA^T) \otimes M_1 M_1^T\right)$ are integers. We claim that:

For each row of the matrix $GC1 := \mathrm{Tr}\left((I + AA^T) \otimes M_1 M_1^T\right)$, there exists at least one entry that is not divisible by p.

As there are exactly nk rows in $GC1$, the definition of L_S implies

$$|\Gamma_C/L_S| = p^{nk} = |\Gamma_C/\Gamma_0|.$$

proof of claim: Let $\{\boldsymbol{c}_j\}_{1\le j\le k}$ be the rows of $(I\ A)$, then each $\rho(\boldsymbol{c}_j)$ is a codeword in C. The jth row of $I + AA^T$ is given by $[\boldsymbol{c}_j\cdot\boldsymbol{c}_1,\ \boldsymbol{c}_j\cdot\boldsymbol{c}_2,\ \ldots \boldsymbol{c}_j\cdot\boldsymbol{c}_k]$, $(1 \le j \le k)$. The ith row of $M_1 M_1^T$ is given by $[v_i v_1,\ v_i v_2,\ \ldots v_i v_n]$, $(1 \le i \le n)$. Thus the first n entries of the ijth row of $GC1$ is given by

$$[\mathbf{c}_j\cdot\mathbf{c}_1 v_i v_1,\ \mathbf{c}_j\cdot\mathbf{c}_1 v_i v_2, \ldots \mathbf{c}_j\cdot\mathbf{c}_1 v_i v_n],\ (1 \le i \le n, 1 \le j \le k).$$

Suppose there is one row of $GC1$ that consists of only multiples of p, then there exists one $\mathbf{c}_{j_0}$ and one v_{i_0} such that

$$\frac{1}{p}\mathrm{Tr}\left(\mathbf{c}_{j_0}\cdot\mathbf{c}_1 v_{i_0} v_k\right) \in \mathbb{Z}\ \forall 1 \le k \le n.$$

As $\{v_k\}_{1\le k\le n}$ is a $\mathbb{Z}-$basis for $\mathcal{O}_K$, this implies

$$\frac{1}{p}\mathrm{Tr}\left(\mathbf{c}_{j_0}\cdot\mathbf{c}_1 v_{i_0}\alpha\right) \in \mathbb{Z}\ \forall \alpha \in \mathcal{O}_K.$$

Then we must have

$$\frac{1}{p}\mathbf{c}_{j_0}\cdot\mathbf{c}_1 v_{i_0} \in \mathcal{D}_K^{-1} \iff \mathbf{c}_{j_0}\cdot\mathbf{c}_1 v_{i_0} \in p\mathcal{D}_K^{-1}.$$

But $\mathbf{c}_{j_0}, \mathbf{c}_1, v_{i_0} \in \mathcal{O}_K$, we have $\mathbf{c}_{j_0}\cdot\mathbf{c}_1 v_{i_0} \in (p)$. As $C\cap C^\perp = \{\mathbf{0}\}$, $\rho(\mathbf{c}_{j_0}\cdot\mathbf{c}_1) \ne 0 \Longrightarrow \mathbf{c}_{j_0}\cdot\mathbf{c}_1 \notin (p)$. This leaves us with the only option that $v_{i_0} \in (p)$. However, then this will imply $v_{i_0} v_k \in (p)$. As p is inert, we have $\mathrm{Tr}\left(v_{i_0} v_k\right) \in p\mathbb{Z}$ for all $1 \le k \le n$. And hence the discriminant of K, $\det\left(\mathrm{Tr}\left(v_i v_j\right)\right)_{1\le i,j\le n}$, is divisible by p, which contradicts with the assumption that p is inert. This proves the claim. ∎

