Constructions of Codes from Number Fields

Venkatesan Guruswami

MIT Laboratory for Computer Science
200 Technology Square
Cambridge, MA 02139.
Email: venkat@theory.lcs.mit.edu.

November, 2000

Abstract

We define number-theoretic error-correcting codes based on algebraic number fields, thereby providing a generalization of Chinese Remainder Codes akin to the generalization of Reed-Solomon codes to Algebraic-geometric codes. Our construction is very similar to (and in fact less general than) the one given by Lenstra [9], but the parallel with the function field case is more apparent, since we only use the non-archimedean places for the encoding. We prove that over an alphabet size as small as 19, there even exist *asymptotically good* number field codes of the type we consider. This result is based on the existence of certain number fields that have an infinite class field tower in which some primes of small norm split completely.

1 Introduction

Algebraic Error-correcting Codes. An error-correcting code over the alphabet $\mathbb{F}_q$ is a subset $\mathcal{C}$ of $\mathbb{F}_q^n$ for some n such that every two distinct elements (called codewords) of $\mathcal{C}$ differ in a large number of coordinates. More formally, an $[n, k, d]_q$-code $\mathcal{C}$ is a subset of $\mathbb{F}_q^n$ of size q^k such that if $c_1 \neq c_2 \in \mathcal{C}$ are two distinct codewords then they differ in at least d of the n positions. If $\mathcal{C}$ is actually a *subspace* of dimension k of the vector space $\mathbb{F}_q^n$ (over $\mathbb{F}_q$) then it is called a *linear code*. The parameters n, k, d are referred to as the blocklength, rate (or dimension) and minimum distance (or simply distance) of the code $\mathcal{C}$.

A broad and very useful class of error-correcting codes are *algebraic-geometric* codes (henceforth AG-codes), where the message is interpreted as specifying an element of some "function field" and it is encoded by its evaluations at a certain fixed set of "points" on an underlying well-behaved algebraic curve. A simple example is the widely used class of Reed-Solomon codes where messages are low degree polynomials and the codewords correspond to evaluations of such a polynomial at a fixed set of points in a finite field. The distance of the code follows from the fact that a low-degree polynomial cannot have too many zeroes in any field, and this is generalized for the case of algebraic-geometric codes using the fact that any "regular function" on an algebraic curve cannot have more zeroes than poles (accordingly the messages are elements of the function field with a small total number of poles: the Reed-Solomon case can be obtained as a special case by viewing degree k polynomials over $\mathbb{F}_q$ as elements of the function field $\mathbb{F}_q(t)$ which have at most k poles at "infinity" and no poles elsewhere).

The class of algebraic-geometric codes are a broad class of very useful codes that include codes which beat the Gilbert-Varshamov bound for alphabet sizes $q \geq 49$ (see for example [22, 2]). In addition to achieving such good performance, they possess a nice algebraic structure which has enabled design of efficient decoding algorithms to decode even in the presence of a large number of errors [18, 5].

Motivation behind our work. Another family of algebraic codes that have received some study are number-theoretic redundant residue codes called the "Chinese Remainder codes" (henceforth called CRT codes) [12, 3]. Here the messages are identified with integers with absolute value at most K (for some parameter K that governs the rate) and a message m is encoded by its residues modulo n primes $p_1 < p_2 < \cdots < p_n$. If $K = p_1 \cdot p_2 \cdots p_k$ and $n > k$, this gives a redundant encoding of m and the resulting "code" (which is different from usual codes in that symbols in different codeword positions are over different alphabets) has distance $n - k + 1$.

In light of the progress in decoding algorithms for Reed-Solomon and algebraic-geometric codes, there has also been progress on decoding CRT codes [3, 1, 6] in the presence of very high noise, and the performance of the best known algorithm matches the number of errors correctable for Reed-Solomon codes [5]. There is quite a bit of similarity between Reed-Solomon and CRT codes: both are redundant residue codes that are MDS (see [10]). Since Reed-Solomon codes are a specific example of the more general family of AG-codes, it is natural to ask if CRT codes can also be realized as certain kind of AG-codes, and further whether there is a natural generalization of CRT codes akin to the generalization of Reed-Solomon codes to algebraic-geometric codes. In addition to the mathematical appeal of this question, such a construction will give yet another construction of algebraic codes (or "ideallic codes", see [6]) which may find other applications outside coding theory (for example the decoding algorithm for the CRT code in [3] was developed initially for a complexity-theoretic motivation, namely to establish an average-case hardness for computing the permanent). Moreover they will naturally fall under the umbrella of codes covered by the "ideallic" decoding principle used in [5, 6], and questions of efficient implementation of this decoding procedure for these codes may lead to questions in algorithmic algebraic number theory that are interesting in their own right.

