Coding for the Lee and Manhattan Metrics with Weighing Matrices

Tuvi Etzion
Department of Computer Science
Technion-Israel Institute of Technology
Haifa 32000, Israel
Email: etzion@cs.technion.ac.il

Alexander Vardy
Dept. of Electrical and Computer Eng.
University California, San Diego
La Jolla, CA 92093, USA
Email: avardy@ucsd.edu

Eitan Yaakobi
Electrical Engineering Department
California Institute of Technology
Pasadena, CA 91125, USA
Email: yaakobi@caltech.edu

***Abstract*—This paper has two goals. The first one is to discuss good codes for packing problems in the Lee and Manhattan metrics. The second one is to consider weighing matrices for some of these coding problems. Weighing matrices were considered as building blocks for codes in the Hamming metric in various constructions. In this paper we will consider mainly two types of weighing matrices, namely conference matrices and Hadamard matrices, to construct codes in the Lee (and Manhattan) metric. We will show that these matrices have some desirable properties when considered as generator matrices for codes in these metrics. Two related packing problems will be considered. The first one is to find good codes for error-correction (i.e. dense packings of Lee spheres). The second one is to transform the space in a way that volumes are preserved and each Lee sphere (or conscribed cross-polytope), in the space, will be transformed into a shape inscribed in a small cube.**

I. Introduction

The Lee metric was introduced in [17], [22] for transmission of signals taken from GF(p) over certain noisy channels. It was generalized for $\mathbb{Z}_m$ in [13]. The Lee distance $d_L(X,Y)$ between two words $X = (x_1, x_2, \ldots, x_n)$, $Y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_m^n$ is given by $d_L(X,Y) \stackrel{\text{def}}{=} \Sigma_{i=1}^n \min\{x_i - y_i \pmod m, y_i - x_i \pmod m\}$. A related metric, the Manhattan metric, is defined for alphabet letters taken from the integers. For two words $X = (x_1, x_2, \ldots, x_n)$, $Y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}^n$ the Manhattan distance between X and Y, $d_M(X,Y)$, is defined as $d_M(X,Y) \stackrel{\text{def}}{=} \Sigma_{i=1}^n |x_i - y_i|$. A code $\mathbb{C}$ in either metric has minimum distance d if for each two distinct codewords $c_1, c_2 \in \mathbb{C}$ we have $d(c_1, c_2) \geq d$, where $d(\cdot,\cdot)$ stands for either the Lee distance or the Manhattan distance.

The main goal of this work is to explore the properties of some interesting dense codes in the Lee and Manhattan metrics. Two related packing problems will be considered. The first one is to find good codes for error-correction (i.e. dense packings of Lee spheres) in the Lee and Manhattan metrics. The second one is to transform the space in such a way that volumes of shapes are preserved and each Lee sphere (or conscribed cross-polytope), in the space, will be transformed to a shape inscribed in a small cube. Some interesting connections between these two problems will be revealed in this work.

An *n-dimensional Lee sphere* $S_{n,R}$, with radius R, is the shape centered at $(0, \ldots, 0)$ consisting of all the points $(x_1, x_2, ..., x_n) \in \mathbb{Z}^n$ which satisfy

$$\sum_{i=1}^{n} |x_i| \leq R \ .$$

Similarly, an *n-dimensional cross-polytope* is the set consisting of all the points $(x_1, \ldots, x_n) \in \mathbb{R}^n$ which satisfy the equation

$$\sum_{i=1}^{n} |x_i| \leq 1 \ .$$

A Lee sphere, $S_{n,R}$, centered at a point $(y_1, \ldots, y_n) \in \mathbb{Z}^n$, contains all the points of $\mathbb{Z}^n$ whose Manhattan distance from $(y_1, \ldots, y_n)$ is at most R. The size of $S_{n,R}$ is well known [13]:

$$|S_{n,R}| = \sum_{i=0}^{\min\{n,R\}} 2^i \binom{n}{i} \binom{R}{i}$$

A code with minimum distance $d = 2R+1$ (or $d = 2R+2$) is a packing of Lee spheres with radius R. Asymptotically, the size of an n-dimensional Lee sphere with radius R is $\frac{(2R)^n}{n!} + O(R^{n-1})$, when n is fixed and $R \longrightarrow \infty$.

The research on codes in the Manhattan metric is not extensive. It is mostly concerned with the existence and nonexistence of perfect codes, e.g. [13], [16], [20]. Nevertheless, all codes defined in the Lee metric over some finite alphabet, (subsets of $\mathbb{Z}_m^n$) can be extended to codes in the Manhattan metric over the integers (subsets of $\mathbb{Z}^n$). The literature on codes in the Lee metric is very extensive, e.g. [2], [6], [13], [19]. Most of the interest at the beginning was in the existence of perfect codes in these metrics. The interest in Lee codes increased in the last decade due to many new applications of these codes. The increased interest is also due to new attempts to settle the existence question of perfect codes in these metrics [16].

Linear codes are usually the codes which can be handled more effectively and hence we will consider only linear codes throughout this paper.