Example 3: The above result is not true in general. For example, if we take $K = \mathbb{Q}(\sqrt{5})$, $p = 5$ is totally ramified in K. Consider the linear code $C \subseteq \mathbb{F}_5^2$ with generator matrix $(1\ 1)$. Take $M = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix}$, the generator matrix for Γ_C can be obtained by a similar matrix as in Proposition 2:

$$\begin{aligned} M_C &= \frac{1}{\sqrt{5}}\begin{bmatrix} 1\otimes M & 1\otimes M \\ 0 & \begin{matrix}\sqrt{5} & \sqrt{5} \\ \frac{\sqrt{5}+5}{2} & \frac{5-\sqrt{5}}{2}.\end{matrix} \end{bmatrix} \\ &= \frac{1}{2\sqrt{5}}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1+\sqrt{5} & 1-\sqrt{5} & 1+\sqrt{5} & 1-\sqrt{5} \\ 0 & 0 & 2\sqrt{5} & -2\sqrt{5} \\ 0 & 0 & 5+\sqrt{5} & 5-\sqrt{5} \end{bmatrix} \end{aligned}$$

and Gram matrix is given by

$$G_C = \begin{bmatrix} 4/5 & 2/5 & 0 & 1 \\ 2/5 & 6/5 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 3 \end{bmatrix}.$$

This gives L_S with generator matrix

$$\begin{aligned} &\frac{1}{2\sqrt{5}}\begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1+\sqrt{5} & 1-\sqrt{5} & 1+\sqrt{5} & 1-\sqrt{5} \\ 0 & 0 & 2\sqrt{5} & -2\sqrt{5} \\ 0 & 0 & 5+\sqrt{5} & 5-\sqrt{5} \end{bmatrix} \\ &= \frac{1}{2\sqrt{5}}\begin{bmatrix} 10 & 10 & 10 & 10 \\ 5+5\sqrt{5} & 5-5\sqrt{5} & 5+5\sqrt{5} & 5-5\sqrt{5} \\ 0 & 0 & 2\sqrt{5} & -2\sqrt{5} \\ 0 & 0 & 5+\sqrt{5} & 5-\sqrt{5} \end{bmatrix} \end{aligned}$$

and Gram matrix

$$G_{LS} = \begin{bmatrix} 20 & 10 & 0 & 5 \\ 10 & 30 & 5 & 5 \\ 0 & 5 & 2 & 1 \\ 5 & 5 & 1 & 3 \end{bmatrix}.$$

However, $\Gamma_{C\cap C^\perp}$ is the preimage of $\mathbf{0}$, i.e., the lattice $(\mathfrak{p}^N, b)$, which has Gram matrix

$$G_{\Gamma_{C\cap C^\perp}} = \begin{bmatrix} 2 & 1 & 1 & -2 \\ 1 & 3 & 3 & -1 \\ 1 & 3 & 6 & -2 \\ -2 & -1 & -2 & 4 \end{bmatrix}.$$

In this case $L_S \subsetneq \Gamma_{C\cap C^\perp}$.

The difference of behavior of L_S in that it is either $\Gamma_{C\cap C^\perp} = \Gamma_C \cap \Gamma_C^*$ or it is a sublattice could be a first attempt at defining a "LCD lattice". We conclude this paper by looking at the properties of $\Gamma_{C\cap C^\perp}$ as a modular lattice.

V. The Lattice $\Gamma_{C\cap C^\perp}$ as a Modular Lattice

Next, $\mathfrak{p}$ is either inert or totally ramified. In the last section we proved if $\mathfrak{p}$ is inert $\Gamma_{C\cap C^\perp} = L_S$. In this section, we will look at the relationship between $\Gamma_{C\cap C^\perp}$ and its dual.

Suppose $[K : \mathbb{Q}] = n$. As $C \cap C^\perp$ is self-orthogonal, by the construction of the lattice $\Gamma_{C\cap C^\perp}$, we have

Lemma 4: $\Gamma_{C\cap C^\perp} = (\mathfrak{p}^N, b)$ is an integral lattice of dimension nN.

We will use Γ_N to denote the lattice $\Gamma_{C\cap C^\perp}$, with N indicating that the dimension is nN. When $N = 1$, we have the *ideal lattice* $(\mathfrak{p}, b)$, which has discriminant $p^{-n}N(\mathfrak{p})^2\Delta = p^{2f-n}\Delta$ [11]. Recall that the discriminant of a lattice is the determinant of its Gram matrix [2]. Thus

Lemma 5: Γ_N has discriminant $p^{N(2f-n)}\Delta^N$.

