ARITHMETIC CONSTRUCTIONS OF BINARY SELF-DUAL CODES

Ying Zhang

A Dissertation

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

2013

Advisor's Name
Supervisor of Dissertation

Graduate Chair's Name
Graduate Group Chairperson

Acknowledgments

ABSTRACT

ARITHMETIC CONSTRUCTIONS OF BINARY SELF-DUAL CODES

Ying Zhang

Advisor: Ted Chinburg

Contents

Chapter 1

Introduction

The goal of this thesis is to explore the interplay between binary self-dual codes and étale cohomology of arithmetic schemes. In chapter 2, we will recall some definitions and general facts of codes. A construction of binary self-dual code is introduced in chapter 3 using arithmetics of the rational number field $\mathbb{Q}$ (which we call *Construction* $\mathbb{Q}$). Construction $\mathbb{Q}$ shows that up to equivalence, all binary self-dual codes have a simple description (not necessarily unique) using a *boxed matrix*, see table 3.1. Starting from chapter 4, the focus of the thesis will be mainly on arithmetic questions inspired by the search of binary self-dual codes. Two more constructions of binary codes are introduced and compared, which we call *Construction G* and *Equivariant Construction*.

From the historic point of view, the study of the interplay between discrete structures and cohomology theory has been very fruitful. As is well known, in 1982

M. Freedman showed that for each unimodular symmetric bilinear form over $\mathbb{Z}$, there is a simply-connected compact 4-manifold M whose intersection form

$$H^2(M,\mathbb{Z}) \times H^2(M,\mathbb{Z}) \to \mathbb{Z}$$

realizes this bilinear form [Fre82]. In fact, this bilinear form "almost determines" the homeomorphism type of the manifold M and puts restriction on when it has smooth structures [GS99].

For an involution τ on a closed manifold, it is well known the cohomology of the fixed loci is related to that of the manifold. In a series of recent papers by Puppe [Pup95], [Pup01], Kreck and Puppe [KP08], this relation is explored to construct binary self-dual codes when τ has isolated fixed points. For convenience of the reader, part of their work is reviewed in appendix A. In particular, we review two constructions of theirs: the *Topological Equivariant Construction* and *Poincaré Duality Construction*. It is these constructions that inspired our constructions over arithmetic schemes.

As a matter of fact, our Construction $\mathbb{Q}$ and Construction G are analogues to the Poincaré Duality Construction. The Equivariant Construction and Topological Equivariant Construction are developed in a common framework. This is not surprising since the classical motivation of étale cohomology is to seek "topological" treatment of schemes.

Never the less, the reader should be careful about some subtle differences that lie between the topological and arithmetic sides of the story. For an involution on a

closed manifold with isolated fixed points, the Topological Equivariant Construction and Pioncaré Duality Construction give rise to the same binary self-dual code, see proposition A.0.10. In the arithmetic situation, the Equivariant Construction and Construction G do not necessarily produce the same code, as is shown in example 5.5.4. The arithmetic situation is different because when τ fixes closed points on an arithmetic scheme, a closed point has cohomological dimension higher than zero when the residue field is not separably closed. So a closed point on a scheme is analogous to a high dimension topological object rather than a topological point. There is also a technical difference in the Equivariant Constructions: while most theorems in the Topological Equivariant Construction are stated and proved up to homotopy type of (finite) CW complexes, we avoid the machinery of étale homotopy theory in this thesis. In stead, we use the modified equivaiant étale cohomology by B. Morin [Mor08] as a technical tool. This tool will help us build up the necessary results for the arithmetic equivariant construction, which in turn answers a question in example 5.5.4 that is raised by Construction G.

Chapter 2

Coding Theory Backgrounds

2.1 General Codes

In this section we will collect some terminologies in coding theory. The main purpose is to set up notations which will be used in later parts of the thesis. For a more complete introduction to the subject, the readers are referred to standard texts like [CS99, Chapter 3][PH][Ple98].

Let $\mathbb{F}$ be a finite set called the *alphabet*. An element in the set $\mathbb{F}^n$ is called a *word* of length n. A *code* C of *length* n is a subset of $\mathbb{F}^n$. If $\mathbb{F}$ has an additive group structure, then C is called *additive* if it is an additive subgroup. If $\mathbb{F}$ has a commutative ring structure, then C is called *linear* if it is additive and closed under scalar-multiplication by elements in $\mathbb{F}$. In this situation, $\mathbb{F}^n$ also has a natural ring structure defined by component-wise multiplication. But C is in general not

required to be a non-unital sub-ring. In this thesis we will only consider linear code over a field $\mathbb{F}$.

When C is a linear code in an n-dimensional space $W/\mathbb{F}$, we will assume W is equipped with a chosen set of basis E under which we can write $W = \mathbb{F}^n$. In the existing literature in coding theory, an n-dimension vector space W is often explicitly given as $\mathbb{F}^n$, with an assumed basis which becomes the canonical basis in $\mathbb{F}^n$. However, in our later constructions of codes from abstract cohomology space, a "canonical" basis is usually not obvious in W. In some cases, the existence of a desirable basis is even in question, see **??**.

Under the canonical basis in $\mathbb{F}^n$, consider a word $u = (u_1, \cdots, u_n)$. The *Hamming weight* of u is the number of nonzero components u_i, denoted by $wt(u)$. Given a code C, we can count the total number of words of each possible weight and store these counts in a vector, called the *weight distribution* vector of C.

For an n-dimensional $\mathbb{F}$ vector space W, $\langle\ ,\ \rangle$: $W \times W \to \mathbb{F}$ is a *non-degenerate bilinear form* if it satisfies the following conditions:

- $\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$.
- $\langle x, y + z\rangle = \langle x, y\rangle + \langle x, z\rangle$.
- if $\langle x, y\rangle = 0$ for all $y \in W$ then $x = 0$,
- if $\langle x, y\rangle = 0$ for all $x \in W$ then $y = 0$.

In addition, if $\forall x, y \in W$, $\langle x, y\rangle = \langle y, x\rangle$, then $\langle, \rangle$ is said to be *symmetric*.

Suppose $\mathbb{F}$ is equipped with an *involution* (which could be trivial), denoted by a bar, satisfying

$$\overline{\overline{x}} = x, \overline{x+y} = \overline{x} + \overline{y}, \overline{xy} = \overline{x}\ \overline{y}$$

We require

$$\langle x, y\rangle = \overline{\langle y, x\rangle}, \langle ax, y\rangle = \langle x, \overline{a}y\rangle$$

Given a non-degenerate bilinear form $\langle , \rangle$, for a code $C \subset W$, we can define its *dual code*

$$C^{\perp} := \{x \in W | \forall y \in C, \langle x, y\rangle = 0\}$$

If $C^{\perp} \subseteq C$, C is called *self-orthogonal*. When $C^{\perp} = C$, C is called self-orthogonal of *maximal dimension*.

Example 2.1.1 (Main Example). Under a basis E in an n-dimensional space $W/\mathbb{F}$, define the product of two words $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n)$ by

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i \bar{y}_i$$

This product satisfies the above requirements. For a bilinear form $\langle , \rangle$, if there is a basis E under which the form is defined as above, then $\langle , \rangle$ is called an *inner product*. When the involution is trivial, we will call it a *Euclidean inner product*; the basis E will be called a *Euclidean basis*. $\triangle$

In the main part of the thesis, we will only focus on the case when $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$ is the field of two elements. The involution is the identity.

2.2 Binary Self-dual Code

Consider an m dimension vector space W over $\mathbb{F}_2$ with a basis E. We can define the inner product associated to this basis. If C is an n dimensional self-orthogonal code of maximal dimension, then $m = 2n$ is even. We will require that E is specified as an *ordered* basis $\{e_i\}_{i=1}^m$. The triple (W, E, V) is called a *binary self-dual code* of length m.

For a code word over $\mathbb{F}_2$, the Hamming weight of the word is just the number of ones in the word. A word that is self-orthogonal has even weight. In addition, if the Hamming weight of each word in a binary self-dual code C is a multiple of 4, we will say C is a *Type II* code, or a *doubly even* code. If not, C is called a *Type I* code or a *singly even* code. If W has a Type II code contained in it, the dimension of W is necessarily a multiple of 8 [RS98].

Two self-dual codes (W, V, E), (W', V', E') are defined to be *equivalent* if there is a bijection between E and E' which when extended to an $\mathbb{F}_2$-linear isomorphism $W \to W'$ maps V to V'. Alternatively, fixing W, if there is a permutation of the basis E that maps V to V', then the two codes (W, E, V) and (W, E', V') are called equivalent. The permutations on the ordered basis E that map the space V to itself will constitute the *automorphism group* of the code. Obviously, the automorphism group of a code is a subgroup of the symmetric group S_{2n}. If V is equivalent to V', then their automorphism groups are conjugate to each other in S_{2n}.

Consider an invertible linear map A on W. If $\langle Ax, y\rangle = \langle x, A^t y\rangle = \langle x, y\rangle$, for

all $x, y \in W$ A is said to be an element in the *orthogonal group* $O(m)$ associated to $\langle , \rangle$. Under a basis E, A can be represented by an element in $GL_{m\times m}(\mathbb{F}_2)$.

Fixing E, a *generator matrix* is a matrix whose row vectors span a basis for a code. For example, a generator matrix for a binary self-dual code is an $n\times 2n$ matrix of rank n. Up to equivalence, every self-dual code has a generator matrix of the form $[I_n, P_n]$ where I_n is the $n \times n$ identity matrix, and $P_n \in O(n)$ is an orthogonal matrix. Let $O(2n)$ act on W by left multiplication. Since $O(n) \hookrightarrow O(2n)$ in the lower right corner, the action of $O(2n)$ is transitive on the set of self-orthogonal spaces V of maximal dimension. This explains why in the definition of equivalence relation we only consider a permutation rather than a general orthogonal change of basis: had we chosen the latter, the definition of equivalence class of codes would not be interesting.

Remark 2.2.1. A useful fact is that for the Euclidean form, $O(n)$ coincides with S_n if and only if $n \leq 3$. Indeed, when $n \leq 3$ it is obvious. An example for an element in $O(4) \setminus S_4$ is provided by the generator matrix for the length 8 binary self-dual code e_8. $\diamondsuit$

Denote by T_{2n} the set of all distinct self-dual codes of length $2n$. There is a simple counting formula

$$|T_{2n}| = \Pi_{i=1}^{n-1}(2^i + 1)$$

When m is divisible by 8, the total number of Type II codes is

$$2\Pi_{i=1}^{n-2}(2^i + 1)$$

Denote the orbit of C under the S_{2n} action by C_E. $|C_E| = \frac{|S_{2n}|}{|Aut(C)|}$. Thus we have:

$$|T_{2n}| = \sum_{\text{Inequivalent } C} \frac{|S_{2n}|}{|Aut(C)|} \tag{2.2.1}$$

We will define

$$p_C := \frac{|C_E|}{|T_{2n}|} \tag{2.2.2}$$

as the density of the equivalence class C_E in T_{2n}.

The following result of [OP92] is relevant. Denote the set of codes that have a non-trivial automorphism group by A_{2n}, then

Proposition 2.2.2 (Rigidity)**.**

$$\lim_{n\to\infty} \frac{|A_{2n}|}{|T_{2n}|} = 0$$

Therefore when n gets big, most codes have density $d_C = \frac{(2n)!}{|T_{2n}|}$.

Remark 2.2.3. One should use caution in such a statement. Based on [OP92] along, it does not qualify to say "most equivalence classes" have the above d_C, since codes with bigger automorphism groups could conceivably break up into more equivalence classes. The author have not seen this question being addressed in the literature. $\diamondsuit$

Equivalent to Equation 2.2.1, one can write

$$\sum_{\text{Inequivalent } C} \frac{1}{|Aut(C)|} = \frac{T_{2n}}{(2n)!} \tag{2.2.3}$$

Equation 2.2.3 is often called the *mass formula* in the literature.

When k is any number smaller than $\frac{1}{2}$, $\frac{T_n}{(2n)!}$ grows faster than e^{kn^2} for large n. Thus the number of inequivalent codes grows exponentially fast in n. The problem

of classifying inequivalent codes of given length is computationally costly. For the reader's interest, there are now several on-line databases of equivalence classes of binary self-dual codes. For example, A. Munemasa summarized on his website a complete list with length up to 40.

2.2.1 Extremal Code

Coding theory has interesting connections with other branches of mathematics, including combinatorial design, lattice theory and invariant theory [CS99, Chapter 3][PH][Ple98]. Codes are also used for *error-correcting* purposes in telecommunication. Some of the best error-correction codes are binary self-dual codes. For error-correction purposes, the relevant combinatorial property is the weight distribution of the code. In particular, its non-zero minimal weight is important, which is an even integer. For a code C of length $2n$, denote its minimal distance by d_{2n}. Two questions are of general interest:

Question 2.2.4. Fixing the length $2n$, what is the largest minimal weight d_{2n}?

Fixing length $2n$, we will call a code with the largest minimal weight an *extremal code*. When $2n$ range between $[56, 110]$, not all the extremal codes (or in some cases even the d_{2n}) are known [DGH97]. Other than the extremal codes, the existence of codes with other prescribed weight enumerators are also conjectured, leading to interesting questions as how to construct them. Existing techniques include beautiful but often sporadic combinatorial designs; gluing techniques using codes

with smaller length; or a systematic study of "descendants" of codes of smaller length. See the references listed above together with [KB12][BB11]. Based on our Construction $\mathbb{Q}$, we propose a "probabilistic" method of generating binary self-dual code, 3.4.

Question 2.2.5. What is $\limsup_{m\to\infty} \frac{d_m}{m}$?

For this question we quote the following result for a lower bound:

Proposition 2.2.6. *[RS98, section 10] There is an infinite sequence of codes C_i where the ratio $\frac{d_i}{m_i}$ is bounded below by an absolute constant, and $m_i \to \infty$.*

Chapter 3

Construction $\mathbb{Q}$

In this chapter we provide a construction of binary self-dual codes using arithmetic information over the rational number field $\mathbb{Q}$. We construct all equivalence classes of binary self-dual codes of length at least 4 in Theorem 3.3.1. The proof relies on finding a special presentation of the generator matrix for an equivalence class of codes, called a boxed matrix (see Table 3.1. This construction can be considered an arithmetic counterpart of [KP08, Prop 3.1] (or cite the the appendix.)

Notation: we will use p_i for a positive prime number or a prime ideal in $\mathbb{Z}$, v_{p_i} for the p-adic valuation of $\mathbb{Q}$. An equivalence class of valuations on a field is called a *place* of the field.

3.1 S-integers

Let K be a number field, S be a finite set of places of K including all the archimedean places. The ring of S-integers $\mathcal{O}_{K,S}$ is defined as follows:

$$\mathcal{O}_{K,S} = \{a \in K | \forall p \notin S, v_p(a) \geq 0\}$$

The unit group in $\mathcal{O}_{K,S}$ is denoted $\mathcal{O}_{K,S}^*$. When S only has archimedean places, $\mathcal{O}_{K,S} = \mathcal{O}_K$. Naturally $S_1 \subseteq S_2$ implies $\mathcal{O}_{K,S_1} \subseteq \mathcal{O}_{K,S_2}$ and $\mathcal{O}_{K,S_1}^* \subseteq \mathcal{O}_{K,S_2}^*$.

Denote the multiplicative group of roots of unity in K by μ_K; the set of finite places in S by S_f. If K has r_1 embeddings into the field of real numbers, r_2 embeddings into the complex numbers, then [Mil11, Chapter 5]

$$rank_{\mathbb{Z}} \mathcal{O}_{K,S}/\mu_K = r_1 + r_2 - 1 + |S_f| \tag{3.1.1}$$

Notation: for a finite set like S_f, we use $|S_f|$ to represent the cardinality of the set.

3.2 Hilbert Symbols

Let k be any field. For a, $b \in k^*$, we can define the multiplicative Hilbert symbol (a, b) with values in ± 1 in the following way:

- $(a, b) = 1$ if the quadratic form $z^2 - ax^2 - by^2 = 0$ is isotropic; in other words, there is a non-zero solution $(x, y, z) \in k^3$;
- $(a, b) = -1$ otherwise.

It is readily seen from the definition that the Hilbert symbol is a map from $k^*/(k^*)^2 \times k^*/(k^*)^2 \to \pm 1$. An equivalent way to characterize the Hilbert symbol is that $(a, b) = 1$ if and only if a belongs to the group $Nm(k(\sqrt{b}))$ in k^*, i.e. it is a norm in the quadratic extension $k(\sqrt{b})/k$ [Ser73, Chapter III].

The Hilbert symbol satisfies the following properties:

- $(a, b) = (b, a)$, $(a, c^2) = 1$.
- $(a, -a) = 1$, $(a, 1 - a) = 1$.
- $(aa', b) = (a, b)(a', b)$.

If the multiplicative groups $k^*/(k^*)^2$ and $\{\pm 1\}$ are interpreted additively, the Hilbert symbol is a non-degenerate bilinear form over $\mathbb{F}_2$.

