SIAM J. DISCRETE MATH.
Vol. 31, No. 2, pp. 1244–1262

DECIDING ORTHOGONALITY IN CONSTRUCTION-A LATTICES*

KARTHEKEYAN CHANDRASEKARAN†, VENKATA GANDIKOTA‡, AND ELENA GRIGORESCU‡

Abstract. Lattices are discrete mathematical objects with widespread applications to integer programs as well as modern cryptography. An important class of lattices are those that possess an orthogonal basis, since *if* such an orthogonal basis is known, then many other fundamental problems on lattices can be solved easily (e.g., the Closest Vector Problem). However, intriguingly, deciding whether a lattice has an orthogonal basis is not known to be either NP-complete or in P. In this paper, we focus on the orthogonality decision problem for a well-known family of lattices, namely Construction-A lattices. These are lattices of the form $C + q\mathbb{Z}^n$, where C is an error-correcting q-ary code, and are studied in communication settings. We provide a complete characterization of lattices obtained from binary and ternary codes using Construction-A that have an orthogonal basis. We use this characterization to give an efficient algorithm to solve the orthogonality decision problem. Our algorithm also finds an orthogonal basis if one exists for this family of lattices.

Key words. orthogonal lattices, lattice isomorphism, construction-A lattices

AMS subject classifications. 68W40, 15B36, 15B10

DOI. 10.1137/15M1054766

1. Introduction.

A lattice is the set of integer linear combinations of a set of basis vectors $B \in \mathbb{R}^{m\times n}$, namely $L = L(B) = \{xB \mid x \in \mathbb{Z}^m\}$. Lattices are well-studied fundamental mathematical objects that have been used to model diverse discrete structures such as in the area of integer programming [6], or in factoring integers [13] and factoring rational polynomials [8]. In a groundbreaking result, Ajtai [1] demonstrated the potential of computational problems on lattices to cryptography, by showing average case/worst case reductions between lattice problems related to finding short vectors in a lattice. This led to renewed interest in the complexity of two fundamental lattice problems: the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). Concretely, in SVP, given a basis B one is asked to output a shortest nonzero vector in the lattice, and in CVP, given a basis B and a target $t \in \mathbb{R}^n$, one is asked to output a lattice vector closest to t.

Both SVP and CVP are NP-hard even to approximate up to subpolynomial factors (see [11] for a survey), and a great deal of research has been devoted to finding families of lattices for which the SVP/CVP are easy. A simplest lattice for which CVP is easy is $\mathbb{Z}^n$: indeed, finding the closest lattice vector to a target $t \in \mathbb{R}^n$ amounts to rounding the entries of t to the nearest integer. Surprisingly, given an arbitrary basis B, it is not known how to efficiently verify whether the lattice generated by B is isomorphic to $\mathbb{Z}^n$ up to an orthogonal transformation. Further, given an arbitrary basis for a lattice, it is not known how to decide efficiently if the lattice has an orthogonal basis

*Received by the editors March 2, 2016; accepted for publication (in revised form) February 14, 2017; published electronically June 15, 2017. The preliminary version of this work appeared in the Proceedings of FSTTCS'15.

http://www.siam.org/journals/sidma/31-2/M105476.html

Funding: The research of the second and third authors was supported in part by NSF CCF-1649515.

†Department of Industrial and Enterprise Systems Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801 (karthe@illinois.edu).

‡Computer Science, Purdue University, West Lafayette, IN 47906 (vgandiko@purdue.edu, elena-g@purdue.edu).

(an orthogonal basis is a basis in which all vectors are pairwise orthogonal). Similar to the case of $\mathbb{Z}^n$, having access to an orthogonal basis leads to an efficient algorithm to solve CVP, but finding an orthogonal basis given an arbitrary basis appears to be nontrivial, with no known efficient algorithms.

Deciding if a lattice is equivalent to $\mathbb{Z}^n$, and deciding if a lattice has an orthogonal basis, are special cases of the more general Lattice Isomorphism Problem (LIP). In LIP, given lattices L_1 and L_2 presented by their bases, one is asked to decide if they are isomorphic, meaning if there exists an orthogonal transformation that takes one to the other. LIP has significant cryptographic applications [15] and is known to have an $n^{O(n)}$ algorithm [5]. Earlier, [12] suggested an algorithm for LIP that works well for certain low-dimensional lattices. Recent results of [9, 10] show that in certain highly symmetric lattices, isomorphism to $\mathbb{Z}^n$ can be decided efficiently. The complexity of LIP is not well understood, and is part of the broader study of isomorphism between mathematical objects, of which Graph Isomorphism (GI) is a well-known elusive problem [2]. Interestingly, there is a polynomial time reduction from GI to LIP [14].

Given that we do not know how to decide isomorphism to $\mathbb{Z}^n$, nor decide whether a lattice has an orthogonal basis in general lattices, it is natural to address families of lattices where these problems can be solved efficiently. In this work, we focus on the problem of deciding orthogonality for a particular family of lattices, commonly known as Construction-A lattices [4]. Construction-A lattices L are obtained from a linear error-correcting code C over a finite field of q elements (denoted $\mathbb{F}_q$) as $L = C + q\mathbb{Z}^n$.[1] We resolve the problem of deciding orthogonality in Construction-A lattices for $q = 2$ and $q = 3$ by showing an efficient algorithm. In addition, the algorithm outputs an orthogonal basis of the input lattice if such a basis exists.

Our main technical contribution is a decomposition theorem for Construction-A lattices that admit an orthogonal basis. A natural way to obtain orthogonal lattices through Construction-A is by taking direct products of lower-dimensional orthogonal lattices. We show that this is the only possible way. We believe that our contributions are a step towards gaining a better understanding of lattice isomorphism problems for more general classes of lattices.

Extending our results to values $q > 3$ might require new techniques. For larger q, a decomposition characterization seems to require a complete characterization of *weighing matrices* of weight q which is a known open problem. In particular, a direct product decomposition characterization of weighing matrices for the case of $q = 4$ is known [3]. However, even in this case the parts in the direct product decomposition may not be of constant dimension, so designing an efficient algorithm for the orthogonality decision problem through a direct product decomposition characterization appears to be nontrivial.

1.1. Our results and techniques. As mentioned above, we start by showing a structural decomposition of orthogonal lattices of the form $C + 2\mathbb{Z}^n$ and $C + 3\mathbb{Z}^n$ into constant-size orthogonal lattices. We remark that the decomposition holds up to permutations of the coordinates, and we use the notation $C_1 \cong C_2$ and $L_1 \cong L_2$ to denote the equivalence of codes and lattices under permutation of coordinates. We use the notation $L_1 \oplus L_2$ to denote the direct sum of two lattices.

THEOREM 1.1. *Let $L_C = C + 2\mathbb{Z}^n$ be a lattice obtained from a binary linear code*

[1]The term "Construction-A" strictly refers to the case $q = 2$, but we will not make the distinction in this paper.

$C \subseteq \mathbb{F}_2^n$. Then the following statements are equivalent:

1. *L_C is orthogonal.*
2. *$L_C \cong \oplus_i L_i$, where each L_i is either $\mathbb{Z}$, or $2\mathbb{Z}$, or the 2-dimensional lattice generated by the rows of the matrix $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.*
3. *$C \cong \oplus_i C_i$, where each C_i is either a length-1 binary linear code $\subseteq \{0,1\}$, or the length-2 binary linear code $\{00, 11\}$.*

The decomposition characterization leads to an efficient algorithm to verify if a given lattice obtained from a binary linear code using Construction-A is orthogonal. For the purposes of this algorithmic problem, the input consists of a basis to the lattice. The algorithm finds the component codes given by the characterization thereby computing the orthogonal basis for such a lattice.

THEOREM 1.2. *Given a basis for a lattice L obtained from a binary linear code using Construction-A, there exists an algorithm running in time $O(n^6)$ that verifies if L is orthogonal, and if so, outputs an orthogonal basis.*

We obtain a similar decomposition and algorithm for lattices obtained from ternary codes. For succinctness of presentation we define the following integer matrix:

$$M = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 \\ 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & 1 \end{bmatrix}.$$

THEOREM 1.3. *Let $L_C = C + 3\mathbb{Z}^n$ be a lattice obtained from a ternary linear code $C \subseteq \mathbb{F}_3^n$. Then the following statements are equivalent:*

1. *L_C is orthogonal.*
2. *$L_C \cong \oplus_i L_i$, where each L_i is either $\mathbb{Z}$, or $3\mathbb{Z}$, or the 4-dimensional lattice generated by the rows of a matrix $\mathcal{T}(M)$ obtained from M by negating some subset of columns.*
3. *$C \cong \oplus_i C_i$, where each C_i is either a linear length-1 ternary code, or the linear length-4 ternary code generated by the rows of $(\mathcal{T}(M) \bmod 3) \in \mathbb{F}_3^{4\times 4}$, where $\mathcal{T}(M)$ is obtained from M by negating some subset of its columns.*

THEOREM 1.4. *Given a basis for a lattice L obtained from a ternary linear code using Construction-A, there exists an algorithm running in time $O(n^8)$ that verifies if L is orthogonal, and if so, outputs an orthogonal basis.*

Theorems 1.1 and 1.2 are proved in section 3. Theorems 1.3 and 1.4 are proved in section 4.

