A Solution of the Energy Minimization Problem for Codes of Codimension 1

by

Yichi Zhang

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Mathematics

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2022

Author .....
Department of Mathematics
September 9, 2022

Certified by .....
Henry Cohn
Professor
Thesis Supervisor

Accepted by .....
Wei Zhang
Chairman, Department Committee on Graduate Theses

A Solution of the Energy Minimization Problem for Codes of Codimension 1

by

Yichi Zhang

Submitted to the Department of Mathematics
on September 9, 2022, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Mathematics

Abstract

In this thesis, we study the space of quasicodes using Delsarte's linear programming bound to solve the energy minimization problem on codes. Our main contribution is we give the optimal code of codimension 1 for any potential function. We also investigate the polytope of quasicodes, where we give a symmetry and a list of vertices in some special cases.

Thesis Supervisor: Henry Cohn
Title: Professor

Acknowledgments

I would love to thank my advisor, Henry Cohn, for patiently and kindly guiding me through my PhD, never giving up on me and always providing tremendous support during all the hard time I had. I wish to show my appreciation to Barbara Peskin and math department for supporting me in my entire PhD life. I also have been influenced and supported by Jeremy Orloff, Hung Cheng and Arthur Mattuck; working and chatting with them is always an enjoyable time for me.

I would also love to thank: Stewart Craig, Hannah Agate and Eric Gibber in MIT Sailing for arousing my passion on sailing and engineering; Coach E.G. LeBre in MIT Archery for encouraging me to attend my first tournament and to fight in my life; Dr Evan Waldheter in MIT Mental Health for four-year consistently helping me fight with my depression; everyone in Harvard Square Homeless Shelter for always infecting me with your shining personality; and everyone I met in MIT for bringing me a colorful life in these six years. I could not survive my depression and go through the hard time without any of you.

Finally, I must thank my friends who influenced and supported me during my PhD: The Harvard reading group (Chengyang Shao, Bohao Wu, Yinan Xue, Yuxuan Yang, Jingyi Tang, Cheng Cheng) for all the delicious meals, profound discussions and exciting road trips I will never forget; Zilin Jiang, for first introducing combinatorics and math research to me; Junqing Qiao for sharing me with your talent on neuroscience and passion on artificial vocal cords; and Junliang Shen for all the sunsets we have seen on Boston seaside.

Do you hear the people sing; Lost in the valley of the night?

–Les Misérables

献刀逃亡洛阳日，何期九锡魏王时?

–Junliang Shen

Contents

Chapter 1

Introduction

A particle system is a model of physics with point particles interacting via a force law. Although particle systems may sound only tangentially connected to information theory, there turn out to be deep analogies between these fields. The key connection is: by considering the particle system in a discrete space, particle arrangements and force laws can be viewed as codes and potential functions in coding theory, so finding the *ground states* of this system, i.e., well-separated particle arrangements minimizing the total energy, is same as finding *optimal* codes.

For finding the ground states, Delsarte in [1] introduced the *linear programming bound*, a powerful tool to give nontrivial constraints on weight enumerators of discrete codes. It remains a central tool in coding theory. In physical terms, weight enumerators are the same as pair correlation functions; i.e., they measure the distribution of pairwise distances between particles in the system. A *quasicode* is any distance information compatible with these Delsarte constraints, so every code yields a quasicode, but not always vice versa.

In this thesis, we investigate the space (polytope) of quasicodes. Theorem 3.7 gives a description of all quasicode vertices of the polytope that use at least half the available points. For quasicodes of codimension 1, Theorem 3.9 shows that all quasicode vertices correspond to actual codes, so this gives the optimal code of codimension

1 for any potential function. Also, Definition 5.2 gives a symmetry on the space of quasicodes, which remained undiscovered in previous studies. It reduces half of cases we need to consider, and indicates a part of the structure on the polytope.

Chapter 2

Background

In this thesis, we denote the alphabet with q elements by $\mathbb{F}_q$ and only use the additive group structure on $\mathbb{F}_q$, so here q can be any number (not limited to prime powers). Now an n-digit codeword can be viewed as an element in $\mathbb{F}_q^n$. Then a *code* is a subset of $\mathbb{F}_q^n$, and we denote the Hamming distance as $d(x, y)$ for any two codewords x and y in $\mathbb{F}_q^n$. We define the *dimension* of a code C as $\log_q |C|$ and *codimension* as $n - \log_q |C|$. For any code C, we define the *distance distribution* of C as the vector $(A_0, A_1, \ldots, A_n)$, where

$$A_i = \frac{1}{|C|}|\{(x, y) \in C^2 : d(x, y) = i\}| \qquad \text{for } i = 0, 1, \ldots, n$$

and we always have $A_0 = 1$. When this code C is closed under addition, i.e., $w+C = C$ for all $w \in C$, then

$$A_i = |\{x \in C : d(x, 0) = i\}|.$$

This space $\mathbb{F}_q^n$ is a discrete model of the universe, where each codeword is a location for a point particle, and a code corresponds to a particle arrangement. The force law between particles can be viewed as a function only depending on the distance between the particles, which is always an integer between 0 and n in this space. So given a code $C \subseteq \mathbb{F}_q^n$ and a function $f : \{0, \ldots, n\} \to \mathbb{R}$, we define the *potential energy* of C

with respect to the potential function f as

$$E_f(C) = \frac{1}{|C|} \sum_{x,y \in C} f(|x-y|) = \sum_{i=0}^{n} A_i f(i) = (f(0), \ldots, f(n))(A_0, \ldots, A_n)^T,$$

and a code C is *optimal* if for every C' with $|C'| = |C|$,

$$E_f(C) \leq E_f(C').$$

Note that our definition of potential energy includes distance 0. It's traditional to exclude it, to allow potential functions such as inverse power laws that are not defined at distance 0. However, since we always have $A_0 = 1$, this does not change which codes are optimal.

Finding optimal codes is hard. Instead, we investigate the distance distribution and introduce the linear programming bound to give nontrivial constraints on the distance distribution. Delsarte in [1] developed the linear programming bound and originally used it to bound the size of codes given their minimum distance. (See [2] for the general theory, and [3] for a survey article.) Yudin in [7] first applied this tool on energy minimization, and Cohn and Zhao in [4] first used it for bounding energy in discrete case.

In general, for codes over $\mathbb{F}_q$, the k-th *Krawtchouk polynomial* is defined by

$$K_k(x; n, q) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j},$$

and let $K_n = (K_i(j; n, q))_{0 \leq i,j \leq n}$ be the $(n+1) \times (n+1)$ *Krawtchouk matrix*.