A linear code in $\mathbb{Z}^n$ is an integer lattice. A *lattice* Λ is a discrete, additive subgroup of the real n-space $\mathbb{R}^n$,

$$\Lambda = \{u_1 \boldsymbol{v}_1 + u_2 \boldsymbol{v}_2 + \cdots + u_n \boldsymbol{v}_n \ : \ u_1, u_2, \cdots, u_n \in \mathbb{Z}\} \ , \quad (1)$$

where $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ is a set of linearly independent vectors in $\mathbb{R}^n$. A lattice Λ defined by (1) is a sublattice of $\mathbb{Z}^n$ if and only if $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\} \subset \mathbb{Z}^n$. We will be interested solely in sublattices of $\mathbb{Z}^n$. The vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ are called *basis* for $\Lambda \subseteq \mathbb{Z}^n$, and the $n \times n$ matrix

$$\mathbf{G} = \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{bmatrix}$$

978-1-4799-0446-4/13/$31.00 ©2013 IEEE

having these vectors as its rows is said to be a *generator matrix* for Λ. The lattice with generator matrix $\mathbf{G}$ is denoted by $\Lambda(\mathbf{G})$.

The *volume* of a lattice Λ, denoted $V(\Lambda)$, is inversely proportional to the number of lattice points per unit volume. There is a simple expression for the volume of Λ, namely, $V(\Lambda) = |\det \mathbf{G}|$. An excellent reference, for more material on lattices and some comparison with our results, is [8].

Sublattices of $\mathbb{Z}^n$ are periodic. We say that the lattice Λ has period $(m_1, m_2, \ldots, m_n) \in \mathbb{Z}^n$ if for each i, $1 \leq i \leq n$, the point $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ is a lattice point in Λ if and only if $(x_1, \ldots, x_{i-1}, x_i + m_i, x_{i+1}, \ldots, x_n) \in \Lambda$. Let m be the least common multiple of the integers $m_1, m_2, \ldots, m_n$. The lattice Λ has also period $(m, m, \ldots, m)$ and it can be reduced to a code $\mathbb{C}$ in the Lee metric over the alphabet $\mathbb{Z}_m$. It is easy to verify that the size of the code $\mathbb{C}$ is $\frac{m^n}{V(\Lambda)}$. The minimum distance of $\mathbb{C}$ can be the same as the minimum distance of Λ, but it can be larger (e.g., most binary codes of length n can be reduced from a sublattice of $\mathbb{Z}^n$, where their Manhattan distance is at most 2. This is the inverse of Construction A [8, p. 137]).

One should note that if the lattice Λ in the Manhattan metric is reduced to a code over $\mathbb{Z}_p$, p prime, in the Lee metric, then the code is over a finite field. But, usually the code in the Lee metric is over a ring which is not a field. It makes its behavior slightly different from a code over a finite field. Codes over rings were extensively studied in the last twenty years, see e.g. [4], [5], [15], and references therein. In our discussion, a few concepts are important and for codes over $\mathbb{Z}_m$ these are essentially the same as the ones in traditional codes over a finite field. For example, the minimum distance of the code is the smallest distance between two codewords. The minimum distance is equal to the weight of the word with minimum Manhattan (Lee) weight.

The definition of a coset for a lattice Λ is very simple. Let Λ be a sublattice of $\mathbb{Z}^n$ and $\boldsymbol{x} \in \mathbb{Z}^n$. The *coset* of $\boldsymbol{x}$ is $\boldsymbol{x}+\Lambda \stackrel{\text{def}}{=} \{\boldsymbol{x}+\boldsymbol{c} \mid \boldsymbol{c} \in \Lambda\}$. For each coset we choose a *coset leader*, which is a point in the coset with minimum Manhattan weight. If there are a few points with the same minimum Manhattan weight we choose one of them (arbitrarily) as the coset leader. Once a set of coset leaders is chosen then each point $\boldsymbol{x} \in \mathbb{Z}^n$ has a unique representation as $\boldsymbol{x} = \boldsymbol{c}+\boldsymbol{s}$, where $\boldsymbol{c}$ is a lattice point of Λ and $\boldsymbol{s}$ is a coset leader. The number of different cosets is equal to the volume of the lattice Λ. In this context, the covering radius of a lattice Λ (a code $\mathbb{C}$) is the distance of the word $\boldsymbol{x}$ whose distance from the lattice (code) is the highest among all words. It equals to the weight of the coset leader with the largest weight. The covering radius of a lattice Λ is the same as the covering radius of the code $\mathbb{C}$ reduced from Λ to $\mathbb{Z}_m$, where m is the period of Λ.

A *weighing matrix* $\mathcal{W}$ of order n and weight w is an $n \times n$ matrix over the alphabet $\{0, 1, -1\}$ such that each row and column has exactly w nonzero entries; and $\mathcal{W} \cdot \mathcal{W}^T = wI_n$, where I_n is the identity matrix of order n. The most important families of weighing matrices are the Hadamard matrices in which $w = n$, and the conference matrices in which $w = n-1$. In most of the results in this paper these families are considered. Our construction in Section IV will use weighing matrices with some symmetry. A weighing matrix $\mathcal{W}$ is *symmetric* if $\mathcal{W}^T = \mathcal{W}$ and *skew symmetric* if $\mathcal{W}^T = -\mathcal{W}$. Information on weighing matrices and parameters in which they exist can be found for example in [7], [12].

