1-1-2013

Arithmetic Constructions Of Binary Self-Dual Codes

Ying Zhang
University of Pennsylvania, yinzhang@sas.upenn.edu

Arithmetic Constructions Of Binary Self-Dual Codes

Abstract

The goal of this thesis is to explore the interplay between binary self-dual codes and the \'etale cohomology of arithmetic schemes. Three constructions of binary self-dual codes with arithmetic origins are proposed and compared: Construction $\Q$, Construction G and the Equivariant Construction. In this thesis, we prove that up to equivalence, all binary self-dual codes of length at least 4 can be obtained in Construction $\Q$. This inspires a purely combinatorial, non-recursive construction of binary self-dual codes, about which some interesting statistical questions are asked. Concrete examples of each of the three constructions are provided. The search for binary self-dual codes also leads to inspections of the cohomology ``ring" structure of the \'etale sheaf μ_2 on an arithmetic scheme where 2 is invertible. We study this ring structure of an elliptic curve over a p-adic local field, using a technique that is developed in the Equivariant Construction.

Degree Type

Dissertation

Degree Name

Doctor of Philosophy (PhD)

Graduate Group

Mathematics

First Advisor

Ted Chinburg

Keywords

Binary self-dual code, Etale cohomology

Subject Categories

Mathematics

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

Supervisor of Dissertation

Ted Chinburg, Professor of Mathematics

Graduate Group Chairperson

David Harbater, Professor of Mathematics

Dissertation Committee

Florian Pop, Professor of Mathematics

Ted Chinburg, Professor of Mathematics

Henry Towsner, Professor of Mathematics

ARITHMETIC CONSTRUCTIONS OF BINARY SELF-DUAL CODES

Dedicated to my parents,
Yongzhao Zhang and Shuyan Zhang

Acknowledgments

I would like to express my sincere thanks to my supervisor Ted Chinburg for his constant support and guidance throughout my graduate studies. His expertise and advice are invaluable to me in many ways beyond I could imagine. Among many other things, I have learned my first class in algebraic number theory from him, prepared for my qualify exam under his directions, and have had his motivating collaboration in my first publication. It has been a great pleasure to work with him. Without his helpful suggestions and instructions, this work would not have been possible.

I would also like to thank Florian Pop and David Harbater for their constant help and illuminating discussions in mathematics. Henry Towsner, for serving on my thesis committee. David Zywina, Jonathan Block and Tony Pantev from whom I have benefited a lot from their classes. Robin Pemantle and Dennis DeTurck for giving me many helpful suggestions. Janet Burns, Monica Pallanti, Paula Scarborough for their constant help in my daily life at the Math department, it is their dedication that makes the department such an enjoyable place to work at.

I want to express my gratitude to Wenxuan Lu, whose passion for mathematics has always been encouraging to me. I have enjoyed my life as a graduate student at Penn to live in a big family of many helpful fellow graduate students: Zhentao Lu, Adam Topaz, Ryan Eberhart, Taisong Jing, Shanshan Ding, Hilaf Hasson, Justin Curry, Ryan Manion, Elaine So, Yang Liu, Ying Zhao, Zhaoting Wei, Tong Li, Haomin Wen, Xiaoxian Liu, Yiqing Cai and many others. I can not forget the many mornings, afternoons and evenings we spent in DRL discussing problems. I am also grateful for my friends in Philadelphia: Hao Sun, Yubin Bai, Zhaoxia Qian, Na Zhang, Rong Shen, Lai Jiang, Yang Jiao, Yin Xia, Chi Liu, Yan Wang, Naibo Chen, Yuyuan Liu, Shaohui Wang, Zuolu Liu. I am grateful for the many happy moments they brought in my life.

Last but not least, I want to thank my parents Yongzhao Zhang and Shuyan Zhang for giving birth to me, raising me up and their unfailing love, understanding and support for me over the years. This thesis is dedicated to them.

ABSTRACT

ARITHMETIC CONSTRUCTIONS OF BINARY SELF-DUAL CODES

Ying Zhang

Ted Chinburg

The goal of this thesis is to explore the interplay between binary self-dual codes and the étale cohomology of arithmetic schemes. Three constructions of binary self-dual codes with arithmetic origins are proposed and compared: Construction $\mathbb{Q}$, Construction G and the Equivariant Construction. In this thesis, we prove that up to equivalence, all binary self-dual codes of length at least 4 can be obtained in Construction $\mathbb{Q}$. This inspires a purely combinatorial, non-recursive construction of binary self-dual codes, about which some interesting statistical questions are asked. Concrete examples of each of the three constructions are provided. The search for binary self-dual codes also leads to inspections of the cohomology "ring" structure of the étale sheaf μ_2 on an arithmetic scheme where 2 is invertible. We study this ring structure of an elliptic curve over a p-adic local field, using a technique that is developed in the Equivariant Construction.

Contents

Chapter 1

Introduction

The goal of this thesis is to explore the interplay between binary self-dual codes and the étale cohomology of arithmetic schemes. In chapter 2, we will recall some definitions and general facts about codes. A construction of binary self-dual codes is introduced in chapter 3 using the arithmetic 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 on arithmetic questions inspired by the search for binary self-dual codes. Two more constructions of binary codes are introduced and compared, which we call *Construction G* and the *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 the existence of smooth structures on it [GS99].

For an involution τ on a closed manifold, it is widely known the cohomology of the fixed loci is related to the cohomology 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 their Poincaré Duality Construction. The Equivariant Construction and the Topological Equivariant Construction can also be developed in a common framework. This is not surprising since the classical motivation of étale cohomology is to seek a "topological" treatment of schemes.

Nevertheless, we draw the readers' attention to some subtle differences between the topological and arithmetic sides of the story. For an involution τ on a closed manifold with isolated fixed points, the Topological Equivariant Construction and Pioncaré Duality Construction give rise to the same binary self-dual codes, see Proposition A.0.12. In the arithmetic situation, the Equivariant Construction and Construction G do not necessarily produce the same codes, 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 another technical difference in the Equivariant Construction: while many theorems about the Topological Equivariant Construction are stated and proved using the homotopy type of CW complexes, we avoid the machinery of étale homotopy theory in this thesis. Instead, we use the modified equivaiant étale cohomology by B. Morin [Mor08] as a technical tool. This tool helps us build up the necessary results for the arithmetic Equivariant Construction, which in addition answers in Example 5.5.4 a question 4.2.6 raised in Construction G.

Finally, as this thesis is the first attempt to explore the interplay between binary self-dual codes and the étale cohomology space of an arithmetic scheme, we also consider it meaningful to raise interesting questions in this field. In particular, the reader is invited to look at Question 3.4.2, Question 3.4.4 and Question 4.1.6.

Chapter 2

Coding Theory Background

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 reader is referred to standard texts like [CS99, Chapter 3][PH98][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 of $\mathbb{F}^n$. 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 codes over a field $\mathbb{F}$.

Let C be a linear code contained in an n-dimensional vector space $W/\mathbb{F}$. We will assume W is equipped with a chosen 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 spaces, a "canonical" basis is usually not obvious in W. In some cases, the existence of a desirable basis is even in question, see Example 4.2.5.

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, $\langle\ ,\ \rangle\colon W \times W \to \mathbb{F}$ is a *non-degenerate symmetric bilinear form* if it satisfies the following conditions:

- $\langle x, y\rangle = \langle y, x\rangle$.

- For a, $b \in \mathbb{F}$, $\langle ax + by, z\rangle = a\langle x, z\rangle + b\langle y, z\rangle$.

- If $\langle x, y\rangle = 0$ for all $y \in W$, then $x = 0$,

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

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i \tag{2.1.1}$$

This product is a non-degenerate symmetric bilinear form. For a bilinear form $\langle, \rangle$, if there is a basis E under which the form is defined as in Equation 2.1.1, then $\langle, \rangle$ is called a *Euclidean inner product*. The basis E is called a *Euclidean basis*. △

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.

2.2 Binary Self-dual Codes

Consider an m dimension vector space W over $\mathbb{F}_2$ with a basis E. We can define the Euclidean inner product under this basis. If C is an n dimensional self-orthogonal code of maximal dimension, then $m = 2n$ is even. In addition, if we specify E 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.x If W has a Type II code contained in it, the dimension of W is necessarily a multiple of 8 [RS98].

Given two codes (W, V, E), (W', V', E'), consider the canonical isomorphism between two ordered sets $\phi : E \to E'$ where $\phi(e_i) = e'_i$. ϕ can be extended to an $\mathbb{F}_2$-linear isomorphism $W \to W'$. If $\phi(V) = V'$, then (W, V, E) is considered to be *isomorphic* to the code (W', V', E'). Without loss of generality, we can assume $W = W'$. Apply a permutation s to the ordered set E. If under the canonical isomorphism $\phi : E \to s(E)$, V is mapped to itself, then s is said to be an element in the *automorphism group* of the code (W, E, V). The automorphism group of a code is a subgroup of the full symmetric group S_m. In general, if there is permutation s such that $(W, s(E), V)$ is isomorphic to (W, E', V'), then (W, E, V) is said to be *equivalent* to (W, E', V'). The automorphism groups of two equivalent codes are conjugate to each other as subgroups in S_m. Also, equivalent codes have the same weight distribution. In this thesis, we will mostly consider binary self-dual codes up to equivalence relation.

Consider an invertible linear transformation A on the vector space 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 the non-degenerate bilinear form $\langle , \rangle$. Under a basis E, A is represented by a matrix in $GL_{m\times m}(\mathbb{F}_2)$.

Fixing E, a *generator matrix* is a matrix whose row vectors span V for a code. Thus a generator matrix 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 with respect to the Euclidean inner product under the basis $\{e_i\}_{i=n+1}^{2n}$. Let $O(2n)$ act on W by left multiplication. By the embedding $O(n) \hookrightarrow O(2n)$ 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 on E rather than an arbitrary orthogonal change of basis: had we chosen the latter, the definition of equivalence relation would not be interesting.

Remark 2.2.1. A useful fact is that for the Euclidean inner product, $O(n)$ coincides with S_n if and only if $n \leq 3$. Indeed, when $n \leq 3$ this fact is obvious. An example for an element in $O(4) \smallsetminus S_4$ can be obtained from the length 8 binary self-dual code A_8, which has a generator matrix (I_4, P) where P is:

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

$\diamondsuit$

Denote by T_{2n} the set of all distinct (up to isomorphism) binary self-dual codes of length $2n$. There is a simple counting formula [RS98]

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

Here we used $|\cdot|$ to denote the cardinality of a finite set.