Theorem 2.1 (Delsarte inequalities)**.** *Let $\boldsymbol{a} = (A_0, A_1, \ldots, A_n)$ be the distance distribution of a code C. Then*

$$\sum_{i=0}^{n} A_i K_j(i; n, q) \geq 0 \qquad \text{for } j = 0, 1, \ldots, n.$$

We can rewrite this as

$$K_n \cdot \boldsymbol{a}^T \geq 0,$$

where a vector $\boldsymbol{b} \geq 0$ *means that all coordinates of* $\boldsymbol{b}$ *are nonnegative.*

So minimizing $\sum_{i=0}^{n} A_i f(i)$ in the variables $A_0, \ldots, A_n$, with constraints

$$\begin{aligned} K_n \cdot \mathbf{a}^T &\geq 0, \\ A_0 + A_1 + \ldots + A_n &= N, \\ A_0 &= 1, \\ A_i &\geq 0 \end{aligned}$$

gives a lower bound for the minimum potential energy $E_f(C)$ when $|C| = N$. This induces the definition of a quasicode:

Definition 2.2. A *quasicode* $\mathbf{a} = (A_0, A_1, \ldots, A_n)$ of length n and size N over $\mathbb{F}_q$ is a real vector satisfying the following constraints:

$$\mathbf{a} \geq 0, \qquad K_n \cdot \mathbf{a}^T \geq 0, \qquad \sum_{i=0}^{N} A_i = N, \qquad \text{and } A_0 = 1.$$

We define the *dimension* of a quasicode as $\log_q N$ and *codimension* as $n - \log_q N$.

So the distance distribution of any code $C \subseteq \mathbb{F}_q^n$ is a quasicode with length n and size $|C|$, and we can define the *potential energy* of a quasicode $\mathbf{a} = (A_0, A_1, \ldots, A_n)$ as

$$E_f(\mathbf{a}) = \sum_{i=0}^{n} A_i f(i) = (f(0), \ldots, f(n)) \cdot \mathbf{a}^T.$$

The space of quasicodes forms a polytope. We introduce the related definitions here:

Definition 2.3. 1. A subset P of $\mathbb{R}^n$ is a *polyhedron* if there exists a positive integer m, an $m \times n$ matrix A and a vector $b \in \mathbb{R}^m$, such that

$$P = \{x \in \mathbb{R}^n : Ax \leq b\}.$$

2. A vector x in $\mathbb{R}^n$ is a *convex combination* of the vectors $a_1, \ldots, a_p \in \mathbb{R}^n$ if there exist nonnegative scalars $\lambda_1, \ldots, \lambda_p$ such that

$$x = \sum_{i=1}^{p} \lambda_i a_i \text{ and } 1 = \sum_{i=1}^{p} \lambda_i.$$

3. Given a set S in $\mathbb{R}^n$, the *convex hull* of S, denoted by $conv(S)$, is the set of all points that are convex combinations of points in S. That is

$$\text{conv}(S) = \left\{ \sum_{i=1}^{p} \lambda_i a_i : a_i \in S,\ \lambda_i \geq 0,\ \sum_{i=1}^{p} \lambda_i = 1 \right\}.$$

4. A subset Q of $\mathbb{R}^n$ is a *polytope* if Q is the convex hull of a finite set of vectors in $\mathbb{R}^n$.

The following theorem shows the relation between polyhedrons and polytopes (Corollary 3.14 in [6]).

Theorem 2.4 (The Minkowski–Weyl Theorem for Polytopes)**.** *A set Q in $\mathbb{R}^n$ is a polytope if and only if Q is a bounded polyhedron.*

Since every entry of a quasicode is between 0 and N, the set of quasicodes is bounded. So this theorem tells that the set of quasicodes is a polytope. We would like to understand more about the structure of polytope of quasicodes. We start with introducing some properties of Krawtchouk polynomial (see [5]):

1. (Symmetry relation) For integers $i, k \geq 0$,

$$(q-1)^i \binom{n}{i} K_k(i; n, q) = (q-1)^k \binom{n}{k} K_i(k; n, q).$$

2. (Orthogonality relation) For integers $r, s \geq 0$,

$$\sum_{i=0}^{n} \binom{n}{i} (q-1)^i K_r(i; n, q) K_s(i; n, q) = q^n (q-1)^r \binom{n}{r} \delta_{rs}.$$

3. (Generating function)

$$(1+(q-1)z)^{n-i}(1-z)^i = \sum_{j=0}^{\infty} K_j(i;n,q)z^j.$$

4. The Krawtchouk matrix K_n is invertible and

$$K_n^2 = q^n I$$

where I is the identity matrix.

From this generating function, we can prove the following relations for the Krawtchouk polynomial:

Lemma 2.5. *For $j = 1, \ldots, n+1$,*

1. $K_j(i;n+1,q) = K_j(i;n,q) + (q-1)K_{j-1}(i;n,q)$ *for* $i = 0, \ldots, n$, *and*
2. $K_j(i;n+1,q) = K_j(i-1;n,q) - K_{j-1}(i-1;n,q)$ *for* $i = 1, \ldots, n+1$.

Proof. 1. For $i = 0, \ldots, n$,

$$\begin{aligned}\sum_{j=0}^{\infty} K_j(i;n+1,q)z^j &= (1+(q-1)z)^{n+1-i}(1-z)^i \\ &= (1+(q-1)z)\sum_{j=0}^{\infty} K_j(i;n,q)z^j \\ &= \sum_{j=0}^{\infty} K_j(i;n,q)z^j + (q-1)\sum_{j=1}^{\infty} K_{j-1}(i;n,q)z^j.\end{aligned}$$

So for $j = 1, \ldots, n+1$, $K_j(i;n+1,q) = K_j(i;n,q) + (q-1)K_{j-1}(i;n,q)$.

2. For $i = 1, \ldots, n+1$,

$$\begin{aligned}\sum_{j=0}^{\infty} K_j(i;n+1,q)z^j &= (1+(q-1)z)^{n+1-i}(1-z)^i \\ &= (1-z)\sum_{j=0}^{\infty} K_j(i-1;n,q)z^j\end{aligned}$$

$$= \sum_{j=0}^{\infty} K_j(i-1;n,q)z^j - \sum_{j=1}^{\infty} K_{j-1}(i-1;n,q)z^j.$$

So for $j = 1, \ldots, n+1$, $K_j(i;n+1,q) = K_j(i-1;n,q) - K_{j-1}(i-1;n,q)$.

□

Lemma 2.6.

1. $K_0(i;n,q) = 1$, $K_n(i;n,q) = (q-1)^{n-i}(-1)^i$ *for* $i = 0, \ldots, n$, *and* $K_j(i;n,q) = 0$ *for* $j > n$.

2. $(1, \ldots, 1) \cdot K_n = (q^n, 0, \ldots, 0)$.

Proof. 1. We get this result by comparing the constant, z^n term, and z^j term on both sides of the generating function.