2. Preliminaries. We denote the set of positive integers up to n by $[n]$, the $n \times n$ identity matrix by I_n, and its jth row by e_j. For a vector $b \in \mathbb{R}^n$, let b_j denote its jth coordinate, and let $\|b\|$ be its ℓ_2 norm.

Given a set of m linearly independent vectors $b_j \in \mathbb{R}^n$, a lattice L is generated by $\{b_1, \ldots, b_m\}$ is defined to be the set of all integer linear combinations of these vectors:

$$L = \left\{ \sum_{i=1}^{m} \alpha_i b_i \mid \alpha_i \in \mathbb{Z} \right\}.$$

If $m = n$, then L is said to be of full rank. The set of vectors which generate L is known as the basis of the lattice L. A lattice L is said to be orthogonal if it is generated by a set of pairwise orthogonal vectors. A lattice L is *integral* if it is contained in $\mathbb{Z}^n$, namely any basis for L only consists of integral vectors.

We will denote by $\mathbb{F}_q$ a finite field with q elements. A *linear* code C of length n over $\mathbb{F}_q$ is a vector space $C \subseteq \mathbb{F}_q^n$. A linear code is specified by a generator matrix G that consists of linearly independent vectors in $\mathbb{F}_q^n$. If $C \subseteq \mathbb{F}_2^n$, then it is called a *binary* code, and if $C \subseteq \mathbb{F}_3^n$, then it is called a *ternary* code.

The Construction-A of a lattice L_C from a linear code $C \subseteq \mathbb{F}_q^n$, where q is a prime, is defined as $L_C := \{c + q \cdot z \mid c \in \phi(C), z \in \mathbb{Z}^n\}$, where ϕ is the (real embedding) mapping $i \in \mathbb{F}_q \mapsto i \in \mathbb{Z}$. Construction-A is often abbreviated as $L_C = C + q\mathbb{Z}^n$. The fact that L_C is a lattice follows from the linearity of C over $\mathbb{F}_q$ [4].

For any vector $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ define $v \bmod q := (v_1 \bmod q, \ldots, v_n \bmod q) \in \mathbb{F}_q^n$. We note that $x \bmod q$ is the same as $\mathrm{res}(x, q)$.

CLAIM 2.1. *Let q be a prime, and L be an integral lattice. If $q\mathbb{Z}^n \subseteq L$, then $C = L \bmod q$ is a linear code over $\mathbb{F}_q$.*

Proof. Let $v \in L$ and $v = (v \bmod q) + qz$ for some $z \in \mathbb{Z}^n$, where here we abuse notation and view $v \bmod q$ as embedded into the integers, instead of a vector in $\mathbb{F}_q^n$. Since $q\mathbb{Z}^n \subseteq L$, it follows that $v - qz = v \bmod q \in L$. To show that $C = L \bmod q$ is a linear code over $\mathbb{F}_q$, let $c_1, c_2 \in C$. Then $c_1 + c_2 \in L$ (where the addition is over $\mathbb{Z}$), and so $(c_1 + c_2) \bmod q \in C$. ∎

We will use the following immediate claim about product of lattices generated from codes.

CLAIM 2.2. *Let $L = C + q\mathbb{Z}^n$, for some q-ary linear code $C \subseteq \mathbb{F}_q^n$. If $L \cong L_1 \oplus L_2$, and $L_1 \subseteq \mathbb{Z}^k$, then $L_1 \cong C_1 + q\mathbb{Z}^k$ and $L_2 \cong C_2 + q\mathbb{Z}^{n-k}$, for q-ary linear codes C_1 and C_2 that are projections of C on the coordinates corresponding to L_1 and L_2, respectively.*

A matrix U is *unimodular* if $U \in \mathbb{Z}^{n \times n}$ and $\det(U) \in \{\pm 1\}$. Two different bases B_1, B_2 give the same lattice if and only if there exists a unimodular matrix U such that $B_1 = UB_2$. The *Hermite Normal Form (HNF) basis* for a full rank lattice $L \subseteq \mathbb{R}^n$ is a square, nonsingular, and upper triangular matrix $B \subseteq \mathbb{R}^{n \times n}$ such that off-diagonal elements satisfy $0 \leq B_{i,j} < B_{j,j}$ for all $1 \leq i < j \leq n$.

FACT 2.3 (see [7]). *There exists an efficient algorithm which on input a set of rational vectors, B, computes a basis for the lattice generated by B: the algorithm simply computes the unique HNF basis of the lattice generated by B.*

We note that $L_C = C + q\mathbb{Z}^n$ contains $q\mathbb{Z}^n$ as a sublattice and hence it is a full rank lattice.

FACT 2.4. *A basis B for the lattice L_C specified by the generator matrix G for the code C can be computed efficiently by taking the HNF of the matrix $\begin{bmatrix} G \\ qI_n \end{bmatrix}$. Conversely, given a basis B of L_C, the generator matrix for C can be computed efficiently by finding a basis for $B \bmod q$ by row reduction over $\mathbb{F}_q$.*

Proof of Fact 2.4. Let L_C be a lattice obtained by Construction-A from a q-ary linear code $C \subseteq \mathbb{F}_q^n$, $L_C = C + q\mathbb{Z}^n$. We first show that given a generator G for the linear code C, the $HNF\left(\begin{bmatrix} G \\ qI_n \end{bmatrix}\right)$ gives a basis for the lattice L_C.

Let $B = HNF\left(\begin{bmatrix} G \\ qI_n \end{bmatrix}\right)$. By definition of the HNF basis, B is a basis for the lattice which contains each generator vector $g \in G$ and each qe_j for all $j \in [n]$. We note that each vector $v \in L_C$ is a linear combination of the generators of C and $3I_n$ which is exactly the lattice $L(B)$. Therefore, B is a basis for L_C.

Given a basis B for L_C, we now show that the set of linearly independent vectors in $\mathbb{F}_q^n$ obtained by embedding B mod q into $\mathbb{F}_q$ gives a generator for the code C. L_C contains $q\mathbb{Z}^n$ as a sublattice, and from Claim 2.1, we can conclude that the code C is the embedding of L_C mod q into $\mathbb{F}_q$. Since any lattice vector $v \in L_C$ is an integer linear combination of rows of B, all codewords in L_C mod q can be obtained as linear combinations of B mod q over $\mathbb{F}_q$. Therefore, the linearly independent set of vectors in B mod q form a generator for the code C. ∎

A *weighing matrix* of order n and weight k is a $n \times n$ matrix with entries in $\{0, 1, -1\}$ such that each row and column has exactly k nonzero entries and the row vectors are orthogonal to each other. By definition, a weighing matrix W satisfies $WW^T = kI_n$. For matrices $A \in \mathbb{R}^{n_1 \times n_1}$ and $B \in \mathbb{R}^{n_2 \times n_2}$, we denote the $(n_1 + n_2) \times (n_1 + n_2)$-dimensional block-diagonal matrix obtained using blocks A and B by $A \oplus B$. We will use the following characterization of weighing matrices of weights 2 and 3. For completeness we present proofs of Theorems 2.5 and 2.7 here.

THEOREM 2.5 (see [3]). *A matrix W is a weighing matrix of order n and weight 2 if and only if W can be obtained from*

$$\oplus_{i=1}^{n/2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

by negating some rows and columns and by interchanging some rows and columns.

Proof. Let $W(n, 2)$ denote a weighing matrix of order n and weight 2. We prove this theorem by induction on the order n of $W(n, 2)$.

For $n = 2$, the matrix $\left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$ is the only possible 2×2 orthogonal matrix up to permutations of columns with entries in $\{1, -1\}$. Therefore, $W(2, 2) \cong \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$.

Let us assume the induction hypothesis about all weighing matrices of order at most $n - 2$ and weight 2.

Let $W \in \{0, 1, -1\}^{n \times n}$ be an orthogonal matrix such that each row of W has exactly two nonzero entries. Since we are characterizing W up to permutations of rows and columns, and negations of rows and columns, we can assume without loss of generality that the first row of W is

$$w_1 = (1, 1, 0, \ldots, 0).$$

Since W is orthogonal, the nonzero entries of every other row, w_i has even intersection with the nonzero entries of w_1, i.e.,

$$|\text{Support}(w_i) \cap \text{Support}(w_1)| \in \{0, 2\}.$$

Let us consider the case when $|\text{Support}(w_i) \cap \text{Support}(w_1)| = 0$ for all $i \in [n] \setminus \{1\}$. Note that the w_i's are mutually orthogonal and supported on $n - 2$ coordinates. This would imply that W has at most $n - 1$ rows in total which contradicts the fact that W is a $n \times n$ matrix. Therefore, there exists at least one row, say w_2 such that $|\text{Support}(w_2) \cap \text{Support}(w_1)| = 2$. Since w_2 is orthogonal to w_1 and it has exactly two nonzero entries, it is of the form

$$w_2 = (1, -1, 0, \ldots, 0).$$

We note that there cannot exist any other row w_3 of W, such that $|\text{Support}(w_3) \cap \text{Support}(w_1)| = 2$ since it is not possible for such a vector to be orthogonal to both

w_1 and w_2. Therefore, for every other row $w_i, i \in \{3, \ldots, n\}$, we have $|\text{Support}(w_i) \cap \text{Support}(w_1)| = 0$. The weighing matrix is, therefore, of the form

$$W \cong \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \oplus W',$$

where W' is a weighing matrices of order at $n-2$ and weight 2. The proof follows from the induction hypothesis. ∎

The following lemma is needed for the proof of Theorem 2.7.

