NONEXISTENCE OF PERFECT 2-ERROR-CORRECTING LEE CODES IN CERTAIN DIMENSIONS

DONGRYUL KIM

ABSTRACT. The Golomb–Welch conjecture states that there are no perfect e-error-correcting codes in \( Z^n \) for \( n \geq 3 \) and \( e \geq 2 \). In this note, we prove the nonexistence of perfect 2-error-correcting codes for a certain class of \( n \), which is expected to be infinite. This result further substantiates the Golomb–Welch conjecture.

1. INTRODUCTION

For an integer \( q \geq 2 \), consider the space \( (Z/qZ)^n \) equipped with the Lee metric \( d \) given by

\[ d(x, y) = \sum_{i=1}^{n} \min\{|x_i - y_i|, q - |x_i - y_i|\}. \]

An \( e \)-error-correcting Lee code is a subset \( C \subseteq (Z/qZ)^n \) such that any two distinct elements of \( C \) have distance at least \( 2e + 1 \). An \( e \)-error-correcting Lee code \( C \) is further called a perfect \( e \)-error-correcting Lee code if for each \( x \in (Z/qZ)^n \), there exists a unique element \( c \in C \) such that \( d(x, c) \leq e \). A perfect \( e \)-error-correcting Lee code in \( (Z/qZ)^n \) is also called simply a \( \text{PL}(n, e, q) \)-code.

There is an equivalent description of error-correcting Lee codes that uses the language of tilings. Consider the Lee sphere

\[ S(n, e, q) = \{ x \in (Z/qZ)^n : d(x, 0) \leq e \} \]

of radius \( e \). An \( e \)-error-correcting Lee code is a subset \( C \subseteq (Z/qZ)^n \) such that for any \( x \neq y \) in \( C \), the two spheres \( x + S(n, e, q) \) and \( y + S(n, e, q) \) are disjoint. Thus it can be naturally identified with a translational packing of \( S(n, e, q) \) in \( (Z/qZ)^n \).

A perfect \( e \)-error-correcting Lee code then corresponds to a translational tiling of \( (Z/qZ)^n \) by \( S(n, e, q) \).

If \( q \geq 2e + 1 \), then the natural projection map \( Z^n \to (Z/qZ)^n \) restricts to a bijection from

\[ S(n, e) = \{ x \in Z^n : |x_1| + |x_2| + \cdots + |x_n| \leq e \} \]

to \( S(n, e, q) \). Any tiling of \( (Z/qZ)^n \) by \( S(n, e, q) \) will then pull back via the projection to a tiling of \( Z^n \) by \( S(n, e) \). Let us call a subset \( C \subseteq Z^n \) a perfect \( e \)-error-correcting Lee code in \( Z^n \), or simply a \( \text{PL}(n, e) \)-code, if the translates of \( S(n, e) \) centered at vectors of \( C \) form a tiling of \( Z^n \). Then a \( \text{PL}(n, e, q) \)-code induces a \( \text{PL}(n, e) \)-code that is a disjoint union of cosets of \( qZ^n \subset Z^n \). Conversely, any such \( \text{PL}(n, e) \)-code clearly comes from a \( \text{PL}(n, e, q) \)-code. We restate this in the following proposition.

1
Proposition 1.1. For $q \geq 2e+1$, there exists a natural bijection between $PL(n,e,q)$-codes and $PL(n,e)$-codes that is a union of cosets of $q\mathbb{Z}^n \subset \mathbb{Z}^n$, given by taking the image or the inverse image with respect to the projection map $\mathbb{Z}^n \to (\mathbb{Z}/q\mathbb{Z})^n$.

Thus to know all about $PL(n,e,q)$-codes, it suffices to study $PL(n,e)$-codes.

Error-correcting codes in the Lee metric have been first investigated by Golomb and Welch [2]. In the paper, they explicitly construct $PL(1,e,2e+1)$-codes, $PL(2,e,2e^2+2e+1)$-codes, and $PL(n,1,2n+1)$-codes. On the other hand, they conjecture the nonexistence of perfect Lee codes for other $n$ and $e$.

Conjecture 1.2. For $n \geq 3$ and $e \geq 2$, there exist no $PL(n,e)$-codes.

