12-1-2010

Error-Correcting Codes and Minkowski's Conjecture

Peter Horak
University of Washington Tacoma, horak@uw.edu

Tatra Mt. Math. Publ. **45** (2010), 37–49
DOI: 10.2478/v10127-010-0004-y

TATRA MOUNTAINS
Mathematical Publications

ERROR-CORRECTING CODES AND MINKOWSKI'S CONJECTURE

Peter Horak

ABSTRACT. The goal of this paper is twofold. The main one is to survey the latest results on the perfect and quasi-perfect Lee error correcting codes. The other goal is to show that the area of Lee error correcting codes, like many ideas in mathematics, can trace its roots to the Phytagorean theorem $a^2+b^2=c^2$. Thus to show that the area of the perfect Lee error correcting codes is an integral part of mathematics. It turns out that Minkowski's conjecture, which is an interface of number theory, approximation theory, geometry, linear algebra, and group theory is one of the milestones on the route to Lee codes.

1. Introduction

Let $\mathcal{S}$ be a space and $\mathcal{T} = \{T_i, i \in I\}$ be a family of subsets of $\mathcal{S}$ called also tiles. Then $\mathcal{T}$ forms a tiling of $\mathcal{S}$ if $\bigcup_{i\in I} T_i = \mathcal{S}$ and $\mathrm{int}(T_i) \bigcap \mathrm{int}(T_j) = \emptyset$ for all $i \neq j$, $i, j \in I$. Throughout this paper $\mathcal{S} = \mathbb{R}^n$ and the tiles will be unit cubes or clusters of unit cubes. It is trivial to tile $\mathbb{R}^n$ by unit cubes. Two unit cubes are called twins if they share a complete $(n-1)$-dimensional face. In Figure 1(a) there are twins in $\mathbb{R}^3$, while in (b) there is an example of two unit cubes which share a 2-dimensional face but not the entire one. It would be natural to ask whether there exists a tiling of $\mathbb{R}^n$ by unit cubes so that there are NO twins. In other words, can we find a tiling of $\mathbb{R}^n$ by unit cubes that is completely "messed up"?

A lattice tiling $\mathcal{T}$ of $\mathbb{R}^n$ by unit cubes is a tiling where the centers of cubes in $\mathcal{T}$ form a lattice; as usual, by a lattice of points in $\mathbb{R}^n$ we mean a subgroup with respect to the vector addition. In 1896 Minkowski formulated a conjecture, which does not sound that natural as the above question, in linear algebra terms, and later in 1907 he added its geometric version that is stated below:

2010 Mathematics Subject Classification: 05B45, 94B99.
Keywords: Lee codes, tilings, unit cubes.
This material is based upon work supported under the grant NIL-I-004 from Iceland, Liechtenstein and Norway through the EEA Financial Mechanism and the Norwegian Financial Mechanism.

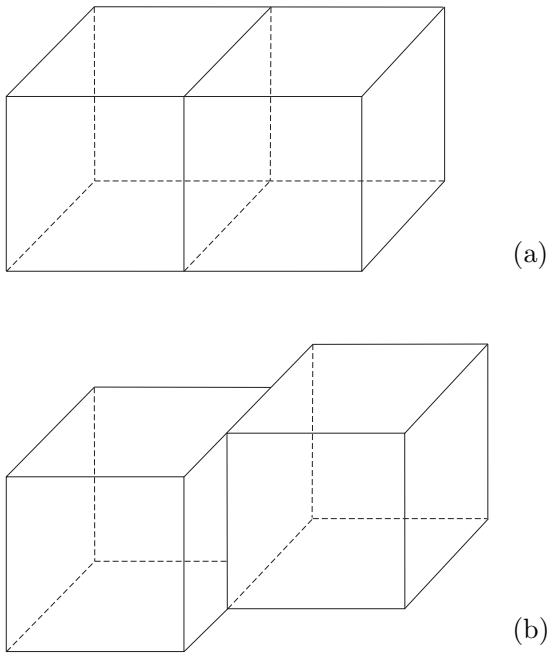

FIGURE 1. (a) Twins in R^3, (b) an example of two unit cubes which share a 2-dimensional face but not the entire one.

CONJECTURE 1 (Minkowski)**.** Each lattice tiling of $\mathbb{R}^n$ by unit cubes contains twins.