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

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

Let S_{2n} acts on a binary self-dual code C, its orbit has all the codes equivalent to it, which breaks into several isomorphism types. Denote the set of distinct codes in this orbit 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}.

One can also 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 constant smaller than $\frac{1}{2}$, by Stirling's formula $\frac{T_n}{(2n)!}$ 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 a given length is computationally costly. For the interested reader, there are now on-line databases of equivalence classes of binary self-dual codes. For example, M. Harada and A. Munemasa summarized on their website a complete list of binary self-dual codes of length up to 40 [HM07].

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

Proposition 2.2.2 (Rigidity)**.**

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

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

Remark 2.2.3. Some caution is required in interpreting this statement. Based on Proposition 2.2.2 alone, it does not qualify to say that "most equivalence classes" have a trivial automorphism group, since codes with bigger automorphism groups could conceivably break into more equivalence classes. ♢

2.3 Extremal Codes

Coding theory has many interesting connections with other branches of mathematics, including combinatorial design, lattice theory and invariant theory [CS99, Chapter 3][PH98][Ple98]. Codes are also widely used for *error-correction* purposes in telecommunication. Some of the best error-correction codes are binary self-dual codes. For error-correction purposes, the most relevant property is the weight distribution of the code. In particular, the non-zero minimal weight is important, which is an even integer. For a code C of length $2n$, denote its nonzero minimal weight by d_{2n}. There are two interesting questions:

Question 2.3.1. Fixing the length $2n$, what is the largest d_{2n}?

Fixing length $2n$, we will call a code with the largest minimal weight an *extremal code.* In general, when $56 \leq 2n \leq 110$, not all the extremal codes are known [DGH97] (for some lengths, even the d_{2n} are conjectural). Other than the extremal codes, the existence of codes with other prescribed weight enumerators are also conjectured. Therefore, interesting construction methods for binary self-dual codes are sought for in the literature. Existing techniques include some brilliant combinatorial designs which give some special codes; "gluing" constructions using codes of smaller length; a systematic study of "descendants" of codes of smaller length. A systematic survey of all these construction methods is outside the scope of this thesis, the reader is referred to the references listed above and also [BHM12] [BB12]. We point out that based on our Construction $\mathbb{Q}$, we propose a "probabilistic" method of generating binary self-dual codes, which is a non-recursive way to generate a comprehensive list of codes, see section 3.4.

Question 2.3.2. What is $\limsup_{m\to\infty} \frac{d_m}{m}$?

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

Proposition 2.3.3. *[RS98, section 10] There is an infinite sequence of binary self-*

dual codes C_i where the ratio $\frac{d_i}{m_i}$ is bounded below by an absolute constant.

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 a code up to equivalence, called a boxed matrix, see Table 3.1. This construction can be considered as an arithmetic counterpart of Theorem A.0.11 in [KP08].

Notation: we will use p_i for a positive prime number or a prime ideal in $\mathbb{Z}$ when there is no danger of confusion. v_{p_i} is the normalized p-adic valuation of $\mathbb{Q}$ associated to p_i. An equivalence class of valuations on a field is also 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 [Mil13, Chapter 5]

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

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, [Ser73, Chapter III]:

- $(a, b) = 1$ 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.

The Hilbert symbol satisfies the following properties:

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

- $(a,-a) = 1$, $(a, 1-a) = 1$.

- $(aa', b) = (a,b)(a',b)$.

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 $k(\sqrt{b})/k$. It is easy to see that the Hilbert symbol is a map

$$k^*/(k^*)^2 \times k^*/(k^*)^2 \to \pm 1$$

Remark 3.2.1. For notation convenience we will write $k^*/2$ for $k^*/(k^*)^2$. If the multiplicative groups $k^*/2$ and $\{\pm 1\}$ are interpreted additively, the Hilbert symbol is a symmetric bilinear form over $\mathbb{F}_2$. Furthermore, it is a non-degenerate bilinear form, i.e. if $a \in k^*$ is a norm in every quadratic extension of k, then $a \in (k^*)^2$. This follows easily from class field theory (or more directly from Kummer theory). $\diamondsuit$

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. In this case, $K_{\mathfrak{p}}^*/2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, which is spanned by a uniformizer in the valuation $\mathfrak{p}$ and a non-square unit u. 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

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

Such a matrix is called *alternate* in [Alb38]. (Over a field of characteristic different from 2, a quadratic form associated to a non-degenerate symmetric bilinear form with an alternate Gram matrix is usually called hyperbolic. Over a field of characteristic 2, the correspondence between bilinear forms and quadratic forms is more complicated.) Over a field of characteristic 2, if $\forall x \in W\ \langle x, x\rangle = 0$, we will follow Albert and call such a bilinear form *alternate.* [Alb38] classified non-degenerate symmetric bilinear forms over a field of characteristic 2:

Theorem 3.2.2 (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 dimension vector space is Euclidean under a suitable basis. For example, $\mathbb{Q}_2^*/2 \cong \mathbb{F}_2^3$ has odd dimension. If we choose the basis $\{-2, -10, -5\}$ (considered as rational numbers embedded in $\mathbb{Q}_2$) 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 3.2.2, when $k^*/2$ 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 3.2.3. *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 may also consider 2 as p_{n-1}, ∞ as p_n ($\mathbb{Q}_{p_n} = \mathbb{R}$), thus we always have $n \geq 2$. 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 $\mathbb{Q}_p^*/2$ 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 $\langle , \rangle : \ W \times W \to \mathbb{F}_2$,

$$\langle , \rangle = \sum_{v_p \in S} \langle , \rangle_{v_p} \tag{3.3.1}$$

A Euclidean basis E of W is provided by the union of the bases for each W_p, namely when p is odd, W_p has a basis $\{pu, p\}$; W_2 has basis $\{-2, -10, -5\}$; $W_{\mathbb{R}}$ has basis $\{-1\}$. Their union basis E will be used throughout the construction.

Consider the diagonal embedding Φ: $\mathbb{Z}_S^*/2 \to \oplus_{v_{p_i} \in S} \mathbb{Q}_{p_i}^*/2 =: W$. 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) $(W, E, \Phi(\mathbb{Z}_S^*))$ is a binary self-dual code.

(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 4.1.3 which works in 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 $\mathbb{Q}_2^*/2$ is a three dimensional vector space over $\mathbb{F}_2$, the order of the basis $\{-2, -10, -5\}$ matters. The entries for a given row in the matrix are the diagonal images from a global S-unit, which are listed to the left of the matrix.

Table 3.1: A boxed code

places	W_{p_1}	W_{p_2}	$\cdots$	W_2		$W_{\mathbb{R}}$
S-units	$\{-p_1, p_1\}$	$\{-p_2, p_2\}$	$\cdots$	$\{-2, -10, -5\}$		$\{-1\}$
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

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.

(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,

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.*

Proof. Taking the product of the i-th row and the j-th row in a half-boxed matrix $(i, j < n, i \neq j)$, the products of identical pairs are 0 in $\mathbb{F}_2$. Thus if the two rows are orthogonal, we have $b_{ij} \cdot (01) + b_{ji} \cdot (01) + (10) \cdot (10) = 0$, thus $b_{ij} + b_{ji} = (11)$.

□

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:

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

01	u
w	M'

In the above table w is a column block-vector of length $n-1$, u is a row block-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 $S = \{2, \infty, p_1, \dots, p_{n-2}\}$. To specify the odd p_i we begin by requiring their classes in $\mathbb{Q}_2^*/2 \times \mathbb{R}^*/2$ 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}. △

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 bottle-necks, 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), and theoretically every binary self-dual codes of length $2n$.

As toy examples, we 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.

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 large 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, 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 some codes of small length from [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%	$\cdots$

In 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

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%	$\cdots$	

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 $2n$?

In 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 for a head, and denote the probability for a code C in the algorithm 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 $\tilde{p}_{\theta,C}$ 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. The construction in this chapter uses duality theorems in étale cohomology over some arithmetic schemes. It is named *Construction G* where G stands for the word geometry.

In section 4.1, we will restate the Hilbert symbol pairing in Construction $\mathbb{Q}$ for a general global field in the cohomological language, and give it a new proof in Proposition 4.1.3 using Artin-Verdier duality. Compared with section 4.2, this is the "relative dimension zero" case. Towards the end of this section, an interesting question is asked in Question 4.1.6, relating the statistical behavior of codes in the construction to the quadratic residues of S-units in the field. In Example 4.1.7, by choosing fibers over different primes in a curve over $\mathbb{Z}$, Construction G is related to the random generation algorithm in Section 3.4.

In section 4.2, an arithmetic duality theorem will be reviewed over an arithmetic scheme of positive relative dimension over the ring of integers of a totally imaginary number field. In our construction for a triple (W, E, V) of a binary self-dual code, W will be the middle dimension cohomology space of an arithmetic scheme; V will be a half-dimensional subspace inside W which is self-orthogonal with respect to a non-degenerate bilinear pairing coming from the Yoneda-pairing on the cohomology space. In general, whether the Yoneda-pairing on W is a Euclidean pairing is an interesting question, which we discuss in Example 4.2.5 and also come back to in Example 5.6.5.

4.1 Arithmetic Duality of Global Fields

For a scheme X, we will denote the category of sheaves of abelian groups on the small étale site X_{et} by $Sh(X)$. When $R \in Sh(X)$ is also a sheaf of rings, the sheaf of R-modules is denoted $Sh(X, R)$. We will mostly be interested in the case when R is the constant sheaf $\mathbb{Z}/2$. When K is a field, it is well known that there is a canonical equivalence of categories between $Sh(\operatorname{Spec} K)$ and the category of discrete $Gal(K)$ modules with a continuous Galois action [Sha72, Proposition 71]. Under this equivalence, étale cohomology groups $H^*_{et}(\operatorname{Spec} K, \mathcal{F})$ correspond to the Galois cohomology groups $H^*(K, Mod(\mathcal{F}))$, where $Mod(\mathcal{F})$ is the $Gal(K)$ module associated to $\mathcal{F}$. In this thesis we will abuse these two notations and simple put $H^*(K, \mathcal{F})$. In general, all $H^*(X, \mathcal{F})$ stands for $H^*_{et}(X, \mathcal{F})$ unless otherwise stated.

