On the nonexistence of linear perfect Lee codes

Tao Zhang
joint work with Yue Zhou

Guangzhou University

July 5, 2018

Lee codes

Definition

For $u = (u_1, \cdots, u_n), v = (v_1, \cdots, v_n) \in \mathbb{Z}^n$, their Lee distance is defined by

$$d_L(u, v) = \sum_{i=1}^{n} |u_i - v_i|.$$

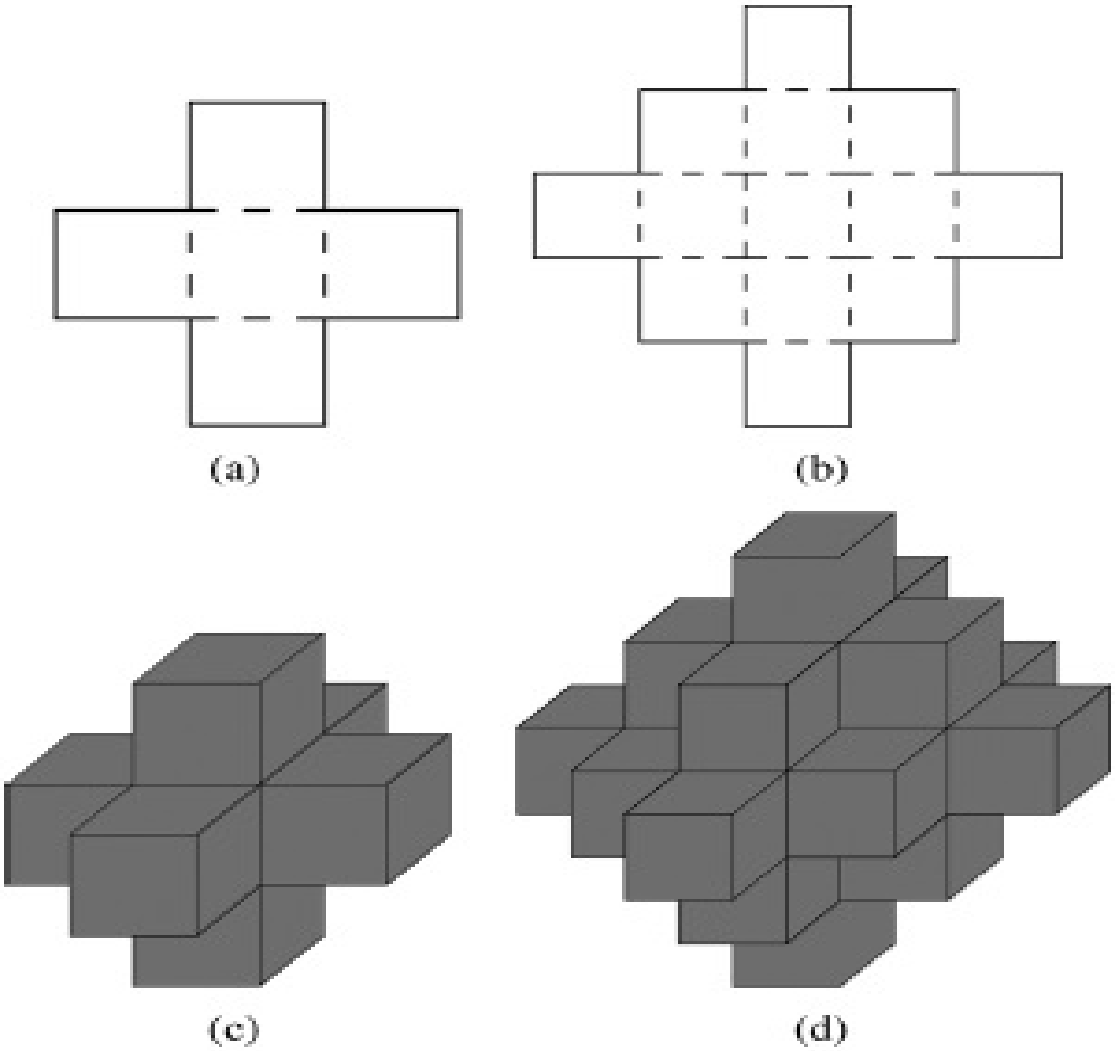
A Lee code C is a subset of $\mathbb{Z}^n$ endowed by the Lee distance.

- If C has further the structure of an additive group, then C is called linear Lee code.
- C is r-error-correcting: for $x \neq y \in C$, $d_L(x, y) \geq 2r + 1$.
- An r-error-correcting Lee code C is called perfect if for each $x \in \mathbb{Z}^n$, there exists a unique $c \in C$ such that $d_L(x, c) \leq r$; denoted by $PL(n, r)$-code.