In this work we examine lattices and codes related to weighing matrices. We prove that the minimum Manhattan (Lee) distance of the lattice (code) derived from a generator matrix taken as a weighing matrix of weight w, is w. We discuss properties of Reed-Muller like codes, i.e. based on Sylvester Hadamard matrices, in the Lee and the Manhattan metrics. These codes were used before for power control in orthogonal frequency-division multiplexing transmission. We prove bounds on their covering radius and extend their range of parameters. We define transformations which transform $\mathbb{R}^n$ to $\mathbb{R}^n$ (respectively $\mathbb{Z}^n$ to $\mathbb{Z}^n$), in which each conscribed cross-polytope (respectively Lee sphere) in $\mathbb{R}^n$ (respectively $\mathbb{Z}^n$), is transformed into a shape which can be inscribed in a relatively small cube. The transformations will preserve the volume of the shape and we believe that they are optimal in the sense that there are no such transformations which preserve volume and transform conscribed cross-polytopes (respectively Lee spheres) into smaller cubes. Generalization of the transformations yield some interesting lattices and codes which are related to the codes based on Sylvester Hadamard matrices.

The rest of the paper is organized as follows. In Section II we discuss the use of weighing matrices as generator matrices for codes (respectively lattices) in the Lee (respectively Manhattan) metric. We will prove some properties of the constructed codes (respectively lattices), their size, minimum distance, and on which alphabet size they should be considered for the Lee metric. In Section III we will construct codes related to the doubling construction of Hadamard matrices. We will discuss their properties and also their covering radius. In Section IV we present the volume preserving transformations which transform each conscribed cross-polytope (respectively Lee sphere) in $\mathbb{R}^n$ (respectively $\mathbb{Z}^n$), into a shape which can be inscribed in a relatively small cube. These transformations are part of a large family of transformations based on weighing matrices and they will also yield some interesting codes. Some connections to the codes obtained in Section III will be discussed. Due to space limitations no proofs are given and some details are omitted. The interested reader can see the full paper in [10].

II. Codes Generated by Weighing Matrices

This section is devoted to codes whose generator matrices are weighing matrices. We will discuss some basic properties of such codes.

Theorem 1: Let $\mathcal{W}$ be a weighing matrix of order n and weight w and $\Lambda(\mathcal{W})$ the corresponding lattice.

- The minimum Manhattan distance of $\Lambda(\mathcal{W})$ is w.
- The volume of $\Lambda(\mathcal{W})$ is $w^{\frac{n}{2}}$.
- $\Lambda(\mathcal{W})$ can be reduced to a code $\mathbb{C}$ of length n, in the Lee metric, over the alphabet $\mathbb{Z}_w$. The minimum Lee distance of $\mathbb{C}$ is w.

A code is called *self-dual* if it equals its dual. Since the inner product of two rows from a weighing matrix $\mathcal{W}$ is either 0 or w, it follows that the code $\mathbb{C}$ reduced from $\Lambda(\mathcal{W})$ is contained in its dual. Since the size of the code is $w^{\frac{n}{2}}$ and the size of the space is w^n, it follows that the dual code has also size $w^{\frac{n}{2}}$. Thus, we have

Theorem 2: Let $\mathcal{W}$ be a weighing matrix of order n and weight w. If $\mathbb{C}$ is the code over $\mathbb{Z}_w$ reduced from $\Lambda(\mathcal{W})$ then $\mathbb{C}$ is a self-dual code.

Let A be an $n \times n$ matrix over $\mathbb{Z}_k$. The *rank* of A over $\mathbb{Z}_k$ is defined to be the maximum number of linearly independent rows of A over $\mathbb{Z}_k$.

Theorem 3: The rank of a Hadamard matrix of order n over $\mathbb{Z}_n$ is $n-1$.

Theorem 4: If $\mathcal{W}$ is a conference matrix of order $n = p+1$, p is a prime, then its rank over $\mathbb{Z}_p$ (also $\mathbb{F}_p$) is $\frac{p+1}{2}$.

Conjecture 1: If $\mathbb{C}$ is a code of length $p+1$ constructed from a generator matrix which is a conference matrix then $\mathbb{C}$ is an MDS code of dimension $\frac{p+1}{2}$ and minimum Hamming distance $\frac{p+3}{2}$. Conjecture 1 was verified to be true up to $n = 23$, where the conference matrices are based on the Paley's construction from quadratic residues modulo p. Codes with these parameters (self-dual MDS of length $q+1$, q a prime power) were constructed in [14].