LEMMA 2.6. *A weighing matrix of order* 4 *and weight* 3 *is equivalent to* M *up to permutations of rows and columns, and negations of rows and columns.*

Proof. Let W be a weighing matrix of order 4 and weight 3. Since each vector has weight at exactly 3, we can assume without loss of generality that $w_1 = (1, 1, 1, 0)$. All rows are mutually orthogonal. Therefore, $|\text{Support}(w_i) \cap \text{Support}(w_j)| \in \{0, 2\}$ and $|\text{Support}(w_1) \cap \text{Support}(w_i)| \neq 0$ for all i.

Let us consider another row w_2 such that $|\text{Support}(w_1) \cap \text{Support}(w_2)| = 2$. So, $w_2 = (1, -1, 0, 1)$ up to permutations of coordinates. For any other row w_3, if $|\text{Support}(w_1) \cap \text{Support}(w_2) \cap \text{Support}(w_3)| = 2$, then the orthogonality condition with either w_1 or w_2 is violated. Therefore, w_3 is of the form $w_3 = (1, 0, -1, -1)$. This forces $w_4 = (0, 1, -1, 1)$ and, hence $W \equiv M$. ∎

THEOREM 2.7 (see [3]). *A matrix* W *is a weighing matrix of order* n *and weight* 3 *if and only if* W *can be obtained from* $\oplus_{i=1}^{n/4} M$ *by negating some rows and columns and by interchanging some rows and columns.*

Proof. Let $W(n, 3)$ denote a weighing matrix of order n and weight 3. We prove this theorem by induction on the order n of $W(n, 3)$.

For $n = 4$, from Lemma 2.6 we have $W(4, 3) \cong M$. Let us assume the induction hypothesis about all weighing matrices of order at most $n-4$ and weight 3.

Let $W \in \{0, 1, -1\}^{n \times n}$ be an orthogonal matrix such that each row of W has exactly three nonzero entries. Since we are characterizing W up to permutations of rows and columns, and negations of rows and columns, we can assume without loss of generality that the first row of W is

$$w_1 = (1, 1, 1, 0, \ldots, 0).$$

Since W is orthogonal, the nonzero entries of every other row, w_i has even intersection with the nonzero entries of w_1, i.e.,

$$|\text{Support}(w_i) \cap \text{Support}(w_1)| \in \{0, 2\} \quad \text{for all } i \in \{2, \ldots, n\}.$$

Let us consider the case when $|\text{Support}(w_i) \cap \text{Support}(w_1)| = 0$ for all $i \in [n] \setminus \{1\}$. Note that the w_i's are mutually orthogonal and supported on $n-3$ coordinates. This would imply that W has at most $n-2$ rows in total which contradicts the fact that W is a $n \times n$ matrix. Therefore, there exists at least two rows, say w_2, w_3 such that $|\text{Support}(w_1) \cap \text{Support}(w_2)| = 2$ and $|\text{Support}(w_1) \cap \text{Support}(w_3)| = 2$. Since these three vectors are mutually orthogonal and $\text{Support}(w_1) = 2$, it follows that $|\text{Support}(w_2) \cap \text{Support}(w_3)| > 0$. Without loss of generality, these three vectors are of the following form:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & \cdots & 0 \\ 1 & -1 & 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & -1 & 0 & \cdots & 0 \end{bmatrix}.$$

We observe that if $|\text{Support}(w_i) \cap \text{Support}(w_2)| = 0$ for all $i \in [n] \setminus \{1, 3\}$, then the number of vectors in W is at most $n-1$. Therefore, there exists at least one other row w_4 such that $|\text{Support}(w_4) \cap \text{Support}(w_2)| = 2$. Since w_4 is orthogonal to all w_1, w_2, and w_3, the unique candidate for w_4 is of the form $(0, 1, -1, 1, 0, \ldots, 0)$. We note that if there exists another row, w_5 such that $|\text{Support}(w_5) \cap \text{Support}(w_j)| > 0$ for any $j \in [4]$, then it cannot be orthogonal to all four vectors w_1, w_2, w_3, and w_4. So, $|\text{Support}(w_i) \cap \text{Support}(w_j)| = 0$ for any $j \in [4]$ and $i \geq 5$.

Therefore, $W(n, 3) \cong M \oplus W'$, where W' is a weighing matrix of order $n-4$ and weight 3. It then follows from the induction hypothesis that

$$W(n, 3) \cong \oplus_i M.$$

3. Orthogonal lattices from binary codes. In this section we focus on lattices obtained from binary linear codes using Construction-A. In section 3.1, we show that any orthogonal lattice obtained from a binary linear code by Construction-A is equivalent to a product lattice whose components are 1-dimensional or 2-dimensional lattices. In section 3.2, we show that given a lattice obtained from a binary linear code by Construction-A, there exists an efficient algorithm to verify if the lattice is orthogonal.

3.1. Decomposition characterization. We prove Theorem 1.1 in this subsection.

Proof of Theorem 1.1. We show that (1) $\equiv$ (2) and (2) $\equiv$ (3) to complete the equivalence of the three statements.
(1) $\equiv$ (2): We show that $L_C = C + 2\mathbb{Z}^n$ is orthogonal if and only if it decomposes into a direct sum of lower-dimensional orthogonal lattices, $L_C \cong \oplus_i L_i$.

If $L_C \cong \oplus_i L_i$ such that each L_i is orthogonal, then L_C is also orthogonal. This is because L_C would have a block diagonal orthogonal basis where each block is in itself orthogonal or a 1×1 matrix.

We prove the other direction of the equivalence by induction on the dimension, n, of the lattice L_C. For the base case consider $n = 1$. Since L is integral and is of the form $C + 2\mathbb{Z}$ for some binary linear code C, it follows that L has to be either $\mathbb{Z}$ or $2\mathbb{Z}$.

Let us assume the induction hypothesis for all $n-1$ or lower-dimensional orthogonal lattices obtained from binary linear codes using Construction-A.

Let L_C be an n-dimensional orthogonal lattice and B be an orthogonal basis of L_C with the rows being basis vectors. Since L_C is an integral lattice, B has only integral entries. The next two claims summarize certain properties of the entries of the basis matrix B.

Claim 3.1. *For every row b of B and for every $j \in [n]$, we have that $2|b_j| \in \{0, \|b\|^2, 2\|b\|^2\}$.*

Proof. Since B is an orthogonal basis, $BB^T = D$, where D is the diagonal matrix with entries $\|b^{(i)}\|^2$, where $b^{(i)}$ denotes the ith basis vector.

$$D = \begin{bmatrix} \|b^{(1)}\|^2 & 0 & 0 & \cdots & 0 \\ 0 & \|b^{(2)}\|^2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \|b^{(n)}\|^2 \end{bmatrix}.$$

We know that $2\mathbb{Z}^n \subseteq L_C$ so, $2e_j \in L_C$ for every $j \in [n]$. Therefore, there is an integral matrix $X \in \mathbb{Z}^{n \times n}$ such that $XB = 2I_n$, i.e., $2B^{-1} \in \mathbb{Z}^{n \times n}$. Since B is an

orthogonal basis,

$$B^{-1} = B^T D^{-1} \in \frac{1}{2}\mathbb{Z}^{n\times n}.$$

Each column of $B^T D^{-1}$ is given by $b/\|b\|^2$, where b is a basis vector. Therefore, for any $j \in [n]$, we have

$$2b_j \equiv 0 \bmod \|b\|^2 \text{ for all } j \in [n], \text{ and rows } b \text{ of } B.$$

Since b_j is integral and $|b_j| \leq \|b\|^2$ for every $j \in [n]$, it follows that $2|b_j| \in \{0, \|b\|^2, 2\|b\|^2\}$. ∎

Claim 3.2. *Let b be a row of B.*

(1) *If there exists $j \in [n]$ such that $2|b_j| = 2\|b\|^2$, then $b_j = \pm 1$ and $b_{j'} = 0$ for every $j' \in [n] \setminus \{j\}$.*
(2) *If there exists $j \in [n]$ such that $2|b_j| = \|b\|^2$ and $b_j = \pm 2$, then $b_{j'} = 0$ for every $j' \in [n] \setminus \{j\}$.*
(3) *If there exists $j \in [n]$ such that $2|b_j| = \|b\|^2$ and $b_j = \pm 1$, then there exist $j_1 \in [n] \setminus \{j\}$, such that $|b_{j_1}| = 1$ and $b_{j'} = 0$ for every $j' \in [n] \setminus \{j, j_1\}$.*

Proof. (1) Since $\|b\|^2 = \sum_{i=1}^n b_i^2$, and each $b_i \in \mathbb{Z}$, we conclude that $|b_j| = 1$ and the remaining coordinates in b have to be 0, i.e., $b_{j'} = 0$ for all $j' \in [n] \setminus \{j\}$.