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. When v is real $K_v = \mathbb{R}$, we will consider the Tate (modified) cohomology groups $\widehat{H}^*(\mathbb{Z}/2, Mod(\mathcal{F}))$ [Ser62]. When v is complex this cohomology space is 0. When v is a finite place, there is the local Tate duality:

Theorem 4.1.1 (Tate)**.** *Suppose K_v is a non-archimedean local field of characteristic different from 2. Given a locally constant constructible sheaf $\mathcal{F} \in Sh(K_v, \mathbb{Z}/2)$, define its dual sheaf by $\mathcal{F}^D := \mathcal{H}om(\mathcal{F}, \mu_2)$.*

$$H^i(K_v, \mathcal{F}) \times H^{2-i}(K_v, \mathcal{F}^D) \to H^2(K_v, \mu_2) = \mathbb{Z}/2 \tag{4.1.1}$$

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

We refer to [Mil06, Chapter II] for the definition of a constructible sheaf. When K is a number field, let $\mathcal{O}_K$ be the ring of integers of K and let $X = \operatorname{Spec}(\mathcal{O}_K)$. When K is a global function field, let X be a smooth projective curve with function field K. $U \subset X$ is an open subscheme. $S = S_\infty \sqcup S_f$ is a set of places of K, where S_f consists of the places determined by the primes in the complement of U, S_∞ contains all of the infinite places of K. For $\mathcal{F} \in Sh(X)$, denote $H^*_c(U, \mathcal{F}|_U)$ the cohomology groups with compact support, where we follow the convention in [Mil06, section II.2] and cite the following long exact sequence:

$$\cdots H^r_c(U, \mathcal{F}|_U) \to H^r(U, \mathcal{F}|_U) \to \sum_{v \in S} H^r(K_v, \mathcal{F}_{K_v}) \to H^{r+1}_c(U, \mathcal{F}|_U) \cdots \tag{4.1.2}$$

There is a global counterpart of the local Tate duality, called the Artin-Verdier duality [Mil06, section II.3]. When S_f contains all places with residue characteristic 2, 2 is invertible on U. Under this condition, Artin-Verdier duality for $Sh(U, \mathbb{Z}/2)$ says:

Theorem 4.1.2 (Artin-Verdier)**.** *For a locally constant constructible sheaf $\mathcal{F} \in Sh(U, \mathbb{Z}/2)$,*

$$H^r_{et}(U, \mathcal{F}) \times H^{3-r}_c(U, \mathcal{F}^D) \to H^3_c(U, \mu_2) \cong \mathbb{Z}/2 \tag{4.1.3}$$

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

The local Tate duality and Artin-Verdier duality are analogous to the Poincaré duality on a topological manifold. When 2 is invertible on U, all the Tate twist $\mu_2^{\otimes i}$ for $i \geq 0$ and their duals can be canonically identified with μ_2. We have our first proposition in Construction G:

Proposition 4.1.3. *The image of the restriction homomorphism*

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

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

$$\begin{aligned}\big(\oplus_{v \in S} H^1_{et}(K_v, \mu_2)\big) \times \big(\oplus_{v \in S} H^1_{et}(K_v, \mu_2)\big) &\to \oplus_{v \in S} H^2_{et}(K_v, \mu_2) \\ &\xrightarrow{\delta_2} H^3_c(U, \mu_2) \cong \mathbb{F}_2 \end{aligned} \tag{4.1.4}$$

which is the Yoneda-pairing composed with the boundary map in Equation 4.1.2. In 4.1.4, δ_2 amounts to taking summations.

Proof. For a finite place v, by the local Tate duality 4.1.1

$$H^1(K_v, \mu_2) \times H^1(K_v, \mu_2) \to H^2(K_v, \mu_2) \tag{4.1.5}$$

is a non-degenerate bilinear pairing. For a real v, this is also true. The fact that δ_2 in Equation 4.1.4 amounts to taking summations is proved in [Mil06, II.2]. It is straightforward to see that the direct sum of the non-degenerate bilinear product structures on each space $H^1(K_v, \mu_2)$ gives a non-degenerate bilinear product structure on $\oplus_{v\in S} H^1(K_v, \mu_2)$, as in Equation 3.3.1.

Now we prove that the image of

$$\Phi\colon H^1(U, \mu_2) \to \oplus_{v\in S} H^1(K_v, \mu_2)$$

is its own orthogonal complement with respect to the product in 4.1.4. This is a pretty standard exercise in linear algebra. For ease of notation, denote $A = H^1(U, \mu_2)$, $B = \oplus_{v\in S} H^1(K_v, \mu_2)$ and $C = H^2_c(U, \mu_2)$. The pairing in Equation 4.1.4 identifies the linear dual $\check{B} = \mathrm{Hom}_{\mathbb{F}_2}(B, \mathbb{F}_2)$ with B. The perfect pairing $A \times C \to \mathbb{F}_2$ in 4.1.2 identifies $\check{A}$ with C. From 4.1.2 for $r = 1$ we have an exact sequence

$$A \xrightarrow{\Phi} B \xrightarrow{\Psi} C \tag{4.1.6}$$

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 4.1.6. Thus $\dim(\mathrm{image}(\Phi)) = \frac{1}{2}\dim(B)$. So if we can show $\mathrm{image}(\Phi) \subseteq \mathrm{image}(\Phi)^{\perp}$, the inclusion is actually an equality since the product 4.1.4 on B is non-degenerate. We have the commutative diagram:

$$\begin{tikzcd}
A \times A \arrow[r, "\cup"] \arrow[d, "\Phi\times\Phi"] & H^2(U,\mu_2) \arrow[d] \\
B \times B \arrow[r, "\cup"] & \oplus_{v\in S} H^2(K_v,\mu_2)
\end{tikzcd} \tag{4.1.7}$$

Since the composition of the maps

$$H^2(U,\mu_2) \to \oplus_{v\in S} H^2(K_v,\mu_2) \xrightarrow{\delta_2} H^3_c(U,\mu_2)$$

is 0 by the exactness of the sequence, we have proved image(Φ) $\subseteq$ image$(\Phi)^{\perp}$. □

Remark 4.1.4. For a triple (W,V,E) to be a binary self-dual code, we need that the non-degenerate bilinear product on W is Euclidean, where E is a Euclidean basis. Apply Galois cohomology to the Kummer sequence

$$0 \to \mu_2 \to \mathbb{G}_m \xrightarrow{\times 2} \mathbb{G}_m \to 0 \tag{4.1.8}$$

By Hilbert's Satz 90 $H^1(K,\mathbb{G}_m)=0$, therefore it is shown $H^1(K_v,\mu_2)=K_v^*/2$. The pairing 4.1.5 is just the Hilbert symbol pairing [Ser62, Chapter XIV]. By Corollary 3.2.3 $W_v := H^1(K_v,\mu_2)$ is Euclidean if and only $-1 \notin (K_v^*)^2$. For a finite extension $K_v/\mathbb{Q}_2$, $dim_{\mathbb{F}_2} K_v^*/2 = 2 + [K_v : \mathbb{Q}_2]$ by the structure theorem of local fields [Neu99, Proposition 5.7, Chap II]. Combined with Corollary 3.2.3 and the discussion in Section 3.2, when W_v is Euclidean, it shows E_v is unique up to permutations if and only if the residue characteristic of v is different from 2 or $K_v = \mathbb{Q}_2$. After choosing a basis E_v for each W_v, we always take $E = \sqcup_{v\in S} E_v$.

By Albert's Theorem 3.2.2, when some subspaces W_v are alternate and some other (nonempty) subspaces $W_{v'}$ are Euclidean, the total space W is still Euclidean.

However, there will be no natural way to choose a Euclidean basis E in W up to permutations unless $dim_{\mathbb{F}_2}W \leq 3$. By Section 2.2, the combinatorial properties of a binary self-dual code depends on the choice of E up to permutations. Thus unless there is a natural way to pick a basis E, a binary self-dual code (W, V, E) is not well-defined. ♢

Example 4.1.5. Suppose K is a number field and $X = \text{Spec}(\mathcal{O}_K)$. Taking cohomology of the Kummer sequence 4.1.8, it produces

$$0 \to \mathcal{O}_{K,S}^*/2 \to H^1(U, \mu_2) \to Pic(U)[2] \to 0$$

where $Pic(U)[2]$ denotes the two torsion elements in the abelian group $Pic(U)$. When $Pic(U)$ is odd, $\mathcal{O}_{K,S}^*/2 = H^1(U, \mu_2)$. The image of Φ in Proposition 4.1.3 is the diagonal image $\mathcal{O}_{K,S}^*/2 \to \oplus_{v \in S} K_v^*/2$ as in Construction $\mathbb{Q}$. We will show that Φ is injective under our assumption that S contains all the infinite places and finite places $v|2$.

By 3.1.1 $h^1(U, \mu_2) = dim_{\mathbb{F}_2}\mathcal{O}_{K,S}^*/2 = |S|$.

When $v|2$, $h^1(K_v, \mu_2) = 2 + [K_v : \mathbb{Q}_2]$. When $v \nmid 2 \in S_f$, $h^1(K_v, \mu_2) = 2$. When v is real, $h^1(K_v, \mu_2) = 1$. When v is complex it is trivial. Therefore

$$\sum_{v \in S} h^1(K_v, \mu_2) = \sum_{v|2}(2 + [K_v : \mathbb{Q}_2]) + (\sum_{v \nmid 2, v \in S_f} 2) + r_1 = 2r_2 + r_1 + 2|S_f| + r_1 = 2|S| \tag{4.1.9}$$

where r_1 is the number of real places, r_2 the number of complex places. By Proposition 4.1.3, $\frac{1}{2}dim_{\mathbb{F}_2}W = dim_{\mathbb{F}_2}\text{image}(\Phi) = h^1(U, \mu_2)$, thus Φ is injective.

When $Pic(U)[2] \neq 0$ the two-torsion elements in the Picard group are also involved in the construction. However this is related to the odd Picard number case. Suppose $U' \subset U$ is a smaller open subscheme, the map Φ factors through

$$H^1(U, \mathbb{Z}/2) \to H^1(U', \mathbb{Z}/2) \to \oplus_{v \in S} H^1(K_v, \mu_2)$$

whence we can take a small enough U' such that such that $Pic(U')$ is odd.

In general, the diagonal image $\Phi : \mathcal{O}^*_{K,S} \to \oplus_{v \in S} K_v^*/2$ has more complicated patterns than a boxed-matrix as in table 3.1. From the above discussion, if for all $v|2$ $K_v = \mathbb{Q}_2$, a binary self-dual code (W, V, E) is well defined. However, when $[K : \mathbb{Q}] > 0$ it is usually hard to give a combinatorial description of image(Φ), besides the fact that it is a binary self-dual code. This is related to the problem of giving an elementary description of a "quadratic reciprocity law" for $v|2$ in K, see [Lem00] for an overview. Characterizing the image of Φ also concerns the behavior of quadratic residues of the S-units in K. It would be interesting to see how a viewpoint from the binary self-dual code structure can help us probe these problems. For example, one can ask the following question:

Question 4.1.6. Consider the set of number fields K where 2 splits completely. Fix the number of embeddings r_1, r_2 of K and let the discriminant $disc(K)$ grow by magnitude. If S_f contains only $v|2$, the length of the code is fixed to be $4r_1 + 6r_2$ by Equation 4.1.9. What is the frequency that a certain equivalence of codes of this length is generated? How is this frequency related to the density $\tilde{p}_\theta$ in section 3.4?