To understand why Minkowski included the lattice condition in his conjecture we will provide a short historic account of the development that led to the conjecture. Already in the ancient Greece they discovered all integer solutions of the equation $x^2 + y^2 = z^2$. In the course of time Diophantos, Fermat, Euler and others studied equations $x^2 + y^2 = z^3$, $x^2 + y^2 = p$, where p is a prime, and forms Ax^2+By^2, etc. Lagrange in 1775 looked at the most general quadratic form $Ax^2 + Bxy + Cy^2$, where A, B, C are fixed integers. In the case $Ax^2 + Bxy + Cy^2$ is positive for any x, y, not both equal to 0, then the form is called positive definite. To estimate the minimum nonzero value of the form for integers would help with his classification of quadratic forms. Gauss showed that instead of looking for the minimum of a positive definite quadratic form we may examine the square of the length of the shortest nonzero vector in a lattice. In one of his deepest results Minkowski improved on the upper bound of the minimum of the

positive definite quadratic forms. His work related to the result led to the above stated conjecture and this is why Minkowski was interested in lattice tilings. For more detailed description of the roots on Minkowski's conjecture we refer the reader to the excellent monograph [20].

In 1930, when Minkowski's conjecture was still open, K e l l e r [14] suggested that the lattice condition in the conjecture is redundant, that the nature of the problem is purely a geometric one, and not algebraic as assumed by Minkowski. Thus he conjectured that each tiling of $\mathbb{R}^n$ by unit cubes contains twin cubes. In 1940 P e r o n [17] verified Keller's conjecture for $n \leq 6$. However, in 1992, L a g a r i a s and S h o r [15] showed that Keller's conjecture is false for each $n \geq 10$. This remarkable result is on one hand surprising, while on the other hand is intuitive. The surprising part is that there is a tiling of $\mathbb{R}^{10}$ by unit cubes not containing twins. However, once we have such a tiling, it is expected that a tiling with this property exists for all higher dimensions. The higher the dimension of the space, the more freedom we get. Keller's conjecture for the remaining dimensions was solved in 2002 by M a c k e y [16], who showed that the conjecture is false for $n = 8, 9$ as well, and finally this year M y r v o l d et al. (private communication) showed, providing a computer based proof, that Keller's conjecture is true for $n = 7$.

Minkowski's conjecture was settled in the affirmative by H a j ó s [7] who first, in 1938, reformulated Minkowski's conjecture in group theory terms, and then solved the conjecture three years later. Hajós reformulation turns out to provide a very strong tool in the area of tilings till nowadays. Therefore we will state it here. Hajós proved that the following statement is equivalent to Minkowski's conjecture:

Theorem 1 (Hajós). *Let G be a finite abelian group. If G can be written as a direct product of cyclic sets A_i; that is, $A = A_1 + A_2 + \cdots + A_n$, where A_i is of the form $A_i = \{e, a, a^2, a^3, \ldots, a^k\}, a \in G, i = 1, \ldots, n$, e being the unit element of G, then A_i is a subgroup of G for at least one i.*

2. Tilings by crosses

After Minkowski's conjecture has been settled tilings of $\mathbb{R}^n$ by different clusters of cubes have been considered. In the paper we first confine ourselves to tilings by n-crosses. Consider a unit cube in $\mathbb{R}^n$, where at each facet another unit cube is attached. Such a cluster of cubes is called the n-cross or simply a cross. It easily follows from the definition that the n-cross consists of $2n + 1$ cubes. We note that the n-cross can be seen as a Lee sphere of radius 1, see Figure 3.

Tiling by crosses were considered independently by several people, e.g., Ulrich [24] in 1957, Kárteszi [12] in 1966, Stein [19] in 1967, and Golomb and Welch [4] in 1968.

Ulrich was working on the subject from the error-correcting codes point of view, and he did not consider tilings of the whole n-space. Kárteszi asked whether there exists a tiling of $\mathbb{R}^3$ by crosses. Feller, for $n = 3$, and then Korchmáros and Golomb and Welch [4] showed that there is a tiling of $\mathbb{R}^n$ by crosses for all $n \geq 2$.

Let $\mathcal{T}$ be a tiling of $\mathbb{R}^n$ by crosses. Then such a tiling is called a lattice tiling if the centers of the crosses in $\mathcal{T}$ form a lattice; and it is called a $\mathbb{Z}$-tiling ($\mathbb{Q}$-tiling) if the centers of the crosses in $\mathcal{T}$ have integer (rational) coordinates. It turns out that all tilings of $\mathbb{R}^n$ by crosses mentioned above were lattice $\mathbb{Z}$-tilings. Molnár [13] has made a big step forward by enumerating all such tilings.

Theorem 2 (Molnár). *The number of non-congruent lattice $\mathbb{Z}$-tilings of $\mathbb{R}^n$ by crosses equals the number of non-isomorphic Abelian groups of order $2n + 1$.*

Molnár's paper, on top of bringing an interesting result, provides a powerful method how to construct different kinds of lattice tiling by clusters of cubes. For longer time only lattice $\mathbb{Z}$-tilings by crosses were known. It was widely believed that there is no $\mathbb{Q}$-tiling by crosses which is not congruent to a $\mathbb{Z}$-tiling. Let us stress that a $\mathbb{Q}$-tiling that is not a $\mathbb{Z}$-tiling has to be a tiling containing crosses C_1 and C_2 so that there is a unit cube K_1 in C_1 and a unit cube K_2 in C_2 so that K_1 and K_2 intersect in an $(n-1)$-dimensional face but not in the whole such face, see Figure 1(b). Therefore, the following result of Szabó [21] came as a big surprise.