(2) Follows from $2|b_j| = \|b\|^2$ and b being integral.

(3) We can rewrite the condition $2|b_j| = \|b\|^2$ as $2|b_j| = \sum_{i=1}^n b_i^2$. Rearranging the terms, we have

$$|b_j|\ (2 - |b_j|) = \sum_{i\neq j} b_i^2.$$

If $b_j = \pm 1$, then $\sum_{i\neq j} b_i^2 = 1$. Further, b is integral. Hence, b has exactly 1 other nonzero coordinates b_{j_1}, $j \neq j_1$, such that $|b_{j_1}| = 1$. ∎

Using the properties of the orthogonal basis B of L_C given in Claims 3.1 and 3.2, we show that B is equivalent (up to permutations of its columns) to a block diagonal matrix, i.e.,

$$B \cong \begin{bmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & B_k \end{bmatrix},$$

where each B_i is either the 1×1 matrix $\begin{bmatrix}1\end{bmatrix}$ or the 1×1 matrix $\begin{bmatrix}2\end{bmatrix}$ or the 2×2 matrix $\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$. It follows that $L_C \cong \oplus_i L_i$ such that B_i is the basis for the lower-dimensional lattice L_i.

Let us pick a row b of B with the smallest support. Fix an index $j \in [n]$ to be the index of a nonzero entry with minimum absolute value in b, i.e., $j := \arg\min_k\{|b_k|\}$. Since b is a row of a basis matrix, b cannot be the all-zeroes vector and, therefore, there exists a $j \in [n]$ such that $|b_j| > 0$. Since we are only interested in equivalence (that allows for permutation of coordinates), we may assume without loss of generality that $j = 1$ by permuting the coordinates. By Claim 3.1, we have that $2|b_1| \in \{\|b\|^2, 2\|b\|^2\}$. We consider each of these cases separately.

1. Suppose $2|b_1| = 2\|b\|^2$. By Claim 3.2(1), $b = (\pm 1, 0, \ldots, 0)$. Since B is an orthogonal basis, $\langle b, b'\rangle = 0 \Rightarrow b'_1 = 0$ for all $b' \neq b \in B$. The orthogonality of B, therefore,

forces all other basis vectors to take a value of 0 in the 1st coordinate. Thus B is of the form

$$B = \left(\begin{array}{c|c} \pm 1 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & B' \\ 0 & \end{array}\right).$$

Therefore, we obtain $L_C \cong \mathbb{Z} \oplus L'$, where L' is an orthogonal $(n-1)$-dimensional lattice generated by the basis matrix restricted to the coordinates other than 1, say, B'. From Claim 2.2, it follows that $L' = C' + 2\mathbb{Z}^{n-1}$ for some binary linear code $C' \subseteq \mathbb{F}_2^{n-1}$. Thus L' satisfies the induction hypothesis and we have the desired decomposition.

2. Suppose $2|b_1| = \|b\|^2$. We can rewrite this condition as $2|b_1| = \sum_{i=1}^{n} b_i^2$. Rearranging the terms, we have

$$|b_1|\ (2 - |b_1|) = \sum_{i \neq 1} b_i^2.$$

Since the right-hand side (RHS) is a sum of squares, it should be nonnegative.

(i) If RHS is 0, then $b_1 = \pm 2$ and, therefore, it follows from Claim 3.2(2) that $b = (\pm 2, 0, \ldots, 0)$. The orthogonality of B forces all other basis vectors to take a value of 0 at the 1st coordinate.

$$B = \left(\begin{array}{c|c} \pm 2 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & B' \\ 0 & \end{array}\right).$$

Therefore, we obtain $L_C \cong 2\mathbb{Z} \oplus L'$, where L' is an orthogonal $(n-1)$-dimensional lattice generated by the basis matrix restricted to the coordinates other than 1, say B'. From Claim 2.2, it follows that $L' = C' + 2\mathbb{Z}^{n-1}$ for some binary linear code $C' \subseteq \mathbb{F}_2^{n-1}$. Thus L' satisfies the induction hypothesis and we have the desired decomposition.

(ii) If RHS is strictly positive, then $|b_1| \in (0, 2) \cap \mathbb{Z} = \{1\}$. By Claim 3.2(3), we have that b has exactly two nonzero coordinates and they are ± 1. By permuting the coordinates of B, we may assume that $b \equiv (\pm 1, \pm 1, 0, \ldots, 0)$.

Since we picked the row b to be the one with the smallest support, it follows that every row has at least two nonzero coordinates. By Claims 3.1 and 3.2, this is possible only if for every other row b' there exists $j' \in [n]$ such that $2|b'_{j'}| = \|b'\|^2$. By Claim 3.2(1) and (2), every other row b' has all its coordinates in $\{0, \pm 1, \pm 2\}$. By Claim 3.2(2), every other row b' has none of its coordinates in $\{\pm 2\}$. Therefore, every other row b' has all its coordinates in $\{0, \pm 1\}$. By Claim 3.2(3), every row of the basis matrix has the same form as b: they have exactly two nonzero entries each of which is ± 1.

Since the rows of the basis matrix are orthogonal, it follows that the basis matrix B is a weighing matrix of order n with weight 2. By Theorem 2.5 the matrix B is obtained from $\oplus_{n/2} \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$ by either negating some rows or columns and by interchanging rows or columns. We recall that interchanging or negating the rows of the basis matrix of a lattice preserves the basis property while interchanging columns is equivalent to permuting the coordinates. Hence $L_C = L(B) \cong \oplus_{i=1}^{n/2} L(\left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right])$.

(2) ≡ (3): We now show that L_C decomposes into a direct sum of lower-dimensional lattices, $L_C \cong \oplus_i L_i$ if and only if the code C also decomposes, $C \cong \oplus_i C_i$.

Let $L_C \cong \oplus_i L_i$. Without loss of generality, we can consider $L_C = \oplus_i L_i$. We have $C = L_C \mod 2 = \oplus_i L_i \mod 2$. We observe that if L_i has dimension n_i, then $L_i \supseteq 2\mathbb{Z}^{n_i}$. Therefore, $C_i = L_i \mod 2$ is a binary code. Let $C_i := L_i \mod 2$ for every i. Then $C = \oplus_i C_i$. (If $c \in C$, then $c \in L$ and hence the projection of c to the subset of coordinates corresponding to L_i is in C_i. Let $c_i \in C_i$ for every i. The concatenated vector $\oplus_i c_i$ is in $\oplus_i L_i \mod 2$ and hence is in C).

To show the other direction of the equivalence, let $C \cong \oplus_i C_i$, where each $C_i \subseteq \mathbb{F}_2^{n_i}$ and $n = \sum_i n_i$. Therefore, $L_C = C + 2\mathbb{Z}^n \cong \oplus_i C_i + 2\mathbb{Z}^n \cong \oplus_i (C_i + 2\mathbb{Z}^{n_i})$ since $\mathbb{Z}^n \cong \oplus_i \mathbb{Z}^{n_i}$. ∎

3.2. Algorithm. Theorem 1.1 shows that a lattice of the form $C + 2\mathbb{Z}^n$ is orthogonal if and only if the underlying code decomposes into a direct sum of binary linear codes isomorphic to $\{0,1\}$ or $\{0\}$ or the 2-dimensional code $\{00,11\}$. We now give a polynomial time algorithm which finds the decomposition of the code C into the component codes, C_i, if there exists one. Therefore, if the lattice L_C is orthogonal, the algorithm decides in polynomial time if it is orthogonal and also gives the orthogonal basis for the lattice.

The algorithm recursively attempts to find the component codes. If it is unable to decompose the code at any stage, then it declares that L_C is not orthogonal. At every step we check if $C \cong \{0,1\} \times C'$ or $\{0\} \times C'$ or $\{00,11\} \times C'$ and then recurse on C'.

Proof of Theorem 1.2. Given a basis for L_C as input, we first compute the generator for C. From Theorem 1.1, we know that if L_C is orthogonal, then $C \cong \oplus_i C_i$ where each C_i is either the length-1 code $\{0,1\}$ or the length-1 code $\{0\}$ or the 2-dimensional code $\{00, 11\}$.

Therefore, the algorithm in each step decides whether $C \cong \{0,1\} \oplus C'$ or $C \cong \{0\} \oplus C'$ or $C \cong \{00,11\} \oplus C'$. Theorem 3.3 shows that by using Algorithm 1 we can check in $O(n^4)$ time, if $C \cong \{0,1\} \oplus C'$. The same algorithm can be modified to check in $O(n^4)$ time, if $C \cong \{0\} \oplus C'$. Theorem 3.4 shows that Algorithm 2 can verify if $C \cong \{00,11\} \oplus C'$ in $O(n^5)$ time. If any one of the algorithms finds a decomposition, then we recurse on the lower-dimensional code C' to find a further decomposition. We recurse at most n times. If all the algorithms fail to find a decomposition, then L_C is not orthogonal. Therefore, it takes $O(n^6)$ time to decide if L_C is orthogonal. ∎

We now describe the individual algorithms to verify if $C \cong \{0,1\} \oplus C'$ or $C \cong \{0\} \oplus C'$ or $C \cong \{00,11\} \oplus C'$.

