Algebraic Number Fields and Codes

Colleen Swanson

A thesis presented to the faculty of Mount Holyoke College
in partial fulfillment of the requirements for the degree of
Bachelor of Arts with Honors.

Department of Mathematics
South Hadley, Massachusetts

May 17, 2006

Acknowledgements

I would like to thank Farshid Hajir for his good humor and encouragement, Don O'Shea for his open nature and desire to help, and Harriet Pollatsek for being a patient and caring advisor.

Abstract

We explore error-correcting codes based on algebraic number fields using a particular code construction given by Guruswami in "Constructions of Codes from Number Fields" ([Guru]). After reviewing the necessary mathematical background, we analyze the rate and relative distance of the given code, and give an example of an asymptotically good code over an alphabet of size 31.

Contents

1 Introduction to Codes

In this chapter we shall provide a brief introduction to the theory of error-correcting codes. We refer the reader to [Rom] and [TV] for a more thorough treatment.

1.1 Basic Terminology

The purpose of codes is to provide an efficient method of transferring information over noisy channels. An important consideration in the communication of information is the possibility of *error*. Hence, it is useful if the code construction allows for *error detection* and *error correction*. In communicating via a telephone, for example, the significance of error detection and error correction is clear; without it, the conversation could become garbled and difficult to understand.

In general, an **error-correcting code** is an algorithm by which a sequence of numbers (letters, etc.) may be expressed in a format which allows for (some) errors in transmission to be detected and corrected. Ultimately, the goal is efficiency, and thus brevity as well as accuracy is key.

The basic idea is that we have a particular *message* we want to send, and to ensure the message is decipherable, we send an *encoded message* instead. Formally, to create a code we use an **alphabet** Q, a set of q distinct symbols. We will call a string of some fixed length k of elements of Q a **word**, and we say a **message** is a string of words. Thus, we may think of our possible word set as Q^k, where Q^k is the set of strings of length k over Q.

We encode a word, which is a a string of length k over Q, by expressing it as a string of length n over Q. That is, we create our code by taking any nonempty subset $\mathcal{C}$ of Q^n, where Q^n is the set of all strings of length n over Q. We call such a subset $\mathcal{C}$ a **q-ary block code**, and we say a **codeword**, or **encoded word**, c, is a string in $\mathcal{C}$, i.e. $c = (c_1, \ldots, c_n) \in \mathcal{C}$. We define an **encoded message** to be a string of codewords. As each codeword is a string of length n over Q, we say $\mathcal{C}$ has **block length** n.

We note that we shall always have $n \geq k$. In fact, in order to have an efficient error-correcting code, we take $n > k$, i.e. we build in some *redundancy* (a concept to be discussed later).

We can view the **encoding** process as a one-to-one function $E : Q^k \to Q^n$. In this sense, we say that a **q-ary block code** $\mathcal{C}$ is the image $E(Q^k) \subset Q^n$. We call the number of codewords in $\mathcal{C}$, $|\mathcal{C}|$, the **size** of $\mathcal{C}$. Similarly, we view the **decoding** process as a function: $D : Q^n \to Q^k$, such that $D \circ E$ is the identity map. For error-correcting codes, we use what is called **minimum**

distance decoding. That is, for a received message a', we decode by taking the codeword which is closest to the received message a'.

For example, suppose $Q = \{0, 1\}$, $k = 1$, and $n = 3$. We can choose $\mathcal{C} = \{000, 111\}$, with our encoding function

$$E(x) = \begin{cases} 000 & \text{if } x = 0 \\ 111 & \text{if } x = 1. \end{cases}$$

(Note that $k = \log_q |\mathcal{C}| = \log_2 2$.) Then the message $m = 1010110$ would be encoded as $E(m) = 111000111000111111000$. If an error occurs in transmission, i.e. suppose $E(m)' = 101000111000111111000$ is received instead, we would know at least one error occurred, as 101 is not a codeword. We would decode by taking the "nearest" codeword, which is of course $E(m)$. We would be correct so long as only one error occurred in transmission, as the only way to turn 101 into a codeword by changing one digit is to take 111. We call such a code a **repetition** code, and we note that this particular example is capable of detecting two errors in a single codeword, and correcting one.

Given two codewords $x, y \in \mathcal{C}$ we define the **Hamming distance** between x and y, denoted $d(x, y)$, to be the number of positions in which x and y differ. We note that Hamming distance satisfies the triangle inequality, and is a metric on $\mathcal{C}$. We define the **minimum distance** of a code $\mathcal{C}$, $\delta(\mathcal{C})$, as follows:

$$\delta(\mathcal{C}) = \min_{x \neq y \in \mathcal{C}} d(x, y).$$

In other words, the minimum distance implies that any two distinct codewords of $\mathcal{C}$ must differ in a at least $\delta(\mathcal{C})$ of the n positions.

We define the **error size** to be the number of errors which occur, i.e. $d(E(a), a')$, where a is the original message and a' is the received word. Now, we call a code $\mathcal{C}$ **t-error-detecting** if whenever $1 \leq$ error size $\leq t$, the received word is not a codeword. If $\mathcal{C}$ is t-error-detecting but not $(t+1)$-error-detecting, we say $\mathcal{C}$ is **exactly t-error-detecting**. Similarly, if minimum distance decoding is able to correctly decode a message with error size t, we say $\mathcal{C}$ is **t-error-correcting**. If $\mathcal{C}$ is t-error-correcting, but not $(t+1)$-error-correcting, we say that $\mathcal{C}$ is **exactly t-error-correcting**.

In fact, we can relate the minimum distance and error-correcting abilities of a code as follows.

Theorem 1 *([Rom]) Let $\mathcal{C}$ be a code. Then $\delta(\mathcal{C}) = d \iff \mathcal{C}$ is exactly $\lfloor \frac{d-1}{2} \rfloor$-error-correcting.*

Proof We note that our proof uses methods similar to that in [Rom]. Suppose $\delta(\mathcal{C}) = d$. Let a be the original codeword, and a' the received word

satisfying $d(a', a) \leq \lfloor \frac{d-1}{2} \rfloor$. Then a is the unique closest codeword to a', for if $a^* \neq a$ is at least as close to a' as a is, then $d(a^*, a') \leq \lfloor \frac{d-1}{2} \rfloor$. But

$$d(a, a^*) \leq d(a, a') + d(a', a^*) \leq 2 \cdot \lfloor \frac{d-1}{2} \rfloor \leq d - 1 < d = \delta(\mathcal{C}),$$

and thus we have a contradiction. Hence $\mathcal{C}$ is $\lfloor \frac{d-1}{2} \rfloor$ error-correcting.

We will now show that $\mathcal{C}$ is *exactly* $\lfloor \frac{d-1}{2} \rfloor$ error-correcting. First, suppose d is even. That is, suppose $d = 2s$ for some $s \in \mathbb{Z}_{\geq 1}$. Let a and a^* be two codewords such that $d(a, a^*) = 2s$. Suppose that the codeword a is received as some word a' with error size $s = \frac{d}{2} = \lfloor \frac{d-1}{2} \rfloor + 1$. Suppose further that all errors in a' occur in exactly those positions in which a and a^* differ, and that a' agrees with a^* in all of those s positions. Then $d(a', a) = s$, but

$$d(a', a^*) = 2s - s = s.$$

Thus there would not be a unique closest codeword to a'.

Second, suppose d is odd. That is, suppose $d = 2s + 1$ for some $s \in \mathbb{Z}_{\geq 0}$. Let a and a^* be two codewords such that $d(a, a^*) = 2s + 1$. Suppose that the codeword a is received as some word a' with error size $s+1 = \lfloor \frac{(2s+1)-1}{2} \rfloor + 1 = \lfloor \frac{d-1}{2} \rfloor + 1$. Suppose further that all errors in a' occur in exactly those positions in which a and a^* differ, and that a' agrees with a^* in all of those $s+1$ positions. Then $d(a', a) = s + 1$, but

$$d(a', a^*) = 2s + 1 - (s + 1) = s.$$

Thus a' would be incorrectly decoded as a^*.

Hence $\mathcal{C}$ is not $\lfloor \frac{d-1}{2} \rfloor + 1$-error-correcting.

Conversely, suppose $\mathcal{C}$ is exactly $\lfloor \frac{d-1}{2} \rfloor$-error-correcting. If we had two codewords a and a^* such that $d(a, a^*) \leq d - 1$, then it is possible the received word a' would have exactly $\lfloor \frac{d-1}{2} \rfloor$ errors such that a' is at least as close to a^* as to a. If we had two codewords a and a^* such that $d(a, a^*) \geq d + 1$, then the code $\mathcal{C}$ would be $\lfloor \frac{d}{2} \rfloor$-error-correcting. Hence $\delta(\mathcal{C}) = d$. ∎

We shall also use the following concepts:

Definition 1 Let $\mathcal{C}$ be a q-ary code of block length n. Then

1. $\mathcal{R}(\mathcal{C}) = \frac{\log_q |\mathcal{C}|}{n}$ is called the **rate** of $\mathcal{C}$.

2. $\mathcal{D}(\mathcal{C}) = \frac{\delta(\mathcal{C})}{n}$ is called the **relative distance** of $\mathcal{C}$.

The rate of a code is one way of expressing the code's redundancy. For the q-ary code $\mathcal{C}$ of block length n, the **redundancy** is $n - \log_q |\mathcal{C}|$, as there are q^n possible possible strings of length n, but $q^n - |\mathcal{C}|$ of them are invalid codewords. We can calculate the redundancy from the rate easily, as the redundancy equals $n(1 - \mathcal{R}(\mathcal{C}))$. We think of the rate as a way to express the amount of information being transmitted per block. The relative distance is simply the minimum percentage of positions by which any two codewords of $\mathcal{C}$ must differ.

1.2 Codes over Finite Fields

Now we will impose more structure on our codes. We let $\mathbb{F}_q$ be the field of q elements, where q is a prime power. (For those in need of a brief review of field terminology, see Chapter 2). We shall define a code $\mathcal{C}$ of block length $n \geq 1$ over alphabet $\mathbb{F}_q$ to be a subset of $\mathbb{F}_q^n$. If $\mathcal{C}$ is an error-correcting code, then we need the minimum distance, $d(\mathcal{C})$, to be 'large'. A formal definition follows.

Definition 2 We define an $[n, k, d]_q$-code $\mathcal{C}$ to be a subset of $\mathbb{F}_q^n$ of size q^k such that two distinct codewords c_1 and c_2 of $\mathcal{C}$ differ in at least d of the n positions.

Thus, we say that an $[n, k, d]_q$-code $\mathcal{C}$ has block length n, dimension k, and minimum distance d. Using this notation, we note that $\mathcal{R}(\mathcal{C}) = \frac{\log_q |\mathcal{C}|}{n} = \frac{k}{n}$ and $\mathcal{D}(\mathcal{C}) = \frac{d}{n}$. If $\mathcal{C}$ is a *subspace* of dimension k of the vector space $\mathbb{F}_q^n$, then we say $\mathcal{C}$ is a **linear** code. For non-linear codes, we note that the dimension, k, need not be an integer.