In this thesis, we will only consider the Hilbert symbols over a local field $K_\mathfrak{p}$ of characteristic different from 2. In addition, if the residue characteristic of $K_\mathfrak{p}$ is different from 2, the Hilbert symbol has a simple description. $K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, which is spanned by a uniformizer $\mathfrak{p}$ and a non-square unit u over $\mathbb{F}_2$. Under the basis $\{\mathfrak{p}, \mathfrak{p}u\}$, the Gram-matrix of the Hilbert symbol is:

$$\begin{pmatrix} (\mathfrak{p}, \mathfrak{p}) & (\mathfrak{p}, \mathfrak{p}u) \\ (\mathfrak{p}u, \mathfrak{p}) & (\mathfrak{p}u, \mathfrak{p}u) \end{pmatrix}$$

Denote the residue field of K_p by $\mathbb{F}_\mathfrak{p}$. When $|\mathbb{F}_\mathfrak{p}| \equiv 3 \bmod 4$, the Gram matrix is the identity matrix I_2. The Hilbert pairing is a Euclidean inner product.

When $|\mathbb{F}_\mathfrak{p}| \equiv 1 \bmod 4$, the Gram matrix is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

We will call such a bilinear form *alternate*. In general, if $\forall x \in W$, $\langle x, x \rangle = 0$, the form is called an alternate form. The following theorem of Albert classified non-degenerate symmetric bilinear forms over any field of characteristic 2 [Alb38]:

(To avoid confusion, we reserve the symbol $\langle , \rangle$ for a bilinear form, and $(,)$ for the multiplicative Hilbert symbol.)

Theorem 3.2.1 (Albert)**.** *Over a field of characteristic* 2*,*

- *Any two alternate forms are equivalent, i.e. they differ by a change of basis.*
- *If a form is not an alternate form, then there is a change of basis such that the Gram-matrix is the identity matrix* I_n*.*

In particular, any non-degenerate symmetric bilinear form over an odd-dimensional vector space is Euclidean. For example, $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong \mathbb{F}_2^3$ has odd dimension. If we choose the basis $\{-2, -10, -5\}$, then the Gram-matrix for the Hilbert symbol is I_3. By remark 2.2.1, this basis is also unique up to permutations.

For the purpose of constructing binary self-dual codes, only fields where the Hilbert symbol induces a Euclidean form are considered. Based on theorem 3.2.1, when $k^*/(k^*)^2$ is finite dimensional over $\mathbb{F}_2$, we look for elements $x \in k^*$ such that $(x, x) = (x, -1) = -1$. This is true if and only if x is not a norm in $k(\sqrt{-1})/k$. By going over all elements $x \in k^*$, we have the following observation:

Corollary 3.2.2. *The Hilbert symbol is Euclidean if and only if $k(\sqrt{-1})/k$ is a non-trivial extension, i.e. -1 is a non-square in k^*.*

3.3 The Construction

Let S be a finite set of places of $\mathbb{Q}$ consisting of the infinite place ∞ (i.e. the archimedean place), the place determined by the prime 2, and the places determined by a finite set of positive primes $p_1, \ldots, p_{n-2}$ which are congruent to 3 mod 4. We will abuse notation and write 2 as p_{n-1}, ∞ as p_n ($\mathbb{Q}_{p_n} = \mathbb{R}$), thus $n \geq 2$. As discussed in Section 3.2, for each place $v_p \in S$, the Hilbert symbol on $\mathbb{Q}_p$ is Euclidean.

For notational convenience, denote the multiplicative group $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ as an additive vector space $W_p/\mathbb{F}_2$. Denote by $\langle , \rangle_{v_p}$ the bilinear form induced by the Hilbert pairing on W_p. The direct sum $W := \oplus_{v_p \in S} W_p$ is equipped with a non-degenerate symmetric pairing $\langle , \rangle : W \times W \to \mathbb{F}_2$,

$$\langle , \rangle = \sum_{v_p \in S} \langle , \rangle_{v_p}$$

A Euclidean basis E of W is provided by the union of the basis for each W_p. This basis will be used throughout the construction.

Consider the diagonal embedding Φ: $\mathbb{Z}_S^*/2 \to \oplus_{v_{p_i} \in S} \mathbb{Q}_{p_i}^*/2 \cong W$. From equation 3.1.1, $\mathbb{Z}_S^*/2$ has rank n. The following theorem characterizes its image:

Theorem 3.3.1. *(a) The diagonal embedding Φ is injective.*

(b) The image $\Phi(\mathbb{Z}_S^*)$ is a binary self-dual code in W.

(c) Up to equivalence, all binary self-dual codes (of length at least 4) can be obtained in this way.

Proof. Part (a) of the theorem follows from part (b). (b) follows from theorem 4.1.4 which proves a more general situation. However, since everything about Construction $\mathbb{Q}$ is so concrete, part (b) can also be seen from Table 3.1. We explain the table as follows:

$\mathbb{Z}_S^*$ is the subgroup of $\mathbb{Q}^*$ generated by $-1, 2, p_1, \ldots, p_{n-2}$. When p is odd, a rational integer l which is prime to p is a non-square in $\mathbb{Q}_p^*$ if and only if l is a non-square mod p. When l is a non-square in $\mathbb{Q}_p^*$, the corresponding image in W_p is $(1,1)$. When l is a square in $\mathbb{Q}_p^*$, the corresponding image is $(0,0)$.

The image of $\Phi(\mathbb{Z}_S^*)$ in W is the matrix indicated in Table 3.1. In this table there are three entries under W_2 because $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is a three dimensional vector space over $\mathbb{F}_2$. The entries for a given row in the matrix are the diagonal images from a global S-unit, which is listed to the left of the row.

We will view the $n \times 2n$ binary matrix M in Table 3.1 as an $n \times n$ block matrix $\tilde{M}$, where each block is a pair of elements (a_{2i}, a_{2i+1}). Properties of this matrix $\tilde{M}$ is summarized as follows:

(1) The bottom row of $\tilde{M}$ has all entries equal to (11).

(2) All entries of the last column of $\tilde{M}$ equal the (10) pair except for the (11) in the final row.

Table 3.1: A boxed code

places / S-units	W_{p_1}	W_{p_2}	$\cdots$	W_2		$W_{\mathbb{R}}$
	$\{-p_1, p_1\}$	$\{-p_2, p_2\}$	$\cdots$	$\{-2, -10, -5\}$		$\{-1\}$
p_1	01	00/11		00/11	1	0
p_2	11/00	01			1	0
$\vdots$	$\vdots$		$\ddots$		$\vdots$	$\vdots$
2	11/00			01	1	0
-1	11	11	$\cdots$	11	1	1

(3) The diagonal elements of $\tilde{M}$ are all (01) except for the final diagonal entry, which is equal to (11).

(4) All other pairs in $\tilde{M}$ are either (00) or (11), which we will call *identical pairs*.

We say that a block matrix having properties (1) - (4) is *half-boxed*. We will say that $\tilde{M}$ is *boxed* if the following is also true:

(5) For all $(n-1) \geq i > j \geq 1$, $b_{ij} + b_{ji} = (11)$.

By definition, a boxed matrix has rank n and its rows are orthogonal to each other in the Euclidean pairing. Thus it is a generator matrix for a binary self-dual code.

The fact that the image of $\Phi(\mathbb{Z}_S^*/2)$ in W is a boxed matrix is a straight forward observation. In particular, property 5 follows from Gauss's law of quadratic

reciprocity. Thus part (b) in theorem 3.3.1 is proved.

There is also a partial converse to the above statement, whose proof we omit:

Lemma 3.3.2. *If $\tilde{M}'$ is half-boxed, and its row vectors are orthogonal to each other, then condition (5) is automatically satisfied, i.e. $\tilde{M}'$ is boxed.*

Now we proceed to prove part (c) of theorem 3.3.1.

We begin by saying the word of all-ones (denoted $\bar{1}$) belongs to every binary self-dual code C, since $\bar{1}$ is orthogonal to all vectors of even weight. Suppose now that M is the generator matrix of a self-dual code C of length $2n$ and that the last row of M is $\bar{1}$. Observe that elementary row operations on M correspond to a change of basis for the code C. Column permutations send C to an equivalent code. We will show by induction on n that after applying a sequence of elementary row operations and column permutations to M, one can make the associated block matrix $\tilde{M}$ into half-boxed form. We will in fact show that this can be done without ever adding another row to the final row $\bar{1}$ of M. This will prove the theorem, since the above operations lead to codes equivalent to C by definition.

For $n = 2$ our claim is obvious. Now suppose $n > 2$, M is the generator matrix for a self-dual code C of length $2n$ and that the last row of M is $\bar{1}$. As the rows of M have full rank, the top row is neither all-zeros $\bar{0}$ nor $\bar{1}$. Therefore the columns of M can be permuted so that the pair on the upper-left corner of $\tilde{M}$ is (01). $\tilde{M}$ has the following form:

In the above table w is a column block-vector of length $n-1$, u is a row block-

Table 3.2: Block form of $\tilde{M}$

01	u
w	M'

vector with the same number of pairs, and $M' \in Mat_{(n-1)\times(2n-2)}$. By adding the top row of $\tilde{M}$ to the j-th row if necessary, where $2 \leq j < n$, we can assume that w consists only of identical pairs. Under this hypothesis, it is easy to check that M' represents a generator matrix of a self-dual code of length $2n-2$ with $\bar{1}$ in the bottom row. By the induction hypothesis, M' can be turned into half-boxed form by applying column permutations and row operations while keeping the bottom row. These same operations can be applied to the augmented matrix M, leading to a matrix whose lower right corner M' is in half-boxed form; the column block-vector w consists of identical pairs; the bottom row of $\tilde{M}$ remains $\bar{1}$.

Now we need to modify the top row u. Note that all diagonal entries of $\tilde{M'}$ are all of the form (01) except in the bottom row, and all other pairs in $\tilde{M'}$ are identical pairs except in the last column. Therefore the top row of $\tilde{M}$ can be added to by the 2rd through $(n-1)$th row in such a way that all pairs of u become identical pairs except possibly for the last pair. During these operations, only identical pairs have been added to the upper-left corner of M, thus it is either 01 or 10. As the weight of this first row is even, the last pair in u should also be either 01 or 10. Adding the bottom row to the top row if necessary, the last pair in u is 10. Finally, if the

upper-left corner of M is 10, it can be turned into 01 by permuting the first two columns of M. The block matrix $\tilde{M}$ is now in half-boxed form. Moreover, it is in fact boxed by lemma 3.3.2.

To complete the proof of (c), we only need to show that every boxed matrix $\tilde{M}$ can be realized by the Hilbert code associated to some set $S = \{2, \infty, p_1, \ldots, p_{n-2}\}$. To specify the odd p_i we begin by requiring their classes in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \times \mathbb{R}^*/(\mathbb{R}^*)^2$ as in the last two block columns of $\tilde{M}$. This can be done with p_i congruent to 3 mod 4. We now choose the p_i sequentially be requiring their residue classes mod p_j for $1 \leq j < i \leq n-2$ according to the entry b_{ij} in $\tilde{M}$. After this we have specified the lower triangular part of a boxed matrix. By Gauss's quadratic reciprocity, the image of these S-integers actually give a boxed matrix $\tilde{M}$ under our basis for the Hilbert symbols. Moreover, by the equidistribution of prime numbers in congruence classes, each self-dual code can be realized by this construction with an infinite number of distinct sets of places S. □

Example 3.3.3. When $S = \{\infty, 2, 3, 7\}$, one gets the Hamming code A_8.

When

$$S = \{\infty, 2, 7, 19, 31, 131, 179, 367, 883, 1223, 1307, 39079\}$$

one gets the Golay code G_{24}. △

Remark 3.3.4. to be modified:

It would also be interesting to see if boxed-matrix descriptions of codes are useful

in the topological context. In the following, we will assume that all involutions that we talk about reverse the orientation on an orientable manifold. Recall to prove every self-dual code can be realized by an involution on an orientable 3-manifold with isolated fixed points, a cobordism calculation involving $\Omega_2((\mathbb{R}P^\infty)^r)$ is used in [KP08]. The proof proceeds by showing that certain embedded surfaces in $(\mathbb{R}P^\infty)^r$ is the boundary of an embeddable 3-manifold. This is an existence proof. Thus to find explicit examples realizing the corresponding 3-manifold remains an interesting question. We remark that while boxed-matrix descriptions of codes may not be directly useful in finding involutions on 3-manifolds with isolated fixed points, it readily describes the situation when the components of the fixed loci are circles. In the quotient of the manifold by involution, there is an orbifold-neighborhood around each fixed circle whose boundary is a 2-dimensional non-orientable surface. Actually, for odd $p \equiv 3 \bmod 4$ the "étale surface" $\mathrm{Spec}(\mathbb{Q}_p)$ is in analogy with a Klein bottle, see section **??** for more discussions. Therefore, given a boxed-matrix, it is hopeful that we will use surgery to find a 3-manifold with an involution whose fixed loci are circles that realizes this box-matrix. This then gives the code.

On the other hand, for readers who are mainly interested on the arithmetic side, we remark that currently it is unknown to the author if the proof of [CZ12, Thm 1.5] could be viewed as an explicit "cobordism calculation" concerning the étale "surfaces" $\mathrm{Spec}(\mathbb{Q}_p)$ inside the étale "three-manifold" $\mathrm{Spec}(\mathbb{Z})$. $\diamondsuit$

3.4 A Random Generation Algorithm

The analysis of the previous section hints at an algorithm to generate all equivalence classes of binary self-dual codes of any fixed length $2n$. Namely, one can assign identical pairs b_{ij} in a block matrix $\tilde{M}$ for $1 \leq i < j \leq n-1$. Then $\tilde{M}$ can be completed to a boxed matrix which gives a binary self-dual code. Since the pairs b_{ij} for $1 \leq i < j \leq n-1$ can be either (11) or (00) freely at will, the algorithm can either exhaust all the $2^{\frac{n^2-n}{2}}$ possibilities, or it can decide b_{ij} by a coin tossing. The advantages of both algorithms are that they are not recursive on n.

The hard work remains, of course, to count the weight distribution of the codes generated; or to determine if two codes generated in this way are equivalent or not. Due to the exponential complexity in these two problems, we are more interested in the random algorithm than the exhaustive one. In fact, the random algorithm can quickly generate non-trivial (i.e. not a direct sum of codes of smaller length), or theoretically every binary self-dual codes of length $2n$.

If one is only interested in codes of small length ($2n \leq 60$), then the existing recursive algorithms mentioned in section 2.2.1 are appropriate. As toy examples, we also generated all binary self-dual codes of length less than 26 by implementing the random algorithm in MATLAB. For simplicity, we count the weight distribution of each outcome and compare it with the known table. The random generation process terminates when all codes in the table are obtained.

Remark 3.4.1. In view of the connection between self-dual codes and unimodular

lattices as stated in [KKM91], our algorithm also gives a quick way to construct a class of unimodular lattices. $\diamondsuit$

Interesting questions arise in the random generation algorithm. Suppose we assign the identical pairs b_{ij} by independently tossing a coin, then what is the probability of generating a certain equivalence class of codes? Suppose we assign the pair to be (11) when the coin tossing produces a head. The probability of producing a head by the coin is θ. When $\theta = \frac{1}{2}$ and n is small, experiments show that this probability is very close to the true densities p_C of the equivalence classes in T_{2n} defined in equation 2.2.2.

In fact, denote the set of binary self-dual codes that have a boxed generator matrix by D_{2n}. We can define the "boxed density" $\tilde{p}_C$ of an codes equivalent to C by

$$\tilde{p}_C = \frac{|C_E \cap D_{2n}|}{|D_{2n}|}$$

Table 3.3 compares p_C and $\tilde{p}_C$ for codes of length 8, 10, 12 where we adopt notations for certain codes of small length in [Ple72]

Table 3.3: Comparison of densities in length 8, 10, 12

	A_8	C_2^4	$A_8 \oplus C_2$	C_2^5	B_{12}	$A_8 \oplus C_2^2$	C_2^6
p_C	22.2%	77.8%	58.9%	41.1%	27.5%	58.8%	13.7%
$\tilde{p}_C$	25%	75%	62.5%	37.5%	29.7%	58.6%	11.7%

When the code length grows slight bigger, say $2n = 18$ and 20, then to calculate

$\tilde{p}_C$ would require a non-trivial amount of work. Therefore, for each length, we run a Monte-Carlo simulation by letting MATLAB randomly generate 10000 codes and count the frequencies that each equivalence class shows up:

Table 3.4: Comparison of densities in length 18

	H_{18}	$F_{16} \oplus C_2$	I_{18}	$D_{14} \oplus C_2^2$	$B_{12} \oplus C_2^3$	$A_8 \oplus C_2^5$	$\cdots$
p_C	47.30%	26.60%	12.16%	8.69%	3.55%	0.76%	$\cdots$
$\tilde{p}_C$	48.97%	26.18%	11.71%	8.45%	3.18%	0.64%	$\cdots$

Table 3.5: Comparison of densities in length 20

	R_{20}	M_{20}	$H_{18} \oplus C_2$	S_{20}	$F_{16} \oplus C_2^2$	$I_{18} \oplus C_2$
p_C	35.03%	23.65%	17.52%	9.85%	4.93%	4.50%
$\tilde{p}_C$	36.19%	23.91%	17.02%	10.12%	4.66%	3.59%
	L_{20}	$D_{14} \oplus C_2^3$	K_{20}	$B_{12} \oplus C_2^4$	$\cdots$	
p_C	2.14%	1.07%	0.66%	0.33%	$\cdots$	
$\tilde{p}_C$	2.34%	1.08%	0.57%	0.29%	$\cdots$	

In both Table 3.4 and 3.5, we did not complete the list when p_C and $\tilde{p}_C$ gets small. It can already be seen from the three tables that the proximity of p_C and $\tilde{p}_C$ does not seem a coincidence. Based on proposition 2.2.2, most codes have p_C equals to $\frac{(2n)!}{|T_{2n}|}$, we ask the following question:

Question 3.4.2. When $n \to \infty$, what is the behavior of $\tilde{p}_C$ for most codes of length $2n$?