2. From part (1), we know $(1, \ldots, 1)$ is the first row of K_n, and we get our result from $K_n^2 = q^n I$.

□

Chapter 3

Vertices of the polytope

The key question in finding optimal codes is: what does the space of distance distribution of codes look like? It's hard to answer, so instead, we focus on the space of quasicodes. This space is typically larger than the space of distance distribution of actual codes. How close are they? In this chapter, Theorem 3.9 tells these two spaces have same size when we consider the codimension 1 codes, as all vertices of the polytope of the quasicodes correspond to actual code. We also list all vertices of the polytope of the quasicodes of size N, when $q^{n-1} \leq N < q^n$, in Theorem 3.7.

We start with defining a function g from $\mathbb{R}^{n+1}$ to $\mathbb{R}^{n+2}$, where

$$g(A_0, A_1, \ldots, A_n) = (A_0, A_1, \ldots, A_n, 0) + (q-1) \cdot (0, A_0, A_1, \ldots, A_n).$$

First we want to show that g maps quasicode to quasicode:

Theorem 3.1. *If $(A_0, A_1, \ldots, A_n)$ is a quasicode of length n and size N, then $g(A_0, A_1, \ldots, A_n)$ is a quasicode of length $n+1$ and size qN. Moreover,*

$$K_{n+1} \cdot g(A_0, A_1, \ldots, A_n)^T = (qK_n \cdot (A_0, A_1, \ldots, A_n)^T, 0),$$

where for a length n vector v, $(v, 0)$ is the length $n+1$ vector obtained by adding one entry 0 to the vector v.

Proof. Let $g(A_0, \ldots, A_n) = (B_0, \ldots, B_{n+1})$. We know $B_i \geq 0$, $B_0 = A_0 = 1$, and $\sum_{i=0}^{N} B_i = q \sum_{i=0}^{N} A_i = qN$. To show $K_{n+1} \cdot (B_0, \ldots, B_{n+1})^T \geq 0$, all we need to show is

$$K_{n+1} \cdot (B_0, \ldots, B_{n+1})^T = (qK_n \cdot (A_0, \ldots, A_n)^T, 0).$$

Let's consider each coordinate; for the first coordinate, we know $K_0(i; n, q) = 1$ for all n and i, so

$$\sum_{i=0}^{n+1} B_i K_0(i; n+1, q) = \sum_{i=0}^{n+1} B_i = q \sum_{i=0}^{n} A_i = q \sum_{i=0}^{n} A_i K_0(i; n, q).$$

For $j = 1, \ldots, n+1$, using the relations in Lemma 2.5, we have

$$\begin{aligned}
\sum_{i=0}^{n+1} B_i K_j(i; n+1, q) &= \sum_{i=0}^{n} A_i K_j(i; n+1, q) + (q-1) \sum_{i=1}^{n+1} A_{i-1} K_j(i; n+1, q) \\
&= \sum_{i=0}^{n} A_i (K_j(i; n, q) + (q-1) K_{j-1}(i; n, q)) \\
&\quad + (q-1) \sum_{i=1}^{n+1} A_{i-1} (K_j(i-1; n, q) - K_{j-1}(i-1; n, q)) \\
&= \sum_{i=0}^{n} A_i (K_j(i; n, q) + (q-1) K_{j-1}(i; n, q)) \\
&\quad + (q-1) \sum_{i=0}^{n} A_i (K_j(i; n, q) - K_{j-1}(i; n, q)) \\
&= q \sum_{i=0}^{n} A_i K_j(i; n, q).
\end{aligned}$$

For $j = n+1$, $K_j(i; n, q) = 0$ for all i, so we have $K_{n+1} \cdot (B_0, \ldots, B_{n+1})^T = (qK_n \cdot (A_0, \ldots, A_n)^T, 0)$. □

For a code $C = \{c_1, \ldots, c_m\} \subseteq \mathbb{F}_q^n$, we define

$$\hat{g}(C) = C \times \mathbb{F}_q = \{\underline{c_i t} \mid t \in \mathbb{F}_q,\ i \in \{1, \ldots, m\}\} \subseteq \mathbb{F}_q^{n+1}$$

where $\underline{c_i t}$ is a length-$n+1$ codeword obtained by adding one entry t to the end of length-n codeword c_i. The following theorem shows that this function $\hat{g}$ on the level

of code induces the previous function g on the level of quasicode.

Theorem 3.2. *If the distance distribution of a code C is $(A_0, \ldots, A_n)$, then the distance distribution of $\hat{g}(C)$ is $g(A_0, \ldots, A_n)$.*

Proof. Let the distance distribution of $\hat{g}(C)$ be $(B_0, \ldots, B_{n+1})$. We know $|\hat{g}(C)| = q|C|$ and $B_0 = 1 = A_0$. First of all,

$$\begin{aligned} B_{n+1} &= \frac{1}{q|C|}|\{(x,y) \in \hat{g}(C)^2 : d(x,y) = n+1\}| \\ &= \frac{1}{q|C|}|\{(\underline{c_i x}, \underline{c_j y}) : d(c_i, c_j) = n,\ x \neq y\}| \\ &= \frac{1}{q|C|} \cdot |C| A_n \cdot q(q-1) \\ &= (q-1)A_n. \end{aligned}$$

For any $i = 1, \ldots, n$,

$$\begin{aligned} B_i &= \frac{1}{q|C|}|\{(x,y) \in \hat{g}(C)^2 : d(x,y) = i\}| \\ &= \frac{1}{q|C|}(|\{(\underline{c_i x}, \underline{c_j y}) : d(c_i, c_j) = i-1, x \neq y\}| + |\{(\underline{c_k z}, \underline{c_l z}) : d(c_k, c_l) = i\}|) \\ &= \frac{1}{q|C|}(|C|A_{i-1} \cdot q(q-1) + |C|A_i \cdot q) \\ &= (q-1)A_{i-1} + A_i. \end{aligned}$$

So $(B_0, \ldots, B_{n+1}) = (A_0, \ldots, A_n, 0) + (q-1)(0, A_0, \ldots, A_n) = g(A_0, \ldots, A_n)$. □

Now we consider the following code C_n:

Definition 3.3. Let $C_n = \{w \in \mathbb{F}_q^n : \sum_{i=1}^n w_i = 0\}$, i.e., the sum of all coordinates of w is zero. Then $|C_n| = q^{n-1}$ and C_n is closed under addition. (Note that we only use the group structure of $\mathbb{F}_q$ in this definition.)

