Coding theory and Grassmannian varieties

Pengrun Huang
Advised by Eric Canton

August 20, 2020

Abstract

The main goal of this REU project is to study linear codes using Grassmannian varieties.

Contents

1 Introduction **2**

2 Basic concepts in coding theory **3**
2.1 Linear code and generator matrix 3
2.2 Weight, distance and error-correcting capability 3

3 Grassmannian varieties **5**
3.1 Varieties and projective varieties 5
3.2 Plucker embedding 6
3.3 Basic Topology and Zariski topology 8

4 Isometric code and Grassmannian varieties **10**

I would like to acknowledge David Speyer, Christina Certo and people running the University of Michigan REU math program for providing this precious research opportunity. I especially want to thank my mentor, Eric Canton, for all his advice.

1 Introduction

Coding theory is the branch of mathematics that studies data transmission and error correction. Claude Shannon began the study of coding theory when he identified that channels have a capacity, and proved that arbitrarily reliable communication is possible at any rate below the channel capacity [1].

The common feature of communication channels is that information is emanating from a source and is sent over the channel to a receiver at the other end. However, the channel can be noisy in the sense that information been sent over the channel may be corrupted. In other words, what is received is not always the same as what is sent. A communication channel is illustrated in Figure 1.1. For example, we can encode voice, music, or data into binary and send it over the channel. Two types of channels are cable channel - such as twisted-pair wire and fiber-optic cable - and broadcast channel -such as microwave, satellite and radio. When a 0 is sent, we hope it can be received as 0, but sometimes it may be received as 1 (or as unrecognizable). Hence, one fundamental problem in coding theory is to determine what message was sent on the basis of what is received. The basic idea for error-correcting codes is to add redundant information to the original codes so that we could decode the received message back to original information. People seek to design codes that have great error correction properties.

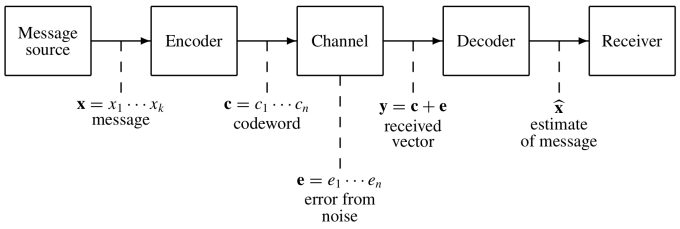

Figure 1: Communication channel

In Section 2, we study some properties of Linear codes that ensure a high error-correcting capability. We prove that the number of errors linear codes are able to detect and correct is determined by minimum distance, or minimum weight. [2] [3]

In section 2 we show that linear code can be understood as subspace of vector space, in Section 3, we study Grassmannian variety in algebraic geometry. We first study Plucker embedding, which embed a subspace into a point in certain projective space, and its property of being a projective variety of a quadratic polynomial. Then, we study basic topology and Zariski topology, a kind of topology defined on varieties. [4] [5] [6]

In Section 4, we first closely examine $G(2, 4)$, every 2 dimensional subspace of a 4 dimensional space. We observe that a subset of linear codes have same hamming distance between every codewords. We study the group structure

of isometric codes in $\mathbb{F}_q$. First we study the most common isometric codes, permutationally isometric codes. Then we generalize it into linearly isometry. We relax the condition of linearity and study semilinear isometric codes. Our presentation here closely follows [7]. We restrict the field into $\mathbb{F}_2$ and prove that in $\mathbb{F}_2$, if two linear codes are isometric, under three different definition of isometry, they will have the same Hamming weight of Grassmannian varieties.

2 Basic concepts in coding theory

2.1 Linear code and generator matrix

Let $\mathbb{F}_q^n$ denote the vector space of all n-tuples over the finite field $\mathbb{F}_q$. An (n, M) *code* over $\mathbb{F}_q$ is a subset $\mathcal{C}$ of $\mathbb{F}_q^n$ of size M. We will write a vector $(a_1, a_2..., a_n)$ in $\mathbb{F}_q^n$ in the form $a_1a_2...a_n$, and call the vectors in $\mathcal{C}$ *codewords*. If $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$, then $\mathcal{C}$ will be called an $[n, k]$ *linear* code. An $[n, k]$ linear code $\mathcal{C}$ has q^k codewords, so is an (n, M) code.

One common ways to present a linear code is through a generator matrix. A generator matrix for an [n, k] linaer code $\mathcal{C}$ is any k $\times$ n matrix G whose rows form a basis for $\mathcal{C}$.

Example 2.1. The following is an example of [4, 2] linear code:

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

In this example, the rows of matrix $\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ form a 2 dimensional subspace of a 4 dimensional space, hence it is a generator matrix for [4,2] linear code. The codewords are $0000, 1011, 0101, 1110$.

2.2 Weight, distance and error-correcting capability

Definition 2.1. The *Hamming weight* of an element $u \in \mathbb{F}_q^n$ is the number of nonzero coordinates in u, denoted as $\mathrm{Wt}(u)$.

Definition 2.2. Let $u, v \in \mathbb{F}_q^n$. The *Hamming distance* between u and v, denoted as $d(u, v)$, is the number of coordinates in which u and v differ.

Example 2.2. Let $u = 01001, v = 10110 \in \mathbb{F}_2^5$. In this case, $\mathrm{Wt}(u) = 2$ and $\mathrm{Wt}(v) = 3$. Since 00000 has weight 0, $\mathrm{Wt}(u) = d(u, 0)$. Finally, $d(u, v) = 5$ since u and v differ in all coordinates.

The next lemma proves the relationship between Hamming weight and distance that we have observed in the previous example.