III. Codes from the Doubling Construction

The most simple and celebrated method to construct Hadamard matrices of large orders from Hadamard matrices of small orders is the *doubling construction*. Given a Hadamard matrix $\mathcal{H}$ of order n, the matrix

$$\begin{bmatrix} \mathcal{H} & \mathcal{H} \\ \mathcal{H} & -\mathcal{H} \end{bmatrix},$$

is a Hadamard matrix of order $2n$.

A Sylvester Hadamard matrix of order m, $\mathcal{H}_m$, is a $2^m \times 2^m$ Hadamard matrix obtained by the doubling construction starting with the Hadamard matrix $\mathcal{H}_0 = [\ 1\ ]$ of order one. This matrix is also based on the first order Reed-Muller code [18]. Let $H_0 = [\ 1\ ]$ and $H_{m+1} = \begin{bmatrix} H_m & H_m \\ 0 & H_m \end{bmatrix}$, $m \geq 0$. Let $G(m,j)$, $0 \leq j \leq m$, be the $2^m \times 2^m$ matrix constructed from H_m as follows. Let 2^ℓ be the Hamming weight of the s-th row of H_m. If $\ell \geq j$ then the s-th row of $G(m,j)$ will be the same as the s-th row of H_m. If $\ell < j$ then the s-th row of $G(m,j)$ will be the s-th row of H_m multiplied by $2^{j-\ell}$.

It is easy to verify that $G(m,j)$ can be defined recursively as follows. For $1 \leq j < m$, $G(m,j)$ is given by

$$G(m,j) = \begin{bmatrix} G(m-1,j-1) & G(m-1,j-1) \\ 0 & G(m-1,j) \end{bmatrix},$$

where $G(m,m)$ is given by

$$G(m,m) = \begin{bmatrix} G(m-1,m-1) & G(m-1,m-1) \\ 0 & 2G(m-1,m-1) \end{bmatrix},$$

and $G(m,0) = H_m$.

The following lemma can be proved by applying a simple induction.

Lemma 1: $\Lambda(G(m,m)) = \Lambda(\mathcal{H}_m)$, for all $m \geq 0$.

Example 1: The Sylvester Hadamard matrix of order 2, is a Hadamard matrix of order 4, given by

$$\mathcal{H}_2 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}.$$

In $\mathbb{Z}^4$ it generates the same lattice as the generator matrix

$$G(2,2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{bmatrix}.$$

Reducing the entries of $G(2,2)$ into *zeroes* and *ones* yields

$$H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Clearly, the rows of $G(m,j)$ are linearly independent. Let $\Lambda(m,j)$ be the lattice whose generator matrix is $G(m,j)$, and $\mathbb{C}(m,j)$ the code reduced from $\Lambda(m,j)$, over $\mathbb{Z}_{2^j}$, whose generator matrix is $G(m,j)$. $\mathbb{C}(m,j)$ was constructed by a completely different approach for the control of the peak-to-mean envelope power ratio in orthogonal frequency-division multiplexing in [21], where its size and minimum distance were discussed. The following lemma is an immediate result from the recursive construction of H_m.

Lemma 2: The number of rows with Hamming weight 2^i, $0 \leq i \leq m$, in H_m is $\binom{m}{i}$.

By Lemma 2 and by the definition of $G(m,j)$, for each ℓ, $j \leq \ell \leq m$, there exist rows in $G(m,j)$ with Manhattan weight 2^ℓ. These are the only weights of rows in $G(m,j)$.

Theorem 5:

- The minimum Manhattan distance of $\Lambda(m,j)$ is 2^j.
- The volume of the lattice $\Lambda(m,j)$ is $\Pi_{i=0}^{j} 2^{(j-i)\binom{m}{i}}$.
- $\Lambda(m,j)$ is reduced to the code $\mathbb{C}(m,j)$. $\mathbb{C}(m,j)$ has minimum Lee distance 2^j.

In Section IV we will consider codes related to the lattice $\Lambda(m,j)$. The covering radius of these codes will be an important factor in our construction for a space transformation. Therefore, we will discuss now bounds on the covering radius of the lattice $\Lambda(m,j)$, which is equal to the covering radius of the code $\mathbb{C}(m,j)$.

$\Lambda(m,0)$ is equal to $\mathbb{Z}^{2^m}$ and hence its covering radius is 0. $\Lambda(m,1)$ consists of all the points in $\mathbb{Z}^{2^m}$ which have an even sum of elements. The covering radius of this code is clearly 1. $\mathbb{C}(m,2)$ is a diameter perfect code with covering radius 2 and minimum distance 4 [9]. In general we don't know the exact covering radius of $\Lambda(m,j)$ except for two lattices (codes) for which the covering radius was found with a computer aid. The covering radius of $\Lambda(3,3)$ equals 6 and the covering radius of $\Lambda(4,3)$ equals 8. We also found that the covering radius of $\Lambda(4,4)$ is at most 20. However, two bounds can be derived from the structure of $G(m,j)$. Let $r(m,j)$ be the covering radius of the lattice $\Lambda(m,j)$ (and also the code $\mathbb{C}(m,j)$).

