An exploration of perfect lee codes

Alex Valentino

May 2, 2024

1 But what is a Lee code?

In 1958, one C.Y. Lee from bell labs published *Some properties of nonbinary error-correcting codes* [2], in which Lee outlines a new kind of metric on which one can define codes, the Lee metric:

Definition 1. *Given two words $u, v \in \mathbb{Z}_q^n$, the Lee distance (or q-Lee distance) is given as*

$$\delta(u,v)_L = \sum_{i=1}^{n} \min\{q - |u_i - v_i|, |u_i - v_i|\}$$

[1] The motivation to define an error metric as such as opposed to the standard hamming distance is to encode relative closeness between words, which has uses in phase modulation transmission, which makes sense since Lee went on to be an early pioneer in implementing CDMA as a technology, but that's besides the point.

Definition 2. *C is an e-error correcting Lee code if it is a subset $C \subset \mathbb{Z}_q^n$ such that for any $u, v \in C, \delta_L(u,v) \geq 2e+1$*

Additionally, based on the definition of the Lee distance one can see that it is the Manhattan metric (taxicab metric, l^1 metric on $\mathbb{Z}^n$) restricted to $\mathbb{Z}_q$:

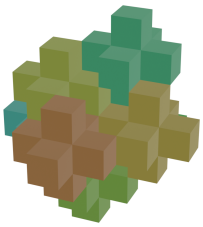
Definition 3. *For any two points $u, v \in \mathbb{Z}^n$, the taxicab metric between the two is given as*

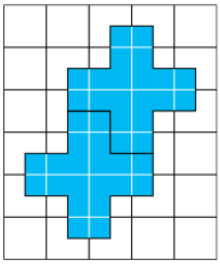
$$\delta(u,v) = \sum_{i=1}^{n} |u_i - v_i|$$

Note that the lee metric and lee codes give us a more tangible geometry to work with than the hamming metric. This gives rise to the natural definition of the lee sphere:

Definition 4. *A lee sphere with radius d centered at point $p \in \mathbb{Z}_q^n$ is the set $\{u \in \mathbb{Z}_q^n : \delta_L(u,p) = d\}$*

Here are some examples of lee spheres of radius 1 for dimensions $n = 2, 3$:





2 But what is a *perfect* Lee code?

The definition is what you think it is

Definition 5. *A perfect lee code C is an e-error correcting code such that for each $x \in \mathbb{Z}_q^n$, there exists $c \in C$ such $\delta_L(c, x) \leq e$*

Now one may ask why these are interesting objects to study, however, there are some associated theorems and conjectures that enrich the subject

Theorem 1. *For every $n \in \mathbb{N}$, there exists a 1-error correcting code on $\mathbb{Z}_{2n+1}^n$ of the form for every $c \in C, \sum_{i=1}^n ix_i \equiv 0 \mod 2n+1$*

Proof: Note for every $c \in C$ such that $\sum_{i=1}^n ic_i \equiv 0 \mod 2n+1$ we have that $c_1 \equiv -\sum_{i=1}^n ic_i \mod 2n+1$, therefore we have uniquely determined $(2n+1)^{n-1}$ points in C. We must now show that every element is within distance 1 of a desired point. Suppose $p \in \mathbb{Z}_{2n+1}^n$. Then $\sum_{i=1}^n ip_i \equiv k \mod 2n+1$. We will consider $-n \leq k \leq n$. If $k \equiv 0 \mod 2n+1$ then p is in the code. If $k \geq 0$ then if we take $p_k \mapsto p_k - 1$ then $\sum_{i=1}^n p_i - k \equiv k - k \equiv 0 \mod 2n+1$, thus placing our modified point within the code. If $k < 0$ then we map $p_k \mapsto p_k + 1$, placing it within the code by a similar logic. Note for each point in our set we have determined $2n$ additional points, thus we reach $(2n+1)(2n+1)^{n-1} = (2n+1)^n = |\mathbb{Z}_{2n+1}^n|$ limit, however we don't know that our spheres are disjointed, points, showing that we have found a perfect 1-error correcting code.

Conjecture 1. *(Golomb-Welch) For $n \geq 3, e \geq 2$ there does not exist a perfect e-error correcting code*

Conjecture 2. *(Horak) For $n \in \mathbb{N}$, if $2n+1$ is prime, there is exactly 1 possible perfect lee code up to isomorphism.*

Theorem 2. *For $n \in \mathbb{N}$, if $2n+1$ is not prime, there is an uncountable number of perfect tilings of $\mathbb{Z}^{2n+1}$ by 1-d lee spheres.*

Note these two above conjectures and the construction of theorem 1 give us potentially the ONLY perfect lee code for the specified dimension. Furthermore, one can uniquely extend these perfect lee codes as tilings of $\mathbb{Z}^n$, which allows us to completely characterize all tilings of $\mathbb{Z}^n$ with respect to the Manhattan metric. Also of interest is that the above conjectures have been proven for $n = 2, 3, 5$, which gives us a full categorization of the Lee sphere tilings in those dimensions.

3 Classifying symmetries of $\mathbb{Z}^n$ tilings

Observe that by the construction in Theorem 1, our code is given as a dot product. Therefore our desired isomorphic codes will be attained via isometries. Note that all orthogonal transformations of $\mathbb{Z}^n$, denoted by the group $O(\mathbb{Z}^n)$ is given by all permutation matrices where each column may or may not be negative. Therefore $|O(\mathbb{Z}^n)| = n!2^n$. Before writing the maple program I conjectured that the lee codes are exactly the same under rotations. One can look above and see that this is the case. However, my maple program to compute the orbit of the theorem 1 code failed this trend for $n = 5$, as the sequence of the size of the orbits was $2, 8, 384$ for dimensions $2, 3, 5$ respectively. Note this implies that the codes have 4, 6, and 10 symmetries respectively when diving by the order of $O(Z^n)$. Note for dimensions $n = 5$ the program took half an hour to run, so further optimizations are necessary to explore the group operation of $O(\mathbb{Z}^n)$ on the codes.

4 Constructing generating matrices for perfect Lee codes

To have efficient computations for a linear code, it's natural to construct a generating matrix. For codes over the hamming metric the theory is well established, however having codes with the same dimension of the ambient space does not occur. Here they do. Therefore there is no clear way to make a generating matrix as before. To create the new generating matrices, one can analyze the requirement to sum to a multiple of $2n+1$. For a given dimension n, the rows the generating matrix are as follows: for $i \equiv 0 \mod 2$, $r_{i1} = i, r_{i,(n-1-\frac{i}{2})} = r_{i,(n-\frac{i}{2})} = 1$, and the rest are 0. For $i \equiv 1 \mod 2, r_{i1} = i, r_{n-\frac{i-1}{2}-1} = 2$, and the rest are 0.

References

[1] Peter Horak and Dongryul Kim. 50 years of the golomb–welch conjecture. *IEEE Transactions on Information Theory*, 64(4):3048–3061, 2017.

[2] C. Lee. Some properties of nonbinary error-correcting codes. *IRE Transactions on Information Theory*, 4(2):77–82, 1958.