On the above we have only considered random generation of codes based on a fair coin tossing, when experiments show that $\tilde{p}_C$ is quite close to p_C. However, we can also use a biased coin with probability θ of producing a head, and denote the corresponding probability by $\tilde{p}_{\theta,C}$. An easy observation is that given a boxed matrix M, one may modify the first $n-1$ rows by adding the bottom row $\bar{1}$ to them. Thus we have a simple observation:

Proposition 3.4.3.

$$\forall C, \quad \tilde{p}_{\theta,C} = \tilde{p}_{1-\theta,C}$$

Other than proposition 3.4.3, the general behavior of $p_{\theta,C}$ is completely open. For example, one may ask does $\theta = \frac{d_{2n}}{2n}$ give a higher probability of producing extremal codes than $\theta = \frac{1}{2}$? In general, we propose the following question:

Question 3.4.4. Is there a function $\theta(n)$, such that for codes of length $2n$, using a biased coin with probability $\theta(n)$ for a head will most likely to produce extremal codes?

We leave both question 3.4.2 and 3.4.4 for future explorations.

Chapter 4

Construction G

In Chapter 4 and 5 we shift gears and mainly consider questions of an arithmetic nature that arise in the search for binary self-dual codes. We will see that general duality statements give rise to possibilities of constructing codes using the arithmetic information over quite general schemes, but surprisingly even some basic questions have not been answered by the literature.

Recall the definition that a binary self-dual code is a triple (W, E, V) over $\mathbb{F}_2$. In the Construction G of this chapter, W will be the middle dimension étale cohomology space of certain arithmetic schemes over $\mathbb{Z}[\frac{1}{2}]$. We will specify a half-dimensional subspace V inside W which is self-orthogonal with respect to the cup product pairing on cohomology. Meanwhile, whether the cup product on W is a Euclidean form in general remains an interesting question. Nonetheless, Construction G recovers Construction $\mathbb{Q}$ in chapter 3 as a special case.

4.1 Arithmetic Duality

In appendix C we recall some glossary of derived category of bounded complexes of sheaves of R modules on the small étale site X_{et}, denoted $\mathcal{D}^b(X, R)$. R is a ring or a field.

Let K be a global field of characteristic different from 2. When v is a place of K , the completion of K at v is denoted K_v. If K is a number field, let $\mathcal{O}_K$ be the ring of integers of K and let $X = \mathrm{Spec}(\mathcal{O}_K)$. If K is a function field, let X be a smooth projective curve with function field K.

Consider $\mathcal{F} \in D^b(\mathrm{Spec}\, K_v)$. When v is real, $K_v = \mathbb{R}$. We will consider the reduced cohomology group $H^*_{red}(K_v, \mathcal{F}) := H^*_T(\mathbb{Z}/2, \mathcal{F})$; in other words, it is the Tate cohomology groups of the $Gal(\mathbb{R}) = \mathbb{Z}/2$ module $\mathcal{F}$. When v is not real, we will consider the usual étale cohomology group $H^*_{et}(K_v, \mathcal{F})$. In the following we will abuse notation and write $H^*_{et}(K_v, \mathcal{F})$ for all v. For an open subscheme $U \subset X$, denote $H^*_c(\mathrm{Spec}(\mathcal{O}_K), \mathcal{F})$ the cohomology group with compact support, defined by Milne [Mil06, section II.2]. $S = S_\infty \sqcup S_f$ is a set of places of K, where S_f contains the places determined by the primes in the complement of U; S_∞ contains all of the real places of K.

Remark 4.1.1. There are slightly different definitions of cohomology group of compact support in the literature, which are only different in the treatment for the real places. ♢

Following the above definitions, when $\mathcal{F} \in \mathcal{D}^b(X)$ there is a long exact sequence

[Mil06, Prop II.2.3(a)]:

$$\cdots H^r_c(U, \mathcal{F}|_U) \to H^r(U, \mathcal{F}) \to \sum_{v \in S} H^r(K_v, \mathcal{F}_{K_v}) \to H^{r+1}_c(U, \mathcal{F}|_U) \cdots \tag{4.1.1}$$

In arithmetic geometry, Artin-Verdier duality on arithmetic schemes [Mil06, section II.3] is the natural analogue of Pioncaré duality on topological manifolds. Denote by μ_2 the sheaf of second roots of unity. If S_f contains all places of residue characteristic 2, then for any $\mathcal{F} \in D^b(U, \mathbb{Z}/2)$ there is a duality

Theorem 4.1.2 (Artin-Verdier)**.**

$$H^r_{et}(U, \mathcal{H}om(\mathcal{F}, \mu_2)) \times H^{3-r}_c(U, \mathcal{F}) \to H^3_c(U, \mu_2) \cong \mathbb{Z}/2 \tag{4.1.2}$$

is a perfect duality of $\mathbb{F}_2$ *vector spaces.*

This duality can be "lifted" to be a duality for cohomology groups of schemes over X. Let $\pi : Y \to X$ be a flat, projective, geometrically connected morphism of relative Zariski dimension d, $d \geq 0$. Assume Y has good reductions outside S. For $\mathcal{F} \in \mathcal{D}^b(Y)$, denote the total direct image by $R\pi\mathcal{F} \in \mathcal{D}^b(X)$. By the Leray spectral sequence, $H^j(Y, \mathcal{F}) = H^j(X, R\pi\mathcal{F})$ for all j. When $i : D \to X$, denote the base change of Y over D by Y_D. We will abuse notation and write $\mathcal{F}$ for its pull-back on Y_D.

The proper base change theorems for torsion sheaves [Mil80, Cor IV.2.3] says that in the Cartesian square:

$$\begin{array}{ccc} Y_D & \xrightarrow{i} & Y \\ {\scriptstyle \pi_D}\downarrow & & \downarrow{\scriptstyle \pi} \\ D & \xrightarrow{i} & X \end{array} \tag{4.1.3}$$

If $\mathcal{F} \in \mathcal{D}^b(Y, \mathbb{Z}/2)$, we have $R\pi_D i^* \mathcal{F} = i^*(R\pi\mathcal{F})$ in $\mathcal{D}^b(D)$. Thus there is no ambiguity to define $H^i_c(Y_U, \mathcal{F}) := H^i_c(U, R\pi\mathcal{F})$.

By assumption, Y_U is regular over U. There is a canonical isomorphism in $\mathcal{D}^b(U, \mathbb{Z}/2)$ [AGV73, XVIII Th 3.2.5],

$$\mathcal{H}om_U(R\pi\mathcal{F}, \mu_2) \cong R\pi\mathcal{H}om_{Y_U}(\mathcal{F}, \mu_2^{\otimes d+1})[2d] \tag{4.1.4}$$

Therefore canonically

$$H^{2d+r}(Y_U, \mathcal{H}om(\mathcal{F}, \mu_2^{\otimes d+1})) = H^r(Y_U, \mathcal{H}om(\mathcal{F}, \mu_2^{\otimes d+1})[2d])$$

$$= H^r(U, R\pi_*\mathcal{H}om(\mathcal{F}, \mu_2^{\otimes d+1})[2d]) = H^r(U, \mathcal{H}om(R\pi_*\mathcal{F}, \mu_2))$$

where the second equality is by the Leray spectral sequence; the third equality is by equation 4.1.4. Combining this with the duality $H^{3-r}_c(U, R\pi\mathcal{F}) = H^{3-r}_c(Y_U, \mathcal{F})$, we get the following duality statement.

Proposition 4.1.3. *The cup product pairing:*

$$H^{2d+3-r}(Y_U, \mathcal{H}om(\mathcal{F}, \mu_2^{\otimes d+1})) \times H^r_c(Y_U, \mathcal{F}) \to H^{2d+3}_c(Y_U, \mu_2^{\otimes d+1}) \cong \mathbb{Z}/2 \tag{4.1.5}$$

is a perfect duality of $\mathbb{F}_2$ vector spaces.

Again by the Leray spectral sequence, equation 4.1.1 translates into a statement on $\mathcal{D}^b(Y, \mathbb{Z}/2)$:

$$\cdots H^r_c(Y_U, \mathcal{F}) \to H^r(Y_U, \mathcal{F}) \to \sum_{v \in S} H^r(Y_{K_v}, \mathcal{F}_{K_v}) \xrightarrow{\delta_r} H^{r+1}_c(Y_U, \mathcal{F}) \cdots \tag{4.1.6}$$

Since 2 is invertible on U and hence on Y_U, the Tate twist $\mu_2^{\otimes i}$ can be identified with μ_2 for all i. The following proposition is an analogue with **??**:

Proposition 4.1.4. *The image of the restriction homomorphism*

$$\Phi\colon H^{d+1}_{et}(Y_U,\mu_2)\to \oplus_{v\in S}H^{d+1}_{et}(Y_{K_v},\mu_2)$$

is its own orthogonal complement with respect to the non-degenerate bilinear product

$$\begin{aligned}\left(\oplus_{v\in S}H^{d+1}_{et}(Y_{K_v},\mu_2)\right)\times\left(\oplus_{v\in S}H^{d+1}_{et}(Y_{K_v},\mu_2)\right)&\to \oplus_{v\in S}H^{2d+2}_{et}(Y_{K_v},\mu_2)\\ &\xrightarrow{\delta_{2d+2}} H^{2d+3}_c(Y_U,\mu_2)\cong\mathbb{F}_2 \qquad (4.1.7)\end{aligned}$$

which is the cup product pairing composed with the boundary map in equation 4.1.6. In 4.1.7, δ_{2d+2} amounts to taking summations.

Proof. We will prove the proposition in several steps.

For each place $v\in S_f$, the local duality statement says that for $\mathcal{F}\in\mathcal{D}^b(\operatorname{Spec}K_v,\mathbb{Z}/2)$,

$$H^i(K_v,\mathcal{F})\times H^{2-i}(K_v,\mathcal{H}om(\mathcal{F},\mu_2))\to H^2(K_v,\mu_2)=\mathbb{Z}/2$$

is a perfect duality for $\mathbb{F}_2$ vector spaces. (When $v\in S_\infty$ the statement is trivially true, in the following we will assume $v\in S$.) By arguments similar to proposition 4.1.4, we have that for $\mathcal{F}\in\mathcal{D}^b(Y,\mathbb{Z}/2)$,

$$H^i(Y_{K_v},\mathcal{F})\times H^{2d+2-i}(Y_{K_v},\mathcal{H}om(\mathcal{F},\mu_2^{\otimes d+1}))\to H^{2d+2}(Y_{K_v},\mu_2^{\otimes d+1})$$

is a perfect duality of $\mathbb{F}_2$ vector spaces. In our setting, we will take $\mathcal{F}=\mu_2$ and ignore all the Tate twists.

We refer to [Mil06, II.2] for the proof that in 4.1.7, δ_{2d+2} amounts to taking summations. Therefore equation 4.1.7 gives a non-degenerate symmetric bilinear pairing over $\mathbb{F}_2$.

Now we prove that the image of

$$\Phi\colon H^{d+1}_{et}(Y_U,\mu_2)\to \oplus_{v\in S}H^{d+1}_{et}(Y_{K_v},\mu_2)$$

is its own orthogonal complement with respect to the product in 4.1.7. This is a pretty standard exercise in linear algebra. For ease of notation, denote $A = H^{d+1}_{et}(Y_U,\mu_2)$, $B = \oplus_{v\in S}H^{d+1}_{et}(Y_{K_v},\mu_2)$ and $C = H^{2d+2}_c(Y_U,\mu_2)$. The pairing in equation 4.1.7 identifies the dual $\check{B} = \mathrm{Hom}_{\mathbb{F}_2}(B,\mathbb{F}_2)$ of B with B. The perfect pairing $A\times C\to\mathbb{F}_2$ in 4.1.5 identifies $\check{A}$ with C. From 4.1.6 for $r = d+1$ we have an exact sequence

$$A\xrightarrow{\Phi}B\xrightarrow{\Psi}C \tag{4.1.8}$$

Here the above pairings identify the map $\Psi : \check{B}\to B\to C = \check{A}$ with the dual $\check{\Phi}$ of Φ. Hence

$$\dim(\mathrm{coker}(\Phi)) = \dim(\ker(\check{\Phi})) = \dim(\ker(\Psi)) = \dim(\mathrm{image}(\Phi))$$

where the last equality follows from equation 4.1.8. Thus $\dim(\mathrm{image}(\Phi)) = \frac{1}{2}\dim(B)$. So if we can show image(Φ) is self-orthogonal, it will be its own orthogonality complement since the product 4.1.7 is non-degenerate. We have the commutative diagram:

$$\begin{array}{ccc} A\times A & \longrightarrow & H^{2d+2}(Y_U,\mu_2) \\ \downarrow & & \downarrow \\ B\times B & \longrightarrow & \oplus_{v\in S}H^{2d+2}(Y_{K_v},\mu_2) \end{array} \tag{4.1.9}$$

But the composition of the maps

$$H^{2d+2}(Y_U,\mu_2)\to\oplus_{v\in S}H^{2d+2}(Y_{K_v},\mu_2)\to H^{2d+3}_c(Y_U,\mu_2)$$

is 0 by the exactness of the sequence. □

The construction in Proposition 4.1.4 works in complete generality. Let's look at two examples when the relative dimension $d = 0$.

Example 4.1.5. When $d = 0$, $Y = X \xrightarrow{Id} X = \mathrm{Spec}(\mathcal{O}_K)$. By the Kummer sequence one has

$$\mathcal{O}^*_{K,S}/2 \to H^1(U, \mu_2) \to Pic(U)[2]$$

Thus when $Pic(U)$ is odd, then $\mathcal{O}^*_{K,S}/2 = H^1(U, \mu_2)$. the image of Φ in proposition 4.1.4 is still the diagonal image $\Phi : \mathcal{O}^*_{K,S}/2 \to \oplus_{v\in S} K^*_v/2$ as in Construction $\mathbb{Q}$. The cup product $H^1(K_v, \mu_2) \times H^1(K_v, \mu_2) \to \mathbb{Z}/2$ is precisely the Hilbert pairing.

However, when $Pic(U)[2] \neq 0$ then the two-torsion elements in the Picard group also come into play. △

Example 4.1.6 (Local-Global Codes). Consider K to be the global function field $\mathbb{F}_q(T)$, where q is a prime power and $q \equiv 3 \bmod 4$, T is a transcendental parameter. $Y = X = \mathbb{P}^1_{\mathbb{F}_q}$. Let $S = \{\frac{1}{T}, g_1(T), \cdots, g_{n-1}(T)\}$ where each $g_i(T)$ is a monic irreducible polynomial in $\mathbb{F}_q[T]$. Then the image of Φ is also given by the global S-units $\langle -1, g_1(T), \cdots, g_{n-1}(T)\rangle$ in $W = \oplus_{v\in S} K^*_v/(K^*_v)^2$. Moreover, when each $g_i(T)$ is of odd degree, then the Hilbert symbol pairing $W \times W \to \mathbb{F}_2$ is Euclidean. It is not hard to see that the diagonal image of Φ is also described by a boxed-matrix.

For simplicity, let's take $g_i(T) = T - a_i$ where a_i are distinct integers in $\mathbb{Z}$. Suppose $q > max_i|a_i|$, then each $g_i(T)$ will give a distinct rational point on $\mathbb{P}^1_{\mathbb{F}_q}$. In the boxed matrix description of the resulting code, the pair b_{ij} is determined

by the Jacobi symbol $(\frac{a_i - a_j}{p})$. By quadratic reciprocity, the Jacobi symbol is also determined by the congruence conditions of q mod the prime factors in $(a_i - a_j)$. Assume $(a_i - a_j)$ have distinct prime divisors when $1 \leq i < j \leq n-1$. If we let the primes in the congruence class of 3 mod 4 grow by magnitude, by the equidistribution of primes in congruence classes, the probability that S generating a certain equivalence classes of length $2n$ is the same as the random algorithm in section 3.4 using a fair coin! $\triangle$

4.2 The Quest for Euclidean Form

The reader will have noticed that the only thing that is not addressed in proposition 4.1.4 is the condition when the bilinear product 4.1.7 is a Euclidean form. When it is so, then upon fixing a basis, $image(\Phi)$ becomes a self-dual code.

Recall theorem 3.2.1, a non-degenerate symmetric bilinear product $\langle , \rangle$ on $W/\mathbb{F}_2$ is Euclidean if and only if $\exists x$, such that $\langle x, x \rangle = 1$.

When $d = 0$ the question is easy. By corollary 3.2.2, when a field k has $k^*/2$ finite, the Hilbert pairing is Euclidean if and only if $\sqrt{-1} \notin k^*$. By remark 2.2.1, a Euclidean basis for $k^*/2$ is unique up to permutation if and only if $dim_{\mathbb{F}_2}(k^*/2) \leq 3$. When $K/\mathbb{Q}$ is a finite Galois extension, $dim_{\mathbb{F}_2}(K_v^*/2) \leq 3$ for every $v \in S$ if and only if the prime 2 splits completely in $K/\mathbb{Q}$. (The reader is referred to [Neu99, Proposition 5.7, Chap II] for the structure of $K_v^*/2$ for local fields K_v.)

When $d > 0$, the question of a Euclidean basis has geometry coming into play.