Theorem 3. *If $2n + 1$ is not a prime, then there exists a $\mathbb{Q}$-tiling of $\mathbb{R}^n$ by crosses that is neither a $\mathbb{Z}$-tiling nor a lattice tiling.*

To prove his result Szabó used a refinement of Molnár's method mentioned above. If tiling a finite space one can use a trial and error method to find it. However, when tiling an infinite space, a clear strategy has to be employed. One approach is to use algebraic methods, another is to find a periodic tiling; a tiling that is obtained by repetitively applying a tiling of a finite space. The tiling produced by Szabó is not a lattice tiling but it is a periodic one. A tiling that is not periodic, i.e., a tiling that is not obtained by repetitively placing a finite block, is called primitive. In [11] primitive tilings of $\mathbb{R}^n$, where $2n + 1$ is not a prime, have been constructed for the first time. In fact a stronger result has been proved there:

Theorem 4. *If $2n+1$ is not a prime, then (i) the total number of non-congruent primitive $\mathbb{Z}$-tilings of $\mathbb{R}^n$ by crosses is $2^{\aleph_0}$; (ii) the total number of non-congruent periodic $\mathbb{Z}$-tilings of $\mathbb{R}^n$ by crosses is $\aleph_0$.*

Not much is known about the number of tilings of $\mathbb{R}^n$ by crosses in the case when $2n+1$ is a prime. From Molnar's result we know that there is the unique, up to a congruency, lattice $\mathbb{Z}$-tiling of $\mathbb{R}^n$ by crosses. Further, a generalization of Hajós result, Theorem 1, due to Rédei, implies that for $2n+1$ being a prime number, each lattice tiling of $\mathbb{R}^n$ by crosses is congruent to a $\mathbb{Z}$-tiling. It is obvious that there is only one tiling, up to a congruency, of $\mathbb{R}^n$ by crosses for $n = 1$. In [11] it was proved

Theorem 5. *For $n = 2$ and $n = 3$, any two tilings of $\mathbb{R}^n$ by crosses are congruent.*

We believe that the statement can be extended to all n when $2n+1$ is a prime. Therefore,

Conjecture 2. If $2n+1$ is a prime number then there exists, up to a congruency, only one $\mathbb{Z}$-tiling of $\mathbb{R}^n$ by crosses.

The above conjecture, if true, would go totally against our intuition that says the higher the dimension of $\mathbb{R}^n$ the more freedom we get; see also a comment on the results on Keller's conjecture. There are $2^{\aleph_0}$ tiling by crosses of $\mathbb{R}^4$ but there would be only ONE tiling of $\mathbb{R}^5$ by crosses. Yet, we believe that we have some evidence that supports the conjecture.

2.1. Hilbert's 18th problem

A modification of a cross provides a counterexample to the 18-th problem of Hilbert.

Problem 1 (Hilbert). *If congruent copies of a polyhedron P tile $\mathbb{R}^3$, is there a group of motions that copies of P under this group of motions tile this space?*

In 1985 S z a b ó [22] modified a 3-cross by adding pyramids at the end of its six arms, which are lopsided to prevent rotational symmetries, see Figure 2.

This polyhedron tiles $\mathbb{R}^3$ but not by a group of motions (= distance preserving bijections). This is probably the most simple and elegant counterexample to Hilbert's problem.

3. Lee error-correcting codes

To make this paper self-contained we start with some basic definitions. Let $(\mathcal{C}, \rho)$ be a metric space. Then a code is any subset M of $\mathcal{C}$, $|M| \geq 2$. The elements of $\mathcal{C}$ will be called *words*, while elements of M will be referred to as *codewords*. Let $A \in \mathcal{C}$. Then $S(A, r)$ will stand for the sphere of radius r centered at A.

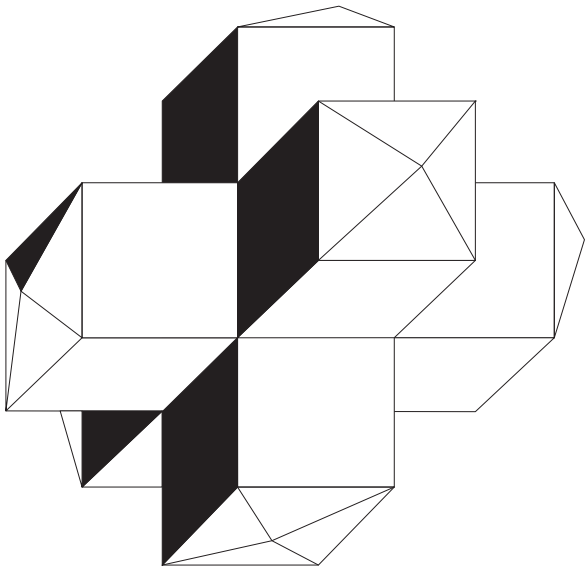

FIGURE 2. Szabó's modification of a 3-cross by adding pyramids.