1.3 Hamming $[7, 4, 3]_2$ Code

Let us consider an example of a linear error-correcting code that can correct single errors. One such code is the Hamming $[7, 4, 3]_2$ code, in which the encoding function $E : \mathbb{F}_2^4 \to \mathbb{F}_2^7$ is a linear transformation and $\mathcal{C} = E(\mathbb{F}_2^4)$ is the image of E. Thus, the Hamming code is linear, and we can find G, the standard matrix representation of the linear transformation E. Formally, we call such a matrix G a **generator** matrix.

For the Hamming $[7, 4, 3]_2$-code,

$$G = \begin{pmatrix} 1000111 \\ 0100011 \\ 0010101 \\ 0001110 \end{pmatrix}.$$

We encode a word $x \in \mathbb{F}_2^4$ by multiplying G on the right of x.

Now, we may use the following **parity check** matrix H, which has the property $GH = \mathbf{0}$, to determine if errors have occurred, and correct single errors.

We let

$$H = \begin{pmatrix} 111 \\ 110 \\ 101 \\ 011 \\ 001 \\ 010 \\ 100 \end{pmatrix}.$$

Suppose we encode [1010]. Multiplying by G, we get [1010010]. Note that $[1010010]H = \mathbf{0}$.

Since $d = 3$ in this case, by Theorem 1, we can correct single errors. Now, suppose we had a single error in transmission, and instead received [1011010]. Then multiplying by H, we get [011], which corresponds to the fourth row of H, and points to an error in the fourth digit, so the fourth digit must be 0 instead of 1.

1.4 Comparing the Rate and Relative Distance

Let $\mathcal{C}$ be an $[n, k, d]_q$-code. Let us note some elementary relationships between these parameters. Clearly, $0 \leq k \leq n$ and $0 \leq d \leq n$. We note that $0 \leq \mathcal{R}(\mathcal{C}) \leq 1$ and $0 \leq \mathcal{D}(\mathcal{C}) \leq 1$.

We may also relate $\mathcal{R}(\mathcal{C})$ and $\mathcal{D}(\mathcal{C})$ using the **Singleton Bound**.

Theorem 2 (Singleton Bound) *Given an $[n, k, d]_q$-code $\mathcal{C}$, we have $k+d \leq n+1$.*

Hence we may conclude $\mathcal{R}(\mathcal{C}) + \mathcal{D}(\mathcal{C}) \leq 1 + \frac{1}{n}$. Now, let us consider some trivial examples of codes.

1. Consider an $[n, 1, n]_q$-code. That is, $k = 1$ and $d = n$. This corresponds to a code in which there are q possible (1-dimensional) messages and each message $x \in \mathbb{F}_q \mapsto (x, x, \ldots, x) \in \mathbb{F}_q^n$. Such a code is called a **repetition** code.

2. Consider an $[n, n, 1]_q$-code. That is, $k = n$ and $d = 1$. This corresponds to a code in which the encoding function is essentially a permutation mapping from $\mathbb{F}_q^n \to \mathbb{F}_q^n$.

3. Consider an $[n, n-1, 2]_2$-code. That is, $q = 2$, $k = n-1$ and $d = 2$. An example of such a code is the **parity** code defined by $\mathcal{C} = \{(v_1, \ldots, v_n) | \sum_{i=1}^{n} v_i = 0\}$. That is, each codeword $x = (v_1, \ldots, v_{n-1}) \in \mathbb{F}_2^{n-1}$ maps to $(v_1, \ldots, v_{n-1}, v_n)$, where $v_n = 0$ if x has an even number of 1s, and $v_n = 1$ if x has an odd number of 1s. In this case we call v_n a **check digit**. Codes with check digits are used, for example, in creating ISBN numbers.

Now, in order to be good, a code $\mathcal{C}$ should have a relatively large minimum distance (for the purposes of error-correction), and as little redundancy as possible (to obtain a high information rate). For any fixed n, the task of determining the "best" code is difficult. We let $n \to \infty$ to get a sense of the possible restrictions on $\mathcal{R}(\mathcal{C})$ and $\mathcal{D}(\mathcal{C})$. This leads us to the concept of **asymptotically good** codes.

Definition 3 A family of codes $\{\mathcal{C}_i\}$, where each $\mathcal{C}_i$ is an $[n_i, k_i, d_i]$-code, is **asymptotically good** if, as $n_i \to \infty$, the following hold:

1. $\mathcal{R}(\{\mathcal{C}_i\}) := \liminf \frac{k_i}{n_i} > 0$,

2. $\mathcal{D}(\{\mathcal{C}_i\}) := \liminf \frac{d_i}{n_i} > 0$.

Later, we will explore a code construction which gives a family of asymptotically good codes based on number fields, a result shown in [Guru]. Next, however, we shall discuss another threshold by which codes may be considered "good": the Gilbert Varshamov threshold. The Gilbert Varshamov threshold is an indicator of the "greatness" of a code.

1.5 Gilbert Varshamov threshold

We shall give only a brief discussion of the Gilbert Varshamov threshold; we refer the reader to [TV].

Let us first introduce the entropy function, and then give the Gilbert Varshamov threshold.

Definition 4 We define the **q-ary entropy function**, denoted $H_q(x)$, as follows.

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x).$$

Definition 5 We call $R_{GV}(\delta) = 1 - H_q(\delta)$ the **Gilbert Varshamov curve**.

Theorem 3 (Gilbert Varshamov threshold) *For a given $\delta > 0$, if $0 < R \leq 1 - H_q(\delta)$, then there exists an asymptotically good family of q-ary codes $\{\mathcal{C}_i\}$ such that $\mathcal{R}(\{\mathcal{C}_i\}) = R$ and $\mathcal{D}(\{\mathcal{C}_i\}) = \delta$.*

That is, we know an asymptotically good family of codes $\{\mathcal{C}_i\}$ exists so long as its parameters fall below the Gilbert Varshamov curve. Thus, an asymptotically good family of codes $\{\mathcal{C}_i\}$ whose rate exceeds the Gilbert Varshamov curve is said to "beat the Gilbert Varshamov threshold," and is considered superior. The existence of such codes, established by Tsfasman, Vladut, and Zink, using algebraic geometry, was a major development of coding theory in the 1980s.

2 Introduction to Number Fields

In this chapter we review the algebraic number theory necessary for our code construction. A more thorough treatment may be found in [Mar] or [Sam], whose notation and treatment we follow closely.

2.1 Fields

Recall that a **field** is a commutative ring with unity in which every nonzero element is a **unit**. A **unit** refers to an invertible element in a ring.

For every field K we may define a (unique) ring homomorphism

$$\phi : \mathbb{Z} \mapsto K, \text{ where}$$

$$\phi(n) = \begin{cases} \overbrace{1 + \ldots + 1}^{n} & \text{if } n \geq 0 \\ -\phi(|n|) & \text{otherwise.} \end{cases}$$

If ϕ is injective, $\mathbb{Z}$ may be identified with the subring $\phi(\mathbb{Z})$ of K, in which case we say that K is of **characteristic 0**. Otherwise, the $\ker(\phi)$ is an ideal $p\mathbb{Z}$ where $p > 0$. Hence $\mathbb{Z}/p\mathbb{Z}$ may be identified with the subring $\phi(\mathbb{Z}/p\mathbb{Z})$ of K, from which it follows that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. Hence p is in fact prime, and K is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ ([Sam]). We say K is of **characteristic p**. By convention, this finite field K is denoted $\mathbb{F}_p$.

Now, we say a field K is an **extension** of a field L, written K/L, if L is a subfield of K. We define the **degree** of an extension K/L to be the dimension of K as a vector space over L. That is, $[K : L] = \dim_L K$.

2.2 Ideals and Integral Domains

We call an additive subgroup A of a ring R an **ideal** of R if for every $a \in A$ and every $r \in R$, we have $ra \in R$ and $ar \in R$. We note that the set of cosets $\{r + A | r \in R\}$ of A is a ring with the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ so long as A is an ideal. We call this the **quotient** or **factor** ring.

Moreover, a **maximal** ideal A of R is a proper ideal of R such that, if B is an ideal of R and $A \subset B \subset R$, we have $B = A$ or $B = R$. An ideal A of R is called a **prime** ideal if A is a proper ideal such that if $\alpha, \beta \in R$ and $\alpha\beta \in A$, then $\alpha \in A$ or $\beta \in A$.

Recall that an **integral domain** is a commutative ring with unity which has no zero divisors. A **zero divisor** is a nonzero element $\alpha \in R$, where R is a commutative ring, such that nonzero $\beta \in R$ exists satisfying $\alpha\beta = 0$.

We call an ideal A of an integral domain R a **principal** ideal if it is generated by a single element $r \in R$. That is, A is principle if $A = rR$ for some $r \in R$. If every ideal of R is principal, we say R is a **principal ideal domain**.

We say that an integral domain R is a **unique factorization domain** if every nonzero unit $r \in R$ may be written as a product of irreducibles. Recall that an **irreducible** is a nonunit element $\alpha \in R$ such that if $\alpha = \beta\gamma$, where $\beta, \gamma \in R$, then either β or γ is a unit. We note that while every principal ideal domain is a unique factorization domain, the converse is not true.

We now remind the reader of two useful facts:

Given a ring R and an ideal A of R,

1. R/A is an integral domain $\iff$ A is prime,

2. R/A is a field $\iff$ A is maximal.

2.3 Modules

Recall that a **module** M over a ring R is a generalization of a vector space. That is, M is an additive abelian group with a mapping $R \times M \to M$ such that the following hold for $r_1, r_2 \in R$ and $m_1, m_2 \in M$:

1. $r_1(m_1 + m_2) = r_1m_1 + r_1m_2$,

2. $(r_1 + r_2)m_1 = r_1m_1 + r_2m_2$,

3. $r_1(r_2m_1) = (r_1r_2)m_1$,

4. $1m_1 = m_1$.

We say that M has a **base** if there exists a set $\{x_1, \ldots, x_n\}$ of elements of M such that each $m \in M$ may be written as a unique R-linear combination of the x_i (for $1 \leq i \leq n$). In this case we say that M is **free**, and the cardinality of the base is called the **rank** of M. Moreover, we say that a module M is of **finite type** if there exists a finite set which generates M.

2.4 Algebraic and Integral Numbers

Given a ring R and a subring K of R, we call an element $\alpha \in R$ **algebraic** over K if α is a root of a polynomial (not necessarily monic) with coefficients in K. We define the **minimal polynomial of** α over K to be the polynomial of lowest degree in $K[x]$ having α as a root, and denote it by Irr_α, to signify that it is an irreducible polynomial, as can easily be seen. If no such polynomial exists, we say α is **transcendental** over K. In addition, if every element of the ring R is algebraic over K, we say that R is **algebraic** over K.

Now, if α satisfies a *monic* polynomial with coefficients in K, we say α is **integral** over K. Thus, if K is a subfield of R, a number α algebraic over K is necessarily integral over K. (This follows from the fact that, in a field, all nonzero elements are units). Moreover, if R is a field containing a subfield K, such that R is algebraic over K, we call R an **algebraic extension** of K.

A basic result of algebraic number theory is that, given a field R and a subfield K, if the **degree** of R over K is finite, then R is an algebraic extension of K.

2.5 Conjugates

Given a ring R and a subring K of R, we say two algebraic elements $\alpha, \alpha' \in R$ are **conjugate** over K if their minimal polynomials coincide.