The case when $e$ is “large” compared to $n$ is studied extensively in the literature. Golomb and Welch [2] proved using a compactness argument that for each $n \geq 3$, there exists a sufficiently large $\rho_n$ such that there exist no $PL(n,e)$-codes for each $e \geq \rho_n$. An effective form of this theorem, that $PL(n,e,q)$-codes do not exist for $3 \leq n \leq 5, e \geq n-1, q \geq 2e+1$ and $n \geq 6, e \geq \frac{\sqrt{7}}{2}n - \frac{3}{4}\sqrt{2} - \frac{1}{2}, q \geq 2e+1$, was subsequently shown by Post [8]. Lepistö [7] improved the bound asymptotically and obtained the following theorem.

Theorem 1.3. For any $n, e, q$ satisfying $n < (e+2)^2/2.1$ and $e \geq 285$ and $q \geq 2e+1$, there exist no $PL(n,e,q)$-codes.

Another direction of approach is to focus on small $n$. Gravier, Mollard, and Payan [3] showed the nonexistence of $PL(3,e)$-codes by analyzing possible local configurations. Later a computer-based proof of the nonexistence of $PL(4,e)$-codes was given by Špacapan [9], and Horak [4] further extended the theorem to prove nonexistence of $PL(n,e)$-codes for $3 \leq n \leq 5$ and $e \geq 2$. In recent years, the case $e = 2$ has been investigated for reasonably small $n$. For $n = 5, 6$, Horak [4] showed that $PL(5,2)$-codes and $PL(6,2)$-codes do not exist, and Horak and Grosˇek [6] further showed using a computer that for $7 \leq n \leq 12$ there are no linear $PL(n,2)$-codes, i.e., $PL(n,2)$-codes that is a lattice in $\mathbb{Z}^n$.

In this note, we continue along this line and provide a number theoretic condition under which $PL(n,2)$-codes do not exist. In particular, we prove the following theorem.

Theorem 1.4. Suppose $p = 2n^2 + 2n + 1$ is prime. Let $a$ be the smallest positive integer for which $p \mid 4^a + 4n + 2$ and $b$ be the smallest positive integer for which $p \mid 4^b - 1$. (For convenience let $a = \infty$ if there is no $a$ with $p \mid 4^a + 4n + 2$.) If the equation $a(x+1) + by = n$ has no nonnegative integer solutions, then $PL(n,2)$-codes do not exist. For instance, there are no $PL(n,2)$-codes for $n = 5, 7, 9, 12, 14, 17, \ldots$.

To illustrate the strength of this theorem, we provide numerical data concerning the number of $n$ to which the theorem can be applied. As in Table I, if $2n^2 + 2n + 1$ is indeed prime, in most cases the second condition about the equation having no nonnegative solutions is also satisfied. It is reasonable to expect that there are infinitely many $n$ such that $2n^2 + 2n + 1$ is prime, although it is far from being proved. This is a special case of the Bunyakovsky conjecture, and moreover the heuristics of the Bateman–Horn conjecture [1] expects there to be asymptotically $C x/\log x$ such $n \leq x$ for some absolute constant $C$.

The condition $2n^2 + 2n + 1 = |S(n,2)|$ being prime is included in order to use a result that allows us to translate the tiling problem to a purely algebraic problem. The following theorem is proved in [10].
NONEXISTENCE OF PERFECT 2-ERROR-CORRECTING LEE CODES IN CERTAIN DIMENSIONS

| $x$ | $\#$ of $n \leq x$ with $2n^2 + 2n + 1$ prime | $\#$ of $n \leq x$ to which Theorem 1.4 can be applied |
|-----|---------------------------------|----------------------------------|
| $10^1$ | 6 | 4 |
| $10^2$ | 36 | 34 |
| $10^3$ | 225 | 222 |
| $10^4$ | 1645 | 1642 |
| $10^5$ | 12706 | 12702 |

Table 1. The number of $n$ to which Theorem 1.4 can be applied

**Theorem 1.5.** Let $T \subset \mathbb{Z}^n$ be a finite subset of prime size $p$, and suppose that $T - T \subset \mathbb{Z}^n$ generates $\mathbb{Z}^n$ as an abelian group. Then there exists a tiling of $\mathbb{Z}^n$ by translates of $T$ if and only if there exists a homomorphism $\phi : \mathbb{Z}^n \rightarrow \mathbb{Z}/p\mathbb{Z}$ that restricts to a bijection from $T$ to $\mathbb{Z}/p\mathbb{Z}$.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