Lemma 2.1. *If $u, v, w \in \mathbb{F}_q^n$, then*

1. $d(u, v) = Wt(u - v)$, *and*

2. $d(u, v) \leq d(u, w) + d(w, v)$.

Proof. Fix $u, v, w \in \mathbb{F}_q^n$.

1. A coordinate of $u - v$ is nonzero if and only if u and v differ in that coordinate. Hence, the number of nonzero coordinates in $u - v$, namely $\mathrm{Wt}(u - v)$, is the same as the number of coordinates in which u and v differ, namely $d(u, v)$.

2. By (1), it is equivalent to prove $\mathrm{Wt}(u, v) \leq \mathrm{Wt}(u - w) + \mathrm{Wt}(w - v)$. We need to verify that whenever $u - v$ has non-zero i-th coordinate, at least one of $u - w$ and $w - v$ also has nonzero i-th coordinate. Suppose the i-th coordinate $u_i - v_i$ is nonzero. If the ith coordinate $u_i - w_i$ is nonzero, then there is nothing to prove. If $u_i - w_i = 0$, then $u_i = w_i$ and $w_i - v_i = u_i - v_i \neq 0$. Therefore, $w_i - v_i$ is nonzero.

□

Given a codeword u is send and the word v is received, the number of errors in the transmission is the number of coordinates in which u and v differ, in other words, the Hamming distance between u and v. According to probability theory, a large number of transmission errors is less likely than a small number of transmission errors, hence the nearest codeword to a received word is most likely to be the codeword that was transmitted. Therefore, a received word is decoded as the codeword that is nearest to it in Hamming distance, which is called *nearest-neighbor decoding*.

Definition 2.3. A linear code is said to *correct t errors* if every codeword that is transmitted with t or fewer errors is correctly decoded by *nearest-neighbor decoding*.

The following theorem proves a direct implication between minimum distance and error correction.

Theorem 2.1. *A linear code* corrects t errors *if and only if the Hamming distance between any two codewords is at least* $2t + 1$.

Proof. Assume the distance between any two codewords is at least $2t + 1$. If the codeword u is transmitted with t or fewer errors and received as w, then $d(u, w) \leq t$. If v is any other codeword, then $d(u, v) \geq 2t + 1$ by hypothesis. Hence, by Lemma 2.1,

$$2t + 1 \leq d(u, v) \leq d(u, w) + d(w, v) \leq t + d(w, v)$$

Subtracting t from both sides of $2t + 1 \leq d(w, v) + t$ shows that $d(w, v) \geq t + 1$. Since $d(u, w) \leq t$, u is the closest codeword to w, so nearest-neighbor decoding correctly decodes w as u. This completes the proof. □

Definition 2.4. A linear code is said to *detect t errors* if the received word in any transmission with at least one, but no more than t errors, is not a codeword.

Just as with error correction, there is a direct implication between minimum distance and error detection:

Theorem 2.2. *A linear code detects t errors if and only if the Hamming distance between any two codewords is at least* $t + 1$.

Proof. Assume that the distance between any two codewords is at least $t + 1$. If the codeword u is transmitted with at least one, but no more than t errors, and received as w, then

$$0 \leq d(u, w) \leq t, \text{ hence } d(u, w) < t + 1,$$

so w cannot be a codeword. Therefore, the code detects t errors. □

Theorem 2.3. *If* $x, y \in \mathbb{F}_q^n$, *then* $d(x, y) = \mathrm{Wt}(x - y)$. *If* $\mathcal{C}$ *is a linear code, the minimum distance between any two codewords in* $\mathcal{C}$ *is the same as the minimum weight of some nonzero codeword of* $\mathcal{C}$.

Proof. The idea of the proof is that if $\mathcal{C}$ is linear codes, then subtraction of two vectors is in the subspace, i.e $x - y$ is a codeword in $\mathcal{C}$. Hence, minimum distance is the same as minimum weight of nonzero codeword of $\mathcal{C}$. □

We see thus that the error-correcting or detecting capability of a code is closely related to the minimum distance of that code. By Theorem 2.3, the minimum distance is the smallest distance between distinct codewords, or minimum weight. Therefore, this property is the most interesting property we are concerned about.

3 Grassmannian varieties

A linear code $\mathcal{C}$ is a subspace of a vector space by section 2. In this section, we introduce Grassmannian varieties, which embeds a d-dimensional subspace of a n dimensional vector space into a certain projective space using Plucker embedding.

3.1 Varieties and projective varieties

Let $\Bbbk$ be an algebraically closed field, and let $\Bbbk[x_1, .., x_n]$ be the polynomial ring with n variables, denoted as $\Bbbk[X]$. We define n-dimensional affine space, $\mathbb{A}^n$, to be $\Bbbk^n$. Given $f \in \Bbbk[X]$, we view f as a $\Bbbk$-valued polynomial on affine space by evaluation, $f : (x_1, ..., x_n) \mapsto f(x_1, ..., x_n)$.

Definition 3.1. Given a subset $S \subset \Bbbk[X]$, let $V(S) = \{X \in \mathbb{A}^n |\ f(X) = 0, \forall f \in S\}$. If $S \subset \mathbb{A}^n$ is such that $W = V(S)$ for some $S \subset \Bbbk[X]$, we say that W is an affine variety.

Definition 3.2. Given an affine variety $W \in \mathbb{A}^n$, let $I(W) = \{f \in \Bbbk[X] | f(a_1, ..., a_n) = 0 \text{ for all } (a_1, ..., a_n) \in W\}$. This set is called the ideal of the variety W.