Perfect Lee codes and tilings

- For $V \subset \mathbb{Z}^n$ and $x \in \mathbb{Z}^n$, $V + x = \{v + x : v \in V\}$.
- A collection $\mathfrak{T} = \{V + l : \ l \in L\}$, $L \subseteq \mathbb{Z}^n$ of copies of V constitutes a tiling of $\mathbb{Z}^n$ by V if $\mathfrak{T}$ forms a partition of $\mathbb{Z}^n$.
- If L further forms a lattice, then $\mathfrak{T}$ is called a *lattice tiling* of $\mathbb{Z}^n$.
- Let $S(n, r) = \{x \in \mathbb{Z}^n : d_L(x, 0) = |x_1| + \cdots + |x_n| \leq r\}$.
- C is a $PL(n, r)$-code if and only if $\{S(n, r) + c : c \in C\}$ constitutes a tiling of $\mathbb{Z}^n$ by $S(n, r)$.
- C is a linear $PL(n, r)$-code if and only if $\{S(n, r) + c : c \in C\}$ forms a lattice tiling of $\mathbb{Z}^n$.

Lee spheres



Golomb-Welch conjecture

In 1968, Golomb and Welch constructed $PL(1, r)$-codes, $PL(2, r)$-codes and $PL(n, 1)$-codes explicitly. In the same paper, they also proposed the following conjecture.

Conjecture (Golomb-Welch conjecture)

For $n \geq 3$ and $r \geq 2$, there does not exist $PL(n, r)$-code.

- In 1970, Golomb and Welch proved the nonexistence of $PL(n, r)$-codes for given n and $r \geq r_n$, where r_n has not been specified.
- Improvements by Post (1975), Lepisto (1981), Horak, Kim (2017).
- Roughly speacking, for given n, if $r \geq \sqrt{2n}$ then there is no $PL(n, r)$.

Golomb-Welch conjecture

A special case of the Golomb-Welch conjecture, the nonexistence of linear $PL(n, r)$-codes, can be converted into an algebraic combinatorics problem.

Theorem (Horak, AlBdaiwi 2012)

Let $S \subseteq \mathbb{Z}^n$ such that $|S| = m$. There is a lattice tiling of $\mathbb{Z}^n$ by translates of S if and only if there are both an abelian group G of order m and a homomorphism $\phi : \mathbb{Z}^n \mapsto G$ such that the restriction of ϕ to S is a bijection.

Corollary

There is a linear $PL(n, r)$-code if and only if there are both an abelian group G and a homomorphism $\phi : \mathbb{Z}^n \mapsto G$ such that the restriction of ϕ to $S(n, r)$ is a bijection.

Example

For $n = 2$ and $r = 2$, $G = C_{13}$. Note that each homomorphism $\phi : \mathbb{Z}^n \mapsto G$ is determined by the values of $\phi(e_i)$ for $i = 1, \cdots, n$, where $\{e_i : i = 1, \cdots, n\}$ is the standard basis of $\mathbb{Z}^n$. Here we may take $\phi(e_1) = 1$ and $\phi(e_2) = 5$.

5	6	7	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9	10	11	12	0	1	2	3	4
8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11	12
3	4	5	6	7	8	9	10	11	12	0	1	2	3	4	5	6	7
11	12	0	1	2	3	4	5	6	7	8	9	10	11	12	0	1	2
6	7	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	11	12	0	1	2	3	4	5
9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11	12	0
4	5	6	7	8	9	10	11	12	0	1	2	3	4	5	6	7	8
12	0	1	2	3	4	5	6	7	8	9	10	11	12	0	1	2	3
7	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11

Linear Perfect Lee codes and degree-diameter problem

- In a graph Γ, the *distance* $d(u, v)$ from a vertex u to another vertex v is the length of a shortest u-v path in Γ.
- The largest distance between two vertices in Γ is the *diameter* of Γ.
- Let $\Gamma = (V, E)$ be a graph of maximum degree d and diameter k. According to the famous Moore bound, Γ has at most $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$ vertices. When the order of V equals $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$, the graph Γ is called a *Moore graph*.

Problem

Given positive integers d and k, find the largest possible number $N(d, k)$ of vertices in a graph with maximum degree d and diameter k.