Now, suppose $\alpha \in \mathbb{Q}^{\mathrm{alg}}$, where $\mathbb{Q}^{\mathrm{alg}}$ is the set of algebraic numbers in $\mathbb{C}$. Let

$$\mathrm{Conj}_\alpha = \{\alpha' \in \mathbb{C} \mid \alpha' \text{ is a conjugate of } \alpha\}.$$

We may interpret Conj_α as the set of all the roots of the minimal polynomial of α over $\mathbb{Q}$. That is,

$$\mathrm{Irr}_\alpha(x) = \prod_{\mathrm{Conj}_\alpha} (x - \alpha').$$

2.6 Integral Closure

Given a ring R and a subring A of R, we define the **integral closure of** A **in** R to be the set A' of elements of R which are integral over A. It can be shown that A' is in fact a subring of R which contains A. Also, if every element of R is integral over A, we say R is **integral** over A.

Moreover, if A is an integral domain, and K its field of fractions, the integral closure of A in K is called the **integral closure** of A. If A is its own integral closure, we say that it is **integrally closed**. That is, if every element $x \in K$ which is integral over A is also in A, we say A is integrally closed.

2.7 Number Fields

Now, a **number field** K is simply an extension of finite degree over $\mathbb{Q}$. Note that, as its degree is finite, a number field is necessarily an algebraic extension of $\mathbb{Q}$. In fact, if we take any algebraic number α, we may generate a number field, denoted $\mathbb{Q}(\alpha)$, by taking the set of all expressions resulting from repeated multiplication, division, addition, and subtraction of α to itself.

Let us note that we may also construct a degree n number field by choosing an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree n, and 'finding' an α whose minimal polynomial is f. We do so in the following way: Take the ideal $I = (f) = f\mathbb{Q}[x]$ generated by f. One may show that I is a maximal ideal of $\mathbb{Q}[x]$. (This follows from the fact that $\mathbb{Q}[x]$ is a principal ideal domain). Now, since (f) is maximal, the quotient ring $\mathbb{Q}[x]/(f)$ is a field. Consider the natural maps $\mathbb{Q} \hookrightarrow \mathbb{Q}[x] \twoheadrightarrow \mathbb{Q}/(f)$ such that $a \mapsto a + I$. We can consider $\mathbb{Q}$ as a subfield of $\mathbb{Q}/(f)$ (with some abuse of language), and we note that in $\mathbb{Q}/(f)$ we have a root of f: $x + I$. (We have $f(x + I) = f(x) + I = I$). Letting $\alpha = x + I$, we have constructed the number field $\mathbb{Q}[x]/(f) = \mathbb{Q}(\alpha)$.

A perhaps more concrete definition of a number field is as a subfield of $\mathbb{C}$ of finite degree over $\mathbb{Q}$. We note that, by the Fundamental Theorem of Algebra, every finite extension of $\mathbb{Q}$ is in fact isomorphic to a subfield of $\mathbb{C}$ having finite degree over $\mathbb{Q}$.

2.8 Ring of Algebraic Integers

Just as arithmetic operations with elements of $\mathbb{Q}$ may be viewed as ratios of elements of the discrete ring $\mathbb{Z}$, we would like to identify a discrete subring of K such that every element of K may be viewed as a ratio of elements of this subring.

To do so, we introduce the concept an algebraic integer. We define an **algebraic integer** of K to be an element $x \in K$ such that x is the root of a monic polynomial with coefficients in $\mathbb{Z}$, i.e. x is integral over $\mathbb{Z}$.

For the remainder of this paper, we use the notation

$$\mathcal{O}_K = \{\alpha \in K | \, \alpha \text{ is an algebraic integer}\}.$$

The set $\mathcal{O}_K$ forms a (discrete) subring so long as K is an algebraic number field, and we call this set the **ring of algebraic integers** of K. We note that $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

We have the following standard properties of $\mathcal{O}_K$.

1. Just as for $\mathbb{Z}$, every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

2. Every ideal I of $\mathcal{O}_K$ has a unique expression as a product of prime ideals.

3. We have that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

Now we shall define a norm function on the nonzero ideals and elements of $\mathcal{O}_K$, which is possible since for any nonzero ideal I of $\mathcal{O}_K$, $\mathcal{O}_K/I$ is finite.

Definition 6 Let I be a nonzero ideal of $\mathcal{O}_K$. Then we define the **norm of the ideal** I, $\|I\|$, as follows.

$$\|I\| = |\mathcal{O}_K/I|.$$

Definition 7 Let $x \in \mathcal{O}_K$ nonzero. Then we define the **norm of the element** x, $\|x\|$, to be the norm of the ideal generated by x. That is,

$$\|x\| = \|(x)\|.$$

Further, if $x = 0$, we say $\|0\| = 0$.

Suppose K is a number field, with I an ideal of $\mathcal{O}_K$. A standard fact is that, if $x \in I$, then $\|I\|$ divides $\|x\|$.

2.9 Representing Algebraic Numbers as Matrices

Consider a number field $\mathbb{Q}(\alpha)$ with degree n. We may think of $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$, and hence fix a basis $\mathcal{B} = [1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$. Now, for any $\gamma \in \mathbb{Q}(\alpha)$, we may define the linear map $L_\alpha : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$, where $\gamma \mapsto \alpha\gamma$. Further, as this transformation is linear, we may represent this "left-multiplication by α" as some matrix $M_{\alpha,\mathcal{B}}$ (dependent on our choice of a basis).

In this way, we have created a tangible model for α in a commutative subset of $M_n(\mathbb{Q}(\alpha))$ (the set of $n \times n$ matrices over $\mathbb{Q}(\alpha)$). We will see that we can use $M_{\alpha,\mathcal{B}}$, among other things, to calculate the minimal polynomial of α, as well as the norm and trace of α.

First, we note that we may find the minimal polynomial of α by calculating the characteristic polynomial of $M_{\alpha,\mathcal{B}}$. If the resulting polynomial is irreducible, we have found the minimal polynomial. Otherwise we may write the characteristic polynomial as a product of irreducibles, and check which factor has α as a root.

We are now ready for the following definitions:

Definition 8 Given $\mathbb{Q}(\alpha)$ with fixed basis $\mathcal{B}$ as above, the **norm** of α from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}$ with respect to $\mathcal{B}$ is

$$\mathbb{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}} = \det(M_\alpha).$$

Definition 9 Given $\mathbb{Q}(\alpha)$ with fixed basis $\mathcal{B}$ as above, the **trace** of α from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}$ with respect to $\mathcal{B}$ is

$$\mathrm{tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}} = \mathrm{trace}(M_\alpha).$$

From basic linear algebra, we know that $\mathbb{N}_{(\mathbb{Q}(\alpha)/\mathbb{Q}}$ and $\mathrm{tr}_{(\mathbb{Q}(\alpha)/\mathbb{Q}}$ do not depend on the choice of basis $\mathcal{B}$. If $\mathcal{B}'$ is a different basis for $K/\mathbb{Q}$, then $M_{\alpha,\mathcal{B}'} = AM_{\alpha,\mathcal{B}}A^{-1}$ for some invertible A.

2.10 Embedding Number Fields into $\mathbb{C}$

Let $\mathbb{Q}(\alpha)$ be a number field of degree n. In contrast to the previous approach of embedding $\mathbb{Q}(\alpha)$ in a noncommutative ring, we can embed $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ in numerous ways. For a number field of degree n, we have n distinct embeddings into $\mathbb{C}$. We shall now describe these embeddings.

Let $f(x) = \mathrm{Irr}_\alpha(x) \in \mathbb{Q}[x]$, and recall that

$$f(x) = \prod_{i=1}^{n}(x - \alpha^{(i)}),$$

where $\alpha^{(i)} \in \mathrm{Conj}_\alpha$.

Define

$$\sigma_i : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C},$$

where

$$g(\alpha) \mapsto g(\alpha^{(i)}) \text{ for } g \in \mathbb{Q}[x].$$

Further suppose that r_1 of the n embeddings are from $K \hookrightarrow \mathbb{R}$, leaving $n - r_1$ nonreal embeddings from $K \hookrightarrow \mathbb{C}$. Note that the complex embeddings come in complex conjugate pairs, and suppose we have $r_2 = \frac{n-r_1}{2}$ such pairs. We call (r_1, r_2) the **signature** of K.

With this approach, we have the following alternative definitions for norm and trace:

Definition 10 Let K be a number field of degree n, and let $\sigma_1, \ldots, \sigma_n$ denote the n distinct embeddings of K into $\mathbb{C}$. Suppose $\alpha \in K$ and suppose $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$.

We define the **trace** of α from K to $\mathbb{Q}$ as

$$\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) = \frac{n}{d}\,\mathrm{tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha).$$

We define the **norm** of α from K to $\mathbb{Q}$ as

$$\mathbb{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \mathbb{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)^{\frac{n}{d}}.$$

Moreover, $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = -a_{n-1}$ and $\mathbb{N}_{K/\mathbb{Q}}(\alpha) = (-1)^n a_0$, where the characteristic polynomial of α is $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0$.

2.11 Absolute Values on Fields

Let us the introduce the concept of an **absolute value**.

Definition 11 Let K be a field. We say that a function

$$|\ | : K \to \mathbb{R}_{\geq 0}$$

is an **absolute value** if the following hold $\forall x, y \in K$:

1. $|x| = 0 \iff x = 0$,

2. $|xy| = |x||y|$,

3. $|x + y| \leq |x| + |y|$.

Definition 12 An absolute value $|\ |$ which satisfies $|x+y| \leq \max\{|x|, |y|\}$, $\forall x, y \in K$ is called **ultrametric** or **non-archimedean**. Otherwise, we say $|\ |$ is **archimedean**.

Definition 13 Two absolute values on K, $|\ |_1$ and $|\ |_2$, are **equivalent** if there exists $c \in \mathbb{R}_{>0}$ such that $|x|_1 = |x|_2^c \ \forall x \in K$.