Define n-dimensional projective space, $\mathbb{P}^n$, to be the quotient of $\mathbb{A}^n \setminus 0$ by the action of $\Bbbk^\times$ on $\mathbb{A}^{n+1}$ by multiplications, that is, $[a_0 : ... : a_n] \sim [\lambda a_0 : ... : \lambda a_n]$ for all nonzero $\lambda \in \Bbbk$. This induces a coordinate system on the resulting quotient space $\mathbb{P}^n$ called homogeneous coordinates. A point in $\mathbb{P}^n$ is denoted by $[a_1, ..., a_n]$, and $[a_1 : ... : a_n] = [\lambda a_1 : ... : \lambda a_n]$ for all nonzero λ in $\Bbbk$. We observe that two points in $\mathbb{A}^n$ are identical in projective space if and only if they lie on the same line through the origin. Hence, we can also view $\mathbb{P}^n$ as the space of lines in $\mathbb{A}^{n+1}$ through the origin.

In general, a polynomial $f \in k[x_0, ..., x_n]$ is not a function on $\mathbb{P}^n$, for $f(a_0, ..., a_n)$ need not equal $f(\lambda a_0, ..., \lambda a_n)$. Hence, on projective space, we only focus our attention to the homogeneous polynomials.

Definition 3.3. A homogeneous polynomial of degree m is a polynomial $f \in \Bbbk$[x] such that $f(\lambda a_0, ..., \lambda a_n) = \lambda^m f(a_0, ..., a_n)$ for all $\lambda \in \Bbbk^\times$.

Even though homogeneous polynomials are not always well-defined on $\mathbb{P}^n$, they have well-defined zero locus.

Definition 3.4. A projective variety is a subset $W \subset \mathbb{P}^n$ such that $W = V(S)$ for some collection of homogeneous polynomials $S \in \Bbbk[X]$.

3.2 Plucker embedding

Definition 3.5. Let $n \geq 2$ and consider the $\Bbbk$-vector space M of dimension n. For $1 \leq d \leq n$, we define the Grassmannian $G_{d,M}$, or it can be denoted as $G(n, k)$, to be the space of d-dimensional vector subspaces of M.

Fix a field $\Bbbk$, a vector space M of dimension $n < \infty$ over $\Bbbk$, and a basis $\{e_1, ..., e_n\}$ for M. Define $\wedge^d M$ (d-fold $\wedge$ -product) to be the vector space whose elements are string of the form $x_1 \wedge x_2 \wedge ... \wedge x_d$, with all $x_i \in M$, with following condition

1. If $x_i = x_{i+1}$ for some $1 \leq$ i $<$ k, then $x_1 \wedge ... \wedge x_i \wedge x_i \wedge ... \wedge x_k = 0$.
2. $x_i \wedge x_j =$ - $x_j \wedge x_i$, for all $x_i, x_j \in$ M.

Example 3.1. Suppose the dimension n of M is 2, so we have a basis $\{e_1, e_2\}$. Given any x $\in$ M, there are $x_1, x_2 \in$ k so that $x = x_1 e_1 + x_2 e_2$. We have

$$\begin{aligned} x \wedge y &= (x_1 e_1 + x_2 e_2) \wedge (y_1 e_1 + y_2 e_2) \\ &= x_1 y_1 (e_1 \wedge e_2) + x_1 y_2 (e_1 \wedge e_2) + x_2 y_1 (e_2 \wedge e_1) + x_2 y_2 (e_2 \wedge e_2) \\ &= (x_1 y_2 - x_2 y_1) e_1 \wedge e_2 \end{aligned}$$

We observe that the coefficient of $e_1 \wedge e_2$ is the determinant of $\begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix}$. Hence, we introduce another useful interpretation of exterior product in our use.

Definition 3.6. Let $e_k = (0, ..0, 1, 0, ..0) \in \mathbb{R}^n$, and $x_1 ... x_n$ be n vectors in $\mathbb{R}^n$ $x_1 \wedge ... \wedge x_n$ = c $e_1 \wedge ... \wedge e_n$, and c is the determinant of the matrix $\begin{bmatrix} a_{1_1} & a_{1_2} ... & a_{1_n} \\ a_{1_1} & a_{2_2} ... & a_{2_n} \\ \\ a_{n_1} & a_{n_2} ... & a_{n_n} \end{bmatrix}$, where $x_j = \sum_{i=1}^{n} a_{ij} e_i$, j= 1, 2,.., n.

Theorem 3.1. *The dimension of $\wedge^d M$ is $\binom{n}{d}$, with a basis given by vectors of the form $e_{i_1} \wedge e_{i_2} \wedge ... \wedge e_{i_d}$ with $1 \leq i_1 < i_2 < ... < i_d \leq n$. When $d = n$ the space $\wedge^d M$ is one dimensional, and for $d > n$ the space $\wedge^d M = 0$.*

Proof. This is only a sketch of prove that convey the main idea. The formal proof of this theorem is more technical. Fixed a basis $\{v_1, ..., v_n\}$ for M, and consider the set $\{v_{i_1} \wedge ... \wedge v_{i_d} | 1 \leq i_1 < ... < i_d \leq n\}$. This set forms a basis for $\wedge^d M$. Given the rules of exterior product, we can see that $\wedge^d M$ is a vector space of dimension $\binom{n}{d}$. □

Plucker embedding is defined as the map in the following:

$$\phi : Gr_{d,M} \mapsto \mathbb{P}(\wedge^d M)$$

Given a subspace W $\in G_{d,V}$ and a basis $\{w_1, w_2, ..., w_d\}$ of W, Plucker embedding map W to $w_1 \wedge ... \wedge w_d$. Even though different choices of basis will give different wedge product, we will show that this transformation is defined in $\mathbb{P}(\wedge^d M)$ by following lemma. In other words, the wedge product of different selection of basis differ by scalar multiplication. We will also show that this transformation is injective, i.e two linear code are the same if and only if the coordinate of Grassmannian varieties are equivalent.