Lemma 3.4. *The distance distribution of C_n is $\vec{c_n}$, where the i-th coordinate of $\vec{c_n}$ is $(\vec{c_n})_i = \frac{1}{q}\binom{n}{i}((q-1)^i + (q-1)(-1)^i)$.*

Proof. As C_n is closed under addition, $(\vec{c_n})_i = |\{w \in C_n : d(x,0) = i\}|$. For $i \geq 1$, we first choose the i non-zero digits out of n; for these i digits, we can arbitrarily pick numbers for the first $i-1$ digits, and the unique choice of the last digit will make the total sum equal to zero. However, we have to rule out the case that the sum of first $i-1$ digits is already zero, as the last digit has to be non-zero. We can get this number by applying the same logic for $i-1$. Thus,

$$\begin{aligned}
(\vec{c_n})_i &= \binom{n}{i}((q-1)^i - \text{sum of } i-1 \text{ non-zero digits is zero}) \\
&= \binom{n}{i}((q-1)^{i-1} - ((q-1)^{i-2} - \text{sum of } i-2 \text{ non-zero digits is zero})) \\
&= \binom{n}{i}((q-1)^{i-1} - ((q-1)^{i-2} - \ldots - ((q-1)^2 - \text{sum of 2 non-zero digits is zero})\ldots)) \\
&= \binom{n}{i}\sum_{k=0}^{i-2}(q-1)^{i-1-k}(-1)^k \\
&= \frac{1}{q}\binom{n}{i}((q-1)^i + (q-1)(-1)^i).
\end{aligned}$$

This formula coincides with $(\vec{c_n})_0 = 1$ as well. □

Now for $i = 1, \ldots, n$, let's consider the code

$$\hat{g}^{(n-i)}(C_i) = \underbrace{\hat{g}(\ldots\hat{g}(\hat{g}}_{n-i}(C_i))\ldots) = \{w \in \mathbb{F}_q^n : \sum_{k=1}^{i} w_k = 0\},$$

which is the code with the sum of first i coordinate equal to zero and having no restrictions on the rest coordinates. From Theorem 3.1 and Theorem 3.2, we know the distance distribution of this code is $g^{(n-i)}(\vec{c_i})$, with size q^{n-1}.

Definition 3.5.

1. Let $\vec{u}$ be the distance distribution of the full-set code $\mathbb{F}_q^n$. Then $\vec{u}$ has size q^n and the i-th coordinate is

$$(\vec{u})_i = \binom{n}{i}(q-1)^i.$$

2. For $i = 1, \ldots, n$, we let

$$\vec{v_i} = g^{(n-i)}(\vec{c_i}),$$

and for $q^{n-1} \leq N < q^n$,

$$\begin{aligned}\overrightarrow{\alpha_{N,i}} &= \vec{v_i} + \frac{N - q^{n-1}}{q^n - q^{n-1}}(\vec{u} - \vec{v_i}) \\ &= \frac{1}{q^n - q^{n-1}}((q^n - N)\vec{v_i} + (N - q^{n-1})\vec{u}).\end{aligned}$$

Then we have the following properties of these vectors:

Lemma 3.6. *1.* $K_n\vec{c_n} = q^{n-1}(1, 0, \ldots, 0, q-1)^T$.

2. $K_n\vec{v_i} = q^{n-1}(1, 0, \ldots, 0, \underbrace{q-1}_{i\ th}, 0, \ldots, 0)^T$, $K_n\vec{u} = (q^n, 0, \ldots, 0)^T$.

3. $K_n\overrightarrow{\alpha_{N,i}} = (N, 0, \ldots, 0, \underbrace{q^n - N}_{i\ th}, 0, \ldots, 0)^T$. *For* $q^{n-1} \leq N < q^n$, *the vectors* $\overrightarrow{\alpha_{N,1}}, \ldots, \overrightarrow{\alpha_{N,n}}$ *are linearly independent, which implies that they are not convex combinations of each other.*

Proof.

1. We have

$$\begin{aligned}\sum_{i=0}^{n}(\vec{c_n})_i K_j(i; n, q) &= \sum_{i=0}^{n}\frac{1}{q}\binom{n}{i}((q-1)^i + (q-1)(-1)^i)K_j(i; n, q) \\ &= \frac{1}{q}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_0(i; n, q)K_j(i; n, q) \\ &\quad + \frac{q-1}{q(q-1)^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_n(i; n, q)K_j(i; n, q) \\ &= \begin{cases} 0 & \text{if } j \neq 0 \text{ or } n \\ q^{n-1} & \text{if } j = 0 \\ (q-1)q^{n-1} & \text{if } j = n \end{cases}\end{aligned}$$

by the orthogonality relation on Krawtchouk polynomials. So $K_n\vec{c_n} = q^{n-1}(1, 0, \ldots, 0, q-1)^T$.

2. We have

$$K_n \overrightarrow{v_i} = K_n g^{(n-i)}(\overrightarrow{c_i}) = q^{n-1}(1, 0, \ldots, 0, \underbrace{q-1}_{i\ th}, 0, \ldots, 0)^T$$

by the previous part and Theorem 3.1. Thus,

$$\begin{aligned}\sum_{i=0}^{n} (\overrightarrow{u})_i K_j(i; n, q) &= \sum_{i=0}^{n} \binom{n}{i} (q-1)^i K_0(i; n, q) K_j(i; n, q) \\ &= \begin{cases} 0 & \text{if } j \neq 0 \\ q^n & \text{if } j = 0. \end{cases}\end{aligned}$$

So $K_n \overrightarrow{u} = (q^n, 0, \ldots, 0)^T$.

3. From the previous parts,

$$\begin{aligned}K_n \overrightarrow{\alpha_{N,i}} &= \frac{1}{q^n - q^{n-1}} K_n((q^n - N)\overrightarrow{v_i} + (N - q^{n-1})\overrightarrow{u}) \\ &= (N, 0, \ldots, 0, \underbrace{q^n - N}_{i\ th}, 0, \ldots, 0)^T.\end{aligned}$$

As K_n is invertible and $q^n - N > 0$, the vectors $\overrightarrow{\alpha_{N,1}}, \ldots, \overrightarrow{\alpha_{N,n}}$ are linearly independent, so they are not convex combinations of each other.

□

Theorem 3.7. *For $q^{n-1} \leq N < q^n$, $\overrightarrow{\alpha_{N,i}}$ are quasicodes of length n and size N. Moreover, $\{\overrightarrow{\alpha_{N,i}}\}_i$ with $i = 1, \ldots, n$ are all vertices of the polytope of the quasicodes of size N, which means*

1. *the vectors $\{\overrightarrow{\alpha_{N,i}}\}_i$ are not convex combinations of each other, and*
2. *any quasicode of size N can be written as a convex combination of $\{\overrightarrow{\alpha_{N,i}}\}_i$.*

Note that we can confidently call $\{\overrightarrow{\alpha_{N,i}}\}_i$ vertices, as Theorem 3.34 in [6] states the following: A vector v in a polytope Q is a *vertex* if and only if it is not a proper convex combination of two distinct points in Q (i.e., if two vectors x, y in Q satisfying

$v = tx + (1-t)y$ for some $0 < t < 1$, then $v = x = y$). From the two properties in the theorem, our vertices $\{\overrightarrow{\alpha_{N,i}}\}_i$ match with this definition.