Theorem 6: $r(m,m) \leq 3r(m-1,m-1) + 2^{m-1}$, $m \geq 5$, where $r(2,2) = 2$, $r(3,3) = 6$ and $r(4,4) \leq 20$.

One can analyze the bound of Theorem 6 and obtain that when m is large $r(m,m)$ is less than approximately $4 \cdot 3^{m-2}$, or $n^{1.585}$. But, we believe that the covering radius of $\mathbb{C}(m,m)$ is considerably smaller.

Theorem 7: $r(m,j) \leq r(m-1,j-1) + r(m-1,j)$, $2 < j < m$, where $r(m,2) = 2$ for $m \geq 2$ and the upper bound on $r(m,m)$ is given in Theorem 6.

IV. Lee Sphere Transformations

In multidimensional coding, many techniques are applied on multidimensional cubes of $\mathbb{Z}^n$ and cannot be applied on other shapes in $\mathbb{Z}^n$, e.g. [1], [3], [11]. Assume that we want to apply a technique which is applied on any n-dimensional cube of $\mathbb{Z}^n$ to a different n-dimensional shape $\mathcal{S}$ of $\mathbb{Z}^n$. This problem can be solved by a transformation from $\mathbb{Z}^n$ to $\mathbb{Z}^n$, which preserves volumes, in which each n-dimensional shape $\mathcal{S}$ of $\mathbb{Z}^n$ is transformed into a shape $\mathcal{S}'$ which can be inscribed in a relatively small n-dimensional cube of $\mathbb{Z}^n$. The technique is now applied on the image of the transformation and then transformed back into the domain. One of the most important shapes in this context is the n-dimensional Lee sphere with radius R, $S_{n,R}$. Clearly, an n-dimensional Lee sphere with radius R can be inscribed in an $\underbrace{(2R+1)\times\cdots\times(2R+1)}_{n \text{ times}}$ $n-$dimensional cube. In [11] a transformation of $\mathbb{Z}^n$ is given for which $S_{n,R}$ is transformed into a shape inscribed in a cube of size $\underbrace{(R+1)\times(R+1)\times\cdots\times(R+1)}_{n-1 \text{ times}}\times(2R+1)$. The gap from the theoretical size of the cube is still large since the size of the n-dimensional Lee sphere with radius R is $\frac{(2R)^n}{n!}+O(R^{n-1})$, when n is fixed and $R\longrightarrow\infty$. The goal of this section is to close on this gap. In the process, some interesting codes and coding problems will arise. The transformation we have to define is clearly a discrete transformation, but for completeness, and since it has an interest of its own, we will consider also the more simple case of a continuous transformation $T:\mathbb{R}^n\to\mathbb{R}^n$. This can be viewed also as a transformation on conscribed cross-polytopes, which were defined in [13], rather than on Lee spheres. For every Lee sphere, $S_{n,R}$, the *conscribed cross-polytope*, $CP_{n,R}$, is defined [13] to be the convex hull of the $2n$ centers points of the $(n-1)$-dimensional extremal hyperfaces of $S_{n,R}$. What makes this figure more attractive to us than similar figures is that the volume of $CP_{n,R}$ is exactly $\frac{(2R+1)^n}{n!}$.

A. The Continuous Transformation

In this subsection we are going to define a sequence of transformations based on symmetric or skew symmetric weighing matrices. These transformations will transform Lee spheres (or conscribed cross-polytopes) in the space, into shapes inscribed in a relatively small cubes. These transformations also form some interesting codes.

Let $\mathcal{W}$ be a symmetric or skew symmetric weighing matrix of order n and weight w. Given a real number $s>0$, we define a transformation $T_s^{\mathcal{W}}:\mathbb{R}^n\to\mathbb{R}^n$, as follows. For each $\boldsymbol{x}=(x_1,\ldots,x_n)^t\in\mathbb{R}^n$,

$$T_s^{\mathcal{W}}(\boldsymbol{x})\stackrel{\text{def}}{=}\frac{\mathcal{W}\boldsymbol{x}}{s}. \tag{2}$$

Lemma 3: Let $\mathcal{W}$ be a weighing matrix of order n and weight w and let $s>0$ be a positive real number.

- If $\mathcal{W}$ is symmetric then for all $\boldsymbol{x}=(x_1,\ldots,x_n)^t\in\mathbb{R}^n$,
$$T_{\frac{w}{s}}^{\mathcal{W}}(T_s^{\mathcal{W}}(\boldsymbol{x}))=\boldsymbol{x}.$$
- If $\mathcal{W}$ is skew symmetric then for all $\boldsymbol{x}=(x_1,\ldots,x_n)^t\in\mathbb{R}^n$,
$$T_{\frac{w}{s}}^{\mathcal{W}}(T_s^{\mathcal{W}}(\boldsymbol{x}))=-\boldsymbol{x}.$$

Let $\mathcal{W}$ be a symmetric or a skew symmetric weighing matrix of order n and weight w and let s be a positive integer which divides w. Let $\Lambda_s^{\mathcal{W}}$ be the set of points in $\mathbb{Z}^n$ which are mapped to points of $\mathbb{Z}^n$ by the transformation $T_s^{\mathcal{W}}$ given by (2), i.e.