We leave this question for further research. $\triangle$

Example 4.1.7 (Local-Global Codes). Consider the global function field $\mathbb{F}_q(T)$, where $q = p^n \equiv 3 \bmod 4$, T is a transcendental parameter. $X = \mathbb{P}^1_{\mathbb{F}_q}$. Let $S = \{\frac{1}{T}, g_1(T), \cdots, g_{n-1}(T)\}$ where each $g_i(T)$ is a monic irreducible polynomial in $\mathbb{F}_q[T]$. The image of Φ is given by the global S-units $\langle -1, g_1(T), \cdots, g_{n-1}(T)\rangle$ in $W = \oplus_{v \in S} K_v^*/(K_v^*)^2$. Suppose each $g_i(T)$ has odd degree, then the Hilbert symbol pairing $W \times W \to \mathbb{F}_2$ has a natural choice of Euclidean basis. It is not hard to see that the diagonal image of Φ is also described by a boxed-matrix in table 3.1.

When $\mathbb{F}_q = \mathbb{F}_p$ is a prime field, X can be considered to be the fiber over $\operatorname{Spec}\mathbb{F}_p$ in $\mathbb{P}^1_{\mathbb{Z}}$. Consider some horizontal divisors defined by linear integral polynomials $g_i(T) = T - a_i$ on $\mathbb{P}^1_{\mathbb{Z}}$, where $a_i \in \mathbb{Z}$. The pull-back of these horizontal divisors on X are rational points defined by $g_i(T)$ mod p. When $|p| > max_{1 \le i \le n-1} 2|a_i|$, $g_i(T)$ mod p will give distinct rational points on X. In the boxed-matrix description of the resulting code, the pair b_{ij} is determined by the Legendre symbol $(\frac{a_i - a_j}{p})$. By Gauss's quadratic reciprocity, the Legendre symbol is also determined by the congruence conditions of p mod the prime factors in $(a_i - a_j)$. For simplicity, assume for all sets of indices $\{i, j\}$, there is an odd prime number f_{ij} and n, such that $f_{ij}^n | (a_i - a_j)$, $f_{ij}^{n+1} \nmid (a_i - a_j)$, and $f_{ij} \nmid (a_{i'} - a_{j'})$ when $\{i, j\} \neq \{i', j'\}$. Now let the prime number p grow by magnitude in the congruence class of 3 mod 4. By the equidistribution of the prime number p in the congruence classes mod the f_{ij}'s, the Legendre symbol $(\frac{a_i - a_j}{p})$ is 1 or -1 exactly half of the time. Therefore, when we take X to be the fiber over different prime $p \equiv 3 \bmod 4$ in $\mathbb{P}^1_{\mathbb{Z}}$, the pull-back divisors S generate binary self-dual codes like the random algorithm in section 3.4 using a fair coin! $\triangle$

4.2 Duality of Arithmetic Schemes

In this section, we will continue the construction from the previous section and generalize Proposition 4.1.3 to certain arithmetic schemes of positive relative dimension over X, where X, K, S and U have the same meaning from the previous section. Recall that K is a global field of characteristic different from 2 and 2 is invertible on U. Let $\pi : Y \to X$ be an integral, projective scheme over X of relative dimension $d > 0$. Suppose Y is smooth over an open subscheme $U \subseteq X$ and its generic fiber Y_K is geometrically irreducible. First we recall the following generalization of the local Tate duality [Sai89]:

Proposition 4.2.1. *K_v is a non-archimedean local field of characteristic different from 2. Given a locally constant constructible sheaf $\mathcal{F} \in Sh(Y_{K_v}, \mathbb{Z}/2)$,*

$$H^i(Y_{K_v}, \mathcal{F}) \times H^{2d+2-i}(Y_{K_v}, \mathcal{F}^D) \to H^{2d+2}(Y_{K_v}, \mu_2) = \mathbb{Z}/2 \tag{4.2.1}$$

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

When v is a complex place, the Tate cohomology groups $\widehat{H}^i(\mathbb{C}, M) = 0$ for any module M and $i \in \mathbb{Z}$. Therefore for a complex variety $\pi : Z \to \mathbb{C}$ and $\mathcal{F} \in Sh(Z)$, $\widehat{H}^i(Z, \mathcal{F}) = \widehat{H}^i(\mathbb{C}, R\pi_*\mathcal{F}) = 0$. Proposition 4.2.1 is trivially satisfied.

There is a generalization of Artin-Verdier duality [Mil06]:

Proposition 4.2.2. *Given a locally constant constructible sheaf $\mathcal{F} \in Sh(Y, \mathbb{Z}/2)$,*

$$H^r_{et}(Y_U, \mathcal{F}) \times H_c^{3+2d-r}(Y_U, \mathcal{F}^\vee) \to H_c^{3+2d}(Y_U, \mu_2) \cong \mathbb{Z}/2 \tag{4.2.2}$$

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

Using Proposition 4.2.1 and 4.2.2, the following is a corollary of Proposition 4.1.3:

Corollary 4.2.3. *When K is a totally imaginary number field or a global function field of characteristic different from 2, 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

$$\begin{aligned}\left(\oplus_{v\in S} H^{d+1}_{et}(Y_{K_v}, \mu_2)\right) \times \left(\oplus_{v\in S} H^{d+1}_{et}(Y_{K_v}, \mu_2)\right) \to \oplus_{v\in S} H^{2d+2}_{et}(Y_{K_v}, \mu_2)\\ \xrightarrow{\delta_{2d+3}} H_c^{3+2d}(Y_U, \mu_2) \cong \mathbb{F}_2\end{aligned} \tag{4.2.3}$$

which is the Yoneda-pairing composed with taking summations.

Remark 4.2.4. The reason we do not consider the case when K has a real embedding is that although Proposition 4.2.2 remains valid, Proposition 4.2.1 is in general not true for a real local field, see [Cox79]. ♢

When $d = 1$, V is the diagonal image $\Phi : H^2(Y_U, \mu_2) \to \sum_{v\in S} H^2(Y_{K_v}, \mu_2)$. By the Kummer sequence, $H^2(Y, \mu_2)$ can be computed by

$$0 \to Pic(Y)/2 \to H^2(Y, \mu_2) \to Br(Y)[2] \to 0$$

where $Br(Y) := H^2(Y, \mathbb{G}_m)$ is the cohomological Brauer group. An explicit description of the map Φ would be very interesting, which we leave for further study.

In general, it is not an easy problem to determine if the Yoneda-pairing

$$\langle , \rangle : H^{d+1}(Y_{K_v}, \mu_2) \times H^{d+1}(Y_{K_v}, \mu_2) \to H^{2d+1}(Y_{K_v}, \mu_2) \tag{4.2.4}$$

used in Corollary 4.2.3 is Euclidean or alternate, as is illustrated in the following example.

Example 4.2.5. Consider the case $Y_{K_v} = P^1_{K_v}$. The Hochschild-Serre spectral sequence is often used to calculate $H^*(P^1_{K_v}, \mu_2)$:

$$H^i(K_v, H^j(P^1_{\overline{K_v}}, \mu_2)) \Rightarrow H^{i+j}(P^1_{K_v}, \mu_2) \tag{4.2.5}$$

where $\overline{K_v}$ denotes an algebraic closure of K_v. This spectral sequence is multiplicative, in the sense that there is a pairing on the E_2 page:

$$E_2^{p_1,q_1} \cup E_2^{p_2,q_2} \to E_2^{p_1+p_2,q_1+q_2}$$

which when passing to E_∞ is compatible with the cup product structure on $H^*(P^1_{K_v}, \mu_2)$. It is easy to see that the spectral sequence 4.2.5 degenerates on the E_2 page. Denote $E_2^{2,0} = \{0, y\} \hookrightarrow H^2(P^1_{K_v}, \mu_2) = \{0, x, y, x + y\} =: W_v$. $E_2^{0,2}$ can be naturally identified with the quotient $\{0, \bar{x}\}$ of W_v modulo the subspace $\{0, y\}$.

Since the pairing $\langle , \rangle$ on W_v is non-degenerate, the fact that $y \cup y \in E_2^{4,0} = 0$ implies $\langle x, y \rangle = 1$ is non-trivial. Thus on the quotient space $E_2^{0,2}$,

$$\langle \bar{x}, \bar{x} \rangle = 0 = \langle x, x \rangle \text{ mod } \langle x, y \rangle$$

The multiplicative structure on E_2 of 4.2.5 alone does not suffice to determine if 4.2.4 is Euclidean or alternate. In Example 5.6.5, we will prove the following theorem using techniques from an equivariant étale cohomology theory.

Theorem 4.2.6. *The cup product pairing 4.2.4 is alternate when $Y_{K_v} = P^1_{K_v}$ or E_{K_v}, where E_{K_v} is an elliptic curve with good reduction over a local field K_v with residue characteristic different from* 2.

$\triangle$

Chapter 5

The Equivariant Construction

Ever since the 1950s, equivariant cohomology has been a powerful tool in the study of group actions on spaces. Borel defined an equivariant cohomology for the action of a compact group G on a topological space [Bor60]. In [Gro57], Grothendieck defined an equivariant sheaf cohomology for the action of a discrete group. For a finite group, the Borel construction can be generalized to actions on sheaves and it coincides with Grothendieck's equivariant sheaf cohomology [Sti79]. In this chapter, we will transplant certain statements for a finite group action on a finite CW complex to an action on equivariant étale sheaves over a scheme. For an application to the construction of binary self-dual codes, we will mainly be concerned with the case $G = \mathbb{Z}/2$.