Moreover, if v_1 and v_2 are equivalent absolute values on K, either v_1 and v_2 are both archimedean, or both non-archimedean. We call an equivalence class of absolute values of K a **place** of K. For a number field K, we define the **finite places** of K to be the *non-archimedean* places of K. In fact, these correspond to the nonzero prime ideals of $\mathcal{O}_K$. The correspondence is as follows. Suppose $\wp \subset \mathcal{O}_K$ is a prime ideal, and $x \in K$ is nonzero. Then there is a well defined integer $n \geq 0$ such that $\wp^n | (x)$ but $\wp^{n+1} \nmid (x)$. We define

$$|x|_\wp = \mathbb{N}_{K/\mathbb{Q}}(\wp)^{-n}.$$

Alternatively, we may define $|\lambda|_{\wp_i} = \mathbb{N}_{K/\mathbb{Q}}(\wp_i)^{-m_i}$ for $\lambda \in \mathcal{O}_K$, where $\lambda = \prod_{i=1}^{r} \wp_i^{m_i}$, where $r \in \mathbb{Z}_{>0}$ and $m_i \in \mathbb{Z}\ \forall 1 \leq i \leq r$. Writing $x = \frac{\alpha}{\beta}$, where $\alpha, \beta \in \mathcal{O}_K$, we have

$$|x|_{\wp} = \frac{|\alpha|_{\wp}}{|\beta|_{\wp}}.$$

We define the **infinite places** of K to be the *archimedean* places of K. If K has signature (r_1, r_2), then K has exactly $(r_1 + r_2)$ infinite places. Suppose $\sigma_1, \ldots, \sigma_{r_1}$ are the real embeddings of K into $\mathbb{C}$, and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_{r_1}$ denote the r_1 infinite places of K. Then these r_1 infinite places are given by the following valuations:

$$|x|_{\mathfrak{q}_i} = |\sigma_i(x)|, \text{ where } 1 \leq i \leq r_1.$$

Similarly, let $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ be nonreal embeddings of K into $\mathbb{C}$, such that the σ_{r_1+j} are pairwise non-conjugate, and let $\mathfrak{q}_{r_1+1}, \ldots, \mathfrak{q}_{r_1+r_2}$ denote the r_2 infinite places of K. Then these r_2 infinite places are given by the following valuations:

$$|x|_{\mathfrak{q}_{r_1+j}} = |\sigma_{r_1+j}(x)|^2, \text{ where } 1 \leq j \leq r_2.$$

2.12 The Discriminant and Root Discriminant

We now turn to the discriminant of a polynomial and number field.

Definition 14 Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x^1 + a_0 \in \mathbb{Q}[x]$, and let $(x - \alpha_1) \cdots (x - \alpha_n)$ be its linear factorization over $\mathbb{C}$. The **discriminant of** f is as follows:

$$\operatorname{disc}(f) = \prod_{1 \leq i \leq j \leq n} (\alpha_i - \alpha_j)^2.$$

In analyzing the discriminant of a polynomial f, we first note that $\operatorname{disc}(f) \in \mathbb{Z}$. We also note that $\operatorname{disc}(f) = 0$ whenever f has a root of multiplicity greater than one. This motivates the idea of a **prime divisor** of $\operatorname{disc}(f)$, a prime p for which two distinct roots of f, once reduced modulo p, are congruent. This will become useful in discussing *ramification*, but for now, let us introduce the discriminant of a number field.

Definition 15 Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, and $\mathcal{O}_K$ its ring of integers. The **discriminant of** K is as follows:

$$\operatorname{disc}_K = \mathrm{d}_K = \operatorname{disc}(\mathcal{O}_K) = \det(\operatorname{tr}(\omega_i\omega_j)),$$

where $\mathcal{O}_K = [\omega_1, \omega_2, \ldots, \omega_n]_{\mathbb{Z}}$.

Let us clarify the above definition. Let K and $\mathcal{O}_K$ be as above. Let $\omega \in \mathcal{O}_K$, and let f_ω be the characteristic polynomial of ω. We have $f_\omega =$

$x^n - \mathrm{tr}(\omega)x^{n-1} + \ldots + (-1)^n\mathbb{N}(\omega)$. In addition, we may calculate the trace of ω as $\mathrm{tr}(\omega) = \omega^{(1)} + \omega^{(2)} + \ldots + \omega^{(n)}$, where $\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)} \in \mathrm{Conj}_\omega$.

We are now ready for the following theorem.

Theorem 4 *Let $K = \mathbb{Q}(\alpha)$, where α is an algebraic integer, and $f = \mathrm{Irr}_\alpha$. Then $\mathrm{d}_K = \frac{\mathrm{disc}(f)}{g^2}$, for some $g \in \mathbb{Z}_{\geq 1}$ and $[1, \alpha, \alpha^2, \ldots, \alpha^n]_\mathbb{Z}$ is a subring of $\mathcal{O}_K$ of index g.*

We shall also find the concept of a root discriminant useful.

Definition 16 Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n. The **root discriminant** of K, denoted rd_K, is $|\,\mathrm{d}_K\,|^{1/n}$.

A standard fact is that if L/K is an extension of number fields, then $\mathrm{rd}_L \geq \mathrm{rd}_K$. We shall see the case in which we have equality shortly.

The discriminant of a quadratic field is particularly easy to calculate. A **quadratic field** is a field extension of degree 2 over $\mathbb{Q}$. That is, a quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for some nonzero square-free $d \in \mathbb{Q}$. If $d < 0$, the we say that $\mathbb{Q}(\sqrt{d})$ is an **imaginary** quadratic field. If $d > 0$, we say that $\mathbb{Q}(\sqrt{d})$ is a **real** quadratic field. In this case, we have:

$$\mathrm{disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{otherwise.} \end{cases}$$

2.13 Galois Groups

Definition 17 Suppose K is a finite extension of a field L. Consider the set $\mathrm{Aut}_L(K)$, the group of field automorphisms α of K such that $\alpha(x) = x\ \forall x \in L$. If $|\,\mathrm{Aut}_L(K)| = [K : L]$, we say that K/L is a **Galois extension** with **Galois group** $\mathrm{Gal}(K/L) := \mathrm{Aut}_L(K)$.

Moreover, for any finite extension K/L, the intersection of all fields M/K with the property that M/L is Galois is a field J, itself Galois over L, called the **Galois closure** of K/L.

To clarify this definition, let us consider some examples. If we take $K = L$. Then the $\mathrm{Gal}(K/L)$ is the trivial group, containing only the identity automorphism. If we take the extension $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$, then the Galois group contains the identity automorphism, and the automorphism which exchanges $\sqrt{5}$ and $-\sqrt{5}$.

Now, suppose $L = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt[3]{2})$. Then $\mathrm{Aut}_L(K) = \{1\}$, because the conjugates of $\sqrt[3]{2}$, namely $e^{\frac{2\pi i}{3}}\sqrt[3]{2}$ and $e^{\frac{4\pi i}{3}}\sqrt[3]{2}$, are not real numbers. Thus, K/L is not a Galois extension. The Galois closure in this case is $J = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$.

2.14 Behavior of Primes

While number rings are not necessarily unique factorization domains, we do have that nonzero ideals in a number ring factor uniquely into a product of prime ideals.

Now, let K/k be a finite extension of a number field k of degree n, with $\mathcal{O}_K$ its ring of integers. Let $\wp$ be a prime ideal of $\mathcal{O}_k$, and suppose

$$\wp\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_l^{e_l}, \text{ where } \mathfrak{p}_i \text{ for } 1 \leq i \leq l \text{ are distinct prime ideals of } \mathcal{O}_K.$$

We say that $\mathfrak{p}_i$, for $1 \leq i \leq l$, are the prime ideals that **lie above** $\wp$ in $\mathcal{O}_K$. Moreover, we call $e_i = e(\mathfrak{p}_i|\wp)$ the **ramification index** of $\mathfrak{p}_i$. If there exists $e_i > 1$, we say that the prime ideal $\wp$ is **ramified** in K/k; otherwise we say $\wp$ is **unramified** in K/k.

Moreover, if $l = 1$ and $e_1 = 1$, we say the prime ideal $\wp$ is **inert** in K/k. That is, a prime ideal $\wp$ is inert in K/k if it remains prime. If $l > 1$, we say $\wp$ is **split** in K/k.

The following are standard results of algebraic number theory.

Theorem 5 *Let K/k be as above. A prime ideal $\wp \in \mathcal{O}_k$ ramifies in K/k $\iff$ $\wp | \operatorname{d}_{K/k}$.*

Theorem 6 *Let L/K be an extension of number fields. Then $\operatorname{rd}_L = \operatorname{rd}_K$ $\iff$ L/K is unramified for every prime in K.*

Now, remembering that every nonzero prime ideal in $\mathcal{O}_K$ is maximal, note that each $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field of characteristic p, where $\wp$ lies over $p \in \mathbb{Q}$. (Note that $\wp \cap \mathbb{Z} = p\mathbb{Z}$). Thus, it is a finite extension of $\mathbb{Z}/(\wp)$. We say the **residual degree**, $f_i = f(\mathfrak{p}_i|\wp)$, of $\mathfrak{p}_i$ lying over $\wp$ is the degree of the field extension $[\mathcal{O}_K/\mathfrak{p}_i : \mathcal{O}_k/(\wp)]$. Equivalently we note that $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field of size $\mathbb{N}_{k/\mathbb{Q}}\wp^{f(\mathfrak{p}_i|\wp)}$.

Recall that the degree of K/k is n. We may relate the ramification indices and residual degrees in the following way:

$$\sum_{i=1}^{l} e_i f_i = n.$$

Furthermore, we say that the prime $\wp$ **splits completely** if $e_i = f_i = 1\,\forall i$.

Now, suppose K/k is Galois. Then $e_1 = e_2 = \cdots = e_l$, and we shall call this quantity e. Similary, $f_1 = f_2 = \cdots = f_l$, and we call this quantity f. We then have $efl = n$. We say $\wp$ is **totally ramified** if $e = n$ and $f = l = 1$, **inert** if $e = l = 1$ and $f = n$, **split completely** if $e = f = 1$ and $l = n$.

For a quadratic extension $K = \mathbb{Q}(\sqrt{d})$, we may use the concept of quadratic residues to determine whether a prime p splits in K. In fact, if d is a quadratic residue modulo p, then p splits completely in K. Recall that $d \in \mathbb{Z}$ is a **quadratic residue** modulo p if $d \equiv x^2 \pmod{p}$ for some $0 < x < p$. Moreover, d is a quadratic residue if and only if the **Legendre symbol**, $\left(\frac{d}{p}\right)$, is 1. In general, we have $\left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \pmod{p}$.

3 Infinite Class Field Towers

In this chapter we review the basic elements of class field theory, which shall be necessary for our code construction.

3.1 Class Groups and Class Number

Let K be a number field, and $\mathcal{O}_K$ be its ring of integers. We shall now introduce the notion of a class group. Essentially, a class group is a finite Abelian group which measures how far $\mathcal{O}_K$ is from being a principal ideal domain.

First, we need to define a fractional ideal. A **fractional** ideal is a subset of K of the form $a^{-1}\mathfrak{i}$, where $a \neq 0 \in \mathcal{O}_K$ and $\mathfrak{i}$ is an ideal of $\mathcal{O}_K$. It is clear how to multiply two fractional ideals: $a^{-1}\mathfrak{i} \cdot b^{-1}\mathfrak{j} = (ab)^{-1}\mathfrak{ij}$.

Let us now give a formal definition.

Definition 18 Let I_K be the group of fractional ideals of $\mathcal{O}_K$, and let P_K be the subgroup of principal ideals of $\mathcal{O}_K$. Then the **class group** of K, denoted $\mathrm{Cl}(K)$, is as follows:

$$\mathrm{Cl}(K) = I_K/P_K.$$

We shall also need to understand the S class group, where S is a finite set of primes of $\mathcal{O}_K$.

Definition 19 Let K be a number field, and S be a finite set of primes of $\mathcal{O}_K$. Let us denote the subgroup of $\mathcal{O}_K$ generated by S by $\langle S \rangle$. We define the S **class group** of K, $\mathrm{Cl}_{K,S}$, in the following manner.

$$\mathrm{Cl}_{K,S} = \mathrm{Cl}_K / \langle S \rangle,$$

i.e. $\mathrm{Cl}_{K,S}$ is the group of ideal classes generated by all the prime ideals of $\mathcal{O}_K$ different from those in S.