The code M is an *e-error correcting* code if for any two codewords $W, Z \in M$ it holds $S(W, e) \cap S(Z, e) = \emptyset$; that is, if $\rho(W, Z) \geq 2e + 1$. If, in addition, $\bigcup_{W \in \mathcal{C}} S(W, e) = \mathcal{C}$, then M is a *perfect* e-error correcting code. In other words, a code M is a perfect e-error correcting if for each word $A \in \mathcal{C}$ there exists the unique codeword $W \in M$ so that $\rho(A, W) \leq e$.

The Lee codes are subsets of the metric space $(\mathcal{C}, \rho_L)$, where $\mathcal{C} = \mathbb{Z}_q^n$, and ρ_L is the Lee metric (= the Manhattan metric, the zig-zag metric). That is, for any two words $U, V \in \mathbb{Z}_q^n$, $U = (u_1, u_2, \ldots, u_n)$, $V = (v_1, v_2, \ldots, v_n)$, $\rho_L(U, V)$ is given by $\rho_L(U, V) = \sum_{i=1}^{n} \min(|u_i - v_i|, q - |u_i - v_i|)$. Such code is called a Lee code of block size n over $\mathbb{Z}_q$. A perfect e-error correcting code of block size n over $\mathbb{Z}_q$ will be denoted by $PL(n, e, q)$. By a Lee code of block size n over $\mathbb{Z}$ we will understand a code $M \subset \mathbb{Z}^n$. The Lee metric in this case is given by $\rho_L(U, V) = \sum_{i=1}^{n} |u_i - v_i|$, where $U = (u_1, u_2, \ldots, u_n)$, $V = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$. A perfect e-error correcting Lee code over $\mathbb{Z}$ will be denoted by $PL(n, e)$.

Let $n, q, e \in N$, $q \geq 2e+1$, be numbers so that there exists a $PL(n, e, q)$ code. Then it is easily seen that a periodic repetition of this code results in a $PL(n, e)$ code. This immediately yields

THEOREM 6. *Let n, e be numbers so that there is no $PL(n, e)$ code. Then $PL(n, e, q)$ code exists for no $q \geq 2e + 1$.*

Therefore, we first will concentrate on $PL(n,e)$ codes. Since $PL(n,e)$ code can be seen as a partition of $\mathbb{Z}^n$, only a small step is needed to get a geometrical interpretation of $PL(n,e)$ codes. Let $\mathbb{R}$ be the set of real numbers. Consider the n-dimensional space $\mathbb{R}^n$ endowed with the Lee metric ρ_L. The n-cube centered at $X=(x_1,\dots,x_n)\in\mathbb{R}^n$ is the set $C(X)=\{Y=(y_1,\dots,y_n)|\, y_i=x_i+\alpha_i\,,$ where $-\frac{1}{2}\le\alpha_i\le\frac{1}{2}\}$. By a Lee sphere of radius r in $\mathbb{R}^n$, $L(n,r)$, centered at O, we understand the union of n-cubes centered at Y, where $\rho_L(O,Y)\le r$, and Y has integer coordinates. Finally, a Lee sphere of radius r in $\mathbb{R}^n$ centered at $X\in\mathbb{R}^n$ is a translation of $L(n,r)$ centered at O along the coordinate axes so that O is mapped on X. Clearly, a $PL(n,e)$ code exists if and only if there is a tiling of $\mathbb{R}^n$ by Lee spheres of radius e. The Lee spheres $L(2,1), L(2,2), L(3,1)$, and $L(3,2)$ are depicted in Figure 3. As it can be easily seen from the definition of the Lee sphere, the n-cross is the Lee sphere of radius 1.