In Section 5.1, we will follow [AP93, Chapter I] and review the set-up of a construction for Grothendieck's equivariant cohomology. When $G = \mathbb{Z}/2$, we will use a minimal Hirsch-Brown model for an equivariant G-complex. In section 5.2, we will specialize to consider equivariant étale sheaves over a scheme, and recall Morin's construction of a modified equivariant étale cohomology. In section 5.3, we prove a "Smith-type inequality" 5.3.1 using Theorem 5.3.3 from [Mor08]. We will call it the *maximal case* when 5.3.1 is an equality. In the maximal case for a $\mathbb{Z}/2$ action on a scheme Y where 2 is invertible, cohomological duality statements on Y can be utilized to construct binary self-orthogonal spaces, following [Pup01]. In section 5.5 we compare the Equivariant Construction and Construction G in the previous chapter. In Example 5.5.4, the reader will find that while the two constructions give the same underlying vector spaces for a code, their product structures are not necessarily the same. In the final section 5.6, we provide some more discussions on the maximum condition 5.3.8. In particular, in Example 5.6.5 the maximum condition is met, and the deformation trick can be used to prove Theorem 4.2.6.

5.1 Cohomology of a G-Complex

Let G be a finite group and k be a field. C^* is a bounded below cochain complex of $k[G]$-modules, we will call C^* a $\delta gk[G]$-Mod, where $\delta : C^i \to C^{i+1}$ is the G-equivariant differential. Similarly, we will call a bounded above chain complex of $k[G]$-modules a $\partial gk[G]$-Mod. Recall the following construction of the hyper-derived functor $\mathbb{E}xt^*_{k[G]}(k, C^*)$ [Ben98, 2.7]: take a free resolution $\mathcal{E}_*$ of the trivial G-module

k,

$$\cdots \mathcal{E}_i \to \mathcal{E}_{i-1} \cdots \to \mathcal{E}_1 \to \mathcal{E}_0 \to k \to 0$$

Define $\beta^n_G(C^*) := \Pi_{i+j=n} Hom_{k[G]}(\mathcal{E}_i, C^j)$. Equivalently, define the dual complex $\mathcal{E}^*$ as $\mathcal{E}^i := Hom_{k[G]}(\mathcal{E}_i, k[G])$, since C^* is bounded from below, $\beta^n_G(C^*) \cong \oplus_{i+j=n} C^j \otimes_{k[G]} \mathcal{E}^i$. Then $\mathbb{E}xt^n_{k[G]}(k, C^*) := H^n(\beta^*_G(C^*))$. We will follow [AP93] and call this group $H^*_G(C^*)$. Recall [Ben98, 3.2], the cup product

$$H^i_G(C^*) \otimes H^j_G(S^*) \to H^{i+1}_G(C^* \otimes S^*)$$

is associative and graded-commutative. When there is an associative, graded-commutative $\delta gk[G]$-Mod morphism $C^* \otimes C^* \to C^*$, $H^*_G(C^*)$ is a graded-commutative algebra over $H^*_G(k)$. For our purpose, we will only consider the case when $G = \mathbb{Z}/2$ and k is a field of characteristic 2. Thus it is not necessary to distinguish between left and right G-actions and the ± sign doesn't matter. Following [AP93, Chapter I], we will pick a particular (minimal) resolution $\mathcal{E}^*$ such that for any $\delta gk[G]$-Mod C^*, $\beta^*_G(C^*)$ is already a right graded $\beta^*_G(k)$-module on the cochain level.

Denote $G = \mathbb{Z}/2 = \{1, g\}$. Take $\mathcal{E}^* = k[G] \otimes W^*$, where each graded piece W^n is freely generated by $\{w^n\}$ as a k-module. The G-equivariant differential δ is defined by $\delta w^n := (1-g)w^{n+1}$. Under this $\mathcal{E}^*$, $\beta^n_G(k)$ is generated as a k-module by $w^n \otimes_{k[G]} 1 \in \mathcal{E}^n \otimes k$. The differential on $\beta^n_G(k)$ is trivial, and $\beta^*_G(k) \cong H^*(G, k)$ as δgk-Mod. $\beta^*_G(k)$ obtains a commutative ring structure from $H^*_G(k)$, which is isomorphic to $k[t]$, $deg(t) = 1$.

Consider the δgk-Mod $\beta^*_G(C^*) = C^* \otimes_{k[G]} \mathcal{E}^*$. Since tensor product is commutative for graded k-modules,

$$C^* \otimes_{k[G]} \mathcal{E}^* \cong C^* \otimes_{k[G]} (k[G] \otimes W^*) \cong (C^* \otimes_{k[G]} k[G]) \otimes_k W^* \cong C^* \otimes_k W^*$$

Under this isomorphism, $C^* \otimes W^*$ obtains a differential $\widetilde{\delta}$ from $\beta^*_G(C^*)$.

Lemma 5.1.1. *[AP93, Proposition 1.3.4] The cochain complex $\beta^*_G(C^*)$ is a free graded right $k[t]$-module isomorphic to $C^* \otimes k[t]$, and the differential $\widetilde{\delta}$ on $C^* \otimes k[t]$ is right $k[t]$-linear.*

Remark 5.1.2. Multiplication of $k[t]$ on the left of $C^* \otimes k[t]$ is associative only up to cochain homotopy, loc. cit. ♢

We will call a graded $k[t]$-module with a $k[t]$-linear differential a $\delta gk[t]$-Mod. Explicitly, the differential $\widetilde{\delta}$ on $C^* \otimes k[t]$ is given by

$$\widetilde{\delta}(c \otimes 1) = \delta(c) \otimes 1 + c(1-g) \otimes t \tag{5.1.1}$$

In particular, $\widetilde{\delta}$ is not the usual differential of the tensor product of two δgk-Mod C^* and $k[t]$, a phenomenon which was already observed in [Bro59]. In general, given a δgk-Mod (C, δ), a $\delta gk[t]$-Mod $(C \otimes k[t], \widetilde{\delta})$ is called a *deformation* of (C, δ) if

$$\widetilde{\delta}(c \otimes 1) = \sum_i b_i \otimes t^i$$

where $b_0 = \delta(c)$. We denote $(C \otimes k[t], \widetilde{\delta})$ by $C^* \widetilde{\otimes} k[t]$ to emphasis the deformation.

Since k is a field, all exact sequences of k-modules split (non-canonically), by [AP93, B.1.8], a δgk-Mod is homotopic to the trivial complex if it has trivial cohomology group. Therefore a δgk-Mod C^* is homotopic to $H^*(C^*)$ with trivial differential. By [AP93, B.2.4], $C^*\widetilde{\otimes}k[t]$ is homotopic to $H^*(C^*)\widetilde{\otimes}k[t]$, which is called the *minimal Hirsch-Brown model* for $\beta_G^*(C^*)$.

For applications in the next section, we also consider the *localization* at t of a $\delta gk[t]$-Mod M^*. As usual, given a graded $k[t]$-module $M^* = \oplus_{n\in\mathbb{Z}}M^n$, the degree n piece of its localization at the homogeneous ideal (t) is given by $\oplus_{j\in\mathbb{Z}}M^{n-j}\otimes t^j$. We extend the differential $k[t,\frac{1}{t}]$-linearly, and denote this localization by $M^*\otimes_{k[t]}k[t,\frac{1}{t}]$.

5.2 Equivariant Etale Sheaves

In this section we will recall some facts about the category of equivariant étale sheaves on the étale site of a locally noetherian scheme X_{et}, denoted $Sh(X,G)$. In this section, G is a finite group acting on X, and $\mathcal{F}$ is a sheaf on X_{et}.

Definition 5.2.1. 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

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

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

$Sh(X, G)$ is an abelian category with enough injectives. When $\mathcal{F}$ is an injective object in $Sh(X, G)$, it is also injective in $Sh(X)$ [Mor08] and the group of global sections $\mathcal{F}(X)$ is an injective $\mathbb{Z}[G]$-Mod [Gro57, Lemma 4.3.1].

We can apply the construction in the previous section to define equivariant étale cohomology groups of equivariant sheaves. Given a sheaf of k-modules $\mathcal{F} \in Sh(X, G)$ where k is a field, take an injective resolution $\mathcal{I}^*$ in $Sh(X, G)$ and apply the global section functor. This gives a complex of $k[G]$-modules $\mathcal{I}^*(X)$:

$$\mathcal{I}^0(X) \to \mathcal{I}^1(X) \to \mathcal{I}^2(X) \cdots$$

Define a δgk-Mod $\beta_G^*(\mathcal{F})$ where $\beta_G^n(\mathcal{F}) := \oplus_{i+j=n} Hom_{k[G]}(\mathcal{E}_i, \mathcal{I}^j(X))$.

Definition 5.2.2. The equivariant sheaf cohomology is defined as $H_G^*(X, \mathcal{F}) := H^*(\beta_G^*(\mathcal{F}))$. $\diamondsuit$

Remark 5.2.3. A standard spectral sequence argument shows that $H_G^*(X, \mathcal{F})$ defined in this way is equal to Grothendieck's equivariant cohomology groups $H^*(X, G, \mathcal{F})$, which are derived functors of $\mathcal{F}(X)^G$ [Wei94, 5.8]. $\diamondsuit$

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

Definition 5.2.4. Define $\widehat{\beta}^*_G(\mathcal{F}) := Hom_{k[G]}(\mathcal{J}_*, \mathcal{I}^*(X))$ where $\widehat{\beta}^n_G(\mathcal{F}) := \oplus_{i+j=n} Hom_{k[G]}(\mathcal{J}_i, \mathcal{I}^j(X))$. Define $\widehat{H}^*_G(X, \mathcal{F}) := H^*(\widehat{\beta}^*_G(\mathcal{F}))$. $\diamondsuit$

When $G = \mathbb{Z}/2$, we can choose a (minimal) complete resolution $\mathcal{J}^*$ by splicing together a (minimal) resolution $\mathcal{E}^*$ and its dual. Under this $\mathcal{J}^*$, the following is a corollary of Lemma 5.1.1:

Corollary 5.2.5. *As a $\delta gk[t, \frac{1}{t}]$-Mod, $\widehat{\beta}^*_G(\mathcal{F}) \cong \beta^*_G(X, \mathcal{F}) \otimes_{k[t]} k[t, \frac{1}{t}] \cong C^* \widetilde{\otimes} k[t, \frac{1}{t}]$.*

By definition, it is obvious that $\widehat{\beta}^{i+1}_G(\mathcal{F}) \cong \widehat{\beta}^i_G(\mathcal{F}) \otimes_{k[t, \frac{1}{t}]} t$ and $\widehat{H}^{i+1}_G(X, \mathcal{F}) \cong \widehat{H}^i_G(X, \mathcal{F}) \otimes_{k[t, \frac{1}{t}]} t$. In particular, $\widehat{H}^*_G(X, \mathcal{F})$ is a free $k[t, \frac{1}{t}]$ module.