When $d = 1$, suppose Y is a flat projective curve over $\mathrm{Spec}(\mathcal{O}_K)$, regular over U. The Hochschild-Serre spectral sequence can be used to calculate $H^r(Y_{K_v}, \mu_2)$:

$$H^i(K_v, H^j(Y_{\overline{K_v}}, \mu_2)) \Rightarrow H^{i+j}(Y_{K_v}, \mu_2) \tag{4.2.1}$$

where $\overline{K_v}$ denotes an algebraic closure of K_v. This spectral sequence is multiplicative, where the multiplication is compatible with the cup product structure in cohomology. However, the spectral sequence along often does not suffice to determine whether the product on $H^2(Y_{K_v}, \mu_2) =: W$ is Euclidean or not, as is shown in the following example:

Example 4.2.1 (Non-Example). Suppose Y_{K_v} is the projective line $\mathbb{P}^1_{K_v}$. The spectral sequence 4.2.1 degenerates on the E_2 page. Denote $H^{2,0} = \mathbb{Z}/2 \hookrightarrow W$ generated by $\{y\}$ as an $\mathbb{F}_2$ vector space. In the multiplicative spectral sequence, $y^2 \in H^{4,0} = 0$ for the dimension reason. Moreover, $H^{1,1} = 0$; $H^{0,2} = \mathbb{Z}/2$ also pairs trivially with itself for the same dimension reason. By the short exact sequence

$$0 \to H^{2,0} \to W \to H^{0,2} \to 0$$

Does it mean the cup product on W is necessarily hyperbolic?

Suppose $W = \{x, y\}$ is spanned by two elements x, y additively over $\mathbb{F}_2$. $H^{0,2} = \{\bar{x}\} \in W/\{y\}$ is a quotient space of W. The multiplicative structure on $H^{0,2}$ is naturally induced from W as a quotient space. Since $\langle , \rangle$ is non-degenerate on W, $\langle y, y\rangle = 0$ implies $\langle x, y\rangle = 1$ is non-trivial. Thus on the quotient space

$$\langle \bar{x}, \bar{x}\rangle = \langle x, x\rangle \bmod \langle x, y\rangle$$

Therefore the cup product $\langle \bar{x}, \bar{x} \rangle = 0$ bears no information on $\langle x, x \rangle$. We are unable to conclude whether the product on W is Euclidean or not from the spectral sequence 4.2.1. $\triangle$

In the topological category, product structures on the cohomology are used as a ubiquitous invariant for topological manifolds. It is very natural to explore this similar structure as an invariant for arithmetic schemes. In the arithmetic situation, when a base scheme (say $\operatorname{Spec} \mathcal{O}_K$ or $\operatorname{Spec} K_v$) contains n-th roots of unity, the sheaf μ_n is canonically isomorphic to $\mathbb{Z}/n$. When X is a scheme over such a base, the cup product pairing

$$H^i(X, \mu_n) \cup H^j(X, \mu_n) \to H^{i+j}(X, \mu_n^2) \cong H^{i+j}(X, \mu_n)$$

makes $H^*(X, \mu_n)$ a ring. It is natural to ask what kind of information is encoded in the product structure.

In our discussion on the Hilbert symbols for a local field in section 3.2, the cup product $H^1(\mathbb{Q}_p, \mu_2) \cup H^1(\mathbb{Q}_p, \mu_2)$ depends on the congruence condition p mod 4. One can ask the following question:

Question 4.2.2. How does the congruence condition on p affect the cup product structure on $H^*(\mathbb{P}^1_{\mathbb{Q}_p}, \mu_2)$, or $H^*(E_{\mathbb{Q}_p}, \mu_2)$ where E is an elliptic curve?

We will answer this question in section 5.6, using a "deformation trick'" in the context of equivariant étale cohomology.

Chapter 5

Equivariant Construction

Ever since the 1950s and 60s, equivariant cohomology has been a powerful tool in the study of group actions on manifolds and schemes alike. Pioneers in the field include Borel, Bredon and Grothendieck, to name a few. On the large scale, the equivariant machinery in both the topological and the arithmetic category can be stated using Grothendieck's language of homological algebra. Some technical differences remain, of course. In the topological category, theorems in equivariant cohomology are often proved in the homotopy category of finite CW-complexes. Statements are often broken down to the "cellular level" and then "glued together". However, in the arithmetic category it is in general more difficult to work with the étale homotopy theories.

In this chapter, we review the general construction of equivariant cohomology theory historically known as "Borel's construction" in section **??**. We prove a

"Smith-type inequality" by invoking a result of Morin (theorem **??**). In section **??** some examples are provided where the Smith type inequalities become equalities, which are the most convenient case from the point of view of constructing codes.

The goal of this chapter is two-fold: in **??** we answer question **??** by showing the pairing is hyperbolic; in **??** we provide yet one more possible construction of binary self-dual codes, which is analogous to **??**.

5.1 Borel's Equivariant Cohomology

In this section we recall Borel's construction of equivariant cohomology. Consider a finite group G action on a complex of k-modules C^*, where k is a field. We will denote C^* as a object in $\delta gk[G]$-Mod, where $\delta : C^i \to C^{i+1}$ means the differential in the complex; g refers to the fact that the complex is graded; $k[G]$ means the complex is a module for the group ring $k[G]$. We refer the reader to [AP93] for a more thorough treatment.

Take a free resolution $\mathcal{E}_* := W_* \otimes k[G]$ of the trivial G-module k,

$$\mathcal{E}_* \to k \to 0$$

where $\mathcal{E}_*$ is a complex

$$\cdots \mathcal{E}_i \to \mathcal{E}_{i-1} \cdots \to \mathcal{E}_1 \to \mathcal{E}_0$$

This is a $\delta gk[G]$-Mod.

The group cohomology ring of $H^*(G,k)$ can be computed by the complex

$$H^*(G,k) = H^*(Hom_{k[G]}(\mathcal{E}_*, k))$$

It is well known that when $G \cong \mathbb{Z}/2$ and $char\ k = 2$, $H^*(G,k) \cong k[t]$ where $deg(t) = 1$. In the following, for simplicity we will assume $char\ k = 2$ whenever $G = \mathbb{Z}/2$.

For a $\delta gk[G]$-Mod C^*, denote

$$\beta^*_G(C^*) := Hom_{k[G]}(\mathcal{E}_*, C^*)$$

The equivariant cohomology of C^* is defined to be the cohomology of this complex,

$$H^*_G(C^*) := H^*(\beta^*_G(C^*))$$

This was historically called Borel's construction of equivariant cohomology when C^* was the equivariant singular cochain complex of a CW complex.

We will further assume that C^* carries a $\delta gk[G]$ morphism $C^* \otimes C^* \to C^*$ which induces a cup product structure on $H^*(\beta^*_G(C^*))$.

Remark 5.1.1. We will denote the dual complex of $\mathcal{E}_*$ as $\mathcal{E}^* := Hom_{k[G]}(\mathcal{E}_*, k[G])$. When C^* is bounded from below, there is an isomorphism

$$\beta^*_G(C^*) = C^* \otimes_{k[G]} \mathcal{E}^*(G)$$

$\diamondsuit$

It is often convenient to write $C^* \otimes_{k[G]} \mathcal{E}^*(G) \cong C^* \widetilde{\otimes} W^*$, where the twisting $\widetilde{\otimes}$ implies that the derivation and multiplication of the tensor product $C^* \widetilde{\otimes} W^*$ are not the component-wise operations on each factor. In fact, they are "twisted'' by the $k[G]$-Mod isomorphism $C^* \otimes_{k[G]} \mathcal{E}^*(G) \cong C^* \otimes W^*$.

In this chapter we will not seek to state our results in the most general context. For the purpose of constructing codes, we will mainly focus on the special case when $G = \mathbb{Z}/2$ is the group of order 2. In this case, the following lemma gives a better description of the $\delta gk[G]$-Mod $\beta_G^*(C^*)$:

Lemma 5.1.2. *[AP93, Proposition 1.3.4]*

Suppose $G \cong \mathbb{Z}/2$, then

1. *As a right $k[t]$-module, $\beta_G^*(C^*) \cong C^* \otimes k[t]$.*
2. *The twisted differential $\tilde{\delta}$ is $k[t]$ linear, where the differential on $k[t]$ is trivial.*
3. *In particular, when $C^* = k$, $\beta_G^*(k) \cong H^*(\beta_G^*(k))$.*

Lemma 5.1.2 (1) says that *multiplication by t* is not twisted. Thus $\beta_G^*(C^*)$ is a torsion-free module over $k[t]$. Since $k[t]$ is a P.I.D., a torsion-free module is also a free module.

5.2 Equivariant Etale Sheaves

In this section we first recall the definition of the category of equivariant étale sheaves on a scheme X, denoted $Sh(X, G)$. G is a finite group acting on X

[AGV73][Mor08]. $\mathcal{F}$ is a sheaf on X_{et}. A G-linearization of $\mathcal{F}$ is a family of morphisms $\varphi_{\sigma,} : \sigma_*\mathcal{F} \to \mathcal{F}$ indexed by $\sigma \in G$ that satisfy the following conditions:

- $\varphi_1 = Id.$
- $\varphi_{\tau\sigma} = \varphi_\tau \circ \tau_*(\varphi_\sigma)$.

A G-linearized sheaf $\mathcal{F}$ is called an equivariant G-sheaf, $\mathcal{F} \in Sh(X, G)$. A morphism of G-sheaves $\alpha : \mathcal{F} \to \mathcal{L}$ on X_{et} is a morphism of sheaves that commutes with the linearizations on $\mathcal{F}$ and $\mathcal{L}$. In other words, if we define the action of G on $Hom_{Sh(X)}(\mathcal{F}, \mathcal{L})$ by

$$\sigma(\alpha) := \varphi_{\mathcal{L},\sigma} \circ \sigma_*(\alpha) \circ \varphi^{-1}_{\mathcal{F},\sigma}$$

Then $Hom_{Sh(X,G)}(\mathcal{F}, \mathcal{L})$ is the invariant subgroup of this action.

$Sh(X, G)$ is an abelian category with enough injectives. When $\mathcal{F}$ is an inject object in $Sh(X, G)$, $\Gamma(\mathcal{F})$ is an injective $\mathbb{Z}[G]$-Mod, [Gro57, Lemma 4.3.1].

Given a sheaf of k-modules $\mathcal{F} \in Sh(X, G)$ (k is a field), take an injective resolution $\mathcal{I}^*$ on X_{et} and apply the global section functor, this gives a complex of $k[G]$-modules:

$$0 \to \mathcal{F}(X) \to \mathcal{I}^0(X) \to \mathcal{I}^1(X) \cdots$$

The complex $\mathcal{I}^*(X)$:

$$0 \to \mathcal{I}^0(X) \to \mathcal{I}^1(X) \cdots$$

is a complex of injective $k[G]$-modules. Apply Borel's construction on this complex $\mathcal{I}^*(X)$: take a free resolution $\mathcal{E}_*$ of the trivial module k, define

$$\beta_G^n(\mathcal{F}) := Tot^n Hom(\mathcal{E}_*, \mathcal{I}^*(X)) = \oplus_{i+j=n} Hom_{k[G]}(\mathcal{E}_i, \mathcal{I}^j(X))$$

The equivariant sheaf cohomology is defined as:

$$H_G^*(X, \mathcal{F}) := H^*(\beta_G^*(\mathcal{F}))$$

The reader will also recognize this as Grothendieck's equivariant cohomology $H^*(X, G, \mathcal{F})$, which are the derived functors of $\Gamma(\mathcal{F})^G$. The above double complex construction just computes the derived functors of this composite functor–it is the composition of the *global section* functor followed by the *invariant under* G functor.

In [Mor08] a modified equivariant étale cohomology is introduced. Consider a complete resolution $\mathcal{J}_*$ of the trivial G module k,

Define

$$\widehat{\beta}_G^n(\mathcal{F}) := Tot^n Hom(\mathcal{J}_*, \mathcal{I}^*(X)) = \oplus_{i+j=n} Hom_{k[G]}(\mathcal{J}_i, \mathcal{I}^j(X))$$

$$\widehat{H}_G^*(X, \mathcal{F}) := H^*(\widehat{\beta}_G^*(\mathcal{F}))$$

Similar to lemma 5.1.2, when $G = \mathbb{Z}/2$, we have

Lemma 5.2.1. *As a $\delta gk[G]$-Mod, $\beta_G^*(\mathcal{F}) \cong \mathcal{I}^* \widetilde{\otimes} k[t, \frac{1}{t}]$, where multiplication by t is linear; the derivation $\widetilde{\delta}$ is also linear on t.*

Remark 5.2.2. From Lemma 5.2.1 it is straight forward to see the following facts:

- $\widehat{\beta}^*_G(k) \cong k[t, \frac{1}{t}]$ where the differential δ on the later is trivial. This induces the familiar fact that $\widehat{H}^*(G, k) = k[t, \frac{1}{t}]$ by passing to cohomology.
- $\widehat{\beta}^{i+1}_G(\mathcal{F}) \cong \widehat{\beta}^i_G(\mathcal{F}) \otimes_{k[t,\frac{1}{t}]} t$.
- $\widehat{H}^{i+1}_G(X, \mathcal{F}) \cong \widehat{H}^i_G(X, \mathcal{F}) \otimes_{k[t,\frac{1}{t}]} t$.
- $\widehat{H}^*_G(X, \mathcal{F})$ is a free $k[t, \frac{1}{t}]$ module.

$\diamondsuit$

The following observation is also straight-forward, but we state it separately due to its relevance in later discussions:

Proposition 5.2.3. *As a free $\delta gk[t]$-Mod,*

$$\beta^*_G(\mathcal{F}) \otimes_{k[t]} k[t, \frac{1}{t}] \cong \widehat{\beta}^*_G(\mathcal{F})$$

Both $H^*_G(X, -)$ and $\widehat{H}^*_G(X, -)$ satisfy the usual properties as a cohomological functor. For example, a short exact sequence of G-sheaves

$$0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$$

leads to a long exact sequence of cohomological groups in both functors. Moreoever, there are functorial spectral sequences abutting to these functors, whose E^2 pages look like:

$$H^p(G, H^q(X, \mathcal{F})) \Rightarrow H^{p+q}_G(X, \mathcal{F}) \tag{5.2.1}$$

$$\widehat{H}^p(G, H^q(X, \mathcal{F})) \Rightarrow \widehat{H}^{p+q}_G(X, \mathcal{F}) \tag{5.2.2}$$

where $\widehat{H}^*(G, -)$ means the Tate cohomology groups.

5.3 The Localization Theorem

In topology, the classical *Localization theorem* relates the equivariant cohomology of a manifold to that of its ramification loci [AP93, Theorem 3.1.6]. In the étale context, similar results have been obtained in a recent paper [Mor08], which we briefly recall in the following.

Let X be a connected, locally Noetherian scheme. A finite group G action on X is called *admissible* if X is covered by a collection of affine opens which are invariant under G, and that every orbit of G is contained in an affine open. Under this condition, the quotient scheme X/G can be defined. When the G-action is free, the quotient map $\pi : X \to X/G =: W$ is an étale G-cover. We say $\mathcal{F} \in Sh(X, G)$ is *adapted* if $\exists n$, $\forall V$ on W_{et}, $H^q(V, \pi_*^G \mathcal{F}) = 0$ when $q \geq n+1$. For example, when W is a regular quasi-projective scheme over $\mathbb{Z}$, and $\mathcal{F}$ is a locally constructible torsion sheaf, then $\mathcal{F}$ is adapted.

Remark 5.3.1. When the G action on X is free, $H_G^*(X, \mathcal{F}) \cong H^*(X/G, \pi_* \mathcal{F})$. When the action of G on X is trivial and $\mathcal{F}$ is a constant sheaf, $H_G^*(X, \mathcal{F}) \cong H^*(X, \mathcal{F}) \otimes H^*(G, \mathcal{F})$. ♢

When the G-action on X is not free, denote by $Z \subset X$ the closed sub-scheme where the inertia group is non trivial, i.e. Z the ramification locus in the cover $X \to X/G =: W$. Denote X' the open complement of Z in X. An étale neighborhood of Z in X is an étale affine-morphism $\phi : U \to X$ such that $U \times_Z X \to Z$ is an isomorphism.

If $\phi : U \to X$ is a G-equivariant étale neighborhood of Z and that $\phi^{-1}(Z)$ intersects each connected component of U non-empty, then U is called a G-étale neighborhood of Z in X. Denote $\widetilde{Z}$ by the projective limit of the G-étale neighborhoods of Z in X. Denote the canonical embedding $i : Z \to X$, $\widetilde{i} : \widetilde{Z} \to X$.