Note that for a number field K, $\mathrm{Cl}(K) = \{1\}$ if and only if K is a principal ideal domain, and $\mathrm{Cl}_{K,S} = \{1\}$ if and only if every ideal of $\mathcal{O}_K$ is a principal ideal times a product of elements of S.

Moreover, a fundamental result says that $\mathrm{Cl}(K)$ is finite ([Sam], [Mar]). We call the $|\mathrm{Cl}(K)|$, the order of the $\mathrm{Cl}(K)$, the **class number** of K.

In addition we shall need to speak of the p**-rank** of the class group of K, and the S class group of K. Recall that by the Fundamental Theorem of Abelian Groups, if G is an abelian group, $G \simeq \mathbb{Z}^r \times \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_k\mathbb{Z}$, where $m_i \in \mathbb{Z} \, \forall 1 \leq i \leq k$. We define the $p\text{-rk}\, G = r + |\{1 \leq i \leq k : p|m_i\}|$.

Genus theory gives us the following threshold on the 2-rank of the class group of a number field K, and may be found in any reference on class groups or class field theory, such as [S].

Theorem 7 (Genus Theory) *Let K be a quadratic number field, i.e. $[K : \mathbb{Q}] = 2$. Let Q be the set of primes such that $q \in Q \iff q | \mathrm{d}_K$, and suppose $|Q| = r$. Then the 2-rk$\mathrm{Cl}_K \geq r - 2$. If K is imaginary, i.e. $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$, then 2-rk$\mathrm{Cl}_K = r - 1$.*

3.2 Hilbert Class Fields

In this section we shall introduce the notion of Hilbert Class Fields, but before we do so, let us define the following.

Definition 20 Let K/k be an extension of number fields. We say K/k is

1. **unramified** if every prime ideal of k is unramified in K/k,

2. **abelian** if K/k is Galois with abelian Galois group,

3. a p**-extension** if K/k is Galois with $[K : k] = p^n$ for some integer n and prime p.

Definition 21 Let K be a number field. The **Hilbert Class Field** of K, denoted $HCF(K)$, is an extension of K which satisfies the following properties:

1. HCF(K) is Galois over K

2. Gal$(HCF(K)/K)$ is abelian

3. HCF$(K)/K$ is unramified

4. HCF(K) is maximal with respect to the above properties

Let H be the Hilbert Class Field of a number field K. By a famous theorem called the Artin Reciprocity Law, there is a canonical isomorphism from Gal(H/K) to Cl(K). Thus, the degree of H over K is equal to the class number of K. That is, $[H : K] = |\,\mathrm{Cl}(K)|$. Moreover, $H = K$ exactly when $\mathrm{Cl}(K) = \{1\}$. In addition, a prime ideal $\wp$ of K splits completely in H if and only if $\wp$ is principal in K.

Also, H contains all other unramified abelian extensions of K, Gal$(H/K) \cong$ Cl(K) and each subgroup G of Gal(H/K) is isomorphic to Gal(H/H'), where H' is a unique unramified abelian extension of K.

We shall also need the notion of a **Hilbert p-class field**.

Definition 22 Let K be a number field. The **Hilbert p-class field** is the maximal p-extension of K contained in $\mathrm{HCF}(K)$.

3.3 Class Field Towers

We may use Hilbert Class Fields in the construction of **class field towers**, which will become useful later. The formal definition follows.

Definition 23 Let K_0 be a field. The **class field tower** of K_0 is the sequence of field extensions $K_1, K_2, \ldots, K_i, \ldots$ of K_0 where

$$\begin{aligned} K_1 &= HCF(K) \\ K_2 &= HCF(K) \\ &\vdots \\ K_i &= HCF(K_{i-1}) \\ &\vdots \end{aligned}$$

Hence we see that the sequence $K_1, K_2, \ldots, K_i, \ldots$ stabilizes when some K_i has trivial class group. That is, $K_i = K_{i-1}\ \forall i \geq n$ if there exists K_n such that $\mathrm{Cl}(K_n) = \{1\}$.

Class field towers also have a useful property relating to root discriminants. Namely, if $\mathrm{rd}(K_0) = r$, then $\mathrm{rd}(K_i) = r\ \forall i$. That is, the root discriminant remains constant all the way up the tower.

The **p-class field tower** is defined similarly, where each term K_i of the sequence $K_1, K_2, \ldots, K_i, \ldots$ is the p-Hilbert class field of K_{i-1}.

In fact, there exist *infinite* class field towers, a result shown by Golod and Shafarevich. In the next few sections, we will see how such infinite towers may be constructed.

3.4 Class Field Towers with Primes Splitting

For our purposes, we shall need to understand a modified version of p-class field towers, in which a set of primes split completely up the tower.

Definition 24 Let K be a number field, and $T \subset \mathcal{O}_K$ be a set of prime ideals. The p-class field of K in which every prime in T splits completely is called the **T-decomposing p- class field** of K, denoted K_p^T.

Definition 25 Let K_0 be a number field and $T \subset \mathcal{O}_{K_0}$ a set of prime ideals. The **T-decomposing p-class field tower** of K_0 is the sequence of

field extensions $K_1, K_2, \ldots, K_i, \ldots$ of K_0 where

$$\begin{aligned} K_1 &= (K_0)p^T \\ K_2 &= (K_1)_p^T \\ &\vdots \\ K_i &= (K_{i-1})_p^T \\ &\vdots \end{aligned}$$

3.5 Golod-Shafarevich Theory

Golod and Shafarevich showed that there exist number fields K with infinite class field towers. The criteria for the existence of such towers is based on lower thresholds on the p-rank of $\mathrm{Cl}(K)$.

Theorem 8 *([FM]) Let K be a number field with signature (r_1, r_2), and $p \in \mathbb{Z}$ be prime. Suppose*

$$p\text{-rk}\mathrm{Cl}(K) \geq 2 + 2\sqrt{r_1 + r_2 + 1}.$$

Then the p-class field tower of K is infinite.

The following modified version of the Golod-Shafarevich Criterion, involving T- decomposing 2-class fields in which a given set of primes split completely, may be found in [Mai]

Theorem 9 *Let K be a number field with signature (r_1, r_2) and T be a finite set of primes of $\mathcal{O}_K$. Suppose*

$$2\text{-}rk\ Cl_{K,T} \geq 2 + 2\sqrt{r_1 + r_2 + |T| + 1}.$$

Then the T-decomposing class field tower of K is infinite.

For our purposes, the following constrained version of Golod-Shafarevich, which is applicable for imaginary quadratic extensions, will suffice.

Theorem 10 *([Guru]) Let P and Q be nonempty disjoint sets of primes. Suppose $K/\mathbb{Q}$ is an imaginary quadratic extension such that K is ramified at a prime $q \iff q \in Q$. Now, let T be the set of all prime ideals of $\mathcal{O}_K$ that lie above the primes in P. If*

$$|Q| \geq 3 + |T| - |P| + 2\sqrt{2 + |T|},$$

then K has an infinite T-decomposing 2-class field tower.

Proof

Suppose $P = \{p_1, \ldots, p_s\}$. Since Q contains all primes at which K is ramified, and $P \cap Q = \emptyset$, we know P contains only primes which are inert or split.

Let $P_{\text{split}} = \{p \in P |\, p \text{ splits in } K/\mathbb{Q}\}$, and $P_{\text{inert}} = \{p \in P |\, p \text{ is inert in } K/\mathbb{Q}\}$.

Further suppose that $|P_{\text{split}}| = a$, from which it follows that $|P_{\text{inert}}| = s - a$.

Thus T will have the form

$$T = \{\underbrace{\wp_1, \overline{\wp_1}, \ldots, \wp_a, \overline{\wp_a}}_{2a}, \underbrace{\wp_{a+1}, \ldots, \wp_s}_{s-a}\},$$

where $\wp_i$ and $\overline{\wp_i}$, for $1 \leq i \leq a$ are the $2a$ prime ideals in T lying above the a primes in P_{split} and $\wp_i$, for $a+1 \leq i \leq s$ are the $s-a$ primes ideals which lie above the $s-a$ primes in P_{inert}.

Now, inert primes are clearly principal, and for a split prime $\wp$ we have $(\wp) = \wp\overline{\wp} \Rightarrow \overline{\wp} = \wp^{-1}(\wp) \Rightarrow [\overline{\wp}] = [\wp]^{-1}$, so $\wp$ and $\overline{\wp}$ generate the same cyclic subgroup. That is, $\langle T \rangle = \langle \{\wp_1, \ldots, \wp_a\} \rangle$.

Thus, if the $|T| = t$, we have $s - a + 2a = t \Rightarrow a = t - s$, and an upper threshold on the 2-rk of the subgroup generated by T is a.

We have $2\text{-rkCl}_{K,T} \geq 2\text{-rkCl}_K - a$. From genus theory (Theorem 7), we know $2\text{-rkCl}_K \geq |Q| - 1$. Thus, we have

$$\begin{aligned} 2\text{-rkCl}_{K,T} &\geq 2\text{-rkCl}_K - a \\ &\geq |Q| - 1 - a. \end{aligned}$$

Further, note the signature of an imaginary quadratic field is $(r_1, r_2) = (0, 1)$.

Now, we have

$$\begin{aligned} & |Q| \geq 3 + |T| - |P| + 2\sqrt{|T| + 2} \\ \iff \quad & |Q| \geq 3 + t - s + 2\sqrt{t + 2} \\ \iff \quad & |Q| \geq 1 + t - s + 2 + 2\sqrt{0 + 1 + t + 1} \\ \iff \quad & |Q| \geq 1 + a + 2 + 2\sqrt{r_1 + r_2 + t + 1} \\ \iff \quad & |Q| - 1 - a \geq 2 + 2\sqrt{r_1 + r_2 + t + 1} \end{aligned}$$

As $2\text{-rkCl}_{K,T} \geq |Q| - 1 - a$, we have satisfied the constrained Golod-Shafarevich criterion of Theorem 9. Thus, K has an infinite T-decomposing 2-class field tower.

■

4 Code Construction

We are now ready to summarize Guruswami's Code Construction ([Guru]). We shall first establish the general form of the code, and then provide the constraints on the given parameters.

The basic idea of the code construction is as follows. Suppose K is a number field of degree m and signature (r_1, r_2). Let $\mathfrak{p}_1, \ldots \mathfrak{p}_n$ be nonzero prime ideals of $\mathcal{O}_K$, such that $\|\mathfrak{p}_1\| \leq \|\mathfrak{p}_2\| \cdots \leq \|\mathfrak{p}_n\|$. We will take our message set to be those elements of $\mathcal{O}_K$ which are bounded in "size" by a positive constant B, which will be dependent on rd_K.

There exists a good notion of **size** of the elements of $\mathcal{O}_K$ using a "shift parameter" $\mathbf{z}$, a slight technical modification of adding the absolute values of the embeddings of K into $\mathbb{C}$. We take our message set to be all the elements of $\mathcal{O}_K$ with size bounded by a particular constant B, which is chosen to guarantee a one-to-one encoding function with particular minimum distance. More technically, we will take our message set of the code to be $\{x \in \mathcal{O}_K | \, \mathrm{size}_z(x) \leq B\}$.