Lemma 3.1. *Let W be a subspace of a finite dimensional $\mathbb{k}$ -vector space M, and let $\mathcal{B}_1 = \{w_1, ..., w_d\}$ and $\mathcal{B}_2 = \{v_1, ..., v_d\}$ be two bases for W. Then $v_1 \wedge ... \wedge v_d = \lambda w_1 \wedge ... \wedge w_d$ for some $\lambda \in k$.*

Proof. Write $w_j = a_1 v_1 + ... + a_{dj} v_d$. Then

$$\begin{aligned} w_1 \wedge ... \wedge w_d &= (a_{11} v_1 + ... + a_{d1} v_d) \wedge ... \wedge (a_{1d} v_1 + ... + a_{dd} v_d) \\ &= \sum_{\sigma \in S_d} \epsilon(\sigma) a_{1\sigma(1)} ... a_{d\sigma(d)} v_1 \wedge ... \wedge v_d \end{aligned}$$

where $\epsilon(\sigma)$ is the sign of σ. $\sum_{\sigma \in S_d} \epsilon(\sigma) a_{1\sigma(1)} a_{d\sigma(d)}$ is the determinant of the change of basis matrix from $\mathcal{B}_1$ to $\mathcal{B}_2$. □

Proposition 3.1. $\phi : Gr_{d,M} \mapsto \mathbb{P}(\wedge^d M)$ is injective.

Proof. Define a map

$$p : \mathbb{P}(\wedge^d M) \mapsto G_{d,M}$$

$$\forall [w] \in \mathbb{P}(\wedge^d M), p([w]) = \{v \in M | v \wedge w = 0 \in \wedge^{d+1} V\}$$

We want to show that the composition of function $\phi \circ p$ is id. Let $W \in G_{d,n}$ has basis $\{w_1, ..., w_d\}$ so that $[w_1 \wedge ... \wedge w_d] = p(W)$. Then for each $w \in W$, $w \wedge w_1 \wedge ... \wedge w_d = 0$. Extend the linearly independent set$\{w_1 ... w_d\}$ to a basis $\{w_1 ... w_n\}$ for M. Then writing

$$v = \sum a_i w_i, (\sum a_i w_i) \wedge w_1 \wedge ... \wedge w_n = 0$$

After distributing and using the properties of the wedge product, we see that all the $a_i = 0$ for $i > d$ and thus $v = a_1 w_1 + ... + a_d w_d$. Therefore, $v \in W$ and $\phi \circ p \in W$, completing the proof that $\phi \circ p = id$ □

The following lemma prove that the coordinates of Grassmannian varieties are maximal minor of generator matrix, which is helpful for our use.

Proposition 3.2. The i^{th} homogeneous coordinate for $\phi(W) \in \mathbb{P}^n$ is given by the corresponding $d \times d$ minor of M_W.

Proof. Let $I_{d,n} = \{\bar{i} = (i_1, ..., i_d) | 1 \leq i_1 < ... < i_d \leq n\}$ and index the coordinates of $\mathbb{P}^{\binom{n}{k}-1}$ by $I_{d,n}$. More specifically, let the basis vector of $\mathbb{P}^{\binom{n}{k}-1}$ indexed by $\bar{i} = (i_1, ..., i_d)$ be $v_{i_1} \wedge ... \wedge v_{i_d}$. Given a subspace W $\in G_{d,n}$, choose a basis $\{w_1, ..., w_d\}$ for the subspace W. We write each w_j in terms of the basis vectors for V as $w_j = a_{1j} v_1 + ... + a_{nj} v_n$. Define an n$\times$ d matrix M_W by $M_W = (a_{ij})$. Note that the j-th column of M_W is the coordinates of w_j. Then p: W $\mapsto [w_1 \wedge w_2 \wedge ... \wedge w_d]$ and

$$\begin{aligned} w_1 \wedge ... \wedge w_d &= (a_{11} v_1 + ... + a_{d1} v_d) \wedge ... \wedge (a_{1d} v_1 + ... + a_{dd} v_d) \\ &= \sum_{\bar{i} \in I_{d,n}} \sum_{\sigma \in S_d} \epsilon(\sigma) a_{i_1 \sigma(1)} ... a_{i_d \sigma(d)} v_{\bar{i}} \end{aligned}$$

Where $\epsilon(\sigma)$ denotes the sign of the permutation of σ. The i-th coordinate for $p(W)$ is $p_{\bar{i}} = det(M_{\bar{i}})$ where $M_{\bar{i}}$ is the $d \times d$ submatrix formed from the $i_1 ... i_d$ rows of M_W □

3.3 Basic Topology and Zariski topology

Definition 3.7. A topology on a set X is a collection U of subsets of X which satisfies:

1. $\emptyset$ and X are in U
2. U is closed under finite intersection
3. U is closed under arbitrary union

Members of U are called the *openset* of the topology. There is an equivalent formulation using closed sets, which is the complement of an open set - a finite union of closed sets is closed, as is any intersection of closed sets.

Zariski topology is a kind of topology on $\Bbbk^n$ in which the closed sets are affine varieties. We can check that it satisfies the definition of topology.

$$V(\Bbbk[X]) = \emptyset$$

$$V(0) = \mathbb{A}^n$$

Hence it is enough to check that the finite union and arbitrary intersection of closed sets is closed. Given $I, U \subset \Bbbk[X]$, $V(I), V(U)$ are closed sets in the topological space.

$$V(I) \cap V(U) = V(IU)$$

$$V(I) \cup V(U) = V(I + U)$$

Hence, the set of affine varieties is a topological space. In the following, we will show that the coordinates of Grassmannian under Plucker embedding is a projective variety, hence it is also called Grassmannian varieties.