Linear Perfect Lee codes and degree-diameter problem

- Let G be a multiplicative group with the identity element e and $S \subseteq G$ such that $S^{-1} = S$ and $e \notin S$. Here $S^{-1} = \{s^{-1} : s \in S\}$. The Cayley graph $\Gamma(G, S)$ has a vertex set G, and two distinct vertices g, h are adjacent if and only if $g^{-1}h \in S$.
- The diameter of a Cayley graph $\Gamma(G, S)$ is k if and only if k is the smallest integer such that all elements in G appear in $\{\prod_{i=1}^{k} s_i : s_i \in S \cup \{e\}\}$.
- **There exists a linear $PL(n, r)$-code if and only if there exists an abelian Cayley graph with degree $2r$, diameter n and vertices $|S(n, r)|$.**

Two algebraic approaches

As summarized in a survey by Horak and Kim, it appears that for a small radius r and a large dimension n, the nonexistence of a $PL(n, r)$-code is difficult.
Two different approaches.

- A polynomial method for $r = 2$ by Kim.
- An algebraic number theory method for $r = 2, 3$.

Kim's method

Theorem

Suppose that $2n^2 + 2n + 1 = mv$ *where* v *is a prime and* $v > 2n + 1$. *Define* $a = \min\{a \in \mathbb{Z}^+ : v \mid 4^a + 4n + 2\}$ *and* b *is the order of* 4 *modulo* v. *(If there is no* a *with* $v \mid 4^a + 4n + 2$, *then we let* $a = \infty$.*) Assume that there is a linear* $PL(n, 2)$*-code. Then there exists at least one* $\ell \in \{0, 1, \ldots, \lfloor \frac{m}{4} \rfloor\}$ *such that the equation*

$$a(x + 1) + by = n - \ell$$

has nonnegative integer solutions.

Kim's method–main idea

- Let the abelian group G be additive and let 0 be its identity element.
- Then there exists $S = \{s_i : i = 1, \ldots, n\} \subseteq G$ such that

$$\{0\}, \{\pm s_i : i = 1, \ldots, n\}, \{2s_i : i = 1, \ldots, n\}, \{\pm s_i \pm s_j : 1 \leq i < j \leq n\}$$

form a partition of G.

- Let H be a subgroup of G of index v. Let $\rho : G \to G/H$ be the canonical homomorphism and $x_i = \rho(s_i)$. Then the multisets

$$\{0\}, \{* \ \pm x_i : i = 1, \ldots, n *\}, \{* \ \pm 2x_i : i = 1, \ldots, n *\},$$
$$\{* \ \pm x_i \pm x_j : 1 \leq i < j \leq n *\}$$

form a partition of mG/H.

Kim's method–main idea

- Let k be an integer
- $$\sum_{i=1}^{n}\left((x_i^{2k}+(-x_i)^{2k}+(2x_i)^{2k}+(-2x_i)^{2k}\right)$$
$$+\sum_{1\le i<j\le n}\left((x_i+x_j)^{2k}+(x_i-x_j)^{2k}+(-x_i+x_j)^{2k}+(-x_i-x_j)^{2k}\right)$$
$$=(4^k+4n+2)\overline{S}_{2k}+2\sum_{t=1}^{k-1}\binom{2k}{2t}\overline{S}_{2t}\overline{S}_{2(k-t)}$$
where $\overline{S}_t:=\sum_{i=1}^{n}x_i^t$.
- $$(4^k+4n+2)\overline{S}_{2k}+2\sum_{t=1}^{k-1}\binom{2k}{2t}\overline{S}_{2t}\overline{S}_{2(k-t)}=\begin{cases}0, & v-1\nmid 2k,\\ -m, & v-1\mid 2k.\end{cases}$$

Kim's method–main idea

- Let a and b be the least positive integers satisfying $v \mid 4^a + 4n + 2$ and $p \mid 4^b - 1$. Define

$$X = \{ax + by : x \geq 1, y \geq 0\}.$$

- **Claim 1:** If $1 \leq k < \frac{v-1}{2}$ is not in X, then $\overline{S}_{2k} = 0$.
  - Suppose that $\overline{S}_{2k} = 0$ for each $k \leq k_0 - 1$ that is not in X.
  - Assume that $k_0 \notin X$.
  - As X is closed under addition, for any t, at least one of t and $k_0 - t$ is not in X.
  - For any integer k, if $v \mid 4^k + 4n + 2$, then k must be of the form $a + by$ whence $k \in X$. This implies that $v \nmid 4^{k_0} + 4n + 2$.
  - $0 = (4^{k_0} + 4n + 2)\overline{S}_{2k_0} + 2\sum_{t=1}^{k_0-1} \binom{2k_0}{2t} \overline{S}_{2t}\overline{S}_{2(k_0-t)} = (4^{k_0} + 4n + 2)\overline{S}_{2k_0}$.
  - Thus $\overline{S}_{2k_0} = 0$.