Algorithm 1 : decompose − length − 1(G):

Input: $G = \{g_1, \ldots, g_n\} \in \mathbb{F}_2^n$ (A generator for the code C)

1: **for** $j \in \{1, \cdots, n\}$ **do**
2: Let $G' \leftarrow$ projection of vectors in G on coordinates $[n] \setminus \{j\}$
3: For $g \in G'$, define $g^0, g^1 \in \mathbb{F}_2^n$ as the n-dimensional vectors obtained by extending g using 0 and 1 along the jth coordinate, respectively.
4: **if** $g^0,\ g^1 \in C$ for all $g \in G'$ **then**
5: **return** j
6: **return** FAIL

THEOREM 3.3. *Let C be a binary linear code, and let $G = \{g_1, \ldots, g_n\} \in \mathbb{F}_2^{n \times n}$ be its generator. Then Algorithm 1 decides whether $C \cong \{0,1\} \oplus C'$ for some linear code $C' \subseteq \mathbb{F}_2^{n-1}$ and, if so, outputs the coordinate corresponding to the direct sum decomposition. Moreover, the algorithm runs in time $O(n^4)$.*

Proof. For $j \in [n]$, let $C'_{\bar{j}} \subseteq \mathbb{F}_2^{n-1}$ be the projection of C on the indices $[n] \setminus \{j\}$ and for a vector $c \in C'_{\bar{j}}$, let $c^0, c^1 \in \mathbb{F}_2^n$ be extensions of c using $0, 1$, respectively, along the jth coordinate. We note that $C \cong \{0,1\} \oplus C'$ for some binary linear code C' if and only if there exists an index $j \in [n]$, such that

$$C = \left\{ c^\ell \mid c \in C'_{\bar{j}}, \ell \in \{0,1\} \right\}.$$

From the definition of $C'_{\bar{j}}$, it follows that $C \subseteq \left\{ c^\ell \mid c \in C'_{\bar{j}}, \ell \in \{0,1\} \right\}$ up to a permutation of coordinates. So, the algorithm just needs to verify if the other side of the containment holds for some $j \in [n]$.

Let G' be the set of vectors of G projected on the coordinates $[n] \setminus \{j\}$. Algorithm 1 verifies if g^0 and g^1 are codewords in C, for every vector $g \in G'$. We now show that this is sufficient. Since C is a code, if g^0, $g^1 \in C$ for every $g \in G'$, then all linear combinations of these vectors are also in C. Therefore, $\left\{ c^\ell \mid c \in C'_{\bar{j}}, \ell \in \{0,1\} \right\} \subseteq C$.

It takes $O(n^2)$ time to compute a parity check matrix from the generator G and $O(n^2)$ time to verify if an input vector is a codeword using the parity check matrix. For every possible choice of the index j, Algorithm 1 checks if each of the $2n$ vectors of the form g^0, g^1 are in C. Therefore, Algorithm 1 takes $O(n^4)$ time to decide if $C \cong \{0,1\} \oplus C'$. ∎

Algorithm 2 : **decompose − length − 2(G)**:

Input: $G = \{g_1, \ldots, g_n\} \in \mathbb{F}_2^n$ (A generator for the code C)

```
for j1, j2 ∈ {1, 2, ..., n} do
    Let G' ← projection of vectors in G on coordinates [n] \ {j1, j2}
    Let G'' ← projection of vectors in G on coordinates {j1, j2}
    if Code generated by G'' ≡ {00, 11} then
        For g ∈ G' define g^00, g^11 ∈ F_2^n be n-dimensional vectors obtained by extending g using 00 and 11 along the j1, j2 coordinates.
        if g^00, g^11 ∈ C for all g ∈ G' then
            return j1, j2
return FAIL
```

THEOREM 3.4. *Let C be a binary linear code, and let $G = \{g_1, \ldots, g_n\} \in \mathbb{F}_2^{n \times n}$ be its generator. Then Algorithm 2 decides whether $C \cong \{00, 11\} \oplus C'$ for some linear codes $C' \subseteq \mathbb{F}_2^{n-2}$ and, if so, outputs the coordinates corresponding to the direct sum decomposition. Moreover, the algorithm runs in time $O(n^5)$.*

Proof. For $j_1, j_2 \in [n]$, let C''_{j_1,j_2} be the projection of C on the indices $\{j_1, j_2\}$. We first verify if C''_{j_1,j_2} is the code $\{00, 11\}$. For this purpose, it is sufficient to check if C''_{j_1,j_2} is generated by $\{11\}$. Now, to see if $C \cong \{00, 11\} \oplus C'$ for some binary linear code $C' \subseteq \mathbb{F}_2^{n-2}$. Define $C'_{\bar{j_1},\bar{j_2}}$ to be the projection of C on the indices $[n] \setminus \{j_1, j_2\}$. For a vector $c \in C'_{\bar{j_1},\bar{j_2}}$, let $c^{00}, c^{11} \in \mathbb{F}_2^n$ be the extensions of c using $\{00, 11\}$ along

the j_1, j_2 coordinates. We note that $C \cong \{00, 11\} \oplus C'$ for some binary linear code C' if and only if there exist indices $j_1, j_2 \in [n]$, such that

$$C = \left\{ c^\ell \mid c \in C'_{\bar{j_1},\bar{j_2}}, \ell \in \{00, 11\} \right\}. \tag{1}$$

From the definition of $C'_{\bar{j_1},\bar{j_2}}$ and $C''_{j_1,j_2} = \{00, 11\}$, it follows that $C \subseteq \left\{ c^\ell \mid c \in C'_{\bar{j_1},\bar{j_2}}, \ell \in \{00, 11\} \right\}$. So, the algorithm just needs to verify if the other side of the containment holds for some indices $j_1, j_2 \in [n]$.

Let G' be the set of vectors of G projected on the coordinates $[n] \setminus \{j_1, j_2\}$. Algorithm 2 verifies if g^{00} and g^{11} are codewords in C, for every vector $g \in G'$. We now show that this is sufficient. Since C is a code, if $g^{00}, g^{11} \in C$ for every $g \in G'$, then all linear combinations of these vectors are also in C. Therefore, $\left\{ c^\ell \mid c \in C'_{\bar{j_1},\bar{j_2}}, \ell \in \{00, 11\} \right\} \subseteq C$.

For each choice of $\{j_1, j_2\}$, it takes $O(n)$ time to verify if $C''_{j_1,j_2} = \{00, 11\}$. Time to verify if an input vector is a codeword using the parity check matrix is $O(n^2)$. We perform this check for $2n$ vectors of the form $\{g^\ell \mid g \in G', \ell \in \{00, 11\}\}$.

It takes $O(n^3)$ time to verify if $C \cong \{00, 11\} \oplus C'_{\bar{j_1},\bar{j_2}}$ for every pair of indices $j_1, j_2 \in [n]$. There are at most $\binom{n}{2}$ possible choices of indices, j_1, j_2; therefore, it takes $O(n^5)$ time in total to decide if $C \cong \{00, 11\} \oplus C'$. ∎

4. Orthogonal lattices from Ternary codes. In this section we focus on lattices obtained from ternary linear codes using Construction-A. In section 4.1, we show that any orthogonal lattice obtained from a ternary linear code by Construction-A is equivalent to a product lattice whose components are 1-dimensional or 4-dimensional. In section 4.2, we show that given a lattice obtained from a ternary linear code by Construction-A, there exists an efficient algorithm to verify if the lattice is orthogonal.

4.1. Decomposition characterization. We prove Theorem 1.3 in this subsection.

Proof of Theorem 1.3. We show that (1) ≡ (2) and (2) ≡ (3) to complete the equivalence of the three statements.

(1) ≡ (2): We show that $L_C = C + 3\mathbb{Z}^n$ is orthogonal if and only if it decomposes into a direct sum of lower-dimensional orthogonal lattices, $L_C \cong \oplus_i L_i$.

If $L_C \cong \oplus_i L_i$ such that each L_i is orthogonal, then L_C is also orthogonal. This is because L_C has a block diagonal basis where each block is itself an orthogonal matrix (by definition, a 1×1-dimensional matrix is orthogonal).

We prove the other direction of the equivalence by induction on the dimension, n, of the lattice L_C. For the base case consider $n = 1$. Since L is integral and is of the form $C + 3\mathbb{Z}$ for some ternary code C, it follows that L has to be either $\mathbb{Z}$ or $3\mathbb{Z}$.

Let us assume the induction hypothesis for all $n-1$ or lower-dimensional orthogonal lattices obtained from ternary linear codes using Construction-A.

Let L_C be an n-dimensional orthogonal lattice and B be an orthogonal basis of L_C with the rows being basis vectors. Since L_C is an integral lattice, B has only integral entries. The next two claims summarize certain properties of the entries of the basis matrix B.