Theorem 3.2. *The Grassmannian $G(k, n) \subset \mathbb{P}(K^{\binom{n}{k}})$ is Zariski closed and irreducible.*

Proof. First let us assume that the matrix M_w representing W as of the form:

$$\left[\begin{array}{cccc|c} 1 & 0 & \dots & 0 & \\ 0 & 1 & \dots & 0 & A \\ \vdots & & \ddots & \vdots & \\ 0 & \dots & 0 & 1 & \end{array}\right]$$

where A is a $k \times (n-k)$ matrix. Each maximal minor of M_w is, up to sign, a minor of A of some size. Further, by Laplace expansion, a $q \times q$ minor of A for $q > 1$ may be expressed, as a quadratic polynomial, in terms of smaller minors. This gives us a collection of

$$\sum_{q=2}^{min(k,n-k)} \binom{k}{q}\binom{n-k}{q}$$

inhomogeneous quadratic equation in the entries of the $k \times (n-k)$ matrix A. This quadratic equation define the part of image of our map ϕ that lies in the affine open set $\Bbbk^{\binom{n}{k}-1} \subset \mathbb{P}(\Bbbk^{\binom{n}{k}})$ given by the nonvanishing of the first coordinate.
If $\phi(W)$ has its first coordinate zero then some other coordinate will be non-zero. Since W is a d dimensional subspace, the matrix M_w must have some invertible $k \times k$ submatrix. If we multiply M_w on the left by the inverse of that matrix then we obtain a matrix that looks like the matrix above but with its

columns permuted. This gives us a system of $\sum_{q=2}^{min(k,n-k)} \binom{k}{q}\binom{n-k}{q}$ inhomogeneous quadratic equations in the $k \times (n-k)$ entries of the new matrix A.
Each of the quadratic equation in $k \times (n-k)$ variables obtained above can be written as a homogeneous quadratic equation in the $\binom{n}{k}$ coordinates on $\mathbb{P}(K^{\binom{n}{k}})$. The collection of all these homogeneous quadratic equations gives a full polynomial description of $G(k,n)$.
The Grassmannian $G(k,n)$ is an irreducible subvariety of $\mathbb{P}(\Bbbk^{\binom{n}{k}})$ because it is the image of a polynomial map ϕ, namely the image of the space $\Bbbk^{k\times n}$ of all $k \times n$ matrices under taking all maximal minors. □

4 Isometric code and Grassmannian varieties

Definition 4.1. A *metric space* is a set X together with a function d (called a *metric* or distance function) which assign a real number $d(x,y)$ to every pair $x, y \in X$ satisfying the axioms below:

1. $d(x,y) > 0$ and $d(x,y) = 0 \iff x = y$
2. $d(x,y) = d(y,x)$
3. $d(x,z) \leq d(x,y) + d(y,z)$

Theorem 4.1. *The function:*

$$d : \mathbb{F}^n \times \mathbb{F}^n \mapsto \mathbb{N} : (u,v) \mapsto |\{i | i \in n, u_i \neq v_i|$$

is a metric on the vector space $\mathbb{F}^n$, called the Hamming metric.

Proof. We can check that this function satisfies, for all u, v, w $\in \mathbb{F}^n$: by definition of Hamming distance, number of different coordinate is a positive integer; if the number of coordinate u and v differ is 0, then u = v, hence

$$d(u,v) = 0 \iff u = v$$

Similarly,

$$d(u,v) = d(v,u)$$

By lemma 2.1, the following holds,

$$d(u,v) \leq d(u,w) + d(w,v)$$

□

An isometry between two linear code is defined on Hamming distance as follows.

Definition 4.2. Two linear codes $\mathcal{C}, \mathcal{C}' \subseteq Gr(k,n)$ are called isometric if there exists an isometry ι that maps $\mathcal{C}$ onto $\mathcal{C}'$, where ι is defined as:

$$\iota : Gr(k,n) \mapsto Gr(k,n)$$

$$d(u,w) = d(\iota(u), \iota(w)), \forall u, w \in Gr(k,n)$$

Definition 4.3. Two linear codes $C, C' \subset Gr(k,n)$ are *permutationally equivalent* if there exists a permutational isometry of $Gr(k,n)$ that maps C onto C', i.e there is a permutation π in the symmetric group S_n such that

$$C' = \pi(C) = \{\pi(c)|c \in C\}, d(c,\tilde{c}) = d(\pi(c),\pi(\tilde{c}))$$

$\forall c, \tilde{c} \in C$, where

$$\pi(c) = \pi(c_0, ..., c_{n-1} := (c_{\pi^{-1}(0)}, ..., c_{\pi^{-1}(n-1)})$$

Two isometric codes need not be permutationally equivalent codes, hence we generalize this definition into a more general one, i.e linear isometric code.

Definition 4.4. Two linear codes $\mathcal{C}, \mathcal{C}' \subseteq$ Gr(k, n) are called linear isometric if there exists a linear isometry of Gr(k, n) that maps $\mathcal{C}$ onto $\mathcal{C}'$

Definition 4.5. Consider an action ${}_GX$ and a group H. The *wreath product* of H with G, with respect to ${}_GX$, consist of the set

$$H \wr_X G := H^X \times G = \{(\varphi; g)|\varphi : X \mapsto H, g \in G\},$$

with multiplication defined by

$$(\varphi; g)(\varphi'; g') := (\varphi\varphi'_g; gg')$$

where $(\varphi\varphi'_g)(x) := \varphi(x)\dot{\varphi}'_g(x)$ and $\varphi'_g(x) := \varphi'(g^{-1}x)$, for $x \in X$.