$H^*_G(X, -)$ satisfies the usual properties as a derived functor, and there is a spectral sequence converging to it:

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

On the other hand, it is also proved in [Mor08] that $\widehat{H}^*_G(X, -)$ satisfies some nice properties. 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 in $\widehat{H}^*_G(X, -)$. There is also a functorial spectral sequences converging to $\widehat{H}^*_G(X, -)$, whose E_2 page is given by

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

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

5.3 The Localization Theorem

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

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 such 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. For $\mathcal{F} \in Sh(X, G)$, one can define the *equivariant push-forward* $\pi_*^G(\mathcal{F})$: for an étale open V on W_{et}, $\pi_*^G\mathcal{F}(V) := \mathcal{F}(X \times_W V)^G$. π^* and π_*^G are quasi-inverses of categories between $Sh(X, G)$ and $Sh(W)$. 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 $q \geq n + 1$.

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

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. In other words, Z is the ramification loci in the cover $X \to X/G =: W$. X' is 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.

Suppose $\phi : U \to X$ is an étale neighborhood of Z, where ϕ is a G-equivariant map and $\phi^{-1}(Z)$ intersects with each connected component of U non-empty, then U is called a *G-étale neighborhood* of Z in X. The system of G-étale neighborhoods is cofinal in the system of étale neighborhoods of $Z \subset X$. $\widetilde{Z}$ is the projective limit of the G-étale neighborhoods of Z in X. Denote by i the embedding $i : Z \to X$ and $\widetilde{i}$ the canonical map $\widetilde{i} : \widetilde{Z} \to X$. i factors through $\widetilde{i}$.

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

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 and $\mathcal{F}$ is torsion, there is an isomorphism [Hub93]:

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

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

In the following, we will abuse notation and write $\mathcal{F}$ or $\mathcal{F}|_Z$ for $i^*\mathcal{F}$ on Z, and similarly for $\widetilde{i}^*\mathcal{F}$ on $\widetilde{Z}$. Using the localization theorem, one can prove a Smith-type inequality 5.3.1 on the étale site of schemes when $G = \mathbb{Z}/2$. (The case $G = \mathbb{Z}/p$ for an odd prime p can also be treated with similar techniques.) Given a field k, we write $k_1 := k[t]/(t-1) = k[t, \frac{1}{t}]/(t-1)$. $k_0 := k[t]/(t)$. For a graded $k[t]$-Mod, $- \otimes_{k[t]} k_1$ is an exact functor from graded $k[t]$-Mod to k-Mod. When $k = \mathbb{F}_2$, we will still write k_0 and k_1 to avoid overloading the notations.

Proposition 5.3.6. *Suppose $G = \mathbb{Z}/2$, under the hypothesis in Corollary 5.3.5,*

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

for any m, where $h^i := dim_k H^i$.

Proof. For the proof of this proposition we will use the minimal Hirsch-Brown model for $\beta^*_G(\mathcal{F})$,

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

There are also minimal Hirsch-Brown models for the other complexes

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

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

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

Since the action of G on Z is trivial, the complex 5.3.3 has trivial differentials. 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 then fits into the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{F}_{m-1}(\beta_G^*(\mathcal{F})) \arrow[r] \arrow[d, "i^\sharp"'] & \beta_G^*(\mathcal{F}) \arrow[r] \arrow[d, "i^\sharp"'] & \beta_G^*(\mathcal{F})/\mathcal{F}_{m-1} \arrow[r] \arrow[d, "\bar{i}^\sharp"'] & 0 \\
0 \arrow[r] & \mathcal{F}_{m-1}(\beta_G^*(\mathcal{F}_Z)) \arrow[r] & \beta_G^*(\mathcal{F}|_Z) \arrow[r] & \beta_G^*(\mathcal{F}|_Z)/\mathcal{F}_{m-1} \arrow[r] & 0
\end{tikzcd} \tag{5.3.7}$$

After localizing at $\otimes_{k[t]} k_1$ and taking cohomology, the middle map $i^\sharp \otimes_{k[t]} k_1$ becomes an isomorphism by Corollary 5.3.5. Since the differentials on $H^*(Z, i^*\mathcal{F}) \otimes k[t]$ is trivial, the map $\bar{i}^\sharp \otimes_{k[t]} k_1$ is surjective on the cochain level as well. Since

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

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

one gets the desired inequality in Equation 5.3.1.

□

Remark 5.3.7. Proposition 5.3.6 can be compared with the result in [Sym04], which uses Bredon's equivariant cohomology of a *local system.* ♢

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)

$$\sum_{i=0}^{\infty} h^i(Z,\mathcal{F}) = \sum_{i=0}^{\infty} h^i(X,\mathcal{F}) \tag{5.3.8}$$

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

$(b) \Rightarrow (a)$: Factor δ into a surjection followed by an injection: $H^*(X,\mathcal{F})\widetilde{\otimes}k[t] \to M \to H^*(X,\mathcal{F})\widetilde{\otimes}k[t]$. M is a sub-module of the free $k[t]$-Mod $\beta_G^*(\mathcal{F})$, therefore M is also a free $k[t]$-Mod. 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 $\otimes_{k[t]} k_1$ is exact and M is free. □

Based on Proposition 5.3.8, when equality is reached in 5.3.8, 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. We will later refer to this condition as the *maximum* condition. Under the maximum condition, $H^*_G(X,\mathcal{F}) \cong \beta^*_G(\mathcal{F})$ as $\delta gk[t]$-Mod. The map $i^\sharp$ induces a map between two free $k[t]$-Mod which is an isomorphism after tensoring with k_1, which implies that $i^\sharp$ is injective.

5.4 The Equivariant Construction

Now consider a situation that is comparable to Chapter 4. Suppose Y is a regular projective variety over a finite field $\operatorname{Spec}\mathbb{F}_q$ of odd characteristic. Suppose the group $G = \mathbb{Z}/2$ acts on Y. The constant sheaf $\mathcal{F} = \mu_2 \in Sh(Y,G)$ is adapted on Y [Mor08, 3.12]. Since $\mu_2^{\otimes n} \cong \mathbb{Z}/2$ on Y, by ignoring the Tate twists $H^*(Y,\mu_2)$ is a Pioncaré algebra [Ras95, 1.12], which is an algebra that satisfies the following requirements:

Definition 5.4.1. 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 the orientation $A \times A \to A \xrightarrow{\mathcal{O}_A} k$ induces a k-linear isomorphism $A \xrightarrow{\cong} Hom_k(A,k)$.

- Suppose $A = \oplus_{i=0}^n A_i$ is a graded algebra. If $\mathcal{O}_A(A_i) = 0$ when $i < n$, then $A \xrightarrow{\cong} Hom_k(A,k)$ implies that $\forall i$, $A_i \xrightarrow{\cong} Hom_k(A^{n-i},k)$. $(A,\mathcal{O}_A)$ 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 $\mathcal{F}_iA \times \mathcal{F}_jA \subset \mathcal{F}_{i+j}A$.

If $\mathcal{O}_A(\mathcal{F}_{n-1}A) = 0$, then $A \xrightarrow{\cong} Hom_k(A, k)$ implies that $\forall i$, $\mathcal{F}_iA \xrightarrow{\cong}$ $Hom_k(A/\mathcal{F}_{n-i-1}A, k)$. $(A, \mathcal{O}_A)$ is called a filtered Poincaré algebra.

$\diamondsuit$

Given a graded algebra A, there is an associated filtered algebra $\mathcal{A}$, where $\mathcal{F}_m\mathcal{A} := \oplus_{i=0}^m A_i$. Conversely, given a filtered algebra $\mathcal{A}$, there is an associated graded algebra $A := gr(\mathcal{A})$, where $A_m := \mathcal{A}_m/\mathcal{A}_{m-1}$.

Proposition 5.4.2. *[AP93, Proposition 5.1.3] $\mathcal{A}$ is a filtered Poincaré algebra if A is a graded Poincaré algebra, and vice versa.*

We will apply Proposition 5.4.2 when $H^*(Y, \mu_2)$ is a graded Poincaré algebra. Recall when the maximum condition is reached in 5.3.8, we have an isomorphism of $\mathbb{F}_2$ vector spaces:

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

where the multiplication in the algebra structure on the R.H.S is "deformed" 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 5.3.8. We have a straightforward observation:

Lemma 5.4.3. *$H^*(Y, \mu_2) \cong gr((H^*(Y, \mu_2)\widetilde{\otimes}\mathbb{F}_2[t]) \otimes_{\mathbb{F}_2[t]} k_1)$ as a graded algebra.*

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

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

Remark 5.4.4. We will denote the original filtration on $\beta^*_G(Z, \mu_2)$ by $\widetilde{\mathcal{F}}$, i.e.

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

Since the differential is trivial, this filtration passes to the cohomology

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

Applying the functor $\otimes_{\mathbb{F}_2[t]} k_1$ to Equation 5.4.3, which commutes with taking cohomology, one gets $\widetilde{\mathcal{F}}$ on $H^*_G(Z, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1$.

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. To distinguish the situation, we will denote the new filtered algebra structure on $H^*_G(Z, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1$ by $\mathcal{F}$, which is in general different from $\widetilde{\mathcal{F}}$ defined above. ♢

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

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

Remark 5.4.5. Suppose the algebra structure of $H^*(Y, \mu_2)$ is not known, but one knows the image of the filtration $\mathcal{F}_m(H^*(Y, \mu_2) \widetilde{\otimes}_{\mathbb{F}_2[t]} k_1) \to H^*(Z, \mu_2)$ and the algebra structure of $H^*(Z, \mu_2)$ (which is often easier to calculate since Z has lower dimension) one can recover the algebra structure of $H^*(Y, \mu_2)$ by considering the associated graded algebra. We call this the *deformation trick*. It is used in Example 5.6.5. ♢

Definition 5.4.6. When $H^*(Y, \mu_2)$ is a graded Poincaé algebra of dimension $2d+1$, the image $\mathcal{F}_d H^*(Z, \mu_2)$ becomes its own orthogonal complement in the filtered algebra structure. When the induced bilinear product:

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

is a Euclidean form, $\mathcal{F}_d H^*(Z, \mu_2)$ is a self-dual code. This is the third approach to the construction of binary self-dual codes, the *Equivariant Construction.* $\diamondsuit$

Remark 5.4.7. A difference in the applicability between Construction G and the Equivariant Construction should be pointed out here. In the Equivaraint construction, it is necessary that $H^*(Y, \mu_2)$ is a graded Poincaré algebra, for example when Y is regular and projective over $\mathbb{F}_q$.