An integral lattice L is said to be an $\ell-$modular lattice, for a positive integer ℓ, if there exists an integral matrix U with determinant ± 1 and a matrix B satisfying $BB^T = I$ such that $\sqrt{\ell}UM^*B = M$, where M, M^* are the generator matrices for L and L^* respectively.

Proposition 6: If the lattice Γ_1 is $\ell-$modular, then the lattices Γ_N are $\ell-$modular for all N.

Proof: Let M_p be a generator matrix for Γ_1, then

$$M_{pN} := \begin{bmatrix} M_p & 0 & \dots & 0 \\ 0 & M_p & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M_p \end{bmatrix}$$

is a generator matrix for Γ_N. Moreover, $M_p^* := (M_p^T)^{-1}$ is a generator matrix for the dual of Γ_1, Γ_1^*, and

$$M_{pN}^* := \begin{bmatrix} M_p^* & 0 & \dots & 0 \\ 0 & M_p^* & \dots & 0 \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & \dots & M_p^* \end{bmatrix}$$

is a generator matrix for Γ_N^*. If Γ_1 is an $\ell-$modular lattice, then there exist U_p, an integral matrix with determinant ± 1, and B_p, a matrix satisfying $B_p B_p^T = I$, such that $\sqrt{\ell} U_p M_p^* B_p = M_p$. Let

$$U_{pN} := \begin{bmatrix} U_p & 0 & \dots & 0 \\ 0 & U_p & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & U_p \end{bmatrix}$$

and

$$B_{pN} := \begin{bmatrix} B_p & 0 & \dots & 0 \\ 0 & B_p & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & B_p \end{bmatrix}.$$

Then $\sqrt{\ell} U_{pN} M_{pN}^* B_{pN} = M_{pN}$. We can then conclude Γ_N is $\ell-$modular. ∎

By Lemma 5 and [13], if Γ_N is an $\ell-$modular lattice,

$$p^{N(2f-n)} \Delta^N = \ell^{\frac{nN}{2}} \iff p^{2f-n} \Delta = \ell^{\frac{n}{2}} \iff \Delta = \ell^{\frac{n}{2}} p^{n-2f}.$$

Proposition 7: If Γ_N is an $\ell-$modular lattice, then $p | \ell$. If furthermore p is inert, then $p^2 || \ell$.

Proof: By the above, we have $\Delta = \ell^{\frac{n}{2}} p^{n-2f}$. If p is inert, $f = n$ and $p \nmid \Delta$, $\Delta = \ell^{\frac{n}{2}} p^{n-2n} = \ell^{\frac{n}{2}} p^{-n}$. As Δ is an integer, we must have $p^2 || \ell$.

If p is totally ramified, $f = 1$ and $\Delta = \ell^{\frac{n}{2}} p^{n-2}$. Suppose $(\ell, p) = 1$. Recall that $|N(\mathcal{D}_K)| = \Delta$, $N(\mathfrak{p}) = p^f = p$. Then we have $\mathfrak{p}^{n-2} || \mathcal{D}_K$. By [12], if p is tamely ramified, $\mathfrak{p}^{n-1} || \mathcal{D}_K$ and if p is widely ramified, $\mathfrak{p}^n | \mathcal{D}_K$. Thus $\mathfrak{p}^{n-2} || \mathcal{D}_K$ is impossible. ∎

Now we consider the special case when $\ell = p$.

By Proposition 7, we can assume p is totally ramified. If Γ_N is $p-$modular,

$$\Delta = p^{\frac{n}{2}} p^{n-2} = p^{\frac{3n}{2}-2}$$

and p is the only prime that ramifies in K.

Let s be the integer that $\mathcal{D}_K = \mathfrak{p}^s$, then

$$N(\mathfrak{p}^s) = p^s = p^{\frac{3n}{2}-2} \Longrightarrow s = \frac{3n}{2} - 2.$$

Proposition 8: If $p \neq 2$ is tamely ramified, Γ_N is $p-$modular if and only if $K = \mathbb{Q}(\sqrt{p})$ and $p \equiv 2, 3 \bmod 4$

Proof: If p is tamely ramified, we have $\frac{3n}{2} - 2 = n - 1$, i.e., $n = 2$. Then K is a quadratic number field with absolute value of discriminant equal to p, hence the conclusion.