Proposition 4.1. Take H the multiplicative group $\mathbb{F}_q^*$ of the field F_q. Let G be the symmetric group S_n acting on the set $n = \{0, 1, ..., n-1\}$, then the group of linear isometries of the Hamming space is given by:

$$H \wr_X G := \mathbb{F}_q^* \wr_n S_n = \{(\varphi; \pi)|\varphi : n \mapsto \mathbb{F}_q^*, \pi \in Sn\}.$$

The action on $\mathbb{F}_q^n$ is given in the following way:

$$\mathbb{F}_q^* \wr_n S_n \times \mathbb{F}_q^n \mapsto \mathbb{F}_q^n : ((\varphi; \pi), v) \mapsto (\varphi(0)v_{\pi^{-1}(0)}, ..., \varphi(n-1)v_{\pi^{-1}(n-1)})$$

Proof. Any linear map is defined by the images of the unit vectors. Since linear isometric preserve the Hamming weight, a unit vector $e^{(i)}$ is mapped to a nonzero multiple of a unit vector, i.e:

$$\iota(e^{(i)}) = \kappa_j e^{(j)}, for suitable j \in n, \kappa_j \in \mathbb{F}_q^* := \mathbb{F}_q \setminus 0$$

Moreover, the sum of two different unit vectors is of weight 2, and so different unit vector are mapped under ι to nonzero multiples of different unit vectors. Hence there exists a unique permutation π in the symmetric group S_n and a unique mapping ϕ from n=0,...,n-1 to $\mathbb{F}_q^*$ such that

$$\iota(e^{(i)} = \varphi(\pi(i))e^{(\pi(i))}$$

In terms of these mappings, applying ι to v:= $\sum_{i\in n} v_i e^{(i)}$ gives

$$\iota(v) = (\varphi;\pi)(v) = \sum_{i\in n} v_i \varphi(\pi(i)) e^{(\pi(i))} = \sum_{i\in n} \varphi(i) v_{\pi^{-1}(i)} e^{(i)}$$

i.e

$$(\varphi;\pi)((v_0,...,v_{n-1})) = (v_0,...v_n)\cdot M^T_{(\varphi;\pi)}$$

where $M_{(\varphi;\pi)}$ is the matrix whose k-th column is zero except for the (i, k)-entry which is $\varphi(i)$. Here i = $\pi(k)$, so that

$$M^T_{(\varphi;\pi)} = \begin{pmatrix} & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \dots & 0 & \phi(i) & 0 & \dots 0 & \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{pmatrix} i = \pi(k)$$

□

Theorem 4.2. *1. Assume that $\mathbb{F}_q^{k\times n,k}$ denotes the set of all $k \times n$ matrices of rank k over $\mathbb{F}_q$, $k \geq 1$, and $GL_k(q)$ the set of all regular $k \times k$ matrices over $\mathbb{F}_{||}$. The set of all generator matrices of the linear (n, k)-code $\mathcal{C}$ with generator matrix $\Gamma \in \mathbb{F}_q^{k\times n,k}$ is the orbit $GL_k(q)(\Gamma) = B\cdot\Gamma|B \in GL_k(q)$. Whence the set of all linear (n, k)-codes over $\mathbb{F}_q$, indicated it as $\mathcal{U}(n, k, q)$, can be identified with*

$$GL_k(q)\backslash\backslash\mathbb{F}_q^{k\times n,k}$$

2. The linear isometry group $M_n(q)$ acts on $\mathcal{U}(n, k, q)$, $k \geq 1$, according to

$$M_n(q)\times\mathcal{U}(n,k,q) \mapsto \mathcal{U}(n,k,q) : (M_{(\phi;\pi)},\mathcal{C}) \mapsto \{c\cdot M^T_{(\phi;\pi)}|c\in\mathcal{C}\}$$

The linear isometry class of the linear (n,k)-code C is the orbit

$$M_n(q)(\mathcal{C}).$$

Hence, the set of linear isometry class of linear (n,k)-codes is

$$M_n(q)\backslash\backslash\mathcal{U}(n,k,q)$$

3. The direct product $(GL_k(q)\times M_n(q))$, $k \geq 1$, acts on $\mathbb{F}_q^{k\times n,k}$ by

$$(GL_k(q)\times M_n(q))\times\mathbb{F}_q^{k\times n,k} \mapsto \mathbb{F}_q^{k\times n,k} : ((B, M_{(\phi;\pi)}),\Gamma) \mapsto B\cdot\Gamma\cdot M^T_{\phi;\pi}$$

and so the set of linear isometry classes of linear (n, k)-codes corresponds to the set of orbits

$$(GL_k(q)\times M_n(q))\backslash\backslash\mathbb{F}_q^{k\times n,k} : ((B, M_{(\phi;\pi)})$$

Proposition 4.2. In $\mathbb{F}_2$, linearly isometric is equivalent to permutationally isometric.

Proof. From proposition 4.1, we see that the mapping of unit vector in $\mathbb{F}_2$ is the identity map. Hence, φ is id and π is the symmetry group. □

Proposition 4.3. In $\mathbb{F}_2$, linear isometric code will have same Hamming weight of Grassmannian variety.