Our Results. For those familiar with the algebraic-geometric notion of *schemes*, it is not hard to see that the CRT code can be captured by a geometric framework using the idea of "one-dimensional schemes" and can thus be cast as a geometric code via an appropriately defined non-singular curve (namely $\mathrm{Spec}(\mathbb{Z})$ which is space of all prime ideals of $\mathbb{Z}$) and viewing integers (which are the messages) as regular functions on that curve. More generally, using this idea we are able to define error-correcting codes based on any number field (a finite field extension of the field $\mathbb{Q}$ of rational numbers) – we call such codes *number field codes* (or NF-codes).

We prove that over a large enough alphabet ($\mathrm{GF}(19)$ suffices), there in fact exist *asymptotically good* number field codes. A code family $\{\mathcal{C}_i\}$ of $[n_i, k_i, d_i]_q$ codes of increasing blocklength $n_i \to \infty$ is called *asymptotically good* if $\liminf \frac{k_i}{n_i} > 0$ and $\liminf \frac{d_i}{n_i} > 0$. Explicit constructions of asymptotically good codes is a central problem in coding theory and several constructions are known, the best ones (for large enough q) being certain families of algebraic-geometric codes. Our construction of asymptotically good number fields uses concepts from class field theory and in particular is based on the existence of certain number fields that have an infinite Hilbert class field tower in which several primes of small norm split completely all the way up the tower. Obtaining such a construction over as small an alphabet size as possible is one of the primary focuses of this paper.

Comparison with [9]. It is our pleasure to acknowledge here that Lenstra [9] (see also the account in [20]) had long back already considered the construction of codes from algebraic number fields, and we are therefore by no means the first to consider this question. Unfortunately, we were unaware of his work when we came up with our constructions. In fact, Lenstra [9] also shows that, under the GRH, asymptotically good codes that beat the Gilbert-Varshamov bound can be constructed based on number fields for a large enough alphabet size.

The main point of difference between his constructions and ours is the following. In our constructions, messages are taken to be an appropriate subset of elements of the ring of integers in a number field and they are encoded by their residues modulo certain *non-archimedean* (also referred to as *finite*) places. This corresponds exactly to the "ideallic" view of codes (see [6]) since we have an underlying ring and messages are encoded by their residues modulo a few prime ideals. The construction in [9] is actually more general, and also allows *archimedean* (also referred to as *infinite*) places to be used for encoding. (We stress that it is not *necessary* to use the archimedean places for the constructions in [9], but doing so enabled [9] to prove the existence of asymptotically good codes more easily.) In particular, for encoding corresponding to a real archimedean place τ, the segment of the real line of interest is divided into q equal subsegments (assuming we want a q-ary code), and a message is encoded by the index of the subsegment where its embedding (w.r.t the place τ) lies.

The use of archimedean places as in [9] is extremely insightful and cute, and also makes it easier to get good code parameters. But, not using them maintains the parallel with the function field situation, and gives a base case of NF-code constructions which is most amenable to encoding/decoding, assuming algorithms for these will eventually be studied. Also focusing only on the finite places allows us to pick messages for the code from a slightly larger space (we can pick them from an "octahedron" instead of a "cube"). Consequently, we can quantify the "size" of a message by a single real number, and this way the parallel with AG-codes is even more transparent (in the function field case, the "size" of a message would be its pole order at a specified point on the algebraic curve).

Finally, the results in [9] are of an asymptotic flavor, i.e. focus on what can be achieved in the limit for large alphabet size q, and do not imply asymptotically good codes exist for some reasonably small q. Also, no unconditional result (i.e. without assuming the GRH) guaranteeing the existence of asymptotically good codes can be directly inferred from [9] **if** one modifies the constructions therein to include *only* codeword positions corresponding to the finite places. We are able to prove, using some results on the existence of infinite class field towers, that asymptotically good codes of the kind we construct exist for reasonable values of q (for example, $q = 19$ suffices).

Disclaimer. Many of the lemmas in this paper implicitly have identical or near-identical parallels in [9]. Since most of this paper was written without knowledge of [9], we may not give [9] its due credit in a few places. We apologize for this. One plus point of this, however, is that our presentation is essentially self-contained modulo some standard (but possibly deep!) facts from algebraic number theory.