$$\Lambda_s^{\mathcal{W}}\stackrel{\text{def}}{=}\{\boldsymbol{x}\in\mathbb{Z}^n\ :\ T_s^{\mathcal{W}}(\boldsymbol{x})\in\mathbb{Z}^n\}\ .$$

Theorem 8: Let $\mathcal{W}$ be a symmetric or a skew symmetric weighing matrix of order n and weight w. Then $\Lambda_s^{\mathcal{W}}$ is a lattice with minimum Manhattan distance s; moreover, $\Lambda_s^{\mathcal{W}}=T_{\frac{w}{s}}^{\mathcal{W}}(\Lambda_{\frac{w}{s}}^{\mathcal{W}})$. Finally, $\Lambda_s^{\mathcal{W}}$ can be reduced to a code $\mathbb{C}_s^{\mathcal{W}}$ of length n, in the Lee metric, over the alphabet $\mathbb{Z}_s$.

Theorem 9: Let $\mathcal{H}$ be a Hadamard matrix of order $n>4$ and let $s>1$ be an integer which divides n. If s is even then the minimum Lee distance of $\mathbb{C}_s^{\mathcal{H}}$ is s. If s is odd then the minimum Lee distance of $\mathbb{C}_s^{\mathcal{H}}$ is greater than s and is at most $\frac{n}{2}$.

Theorem 9 provides some information on the minimum Lee distance of the code $\mathbb{C}_s^{\mathcal{H}}$, where $\mathcal{H}$ is a Hadamard matrix. In general for a weighing matrix $\mathcal{W}$, what is the minimum Lee distance of the code $\mathbb{C}_s^{\mathcal{W}}$? It appears that it is not always reduced to s as the minimum Manhattan distance of $\Lambda_s^{\mathcal{W}}$. In fact, if $\frac{n}{2}<w<n$ we conjecture that it is always w, in contrast to the result in Theorem 9 for $w=n$.

Theorem 10: If $\mathcal{W}$ is a weighing matrix of order n and weight w then $\Lambda_w^{\mathcal{W}}=\Lambda(\mathcal{W})$.

Lemma 4: If s_1 divides s_2 and $s_1<s_2$, then $\Lambda_{s_2}^{\mathcal{W}}\subset\Lambda_{s_1}^{\mathcal{W}}$.

Corollary 1: If s divides w then $\Lambda_s^{\mathcal{W}}$ contains $\Lambda(\mathcal{W})$.

We now turn to a volume preserving transformation from the set of all transformations which were defined. This transformation is $T_{\sqrt{w}}^{\mathcal{W}}$ and it is redefined as $T^{\mathcal{W}}:\mathbb{R}^n\to\mathbb{R}^n$ to be

$$T^{\mathcal{W}}(\boldsymbol{x})\stackrel{\text{def}}{=}\frac{\mathcal{W}\boldsymbol{x}}{\sqrt{w}}. \tag{3}$$

Theorem 8 is applied also with the transformation $T^{\mathcal{W}}$. In this case $w=D^2$, where D is a positive integer, $\Lambda^{\mathcal{W}}\stackrel{\text{def}}{=}\Lambda_D^{\mathcal{W}}$ is a lattice with minimum Manhattan distance D, and $\Lambda^{\mathcal{W}}=T^{\mathcal{W}}(\Lambda^{\mathcal{W}})$. Finally, $\Lambda^{\mathcal{W}}$ can be reduced to a code $\mathbb{C}^{\mathcal{W}}$ of length n, in the Lee metric, over the alphabet $\mathbb{Z}_D$.

Lemma 5: A conscribed cross-polytope, centered at $\boldsymbol{c}=(c_1,\ldots,c_n)^t\in\mathbb{R}^n$, $CP_{n,R}(\boldsymbol{c})$, is inscribed after the transformation $T^{\mathcal{W}}$ inside an n-dimensional cube of size

$$\left(\frac{2R+1}{\sqrt{w}}\right)\times\cdots\times\left(\frac{2R+1}{\sqrt{w}}\right).$$

Note that since $\det(\mathcal{W}/\sqrt{w})=1$, it follows that the transformation $T^{\mathcal{W}}$ also preserves volumes. The volume of the inscribing n-dimensional cube is $\frac{(2R+1)^n}{\sqrt{w^n}}$. If we choose $w=n$, i.e. a Hadamard matrix of order n, then we get that the ratio between the volumes of the n-dimensional cube and the conscribed cross-polytope is $\frac{n!}{n^{n/2}}$. We conjecture that there is no transformation which preserves volumes and achieves a better ratio. The shape of the Lee sphere is very similar to the one of the conscribed cross-polytope and hence a similar result can be obtained for a Lee sphere.

B. On the connection between $\mathbb{C}(m,j)$ and $\mathbb{C}_{2^j}^{\mathcal{H}_m}$

In this subsection we consider connections between the code $\mathbb{C}(m,j)$ and the code $\mathbb{C}_{2^j}^{\mathcal{H}_m}$ defined in Theorem 8, where the weighing matrix $\mathcal{W}$ is the Hadamard matrix $\mathcal{H}_m$.