Taking the block length of the code to be n, we encode a message $x \in \mathcal{O}_K$ by the encoding function

$$E : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{p}_n,$$
$$\text{where } x \mapsto (x/\mathfrak{p}_1, \ldots, x/\mathfrak{p}_n).$$

Here, $x/\mathfrak{p}_i$ is shorthand for $x + \mathfrak{p}_i \in \mathcal{O}_K/\mathfrak{p}_i$, for $1 \leq i \leq n$.

We shall call such a code a **number field code**, and denote it by $\mathcal{C}_K$. We say that $\mathcal{C}_K$ has parameters $(n, \mathfrak{p}_1, \ldots, \mathfrak{p}_n; B; z)$. We consider the number of elements in our alphabet to be $\|\mathfrak{p}_n\|$, as $\mathfrak{p}_n$ is the ideal of largest norm.

4.1 Notion of Size

We shall now make the notion of size more precise.

Let K be a number field of degree m with signature (r_1, r_2). Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_{r_1+r_2}$ denote the $(r_1 + r_2)$ infinite places of K. Further, let $|\,|_{\mathfrak{q}_1}, |\,|_{\mathfrak{q}_2}, \ldots, |\,|_{\mathfrak{q}_{r_1}}$ be the archimedean absolute values corresponding to the r_1 real embeddings of K into $\mathbb{C}$, and $|\,|_{\mathfrak{q}_{r_1+1}}, \ldots, |\,|_{\mathfrak{q}_{r_1+r_2}}$ be the archimedean absolute values corresponding to the r_2 complex embeddings of K into $\mathbb{C}$. We define the **size** of x to be

$$\mathrm{size}(x) = \sum_{i=1}^{r_1} |x|_{\mathfrak{q}_i} + \sum_{j=1}^{r_2} 2\sqrt{|x|_{\mathfrak{q}_{r_1+j}}}.$$

This definition of size has the following properties, which are shown in [Guru].

1. If $x_1, x_2 \in \mathcal{O}_K$, then $\text{size}(x_1 - x_2) \leq \text{size}(x_1) + \text{size}(x_2)$,

2. If $x \in \mathcal{O}_K$, then $\|x\| \leq \left(\frac{\text{size}(x)}{m}\right)^m$.

   From the above properties we obtain:

3. If $x_1, x_2 \in \mathcal{O}_K$, where $\text{size}(x_1) \leq B$ and $\text{size}(x_2) \leq B$, then $\|x_1 - x_2\| \leq \left(\frac{2B}{m}\right)^m$.

Now, when we talk about a "shift" parameter of size, we simply mean that we are adjusting the absolute value by some constant. For example, if we have the absolute value $|\sqrt{3} + \sqrt{-5}|$, and we wish to shift by 1, we take $|\sqrt{3} + \sqrt{-5} - 1|$. Now, take $x \in \mathcal{O}_K$ as above, and take the shift parameter $z \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Then the i^{th} component of z is simply the constant by which we are shifting $|x|_{\mathfrak{q}_i}$. That is, we are shifting the archimedean absolute values by z. A formal definition of this size modification follows.

Definition 26 Let K be as above, where $\sigma_1, \ldots \sigma_{r_1}$ denote the real embeddings of K into $\mathbb{C}$, and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ denote the nonreal embeddings of K into $\mathbb{C}$. Let $z \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

1. We define the **real shifted absolute value**, $a_i^{(x)}$, to be

$$a_i^{(x)} = |\sigma_i(x) - z_i| \text{ where } 1 \leq i \leq r_1.$$

2. We define the **nonreal shifted absolute value**, $b_j^{(x)}$, to be

$$b_j^{(x)} = |\sigma_{r_1+j}(x) - z_{r_1+j}|^2 \text{ where } 1 \leq j \leq r_2.$$

3. We define the **size shifted by** z, $\text{size}_z(x)$, to be

$$\text{size}_z(x) = \sum_{i=1}^{r_1} a_i^{(x)} + \sum_{j=1}^{r_2} 2\sqrt{b_j^{(x)}}.$$

Recall that we wish to take our message set to the set of elements of $\mathcal{O}_K$ with size bounded by B. In fact, there exists a size shift z which allows us to calculate a lower bound for the number of elements in the message set of $\mathcal{C}_K$, i.e. $|\{x \in \mathcal{O}_K | \operatorname{size}_z(x) \leq B\}|$. From now on, we adopt the convention that whenever the value of B is chosen, a choice of z satisfying the following theorem is also chosen and fixed. Using such a z will become useful in analyzing the rate of the code.

Theorem 11 *([Guru]) Let K be a number field of degree m and signature (r_1, r_2), with discriminant d_K. For any $B \in \mathbb{R}_{>0}$, there exists $z \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ such that*

$$|\{x \in \mathcal{O}_K | \operatorname{size}_z(x) \leq B\}| \geq \frac{2^{r_1}\pi^{r_2}B^m}{m!\sqrt{|\mathrm{d}_k|}}.$$

4.2 Lower Bounds on $\mathcal{D}(\mathcal{C}_K)$ and $\mathcal{R}(\mathcal{C}_K)$

Guruswami ([Guru]) shows the following lower bound for the minimum distance of our code $\mathcal{C}_K$.

Theorem 12 *Let $\mathcal{C}_K$ be the number field code with parameters $(n, \mathfrak{p}_1, \ldots, \mathfrak{p}_n; B; z)$, where $[K : \mathbb{Q}] = m$. Suppose*

$$\|\mathfrak{p}_1\| \times \|\mathfrak{p}_2\| \times \cdots \times \|\mathfrak{p}_l\| > \left(\frac{2B}{m}\right)^m \text{ for some integer } 1 \in [1, n].$$

Then $\delta(\mathcal{C}_K) \geq (n - l + 1)$.

Proof Suppose there exist two codewords, $E(x_1)$ and $E(x_2)$, whose Hamming distance is $n - l$. That is, suppose $E(x_1)$ and $E(x_2)$ agree in l places. Let us denote these l places by $1 \leq i_1 < i_2 < \cdots < i_l \leq n$.

Then

$$\begin{aligned} & (x_1 - x_2) \in \mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_l} \\ \Longrightarrow \quad & \|\mathfrak{p}_{i_1}\| \times \cdots \times \|\mathfrak{p}_{i_l}\| \ \mid \ \|x_1 - x_2\| \\ \Longrightarrow \quad & \|x_1 - x_2\| \geq \|\mathfrak{p}_{i_1}\| \times \cdots \times \|\mathfrak{p}_{i_l}\| \\ \Longrightarrow \quad & \|x_1 - x_2\| \geq \|\mathfrak{p}_1\| \times \cdots \times \|\mathfrak{p}_l\|, \end{aligned}$$

since $\|\mathfrak{p}_1\| \leq \cdots \leq \|\mathfrak{p}_l\|$.

Also, as $\operatorname{size}_z(x_1) \leq B$ and $\operatorname{size}_z(x_2) \leq B$, we have $\left(\frac{2B}{m}\right)^m \geq \|x_1 - x_2\|$.

Thus, we have

$$\left(\frac{2B}{m}\right)^m \geq \|x_1 - x_2\| \;\geq\; \prod_{i=1}^{l} \|\mathfrak{p}_i\|.$$

Hence, if $\|\mathfrak{p}_1\| \times \|\mathfrak{p}_2\| \times \cdots \times \|\mathfrak{p}_l\| > \left(\frac{2B}{m}\right)^m$, then two codewords agree to at most $l-1$ places. That is, $\delta(\mathcal{C}_K) \geq n - l + 1$. ∎

Definition 27 For the code $\mathcal{C}_K$ with parameters $(n, \mathfrak{p}_1, \ldots, \mathfrak{p}_n; B; z)$, where $[K : \mathbb{Q}] = m$, we define

$$\Delta := 1 - \frac{m \log_2 \frac{2B}{m}}{n \log_2 \|\mathfrak{p}_1\|},$$

and call this the **designed relative distance** of the code.

Corollary 1 *Let $\mathcal{C}_K$ be as in Theorem 12.*
If

$$\Delta := 1 - \frac{m \log_2 \frac{2B}{m}}{n \log_2 \|\mathfrak{p}_1\|} > 0,$$

then $\mathcal{D}(\mathcal{C}_K) > \Delta > 0$.

Proof
Let $l = \left\lceil \left(\frac{m \log_2(\frac{2B}{m})}{\log_2 \|\mathfrak{p}_1\|} \right) \right\rceil$.
Clearly $l > \frac{m \log_2(\frac{2B}{m})}{\log_2 \|\mathfrak{p}_1\|} \Rightarrow \|\mathfrak{p}_1\|^l > \left(\frac{2B}{m}\right)^m$, and we have

$$\|\mathfrak{p}_1\| \times \|\mathfrak{p}_2\| \times \cdots \times \|\mathfrak{p}_l\| \geq \|\mathfrak{p}_1\|^l > \left(\frac{2B}{m}\right)^m.$$

Thus, by Theorem 12, we have $\delta(\mathcal{C}_K) \geq n - l + 1$.
Then

$$\begin{aligned} \delta(\mathcal{C}_K) &\geq n - \left\lceil \left(\frac{m \log_2(\frac{2B}{m})}{\log_2 \|\mathfrak{p}_1\|} \right) \right\rceil + 1 \\ &> n - \left(\frac{m \log_2(\frac{2B}{m})}{\log_2 \|\mathfrak{p}_1\|} \right), \text{ as} \end{aligned}$$

$$\begin{aligned} \left(\frac{m \log_2(\frac{2B}{m})}{\log_2 \|\mathfrak{p}_1\|} \right) + 1 &> \left\lceil \left(\frac{m \log_2(\frac{2B}{m})}{\log_2 \|\mathfrak{p}_1\|} \right) \right\rceil \\ \iff -\left\lceil \left(\frac{m \log_2(\frac{2B}{m})}{\log_2 \|\mathfrak{p}_1\|} \right) \right\rceil + 1 &> -\left(\frac{m \log_2(\frac{2B}{m})}{\log_2 \|\mathfrak{p}_1\|} \right). \end{aligned}$$

Thus we have

$$\mathcal{D}(\mathcal{C}_K) > 1 - \frac{m \log_2 \left(\frac{2B}{m}\right)}{n \log_2 \|\mathfrak{p}_1\|}.$$

That is,

$$\mathcal{D}(\mathcal{C}_K) > \Delta > 0.$$

■

We shall let $d_0 = n\Delta = n - \frac{m \log_2\left(\frac{2B}{m}\right)}{\log_2 \|\mathfrak{p}_1\|}$, the resulting lower bound on the minimum distance.

Remark We note that the condition in Corollary 1, that $\Delta > 0$, leads us to the following constraint on our choice of the constant B.