Remark 5.3.2. Suppose Z is contained in an open affine scheme $\operatorname{Spec} A$, where Z is defined by a radical ideal I. Denote $(\widetilde{A}, \widetilde{I})$ the Henselization of the pair (A, I), then $\widetilde{Z} = \operatorname{Spec} \widetilde{A}$. ♢

The following Theorem 5.3.3 and Corollary 5.3.5 are *localization theorems* in the scheme-theoretic setting:

Theorem 5.3.3. *[Mor08, Theorem 3.10] A finite group G acts admissibly on a locally Noetherian scheme X. $\mathcal{F} \in Sh(X, G)$ and suppose that $\mathcal{F}|_{X'}$ is adapted. Then there is an isomorphism*

$$\widehat{H}^*_G(X, \mathcal{F}) \cong \widehat{H}^*_G(\widetilde{Z}, \widetilde{i}^*\mathcal{F})$$

When Z is affine, we can the following isomorphism [Hub93]:

Lemma 5.3.4. *Suppose $\mathcal{F}$ is an abelian torsion sheaf on $\widetilde{Z}$, and $i : Z \to \widetilde{Z}$ is the inclusion,*

$$\forall n, \quad H^n(\widetilde{Z}, \mathcal{F}) = H^n(Z, i^*\mathcal{F})$$

By the functorial spectral sequence 5.2.1 and 5.2.2, when G acts on $\widetilde{Z}$, there are isomorphisms of equivariant cohomology groups:

$$\forall n, \quad H^n_G(\widetilde{Z}, \mathcal{F}) = H^n_G(Z, i^*\mathcal{F}), \quad \widehat{H}^n_G(\widetilde{Z}, \mathcal{F}) = \widehat{H}^n_G(Z, i^*\mathcal{F})$$

Corollary 5.3.5. *[Mor08, Corollary 3.11] When Z is affine and $\mathcal{F}$ is torsion:*

$$\widehat{H}^*_G(X, \mathcal{F}) \cong \widehat{H}^*_G(Z, i^*\mathcal{F})$$

Using the localization theorem, we can prove a Smith type inequality on the étale site of schemes. For notational convenience, given a field k, denote $k_1 := k[t]/(t-1) = k[t, \frac{1}{t}]/(t-1)$. $k_0 := k[t]/(t)$. For a graded module, $- \otimes_{k[t]} k_1$ is an exact functor. When $k = \mathbb{F}_2$, we will still write k_0 and k_1 to avoid overloading the notations.

Proposition 5.3.6. *Under the hypothesis in corollary 5.3.5, and suppose $G = \mathbb{Z}/2$,*

$$\sum_{i=0}^{\infty} dim_k H^{m+i}(Z, \mathcal{F}) \leq \sum_{i=0}^{\infty} dim_k H^{m+i}(X, \mathcal{F}) \tag{5.3.1}$$

for any m.

Proof. For the proof of this proposition we will use the minimal Hirsch-Brown model,

$$\beta^*_G(\mathcal{F}) \cong H^*(X, \mathcal{F}) \widetilde{\otimes} k[t] \tag{5.3.2}$$

as introduced in appendix B. Similarly, we have the minimal Hirsch-Brown models

$$\beta^*_G(\mathcal{F}|_Z) \cong H^*(Z, \mathcal{F}) \otimes k[t] \tag{5.3.3}$$

$$\widehat{\beta}^*_G(\mathcal{F}) \cong H^*(X, \mathcal{F}) \widetilde{\otimes} k[t, \frac{1}{t}] \tag{5.3.4}$$

$$\widehat{\beta}^*_G(\mathcal{F}|_Z) \cong H^*(Z, \mathcal{F}) \otimes k[t, \frac{1}{t}] \tag{5.3.5}$$

Since the action of G on Z is trivial, the complex 5.3.3 has trivial differential. Thus $H^*_G(Z, \mathcal{F}) = H^*(Z, \mathcal{F}) \otimes k[t]$.

Define a filtration:

$$\mathcal{F}_m(\beta_G^*(\mathcal{F})) := \oplus_{i=0}^m H^i(X,\mathcal{F})\widetilde{\otimes}k[t] \tag{5.3.6}$$

$$\mathcal{F}_m(\beta_G^*(\mathcal{F}|_Z)) := \oplus_{i=0}^m H^i(Z,\mathcal{F}) \otimes k[t]$$

The inclusion morphism $i : Z \to X$ induces a graded morphism in equivariant cohomology

$$i^\sharp : \sum_{p+q=n} H^p(X,\mathcal{F})\widetilde{\otimes}t^q \to \sum_{p+q=n} H^p(Z,i^*\mathcal{F}) \otimes t^q$$

Induction on n shows that the morphism $i^\sharp$ respects the filtration: $\forall m$, $i^\sharp$: $\mathcal{F}_m(\beta_G^*(\mathcal{F}|_Z)) \to \mathcal{F}_m(\beta_G^*(\mathcal{F}))$, which fits into the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{F}_{m-1}(\beta_G^*(\mathcal{F})) & \longrightarrow & \beta_G^*(\mathcal{F}) & \longrightarrow & \beta_G^*(\mathcal{F})/\mathcal{F}_{m-1} \to 0 \\ & & \downarrow{\scriptstyle i^\sharp} & & \downarrow{\scriptstyle i^\sharp} & & \downarrow{\scriptstyle \overline{i}^\sharp} \\ 0 & \longrightarrow & \mathcal{F}_{m-1}(\beta_G^*(\mathcal{F}_Z)) & \longrightarrow & \beta_G^*(\mathcal{F}|_Z) & \longrightarrow & \beta_G^*(\mathcal{F}|_Z)/\mathcal{F}_{m-1} \to 0 \end{array} \tag{5.3.7}$$

After localizing at $\otimes_{k[t]}k_1$ and taking cohomology, the middle map $i^\sharp \otimes_{k[t]} k_1$ becomes an isomorphism. Since the differential on $H^*(Z,i^*\mathcal{F}) \otimes k[t]$ is trivial, the map $\overline{i}^\sharp \otimes_{k[t]} k_1$ is surjective on the cochain level as well. Since

$$\sum_{i=m}^{\infty} dim_k H^i(X,\mathcal{F}) = \dim_k(\beta_G^*(\mathcal{F})/\mathcal{F}_{m-1}) \otimes_{k[t]} k_1$$

$$\sum_{i=m}^{\infty} dim_k H^i(Z,\mathcal{F}) = \dim_k(\beta_G^*(\mathcal{F}|_Z)/\mathcal{F}_{m-1}) \otimes_{k[t]} k_1$$

we get the desired inequality.

□

Remark 5.3.7. One can compare proposition 5.3.6 with Corollary1.3.8 in [AP93], and the following proposition 5.3.8 with Proposition 1.3.14 in the topological setting in [AP93].

Proposition 5.3.6 can also be compared with Bredon's equivariant cohomology of a *local system* on a variety over an algebraically closed field [Sym04], which proves the same Smith type inequality when $G = \mathbb{Z}/2$. $\diamondsuit$

Proposition 5.3.8. *[AP93, Proposition 1.3.14] The following two conditions are equivalent:*

(a) The differential δ in the minimal Hirsch-Brown model 5.3.2 of $\beta_G^*(\mathcal{F})$ vanishes;

(b)

$$\sum_{i=0}^{\infty} dim_k H^i(Z, \mathcal{F}) = \sum_{i=0}^{\infty} dim_k H^i(X, \mathcal{F})$$

Proof. $(a) \Rightarrow (b)$ is obvious.

$(b) \Rightarrow (a)$: Factor δ into a surjection followed by an injection: $H^*(X, \mathcal{F})\widetilde{\otimes}k[t] \rightarrow M \rightarrow H^*(X, \mathcal{F})\widetilde{\otimes}k[t]$. M is a sub-module of the free $k[t]$-Mod $\beta_G^*(\mathcal{F})$. When equality is reached in (b), the differential in $\beta_G^*(\mathcal{F})\otimes_{k[t]}k_1$ is trivial. Thus $M\otimes_{k[t]}k_1 = 0$, which implies $M = 0$ since M is free. $\square$

Based on proposition 5.3.8, when equality is reached, the differential on both of the minimal Hirsch-Brown models $\beta_G^*(\mathcal{F})$ (5.3.2) and $\beta_G^*(\mathcal{F}|_Z)$ (5.3.3) are trivial. In this case, $H_G^*(X, \mathcal{F}) \cong \beta_G^*(\mathcal{F})$ as $\delta g k[t]$-Mod. $i^\sharp$ induces a map between two free $k[t]$-Mod which is an isomorphism after tensoring with k_1, this implies that $i^\sharp$ is injective.

5.4 Equivariant Construction

Now consider the situation in Chapter 4. Y is an integral projective scheme over $\operatorname{Spec}\mathbb{Z}[\frac{1}{2}]$, regular over an open sub-scheme $U \subset \operatorname{Spec}\mathbb{Z}[\frac{1}{2}]$. The group $G = \mathbb{Z}/2$ acts on Y. The constant sheaf $\mathcal{F} = \mu_2 \in Sh(Y, G)$ is adapted on Y. We have Artin-Verdier duality for the ring $H^*(Y_U, \mu_2)$ by ignoring the Tate twists since $\mu_2^{\otimes n} \cong \mathbb{Z}/2$ on Y. $H^*(Y_U, \mu_2)$ will be called a Pioncaré algebra, which is an algebra that satisfies the following requirements:

An *orientation* on a k-algebra A is a non-trivial k-linear map:

$$\mathcal{O}_A : A \to k$$

A is called a Poincaré algebra if the multiplication in A followed by orientation $A \times A \to A \xrightarrow{\mathcal{O}_A} k$ induces an k-linear isomorphism $A \to Hom_k(A, k)$.

- Suppose $A = \oplus_{i=0}^{n} A_i$ is a graded algebra. If $\mathcal{O}_A(A_i) = 0$ when $i < n$, A is called a graded Poincaré algebra of formal dimension n.

- A is called a filtered algebra of formal length $n+1$ if there is a filtration

  $$0 \subset \mathcal{F}_{-1}A \subset \mathcal{F}_0 A \subset \cdots \subset \mathcal{F}_n A = A$$

  which is compatible with the product $\mathcal{F}_i A \times \mathcal{F}_j A \subset \mathcal{F}_{i+j} A$.

  If $\mathcal{O}_A(\mathcal{F}_{n-1}A) = 0$; $\forall i$, $\mathcal{F}_i A$ is isomorphic to $Hom_k(A/\mathcal{F}_{n-i-1}A, k)$, then $(A, \mathcal{O}_A)$ is called a filtered Poincaré algebra.

Given a graded algebra A, we can associate to it a filtered algebra $\mathcal{A}$, where $\mathcal{F}_m\mathcal{A} := \oplus_{i=0}^{m} A_i$. Conversely, given a filtered algebra $\mathcal{A}$, we can associate to it a graded algebra $A := gr(\mathcal{A})$, where $A_m := \mathcal{A}_m/\mathcal{A}_{m-1}$.

Proposition 5.4.1. *[AP93, Proposition 5.1.3] $\mathcal{A}$ is a filtered Poincaré algebra if A is a graded Poincaré algebra, and vice versa.*

Thanks to Artin-Verdier duality, we have already seen that $H^*(Y_U, \mu_2)$ is a graded Poincaré algebra under the cup-product. Moreover, when equality is reached in proposition 5.3.8, we have an isomorphism of $\mathbb{F}_2$ vector spaces:

$$H^*(Y, \mu_2) \cong H^*(Y, \mu_2)\widetilde{\otimes}\mathbb{F}_2[t] \otimes_{\mathbb{F}_2[t]} k_1 \tag{5.4.1}$$

However, the multiplication structure of the algebra on the R.H.S is "twisted" from that on the L.H.S. Recall the R.H.S. has a natural filtration $\mathcal{F}_m$ defined in the proof of proposition 5.3.6. We have a straight forward observation:

Lemma 5.4.2. *$gr(H^*(Y, \mu_2)\widetilde{\otimes}\mathbb{F}_2[t] \otimes_{\mathbb{F}_2[t]} k_1) \cong H^*(Y, \mu_2)$ as a graded algebra.*

In corollary 5.3.5, $i^\sharp \otimes_{\mathbb{F}_2[t]} k_1$ induces an isomorphism of $\mathbb{F}_2$ vector spaces.

$$H^*(Y, \mu_2)\widetilde{\otimes}\mathbb{F}_2[t] \otimes_{\mathbb{F}_2[t]} k_1 \underset{\cong}{\overset{i^\sharp \otimes_{\mathbb{F}_2[t]} k_1}{\longrightarrow}} H^*(Z, \mu_2) \otimes \mathbb{F}_2[t] \otimes_{\mathbb{F}_2[t]} k_1 \tag{5.4.2}$$

Remark 5.4.3. Equation 5.4.2 is a map of filtered algebras. To distinguish the situation, we will denote the original filtration on $\beta_G^*(Z, \mu_2)$ by $\widetilde{\mathcal{F}}$, i.e.

$$\widetilde{\mathcal{F}}_m(\beta_G^*(Z, \mu_2)) = \sum_{i=0}^{m} H^i(Z, \mu_2) \otimes k[t] \tag{5.4.3}$$

as a filtered differential algebra. Since the differential is trivial, this filtration structure passes to the cohomology

$$\widetilde{\mathcal{F}}_m(H^*_G(Z,\mu_2)) = \sum_{i=0}^{m} H^i(Z,\mu_2)\otimes k[t]$$

One can also apply the functor $\otimes_{\mathbb{F}_2[t]}k_1$ to equation 5.4.3, which commutes with taking cohomology.

On the other hand, one can also translate the filtered algebra structure from the L.H.S. of equation 5.4.2 to the R.H.S. by the vector space isomorphism. We will denote this filtered algebra structure on $H^*_G(Z,\mu_2)\otimes_{\mathbb{F}_2[t]} k_1$ by $\mathcal{F}$. $\diamondsuit$

Since the G-action on Z is trivial, the algebra structure on $H^*_G(Z,\mu_2)\otimes_{\mathbb{F}_2[t]} k_1 = H^*(Z,\mu_2)\otimes \mathbb{F}_2[t]\otimes_{\mathbb{F}_2[t]} k_1$ and $H^*(Z,\mu_2)$ are the same. One gets a filtration $\mathcal{F}$ on $H^*(Z,\mu_2)$ by a chain of isomorphisms

$$H^*(Y,\mu_2) \overset{gr}{\longleftarrow} H^*(Y,\mu_2)\widetilde{\otimes}\mathbb{F}_2[t]\otimes_{\mathbb{F}_2[t]} k_1 \cong H^*(Z,\mu_2)\otimes\mathbb{F}_2[t]\otimes_{\mathbb{F}_2[t]} k_1 \cong H^*(Z,\mu_2)$$

When Y has relative dimension d over $\operatorname{Spec}\mathbb{Z}[\frac{1}{2}]$, $\mathcal{F}_{d+1}H^*(Z,\mu_2)$ becomes its own orthogonal complement in the filtered algebra structure. When the induced bilinear product:

$$H^*(Z,\mu_2)\times H^*(Z,\mu_2)\to H^*(Z,\mu_2)/\mathcal{F}_{2d+2}\cong\mathbb{F}_2$$

is a Euclidean form, $\mathcal{F}_{d+1}H^*(Z,\mu_2)$ is a self-dual code. This is our third construction of binary self-dual code, the *equivariant construction*.

Example 5.4.4. Suppose Y is a hyper-elliptic curve defined by $y^2 = f(x)$ over a finite field $\mathbb{F}_q$. Suppose $f(x)$ has degree $2g+1$, and $f(x) = \Pi_{i=1}^m f_i(x)$ breaks

into m irreducible factors over $\mathbb{F}_q$. Consider the double cover $\pi : Y \to \mathbb{P}^1_{\mathbb{F}_q}$. The Galois group of this cover acts on Y as an involution τ. There are $m+1$ closed points which ramify in this cover: each $f_i(x)$ gives a closed point Z_i of degree $d_i = deg(f_i)$; and there is the point at infinity ∞. Denote their union by Z. $\sum_{j=0}^{\infty} h^j(Z, \mu_2) = \sum_{i=1}^{m+1} \sum_{j=0}^{1} h^j(Z_i, \mu_2) = 2(m+1)$.

Now we will compute $\sum_{i=0}^{\infty} h^i(Y, \mu_2)$:

- $h^0(Y, \mu_2) = 1$.
- By the Kummer sequence:

$$0 \to \mathbb{F}_q^*/2 \to H^1(Y, \mu_2) \to Pic^0(Y)[2] \to 0$$

Thus $h^1(Y, \mu_2) = 1 + \dim_{\mathbb{F}_2} Pic^0(Y)[2]$.

Geometrically, $Pic^0(Y_{\overline{\mathbb{F}_q}})[2]$ is generated as a group by the ramification points of $Y_{\overline{\mathbb{F}_q}}/\mathbb{P}^1_{\overline{\mathbb{F}_q}}$. Therefore $Pic^0(Y)[2]$ is generated by the divisors $(Z_i) - d_i(\infty)$ for $0 \leq i \leq m$, subject to the relation $\sum_{i=0}^{m}(Z_i) - (2g+1)(\infty) = 0$ in $Pic^0(Y)$. Hence

$$dim_{\mathbb{F}_2} Pic^0(Y)[2] = m - 1$$

By Artin-Verdier duality for $Y_{\mathbb{F}_q}$,

$$\sum_{i=0}^{\infty} h^i(Y, \mu_2) = \sum_{i=0}^{4} h^i(Y, \mu_2) = 2(m - 1 + 1 + 1) = \sum_{i=0}^{\infty} h^i(Z, \mu_2)$$

Therefore maximality condition in proposition 5.3.8 is reached.

The isomorphism $H^*_\tau(Y, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1 \cong H^*(Z, \mu_2)$ gives $H^*(Z, \mu_2)$ a filtered Poincaré algebra structure of length 4. The orientation in $H^*(Z, \mu_2)$ is defined by taking the quotient over $\mathcal{F}_2$. The question that whether the bilinear product

$$H^*(Z, \mu_2) \times H^*(Z, \mu_2) \to H^*(Z, \mu_2)/\mathcal{F}_2 \cong \mathbb{F}_2$$

is a Euclidean or an alternate form depends on Y. When the form is Euclidean, then upon fixing a basis, the image $\mathcal{F}_1(H^*(Y, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1) \to H^*(Z, \mu_2)$ is a binary self-dual code. However, in example 5.5.4 we will see an example when this form is alternate. $\triangle$

5.5 Comparison with Construction G

In this section, we will compare the Equivariant Construction in section 5.4 with Construction G in chapter 4. The reader is referred to proposition A.0.10 for a comparison result in the topological situation. The comparison in the arithmetic situation is more complicated though, due to the fact that a *closed point* on an algebraic variety Y_K has cohomological dimension higher than zero, when the base field K is not algebraically closed.

