European Journal of Combinatorics 63 (2017) 1–5

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions

Dongryul Kim

Harvard College, Cambridge, MA 02138, USA

ARTICLE INFO

Article history:
Received 4 September 2016
Accepted 30 January 2017
Available online 24 February 2017

ABSTRACT

The Golomb–Welch conjecture states that there are no perfect e-error-correcting codes in $\mathbb{Z}^n$ 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 $(\mathbb{Z}/q\mathbb{Z})^n$ equipped with the Lee metric d given by

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

An *e-error-correcting Lee code* is a subset $C \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ 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 $x \in (\mathbb{Z}/q\mathbb{Z})^n$, there exists a unique element $c \in C$ such that $d(x, c) \leq e$. A perfect e-error-correcting Lee code in $(\mathbb{Z}/q\mathbb{Z})^n$ is also called simply a $PL(n, e, q)$-code.

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

$$S(n, e, q) = \{\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n : d(\mathbf{x}, \mathbf{0}) \leq e\}$$

of radius e. An e-error-correcting Lee code is a subset $C \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ such that for any $\mathbf{x} \neq \mathbf{y}$ in C, the two spheres $\mathbf{x} + S(n, e, q)$ and $\mathbf{y} + S(n, e, q)$ are disjoint. Thus it can be naturally identified with a translational packing of $S(n, e, q)$ in $(\mathbb{Z}/q\mathbb{Z})^n$. A perfect e-error-correcting Lee code then corresponds to a translational tiling of $(\mathbb{Z}/q\mathbb{Z})^n$ by $S(n, e, q)$.

E-mail address: kdr0515@gmail.com.

http://dx.doi.org/10.1016/j.ejc.2017.01.007
0195-6698/

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

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

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

Proposition 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 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 ρ_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 $n \geq 6$, $e \geq \frac{\sqrt{2}}{2}n - \frac{3}{4}\sqrt{2} - \frac{1}{2}$, $q \geq 2e+1$, was subsequently shown by Post [8]. Lepistö [7] improved the bound asymptotically and obtained the following theorem.

Theorem 3. *For any n, e, q satisfying $n \geq (e+2)^2/2.1$ 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 [5] 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 Grosěk [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 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 1, 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 $Cx/\log x$ 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].