Proof of Theorem 3.7. Part 1 is directly from Lemma 3.6 Part 3; before we check Part 2, we first check $\overrightarrow{\alpha_{N,i}}$ is a quasicode. We have

$$\overrightarrow{\alpha_{N,i}} = \frac{1}{q^n - q^{n-1}}((q^n - N)\vec{v_i} + (N - q^{n-1})\vec{u}).$$

We know $\vec{u}$ and $\vec{v_i}$ are quasicodes, so all coordinates of $\vec{u}$ and $\vec{v_i}$ are nonnegative. Here $\overrightarrow{\alpha_{N,i}}$ is a nonnegative linear combination of $\vec{u}$ and $\vec{v_i}$, so $\overrightarrow{\alpha_{N,i}} \geq 0$, and $K_n\overrightarrow{\alpha_{N,i}} \geq 0$ from Lemma 3.6. The vectors $\vec{v_i}$ and $\vec{u}$ have size q^{n-1} and q^n respectively, so $\overrightarrow{\alpha_{N,i}}$ has size N. And

$$(\overrightarrow{\alpha_{N,i}})_0 = \frac{1}{q^n - q^{n-1}}((q^n - N)(\vec{v_i})_0 + (N - q^{n-1})(\vec{u})_0) = 1.$$

This shows that $\overrightarrow{\alpha_{N,i}}$ is a quasicode. For Part 2, we consider any quasicode $\vec{z}$ with size N, let $K_n\vec{z} = (x_0, \ldots, x_n)^T$. As the first row of K_n is $(1, \ldots, 1)$, we have $x_0 = N$. Also we know $(1, \ldots, 1)K_n = (q^n, 0, \ldots, 0)$, so

$$x_0 + \cdots + x_n = (1, \ldots, 1)K_n\vec{z} = (q^n, 0, \ldots, 0)\vec{z} = q^n$$

as $(\vec{z})_0 = 1$. So we have $0 \leq x_1, \ldots, x_n \leq q^n - N$.
Now we consider

$$\begin{aligned} K_n\frac{1}{q^n - N}(x_1\overrightarrow{\alpha_{N,1}} + \cdots + x_n\overrightarrow{\alpha_{N,n}}) &= (\frac{N}{q^n - N}(x_1 + \cdots + x_n), x_1, \ldots, x_n)^T \\ &= (x_0, \ldots, x_n)^T. \end{aligned}$$

As K_n is invertible, we have

$$\vec{z} = \frac{1}{q^n - N}(x_1\overrightarrow{\alpha_{N,1}} + \cdots + x_n\overrightarrow{\alpha_{N,n}}),$$

which is a nonnegative linear combination of $\{\overrightarrow{\alpha_{N,i}}\}_i$ with the sum of coefficients equal

to 1. □

We want to minimize the potential energy first over quasicodes, and eventually over codes. From Theorem 3.7, for any quasicode $(A_0, \ldots, A_n)$ with size $q^{n-1} \leq N < q^n$, we can always write it as a nonnegative linear combination of $\overrightarrow{\alpha_{N,i}}$. So

$$\begin{aligned} E_f((A_0, \ldots, A_n)) &= (f(0), \ldots, f(n))(A_0, \ldots, A_n)^T \\ &= \frac{1}{q^n}(f(0), \ldots, f(n))K_n^2(\lambda_1\overrightarrow{\alpha_{N,1}} + \ldots + \lambda_n\overrightarrow{\alpha_{N,n}}) \\ &= \frac{q^n - N}{q^n}(f(0), \ldots, f(n))K_n(\frac{N}{q^n - N}, \lambda_1, \ldots, \lambda_n)^T, \end{aligned}$$

which gives the following theorem.

Theorem 3.8. *Let* $(a_0, \ldots, a_n) = (f(0), \ldots, f(n))K_n$ *and index set* $I = \{i \in \{1 \ldots, n\} : a_i = \min\{a_1, \ldots, a_n\}\}$*, then for quasicodes with size* $q^{n-1} \leq N < q^n$*, the minima of the potential energy are achieved by the polytope generated by vertices* $\{\overrightarrow{\alpha_{N,i}}\}_{i \in I}$*.*

For the special case $N = q^{n-1}$ (code with codimension 1), we have $\overrightarrow{\alpha_{N,i}} = \vec{v_i}$, which is the distance distribution of the code $\hat{g}^{(n-i)}(C_i) = \{w \in \mathbb{F}_q^n : \sum_{k=1}^{i} w_k = 0\}$, so we have the following theorem for potential energy over codes:

Theorem 3.9. *Let* $(a_0, \ldots, a_n) = (f(0), \ldots, f(n))K_n$ *and index set* $I = \{i \in \{1 \ldots, n\} : a_i = \min\{a_1, \ldots, a_n\}\}$*, then for codes with codimension* 1 *(size* q^{n-1}*), the potential energy reaches minimum at the codes* $\{w \in \mathbb{F}_q^n : \sum_{k=1}^{i} w_k = 0\}$ *with* $i \in I$*.*

Chapter 4

Properties of binary quasicode

In this section, we consider binary quasicodes, the special case when $q = 2$. For any binary code in $\mathbb{F}_2^n$, any codeword x has at most one codeword with distance n; we call this codeword the antipode of x and write it as $\underbrace{1\ldots1}_{\text{n}} - x$. So for the distance distribution of any binary code, we always have $A_n \leq 1$. When $A_n = 1$, this means every codeword has its unique antipode in the code, so we have $A_i = A_{n-i}$ by symmetry. By taking these simple combinatorial observations for binary codes, Theorem 4.2 and Theorem 4.4 show that these properties hold for binary quasicodes as well.

We first prove some properties for Krawtchouk polynomials in $q = 2$ case:

Lemma 4.1. *$K_j(n-x; n, 2) = (-1)^j K_j(x; n, 2)$ and $K_{n-j}(x; n, 2) = (-1)^x K_j(x; n, 2)$.*

Proof. We have

$$\begin{aligned} K_j(n-x; n, 2) &= \sum_{i=0}^{j} (-1)^i \binom{n-x}{i}\binom{x}{j-i} \\ &= \sum_{k=0}^{j} (-1)^{j-k} \binom{n-x}{j-k}\binom{x}{k} \\ &= (-1)^j K_j(x; n, 2). \end{aligned}$$

The symmetry relation of Krawtchouk polynomial gives

$$\binom{n}{i} K_x(i;n,2) = \binom{n}{x} K_i(x;n,2),$$

so

$$\begin{aligned}
\binom{n}{x} K_{n-j}(x;n,2) &= \binom{n}{n-j} K_x(n-j;n,2) \\
&= \binom{n}{n-j} K_x(j;n,2)(-1)^x \\
&= \binom{n}{j} K_x(j;n,2)(-1)^x \\
&= \binom{n}{x} K_j(x;n,2)(-1)^x.
\end{aligned}$$