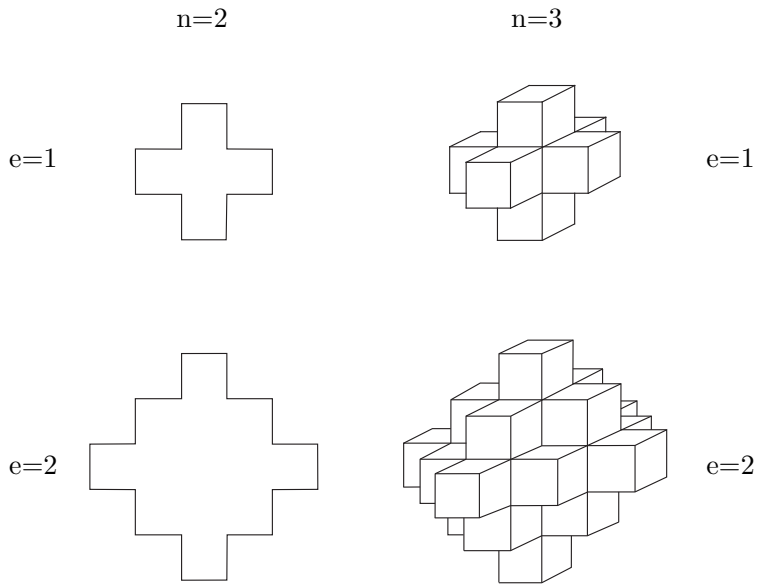

FIGURE 3. The Lee spheres $L(2,1), L(2,2), L(3,1)$, and $L(3,2)$.

3.1. The Golomb-Welch conjecture

G o l o m b and W e l s h [4] constructed a perfect e-error correcting Lee code for parameters $(n,e,q)=(1,e,2e+1)\,,\ \big(2,e,e^2+(e+1)^2\big)$, and $(n,1,2n+1)$ (tiling by crosses). In [4] they conjectured that these are the only perfect Lee error-correcting codes.

Conjecture 3 (Golomb-Welch). There are no $PL(n,e)$ codes for $n > 2, e > 1$.

Thus, in other words, see Theorem 6, they conjectured that there are no perfect e-error correcting codes $PL(n,e,q)$ for $n > 2$, $e > 1$, and $q \geq 2e+1$. There are many results supporting the conjecture. In [18] P o s t proved:

Theorem 7 (Post). *$PL(n,e)$ codes do not exist for $3 \leq n \leq 5$, $e \geq n-2$, and for $n \geq 6$, $e \geq \frac{\sqrt{2}}{2}n - \frac{1}{4}\big(3\sqrt{2}-2\big)$.*

In the final remark in [18] P o s t states that by using a computer to evaluate coefficients of the Taylor series of a suitable function it is possible to show that there are no perfect e-error correcting codes for

$$6 \leq n \leq 130, \text{ and } e \geq \frac{1}{16}(9n-15), \text{ and } 131 \leq n \leq 305, \text{ and } e \geq \frac{1}{16}(9n-14).$$

To the best knowledge of the author, so far the nonexistence of $PL(n,e)$ codes has not been proved for other values of n and e. To provide a support for the non-existence of $PL(n,e)$ codes A s t o l a [1] and others showed the non-existence of $PL(n,e,q)$ codes for specific values of n, e, and $q \geq 2e+1$. It seems that the bigger e is, the easier it is to show that a perfect Lee code does not exist. Moreover, the value of $e = 2$ is the threshold value for the non-existence of perfect Lee codes. Thus, we guess that the most difficult case of the Golomb-Welch conjecture is that for $e = 2$. There are only some sporadic results for $e = 2$ and $n > 4$. The non-existence of a perfect 2-error correcting Lee code $PL(n,2,q)$ for $q = 13$; q not divisible by a prime of the form $4m+1$, and $q = p^k$, p is a prime, $p \neq 13$, $p < \sqrt{2n^2+2n+1}$ is shown in [1].

In [10] we proved:

Theorem 8. *There is no $PL(n,2)$ code for $n = 5$ and 6.*

This way the Golomb-Welch conjecture is proved for all pairs (n,e), where $6 \geq n$.

3.2. 1-error correcting Lee codes

It is very likely, see the Golomb-Welch conjecture, that for $n > 2$, perfect e-error correcting Lee codes exist only for $e = 1$. As only linear codes are interesting from the practical point of view, in [3] we determined all numbers q for which there exists a perfect, linear 1-error correcting Lee code of block length n over $\mathbb{Z}_q$, that is a linear $PL(n,e,q)$ code. In this subsection we briefly describe the main results of the paper.

In order to be able to describe the structure of linear $PL(n,1,q)$ codes, and then to enumerate them, we first generalize this notion. Let $q_1, \ldots, q_n \in \mathbb{N}$. Then by $PL(n,1;\, q_1, \ldots, q_n)$ we will denote a perfect 1-error correcting Lee code of block size n over $\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_n}$. Clearly, if $q_1 = \cdots = q_n = q$, then $PL(n,1,q)$

code is obtained. The following theorem provides a sufficient condition for the existence of a linear $PL(n, e; q_1, \ldots, q_n)$ code. To be able to facilitate our discussion we need one more definition.