Let Z be a reduced closed sub-scheme of Y. U is the open complement of Z. Denote by $\widetilde{Z}$ the projective limit of the étale neighborhood of Z in Y; denote by $\widetilde{U}$ the open complement of Z in $\widetilde{Z}$.

Proposition 5.5.1. *There is a Mayer-Vietoris sequence:*

$$\cdots H^{i-1}(\widetilde{U},\mathcal{F}) \to H^i(Y,\mathcal{F}) \to H^i(U,\mathcal{F}) \oplus H^i(\widetilde{Z},\mathcal{F}) \to H^i(\widetilde{U},\mathcal{F}) \cdots \tag{5.5.1}$$

Proof. By the long exact sequence [Mil80, proposition III.1.25]:

$$\cdots \to H^i_Z(Y,\mathcal{F}) \to H^i(Y,\mathcal{F}) \to H^i(U,\mathcal{F}) \to H^{i+1}_Z(Y,\mathcal{F}) \cdots \tag{5.5.2}$$

Replace Y by $\widetilde{Z}$, one gets

$$\cdots \to H^i_Z(\widetilde{Z},\mathcal{F}) \to H^i(\widetilde{Z},\mathcal{F}) \to H^i(\widetilde{U},\mathcal{F}) \to H^{i+1}_Z(\widetilde{Z},\mathcal{F}) \cdots \tag{5.5.3}$$

Now we will relate equation 5.5.2 with equation 5.5.3. Suppose Y' is an étale neighborhood of Z, i.e. $Y' \times_Y Z \cong Z$. There is an excision theorem [Mil80, Proposition III.1.27]:

$$H^i_Z(Y,\mathcal{F}) \cong H^i_Z(Y',\mathcal{F})$$

The system of étale neighborhoods of $Z \subset Y$ is a naturally filtered projective system. Since étale cohomology commutes with taking filtered projective limit of schemes, [Mil80, III Lemma 1.16]:

$$H^i_Z(Y,\mathcal{F}) \cong \varinjlim_{Y'} H^i_Z(Y',\mathcal{F}) \cong H^i_Z(\varprojlim Y',\mathcal{F}) = H^i_Z(\widetilde{Z},\mathcal{F})$$

Piecing together equation 5.5.2 and equation 5.5.3, one gets the Mayer-Vietoris sequence in equation 5.5.1. □

Remark 5.5.2. Comparing with the topological Mayer-Vietoris sequence, the intuition behind proposition 5.5.1 is that $\widetilde{Z}$ is viewed as a "tubular neighborhood" of $Z \subset Y$; $\widetilde{U}$ is viewed as the "intersection" of $\widetilde{Z} \cap U$; $U \cup \widetilde{Z}$ "covers" Y. ♢

Corollary 5.5.3. *By the functorial spectral sequence in equation 5.2.1, one gets an equivariant Mayer-Vietoris sequence:*

$$\cdots H_G^{i-1}(\widetilde{U},\mathcal{F}) \to H_G^i(Y,\mathcal{F}) \to H_G^i(U,\mathcal{F}) \oplus H_G^i(\widetilde{Z},\mathcal{F}) \to H_G^i(\widetilde{U},\mathcal{F}) \cdots$$

Example 5.5.4. In the situation of example 5.4.4, $\mathcal{F}_1(H^*(Y,\mu_2)\otimes_{\mathbb{F}_2[t]}k_1) \to H^*(Z,\mu_2)$ is its own orthogonal complement, according to the equivariant construction. The function field of Y is K. $Z = \sqcup_{i=1}^{m+1}$ is the ramification loci in the double cover $\pi : Y \to \mathbb{P}^1_q$. Each closed point Z_i corresponds to a ramified place $\mathfrak{p}_i$ of K. $Z_i = \operatorname{Spec}\mathbb{F}_{\mathfrak{p}_i}$ where $\mathbb{F}_{\mathfrak{p}_i}$ is the residue field of the valuation at $\mathfrak{p}_i$. $\widetilde{Z}_i = \operatorname{Spec}\mathcal{O}^a_{K,\mathfrak{p}_i}$ where $\mathcal{O}^a_{K,\mathfrak{p}_i}$ means the algebraic elements in $\mathcal{O}_{K,\mathfrak{p}_i}$, i.e. the Henselization of $\mathcal{O}_K$ at $\mathfrak{p}_i$. As far as étale cohomology is concerned, one can safely replace $\mathcal{O}^a_{K,\mathfrak{p}_i}$ by $\mathcal{O}_{K,\mathfrak{p}_i}$. $\widetilde{Z} = \sqcup_{i=1}^{m+1}\operatorname{Spec}\mathcal{O}_{K,\mathfrak{p}_i}$. Denote the open complement of $Z \subset \widetilde{Z}$ by $\widetilde{U}$. $\widetilde{U} = \sqcup_{i=1}^{m+1}\operatorname{Spec}K_{\mathfrak{p}_i}$.

Denote the branch loci in $\mathbb{P}^1_{\mathbb{F}_q}$ by Z'; the open complement of $Z' \subset \mathbb{P}^1_{\mathbb{F}_q}$ by A. As reduced schemes $Z' = Z$. Denote the open complement of $Z' \subset \widetilde{Z}'$ by U'. Then $U' = \sqcup_{i=1}^{m+1}\operatorname{Spec}\mathbb{F}_q(x)_{p_i}$, where p_i is the restriction of the place $\mathfrak{p}_i$ on the subfield $\mathbb{F}_q(x) \subset K$. In Construction G, the image of $H^1(A,\mu_2) \to H^1(U',\mu_2)$ is its own orthogonal complement.

Recall a binary self-dual code is a triple: (W,E,V). We will compare the Equivariant Construction and Construction G in two steps. First we will compare the vector spaces (W,V) from the two constructions; Second we will compare whether the product structures on W from the two constructions are the same, together with their basis E.

Comparison of vector spaces:

This argument is similar to proposition A.0.10. By corollary 5.5.3, there is an equivariant Mayer-Vietoris sequence:

$$\cdots \to H^j_\tau(Y,\mu_2) \to H^j(A,\mu_2) \oplus H^j_\tau(\widetilde{Z},\mu_2) \to H^j_\tau(\widetilde{U},\mu_2) \to H^{j+1}_\tau(Y,\mu_2) \to \cdots \tag{5.5.4}$$

We will show that $\forall i$, the map $H^1_\tau(\widetilde{Z}_i,\mu_2) \to H^1_\tau(\widetilde{U}_i,\mu_2)$ is an isomorphism.

By lemma 5.3.4, $H^j(\widetilde{Z}_i,\mu_2) = H^j(Z_i,\mu_2)$. Thus it is easy to see that τ reaches the maximality condition on $\widetilde{Z}_i$. Therefore $H^*_\tau(\widetilde{Z}_i,\mu_2) = H^*(Z_i,\mu_2)\otimes \mathbb{F}_2[t]$.

$h^1_\tau(\widetilde{Z}_i,\mu_2) = 2$.

On the other hand, $H^1_\tau(\widetilde{U},\mu_2) \cong H^1(U',\mu_2)$. Dimension calculation says that the spectral sequences in equation 5.2.1 for both $H^1_\tau(\widetilde{Z}_i,\mu_2)$ and $H^1_\tau(\widetilde{U}_i,\mu_2)$ converge on the E_2 page. We can compare the sequences:

$$\begin{array}{ccccccc} 0 \to H^1(\mathbb{Z}/2, H^0(\mathcal{O}_{K,\mathfrak{p}_i},\mu_2)) & \longrightarrow & H^1_\tau(\mathcal{O}_{K,\mathfrak{p}_i},\mu_2) & \longrightarrow & H^0(\mathbb{Z}/2, H^1(\mathcal{O}_{K,\mathfrak{p}_i},\mu_2)) \to 0 \\ \downarrow d_1 & & \downarrow d_2 & & \downarrow d_3 \\ 0 \to H^1(\mathbb{Z}/2, H^0(K_{\mathfrak{p}_i},\mu_2)) & \longrightarrow & H^1_\tau(K_{\mathfrak{p}_i},\mu_2) & \longrightarrow & H^0(\mathbb{Z}/2, H^1(K_{\mathfrak{p}_i},\mu_2)) \to 0 \end{array} \tag{5.5.5}$$

It is easy to see d_1 is an isomorphism.

On the other hand, $H^1(K_{\mathfrak{p}_i},\mu_2) \cong K^*_{\mathfrak{p}_i}/2$ is generated as a group by $\{\mathfrak{p}_i, u_i\}$, where $\mathfrak{p}_i$ is a uniformizer and u_i is a non-square unit. However, since $K_{\mathfrak{p}_i}/\mathbb{F}_q(t)_{p_i}$ is a ramified extension, $\mathbb{Z}/2$ acts non-trivially on the uniformizer $\mathfrak{p}_i$. Thus $H^0(\mathbb{Z}/2, H^1(K_{\mathfrak{p}_i},\mu_2))$ is represented by $\{u_i\}$ which is the isomorphic image of $d_3(H^0(\mathbb{Z}/2, H^1(\mathcal{O}_{K,\mathfrak{p}_i},\mu_2)))$.

Therefore d_2 is an isomorphism as well.

In equation 5.5.4, by the maximality condition $H^*_\tau(Y,\mu_2) = \beta^*_\tau(Y,\mu_2)$, $H^*_\tau(\widetilde{Z},\mu_2) = \beta^*_\tau(\widetilde{Z},\mu_2)$. Tensor this equation with $\otimes_{\mathbb{F}_2[t]} k_1$, one has

$$\mathcal{F}_1(H^*_\tau(Y,\mu_2)\otimes_{\mathbb{F}_2[t]} k_1) \to H^1(W,\mu_2) \oplus \widetilde{\mathcal{F}}_1(H^*_\tau(\widetilde{Z},\mu_2)\otimes_{\mathbb{F}_2[t]} k_1) \to H^1(U',\mu_2)$$

Since $\widetilde{\mathcal{F}}_1(H^*_\tau(\widetilde{Z},\mu_2)\otimes_{\mathbb{F}_2[t]} k_1) = H^*(Z,\mu_2)$, and the map $H^*(Z,\mu_2) \to H^1(U',\mu_2)$ is an isomorphism. It is easy to see that Equivariant Construction and Construction G have the same W and V.

Comparison of the product structure:

In this section we explore whether the Equivariant Construction and Construction G give the same bilinear product structure on W.

In Construction G, $H^1(U',\mu_2) = \oplus_{i=1}^{m+1} H^1(K_{\mathfrak{p}_i},\mu_2)$. If $\forall i$, $|\mathbb{F}_{\mathfrak{p}_i}| \equiv 3 \bmod 4$, then there is a Euclidean basis for each $H^1(K_{\mathfrak{p}_i},\mu_2)$ which is unique up to permutations, see section 3.2.

In the Equivariant Construction, for simplicity we will only consider the case when Y is an elliptic curve defined by an equation $y^2 = f(x)$. The degree three polynomial $f(x)$ will break into m factors over $\mathbb{F}_q$, where $m = 1$, 2 or 3. We will calculate the filtration $\mathcal{F}$ in $H^*(Z,\mu_2)$ for each value of m. In all three cases, we will see the non-degenerate bilinear product on $H^*(Z,\mu_2)$ is an alternate form. Thus this product is different from that in Construction G. This situation is in marked difference from proposition A.0.10, where different constructions (i.e. the Topological Equivariant Construction and Construction PD) give the same product structure.

We are interested in calculating the map:

$$P : \mathcal{F}_m(H^*_\tau(Y, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1) \to H^*(Z, \mu_2) \tag{5.5.6}$$

We will first consider the L.H.S. of equation 5.5.6. $H^*(Y, \mu_2)$ can be calculated by the Hochschild-Serre spectral sequence $H^i(\mathbb{F}_q, H^j(Y_{\overline{\mathbb{F}}_q}, \mu_2))$, which converges on the E_2 page. $H^i(\mathbb{F}_q, H^j(Y_{\overline{\mathbb{F}}_q}, \mu_2)) = 0$ unless $0 \leq i \leq 1$, $0 \leq j \leq 2$. Each $H^j(Y_{\overline{\mathbb{F}}_q}, \mu_2)$ is a $Gal(\mathbb{F}_q)$ module, and the Galois action commutes with the action of τ. Thus $\mathcal{F}_m(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)$ is also a $Gal(\mathbb{F}_q)$ module, and it is isomorphic to $\oplus_{i=1}^m H^i(Y_{\overline{\mathbb{F}}_q}, \mu_2)$ as a $Gal(\mathbb{F}_q)$ module.

Lemma 5.5.5. *The sequence* $H^i(\mathbb{F}_q, \mathcal{F}_j(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1))$, $i + j = m$ *abuts to* $\mathcal{F}_m(H^*_\tau(Y, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)$ *in increasing order of* i.

Proof. The action of τ on $(Y_{\overline{\mathbb{F}}_q}, \mu_2)$ commutes with the Frobenius action of $Gal(\mathbb{F}_q)$. We have an algebra isomorphism:

$$H^i(\mathbb{F}_q, H^j(Y_{\overline{\mathbb{F}}_q}, \mu_2))\widetilde{\otimes}\mathbb{F}_2[t] \otimes_{\mathbb{F}_2[t]} k_1 \cong H^i(\mathbb{F}_q, H^j(Y_{\overline{\mathbb{F}}_q}, \mu_2)\widetilde{\otimes}\mathbb{F}_2[t] \otimes_{\mathbb{F}_2[t]} k_1) \tag{5.5.7}$$

$\mathcal{F}_m(H^*_\tau(Y, \mu_2)\widetilde{\otimes}\mathbb{F}_2[t] \otimes_{\mathbb{F}_2[t]} k_1)$ is abutted by the spectral sequence $H^i(\mathbb{F}_q, H^j(Y_{\overline{\mathbb{F}}_q}, \mu_2))\widetilde{\otimes}\mathbb{F}_2[t] \otimes_{\mathbb{F}_2[t]} k_1$ where $i + j \leq m$. The later is isomorphic to $H^i(\mathbb{F}_q, \mathcal{F}_j(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2)) \otimes_{\mathbb{F}_2[t]} k_1)$ where $i + j = m$ by equation 5.5.7. △

Now we consider the R.H.S. of equation 5.5.6. $Z = \sqcup_{r=1}^{m+1} Z_r$ is a union of $m + 1$ closed points. Each closed point Z_r corresponds to a map $\pi_r : \operatorname{Spec} \mathbb{F}_{\mathfrak{q}_r} \to \operatorname{Spec} \mathbb{F}_q$. $Z_{r,\overline{\mathbb{F}}_q}$ further breaks into some geometric points over $\overline{\mathbb{F}}_q$. Altogether

$Z_{\overline{\mathbb{F}}_q} = \sqcup_{r=1}^4 pt_r$ has four geometric points. Write $H^0(Z_{\overline{\mathbb{F}}_q}, \mu_2) = \oplus_{r=1}^4 H^0(pt_r, \mu_2)$ with basis $e_r = H^0(pt_r, \mu_2)$. As a $Gal(\mathbb{F}_q)$ module, $H^0(Z_{r,\overline{\mathbb{F}}_q}, \mu_2) \cong \pi_{r,*}\mu_2$. Thus $H^j(\mathbb{F}_q, H^0(Z_{r,\overline{\mathbb{F}}_q}, \mu_2)) = H^j(\mathbb{F}_{\mathfrak{q}_r}, \mu_2)$.

On each closed point $Z_i = \operatorname{Spec} \mathbb{F}_{\mathfrak{q}_i}$, denote $H^0(\mathbb{F}_{\mathfrak{q}_i}, \mu_2) = a_i$, $H^1(\mathbb{F}_{\mathfrak{q}_i}, \mu_2) = b_i$. When $i \neq j$, $H^*(\mathbb{F}_{\mathfrak{q}_i}, \mu_2) \cup H^*(\mathbb{F}_{\mathfrak{q}_j}, \mu_2) = 0$.

Lemma 5.5.6. *As a $Gal(\mathbb{F}_q)$ module, $\mathcal{F}_0(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)$ maps to $\{\sum_{i=1}^4 e_i\}$ in equation A.0.2; $\mathcal{F}_1(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)$ maps to the vector space generated by $\{e_1 + e_2, e_1 + e_3\} + \mathcal{F}_0$; $\mathcal{F}_2(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)$ maps to $\{e_1\} + \mathcal{F}_1$.*

Remark 5.5.7. As a $Gal(\mathbb{F}_q)$ module, $H^*(Z_{\overline{\mathbb{F}}_q}, \mu_2) \cong \mathcal{F}_2(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1) \cong H^*(Y_{\overline{\mathbb{F}}_q}, \mu_2) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus H^1(Y_{\overline{\mathbb{F}}_q}, \mu_2)$. ♢

Remark 5.5.8. If one ignores the $Gal(\mathbb{F}_q)$ structure, it is easily seen from this presentation that the cup-product $H^1 \times H^1 \to H^2 \cong \mathbb{F}_2$ is alternate, which is compatible with a well-known fact on a topological torus. ♢

The map of Galois modules in lemma 5.5.6 induces maps

$$H^i(\mathbb{F}_q, \mathcal{F}_j(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)) \to H^i(\mathbb{F}_q, H^0(Z_{\overline{\mathbb{F}}_q}, \mu_2)) \tag{5.5.8}$$

which are used to compute the map in equation 5.5.6 by lemma 5.5.5.