We have

$$\begin{aligned}
& \Delta > 0 \\
\iff \quad & 1 - \frac{m \log_2 \frac{2B}{m}}{n \log_2 \|\mathfrak{p}_1\|} > 0 \\
\iff \quad & \frac{m \log_2 \left(\frac{2B}{m}\right)}{\log_2 \|\mathfrak{p}_1\|} < n \\
\iff \quad & m \log_2 \left(\frac{2B}{m}\right) < n \log_2 \|\mathfrak{p}_1\| \\
\iff \quad & \log_2 \left(\frac{2B}{m}\right) < \frac{n}{m} \log_2 \|\mathfrak{p}_1\| \\
\iff \quad & \left(\frac{2B}{m}\right) < \|\mathfrak{p}_1\|^{\frac{n}{m}} \\
\iff \quad & B < \frac{m}{2} \|\mathfrak{p}_1\|^{\frac{n}{m}}.
\end{aligned}$$

■

We remark that our constraint on B from Corollary 4.2 also guarantees that our encoding function

$$\begin{aligned}
E : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{p}_n, \\
\text{where } x \mapsto (x/\mathfrak{p}_1, \ldots, x/\mathfrak{p}_n),
\end{aligned}$$

is one-to-one.

Let us now turn to the rate of the code $\mathcal{C}_K$. We have the following:

Theorem 13 *Let $\mathcal{C}_K$ be the number field code with parameters $(n, \mathfrak{p}_1, \ldots, \mathfrak{p}_n; B; z)$, where $[K : \mathbb{Q}] = m$, and the signature of K is (r_1, r_2). Then*

$$\mathcal{R}(\mathcal{C}_K) \geq \frac{\log_2(2^{r_1}\pi^{r_2}B^m) - \log_2 m! - \log_2 \sqrt{|\,\mathrm{d}_K\,|}}{n \log_2 \|\mathfrak{p}_\mathfrak{n}\|}.$$

Proof Recall that $\mathcal{R}(\mathcal{C}_K) = \frac{k}{n}$, where k is the dimension and n is the block length.

Moreover, from Theorem 11, we have chosen z such that the size of our message set is bounded:

$$|\{x \in \mathcal{O}_K | \operatorname{size}_z(x) \leq B\}| \geq \frac{2^{r_1}\pi^{r_2}B^m}{m!\sqrt{|d_k|}}.$$

As our encoding function E is one-to-one, we have $|C_K| = |\{x \in \mathcal{O}_K | \operatorname{size}_z(x) \leq B\}|$. So in our case $k = \log_{\|\mathfrak{p}_n\|} |\mathcal{C}_K| = \frac{\log_2 |C_K|}{\log_2 \|\mathfrak{p}_n\|} = \frac{\log_2 |\{x \in \mathcal{O}_K | \operatorname{size}_z(x) \leq B\}|}{\log_2 \|\mathfrak{p}_n\|}$.

Thus we have

$$\begin{aligned}
\mathcal{R}(\mathcal{C}_K) &\geq \frac{\log_2 |\{x \in \mathcal{O}_K | \operatorname{size}_z(x) \leq B\}|}{n \log_2 \|\mathfrak{p}_n\|} \\
&\geq \frac{\log_2 \left(\frac{2^{r_1}\pi^{r_2}B^m}{m!\sqrt{|\,\mathrm{d}_k\,|}} \right)}{n \log_2 \|\mathfrak{p}_n\|} \\
&= \frac{\log_2(2^{r_1}\pi^{r_2}B^m) - \log_2 m! - \log_2 \sqrt{|\,\mathrm{d}_K\,|}}{n \log_2 \|\mathfrak{p}_\mathfrak{n}\|}.
\end{aligned}$$

■

Corollary 2 *Let $\mathcal{C}_K$ be as in Theorem 13, and suppose $B < \frac{m}{2}\|\mathfrak{p}_1\|^{\frac{n}{m}}$. Then*

$$\begin{aligned}
&n \log_2 \|\mathfrak{p}_n\| \mathcal{R}(\mathcal{C}_K) > \\
&(n - \delta(\mathcal{C}_K)) \log_2 \|\mathfrak{p}_1\| + r_2 \log_2 \frac{\pi}{4} + m \log_2 e - m \log_2 \sqrt{\mathrm{rd}_K} - \log_2 3m.
\end{aligned}$$

Proof To obtain this more explicit lower bound, let us recall the **Stirling approximation** for factorials [Rob]:

$$m! \approx \widehat{m!} := \sqrt{2\pi m} \left(\frac{m}{e} \right)^m \ \forall m \geq 1.$$

The error in this approximation is estimated by

$$e^{\left(\frac{1}{12m+1}\right)} < \frac{m!}{\widehat{m!}} < e^{\left(\frac{1}{12m}\right)}.$$

In fact, it's enough to use

$$\sqrt{2\pi m} \left(\frac{m}{e} \right)^m \leq 3m \left(\frac{m}{e} \right)^m,$$

from which we obtain

$$n \log_2 \|\mathfrak{p}_n\| \mathcal{R}(\mathcal{C}_K) > (n - d_0) \log_2 \|\mathfrak{p}_1\| + r_2 \log_2 \frac{\pi}{4} + m \log_2 e - m \log_2 \sqrt{\mathrm{rd}_K} - \log_2 3m,$$

where $d_0 = n\Delta = n - \frac{m \log_2\left(\frac{2B}{m}\right)}{\log_2 \|\mathfrak{p}_1\|}$, as before.

Then, by Corollary 1, we have $\delta(\mathcal{C}_K) > d_0$, which implies

$$n \log_2 \|\mathfrak{p}_n\| \mathcal{R}(\mathcal{C}_K) > (n - \delta(\mathcal{C}_K)) \log_2 \|\mathfrak{p}_1\| + r_2 \log_2 \frac{\pi}{4} + m \log_2 e - m \log_2 \sqrt{\mathrm{rd}_K} - \log_2 3m.$$

■

5 Constructing a Family of Codes $\{\mathcal{C}_i\}$ from Totally Complex Fields

We shall now explore the code construction from the previous section with K a totally complex number field. This will allow us to construct an asymptotically good family of codes.

Now, we would like our infinite sequence of number fields $K_0, K_1, \ldots, K_i, \ldots$, from which we will construct our family of codes $\{\mathcal{C}_i\}$, to have several properties. First, we would like rd_K to be bounded, as this will become useful in ensuring $\mathcal{R}(\{\mathcal{C}_i\}) > 0$ and $\mathcal{D}(\{\mathcal{C}_i\}) > 0$. In addition, as we would like to keep the alphabet size of our code as small as possible, we need our sequence of number fields to have several prime ideals of small norm. We can ensure the first criterion by taking the K_i to be non-trivial unramified extensions, in which case $\mathrm{rd}_K := \mathrm{rd}_{K_0} = \mathrm{rd}_{K_1} = \cdots = \mathrm{rd}_{K_i} = \cdots$. The second may be satisfied if we have a set of primes $P \subset \mathbb{Q}$ which splits completely in each K_i. Given these properties, a natural choice is to take $K_0 \subset K_1 \subset \cdots \subset K_i \subset \cdots$ to be an infinite T-decomposing p-class field tower, where T is the set of prime ideals in K_0 lying above P.

In terms of actual construction, we will use the constrained version of Golod-Shafarevich, found in Theorem 10, which gives a criterion for the existence of infinite T-decomposing 2-class field towers, where K_0 is an imaginary quadratic field.

5.1 $\mathcal{R}(\{\mathcal{C}_i\})$ and $\mathcal{D}(\{\mathcal{C}_i\})$

We shall now assume our code is constructed from a totally complex number field K_0, such that we have an infinite sequence $K_0, K_1, \ldots, K_i, \ldots$, where each K_i is a non-trivial unramified extension of K_{i-1}, for $i \geq 1$, and there exists a set $P = \{p_1, \ldots, p_s\}$ of primes which split completely in $K_i/\mathbb{Q}$, $\forall i$.

Let us fix an arbitrary $K = K_i$ for some i. Suppose $[K : \mathbb{Q}] = m$, $[K_0 : \mathbb{Q}] = m_0$, and $|P| = s$. Thus the signature of K is $(0, \frac{m}{2})$, and there are $m_0 s$ prime ideals of K_0 which split completely up the tower. We shall consider the code $\mathcal{C}_K$ with parameters $(n, \mathfrak{p}_1^{(1)}, \ldots, \mathfrak{p}_1^{(m)}, \ldots, \mathfrak{p}_s^{(1)}, \ldots, \mathfrak{p}_s^{(m)}; B; z)$, where $\mathfrak{p}_j^{(1)}, \ldots, \mathfrak{p}_j^{(m)}$ are the prime ideals of K lying above p_j for $1 \leq j \leq s$, where $n = sm$, $B = cm$ for some fixed $c \in \mathbb{R}_{>0}$, and $z \in \mathbb{C}^{\frac{m}{2}}$, the shift parameter noted earlier.

We note that for each $1 \leq j \leq s$, $\|\mathfrak{p}_j^{(1)}\| = \|\mathfrak{p}_j^{(2)}\| = \cdots = \|\mathfrak{p}_j^{(m)}\| = p_j$. We also note $\mathrm{rd}_{K_0} = \mathrm{rd}_K$, as before.

We have thus constructed a family of codes $\{\mathcal{C}_i\}$, where the code $\mathcal{C}_i$ is based

on $K = K_i$ as above, for $i \geq 1$.

Let us now consider the rate and relative distance of our family of codes $\{\mathcal{C}_i\}$. More specifically, we are interested in which parameters yield asymptotically good codes.

Theorem 14 *Let the family of codes $\{\mathcal{C}_i\}$ be as above. If $c < \frac{1}{2}p_1^s$, then in the limit of large $m \to \infty$, we have*

$$\mathcal{R}(\{\mathcal{C}_i\}) > \frac{\log_2 p_1}{\log_2 p_s}\left(1 - \mathcal{D}(\{\mathcal{C}_i\}) - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}\right).$$

Proof Analyzing c, we have

$$\begin{aligned} & c < \frac{1}{2}p_1^s \\ \iff \quad & cm < \frac{m}{2}(p_1)^{\frac{sm}{m}} \\ \iff \quad & B < \frac{m}{2}(p_1)^{\frac{n}{m}}, \end{aligned}$$

and thus we may apply Corollary 2.