Conversely, let $p \equiv 2, 3 \bmod 4$ and $K = \mathbb{Q}(\sqrt{p})$. Then $\Gamma_1 = (\mathfrak{p}, b) = (\sqrt{p}, b)$ and Γ_1^* is $(\mathfrak{p}^*, b)$, where [11]

$$\mathfrak{p}^* = p \mathcal{D}_K^{-1} \mathfrak{p}^{-1} = \mathfrak{p}^2 \mathfrak{p}^{-1} \mathfrak{p}^{-1} = \mathcal{O}_K.$$

Consider the map

$$\begin{aligned} \varphi : \mathfrak{p}^* &\to \mathfrak{p} \\ x &\mapsto \sqrt{p} x, \end{aligned}$$

then φ is a bijective $\mathbb{Z}-$module homomorphism, and

$$b(\varphi(x), \varphi(y)) = b(\sqrt{p}x, \sqrt{p}y) = \frac{1}{p} \mathrm{Tr}\,(\sqrt{p}x \sqrt{p}y) = p b(x, y).$$

Thus $(\mathfrak{p}^*, pb) \cong (\mathfrak{p}, b)$ as lattices and $(\mathfrak{p}, b)$ is a $p-$modular lattice. By Proposition 7, the lattices Γ_N are $p-$modular for all N. ∎

ACKNOWLEDGMENTS

The authors thank Patrick Solé for attracting their attention to his work on LCD codes. X. Hou is supported by Nanyang President Graduate Scholarship. The research of F. Oggier for this work is supported by Nanyang Technological University under Research Grant M58110049.

REFERENCES

[1] J.L. Massey, "Linear codes with complementary duals, Discrete Mathematics," 106 - 107, 337-342, 1992.
[2] J.H. Conway, N.J.A. Sloane, "Sphere Packings, Lattices and Groups", 3rd edition, Springer.
[3] C. Carlet, S. Guilley, "Complementary Dual Codes for Counter-Measures to Side-Channel Attacks", Coding Theory and Applications, Vol. 3, series CIM Series in Mathematical Sciences, pp. 97-105, 2015.
[4] S. T. Dougherty, J.-L. Kim, B. Ozkaya, L. Sok, P. Solé, "The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices", http://arxiv.org/abs/1506.01955
[5] N. J. A. Sloane and B. Beferull-lozano, "Quantizing using lattice intersections", *Journal of Discrete and Computational Geometry*, 2003, pp. 799–824.
[6] O. T. OMeara, "Introduction to Quadratic Forms, *Springer Verlag*, 1971.
[7] W. Kositwattanarerk, S. S. Ong, F. Oggier, "Construction A of Lattices over Number Fields and Block Fading (Wiretap) Coding",*IEEE Trans. on Information Theory*, vol. 61, no 5, March 2015.
[8] X. Hou, F. Lin, F. Oggier, "Construction and Secrecy Gain of a Family of 5-modular Lattices", IEEE ITW 2014, Hobart, Tasmania, Australia.
[9] S.T. Dougherty, J-L Kim, B.Ozkaya, L. Sok and P. Solé, "The combinatorics of LCD codes: Linear programming bound and orthogonal matrices", Jun. 2015, preprint at arXiv:1506.01955.
[10] D.S. Dummit, R.M. Foote, "Abstract algebra", third edition, *Englewood Cliffs: Prentice Hall.*, 1991.
[11] E. Bayer-Fluckiger, "Ideal Lattices", in A Panorama of Number Theory or The View from Bakers Garden, edited by Gisbert Wustholz Cambridge Univ. Press, Cambridge (2002), 168184.
[12] J. Neukirch, "Algebraic Number Theory", *Springer-Verlag, NY*, 1999.
[13] H.-G. Quebbemann, "Modular lattices in Euclidean Spaces", *Journal of Number Theory* **54** (1995), 190-202.