On the other hand, in Construction G, it is not necessary for $H^*(Y, \mu_2)$ to be dual to itself. The only duality statement required there is that $H^*(Y, \mu_2)$ is dual to $H^*_c(Y, \mu_2)$. For example, Construction G works when a regular, relative projective variety Y is supported on an open subscheme of the ring of integers of a totally imaginary number field. $\diamondsuit$

Example 5.4.8. 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 $0 \le i \le m$, 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 the maximum condition in 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. △

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 when Y is a smooth projective curve over a finite field $\mathbb{F}_p$. The reader is referred to Proposition A.0.12 for an analogous comparison result in the topological situation. The comparison in the arithmetic situation is more complicated, due to the fact that a *closed point* on $Y_{\mathbb{F}_p}$ has cohomological dimension one rather than zero.

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. Compared 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:*

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

Example 5.5.4. In the situation of example 5.4.8, $\mathcal{F}_1(H^*(Y,\mu_2)\otimes_{\mathbb{F}_2[t]}k_1) \to H^*(Z,\mu_2)$ 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 $\pi : Y \to \mathbb{P}^1_{\mathbb{F}_q}$. 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.

Comparison of vector spaces:

This argument is similar to Proposition A.0.12. 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, $H^j(\widetilde{Z}_i,\mu_2) = H^j(Z_i,\mu_2)$, therefore τ reaches the maximum condition on $\widetilde{Z}_i$: $\sum_{j=0}^{\infty} h^j(\widetilde{Z}_i,\mu_2) = \sum_{j=0}^{\infty} h^j(Z_i,\mu_2)$. Thus
$H^*_\tau(\widetilde{Z}_i,\mu_2) = H^*(Z_i,\mu_2) \otimes \mathbb{F}_2[t]$, in particular $h^1_\tau(\widetilde{Z}_i,\mu_2) = 2$.

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 $H^1_\tau(\widetilde{U}_i,\mu_2)$ degenerate on the E_2 page. We can compare the sequences:

$$\begin{tikzcd}
0 \to H^1(\mathbb{Z}/2, H^0(\mathcal{O}_{K,\mathfrak{p}_i},\mu_2)) \arrow[r] \arrow[d, "d_1"] & H^1_\tau(\mathcal{O}_{K,\mathfrak{p}_i},\mu_2) \arrow[r] \arrow[d, "d_2"] & H^0(\mathbb{Z}/2, H^1(\mathcal{O}_{K,\mathfrak{p}_i},\mu_2)) \to 0 \arrow[d, "d_3"] \\
0 \to H^1(\mathbb{Z}/2, H^0(K_{\mathfrak{p}_i},\mu_2)) \arrow[r] & H^1_\tau(K_{\mathfrak{p}_i},\mu_2) \arrow[r] & H^0(\mathbb{Z}/2, H^1(K_{\mathfrak{p}_i},\mu_2)) \to 0
\end{tikzcd} \tag{5.5.5}$$

It is easy to see that 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 $d_3(H^0(\mathbb{Z}/2, H^1(\mathcal{O}_{K,\mathfrak{p}_i},\mu_2)))$.

By the five lemma, d_2 is an isomorphism as well. This proves $H^1_\tau(\widetilde{Z}_i,\mu_2) \to H^1_\tau(\widetilde{U}_i,\mu_2)$.

Therefore in Equation 5.5.4, the image of $H^1_\tau(Y, \mu_2) \to H^1_\tau(\widetilde{Z}, \mu_2)$ is isomorphic to the image from $H^1(A, \mu_2) \to H^1_\tau(\widetilde{U}, \mu_2)$. By the maximum condition $H^*_\tau(Y, \mu_2) = \beta^*_\tau(Y, \mu_2)$, $H^*_\tau(\widetilde{Z}, \mu_2) = \beta^*_\tau(\widetilde{Z}, \mu_2)$ are free $k[t]$-modules, thus the image of $H^1_\tau(Y, \mu_2) \to H^1_\tau(\widetilde{Z}, \mu_2)$ is isomorphic to $H^1_\tau(\widetilde{Z}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1 = \widetilde{\mathcal{F}}_1(H^*_\tau(\widetilde{Z}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1) = H^*(Z, \mu_2)$. On the other hand, $H^1_\tau(\widetilde{U}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1 = H^1(U', \mu_2)$ in Construction G. Thus the 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 use 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.0.12, 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* $H^i(\mathbb{F}_q, \mathcal{F}_j(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1))$, $i + j = m$ *converges to* $\mathcal{F}_m(H^*_\tau(Y, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)$ *in increasing order of* i.

Proof. $\mathcal{F}_m(H^*_\tau(Y, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1) \cong \mathcal{F}_m((H^*(Y, \mu_2)\widetilde{\otimes}\mathbb{F}_2[t]) \otimes_{\mathbb{F}_2[t]} k_1)$ is approximated 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 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:

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

This proves the claim. △

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 by the Leray spectral sequence $H^j(\mathbb{F}_q, H^0(Z_{r,\overline{\mathbb{F}}_q}, \mu_2)) = H^j(\mathbb{F}_{\mathfrak{q}_r}, \mu_2)$.

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. Lemma 5.5.6 shows, as a $Gal(\mathbb{F}_q)$ module,
$H^*(Z_{\overline{\mathbb{F}}_q}, \mu_2) \cong \mathcal{F}_2(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1) \cong H^*(Y_{\overline{\mathbb{F}}_q}, \mu_2) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus H^1(Y_{\overline{\mathbb{F}}_q}, \mu_2)$.

On the other hand, if one ignores the $Gal(\mathbb{F}_q)$ structure, it is easily seen from Lemma 5.5.6 that the cup-product $H^1 \times H^1 \to H^2 \cong \mathbb{F}_2$ is alternate on a topological torus, which is well-known. ♢

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: $N = \mu_2$, $H^1(Y_{\overline{\mathbb{F}}_q}, \mu_2)$ and $\pi_{r,*}\mu_2$. Suppose $Gal(\mathbb{F}_{q_r}/\mathbb{F}_q) = \mathbb{Z}/r$, the inflation map
$H^i(\mathbb{Z}/(2r), N) \xrightarrow{\cong} H^i(\mathbb{F}_q, N)$ is an isomorphism when $i \leq 1$. We will use the cyclic

group $\mathbb{Z}/(2r)$ to do some explicit computations $P : H^i(\mathbb{Z}/(2r), N) \to H^i(\mathbb{Z}/(2r), N')$ for various modules N and 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 the image of $P : H^i(\mathbb{F}_q, \mathcal{F}_j(H^*_\tau(Y_{\overline{\mathbb{F}}_q}, \mu_2) \otimes_{\mathbb{F}_2[t]} k_1)) \to H^i(Z, \mu_2)$.

- $P(H^0(\mathcal{F}_0)) = \{\sum_{r=1}^4 a_r\}$.
- $P(H^1(\mathcal{F}_0)) = \{\sum_{r=1}^4 b_r\}$.
- $P(H^0(\mathcal{F}_1)) = \{a_1 + a_2, a_1 + a_3\} + P(H^0(\mathcal{F}_0))$.
- Using $P(H^1(\mathcal{F}_0) \times H^0(\mathcal{F}_1)) \subset P(H^1(\mathcal{F}_1))$, it is easy to see

  $P(H^1(\mathcal{F}_1)) = \{b_1 + b_2, b_1 + b_3\} + P(H^1(\mathcal{F}_0))$.
- $P(H^0(\mathcal{F}_2)) = \{a_1\} + P(H^0(\mathcal{F}_1))$.
- $P(H^1(\mathcal{F}_2)) = \{b_1\} + P(H^1(\mathcal{F}_1))$.

Remark 5.5.8. 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, (for example, when it is a Poincaré algebra) $b_r \notin \mathcal{F}_2$. Therefore the fact that $P(H^1(\mathcal{F}_2)) = b_1 + P(H^1(\mathcal{F}_1))$ can be seen more directly. $\diamondsuit$

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. $\triangle$

Remark 5.5.9. Suppose Y is $P^1_{\mathbb{F}_q}$ double covering itself with two ramification points, say the point 0 and ∞. It is straightforward to check that the maximum condition in 5.3.8 is also met. The calculation for the ring structure of $H^*(P^1_K, \mu_2)$ is the same as the above Condition (2) in a verbatim way. ♢

5.6 The Smith Type Inequality

In this section we illustrate with two more examples when the maximum 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 $\mathbb{C}$. We simply remark that when σ is “geometric”, i.e. σ acts trivially on the constants $\mathbb{C}$, then the Smith type inequality 5.3.1 gives a restriction on the topological type of the ramification loci and the intersection behavior among its connected components. ♢

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 $|S_f| = n$.

- $h^0(X, \mu_2) = 1$.
- Suppose $dim_{\mathbb{Z}/2} Pic(\mathcal{O}_K)[2] = r$. By the Kummer sequence, $h^1(X, \mu_2) = 1 + r$.
- Since $H^2(X, \mathbb{G}_m) = 0$, by the Kummer sequence $h^2(X, \mu_2) = r$. (Since 2 is not invertible on $\mathcal{O}_K$, μ_2 is not isomorphic to $\mathbb{Z}/2$ on $\mathcal{O}_K$. Thus $H^*(X, \mu_2)$ is

not a graded Poincaré algebra in the sense of Definition 5.4.1.)

- $h^3(X, \mu_2) = 1$.

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 inequality 5.3.1 says $r \geq n - \frac{3}{2}$. Since r is an integer, $r \geq n - 1$. On the other hand, it is a classical result of genus theory that $r = n - 1$. Although the maximum condition is not met in this example, the lower bound on $Pic(\mathcal{O}_K)[2]$ predicted by 5.3.1 is optimal. $\triangle$

Remark 5.6.3. If a number field K has a real embedding, $\sum_{i=0}^{\infty} h^i(\mathcal{O}_K, \mu_2) = \infty$, see [Mil06, Chapter 2]. The inequality 5.3.1 is trivially satisfied. $\diamondsuit$

Example 5.6.4. For a second example, consider a hyper-elliptic curve defined by an affine equation $y^2 = f(x)$ over a local field K with odd residue characteristic. Suppose $f(x)$ has good reduction over K, in other words, all of its coefficients have valuation 0 in K. $f(x)$ has degree $2g + 1$, and $f(x) = \Pi_{i=1}^{m} f_i(x)$ breaks into m irreducible factors over K. Consider the double cover $\pi : Y \to \mathbb{P}^1_K$. 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. $\sum_{j=0}^{\infty} h^j(Z, \mu_2) = \sum_{i=1}^{m+1} \sum_{j=0}^{2} h^j(Z_i, \mu_2) = 4(m + 1)$.