Remarks. Despite the striking similarity with the geometric situation of function fields, one fundamental difference in the number field case is that we have to work over characteristic zero. As it turns out, this makes the situation more complicated (and leads to worse parameters and loss of linearity in general) than the function field case. We do not believe these codes will be practical, or will achieve trade-offs between parameters that are beyond the reach of the more well-understood AG-codes (see [9] for some quantitative statements concerning this). We also focus on the *existence* of such codes and do not discuss how they may be constructed or represented efficiently, let alone how they may be encoded or decoded. These could be directions for future work which might have some exciting number-theoretic content.

2 Algebraic Codes: Construction Philosophy

We now revisit, at a high level, the basic principle that underlies the construction of all algebraic error-correcting codes, including Reed-Solomon codes, Algebraic-geometric codes, and the Chinese Remainder code. A similar discussion can also be found in [6].

An algebraic error-correcting code is defined based on an underlying ring R (assume it is an integral domain) whose elements r come equipped with some notion of "size", denoted $\mathsf{size}(r)$.[1] For example, for Reed-Solomon codes, the ring is polynomial ring $F[X]$ over a (large enough) finite field F, and the "size" of $f \in F[X]$ is simply its degree as a polynomial in X. Similarly, for the CRT code, the ring is $\mathbb{Z}$, and the "size" is the usual absolute value.

The messages of the code are the elements of the ring R whose size is at most a parameter Λ (this parameter governs the rate of the code). The encoding of a message $m \in R$ is given by

$$m \mapsto \mathsf{Enc}(m) = (m/I_1, m/I_2, \cdots, m/I_n)$$

where I_j, $1 \le j \le n$ are n (distinct) prime ideals of R. (For instance, in the case of Reed-Solomon codes, we have $R = F[X]$ and $I_j = (X - \alpha_j)$ – the ideal generated by the polynomial $(X - \alpha_j)$ – for $1 \le j \le n$, where $\alpha_1, \dots, \alpha_n$ are *distinct* elements of F. This ideal-based view was also at the heart of the decoding algorithm for CRT codes presented in [6].)

There are two properties of a code that of primary concern in its design, namely (a) its rate, and (b) its minimum distance. The rate property of the code constructed by the above scheme follows from an estimate of the number of elements m of R that have $\mathsf{size}(m) \le \Lambda$. The distance of the code follows by using further properties of the $\mathsf{size}(\cdot)$ function which we mention informally below.

1. For elements $a, b \in R$, $\mathsf{size}(a - b)$ is "small" whenever $\mathsf{size}(a)$ and $\mathsf{size}(b)$ are both "small".
2. If $f \neq 0$ belongs to "many" ideals among $I_1, I_2, \dots, I_n$, then $\mathsf{size}(f)$ cannot be "too small".

It is not difficult to see that, together these two properties imply that if $m_1 \neq m_2$ are distinct messages, then their encodings $\mathsf{Enc}(m_1)$ and $\mathsf{Enc}(m_2)$ cannot agree in too many places, and this gives the distance property of the code.

3 Constructing Codes from Number Fields

The previous section described how to construct codes from rings provided an appropriate notion of size can be defined on it. We now focus on the specific problem of constructing codes based on number fields which will be a generalization of CRT codes akin to the generalization of Reed-Solomon codes to AG-codes. The necessary background on number fields can be found in any standard algebraic number theory text (for example [15, 13]), though most facts we will use are mentioned in the next few subsections.

An algebraic number field (or number field for short) is a finite (algebraic) extension of the field $\mathbb{Q}$ of rational numbers. Given some algebraic number field $K/\mathbb{Q}$ of degree $[K : \mathbb{Q}] = m$ (i.e., $K = \mathbb{Q}(\alpha)$ where α satisfies an irreducible polynomial of degree m over $\mathbb{Q}$), the code will comprise of a subset of elements from its ring of integers, denoted $\mathcal{O}_K$. (Recall that the ring of integers of a

[1] It is possible to define error-correcting codes more generally based on a field together with the valuations of that field, and the messages belong to some "divisor" class with respect to these valuations. AG-codes are usually defined this way (see for example [19]), but we choose the "ring based" definition since it is easier to explain, saves the effort of introducing the language of divisors, and seems somewhat more natural for the definition of number field codes.

number field K is the integral closure of $\mathbb{Z}$ in K, i.e., it consists of elements of K that satisfy some monic polynomial over $\mathbb{Z}$.) It is well known that $\mathcal{O}_K$ is a *Dedekind domain*, i.e., is an integrally closed Noetherian domain of dimension one. In "geometric" terms this means that $\mathcal{O}_K$ is the ring of regular functions on a certain non-singular algebraic curve (namely the spectrum $\mathrm{Spec}(\mathcal{O}_K)$ of $\mathcal{O}_K$ which consists of all prime ideals of $\mathcal{O}_K$). We next review some standard properties which are satisfied by the ring of integers of any number field.