Proof. From proposition 3.2 and theorem 3.1 we proof that coordinates of Grassmannian varieties are maximal minor of M_w, and the set $\{v_{i_1} \wedge ... \wedge v_{i_d} | 1 \leq i_1 < ... < i_d \leq n\}$ forms a basis for $\wedge^d(V)$. From proposition 4.2, we prove that in $\mathbb{F}_2$, linearly isometric code is equivalent to permutational isometric code. Hence permutation of column of M will only permute the coordinates of Grassmannian varieties while the number of number coordinates in Grassmannian varieties leaves unchanged. □

Last but not the least, we can generalize the concept of linear isometric by relaxing the condition of *linearity*.

Definition 4.6. The mapping $\sigma : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ is called *semilinar* if there exist an automorphism α of $\mathbb{F}_q$ such that, for all $u, v \in \mathbb{F}_q^n$ and all $\kappa \in \mathbb{F}_q$ we have

$$\sigma(u+v) = \sigma(u) + \sigma(v), \sigma(\kappa u) = \alpha(\kappa)\sigma(u).$$

Lemma 4.1. *If the isometry $\iota : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n, n \geq 3$, maps subspace onto subspaces, then for each $u \in \mathbb{F}_q^n$ we have*

$$\iota(\mathbb{F}_q^*(u)) = \mathbb{F}_q^*(\iota(u))$$

Moreover, there exists an automorphism α of $\mathbb{F}_q$ such that, for each $\kappa \in \mathbb{F}_q$,

$$\iota(\kappa u) = \alpha(\kappa)\iota(u)$$

Proof. 1. First we consider the case $u = 0$. Since ι maps subspaces onto subspaces, the space $\{0\}$ must be mapped onto itself. Therefore, the assertion is true for $u = 0$

2. Assume that $u \neq 0$. Since ι is bijective and it maps subspaces to subspaces, $\iota(\langle u \rangle)$ is a one-dimensional subsapce, and so, using $\iota(u) \neq 0$, we have $\iota(\langle u \rangle) = \langle \iota(u) \rangle$. Moreover, as $\iota(0) = 0$,

$$\iota(\mathbb{F}_q^*(u)) = \mathbb{F}_q^*(\iota(u)).$$

Hence, there is a permutation of the scalars $\phi_u \in S_{\mathbb{F}_q^*} \leq S_{\mathbb{F}_q}$, depending possibly on the vector u, which satisfies

$$\iota(\kappa u) = \phi_u(\kappa)\iota(u)$$

The following shows that ψ_u is independent of u and that it is a field automorphism.

3. For the special case $e := \sum_{i\in n} e^{(i)}$ we have

$$\iota(\kappa e) = \phi_e(\kappa)\iota(e) = \phi_e(\kappa)\sum_{i\in n}\psi(\pi(i))(1)e^{(\pi(i))}, \kappa \in \mathbb{F}_q^*,$$

as well as

$$\iota(\kappa e) = \sum_{i\in n}\psi(\pi(i))(\kappa)e^{(\pi(i))}, \kappa \in \mathbb{F}_q^*,$$

so we obtain

$$\forall i \in n : \phi_e(\kappa) = \frac{\psi(\pi(i))(\kappa)}{\psi(\pi(i))(1)}, \kappa \in \mathbb{F}_q^*.$$

4. The following prove that $\phi_e(\kappa\mu) = \phi_e(\kappa)\phi_e(\mu)$, for $\kappa, \mu \in \mathbb{F}_q$. The assertion is trivial for $\kappa = 0$ or $\mu = 0$. Hence we restrict attention to$\kappa, \mu \in \mathbb{F}_q^*$. First, we consider a special case: Let $w := e^(0) + \mu e^(i)$, for $i \neq 0$ and $\mu \in \mathbb{F}_q^*$. The corresponding equation $\iota(\kappa w) = \phi_w(\kappa)\iota(w), \kappa \in \mathbb{F}_q^*$, implies that

$$\psi(\pi(0))(\kappa)e^{(\pi(0))} + \psi(\pi(i))(\kappa\mu)e^{(\pi(i))}$$
$$= \phi_w(\kappa)(\psi(\pi(0))(1)e^{\pi(0)} + \psi(\pi(i))(\mu)e^{(\pi(i))})$$

Comparing the coefficients of the basis vectors on both sides get two useful identities. The coefficient of $e^(\pi(0))$ give

$$\psi(\pi(0))(\kappa) = \phi_w(\kappa)\psi(\pi(0))(1),$$

so that we can deduce

$$\phi_w(\kappa) = \frac{\psi(\pi(0))(\kappa)}{\psi(\pi(0))(1)} = \phi_e(\kappa), \kappa \in \mathbb{F}_q^*$$

and hence $\phi_w = \phi_e$ in this particular situation. The second identity, obtained by comparing the coefficient of $e^(\pi(i))$, is

$$\psi(\pi(i))(\kappa\mu) = \phi_w(\kappa)\psi(\pi(i))(\mu).$$

Using $\phi_w = \phi_e$ and dividing both sides by $\psi(\pi(i))(1)$ we derive that

$$\phi_e(\kappa\mu) = \phi_e(\kappa)\phi_e(\mu), \kappa\mu \in \mathbb{F}_q^*,$$

hence in this special case, ϕ_e is multiplicative.

5. Now consider the case when $u \neq 0$, we want to show that $\phi_u = \phi_e$. For $u = \sum_{i\in n} u_i e^{(i)}$ we get

$$\iota(u) = \sum_{i\in n}\iota(u_i e^(i)) = \sum_{i\in n}\psi(\pi(i))(1)e^{\pi(i)}$$
$$= \sum_{i\in n}\phi_e(u_i)\psi(\pi(i))(1)e^{(\pi(i))}.$$

Since ϕ_e is multiplicative, we derive from $\kappa \in \mathbb{F}_q^*$ that

$$\begin{aligned}\iota(\kappa\mu) &= \sum_{i\in n} \phi_e(\kappa u_i)\psi(\pi(i))(1)e^{(\pi(i))} \\ &= \phi_e(\kappa)\sum_{i\in n} \phi_e(u_i)\psi(\pi(i))(1)e^{(\pi(i))} = \phi_e(\kappa\iota(u)),\end{aligned}$$

which can be compared with the identity

$$\iota(\kappa u) = \phi_u(\kappa)\iota(u),$$

obtaining $\phi_e(\kappa) = \phi_u(\kappa)$ for all $\kappa \in \mathbb{F}_q^*$. Hence we have proved that in fact $\phi_u = \phi_e$ as stated.