Lemma 6: The inner product of a lattice point from $\Lambda(m,j)$ and a lattice point from $\Lambda(m,m)$ is divisible by 2^j.

Corollary 2: The inner product of a codeword from $\mathbb{C}(m,j)$ and a codeword from $\mathbb{C}(m,m)$ is divisible by 2^j.

Lemma 7: $\mathbb{C}(m,j) \subseteq \mathbb{C}_{2^j}^{\mathcal{H}_m}$.

Corollary 3: The covering radius of the code $\mathbb{C}_{2^j}^{\mathcal{H}_m}$ is less than or equal to the covering radius of the code $\mathbb{C}(m,j)$.

Conjecture 2: $\mathbb{C}(m,j) = \mathbb{C}_{2^j}^{\mathcal{H}_m}$.

For a given word $\boldsymbol{x}$, the *reverse* of $\boldsymbol{x}$, $\boldsymbol{x}^R$, is the word obtained from $\boldsymbol{x}$ by reading its elements from the last to the first.

Lemma 8: If $\boldsymbol{x}$, the i-th row of the matrix H_m, has Manhattan weight 2^ℓ then $\boldsymbol{x}^R \cdot \mathcal{H}_m$ is a multiple by 2^ℓ of the reverse for the (2^m+1-i)-th row of the matrix H_m.

Lemma 9: If the i-th row of H_m has weight 2^ℓ then the (2^m+1-i)-th row of H_m has weight $2^{m-\ell}$.

Lemma 10: $T_{2^j}^{\mathcal{H}_m}(\Lambda(m,j)) = \Lambda(m,m-j)$.

Corollary 4: $\mathbb{C}_{2^j}^{\mathcal{H}_m} = \mathbb{C}(m,j)$ if and only if $\mathbb{C}_{2^{m-j}}^{\mathcal{H}_m} = \mathbb{C}(m,m-j)$.

C. The Discrete Transformation

For the discrete case we want to modify the transformation $T^{\mathcal{W}}$, used for the continuous case. Let D be a positive integer and $\mathcal{W}$ a symmetric weighing matrix of order n and weight $w = D^2$. Let $\mathbb{S}$ be the set of coset leaders of the lattice $\Lambda^{\mathcal{W}}$ defined in Theorem 8 based on (3). The discrete transformation $\tilde{\mathbf{T}}^{\mathcal{W}} : \mathbb{Z}^n \to \mathbb{Z}^n$ is defined as follows. For each $(x_1,\ldots,x_n) \in \mathbb{Z}^n$, let $(x_1,\ldots,x_n) = (c_1,\ldots,c_n) + (s_1,\ldots,s_n)$, where $(c_1,\ldots,c_n)^t \in \Lambda^{\mathcal{W}}$ and $(s_1,\ldots,s_n)^t \in \mathbb{S}$.

$$\tilde{\mathbf{T}}^{\mathcal{W}}((x_1,\ldots,x_n)^t) = T^{\mathcal{W}}((c_1,\ldots,c_n)^t) + (s_1,\ldots,s_n)^t,$$

where $T^{\mathcal{W}}$ is defined in (3).

Lemma 11: For each $\boldsymbol{x} = (x_1,\ldots,x_n)^t \in \mathbb{Z}^n$,

$$\tilde{\mathbf{T}}^{\mathcal{W}}(\tilde{\mathbf{T}}^{\mathcal{W}}(\boldsymbol{x})) = \boldsymbol{x}.$$

Theorem 11: Let ρ be the covering radius of the lattice $\Lambda^{\mathcal{W}}$. A Lee sphere with radius R is inscribed after the transformation $\tilde{\mathbf{T}}^{\mathcal{W}}$, inside an n-dimensional cube of size

$$\left(2\left\lfloor\frac{R+\rho}{D}\right\rfloor + 2\rho + 1\right) \times \cdots \times \left(2\left\lfloor\frac{R+\rho}{D}\right\rfloor + 2\rho + 1\right).$$

The size of an n-dimensional Lee sphere with radius R is $\frac{(2R)^n}{n!} + O(R^{n-1})$, when n is fixed and $R \longrightarrow \infty$. The size of the inscribing n-dimensional cube is $\left(2\left\lfloor\frac{R+\rho}{D}\right\rfloor + 2\rho + 1\right)^n$. Since the covering radius ρ of the code $\mathbb{C}^{\mathcal{W}}$ is a low degree polynomial in n (see the next paragraph), and n is fixed, we get that for $R \longrightarrow \infty$ the size of the inscribing n-dimensional cube is $\frac{(2R)^n}{n^{n/2}} + O(R^{n-1})$. Therefore, the size of the cube is greater roughly $\frac{n!}{n^{n/2}}$ times than the size of the n-dimensional Lee sphere. This is a significant improvement with respect to the transformation given in[11], where the n-dimensional Lee sphere is inscribed inside an n-dimensional cube of size $\frac{(2R)^n}{2^{n-1}} + O(R^{n-1})$.