This shows $K_{n-j}(x;n,2) = (-1)^x K_j(x;n,2)$. □

Theorem 4.2. *For any binary quasicode $(A_0, \ldots, A_n)$, we always have $A_n \leq 1$.*

Proof. We know $\sum_{i=0}^{n} A_i K_j(i;n,2) \geq 0$ for all $j = 0, \ldots n$, so we have

$$0 \leq \sum_{j=0,\ \text{odd}}^{n} \sum_{i=0}^{n} A_i K_j(i;n,2) = \sum_{i=0}^{n} A_i \sum_{j=0,\ \text{odd}}^{n} K_j(i;n,2).$$

The generating function for $q = 2$ is

$$(1+z)^{n-i}(1-z)^i = \sum_{j=0}^{\infty} K_j(i;n,2) z^j = \sum_{j=0}^{n} K_j(i;n,2) z^j.$$

Case 1: For any $i \neq 0, n$, plugging in $z = 1$ and $z = -1$ gives

$$\sum_{j=0,\ \text{odd}}^{n} K_j(i;n,2) + \sum_{j=0,\ \text{even}}^{n} K_j(i;n,2) = 0$$

and

$$\sum_{j=0,\ \text{even}}^{n} K_j(i;n,2) - \sum_{j=0,\ \text{odd}}^{n} K_j(i;n,2) = 0,$$

which implies

$$\sum_{j=0,\text{ odd}}^{n} K_j(i;n,2) = 0.$$

Case 2: For $i = 0$, plugging in $z = 1$ and $z = -1$ gives

$$\sum_{j=0,\text{ odd}}^{n} K_j(0;n,2) + \sum_{j=0,\text{ even}}^{n} K_j(0;n,2) = 2^n$$

and

$$\sum_{j=0,\text{ even}}^{n} K_j(0;n,2) - \sum_{j=0,\text{ odd}}^{n} K_j(0;n,2) = 0,$$

which implies

$$\sum_{j=0,\text{ odd}}^{n} K_j(0;n,2) = 2^{n-1}.$$

Case 3: For $i = n$, plugging in $z = 1$ and $z = -1$ gives

$$\sum_{j=0,\text{ odd}}^{n} K_j(n;n,2) + \sum_{j=0,\text{ even}}^{n} K_j(n;n,2) = 0$$

and

$$\sum_{j=0,\text{ even}}^{n} K_j(n;n,2) - \sum_{j=0,\text{ odd}}^{n} K_j(n;n,2) = 2^n,$$

which implies

$$\sum_{j=0,\text{ odd}}^{n} K_j(n;n,2) = -2^{n-1}.$$

So $0 \le \sum_{i=0}^{n} A_i \sum_{j=0,\text{ odd}}^{n} K_j(i;n,2)$ implies $2^{n-1}A_0 - 2^{n-1}A_n \ge 0$. As $A_0 = 1$, we have $A_n \le 1$. □

Lemma 4.3. *For any $i, j \in \{0, \ldots, n-2\}$ with j odd,*

$$K_j(i;n-2,2) = \sum_{s=1,\ odd}^{j} K_s(i+1;n,2).$$

Proof. Multiplying both sides of $(1+z)^{n-2-i}(1-z)^i = \sum_{j=0}^{n-2} K_j(i;n-2,2)z^j$ by $1-z^2$

gives

$$\begin{aligned}(1+z)^{n-i-1}(1-z)^{i+1} &= \sum_{j=0}^{n-2} K_j(i;n-2,2)z^j - K_j(i;n-2,2)z^{j+2} \\ &= \sum_{j=0}^{n-2} K_j(i;n-2,2)z^j - \sum_{j=2}^{n} K_{j-2}(i;n-2,2)z^j,\end{aligned}$$

where the left side is $\sum_{j=0}^{n} K_j(i+1;n,2)z^j$, so

$$K_j(i+1;n,2) = \begin{cases} K_j(i;n-2,2) & \text{for } j \in \{0,1\} \\ K_j(i;n-2,2) - K_{j-2}(i;n-2,2) & \text{for } j \in \{2,\ldots,n-2\} \\ -K_{j-2}(i;n-2,2) & \text{for } j \in \{n-1,n\}. \end{cases}$$

Now we check the claim:

If $j = 1$, then

$$K_j(i;n-2,2) = K_j(i+1;n,2).$$

If $1 < j \leq n-2$ with j odd, then

$$\begin{aligned}K_j(i;n-2,2) &= K_j(i+1;n,2) + K_{j-2}(i;n-2,2) \\ &= K_j(i+1;n,2) + K_{j-2}(i+1;n,2) + K_{j-4}(i;n-2,2) \\ &= \sum_{s=1,odd}^{j} K_s(i+1;n,2).\end{aligned}$$

□

Theorem 4.4. *For any binary quasicode $(A_0,\ldots,A_n)$, if $A_n = 1$, then $A_i = A_{n-i}$ for all i.*

We know $\sum_{i=0}^{n} A_i K_j(i;n,2) \geq 0$ for all $j = 0,\ldots,n$. Let $B_i = A_i - A_{n-i}$. For j odd, we have

$$K_j(n-i;n,2) = (-1)^j K_j(i;n,2) = -K_j(i;n,2),$$

so $\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} B_i K_j(i;n,2) \geq$ for any odd j.

If we let $\vec{w}_{j,n} = (K_j(1;n,2), \ldots, K_j(\lceil \frac{n}{2} \rceil - 1; n, 2))$ and $\vec{v}_{j,n} = (K_j(0;n,2), \vec{w}_{j,n})$, then

$$\vec{v}_{j,n} \cdot (B_0, B_1, \ldots, B_{\lceil \frac{n}{2} \rceil - 1}) \geq 0$$

for j odd in $\{0, \ldots, n\}$. Then Theorem 4.4 converts into the following proposition:

Proposition 4.5. *If $\vec{v}_{j,n} \cdot (B_0, B_1, \ldots, B_{\lceil \frac{n}{2} \rceil - 1}) \geq 0$ for all j odd in $\{0, \ldots, n\}$, and $B_0 = 0$, then $(B_0, B_1, \ldots, B_{\lceil \frac{n}{2} \rceil - 1}) = (0, \ldots, 0)$ for all i.*

Proof by induction on n. For $n = 1$, this is trivial.
For $n > 1$, as $B_0 = 0$, then we have $\vec{w}_{j,n} \cdot (B_1, \ldots, B_{\lceil \frac{n}{2} \rceil - 1}) \geq 0$. From the previous lemma, for j odd in $\{0, \ldots, n-2\}$, we know

$$\begin{aligned}
\vec{v}_{j,n-2} &= (K_j(0;n-2,2), K_j(1;n-2,2) \ldots, K_j(\lceil \frac{n}{2} \rceil - 2; n-2, 2)) \\
&= \left(\sum_{s=1,\ \text{odd}}^{j} K_s(1;n,2), \sum_{s=1,\ \text{odd}}^{j} K_s(2;n,2), \ldots, \sum_{s=1,\ \text{odd}}^{j} K_s(\lceil \frac{n}{2} \rceil - 1; n, 2) \right) \\
&= \sum_{s=1,\ \text{odd}}^{j} \vec{w}_{s,n}.
\end{aligned}$$