6. We also need to prove that ϕ_e is additive, i.e. $\phi_e(\lambda+\mu) = \phi_e(\lambda) + \phi_e(\mu)$, $\lambda, \mu \in \mathbb{F}_q$. Since $\phi_e(0) = 0$, this formula is true for $\lambda = 0$, or$\mu = 0$. By assumption $n \geq 3$, and so we consider

$$u := e^{(0)} + e^{(1)}, w := e^{(1)} + e^{(2)}$$

and the subspace $\mathcal{U} := \langle\{u, w\}\rangle$ generated by these two vectors. For $\lambda, \mu \in \mathbb{F}_q^*$, the vectors $\iota(\lambda u), \iota(\mu w)$ and $\iota(\lambda u) + \iota(\mu w)$, then

$$\begin{aligned}\iota(z) = \phi_e(\lambda)\psi(\pi(0))(1)e^{\pi(0)} + \phi_e(\lambda)\psi(\pi(1))(1)e^{\pi(1)} \\ +\phi_e(\mu)\psi(\pi(1))(1)e^{\pi(1)}) + \phi_e(\mu)\psi(\pi(2))(1)e^{\pi(2)}.\end{aligned}$$

Since $\psi(\pi(i))(1) \neq 0$, we derive from these two representations of $\iota(z)$ that $\phi_e(z_0) = \phi_e(\lambda)$ and $\phi_e(z_2) = \phi_e(\mu)$. Since ϕ_e is a bijective on $\mathbb{F}_q$, we obtain $z_0 = \lambda, z_2 = \mu$ and

$$\phi_e(\lambda) + \phi_e(\mu) = \phi_e(z_0 + z_2) = \phi_e(\lambda + \mu),$$

it completes the proof of the additivity.

7. Hence $\alpha := \phi_e$ is in fact an automorphism of $\mathbb{F}_q$ which satisfies

$$\iota(\kappa u) = \alpha(\kappa)\iota(u), \kappa \in \mathbb{F}_q, u \in \mathbb{F}_q^n.$$

Finally,

$$\begin{aligned}\iota(u+v) &= \iota(\sum_{i\in n}(u_i + v_i)e^{(i)}) \\ &= \sum_{i\in n} \iota((u_i + v_i)e^{(i)}) \\ &= \sum_{i\in n} \alpha(u_i + v_i)\psi(\pi(i))(1)e^{\pi(i)} \\ &= \sum_{i\in n} \alpha(u_i)\psi(\pi(i))(1)e^{\pi(i)} + \sum_{i\in n} \alpha(v_i)\psi(\pi(i))(1)e^{\pi(i)} \\ &= \iota(u) + \iota(v)\end{aligned}$$

□

Follow from lemma 4.1

Theorem 4.3. *For $n \leq 3$, the isometries of $\mathbb{F}_q^n$ which map subspaces onto subspaces are exactly the semiliear mapping of the form $(\varphi; (\alpha, \pi))$, where $(\varphi; \pi)$ is a linear isometry and α is a field automorphism. These mapping form a group, the group of semilinear isometries.*

Definition 4.7. Two (n,k)-codes $\mathcal{C}$ and $\mathcal{C}'$ over $\mathbb{F}_q$ are called semilinarly isometric if and only if there exists an automorphism α in $\mathrm{Aut}(\mathbb{F}_q)$ and a linear isometry $(\varphi; \pi)$ in $\mathbb{F}_q^* \wr_n S_n$, such that the mapping:

$$(c_0, ..., c_{n-1}) \mapsto (\phi(0)\alpha(c_{\pi^{-1}(0)}), ..., \phi(n-1)\alpha(c_{\pi^{-1}(n-1)}))$$

maps $\mathbb{C}$ onto $\mathbb{C}'$. The orbits of the group of semilinear isometries on the set of subspaces of H(n,q) are the semilinear isometry classes of linear codes of length n over $\mathbb{F}_q$.

References

[1] Shannon. C *A mathematical theory of communication* ACM SIGMOBILE Mobile Computing and Communications Review, vol.5, no.1, ACM, 1/1/2001, pp. 3–55, doi:10.1145/584091.584093

[2] Hungerford, Thomas W. *Abstract Algebra* Brooks/Cole. 2014.

[3] Pless, Vera. *Fundamentals of Error-Correcting Codes* Cambridge University Press. 2003.

[4] Drew A. Hudec *The Grassmannian as a Projective Variety.* University of Chicago REU 2017

www.math.uchicago.edu/ may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Hudec.pdf

[5] Mateusz Michalek *Linear Spaces and Grassmannians* Notes for the lecture on May 08, 2018, in the IMPRS Ringvorlesung *Introduction to Nonlinear Algebra* https://personal-homepages.mis.mpg.de/michalek/may08.pdf

[6] Schenck, Hal. *Computational Algebraic Geometry.* Vol. 58, Cambridge University Press, 2003.

[7] Cohen, Arjeh M, et al. *Error-Correcting Linear Codes* Vol. 18, Springer Berlin / Heidelberg, 2006, doi:10.1007/3-540-31703-1.