Let G be an abelian group of order $2k+1$. An ordered set $F = (g_1, \ldots, g_k)$ of k distinct elements of G is fundamental if, for all $i = 1, \ldots, k$, it is $g_i \neq 0$, and $g_i^{-1} \notin F$. By the multiset of orders of G, denoted $\mathrm{Ord}(G)$, we will understand the multiset $\{\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_k)\}$, where $(g_1, \ldots, g_k)$ is a fundamental set. It is not difficult to see that $\mathrm{Ord}(G)$ is well defined. That is, to see that $\mathrm{Ord}(G)$ does not depend on the choice of its fundamental set F. Indeed, as G is of an odd order, there is no convolution in G. Thus, each fundamental set contains exactly one element from every pair g, g^{-1}, $g \neq 0$, and the fact that $\mathrm{ord}(g) = \mathrm{ord}(g^{-1})$ for every $g \in G$ completes the argument.

Theorem 9. *Let G be an abelian group of order $2n+1$, $F = (g_1, \ldots, g_n)$ be a fundamental set of G, and $q_i \in \mathbb{N}$, where $ord(g_i)|q_i$ for $i = 1, \ldots, n$. Then the set $\mathcal{L} \subset \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_n}$ defined by $\mathcal{L} = \{(a_1, \ldots, a_n); a_1 g_1 + \cdots + a_n g_n = 0\}$, is a linear $PL(n, 1; q_1, \ldots, q_n)$ code.*

So Theorem 9 guaranties the existence of such a code and shows how to construct it. It turns out that this condition is also necessary. We will state the condition only for the case $q_1 = \cdots = q_n = q$.

Theorem 10. *A linear $PL(n, 1, q)$ code exists if and only if there is an abelian group G of order $2n+1$ so that $ord(g)|q$ for all $g \in G$.*

As an immediate consequence we get

Corollary 11. *Let $n \in \mathbb{N}$, $2n+1 = p_1^{a_1} \ldots p_k^{a_k}$ be the prime number factorization of $2n+1$ and let $p = \prod_{i=1}^{k} p_i$. Then a linear $PL(n, 1, q)$ code exists if and only if $p|q$. In particular, the smallest q, for which there exists a linear $PL(n, 1, q)$ code, equals p.*

Corollary 12. *For each n there exists a linear $PL(n, 1, 2n+1)$ code.*

The next theorem enumerates linear $PL(n, 1, q)$ codes. As a special case of this theorem we get the result of M o l n á r [13] discussed above.

Theorem 13. *The number of non-isomorphic linear $PL(n, 1, q)$ codes equals the number of non-isomorphic abelian groups G of order $2n+1$ with the property that for each $g \in G$ it holds $ord(g)|q$. In particular, the number of non-isomorphic $PL(n, 1, 2n+1)$ codes equals the number of non-isomorphic abelian groups of order $2n+1$.*

Finally, we design a linear time decoding algorithm for each linear $PL(n, 1; q_1, \ldots, q_n)$ code.

Let $\mathcal{C}$ be a $PL(n,1;q_1,\ldots,q_n)$ code. Then, by [3], $\mathcal{C}$ can be generated by the mapping $\phi : \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_n} \to G$, $\phi(\mathbf{e}_i) = g_i$, where $F = (g_1,\ldots,g_n)$ is a fundamental set of the abelian group $\dot{G}$, and

$$\phi\big((a_1,\ldots,a_n)\big) = a_1\phi(\mathbf{e}_1) + \cdots + a_n\phi(\mathbf{e}_n) = a_1g_1 + \cdots + a_ng_n. \tag{1}$$

As G is abelian, G can be written in a unique way as a direct product of cyclic groups $\mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_t}$ of prime power orders. Thus each element of G can be represented as a t-tuple $(b_1,\ldots,b_t), b_i \in \mathbb{Z}_{r_i}$. We list the elements of G in the lexicographic order. The value $r(b_1,\ldots,b_t)$ is the order of the element $(b_1,\ldots,b_t)$ in this lexicographic ordering. Thus,

$$r(b_1,\ldots,b_t) = a_n + 1 + \sum_{i=1}^{n-1} a_i \prod_{j=i+1}^{n} q_j. \tag{2}$$

Next, we define the function $f\colon \{0,\ldots,2n\} \to \{-n,-(n-1),\ldots,-1,0,1,\ldots,n-1,n\}$ as follows: Let $(b_1,\ldots,b_t) \in G$ with $r(b_1,\ldots,b_t) = k$. If $(b_1,\ldots,b_t) \in F$ and i is the index, $1 \le i \le n$, so that $\phi(\mathbf{e}_i) = (b_1,\ldots,b_t)$, then $f(k) = i$, otherwise, if $(b_1,\ldots,b_t)^{-1} \in F$ and i is the index, $1 \le i \le n$, so that $\phi(\mathbf{e}_i) = (b_1,\ldots,b_t)^{-1}$, then $f(k) = -i$.