On the other hand, $h^j(Y, \mu_2)$ can be calculated by the spectral sequence

$H^i(K, H^j(Y_{\overline{K}}, \mu_2))$ which is concentrated at $0 \leq i \leq 2$, $0 \leq j \leq 2$. The only nontrivial $Gal(K)$ module in this spectral sequence is $H^1(Y_{\overline{K}}, \mu_2)$. Call it M. For similar reason as in Example 5.4.8, $h^0(K, M) = dim_{\mathbb{Z}/2}Pic(Y)[2] = m - 1$.

- $h^0(Y, \mu_2) = 1$.
- $h^1(Y, \mu_2) \leq h^1(K, \mu_2) + (m - 1) = m + 1$.
- $h^2(Y, \mu_2) \leq 2 + h^1(K, M)$. By assumption, the coefficients of $f(x)$ have trivial valuation in K. The $Gal(K)$ action on M factors through the unramified quotient $Gal(K^{un}/K) = \widehat{\mathbb{Z}}$. In other words, the subgroup $Gal(\overline{K}/K^{un}) =: H$ acts trivially on M. There is a short exact sequence

  $$0 \to H^1(\widehat{\mathbb{Z}}, M^H) \to H^1(K, M) \to H^0(\widehat{\mathbb{Z}}, H^1(H, M)) \to 0$$

  By Galois duality over a finite field,

  $$H^1(\widehat{\mathbb{Z}}, M^H) = H^1(\widehat{\mathbb{Z}}, M) \cong H^0(\widehat{\mathbb{Z}}, Hom(M, \mathbb{G}_m))$$

  Since M is an elementary abelian 2-group, $Hom(M, \mathbb{G}_m) = Hom(M, \mu_2) \cong M$ as a $\widehat{Z}$ module. Thus $h^1(\widehat{\mathbb{Z}}, M) = h^0(\widehat{\mathbb{Z}}, M) = m - 1$.

  $H^1(H, M) = Hom(H, M) = Hom(H^{ab}/2, M) = Hom(\mathbb{Z}/2, M) \cong M$ as a $\widehat{\mathbb{Z}}$ module. Therefore $h^0(\widehat{\mathbb{Z}}, H^1(H, M)) = m - 1$.

  To sum up, $h^1(K, M) = 2m - 2$, $h^2(Y, \mu_2) \leq 2m$.
- By Artin-Verdier duality, $h^3(Y, \mu_2) = h^1(Y, \mu_2)$, $h^4(Y, \mu_2) = h^0(Y, \mu_2)$, $h^i(Y, \mu_2) = 0$ for $i \geq 5$.

Summing up the above discussion, $4(m+1) \leq \sum_{i=0}^{\infty} h^i(Y, \mu_2) \leq 4m+4$, therefore it is an equality. The spectral sequence $H^i(K, H^j(Y_{\overline{K}}, \mu_2))$ degenerates on the E_2 page, and the maximum condition is reached in 5.3.8. △

Example 5.6.5. Following the above example, when the maximum condition is met, it is possible to use the deformation trick to calculate the ring structure of $H^*(Y, \mu_2)$. We will carry out a detailed computation when Y is an elliptic curve defined by a cubic equation $y^2 = f(x)$ as in the above example.

In the deformation trick, the image of the map P in equation 5.5.6 will be calculated. $Z = \sqcup_{r=1}^{m+1} Z_r$ is a union of $m+1$ closed points, where $m = 1, 2, 3$. 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 $\overline{K}$. 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 $|\mathbb{F}_r| \equiv 1 \bmod 4$.

Similar to the second half of example 5.5.4, there is

Lemma 5.6.6. *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.

Assume the curve Y has good reduction, and that all elements of $Pic_Y[2]$ are lifts of elements of $Pic_{Y_{\mathbb{F}_p}}[2]$, the $Gal(K)$ action on $H^*(Y_{\overline{K}},\mu_2)$ factors through $Gal(K^{un}/K)$. Lemma 5.5.6 still holds as a map of $Gal(K)$ modules. This map induces

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

which is used to compute the map P in Equation 5.5.6 by Lemma 5.6.6.

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 $i\le 1$. We will use these abelian group to do some explicit computations $P:H^i(\mathbb{Z}/(2r)\times\mathbb{Z}/2,N)\rightarrow H^i(\mathbb{Z}/(2r)\times\mathbb{Z}/2,N')$ when $i\le 1$ in equation 5.6.1. For $i=2$ we will use the functorality of P as a map of rings: if b, c are classes in H^1, $b\cup c$ is a class in H^2, then$P(b\cup c)=P(b)\cup P(c)$.

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 5.6.7. 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. △

Remark 5.6.8. When Y is P^1_K double covering itself with two ramification points, say the point 0 and ∞, it is straightforward to check that the maximum condition in 5.3.8 is also met. The calculation for the ring structure of $H^*(P^1_K, \mu_2)$ is the same as the above Condition (2) in a verbatim way. Thus we have answered Question 4.2.6 in full. $\diamondsuit$

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.0.9.

- *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 "maximum" 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

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

Since $H^*(X,k)$ is a Poincaré algebra of dimension $2r+1$, by proposition 5.4.2 $k^{\oplus m}$ 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.0.10. *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.0.10, 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 maximum. Take out an open ball D_i around each fixed point pt_i, $\tau|_{X \smallsetminus \sqcup_{i=1}^m D_i}$ is free. Denote the quotient manifold by $W := \tau|_{X \smallsetminus \sqcup_{i=1}^m D_i}$. 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 componentwise 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.0.11. *Every binary self-dual code can be obtained from an involution on an orientable 3-manifold.*

In the topological situation, when τ has the maximum 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:

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

Let's look at the short exact sequence

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

By the maximumity 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.0.12. *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.*

Bibliography

[Alb38] A. A. Albert. Symmetric and alternate matrices in an arbitrary field. i. *Trans. Amer. Math. Soc.*, 43(3):386–436, 1938.

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

[BB12] S. Bouyuklieva and I. Bouyukliev. An algorithm for classification of binary self-dual codes. *IEEE Trans. Inform. Theory*, 58(6):3933–3940, 2012.

[Ben98] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Math.* Cambridge Univ. Press, Cambridge, second edition, 1998. Basic representation theory of finite groups and associative algebras.

[BHM12] K. Betsumiya, M. Harada, and A. Munemasa. A complete classification of doubly even self-dual codes of length 40. *Electron. J. Combin.*, 19(3):Paper 18, 12, 2012.

[Bor60] A. Borel. *Seminar on transformation groups.* With contributions by G. Bredon, E. E. Floyd, D. Montgomery, R. Palais. Annals of Mathematics Studies, No. 46. Princeton Univ. Press, Princeton, N.J., 1960.

[Bro59] E. H. Brown, Jr. Twisted tensor products. I. *Ann. of Math. (2)*, 69:223–246, 1959.

[Cox79] D. A. Cox. The étale homotopy type of varieties over **R**. *Proc. Amer. Math. Soc.*, 76(1):17–22, 1979.

[CS99] J. H. Conway and N. J. A Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grund. der Math. Wiss.* Springer-Verlag, New York, third edition, 1999.

[DGH97] S. T. Dougherty, T. A. Gulliver, and M. Harada. Extremal binary self-dual codes. *IEEE Trans. Inform. 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'algèbre homologique. *Tôhoku Math. J. (2)*, 9:119–221, 1957.

[GS99] R. E. Gompf and A. I. Stipsicz. 4-*manifolds and Kirby calculus*, volume 20 of *Graduate Studies in Math.* Amer. Math. Soc., Providence, RI, 1999.

[HM07] M. Harada and A. Munemasa. Database of self-dual codes, Nov 2007. http://www.math.is.tohoku.ac.jp/∼munemasa/selfdualcodes.htm.

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

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

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

[Lem00] F. Lemmermeyer. *Reciprocity laws*. Springer Monographs in Math. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.

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

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

[Mil13] J. S. Milne. *Algebraic Number Theory (v3.05)*. 2013. Available at www.jmilne.org/math/.

[Mor08] B. Morin. Utilisation d'une cohomologie étale équivariante en topologie arithmétique. *Compos. Math.*, 144(01):32–60, January 2008.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grund. der Math. Wiss.* Springer-Verlag, Berlin, 1999.

[OP92] H. Oral and K. T. Phelps. Almost all self-dual codes are rigid. *J. Combin. Theory Ser. A*, 60(2):264–276, 1992.

[PH98] V. Pless and W. C. Huffman. *Handbook of coding theory.* Elsevier, 1998.

[Ple72] V. Pless. A classification of self-orthogonal codes over GF(2). *Discrete Math.*, 3:209–246, 1972.

[Ple98] V. Pless. *Introduction to the theory of error-correcting codes.* Wiley-Interscience Series in Discrete Math. and Optimization. John Wiley & Sons Inc., New York, third edition, 1998.

[Pup95] V. Puppe. Simply connected 6-dimensional manifolds with little symmetry and algebras with small tangent space. In *Prospects in topology (Princeton, NJ, 1994)*, volume 138 of *Ann. of Math. Stud.*, pages 283–302. Princeton Univ. Press, Princeton, NJ, 1995.

[Pup01] V. Puppe. Group actions and codes. *Canad. J. Math.*, 53(1):212–224, 2001.

[Ras95] W. Raskind. Abelian class field theory of arithmetic schemes. In *K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*, volume 58 of *Proc. Sympos. Pure Math.*, pages 85–187. Amer. Math. Soc., Providence, RI, 1995.

[RS98] E. M. Rains and N. J. A Sloane. Self-dual codes. In *Handbook of coding theory*, pages 177–294. Elsevier, 1998.

[Sai89] S. Saito. A global duality theorem for varieties over global fields. In *Algebraic K-theory: connections with geometry and topology (Lake Louise, AB, 1987)*, volume 279 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 425–444. Kluwer Acad. Publ., Dordrecht, 1989.

[Ser62] J. P. Serre. *Corps locaux.* Publications de l'Institut de Mathématique de l'Université de Nancago, VIII. Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962.

[Ser73] J. P. Serre. *A course in arithmetic.* Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Sha72] S. S. Shatz. *Profinite groups, arithmetic, and geometry.* Princeton Univ. Press, Princeton, N.J., 1972. Ann. Math. Studies, No. 67.

[Sti79] A. Stieglitz. Equivariant sheaf cohomology. *Manuscripta Math.*, 26(1-2):201–221, 1978/79.

[Sym04] P. Symonds. Smith theory for algebraic varieties. *Algebr. Geom. Topol.*, 4:121–131 (electronic), 2004.

[Wei94] C. A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Math.* Cambridge Univ. Press, 1994.