Kim's method–main idea

- Let e_k be the elementary symmetric polynomials with respect to x_1^2, $x_2^2, \cdots, x_n^2$.
- **Claim 2**: If $1 \leq k \leq n < \frac{v-1}{2}$ is not in X, then $e_k = 0$.
  - Suppose that $e_k = 0$ for each $k \leq k_0 - 1$ not in X and $k_0 \notin X$.
  - As X is closed under addition, for each $0 < t < k_0$, at least one of t and $k_0 - t$ is not in X.
  - $e_t = 0$ or $S_{2(k_0-t)} = 0$.
  - Together with Newton identities on $x_1^2, \ldots, x_n^2$, we have $k_0 e_{k_0} = e_{k_0-1}S_2 + \cdots + (-1)^{i+1} e_{k_0-i} S_{2i} + \cdots + (-1)^{k_0-1} S_{2k_0} = (-1)^{k_0-1} S_{2k_0} = 0$.
  - $e_{k_0} = 0$.
- 0 appears at most $\lfloor \frac{m}{4} \rfloor$ times in x_i's.
- Suppose that 0 appears ℓ times in $\overline{S}$. Then e_{n-l} is the production of those nonzero x_i^2's, whence $e_{n-l} \neq 0$.
- $n - l$ is in X.

Group ring

- Let G be a finite group.
- The group ring $\mathbb{Z}[G]$ is a free abelian group with a basis $\{g \mid g \in G\}$.
- For any set A whose elements belong to G (A may be a multiset), we identify A with the group ring element $\sum_{g\in G} a_g g$, where a_g is the multiplicity of g appearing in A.
- Given any $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$, we define $A^{(t)} = \sum_{g\in G} a_g g^t$.
- Addition and multiplication:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g,$$

$$\sum_{g\in G} a_g g \sum_{g\in G} b_g g = \sum_{g\in G} (\sum_{h\in G} a_h b_{h^{-1}g}) g.$$

A group ring equation $r = 2$

Lemma

Let $n \geq 2$, then there exists a linear $PL(n, 2)$-code if and only if there exist a finite abelian group G of order $2n^2 + 2n + 1$ and $T \subseteq G$ viewed as an element in $\mathbb{Z}[G]$ satisfying

1. $1 \in T$,
2. $T = T^{(-1)}$,
3. $T^2 = 2G - T^{(2)} + 2n$.

A group ring equation $r = 2$

Proof.

- There exists a linear $PL(n, 2)$-code if and only if there are both an abelian group G (written multiplicatively) of order $2n^2 + 2n + 1$ and a homomorphism $\phi : \mathbb{Z}^n \mapsto G$ such that the restriction of ϕ to $S(n, 2)$ is a bijection.
- Each homomorphism $\phi : \mathbb{Z}^n \mapsto G$ is determined by the values of $\phi(e_i)$ for $i = 1, \cdots, n$, where $\{e_i : i = 1, \cdots, n\}$ is the standard basis of $\mathbb{Z}^n$.
- There exists a linear $PL(n, 2)$-code if and only if there exists an n-subset $\{a_1, a_2, \ldots, a_n\} \subseteq G$ such that

$$G = 1 + \sum_{i=1}^{n}(a_i + a_i^{-1} + a_i^2 + a_i^{-2}) + \sum_{1 \le i < j \le n}(a_i + a_i^{-1})(a_j + a_j^{-1}).$$

- Let $T = 1 + \sum_{i=1}^{n}(a_i + a_i^{-1})$.

Main results $r = 2$

- Let H be a subgroup of G with order m and $\rho : G \to G/H$ be the canonical homomorphism.
- For $S = \sum_{g \in G} s_g g$, we define $\overline{S} = \rho(S) = \sum_{g \in G} s_g \rho(g)$.
- Thus

$$\overline{T} = \sum_{\bar{g} \in G/H} a_{\bar{g}} \bar{g} \in \mathbb{Z}[G/H],$$

where $a_{\bar{g}} = \sum_{\{g : \rho(g) = \bar{g}\}} a_g$.

Then previous conditions become:

1. $\overline{T} = \overline{T}^{(-1)}$,
2. $\overline{T}^2 = 2mG/H - \overline{T}^{(2)} + 2n$.

Main results $r = 2$

For small $|G/H|$, we can prove some results.

Theorem

Suppose that $8n+1$ is not a square in $\mathbb{Z}$. Assume that one collection of the following conditions holds

1. $5 \mid 2n^2+2n+1$, $8n-3 \neq 5k^2$ *for any* $k \in \mathbb{Z}$;
2. $13 \mid 2n^2+2n+1$, $8n-3 \neq 13k^2$ *for any* $k \in \mathbb{Z}$;
3. $17 \mid 2n^2+2n+1$.