Claim 4.1. *For every row b of B and for every $j \in [n]$, we have that $3|b_j| \in \{0, \|b\|^2, 3\|b\|^2\}$.*

Proof. Since B is an orthogonal basis, $BB^T = D$, where D is the diagonal matrix with entries $\|b^{(i)}\|^2$, where $b^{(i)}$ denotes the ith basis vector:

$$D = \begin{bmatrix} \|b^{(1)}\|^2 & 0 & 0 & \cdots & 0 \\ 0 & \|b^{(2)}\|^2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \|b^{(n)}\|^2 \end{bmatrix}.$$

We know that $3\mathbb{Z}^n \subseteq L_C$ so, $3e_j \in L_C$ for every $j \in [n]$. Therefore, there is an integral matrix $X \in \mathbb{Z}^{n\times n}$ such that $XB = 3I_n$, i.e., $3B^{-1} \in \mathbb{Z}^{n\times n}$. Since B is an orthogonal basis,

$$B^{-1} = B^T D^{-1} \in \frac{1}{3}\mathbb{Z}^{n\times n}.$$

Each column of $B^T D^{-1}$ is given by $b/\|b\|^2$, where b is a basis vector. Therefore, for any $j \in [n]$, we have

$$3b_j \equiv 0 \bmod \|b\|^2 \text{ for all } j \in [n], \text{ and rows } b \text{ of } B.$$

Since b_j is integral and $|b_j| \leq \|b\|^2$ for every $j \in [n]$, it follows that $3|b_j| \in \{0, \|b\|^2, 2\|b\|^2, 3\|b\|^2\}$. It now remains to exclude the case $3|b_j| = 2\|b\|^2$. Suppose there exists $j \in [n]$ such that $3|b_j| = 2\|b\|^2$. Since b is a basis vector, it follows that b is not all zeroes. Hence $b_j \neq 0$. We can rewrite the condition $3|b_j| = 2\|b\|^2$ as $3|b_j| = 2\sum_{i=1}^n b_i^2$. Rearranging the terms, we have

$$|b_j|\ (3 - 2|b_j|) = 2\sum_{i\neq j} b_i^2.$$

Since the RHS is a sum of squares, it is always nonnegative. The left-hand side (LHS) is nonzero since $b_j \in \mathbb{Z} \setminus \{0\}$. So the LHS should be strictly positive. Therefore, $|b_j| \in (0, 3/2) \cap \mathbb{Z}$ and hence $|b_j| = 1$. However, this implies that $\sum_{i\neq j} b_i^2 = 1/2$, contradicting the fact that b is integral. Hence, $3||b_j|| = 2\|b\|^2$ is impossible. ∎

CLAIM 4.2. *Let b be a row of B.*

(1) *If there exists $j \in [n]$ such that $3|b_j| = 3\|b\|^2$, then $b_j = \pm 1$ and $b_{j'} = 0$ for every $j' \in [n] \setminus \{j\}$.*
(2) *If there exists $j \in [n]$ such that $3|b_j| = \|b\|^2$ and $b_j = \pm 3$, then $b_{j'} = 0$ for every $j' \in [n] \setminus \{j\}$.*
(3) *If there exists $j \in [n]$ such that $3|b_j| = \|b\|^2$ and $b_j = \pm 1$, then there exist $j_1, j_2 \in [n] \setminus \{j\}$, such that $|b_{j_1}| = |b_{j_2}| = 1$ and $b_{j'} = 0$ for every $j' \in [n] \setminus \{j, j_1, j_2\}$.*
(4) *If there exists $j \in [n]$ such that $3|b_j| = \|b\|^2$, then $b_{j'} \in \{0, \pm 1, \pm 3\}$ for every $j' \in [n]$.*

Proof. (1) Since, $\|b\|^2 = \sum_{i=1}^n b_i^2$, and each $b_i \in \mathbb{Z}$, we conclude that $|b_j| = 1$ and the remaining coordinates in b have to be 0, i.e., $b_{j'} = 0$ for all $j' \in [n] \setminus \{j\}$.

(2) Follows from $3|b_j| = \|b\|^2$ and b being integral.

(3) We can rewrite the condition $3|b_j| = \|b\|^2$ as $3|b_j| = \sum_{i=1}^n b_i^2$. Rearranging the terms, we have

$$|b_j|\ (3 - |b_j|) = \sum_{i\neq j} b_i^2. \tag{2}$$

If $b_j = \pm 1$, then $\sum_{i\neq j} b_i^2 = 2$. Further, b is integral. Hence, b has exactly two other nonzero coordinates b_{j_1}, b_{j_2}, $j \neq j_1, j_2$, such that $|b_{j_1}| = |b_{j_2}| = 1$.

(4) We have equation (2). The RHS is a sum of squares and hence the LHS is nonnegative. Moreover, b is not all-zeroes vector implies that $b_j \neq 0$. Therefore, $|b_j| \in (0,3] \cap \mathbb{Z}$. If $b_j = \pm 2$, then in order to satisfy $\sum_{i \neq j} b_i^2 = 2$ using integral b_i's, exactly two coordinates b_{j_1}, b_{j_2} should be ± 1, where $j \neq j_1, j_2$. However, in this case, $3|b_{j_1}| = 3|b_{j_2}| = 3 \notin \{0, \|b\|^2 = 6, 3\|b\|^2 = 18\}$, thus contradicting Claim 4.1. The conclusion then follows from parts (2) and (3). ∎

Using the properties of the orthogonal basis B of L_C given in Claims 4.1 and 4.2, we show that B is equivalent (up to permutations of its columns) to a block diagonal matrix, i.e.,

$$B \cong \begin{bmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & & \ddots & 0 \\ 0 & 0 & \cdots & B_k \end{bmatrix},$$

where each B_i is either the 1×1 matrix $\begin{bmatrix}1\end{bmatrix}$ or the 1×1 matrix $\begin{bmatrix}3\end{bmatrix}$ or the 4×4 matrix obtained from M by negating a subset of its columns, $\mathcal{T}(M)$. It follows that $L_C \cong \oplus_i L_i$ such that B_i is the basis for the lower-dimensional lattice L_i.

Let us pick a row b of B with the smallest support. Fix an index $j \in [n]$ to be the index of a nonzero entry with minimum absolute value in b, i.e., $j := \arg\min_k\{|b_k|\}$. Since b is a row of a basis matrix, b cannot be the all-zeroes vector and, therefore, there exists a $j \in [n]$ such that $|b_j| > 0$. Since we are only interested in equivalence (that allows for permutation of coordinates), we may assume without loss of generality that $j = 1$ by permuting the coordinates. By Claim 4.1, we have that $3|b_1| \in \{\|b\|^2, 3\|b\|^2\}$. We consider each of these cases separately.

1. Suppose $3|b_1| = 3\|b\|^2$. By Claim 4.2(1), $b = (\pm 1, 0, \ldots, 0)$. Since B is an orthogonal basis, $\langle b, b' \rangle = 0 \Rightarrow b'_1 = 0$ for all $b' \neq b \in B$. The orthogonality of B, therefore, forces all other basis vectors to take a value of 0 in the 1st coordinate. Thus B is of the form

$$B = \left(\begin{array}{c|c} \pm 1 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & B' \\ 0 & \end{array}\right).$$

   Therefore, we obtain $L_C \cong \mathbb{Z} \oplus L'$, where L' is an orthogonal $(n-1)$-dimensional lattice generated by the basis matrix restricted to the coordinates other than 1, say, B'. From Claim 2.2, it follows that $L' = C' + 3\mathbb{Z}^{n-1}$ for some ternary linear code $C' \subseteq \mathbb{F}_3^{n-1}$. Thus L' satisfies the induction hypothesis and we have the desired decomposition.
2. Suppose $3|b_1| = \|b\|^2$. We can rewrite this condition as $3|b_1| = \sum_{i=1}^n b_i^2$. Rearranging the terms, we have

$$|b_1|\ (3 - |b_1|) = \sum_{i \neq 1} b_i^2.$$

   Since the RHS is a sum of squares, it should be nonnegative.

   (i) If RHS is 0, then $b_1 = \pm 3$ and, therefore, it follows from Claim 4.2(2) that $b = (\pm 3, 0, \ldots, 0)$. The orthogonality of B forces all other basis vectors to take a

value of 0 in the 1st coordinate.

$$B = \left(\begin{array}{c|c} \pm 3 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & B' \\ 0 & \end{array}\right).$$

Therefore, we obtain $L_C \cong 3\mathbb{Z} \oplus L'$, where L' is an orthogonal $(n-1)$-dimensional lattice generated by the basis matrix restricted to the coordinates other than 1, say B'. From Claim 2.2, it follows that $L' = C' + 3\mathbb{Z}^{n-1}$ for some ternary linear code $C' \subseteq \mathbb{F}_3^{n-1}$. Thus L' satisfies the induction hypothesis and we have the desired decomposition.

(ii) If RHS is strictly positive, then $|b_1| \in (0,3) \cap \mathbb{Z} = \{1,2\}$. By Claim 4.2(4), $b_1 \neq \pm 2$. Therefore, $b_1 = \pm 1$. By Claim 4.2(3), we have that b has exactly three nonzero coordinates and they are ± 1. By permuting the coordinates of B, we may assume that $b \equiv (\pm 1, \pm 1, \pm 1, 0, \ldots, 0)$.