In our calculation, we will encounter three kinds of $Gal(\mathbb{F}_q)$ modules $N = \mu_2$, $H^1(Y_{\overline{\mathbb{F}}_q}, \mu_2)$ and $\pi_{r,*}\mu_2$. Suppose $Gal(\mathbb{F}_{q_r}/\mathbb{F}_q) = \mathbb{Z}/r$, the canonical map $H^i(\mathbb{Z}/(2r), N) \xrightarrow{\cong} H^i(\mathbb{F}_q, N)$ where $i \leq 1$. We will use the cyclic group to do some explicit computations $P : H^i(\mathbb{Z}/(2r), N) \to H^i(\mathbb{Z}/(2r), N')$ in equation 5.5.8.

Case (1), when $m = 3$:

Z is a union of four closed points over $\mathbb{F}_q$. $dim_{\mathbb{F}_2} Pic(Y)[2] = 2$. The $Gal(\mathbb{F}_q)$ action is trivial. In the following, we will use the shorthand notation $P(H^i(\mathcal{F}_j))$ for $P(H^i(\mathbb{F}_q, \mathcal{F}_j(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)))$.

- $P(H^0(\mathcal{F}_0)) = \{\sum_{r=1}^4 a_r\}$.
- $P(H^1(\mathcal{F}_0)) = \{\sum_{r=1}^4 b_r\}$.
- $P(H^0(\mathcal{F}_1)) = \{a_1 + a_2, a_1 + a_3\} + P(H^0(\mathcal{F}_0))$.
- Using $P(H^1(\mathcal{F}_0) \times H^0(\mathcal{F}_1)) \subset P(H^1(\mathcal{F}_1))$, $P(H^1(\mathcal{F}_1)) = \{b_1 + b_2, b_1 + b_3\} + P(H^1(\mathcal{F}_0))$.
- $P(H^0(\mathcal{F}_2)) = \{a_1\} + P(H^0(\mathcal{F}_1))$.
- $P(H^1(\mathcal{F}_2)) = \{b_1\} + P(H^1(\mathcal{F}_1))$.

Remark 5.5.9. In the algebra $\oplus_{r=1}^{m+1} H^*(\mathbb{F}_{\mathfrak{q}_r}, \mu_2)$, anything multiplied by b_r is either 0 or b_r itself. Thus if the bilinear product induced by the filtration is non-degenerate, $b_r \notin \mathcal{F}_2$. Therefore the fact that $P(H^1(\mathcal{F}_2)) = b_1 + P(H^1(\mathcal{F}_1))$ can be seen more directly. ♢

Case (2), when $m = 1$: Z is a union of two closed points over $\mathbb{F}_q$. Z_1 is the rational point at ∞, Z_2 is a closed point of degree three. $dim_{\mathbb{F}_2} Pic(Y)[2] = 0$.

- $P(H^0(\mathcal{F}_0)) = \{a_1 + a_2\}$.
- $P(H^1(\mathcal{F}_0)) = \{b_1 + b_2\}$.

- Since $H^i(\mathbb{F}_q, H^1(Y_{\overline{\mathbb{F}}_q}, \mu_2)) = 0$, $P(H^i(\mathcal{F}_1)) = P(H^i(\mathcal{F}_0))$.

- $P(H^0(\mathcal{F}_2)) = \{a_1\} + P(H^0(\mathcal{F}_1))$.

- $P(H^1(\mathcal{F}_2)) = \{b_1\} + P(H^1(\mathcal{F}_1))$.

Case (3), when $m = 2$:

Z is a union of three closed points over $\mathbb{F}_q$: Z_1 is the rational point at ∞, Z_2 is another rational point, Z_3 is a closed point of degree two. $dim_{\mathbb{F}_2} Pic(Y)[2] = 1$.

- $P(H^0(\mathcal{F}_0)) = \{a_1 + a_2 + a_3\}$.

- $P(H^1(\mathcal{F}_0)) = \{b_1 + b_2\}$.

- $P(H^0(\mathcal{F}_1)) = \{a_3\} + P(H^0(\mathcal{F}_0))$.

- $P(H^1(\mathcal{F}_1)) = \{b_1 + b_3\} + P(H^1(\mathcal{F}_0))$.

- $P(H^0(\mathcal{F}_2)) = \{a_1\} + P(H^0(\mathcal{F}_1))$.

- $P(H^1(\mathcal{F}_2)) = \{b_1\} + P(H^1(\mathcal{F}_1))$.

It is easily seen that in all the above three cases, the product structures on $H^*(Z, \mu_2)$ are alternate. $\triangle$

5.6 The Maximality Condition

In this section we provide two more examples when the maximality condition in the Equivariant Construction is met.

Remark 5.6.1. In this thesis, we will not compute examples for an involution σ on a high dimension variety over $\mathbb{C}$. If σ is "geometric", i.e. σ acts trivially on the constants $\mathbb{C}$, then the Smith type inequality 5.3.1 does give a restriction on the topological type of the ramification locus and their intersection behaviors. $\diamondsuit$

Example 5.6.2. Suppose $X = \operatorname{Spec} \mathcal{O}_K$ is the ring of integers of an imaginary quadratic number field. Denote by S_f the set of finite ramified places in $K/\mathbb{Q}$. Suppose $|S_f| = n$.

- $h^0(X, \mu_2) = 1$.
- By genus theory, $Pic_X[2] = (\mathbb{Z}/2)^{n-1}$. Thus $h^1(X, \mu_2) = n - 1$.

By Artin-Verdier duality, $\sum_{i=0}^{\infty} h^i(X, \mu_2) = 2n$.

For each finite place $\mathfrak{p} \in S_f$, $\sum_{j=0}^{1} h^j(\mathbb{F}_\mathfrak{p}, \mu_2) = 2$, thus

$\sum_{\mathfrak{p}_i \in S_f} (\sum_{j=0}^{1} h^j(\mathbb{F}_{\mathfrak{p}_i}, \mu_2)) = 2n$. The maximality condition is met. $\triangle$

Example 5.6.3. For a third example, let's consider a hyper-elliptic curve over a local field K. Moreover, suppose we have a model over O_K with good reduction over the residue field k. There is filtration of K-rational points $E^1(K) \subset E(K)$, such that $E^1(K)$ is uniquely divisible prime to the residue characteristic. $E(K)/E^1(K) \cong E(k)$. So $E(K)$ has "less" two-torsion points than $E(K)$, but we may be able to lift the points (x, y) over $\mathbb{F}_p$ to K by Hensel's lemma. Then the Galois module structure is the same.

For any abelian variety J over a local field K, if there is a similar filtration s.t.

there is a uniquely divisible subgroup, and the quotient is isomorphic to its rational point over the finite field, then we can do a similar analysis.

$$\sum_{i=0}^{\infty} dim_{\mathbb{Z}/2} H^i(K, \mu_2) = 4$$

For a hyper-elliptic curve (suppose it is defined by $f(x)$ of degree $2g+1$), suppose there are $m+1$ ramified points, and $Pic_K(X) = m-1$. By our inequality, we have

$$dim_{\mathbb{Z}/2} H^2(X, \mu_2) \geq 2m$$

Look at the spectral sequence $H^p(G_k, H^q(X_{\bar{K}}, \mu_2))$, we know $dim H^2(X, \mu_2) = 2 + H^1(G, H^1(X_{\bar{K}}, \mu_2))$. We can further compute $H^1(G, H^1(X_{\bar{K}}, \mu_2))$ by another Leray-Serre spectral sequence, since the action of G_K on $H^1(X_{\bar{K}}, \mu_2)$ (for simplicity denoted by M) factors through the unramified quotient G_k. Denote $Gal(\bar{K}/K^{un}) = H$.

$$dim H^1(G_K, M) = dim Pic_K[2] + H^1(G_k, H^1(H, M)) = m - 1 + H^1(G_k, H^1(H, M))$$

We claim that as a G_k-Mod, $H^1(H, M)$ is the same as M, then $dim H^1(G_K, M) = 2m - 2$, thus we have an equality, the maximality condition is still met. $\triangle$

Example 5.6.4. In this example we will use the deformation trick to calculate the cohomology "ring" structure of $H^*(Y, \mu_2)$ where Y is an elliptic curve defined by an affine cubic equation $y^2 = f(x)$ over a local field K. In the above example **??** we

have showed that the maximality condition is met in the double cover $Y \to \mathbb{P}^1$, with ramification loci Z. We will calculate the image of equation 5.5.6. The technique is similar to the second half of example 5.5.4. We first collect some useful notation and lemmas.

$H^*(Y, \mu_2)$ can be calculated by the spectral sequence $H^i(K, H^j(Y_{\overline{K}}, \mu_2))$ with terms concentrated on $0 \leq i \leq 2$, $0 \leq j \leq 2$.

Lemma 5.6.5. *The sequence* $H^i(K, \mathcal{F}_j(H^*_\tau(Y_{\overline{K}}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1))$, $i + j = m$ *abuts to* $\mathcal{F}_m(H^*_\tau(Y, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)$ *in increasing order of* i.

$Z = \sqcup_{r=1}^{m+1} Z_r$ is a union of $m+1$ closed points. Each closed point Z_r corresponds to a map $\pi_r : \operatorname{Spec} K_r \to \operatorname{Spec} K$. $Z_{r,\overline{K}}$ further breaks into some geometric points over $\overline{\mathbb{K}}$. Altogether $Z_{\overline{K}} = \sqcup_{r=1}^{4} pt_r$ has four geometric points. Write $H^0(Z_{\overline{K}}, \mu_2) = \oplus_{r=1}^{4} H^0(pt_r, \mu_2)$ with basis $e_r = H^0(pt_r, \mu_2)$. As a $Gal(K)$ module, $H^0(Z_{r,\overline{K}}, \mu_2) \cong \pi_{r,*}\mu_2$. Thus $H^j(K, H^0(Z_{r,\overline{K}}, \mu_2)) = H^j(K_r, \mu_2)$.

For each K_r, denote $H^0(K_r, \mu_2) = \{a_r\}$, $H^1(K_r, \mu_2) \cong K_r^*/2$ is generated by $\{\mathfrak{p}_r, u_r\}$ as a group, where $\mathfrak{p}_r$ is a uniformizer for the valuation in K_r, and u_r is a non-square unit. For notational convenience denote u_r by b_r, $\mathfrak{p}_r$ by c_r as classes in $H^1(K_r, \mu_2)$. $H^2(K_r, \mu_2) = \{d_r\}$.

a_r is an identity element in $H^*(K_r, \mu_2)$, $b_r c_r = d_r$, $b_r^2 = 0$.

$c_r^2 = d_r$ if $|\mathbb{F}_r| \equiv 3 \bmod 4$; $c_r^2 = 0$ if $|\mathbb{F}_r| \equiv 1 \bmod 4$.

Since the $Gal(K)$ action factors through $Gal(K^{un}/K)$, lemma 5.5.6 still holds

as a map of $Gal(K)$ modules. This map induces

$$H^i(K, \mathcal{F}_j(H^*_\tau(Y_{\overline{K}}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)) \to H^i(K, H^0(Z_{\overline{K}}, \mu_2)) \tag{5.6.1}$$

which are used to compute the map P in equation 5.5.6 by lemma 5.6.5.

In the following calculation, we will encounter three kinds of $Gal(K)$ modules $N = \mu_2$, $H^1(Y_{\overline{K}}, \mu_2)$ and $\pi_{r,*}\mu_2$. The canonical map $H^i(Gal(K_r(\sqrt{u_r}, \sqrt{p_r})/K), N) = H^i(\mathbb{Z}/(2r) \times \mathbb{Z}/2, N) \xrightarrow{\cong} H^i(K, N)$ where $i \leq 1$. We will use the abelian group to do some explicit computations $P : H^i(\mathbb{Z}/(2r) \times \mathbb{Z}/2, N) \to H^i(\mathbb{Z}/(2r) \times \mathbb{Z}/2, N')$ in equation 5.6.1. For $i = 2$ we do not need explicit calculations. When b, c are classes in H^1, $b \cup c$ is a class in H^2. As P is a map of cohomology rings, $P(b \cup c) = P(b) \cup P(c)$.

Case (1), when $m = 3$:

Z is a union of four closed points over K. $dim_{\mathbb{F}_2} Pic(Y)[2] = 2$. The $Gal(K)$ action is trivial. In the following, we will use the shorthand notation $P(H^i(\mathcal{F}_j))$ for $P(H^i(K, \mathcal{F}_j(H^*_\tau(Y_{\overline{K}}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)))$.

- $P(H^0(\mathcal{F}_0)) = \{\sum_{r=1}^4 a_r\}$.
- $P(H^1(\mathcal{F}_0)) = \{\sum_{r=1}^4 b_r, \sum_{r=1}^4 c_r\}$.
- Since $P(H^1(\mathcal{F}_0)) \times P(H^1(\mathcal{F}_0)) \subset P(H^2(\mathcal{F}_0))$, $P(H^2(\mathcal{F}_0)) = \{\sum_{r=1}^4 d_r\}$
- $P(H^0(\mathcal{F}_1)) = \{a_1 + a_2, a_1 + a_3\} + P(H^0(\mathcal{F}_0))$.
- Using $P(H^1(\mathcal{F}_0) \times H^0(\mathcal{F}_1)) \subset P(H^1(\mathcal{F}_1))$, $P(H^1(\mathcal{F}_1)) = \{b_1 + b_2, b_1 + b_3, c_1 + c_2, c_1 + c_3\} + P(H^1(\mathcal{F}_0))$.

- $P(H^2(\mathcal{F}_1)) = \{d_1 + d_2, d_1 + d_3\} + P(H^2(\mathcal{F}_0))$.
- $P(H^0(\mathcal{F}_2)) = \{a_1\} + P(H^0(\mathcal{F}_1))$.
- $P(H^1(\mathcal{F}_2)) = \{b_1, c_1\} + P(H^1(\mathcal{F}_1))$.
- $P(H^2(\mathcal{F}_2)) = \{d_1\} + P(H^2(\mathcal{F}_1))$.

Remark 5.6.6. In the algebra $\oplus_{r=1}^{m+1} H^*(K_r, \mu_2)$, anything multiplied by d_r is either 0 or d_r itself. Thus if the bilinear product induced by the filtration is non-degenerate, $d_r \notin \mathcal{F}_3$. Therefore the fact that $P(H^2(\mathcal{F}_2)) = d_1 + P(H^2(\mathcal{F}_1))$ can be seen more directly. $\diamondsuit$

Case (2), when $m = 1$: Z is a union of two closed points over K. Z_1 is the rational point at ∞, Z_2 is a closed point of degree three. $dim_{\mathbb{F}_2} Pic(Y)[2] = 0$.

- $P(H^0(\mathcal{F}_0)) = \{a_1 + a_2\}$.
- $P(H^1(\mathcal{F}_0)) = \{b_1 + b_2\}$.
- Since $H^i(K, H^1(Y_{\overline{K}}, \mu_2)) = 0$, $P(H^i(\mathcal{F}_1)) = P(H^i(\mathcal{F}_0))$.
- $P(H^0(\mathcal{F}_2)) = \{a_1\} + P(H^0(\mathcal{F}_1))$.
- $P(H^1(\mathcal{F}_2)) = \{b_1\} + P(H^1(\mathcal{F}_1))$.

Case (3), when $m = 2$:

Z is a union of three closed points over K: Z_1 is the rational point at ∞, Z_2 is another rational point, Z_3 is a closed point of degree two, thus $c_3^2 = 0$ in $H^2(K_3, \mu_2)$. $dim_{\mathbb{F}_2} Pic(Y)[2] = 1$.

- $P(H^0(\mathcal{F}_0)) = \{a_1 + a_2 + a_3\}$.
- $P(H^1(\mathcal{F}_0)) = \{b_1 + b_2, c_1 + c_2 + c_3\}$.
- Since $P(H^1(\mathcal{F}_0)) \times P(H^1(\mathcal{F}_0)) \subset P(H^2(\mathcal{F}_0))$, $P(H^2(\mathcal{F}_0)) = \{d_1 + d_2\}$
- $P(H^0(\mathcal{F}_1)) = \{a_3\} + P(H^0(\mathcal{F}_0))$.
- $P(H^1(\mathcal{F}_1)) = \{b_1 + b_3, c_3\} + P(H^1(\mathcal{F}_0))$.
- $P(H^2(\mathcal{F}_1))/P(H^2(\mathcal{F}_0))$ needs to pair non-trivially with $P(H^0(\mathcal{F}_1))/P(H^0(\mathcal{F}_0))$, thus $P(H^2(\mathcal{F}_1)) = \{d_1 + d_3\} + P(H^2(\mathcal{F}_0))$.
- $P(H^0(\mathcal{F}_2)) = \{a_1\} + P(H^0(\mathcal{F}_1))$.
- $P(H^1(\mathcal{F}_2)) = \{b_1, c_1\} + P(H^1(\mathcal{F}_1))$.
- $P(H^2(\mathcal{F}_2)) = \{d_1\} + P(H^2(\mathcal{F}_1))$.