Generally, it is straightforward to show that the covering radius of the lattice $\Lambda^{\mathcal{W}}$, where $\mathcal{W}$ is a weighting matrix of order n and weight $w = D^2$, is at most $\frac{n\cdot\sqrt{w}}{4}$, but we believe it is considerably smaller. If $\mathcal{W}$ is $\mathcal{H}_m$ then an analysis of Theorem 7 implies that the covering radius of $\mathbb{C}^{\mathcal{H}_m}$ is at most $n^{1.085}$. But, we believe that the covering radius is much smaller, mainly since we think that the bound of Theorem 6 can be improved, while we conjecture that the bound of Theorem 7 is quite tight.

V. Conclusions

We have considered the linear span of weighing matrices as codes in the Lee and the Manhattan metrics. We have proved that the minimum Lee distance of such a code is equal to the weight of a row in the matrix. A set of codes related to Sylvester Hadamard matrices were defined. Properties of these codes, such as their size, minimum distance, and covering radius were explored. We have defined a transformation which transforms any Lee sphere in the space (also a conscribed cross-polytope in the continuous space) into a shape with the same volume (in the continuous space) located in a relatively small cube. The transformation was defined as one of a sequence of transformations which yield a sequence of error-correcting codes related to the codes obtained from Sylvester type Hadamard matrices. Many interesting questions arise from our discussion.

Acknowledgment

This work was supported in part by the U.S.-Israel Binational Science Foundation, Jerusalem, Israel, under Grant No. 2006097.

References

[1] K. A. S. Abdel-Ghaffar, "An information- and coding-theoretic study of bursty channels with applications to computer memories", *Ph.D. dissertation, California Inst. Technol. Pasadena, CA*, June 1986.

[2] J. T. Astola, "Concatenated codes for the Lee metric", *IEEE Trans. on Inform. Theory*, vol. IT-28, pp. 778–779, September 1982.

[3] M. Breitbach, M. Bossert, V. Zyablov, and V. Sidorenko, "Array codes correcting a two-dimensional cluster of errors", *IEEE Trans. on Inform. Theory*, vol. IT-44, pp. 2025-2031, September 1998.

[4] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic cyclic codes", *Designs, Codes and Cryptography*, vol. 6, pp. 21–35, 1995.

[5] C. Carlet, "Z_{2^k}-linear codes", *IEEE Trans. on Inform. Theory*, vol. IT-44, pp. 1543-1547, July 1998.

[6] J. C.-Y. Chiang and J. K. Wolf, "On channels and codes for the Lee metric", *Information and Control*, vol. 19, pp. 1593–173, Sept. 1971.

[7] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, Boca Raton, Florida: Chapman and Hall/CRC, 2007.

[8] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*, New York: Springer-Verlag, 1988.

[9] T. Etzion, "Product constructions for perfect Lee codes", *IEEE Trans. Inform. Theory*, vol. IT-57, pp. 7473–7481, November 2011.

[10] T. Etzion, A. Vardy and E. Yaakobi, "Coding for the Lee and Manhattan Metrics with Weighing Matrices", *IEEE Trans. Inform. Theory,* submitted, also *arxiv.org/abs/1210.5725.*

[11] T. Etzion and E. Yaakobi, "Error-correction of multidimensional bursts", *IEEE Trans. Inform. Theory*, vol. IT-55, pp. 961–976, 2009.

[12] A. V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, New York-Basel: Marcel Decker, 1979.

[13] S. W. Golomb and L. R. Welch, "Perfect codes in the Lee metric and the packing of polyominos", *SIAM J. Appl. Math.*, vol. 18, pp. 302–317, 1970.

[14] M. Grassl and T. A. Gulliver, "On self-dual MDS codes", in Proc. *IEEE Inter. Symp. on Inform. Theory,* Toronto, pp. 1954–1957, 2008.

[15] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes", *IEEE Trans. on Inform. Theory*, vol. IT-40, pp. 301–319, 1994.

[16] P. Horak, "On perfect Lee codes", *Discrete Mathematics*, vol. 309, pp. 5551–5561, 2009.

[17] C. Y. Lee, "Some properties of nonbinary error-correcting code", *IRE Trans. on Inform. Theory*, vol. IT-4, pp. 72–82, 1958.

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

[19] A. Orlitsky, "Interactive communication of balanced distributions and of correlated files", *SIAM J. Discrete Math.*, vol. 6 pp. 548–564, 1993.

[20] K. A. Post, "Nonexistence theorem on perfect Lee codes over large alphabets", *Information and Control*, vol. 29, pp. 369–380, 1975.

[21] K.-U. Schmidt, "Complementary sets, generalized Reed-Muller codes, and power control for OFDM", *IEEE Trans. on Inform. Theory*, vol. IT-53, pp. 808–814, February 2007.

[22] W. Ulrich, "Non-binary error correction codes", *Bell Sys. Journal*, vol. 36, pp. 1341–1387, 1957.