Now we are ready to describe the algorithm. Supposed that we receive a word $V = (a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n)$. As the first step we calculate $\phi(V) = \phi(a_1\mathbf{e}_1 + \ldots \cdots + a_n\mathbf{e}_n) = g \in G$. If $g = 0$, then V is a codeword. Otherwise, we calculate the value $r(g)$, and subsequently the value $s = f\big(r(g)\big)$. If $s > 0$ then the codeword $W \in \mathcal{C}$ with the property $\rho_L(V,W) \le 1$ is the word $(a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n) - \mathbf{e}_s$, otherwise, if $s < 0$, then $W = (a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n) + \mathbf{e}_s$.

Clearly, the values of the function f are calculated only once and therefore the time needed for obtaining those values is not included in the complexity of the decoding algorithm. Thus, the above described algorithm is a linear time algorithm, as calculating $\phi\big((a_1,\ldots,a_n)\big)$, and $r(b_1,\ldots,b_t)$ requires a linear number of operations with respect to n.

4. Variations and generalizations on the theme of perfect Lee codes

We finish this paper with two generalizations of Lee codes.

4.1. Quasi-perfect Lee codes

Lee distance codes have many practical applications. They are used for phase modulated and multi-level quantized-pulse modulated channels, they have been applied in toroidal interconnection networks, and these codes have been shown to be the foundation of designing placement strategies to distribute commonly

shared resources like Input/Output devices over a toroidal network. On the other hand, the Golomb-Welch conjecture, and the result related to this conjecture, indicate that the perfect Lee codes $P(n, e, q)$ exist only for very few values of n, e, and q. Therefore, to be able to use Lee codes in practical application, the quasi-perfect Lee codes have been introduced in [2]. Here we confine ourselves to $n = 2$.

Let D be a Lee code over $\mathbb{Z}_q^2$. Then D is called a quasi perfect e-error correcting Lee code if

(a) $d_L(U, V) \geq 2e + 1$ for every two code words U, V in D;

(b) Every word in $\mathbb{Z}_q^2$ is at distance at most $e + 1$ from at least one code word.

Thus a quasi-perfect e-error correcting Lee code is a generalization of the perfect e-error correcting Lee code, where (b) is replaced by the condition that every word in $\mathbb{Z}_q^2$ is at distance at most e from exactly one code word.

Further, a code over $\mathbb{Z}_q^2$ generated by $(e, e+1)$, that is the code

$$\big\{(\alpha e, \alpha(e+1)), \alpha \in \mathbb{Z}\big\},$$

is denoted by D_e. It is very well known that there exists, for $q_e = 2e^2 + 2e + 1$, a perfect e-error correcting Lee. In [2] it is shown that for all the values of q between q_e and q_{e+1} there is a quasi-perfect e-error correcting Lee code. Namely, it is proved there:

Theorem 14.

(1) *For $q = 2e^2 + 2e + 1$, $e \geq 1$, D_e is a perfect e-error correcting Lee code.*

(2) *For $2e^2 + 2e + 2 \leq q \leq 2(e+1)^2 + 1, e \geq 1$, D_e is a quasi-perfect e-error correcting Lee code.*

(3) *For $2(e+1)^2 + 2 \leq q \leq 2(e+1)^2 + 2(e+1)$, $e \geq 2$, D_{e+1} is a quasi-perfect e-error correcting Lee code.*

Clearly, the existence of a quasi-perfect e-error correcting Lee code over $\mathbb{Z}_q^2$ implies the existence of such a (replication) code over $\mathbb{Z}_k \times \mathbb{Z}_m$ whenever $q|k$ and $q|m$. Thus, by Theorem 14, for each e, there are infinitely many values of q so that there is a quasi-perfect e-error correcting Lee code over $\mathbb{Z}_q^2$.

It was showed in [8], that there exists a fast decoding algorithm for quasi--perfect Lee codes D over $\mathbb{Z}_q^2$ given by Theorem 14. Regardless of q, the number of elementary operations used by the algorithm to decode a word is bounded from above by an absolute constant. Here by an elementary operation we mean an arithmetic operation or the operation of max of two numbers or the operation of taking the integer part of the number. The basic idea of the algorithm comes from representing the code in a 2-dimensional plane endowed with the Manhattan metric. Using geometric properties of the code, it was showed that to decode a word it is sufficient to calculate its distance to at most 4 code words.

4.2. Lee spheres of different radii

It was proved by several authors, see above, that there is no $PL(3,2)$ code. In [5] a stronger statement is proved. It is shown there:

Theorem 15. *There is no tiling of $\mathbb{R}^3$ with Lee spheres of radii at least two, even with different radii.*

Yet a stronger result is proved in [6], a sequel to [5], where it is shown that there is no tiling of R^3 with Lee spheres if radius of at least one sphere is greater than one. This led the authors of the two papers to suggest the following strengthening of the Golomb-Welch conjecture:

Conjecture 4. There does not exist a tiling of n-dimensional space, $n > 2$, with Lee spheres of radii greater than 0 such that the radius of at least one sphere is greater than 1.