So $\vec{v}_{j,n-2}$ is a positive linear combination of $\vec{w}_{s,n}$ for odd s, which means

$$\vec{v}_{j,n-2} \cdot (B_1, \ldots, B_{\lceil \frac{n}{2} \rceil - 1}) \geq 0$$

for all j odd in $\{0, \ldots, n-2\}$. From the proof of Theorem 4.2, we know

$$\sum_{j=0,\ \text{odd}}^{n-2} \vec{v}_{j,n-2} = (2^{n-3}, 0, \ldots, 0)$$

so $2^{n-3} B_1 \geq 0$, which implies $B_1 \geq 0$.

On the other hand, $\sum_{j=0,\ \text{odd}}^{n-2} \vec{v}_{j,n-2}$ is a positive linear combination of $\vec{w}_{j,n}$, so there

exist $t_j \geq 0$ satisfying

$$\sum_{j=0,\text{ odd}}^{n} t_j w_{j,n} = (2^{n-3}, 0, \ldots, 0).$$

From the proof of Theorem 4.2, we know

$$\sum_{j=0,\text{ odd}}^{n} w_{j,n} = \sum_{j=0,\text{ odd}}^{n} (K_j(1; n, 2) \ldots, K_j(\lceil \frac{n}{2} \rceil - 1; n, 2)) = (0, \ldots, 0).$$

Now let $t_M = \max\{t_j\}_j + 1$. Then

$$\sum_{j=0,\text{ odd}}^{n} (t_M - t_j) w_{j,n} = (-2^{n-3}, 0, \ldots, 0),$$

which is a positive linear combination of $w_{j,n}$, so $-2^{n-3} B_1 \geq 0$, which implies $B_1 \leq 0$.

So we have $\vec{v}_{j,n-2} \cdot (B_1, \ldots, B_{\lceil \frac{n}{2} \rceil - 1}) \geq 0$ for all j odd in $\{0, \ldots, n-2\}$ and $B_1 = 0$, which is the inductive hypothesis for $n-1$, so we have $(B_0, B_1, \ldots, B_{\lceil \frac{n}{2} \rceil - 1}) = (0, \ldots, 0)$. $\square$

Chapter 5

Symmetry on even digit binary code

To understand the structure of the spaces of binary codes and binary quasicode, we want to know what are the symmetries on them. There are not many symmetries; when code has half dimension, the duality provides a symmetry. In this chapter, assuming n is even, we find another symmetry for binary codes and quasicodes with any size.

Definition 5.1. Let $\mathbb{1}$ denote the n-digit codeword $\underbrace{1\ldots1}_{\text{n}}$. Define a map f from n-digit codewords to n-digit codewords by

$$f(a) = \begin{cases} a & \text{if } a \text{ is even (has even weight)} \\ \mathbb{1} + a & \text{if } a \text{ is odd (has odd weight)} \end{cases}$$

where the weight of a codeword is the sum of all digits.

Definition 5.2. For n even, define a permutation F in the symmetric group S_n as

$$F = (1\ n-1)(3\ n-3)\ldots = \prod_{i<\frac{n}{2} \text{ and odd}} (i\ n-i)$$

and we can extend it to a map F' from quasicodes to quasicodes by keeping the even-

distance positions and switching the value of every odd-distance k position with the value at distance $n-k$ position, i.e.,

$$F'((t_0, t_1, t_2 \ldots, t_{n-1}, t_n)) = (t_0, t_{n-1}, t_2, \ldots, t_1, t_n).$$

To prove F' maps quasicodes to quasicodes, the only thing we need to check is

$$K_n \cdot F'(\mathbf{a}) \geq 0$$

for any quasicode $\mathbf{a} = (A_0, A_1, \ldots, A_n)$. This means we need to show

$$\sum_{i=0,\text{ even}}^{n} K_j(i; n, 2)A_i + \sum_{i=0,\text{ odd}}^{n} K_j(i; n, 2)A_{n-i} \geq 0 \text{ for all } j.$$

Proof. Lemma 4.1 tells us that

$$K_j(n-i; n, 2) = (-1)^j K_j(i; n, 2) \text{ and } K_{n-j}(i; n, 2) = (-1)^i K_j(i; n, 2).$$

When j is even, we have

$$K_j(i; n, 2) = K_j(n-i; n, 2),$$

so the left-hand side of our statement is $\sum_{i=0}^{n} K_j(i; n, 2)A_i$, which is nonnegative as $\mathbf{a}$ is a quasicode.

When j is odd,

$$\begin{aligned}
&\sum_{i=0,\text{ even}}^{n} K_j(i; n, 2)A_i + \sum_{i=0,\text{ odd}}^{n} K_j(i; n, 2)A_{n-i} \\
&= \sum_{i=0,\text{ even}}^{n} K_j(i; n, 2)A_i + \sum_{i=0,\text{ odd}}^{n} K_j(n-i; n, 2)A_i \\
&= \sum_{i=0,\text{ even}}^{n} K_j(i; n, 2)A_i - \sum_{i=0,\text{ odd}}^{n} K_j(i; n, 2)A_i
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0,\text{ even}}^{n} K_{n-j}(i;n,2)A_i + \sum_{i=0,\text{ odd}}^{n} K_{n-j}(i;n,2)A_i \\
&= \sum_{i=0}^{n} K_{n-j}(i;n,2)A_i \\
&\geq 0.
\end{aligned}
$$

□

As $|F'(\mathbf{a})| = |\mathbf{a}|$, this F' gives a symmetry on the polytope of quasicodes. Here are some properties of these functions:

Lemma 5.3. *1. f^2=identity, F^2=identity, F'^2 = identity.*

2. f is a linear map, i.e., $f(a+b) = f(a) + f(b)$ and $f(\lambda a) = \lambda f(a)$, for $\lambda = 0, 1$.

The proof of this lemma is immediate.