Based on the above calculation, the 'deformation trick' says that the product $H^2(Y, \mu_2) \times H^2(Y, \mu_2) \to H^4(Y, \mu_2) = \mathbb{Z}/2$ is alternate. $\triangle$

Appendix A

Topological constructions of binary self-dual codes

In Append A we review two constructions of binary self-dual codes coming from topology, which were introduced in [Pup95][Pup01] and [KP08].

Consider an involution τ on a closed (i.e. compact and no boundary) manifold X of dimension $2r+1$ with m isolated fixed points, $\{pt_i\}_{i=1}^{m}$. k is a field of characteristic 2. By [AP93, Corollary 1.3.8]:

Lemma A.0.7.

- *There is a Smith type inequality:*

$$m \leq \sum_{i=0}^{2r+1} h^i(X, k) \tag{A.0.1}$$

- *m is an even integer.*

When equality is reached in equation A.0.1, τ is called an involution with "maximal" number of fixed points. Under this condition, by proposition 5.3.8, the equivariant complex $\beta^*_\tau(X,k)$ has a minimal Hirsch-Brown model $H^*(X,k)\widetilde{\otimes}k[t]$ with trivial differential. Thus $H^*_\tau(X,k) \cong \beta^*_\tau(X,k)$. There is an isomorphism

$$H^*(X,k) \xleftarrow{gr} H^*(X,k)\widetilde{\otimes}k[t]\otimes_{k[t]}k_1 \cong \oplus_{i=1}^m H^*(pt_i,k)\otimes k[t]\otimes_{k[t]}k_1 \cong \oplus_{i=1}^m H^*(pt_i,k) = k^{\oplus m} \tag{A.0.2}$$

Since $H^*(X,k)$ is a Poincaré algebra of dimension $2r+1$, by proposition 5.4.1 $k^{\oplus m}$ gets the structure of a filtered Pioncaré algebra:

$$\mathcal{F}_{-1} = 0 \subset \mathcal{F}_0 \subset \cdots \mathcal{F}_{2r+1} = k^{\oplus m}$$

In particular, there is a non-degenerate pairing $k^{\oplus m} \times k^{\oplus m} \to k^{\oplus m} \to k$ which is the composition of the cup-product in $\oplus_{i=1}^m H^*(pt_i,k)$ followed taking quotient over $\mathcal{F}_{2r}$. The cup-product in $\oplus_{i=1}^m H^*(pt_i,k)$ is just the component-wise multiplication in $k^{\oplus m}$. Since $h^{2r+1}(X,k) = 1$. When $k = \mathbb{F}_2$, $\mathcal{F}_{2r}$ can be specified by the following lemma:

Lemma A.0.8. *Under the component-wise multiplication on $\mathbb{F}_2^m$, there is a unique subspace $\mathcal{F}_{2r}$ making the bilinear product a non-degenerate form. Moreover, this form is Euclidean, and the canonical basis $\{e_i\}_{i=1}^m$ is a Euclidean basis.*

Proof. Write the canonical basis in $\mathbb{F}_2^m$ as $\{e_i\}_{i=1}^m$. Since the product of e_i with any elements in $\mathbb{F}_2^m$ is either 0 or itself, therefore $e_i \notin \mathcal{F}_{2r}$, otherwise the bilinear product is degenerate on e_i. Since $\langle e_i + e_j, e_i\rangle = (e_i+e_j)e_i = e_i \bmod \mathcal{F}_{2r} = 1$,

$\langle e_i + e_j, e_j \rangle = 1$, thus $\langle e_i + e_j, e_i + e_j \rangle = 0$ which implies $e_i + e_j \in \mathcal{F}_{2r}$. Any word of even weight belongs to $\mathcal{F}_{2r}$. The product on $\mathbb{F}_2^m$ is the standard Euclidean form where $\{e_i\}_{i=1}^m$ is a basis. □

By lemma A.0.8, the triple $(\mathbb{F}_2^m, \{e_i\}_{i=1}^m, \mathcal{F}_r)$ is a self-dual code. This is the *Topological Equivariant Construction* of self-dual codes.

A related topological construction, which uses Poincaré duality on a compact manifold with boundary, is sketched in the following. We will call it the *Poincaré Duality Construction* :

Consider an involution τ on a closed (i.e. compact and no boundary) manifold X of dimension $2r + 1$ with m isolated fixed points, where m is not necessarily maximal. Take out an open ball D_i around each fixed point pt_i, $\tau|_{X \setminus \sqcup_{i=1}^m D_i}$ is free. Denote the quotient manifold by $W := \tau|_{X \setminus \sqcup_{i=1}^m D_i}$. W is a manifold with boundary, where $\partial W = \sqcup_{i=1}^m \mathbb{RP}^{2r}$. From the long exact sequence of the pair $(W, \partial W)$,

$$\cdots H^r(W, \partial W, k) \to H^r(W, k) \to H^r(\partial W, k) \to H^{r+1}(W, \partial W, k) \cdots$$

using Poincaré duality, the image of the middle dimension cohomology $H^r(W, k) \to H^r(\partial W, k)$ is its own orthogonal-complement with respect to the non-degenerate pairing

$$H^r(\partial W, k) \times H^r(\partial W, k) \to H^{2r}(\partial W, k) \to H^{2r+1}(W, \partial W, k) \tag{A.0.3}$$

Since $\partial W = \sqcup_{i=1}^m \mathbb{R}P^{2r}$, there is a canonical basis

$$H^j(\partial W, k) \cong \oplus_{i=1}^m H^j(\mathbb{R}P^{2r}, k) \cong k^{\oplus m}$$

for $0 \leq j \leq 2r$. Under this basis, the product $H^r \times H^r \to H^{2r}$ is the component-wise multiplication $k^{\oplus m} \times k^{\oplus m} \to k^{\oplus m}$. On the other hand, it is a geometric fact that $H^{2r}(\partial W, k) = k^{\oplus m} \xrightarrow{\delta} k = H^{2r+1}(W, \partial W, k)$ corresponds to taking sums of the coordinates. Finally, the bilinear form in equation A.0.3 is a Euclidean form, where the canonical basis is a Euclidean basis. When $k = \mathbb{F}_2$ the image $H^r(W, k) \to H^r(\partial W, k)$ is a binary self-dual code.

The universality of the Poincaré Duality Construction is shown by the following result [KP08, Proposition 3.1], which was proved using oriented cobordism theory. This shows that there are a lot of involutions on 3-manifolds:

Theorem A.0.9. *Every binary self-dual code can be obtained from an involution on an orientable 3-manifold.*

In the topological situation, when τ has the maximal number of fixed points, the *Equivariant Construction* and *Construction PD* are compatible with each other, which was proved in [KP08]:

Consider the pair $(X \setminus \sqcup_{i=1}^m D_i, \sqcup_{i=1}^m D_i)$. Up to homotopy, we can say their intersection is a union of $2r$-dimension spheres $\sqcup_{i=1}^m S_i^{2r}$. When a finite group G acts freely on a manifold Y, $H_G^*(Y, k) = H^*(Y/G, k)$. We have the equivariant Mayer-Vietoris sequence:

$$\cdots \oplus_{i=1}^m H^j(\mathbb{R}P_i^{2r}, k) \to H_\tau^j(X, k) \to H^j(W, k) \oplus \oplus_{i=1}^m H_\tau^j(D_i, k) \to \oplus_{i=1}^m H^j(\mathbb{R}P_i^{2r}, k) \cdots \tag{A.0.4}$$

Let's look at the short exact sequence

$$H^j_\tau(X,k) \to H^j(W,k) \oplus \oplus_{i=1}^m H^j_\tau(D_i,k) \to \oplus_{i=1}^m H^j(\mathbb{R}P_i^{2r},k)$$

By the maximality condition, $H^*_\tau(X,k) \cong \beta^*_\tau(X,k)$, $H^*_\tau(D_i,k) \cong \beta^*_\tau(D_i,k)$. Apply the exact functor $\otimes_{k[t]} k_1$ to this exact sequence, we get:

$$\mathcal{F}_j(H^*_\tau(X,k) \otimes_{k[t]} k_1) \to H^j(W,k) \oplus \oplus_{i=1}^m \mathcal{F}_j(H^*_\tau(D_i,k) \otimes_{k[t]} k_1) \to \oplus_{i=1}^m H^j(\mathbb{R}P_i^{2r},k) \tag{A.0.5}$$

For dimension reason, $\forall j \geq 0$,

$$\mathcal{F}_j(H^*_\tau(D_i,k) \otimes_{k[t]} k_1) = H^*_\tau(D_i,k) \otimes_{k[t]} k_1$$

By the localization theorem, $H^*_\tau(D_i,k) \otimes_{k[t]} k_1 \cong H^*_\tau(pt_i,k) \otimes_{k[t]} k_1$. Also

$$H^*_\tau(pt_i,k) \otimes_{k[t]} k_1 \cong H^j(\mathbb{R}P_i^{2r},k) \cong k$$

Combing these identifications, one can show

Proposition A.0.10. *In equation A.0.5, the image of* $\mathcal{F}_j(H^*_\tau(D_i,k) \otimes_{k[t]} k_1) \to \oplus_{i=1}^m H^*_\tau(pt_i,k) \otimes_{k[t]} k_1$ *is the same as the* $H^j(W,k) \to \oplus_{i=1}^m H^j(\mathbb{R}P_i^{2r},k)$. *As a result, when* $j = r$, *the Equivariant Construction and the Poincaré Duality Construction PD give the same code.*

Appendix B

The Minimal Hirsch-Brown Model

Another model is the so-called 'minimal Hirsch-Brown' model. Now we recall some homological algebra construction of the Borel construction of equivariant homology. k is a field. $\mathcal{E}_*(G) = W_*(EG) \cong W_*(BG) \otimes k[G]$ as a $k[G]$-module, $C_* \in \partial gk[G]$-module, form $\beta_*^G(C_*) := \mathcal{E}_*(G) \otimes_{k[G]} C_*$. As a k-module, $\beta_*^G(C_*) = W_*(BG) \otimes C_*$, but the differential is not the componentwise differential on each factor, thus we will sometimes write $W_*(BG)\widetilde{\otimes}C_*$ to indicate the twist in the differential.

Let R be a commutative graded algebra over a field k. R is connected, i.e. $R^i = 0$ for $i < 0$ and $R^0 = k$ and with a canonical augmentation $\epsilon : R \to k$, being the identity on R^0 and 0 otherwise. An object is a graded R module means that the map $R \otimes \widetilde{K} \to \widetilde{K}$ preserves the total degree, and it is a δgR-module if the differential is R linear.

It s easy to see that there is a functor $k\otimes_R : \delta gR - Mod \to \delta gk - Mod$,

$\widetilde{K} \to k \otimes_R \widetilde{K}$. This functor preserves homotopies.

When $\widetilde{K} = R \otimes K$ has a special form, the differential on $\delta_{\widetilde{K}}$ does not necessarily coincide with $id_k \otimes \delta_K$. To indicate the twist, we will sometimes write $\widetilde{K} = R\widetilde{\otimes}K$. By assumption, $\tilde{f} : \widetilde{K} \to \widetilde{L}$ is R-linear, therefore it is completely determined by its restriction to

$$k \otimes K \to \widetilde{L}$$

The situation on $\tilde{\delta_{\widetilde{K}}}$ is analogous. Thus why we call it a 'deformation'.

(More details can be put here. We will be cautious as when R is $\mathbb{Z}[G]$ or $k[t]$?)

For the purpose of explicit calculation one would like to replace a complex by a homotopy equivalent one, which is "as small as possible''. For this purpose we need the following lemmas.

Let $R\widetilde{\otimes}K$ be a twisted tensor product and $f : K \to L$ be a homotopy equivalence in $\delta gk-Mod$. Assume K and L are bounded below, there is a twisted tensor product $R\widetilde{\otimes}L$ and a homotopy equivalence $\tilde{f} : R\widetilde{\otimes}K \to R\widetilde{\otimes}L$ in $\delta gk-Mod$ s.t. $f = id_k \otimes_R \tilde{f}$.

When K is bounded below, $R\widetilde{\otimes}K$ up to homotopy in $\delta gk-Mod$ can be replaced by $R\widetilde{\otimes}H(K)$. This is the so-called 'minimal" HB model.

Appendix C

The Glossary of Derived Categories

Consider the category of complexes of sheaves on the small étale site X_{et}, denote $\mathcal{K}om(X)$. Two complexes K and L are identified if they are chain homotopic to each other. They are called *quasi-isomorphic* if there is a map $f : K \to L$ that induces an isomorphism $f : \mathcal{H}^*(K) \to \mathcal{H}^*(L)$. Here we use the short-hand notation $\mathcal{H}^*(K)$ to denote $\mathcal{H}^i(K)$ for all i. $\mathcal{K}om(X)$ mod out the quasi-isomorphism relations is called the derived category of complexes of sheaves on X_{et}, denoted $\mathcal{D}(X)$.

$\mathcal{K}om^b(X)$ is the full subcategory of $\mathcal{K}om(X)$ of bounded complexes. The objects in $\mathcal{K}om^b(X)$ are a complex K s.t. $H^i(K) \neq 0$ for only finitely many i. If R is a ring, the category of complexes of sheaves of R-modules on X_{et} is denoted $\mathcal{K}om(X, R)$. Corresponding, their derived categories are $\mathcal{D}^b(X)$, $\mathcal{D}(X, R)$ or $\mathcal{D}^b(X, R)$.

One can define derived functors.

Bibliography

[AGV73] M. Artin, A. Grothendieck, and J. L. Verdier. *Thorie des topos et cohomologie tale des schmas, Tome 3*. Lecture notes in math. 305, Springer, 1973.

[Alb38] A. A. Albert. Symmetric and alternate matrices in an arbitrary eld. i. *Trans. Amer. Math. Soc.*, 43(3):386436, 1938.

[AP93] C Allday and Volkern Puppe. *Cohomological methods in transformation groups*. Cambridge University Press, 1993.

[BB11] Stefka Bouyuklieva and Iliya Bouyukliev. An algorithm for classification of binary self-dual codes. *arxiv1106.5930*, June 2011.

[CS99] J H Conway and N.J.A Sloane. *Sphere Packings, Lattices and Groups*. Springer, 1999.

[CZ12] Ted Chinburg and Ying Zhang. Every Binary Self-Dual Codes Arises from Hilbert Symbols. *Homology, homotopy and applications*, 14(2):189–196, 2012.

[DGH97] Steven T Dougherty, T Aaron Gulliver, and Masaaki Harada. Extremal Binary Self-Dual Codes. *IEEE Transactions on Information Theory*, 43(6):2036–2047, 1997.

[Fre82] M. H. Freedman. The topology of four-dimensional manifolds. *J. Differential Geom*, 17(3):357–453, 1982.

[Gro57] A. Grothendieck. Sur quelques points d'algbre homologique, ii. *Tohoku Math. J. (2)*, 9(3):119–221, 1957.

[GS99] Robert E. Gompf and Andraás I. Stipsicz. *4-Manifolds and Kirby Calculus*. Graduate Studies in Mathematics vol 20, AMS, 1999.

[Hub93] Roland Huber. Etale cohomology of henselian rings and cohomology of abstract riemann surfaces of fields. *Mathematische Annalen*, 295(1):703–708, 1993.

[KB12] A. Munemasa K. Betsumiya, M. Harada. A complete classication of doubly even self-dual codes of length 40. *arxiv 1104.3727*, pages 1–15, 2012.

[KKM91] Masaaki Kitazume, Takeshi Kondo, and Izumi Miyamoto. Even lattices and doubly even codes. *J. Math. Soc. Japan*, 43(1):67–87, 1991.

[KP08] Matthias Kreck and Volker Puppe. Involutions on 3-manifolds and self-dual, binary codes. *Homology, Homotopy and Applications*, 10(2):139–148, 2008.

[Mil80] J.S. Milne. *Étale cohomology*. Princeton University Press, 1980.

[Mil06] J. S. Milne. *Arithmetic duality theorems*. Booksurge Publishing, 2006.

[Mil11] J. S. Milne. *Algebraic number theory*. 2011.

[Mor08] Baptiste Morin. Utilisation dune cohomologie étale équivariante en topologie arithmétique. *Compositio Mathematica*, 144(01):32–60, January 2008.

[Neu99] Jurgen Neukirch. *Algebraic Number Theory*. Springer, 1999.

[OP92] Haluk Oral and Kevin T. Phelps. Almost all self-dual codes are rigid. *Journal of Combinatorial Theory (Series A)*, 60:264–276, 1992.

[PH] V.S. Pless and W.C. Huffman. *Handbook of Coding Theory*.

[Ple72] Vera Pless. A Classification of Self-Orthogonal Codes over GF(2). *Discrete Mathematics*, 3:209–246, 1972.

[Ple98] V. Pless. *Introduction to the theory of error-correcting codes-3rd ed.* John Wiley and Sons, Inc., 1998.

[Pup95] V. Puppe. Simply connected 6-dimensional manifolds with little symmetry and algebras with small tangent space. In *Prospects in Topology*, pages 283–302. Annals of Math. Studies 138, Princeton University Press, 1995.

[Pup01] V. Puppe. Group Actions and Codes. *Canadian Journal of Mathematics*, 53(1):212–224, February 2001.

[RS98] E.M Rains and N.J.A Sloane. Self-Dual Codes. In V.S. Pless and W.C. Huffman, editors, *Handbook of Coding Theory*, pages 177–294. Elsevier, 1998.

[Ser73] J. P. Serre. *A Course in Arithmetic*. Springer, 1973.

[Sym04] Peter Symonds. Smith theory for algebraic varieties. *Algebraic and Geometric Topology*, 4:121–131, 2004.