2. Proof of Theorem

In this section, we let $2n^2 + 2n + 1 = p$ be a prime. Since $\mathbb{Z}^n$ is a free abelian group generated by the unit vectors $e_1, \ldots, e_n$, a homomorphism $\phi : \mathbb{Z}^n \rightarrow \mathbb{Z}/p\mathbb{Z}$ is determined uniquely by the values $x_i = \phi(e_i)$ for $1 \leq i \leq n$. Then $\phi$ restricting to a bijection from $S(n, 2)$ to $\mathbb{Z}/p\mathbb{Z}$ is equivalent to the sets

$$\{0\}, \{\pm x_i\}_{1 \leq i \leq n}, \{\pm 2x_i\}_{1 \leq i \leq n}, \{\pm x_i \pm x_j\}_{1 \leq i < j \leq n}$$

forming a partition of $\mathbb{Z}/p\mathbb{Z}$.

Suppose that such $x_1, \ldots, x_n \in \mathbb{Z}/p\mathbb{Z}$ exist. The sum of $2k$-th powers of all the elements is

$$\sum_{i=1}^n (x_i^{2k} + (-x_i)^{2k} + (2x_i)^{2k} + (-2x_i)^{2k})$$

$$+ \sum_{1 \leq i < j \leq n} ((x_i + x_j)^{2k} + (x_i - x_j)^{2k} + (-x_i + x_j)^{2k} + (-x_i - x_j)^{2k})$$

$$= 2(4^k + 1) \sum_{i=1}^n x_i^{2k} + \sum_{1 \leq i < j \leq n} 4 \sum_{t=0}^{k} \binom{2k}{2t} x_i^{2t} x_j^{2(k-t)}$$

$$= (2^{2k+1} + 4(n-1) + 2) \sum_{i=1}^n x_i^{2k} + 4 \sum_{t=1}^{k-1} \sum_{1 \leq i < j \leq n} \binom{2k}{2t} x_i^{2t} x_j^{2(k-t)}$$

$$= (2^{2k+1} + 4n - 2) S_{2k} + 2 \sum_{t=1}^{k-1} \binom{2k}{2t} (S_{2t} S_{2(k-t)} - S_{2k})$$

$$= (2^{2k} + 4n + 2) S_{2k} + 2 \sum_{t=1}^{k-1} \binom{2k}{2t} S_{2t} S_{2(k-t)}$$
where we denote \( S_i = \sum_{t=1}^{n} x_t^i \). On the other hand, this is the sum of the \( 2k \)-th powers of all elements of \( \mathbb{Z}/p\mathbb{Z} \). Thus

\[
(4k + 4n + 2)S_{2k} + 2 \sum_{t=1}^{k-1} \left(\frac{2k}{2t}\right) S_{2t}S_{2(k-t)} = \begin{cases} 
0 & \text{if } p - 1 \nmid 2k, \\
-1 & \text{if } p - 1 \mid 2k.
\end{cases}
\]

Let \( a \) and \( b \) be the least positive integers satisfying \( p \mid 4^a + 4n + 2 \) and \( p \mid 4^b - 1 \). Consider the set
\[ X = \{ax + by : x \geq 1, y \geq 0\} \]
Note that the set \( X \) is closed under addition. We now claim the following.

**Lemma 2.1.** If \( 1 \leq k < (p - 1)/2 \) is not in \( X \), then \( S_{2k} = 0 \).

**Proof.** We prove by induction on \( k \). Suppose \( S_{2k} = 0 \) for all \( k \leq k_0 - 1 \) that is not in \( X \). We now show that \( S_{2k_0} = 0 \) if \( k_0 \notin X \). Assume \( k_0 \) is not in \( X \). Since any \( k \) for which \( p \mid 4^k + 4n + 2 \) is of the form \( a + by \) and thus in \( X \), we see that \( p \nmid 4^k + 4n + 2 \).