Lemma 5.4. *1. For any codewords $a, b \in \mathbb{F}_2^n$, we always have*

$$d(f(a), f(b)) = F(d(a,b)).$$

2. For any code C, the distance distribution of $f(C)$ is equal to applying F' to distance distribution of C.

Proof. Case 1: If a, b are even, then $d(a,b)$ is even, so

$$d(f(a), f(b)) = d(a,b) = F(d(a,b)) = F(d(a,b)).$$

Case 2: If a, b are odd, then $d(a,b)$ is even, so

$$d(f(a), f(b)) = d(\mathbb{1} + a, \mathbb{1} + b) = d(a,b) = F(d(a,b)).$$

Case 3: If a, b has different parity, without loss of generality we can assume a is even and b is odd. Then $d(a,b)$ is odd, and

$$d(f(a), f(b)) = d(a, \mathbb{1} + b) = n - d(a,b) = F(d(a,b)).$$

This proves first property, and the second one is an immediate corollary. □

Definition 5.5. If C is a code, we define the dual code as

$$C^{\perp} = \{w \in \{0,1\}^n : (w,v) = 0, \forall v \in C\},$$

where (,) is the dot product by viewing codewords as vectors modulo 2. So $f(C^{\perp}) = \{f(w) : (w,v) = 0, \forall v \in C\}$ and $f(C)^{\perp} = \{w : (w, f(v)) = 0, \forall v \in C\}$.

Lemma 5.6. *For any two codewords v_1 and v_2, $(f(v_1), f(v_2)) = (v_1, v_2)$.*

Proof. $(\mathbb{1}, a) = 0$ if a has even weight and $(\mathbb{1}, a) = 1$ if a has odd weight, so

$$(f(v_1), f(v_2))$$
$$= \begin{cases} (v_1, v_2) & \text{if } v_1 \text{ and } v_2 \text{ have even weight} \\ (v_1 + \mathbb{1}, v_2) = (v_1, v_2) + (\mathbb{1}, v_2) = (v_1, v_2) & \text{if } v_1 \text{ has odd weight, } v_2 \text{ has even weight} \\ (v_1, \mathbb{1} + v_2) = (v_1, v_2) + (v_1, \mathbb{1}) = (v_1, v_2) & \text{if } v_1 \text{ has even weight, } v_2 \text{ has odd weight} \\ (v_1 + \mathbb{1}, v_2 + \mathbb{1}) = (v_1, v_2) + 1 + 1 + 0 = (v_1, v_2) & \text{if } v_1 \text{ and } v_2 \text{ have odd weight.} \end{cases}$$

□

Lemma 5.7. *The function f commutes with dual operation, i.e., $f(C^{\perp}) = f(C)^{\perp}$.*

Proof. For any $f(w) \in f(C^{\perp})$ and any $v \in C$,

$$(f(w), f(v)) = (w, v) = 0,$$

so $f(w) \in f(C)^{\perp}$ and $f(C^{\perp}) \subseteq f(C)^{\perp}$.
For any $w \in f(C)^{\perp}$ and any $v \in C$,

$$(f(w), v) = (f(f(w)), f(v)) = (w, f(v)) = 0,$$

so $w \in f(C^{\perp})$ and $f(C)^{\perp} \subseteq f(C^{\perp})$, which implies $f(C^{\perp}) = f(C)^{\perp}$. □

From Proposition 5 of [4], we know if $\mathbf{a} = (A_0 \ldots, A_n)$ is the distance distribution of code C, then the distance distribution of $C^\perp$, $\mathbf{a}^\perp = (A_0^\perp, \ldots, A_n^\perp)$, is

$$A_j^\perp = \frac{1}{N} \sum_{i=0}^{n} A_i K_j(i; n, 2),$$

where $N = |C| = \sum A_i$. So

$$\mathbf{a}^{\perp T} = \frac{1}{N} K_n \cdot \mathbf{a}^T.$$

Using this formula, we can extend the dual operation to quasicodes. Since $K_n^2 = 2^n I$, for a quasicode $\mathbf{a}$ of size N, $\mathbf{a}^\perp$ is a quasicode of size $\frac{2^n}{N}$.

Our proof showing F' maps quasicodes to quasicodes also proves the following theorem:

Theorem 5.8. *For any quasicode* $\boldsymbol{a}$, $F'(\boldsymbol{a}^\perp) = F'(\boldsymbol{a})^\perp$, *i.e.,*

$$A_{F(j)}^\perp = \frac{1}{|C|} \sum_{i=0}^{n} A_{F(i)} K_j(i; n, 2).$$

So our symmetry commutes with the dual operation on quasicodes. For the special case $N = 2^{\frac{n}{2}}$ (half dimension), a quasicode and its dual have the same size, which means the dual operation provides another symmetry on the polytope of quasicode.

Chapter 6

Further questions

In Chapter 3, we get a complete list of vertices with size $q^{n-1} \leq N < q^n$. What happens for the polytope of quasicodes with size less than q^{n-1}? For $q = 2$, here is a table on number of vertices of the polytope computed using Polymake [8]:

n	N	Number of Vertices
3	1	1
3	2	3
3	3	4
3	4–7	3
3	8	1
4	1	1
4	2	4
4	3	9
4	4	5
4	5	9
4	6	7
4	7	9
4	8–15	4
4	16	1
5	1	1

n	N	Number of Vertices
5	2	5
5	3	17
5	4	14
5	5	17
5	6	12
5	7	17
5	8	14
5	9	17
5	10	17
5	11	17
5	12	12
5	13	13
5	14	13
5	15	13
5	16–31	5

n	N	Number of Vertices
5	32	1
6	1	1
6	2	6
6	3	28
6	4	16
6	5	29
6	6	40
6	7	41
6	8	24
6	9	41
6	10	41
6	11	41
6	12	29
6	13	29
6	14	29
6	15	29
6	16	16

n	N	Number of Vertices
6	17	28
6	18	28
6	19	28
6	20	28
6	21	28
6	22	28
6	23	28
6	24	22
6	25	24
6	26	24
6	27	20
6	28	20
6	29	20
6	30	20
6	31	20
6	32–63	6
6	64	1

This shows a more complex phenomenon for the case $N < q^{n-1}$, so we can't expect simple generalization of our main theorem on the list of vertices.

Bibliography

[1] P. Delsarte, *Bounds for unrestricted codes by linear programming*, Philips Res. Repts. **27** (1972), 272–289.

[2] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Repts. Suppl. **10** (1973).

[3] P. Delsarte and V. I. Levenshtein, *Association schemes and coding theory*, IEEE Trans. Inform. Theory, **44** (1998), 2477–2504

[4] H. Cohn and Y. Zhao, *Energy-minimizing error-correcting codes*, IEEE Trans. Inform. Theory **60** (2014), 7442–7450.

[5] V. I. Levenshtein, *Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces*, IEEE Trans. Inform. Theory **41** (1995), 1303–1321.

[6] M. Conforti, G. Cornuéjols and G. Zambelli, *Integer Programming*, Graduate Texts in Mathematics, **271**, Springer, (2014).

[7] V. A. Yudin, *The minimum of potential energy of a system of point charges*, Discrete Math. Applicat. **3** (1993), 75–81.

[8] B. Assarf, E. Gawrilow, K. Herr, M. Joswig, B. Lorenz, A. Paffenholz and T. Rehn, *Computing convex hulls and counting integer points with polymake*, Math. Program. Comput. **1** (2017), 1–38.