Recently, Š p a c a p a n [23] extended Theorem 15 to the 4-dimensional case. Unlike [5], where a very elegant "picture says it all" proof for R^3 is provided, the proof for R^4 is computer aided. In [11], a unified proof of the result of Theorem 15 for $\mathbb{R}^n$, $3 \leq n \leq 5$ is provided.

REFERENCES

[1] ASTOLA, J.: *On perfect codes in the Lee metric,* Ann. Univ. Turku, Ser. A I **176** (1978), 56 p.

[2] AL-BDAIWI, B. F.—BOSE, B.: *Quasi-perfect Lee distance codes,* IEEE Tran. Inform. Theory **49** (2003), 1535–1539.

[3] AL-BDAIWI, B. F.—HORAK, P.—MILLAZO, L.: *Perfect 1-error correcting Lee codes,* Des. Codes Cryptogr. **52** (2009), 155–162.

[4] GOLOMB, S. W.—WELSH, L. R.: *Algebraic coding and the Lee metric,* in: Error Correct. Codes, Wiley, New York, 1968, pp. 175–189.

[5] GRAVIER, S.—MOLLARD, M.—PAYAN, CH.: *On the non-existence of 3-dimensional tiling in the Lee metric*, European J. Combin. **19** (1998), 567–572.

[6] GRAVIER, S.—MOLLARD, M.—PAYAN, CH.: *On the nonexistence of three--dimensional tiling in the Lee metric. II.* Discrete Math. **235** (2001), 151–157.

[7] HAJÓS, G.: *Über eifache und merfache Bedeckung des n-dimensional Raumes mit einem Würfelgitter,* Math. Zeit. **47** (1942), 427–467.

[8] HORAK, P.—AL-BDAIWI, B. F.: *Fast decoding quasi-perfect Lee distance codes,* Des. Codes Cryptogr. **40** (2006), 357–367.

[9] HORAK, P.: *Tiling in Lee metric,* European J. Combin. **30** (2009) 480–489.

[10] HORAK, P.: *On perfect Lee codes,* Discrete Math. **309** (2009), 5551–5561.

[11] HORAK, P.—AL-BDAIWI, B. F.: *The number of tilings of $\mathbb{R}^n$ by crosses,* submitted.

[12] KÁRTESZI, F.: *Szemléletes geometria.* Gondolat, Budapest, 1966.

[13] MOLNÁR, E.: *Sui mosaici dello spazio di dimensione n,* Atti Accad. Naz. Lincei, VIII. Ser., Rend., Cl. Sci. Fis. Mat. Nat. **51** (1971), 177–185.

[14] KELLER, O. H.: *Über die lückenlose Einfüllung des Raumes mit Würfeln,* J. Reine Angew. Math. **177** (1930), 231–248.
[15] LAGARIAS, J. F.—SHOR, P. W.: *Keller's cube-tiling conjecture is false in high dimensions,* Bull. Amer. Math. Soc. **27** (1992), 279–283.
[16] MACKEY, J.: *A cube tiling of dimension eight with no facesharing,* Discrete Comput. Geom. **28** (2002) 275–279.
[17] PERRON, O.: *Modulartige lückenlose Ausfüllungdes* $\mathbb{R}^n$ *mit kongruenten Würfeln I, II,* Math. Ann. **117** (1940), 415–447; **117** (1941), 609–658.
[18] POST, K. A.: *Nonexistence theorem on perfect Lee codes over large alphabets,* Inform. and Control **29** (1975), 369–380.
[19] STEIN, S. K.: *Factoring by subsets,* Pacific J. Math. **22** (1967), 523–541.
[20] STEIN, S. K.—SZABÓ, S.: *Algebra and Tilings: Homomorphisms in the Service of Geometry*. Carus Mathematical Monographs, Vol. 25 Math. Assoc. Amer., Washington, DC, 1994.
[21] SZABÓ, S.: *On mosaics consisting of multidimensional crosses,* Acta Math. Acad. Sci. Hung. **38** (1981), 191–203.
[22] SZABÓ, S.: *A star polyhedron that tiles but not as fundamental domain,* Colloq. Math. Soc. Janos Bolyai **48** (1985), 531–544.
[23] ŠPACAPAN, S.: *Nonexistence of face-to-face four-dimensional tilings in the Lee metric,* European. J. Combin. **28** (2007) 127–133.
[24] ULRICH, W.: *Non-binary error-correction codes,* Kibern. Sb. **7** (1963), 7–59; transl. from BEll System Tech. J. **36** (1957), 1341–1387.

Received April 17, 2010

IAS University of Washington
Tacoma, WA 98402–3100
U.S.A
E-mail: horak@u.washington.edu