Moreover, because \( k_0 \notin X \) and \( X \) is closed under addition, for each \( t \) either \( t \) or \( k_0 - t \) is not in \( X \). From Equation (1) and the induction hypothesis it follows that
\[
0 = (4^{k_0} + 4n + 2)S_{2k_0} + 2 \sum_{t=1}^{k_0-1} \left(\frac{2k_0}{2t}\right) S_{2t}S_{2(k_0-1)} = (4^{k_0} + 4n + 2)S_{2k_0}
\]
in \( \mathbb{Z}/p\mathbb{Z} \). Because \( 4^k + 4n + 2 \neq 0 \), we immediately obtain \( S_{2k_0} = 0 \). \( \Box \)

Let
\[
e_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1}^2 x_{i_2}^2 \cdots x_{i_k}^2
\]
be the elementary symmetric polynomials with respect to \( x_1^2, x_2^2, \ldots, x_n^2 \). Using a similar argument, we prove the following lemma.

**Lemma 2.2.** If \( 1 \leq k \leq n \) is not in \( X \), then \( e_k = 0 \).

**Proof.** We again prove by induction on \( k \). Suppose \( e_k = 0 \) for all \( k \leq k_0 - 1 \) not in \( X \), and also assume \( k_0 \notin X \). The Newton identities on \( x_1^2, \ldots, x_n^2 \) can be written as
\[ k_0 e_{k_0} = e_{k_0-1}S_2 - e_{k_0-2}S_4 + \cdots + (-1)^{k_0-2} e_1S_{2(k_0-1)} + (-1)^{k_0-1}S_{2k_0}. \]

Because \( X \) is closed under addition and \( k_0 \notin X \), for each \( 0 < t < k_0 \) either \( t \notin X \) or \( k_0 - t \notin X \). From Lemma 2.1 and the inductive hypothesis, it follows that either \( e_t = 0 \) or \( S_{2(k_0-t)} = 0 \). Therefore
\[
k_0 e_{k_0} = e_{k_0-1}S_2 - e_{k_0-2}S_4 + \cdots + (-1)^{k_0-2} e_1S_{2(k_0-1)} + (-1)^{k_0-1}S_{2k_0}
\]
and thus \( e_{k_0} = 0 \) since \( k_0 \neq 0 \). \( \Box \)

We now note that \( e_n = x_1^2 \cdots x_n^2 \). Since none of \( x_1, \ldots, x_n \) is 0, the square of their product \( e_n \) is also not 0, and hence \( n \in X \). Thus by Theorem 1.3, PL(\( n, 2 \))-codes exist only if \( n \in X \). This finishes the proof of Theorem 1.3.

3. Acknowledgments

The author would like to express gratitude to Peter Horak, who introduced the author to the problem and provided helpful comments.
References

1. Paul T. Bateman and Roger A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. 16 (1962), 363–367. MR 0148632

2. Solomon W. Golomb and Lloyd R. Welch, *Perfect codes in the Lee metric and the packing of polyominos*, SIAM J. Appl. Math. 18 (1970), 302–317. MR 0256766 (41 #1422)

3. Sylvain Gravier, Michel Mollard, and Charles Payan, *On the non-existence of 3-dimensional tiling in the Lee metric*, European J. Combin. 19 (1998), no. 5, 567–572. MR 1637720

4. P. Horak, *On perfect Lee codes*, Discrete Math. 309 (2009), no. 18, 5551–5561. MR 2567958

5. ______, *Tilings in Lee metric*, European J. Combin. 30 (2009), no. 2, 480–489. MR 2489281

6. Peter Horak and Otokar Grošek, *A new approach towards the Golomb-Welch conjecture*, European J. Combin. 38 (2014), 12–22. MR 3149676

7. Timo Lepistö, *A modification of the Elias-bound and nonexistence theorems for perfect codes in the Lee-metric*, Inform. and Control 49 (1981), no. 2, 109–124. MR 640192

8. K. A. Post, *Nonexistence theorems on perfect Lee codes over large alphabets*, Information and Control 29 (1975), no. 4, 369–380. MR 0446719 (56 #5043)

9. Simon Špacapan, *Nonexistence of face-to-face four-dimensional tilings in the Lee metric*, European J. Combin. 28 (2007), no. 1, 127–131. MR 2261809

10. Mario Szegedy, *Algorithms to tile the infinite grid with finite clusters*, Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on, IEEE, 1998, pp. 137–145.

E-mail address: dkim04@college.harvard.edu

Harvard College, Cambridge, MA, 02138