Since we picked the row b to be the one with the smallest support, it follows that every row has at least three nonzero coordinates. By Claims 4.1 and 4.2, this is possible only if for every other row b' there exists $j' \in [n]$ such that $3|b'_{j'}| = \|b'\|^2$. By Claim 4.2(4), every other row b' has all its coordinates in $\{0, \pm 1, \pm 3\}$. By Claim 4.2(2), every other row b' has none of its coordinates in $\{\pm 3\}$. Therefore, every other row b' has all its coordinates in $\{0, \pm 1\}$. By Claim 4.2(3), every row of the basis matrix has the same form as b: they have exactly three nonzero entries each of which is ± 1.

Since the rows of the basis matrix are orthogonal, it follows that the basis matrix B is a weighing matrix of order n with weight 3. By Theorem 2.7, the matrix B is obtained from $\oplus_{n/4} M$ by either negating some rows or columns and by interchanging rows or columns. We recall that interchanging or negating the rows of the basis matrix of a lattice preserves the basis property while interchanging columns is equivalent to permuting the coordinates. Hence $L_C = L(B) \cong \oplus_{i=1}^{n/4} L(\mathcal{T}_i(M))$, where each $\mathcal{T}_i(M)$ is a 4×4 matrix obtained by negating a subset of columns of M.

(2) $\equiv$ (3): We now show that L_C decomposes into a direct sum of lower-dimensional lattices, $L_C \cong \oplus_i L_i$ if and only if the code C also decomposes, $C \cong \oplus_i C_i$.

Let $L_C \cong \oplus_i L_i$. Without loss of generality, we can consider $L_C = \oplus_i L_i$. We have $C = L_C \mod 3 = \oplus_i L_i \mod 3$. We observe that if L_i has dimension n_i, then $L_i \supseteq 3\mathbb{Z}^{n_i}$. Therefore, $C_i = L_i \mod 3$ is a ternary code. Let $C_i := L_i \mod 3$ for every i. Then $C = \oplus_i C_i$. (If $c \in C$, then $c \in L$ and hence the projection of c to the subset of coordinates corresponding to L_i is in C_i. Let $c_i \in C_i$ for every i. The concatenated vector $\oplus_i c_i$ is in $\oplus_i L_i \mod 3$ and hence is in C.)

To show the other direction of the equivalence, let $C \cong \oplus_i C_i$, where each $C_i \subseteq \mathbb{F}_3^{n_i}$ and $n = \sum_i n_i$. Therefore, $L_C = C + 3\mathbb{Z}^n \cong \oplus_i C_i + 3\mathbb{Z}^n \cong \oplus_i (C_i + 3\mathbb{Z}^{n_i})$ since $\mathbb{Z}^n \cong \oplus_i \mathbb{Z}^{n_i}$. ∎

4.2. Algorithm. Theorem 1.3 shows that a lattice of the form $C + 3\mathbb{Z}^n$ is orthogonal if and only if the underlying code decomposes into a direct sum of ternary linear codes isomorphic to $\{0,1,2\}$ or $\{0\}$ or the 4-dimensional code generated by $\mathcal{T}(M) \mod 3$, where $\mathcal{T}(M)$ is obtained from matrix M by negating a subset of its columns. We now give a polynomial time algorithm which finds the decomposition of the code C into the component codes, C_i, if there exists one. Therefore, if the lattice L_C is orthogonal, the algorithm decides in polynomial time if it is orthogonal and also

gives the orthogonal basis for the lattice.

The algorithm recursively attempts to find the component codes. If it is unable to decompose the code at any stage, then it declares that L_C is not orthogonal. At every step we check if $C \cong \{0,1,2\} \times C'$ or $\{0\} \times C'$ or $C_{\mathcal{T}(M)} \times C'$ where $C_{\mathcal{T}(M)}$ is the code generated by $\mathcal{T}(M)$ mod 3 and then recurse on C'.

Proof of Theorem 1.4. Given a basis for L_C as input, we first compute the generator for C. From Theorem 1.3, we know that if L_C is orthogonal, then $C \cong \oplus_i C_i$ where each C_i is either the length-1 code $\{0,1,2\}$ or the length-1 code $\{0\}$ or a 4-dimensional code generated by the rows of $\mathcal{T}(M)$ mod 3 where $\mathcal{T}(M)$ obtained from matrix M by negating a subset of its columns.

Therefore, the algorithm in each step decides if $C \cong \{0,1,2\} \oplus C'$ or $C \cong \{0\} \oplus C'$ or $C \cong C_{\mathcal{T}(M)} \oplus C'$, where $C_{\mathcal{T}(M)}$ denotes the code generated by $\mathcal{T}(M)$ mod 3. Theorem 4.3 shows that using Algorithm 3 we can check in $O(n^4)$ time if $C \cong \{0,1,2\} \oplus C'$. The same algorithm can be modified to check in $O(n^4)$ time if $C \cong \{0\} \oplus C'$. Theorem 4.4 shows that Algorithm 4 can verify if $C \cong C_{\mathcal{T}(M)} \oplus C'$ in $O(n^7)$ time. If any one of the algorithms finds a decomposition, then we recurse on the lower-dimensional code C' to find a further decomposition. We recurse at most n times. If all the algorithms fail to find a decomposition, then L_C is not orthogonal. Therefore, it takes $O(n^8)$ time to decide if L_C is orthogonal. ∎

We now describe the individual algorithms to verify if $C \cong \{0,1,2\} \oplus C'$ or $C \cong \{0\} \oplus C'$ or $C \cong C_{\mathcal{T}(M)} \oplus C'$.

Algorithm 3 : **decompose − length − 1(G)**:

Input: $G = \{g_1, \ldots, g_n\} \in \mathbb{F}_3^n$ (A generator for the code C)

1: **for** $j \in \{1, \ldots, n\}$ **do**
2: Let $G' \leftarrow$ projection of vectors in G on coordinates $[n] \setminus \{j\}$
3: For $g \in G'$, define $g^0, g^1, g^2 \in \mathbb{F}_3^n$ as the n-dimensional vectors obtained by extending g using 0, 1, and 2 along the jth coordinate, respectively.
4: **if** $g^0,\ g^1,\ g^2 \in C$ for all $g \in G'$ **then**
5: **return** j
6: **return** FAIL

THEOREM 4.3. *Let C be a ternary linear code and $G = \{g_1, \ldots, g_n\} \in \mathbb{F}_3^{n \times n}$ be its generator. Then Algorithm 3 decides if $C \cong \{0,1,2\} \oplus C'$ for some linear code $C' \subseteq \mathbb{F}_3^{n-1}$ and, if so, outputs the coordinate corresponding to the direct sum decomposition. Moreover, the algorithm runs in time $O(n^4)$.*

Proof. For $j \in [n]$, let $C'_{\overline{j}} \subseteq \mathbb{F}_3^{n-1}$ be the projection of C on the indices $[n] \setminus \{j\}$ and for a vector $c \in C'_{\overline{j}}$, let $c^0, c^1, c^2 \in \mathbb{F}_3^n$ be extensions of c using $0, 1, 2$, respectively, along the jth coordinate. We note that $C \cong \{0,1,2\} \oplus C'$ for some ternary linear code C' if and only if there exists an index $j \in [n]$, such that

$$C = \left\{ c^\ell \mid c \in C'_{\overline{j}}, \ell \in \{0,1,2\} \right\}.$$

From the definition of $C'_{\overline{j}}$, it follows that $C \subseteq \left\{ c^\ell \mid c \in C'_{\overline{j}}, \ell \in \{0,1,2\} \right\}$ up to a permutation of coordinates. So, the algorithm just needs to verify if the other side of the containment holds for some $j \in [n]$.

Let G' be the set of vectors of G projected on the coordinates $[n]\backslash\{j\}$. Algorithm 3 verifies if g^0, g^1, and g^2 are codewords in C, for every vector $g \in G'$. We now show that this is sufficient. Since C is a code, if g^0, g^1, $g^2 \in C$ for every $g \in G'$, then all linear combinations of these vectors are also in C. Therefore, $\left\{c^\ell \mid c \in C'_{\bar{j}}, \ell \in \{0,1,2\}\right\} \subseteq C$.