Substituting $r_2 = \frac{m}{2}$ and $n = sm$ into the formula from Corollary 2, we have

$$\begin{aligned} & n\log_2 p_s \mathcal{R}(\mathcal{C}) > \\ & (n - \delta(\mathcal{C}))\log_2 p_1 + \frac{m}{\log_2 p_s}\left(\log_2\left(\frac{\pi}{4}\right)^{\frac{1}{2}} + \log_2 e - \log_2\sqrt{\mathrm{rd}_K}\right) - \frac{\log_2 3m}{\log_2 p_s} \\ \iff \quad & \mathcal{R}(\mathcal{C}) > \frac{1}{n\log_2 p_s}\left((n - \delta(\mathcal{C}))\log_2 p_1 + \frac{m}{\log_2 p_s}\log_2\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}} - \frac{\log_2 3m}{\log_2 p_s}\right) \\ & = \left(1 - \frac{\delta(\mathcal{C})}{n}\right)\frac{\log_2 p_1}{\log_2 p_s} - \frac{1}{s\log_2 p_s}\log_2\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}} - \frac{\log_2 3m}{\log_2 p_s}. \end{aligned}$$

Then, in the limit of large $m \to \infty$, we have

$$\begin{aligned}\mathcal{R}(\{\mathcal{C}_i\}) &> (1-\mathcal{D}(\{\mathcal{C}_i\}))\frac{\log_2 p_1}{\log_2 p_s} - \frac{1}{s\log_2 p_s}\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)\frac{\log_2 p_1}{\log_2 p_s} \\ &= \frac{\log_2 p_1}{\log_2 p_s}\left(1-\mathcal{D}(\{\mathcal{C}_i\}) - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}\right).\end{aligned}$$

■

Theorem 15 *If* $\mathrm{rd}_K < \frac{\pi e^2}{4}p_1^{2s}$, *the above construction gives an asymptotically good family of codes* $\{\mathcal{C}_i\}$ *for any value of* c *in the range* $\frac{1}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}} < c < \frac{1}{2}p_1^s$. *In particular, such a family exists with* $\mathcal{D}(\{\mathcal{C}_i\})$ *in the range*

$$0 < \mathcal{D}(\{\mathcal{C}_i\}) < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1},$$

and

$$\mathcal{R}(\{\mathcal{C}_i\}) > \frac{\log_2 p_1}{\log_2 p_s}\left(1-\mathcal{D}(\{\mathcal{C}_i\}) - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}\right).$$

Proof We see that $c < \frac{1}{2}p_1^s$ ensures that we may apply Theorem 14. That is, the construction has the following property:

$$\mathcal{R}(\{\mathcal{C}_i\}) > \frac{\log_2 p_1}{\log_2 p_s}\left(1-\mathcal{D}(\{\mathcal{C}_i\}) - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}\right).$$

Analyzing the above, we see that $\mathcal{R}(\{\mathcal{C}_i\}) > 0$ if and only if $\mathrm{rd}_K < \frac{\pi e^2}{4}p_1^{2s}$, with $c > \frac{1}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}$.

As we want $\mathcal{D}(\{\mathcal{C}_i\}) > 0$, it is clear we must have

$$1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1} > \mathcal{D}(\{\mathcal{C}_i\}) > 0.$$

We see that

$$1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1} > 0 \iff \mathrm{rd}_K < \frac{\pi e^2}{4} p_1^{2s} :$$

We have

$$\begin{aligned}
& \mathrm{rd}_K < \frac{\pi e^2}{4} p_1^{2s} \\
\iff \quad & \frac{\mathrm{rd}_K}{\pi} < \left(\frac{e}{2} p_1^s\right)^2 \\
\iff \quad & \frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}} < p_1^s \\
\iff \quad & \log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right) < s\log_2 p_1 \\
\iff \quad & \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1} < 1 \\
\iff \quad & 0 < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}.
\end{aligned}$$

We see that $\mathrm{rd}_K < \frac{\pi e^2}{4} p_1^{2s}$ implies $\frac{1}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}} < \frac{1}{2} p_1^s$, and thus we may choose c in that range. In fact, $\mathcal{D}(\{\mathcal{C}_i\}) < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}$ so long as we choose $c > \frac{1}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}$:

We have

$$\begin{aligned}
& \mathcal{D}(\{\mathcal{C}_i\}) < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1} \\
\iff \quad & \frac{1}{n}\left(n - \frac{m\log_2(\frac{2B}{m})}{\log_2 p_1}\right) < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1} \\
\iff \quad & 1 - \frac{m\log_2(\frac{2B}{m})}{n\log_2 p_1} < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1} \\
\iff \quad & 1 - \frac{m\log_2(\frac{2B}{m})}{sm\log_2 p_1} < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1} \\
\iff \quad & \frac{\log_2(\frac{2B}{m})}{s\log_2 p_1} > \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1} \\
\iff \quad & \log_2\left(\frac{2B}{m}\right) > \log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right) \\
\iff \quad & \frac{2B}{m} > \frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}} \\
\iff \quad & B > \frac{m}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}} \\
\iff \quad & cm > \frac{m}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}} \\
\iff \quad & c > \frac{1}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}.
\end{aligned}$$

Thus, we have $\mathcal{R}(\{\mathcal{C}_i\}) > 0$ and $\mathcal{D}(\{\mathcal{C}_i\}) > 0$, which implies $\{\mathcal{C}_i\}$ is asymptotically good. By varying c in the given range, we achieve asymptotically good codes $\{\mathcal{C}_i\}$ with $\mathcal{D}(\{\mathcal{C}_i\})$ in the range $0 < \mathcal{D}(\{\mathcal{C}_i\}) < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}$ and $\mathcal{R}(\{\mathcal{C}_i\}) > \frac{\log_2 p_1}{\log_2 p_s}\left(1 - \mathcal{D}(\{\mathcal{C}_i\}) - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}\right)$. ∎

Remark Although Theorem 15 is implicit in Guruswami ([Guru]), we feel it is helpful to state it explicitly. We note that as c approaches $\frac{1}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}$,

$\mathcal{D}(\{\mathcal{C}_i\})$ approaches $1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s\log_2 p_1}$ and $\mathcal{R}(\{\mathcal{C}_i\})$ approaches 0. Also, $c < \frac{1}{2}p_1^s$ ensures $\mathcal{D}(\{\mathcal{C}_i\}) > 0$. The most important point, however, is the bound on the root discriminant; this bound allows us to choose a c giving both positive relative distance and rate. ∎

5.2 Example

We shall now give an example of a family of codes $\{\mathcal{C}_i\}$ based on the previous construction. We shall use the Golod-Shafarevich criterion to construct an infinite T-decomposing 2-class field tower $K_0, K_1, \ldots, K_i, \ldots$, which will have the desired property that $\forall i, K_i$ is unramified, and T splits completely all the way up the tower. We note that our example, although similar, is different from that of Guruswami ([Guru]). Guruswami gives an example of a code with alphabet size 29, which, as in our example, uses prime ideals of the same norm. He also discusses an example using prime ideals of different norms, which yields a code with alphabet size 19.

Let $\alpha = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$, and take $K_0 = \mathbb{Q}(\sqrt{-\alpha})$. This imaginary quadratic number field has the following properties.

Theorem 16 *Let K_0 be as above. Then*

1. $\mathrm{rd}_{K_0} = \sqrt{4\alpha} \approx 4845.9736$,

2. *The prime 31 splits into a set T of two primes ideals of norm 31 in $\mathcal{O}_{K_0}$,*

3. *K_0 has an infinite T-decomposing 2-class field tower.*

Proof

1. As $-\alpha = -3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \equiv 3 \pmod 4$, $\mathrm{d}_{K_0} = -4\alpha$.

2. We check that the Legendre symbol $\left(\frac{-\alpha}{31}\right) = 1 \Rightarrow -\alpha$ is a quadratic residue modulo 31 $\Rightarrow$ the prime 31 splits into a set T of two prime ideals in the quadratic extension $K_0/\mathbb{Q}$.

3. Consider $Q = \{2, 3, 5, 7, 11, 13, 17, 23\}$. From Theorem 5, we know these are the 8 primes which ramify in $K_0/\mathbb{Q}$ (i.e. the primes which divide the

discriminant of K_0). Let $P = \{31\}$. Thus, from Genus Theory (Theorem 7), we know $2\text{-rk}\,\mathrm{Cl}_{K_0} = |Q|-1 = 8-1 = 7$, and $2\text{-rk}\,\mathrm{Cl}_{K_0,P} = 7-1 = 6$.

Now, T is the set of prime ideals lying above P. Applying the modified Golod-Shafarevich criterion of Theorem 10 with $|Q| = 8, |T| = 2$, and $|P| = 1$, we see that K_0 has an infinite T-decomposing 2-class field tower.

■

Now, let $K_0 \subset K_1 \subset \cdots \subset K_i \subset \cdots$ be the infinite T-decomposing 2-class field tower of K_0. We construct our family of codes $\{\mathcal{C}_i\}$, where each code $\mathcal{C}$ is based on the number field K, where $\mathcal{C} = \mathcal{C}_i$ and $K = K_i$ for some i.

Fix an n, and suppose $[K : \mathbb{Q}] = m$. Note that K is totally complex, and thus its signature is $(0, \frac{m}{2})$. Our code $\mathcal{C}$ will have parameters $(m, \mathfrak{p}_1^{(1)}, \ldots, \mathfrak{p}_1^{(m)}; B; z)$, where $\mathfrak{p}_1^{(1)}, \ldots, \mathfrak{p}_1^{(m)}$ are prime ideals of norm 31, $B = cm$ for some $c \in \mathbb{R}_{>0}$, and $z \in \mathbb{C}^{\frac{m}{2}}$ is the appropriate shift parameter.

We shall now use Theorem 15 to show that the above code family is asymptotically good for certain values of c.

As

$$\mathrm{rd}_{K_0} = \mathrm{rd}_K \approx 4845.9736 < \frac{\pi e^2}{4} p_1^{2s} = \frac{\pi e^2}{4} 31^{2\cdot 1} \approx 5577.0204,$$

we see that the primary criterion is satisfied.

Moreover, it suffices to choose c in the following range. We take $c > \frac{1}{e}\sqrt{\frac{\mathrm{rd}_{K_0}}{\pi}} \approx 14.4482$, and $c < \frac{1}{2} p_1^s = \frac{1}{2} p_1^1 = \frac{1}{2} \cdot 37 = 15.5$.

Hence, if $14.4482 < c < 15.5$, we have asymptotically good codes over an alphabet of size 31 for relative distance $\mathcal{D}(\{\mathcal{C}_i\})$ in the range

$$0 < \mathcal{D}(\{\mathcal{C}_i\}) < 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_K}{\pi}}\right)}{s \log_2 p_1} \approx 1 - \frac{\log_2\left(\frac{2}{e}\sqrt{\frac{4845.9736}{\pi}}\right)}{1 \cdot \log_2 31} \approx 1 - .9795 = .0205,$$

where as $\mathcal{D}(\{\mathcal{C}_i\})$ approaches .0205, $\mathcal{R}(\{\mathcal{C}_i\})$ approaches 0, and as $\mathcal{D}(\{\mathcal{C}_i\})$ approaches 0, $\mathcal{R}(\{\mathcal{C}_i\})$ approaches .0205.

Of course, this example falls well below the Gilbert Varshamov threshold. The question of whether such a code construction might yield an asymptotically good family of codes which beats the Gilbert Varshamov threshold is an interesting question, which bears further scrutiny.

References

[Guru] V. Guruswami, *Constructions of Codes From Number Fields*, IEEE Transactions on Information Theory, **49**, No. 3, (2003), 594-603.

[FM] F. Hajir and C. Maire, *Tamely Ramified Towers and Discriminant Bounds for Number Fields*, Compositio Mathematica **128**, Kluwer Academic Publishers, (2001), 35-53.

[Mai] C. Maire, *Finitude de tours et p-pours T-ramifiées moderées S-décomposées*, J. Théorie des Nombres de Bordeaux, **8**, No. 1, (1996), 47-73.

[Mar] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[Rob] Robbins, Herbert, *A remark on Stirling's formula*, Amer. Math. Monthly **62**, (1955), 26-29.

[Rom] S. Roman, *Coding and Information Theory*, Springer-Verlag, New York, 1992.

[Sam] P. Samuel, *Algebraic Theory of Numbers*, Houghton Mifflin Co., Boston, 1970.

[S] R. Schoof, Infinite class field towers of quadratic fields, *J. Reine Angew. Math.* **372** (1986), 209-220.

[TV] M. A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Boston, 1991.