Then there are no linear perfect Lee codes of radius 2 for dimension n.

Main results $r = 2$ (Idea)

Case I: $|G/H| = 5$.

- $\overline{T} \in \mathbb{Z}[C_5]$
- $\overline{T}^2 \equiv -\overline{T}^{(2)} + 2n \pmod{G/H}$,
- $(\overline{T}^{(2)})^2 \equiv -\overline{T}^{(4)} + 2n = -\overline{T} + 2n \pmod{G/H}$,
- $\overline{T}^4 - 4n\overline{T}^2 + \overline{T} + 4n^2 - 2n \equiv 0 \pmod{G/H}$.
- $\overline{T}^4 - 4n\overline{T}^2 + \overline{T} + 4n^2 - 2n = (\overline{T}^2 - \overline{T} - 2n + 1)(\overline{T}^2 + \overline{T} - 2n)$.
- Let $S = a + bG \in \mathbb{Z}[G]$ with $|G| = v$. Assume that positive integers v and m satisfy $a + vb = 2n + 1$ and $mv = 2n^2 + 2n + 1$, and S satisfies

$$S^2 = 2mG - S + 2n.$$

Then $8n + 1$ is a square in $\mathbb{Z}$.

Main results $r = 2$ (Idea)

- $\overline{T}^2 - \overline{T} - 2n + 1 \equiv 0 \pmod{G/H}$.
- Take a non-principle character $\chi \in \widehat{G/H}$, then $\chi(\overline{T}) \in \mathbb{Z}[\zeta_5]$ is such that
$$\chi(\overline{T})^2 - \chi(\overline{T}) - 2n + 1 = 0.$$
- $8n - 3$ is a square in $\mathbb{Z}[\zeta_5]$.

Main results $r = 2$

Theorem

Let n be a positive integer and p be a prime divisor of $2n$. Let G be an abelian group of order $2n^2 + 2n + 1$. Suppose that H is one of its subgroup of index v. Define $m = \frac{2n^2+2n+1}{v}$, $m_1 := \min\{i : i \in \mathbb{Z}_{\geq 0}, i \equiv m \pmod{p}\}$ and $m_2 := \min\{i : i \in \mathbb{Z}_{\geq 0}, i \equiv 2m \pmod{p}\}$. Let f denote the order of p modulo v, $l = \min\{i : p^i \equiv \pm 1 \pmod{v}\}$ and $d = (v-1)/f$. Define

$$\lambda = \max\{r : r \mid (p^l - 1), r \mid (2^i - p^j) \text{ for } 2^i \equiv p^j \pmod{v}\}.$$

Assume that

- *v is a prime,*
- *$2n + 1$ is smaller than $m_1 v$ and $m_2 v$,*
- *σ_2 and σ_p generates the Galois group $Gal(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ where ζ_v is a primitive v-th root of unity.*
- *$\lambda \neq 1$ or v.*

Then there are no linear perfect Lee codes of radius 2 for dimension n.

Main results $r = 2$

Remark

By applying above results, there are no $PL(n, 2)$ *for* $3 \leq n \leq 100$ *except* $n = 16, 21, 36, 55, 64, 66, 78, 92$.

A group ring equation $r = 3$

Lemma

Let $n \geq 3$, then there exists a linear $PL(n, 3)$-code if and only if there exist a finite abelian group G of order $1 + 6n^2 + \frac{4n(n-1)(n-2)}{3}$ and $T \subseteq G$ viewed as an element in $\mathbb{Z}[G]$ satisfying

1. $1 \in T$,
2. $T = T^{(-1)}$,
3. $T^3 = 6G - 3T^{(2)}T - 2T^{(3)} + 6nT$.

Main results $r = 3$

For small $|G/H|$, we can prove some results.

Theorem

Assume that $n \equiv 1, 5 \pmod 7$. *If* $24n + 1$ *is not a square or* $84 \nmid (24n+1)^2 \pm 6\sqrt{24n+1} + 29$, *then there are no linear perfect Lee codes of radius* 3 *for dimension* n.

Remark

When $n \equiv 5 \pmod 7$, $24n + 1$ *can never be a square.*

Conclusion

It appears that our approach can be further applied on the existence of $PL(n, r)$ for $r > 3$. However, for $r = 4, 5, \cdots$, the group ring equations become more complicated and contain much more terms. For instance, for $r = 4$, there are $T^{(4)}$, $T^{(3)}T$, $T^{(2)}T^{(2)}, \cdots$ in the equations.

THANK YOU