It takes $O(n^2)$ time to compute a dual code basis from the generator G and $O(n^2)$ time to verify if an input vector is a codeword using the dual basis. For every possible choice of the index j, Algorithm 3 checks if each of the $3n$ vectors of the form g^0, g^1, g^2 are in C. Therefore, Algorithm 3 takes $O(n^4)$ time to decide if $C \cong \{0,1,2\} \oplus C'$. ∎

Algorithm 4 : decompose − length − 4(G):

Input: $G = \{g_1, \ldots, g_n\} \in \mathbb{F}_3^n$ (A generator for the code C)

```
for j1, j2, j3, j4 ∈ {1, 2, ··· , n} do
  Let G' ← projection of vectors in G on coordinates [n] \ {j1, j2, j3, j4}
  Let G'' ← projection of vectors in G on coordinates {j1, j2, j3, j4}
  for S ⊆ [4] do
    Let T(M) ← M with columns in S negated
    if C_{T(M)} ≡ Code generated by G'' then
      For g ∈ G' define g^{p1}, g^{p2}, g^{p3}, g^{p4} ∈ F_3^n be n-dimensional vectors obtained
      by extending g using the rows of T(M) along the j1, j2, j3, j4 coordinates.
      if g^{p1}, g^{p2}, g^{p3}, g^{p4} ∈ C for all g ∈ G' then
        return j1, j2, j3, j4 and T(M)
return FAIL
```

THEOREM 4.4. *Let C be a ternary linear code, and let $G = \{g_1, \ldots, g_n\} \in \mathbb{F}_3^{n\times n}$ be its generator. For a matrix $\mathcal{T}(M)$ obtained by negating a subset of columns of M, let $C_{\mathcal{T}(M)}$ be the length-4 code whose generators are the rows of $\mathcal{T}(M)$. Then Algorithm 4 decides if $C \cong C_{\mathcal{T}(M)} \oplus C'$ for some linear codes $C' \subseteq \mathbb{F}_3^{n-4}$ and $C_{\mathcal{T}(M)} \subseteq \mathbb{F}_3^4$ and if so outputs the coordinates corresponding to the direct sum decomposition as well as the matrix $\mathcal{T}(M)$. Moreover, the algorithm runs in time $O(n^7)$.*

Proof. For $1 \le j_1 < j_2 < j_3 < j_4 \le n$, let C''_{j_1,j_2,j_3,j_4} be the projection of C on the indices $\{j_1, j_2, j_3, j_4\}$. We first verify if C''_{j_1,j_2,j_3,j_4} is the code generated by the rows of $\mathcal{T}(M)$ (denoted as $C_{\mathcal{T}(M)}$) for some $\mathcal{T}(M)$ which is obtained by negating a subset of columns of M. We would like to check if every $c \in C''_{j_1,j_2,j_3,j_4}$ is in $C_{\mathcal{T}(M)}$ and vice versa. For this purpose, it is sufficient to check if the generator vectors of C''_{j_1,j_2,j_3,j_4} are codewords in $C_{\mathcal{T}(M)}$ and each row of $\mathcal{T}(M)$ is a codeword in C''_{j_1,j_2,j_3,j_4}. We know that the generators of C''_{j_1,j_2,j_3,j_4} are contained in G'' where G'' is the set of vectors in G projected on the indices $\{j_1, j_2, j_3, j_4\}$.

Once we fix $\mathcal{T}(M)$ such that $C''_{j_1,j_2,j_3,j_4} = C_{\mathcal{T}(M)}$, it remains to verify if $C \cong C_{\mathcal{T}(M)} \oplus C'$ for some ternary linear code $C' \subseteq \mathbb{F}_3^{n-4}$. Define $C'_{\bar{j_1},\bar{j_2},\bar{j_3},\bar{j_4}}$ to be the projection of C on the indices $[n] \setminus \{j_1, j_2, j_3, j_4\}$. For a vector $c \in C'_{\bar{j_1},\bar{j_2},\bar{j_3},\bar{j_4}}$, let $c^p \in \mathbb{F}_3^n$ be the extensions of c using a codeword $p \in C_{\mathcal{T}(M)}$ along the j_1, j_2, j_3, j_4 coordinates. We note that $C \cong C_{\mathcal{T}(M)} \oplus C'$ for some ternary linear code C' if and only if there exist indices $j_1, j_2, j_3, j_4 \in [n]$, such that

$$C = \left\{c^p \mid c \in C'_{\bar{j_1},\bar{j_2},\bar{j_3},\bar{j_4}}, p \in C_{\mathcal{T}(M)}\right\}. \tag{3}$$

From the definition of $C'_{\bar{j_1},\bar{j_2},\bar{j_3},\bar{j_4}}$ and C''_{j_1,j_2,j_3,j_4} $(= C_{\mathcal{T}(M)})$, it follows that $C \subseteq \{c^p \mid c \in C'_{\bar{j_1},\bar{j_2},\bar{j_3},\bar{j_4}}, p \in C_{\mathcal{T}(M)}\}$. So, the algorithm just needs to verify if the other side of the containment holds for some indices $j_1, j_2, j_3, j_4 \in [n]$.

Let G' be the set of vectors of G projected on the coordinates $[n] \setminus \{j_1, j_2, j_3, j_4\}$. Algorithm 4 verifies if g^{p_0}, g^{p_1}, g^{p_3}, and g^{p_4} are codewords in C, for every vector $g \in G'$. We now show that this is sufficient. Since C is a code, if $g^{p_0}, g^{p_1}, g^{p_3}, g^{p_4} \in C$ for every $g \in G'$ and $p_i \in \mathcal{T}(M)$, then all linear combinations of these vectors are also in C. Therefore, $\{c^p \mid c \in C'_{\bar{j_1},\bar{j_2},\bar{j_3},\bar{j_4}}, p \in C_{\mathcal{T}(M)}\} \subseteq C$.

There are $2^4 4^4$ possible choices of $\mathcal{T}(M)$ including permutations. For each matrix $\mathcal{T}(M)$, it takes $O(n)$ time to verify if $C_{\mathcal{T}(M)} = C''_{j_1,j_2,j_3,j_4}$. Time to verify if an input vector is a codeword using the dual basis is $O(n^2)$. We perform this check for $4n$ vectors of the form $\{g^{p_0}, g^{p_1}, g^{p_3}, g^{p_4} \mid g \in G'\}$. So, for a given $\mathcal{T}(M)$ such that $C_{\mathcal{T}(M)} = C''_{j_1,j_2,j_3,j_4}$, it takes $O(n^3)$ time to verify $C \cong C_{\mathcal{T}(M)} \oplus C'$.

For every possible choice of indices, $\{j_1, j_2, j_3, j_4\}$, Algorithm 4 takes $O(n^3)$ time to verify if $C \cong C_{\mathcal{T}(M)} \oplus C'_{\bar{j_1},\bar{j_2},\bar{j_3},\bar{j_4}}$. Since there are at most $\binom{n}{4}$ possible choices of indices, it takes $O(n^7)$ time in total to decide if $C \cong C_{\mathcal{T}(M)} \oplus C'$. ∎

Acknowledgments. We thank Daniel Dadush and the anonymous reviewers for helpful suggestions and pointers.

REFERENCES

[1] M. Ajtai, *Generating hard instances of lattice problems (extended abstract)*, in Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, 1996, ACM, New York, 1996, pp. 99–108, https://doi.org/10.1145/237814.237838.

[2] L. Babai, *Automorphism groups, isomorphism, reconstruction*, in Handbook of Combinatorics 27, R. L. Graham, M. Grotschel, and L. Lovasz, eds., North-Holland, Amsterdam, 1996, pp. 1447–1540.

[3] H. Chan, C. Rodger, and J. Seberry, *On inequivalent weighing matrices*, Ars Combin., 21 (1986), pp. 299–333.

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren Math. Wiss. 290, Springer-Verlag, New York, 1999, https://doi.org/10.1007/978-1-4757-6568-7.

[5] I. Haviv and O. Regev, *On the lattice isomorphism problem*, in Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, OR, ACM, New York, SIAM, Philadelphia, 2014, pp. 391–404, https://doi.org/10.1137/1.9781611973402.29.

[6] R. Kannan, *Improved algorithms for integer programming and related lattice problems*, in Proceedings of the 15th Annual ACM Symposium on Theory of Computing, Boston, MA, 1983, pp. 193–206, https://doi.org/10.1145/800061.808749.

[7] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Comput., 8 (1979), pp. 499–507, https://doi.org/10.1137/0208040.

[8] A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515–534.

[9] H. Lenstra and A. Silverberg, *Revisiting the gentry-szydlo algorithm*, in Advances in Cryptology CRYPTO 2014, Lecture Notes in Comput. Sci. 8616, Springer, Berlin, Heidelberg, 2014, pp. 280–296, https://doi.org/10.1007/978-3-662-44371-2_16.

[10] H. W. Lenstra and A. Silverberg, *Lattices with symmetries*, J. Cryptol., in press, https://doi.org/10.1007/s00145-016-9235-7.

[11] D. Micciancio and O. Regev, *Lattice-based cryptography*, in Post-Quantum Cryptography, D. J. Bernstein, J. Buchmann, and E. Dahmen, eds., Springer, Berlin, 2009, pp. 147–191, https://doi.org/10.1007/978-3-540-88702-7_5.

[12] W. Plesken and B. Souvignier, *Computing isometries of lattices*, J. Symbolic Comput., 24 (1997), pp. 327–334, https://doi.org/10.1006/jsco.1996.0130.

[13] C. Schnorr, *Factoring integers by CVP algorithms*, in Number Theory and Cryptography - Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday, Lecture Notes in Comput. Sci. 8260, Springer, Heidelberg, 2013, pp. 73–93, https://doi.org/10.1007/978-3-642-42001-6_6.

[14] M. D. Sikiric, A. Schürmann, and F. Vallentin, *Complexity and algorithms for computing Voronoi cells of lattices*, Math. Comp., 78 (2009), pp. 1713–1731, https://doi.org/10.1090/S0025-5718-09-02224-8.

[15] M. Szydlo, *Hypercubic lattice reduction and analysis of GGH and NTRU signatures*, in International Conference on the Theory and Applications of Cryptographic Techniques, Lecture Notes in Comput. Sci. 2656, Springer, Berlin, 2003, pp. 433–448, https://doi.org/10.1007/3-540-39200-9_27.