3.1 Useful facts about Ring of Integers of a Number Field

The following (standard) facts about the ring of integers $R = \mathcal{O}_K$ will be useful for us (proofs of all these statements can be found, for example, in [13]):

1. **Dimension of R is one:** Every non-zero prime ideal $\mathfrak{P}$ of R is in fact maximal.
2. **Unique Factorization of Ideals:** R has *unique factorization of ideals*; i.e., every ideal I of R can be uniquely expressed as a product of prime ideals.
   - A non-zero ideal J divides I (in the unique factorization of I), denoted $J|I$, if and only if $I \subset J$. (Fact 1 above is a special case of this since a non-zero I is prime iff no J ($\neq I$) divides I, i.e., no J contains I, which is equivalent to saying that I is a maximal ideal.)
3. **Structure of Primes in R:** For a prime $p \in \mathbb{Z}$, suppose the principal ideal pR in R factorizes into prime ideals as $pR = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_\ell^{e_\ell}$ where each $\mathfrak{p}_i$ is a prime ideal of R.
   (a) We say that $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ are all the primes that *lie above p* in R. The number $e_i = e(\mathfrak{p}_i|p)$ is called the *ramification index* of the prime $\mathfrak{p}_i$. We say a prime $\mathfrak{p}_i$ is *ramified* if $e_i > 1$, otherwise it is *unramified*. The prime p is said to be ramified iff some $e_i > 1$, otherwise it is unramified. Similar terminology is used also for a finite extension K/k of a number field k (here we are using $k = \mathbb{Q}$ for purposes of explanation).
   (b) Since each $\mathfrak{p}_i$ is maximal, $R/\mathfrak{p}_i$ is a finite field. Moreover it has characteristic p and is thus a finite extension of $\mathbb{Z}/(p)$. The *inertia degree* of $\mathfrak{p}_i$ lying over p, denoted $f_i = f(\mathfrak{p}_i|p)$ is defined as the degree of the field extension $[R/\mathfrak{p}_i : \mathbb{Z}/(p)]$. In short, $R/\mathfrak{p}_i$ is a finite field of size $p^{f(\mathfrak{p}_i|p)}$.
   (c) The numbers e_i and f_i satisfy $\sum_{i=1}^{\ell} e_i f_i = m$, where m is the degree of the extension $K/\mathbb{Q}$. A prime $p \in \mathbb{Z}$ is said to *split completely* if each $e_i = f_i = 1$. The numbers e_i, f_i are also multiplicative in towers of field extensions (i.e. if $\mathfrak{P}$ lies above $\mathfrak{p}$ in the extension L/K and $\mathfrak{p}$ lies above $\mathfrak{q}$ in the extension K/k, then $e(\mathfrak{P}|\mathfrak{q}) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|\mathfrak{q})$, and similarly for $f(\mathfrak{P}|\mathfrak{q})$).

"Norms" of Ideals: For every non-zero ideal I of a ring of integers R, R/I is finite. One can thus define a norm function on ideals as:

Definition 1 [Norm of Ideals]: *The norm of a non-zero ideal $I \subset R$, denoted $\|I\|$, is defined as $\|I\| = |R/I|$. Note that for a prime ideal $\mathfrak{p}$, $\|\mathfrak{p}\| = p^{f(\mathfrak{p}|p)}$ if $\mathfrak{p}$ lies above $p \in \mathbb{Z}$ and $f(\mathfrak{p}|p)$ is the inertia degree of $\mathfrak{p}$ over p.*

Definition 2 [Norm of Elements in $\mathcal{O}_K$]: *The norm of an element $x \in R$, also denoted $\|x\|$ by abuse of notation, is defined as $\|(x)\|$, i.e., the norm of the ideal generated by x. (Define $\|0\| = 0$.)*

The following fact will be very useful for us later:

Fact 3 *For a number field K, If $x \in I$ for some ideal $I \subset \mathcal{O}_K$, then $\|I\|$ divides $\|x\|$.* □

3.2 Defining size of an element

By Fact 3, it is tempting to define the size of an element f as $\mathsf{size}(f) = \|f\|$. In fact, this satisfies one of the properties we required of size, namely that if $m \neq 0$ has small size, then it cannot belong to several ideals I_i. Unfortunately, the other property we would like our size function to satisfy, namely $\mathsf{size}(a-b)$ is "small" whenever $\mathsf{size}(a)$ and $\mathsf{size}(b)$ are both small, is not satisfied in general for all number fields by the definition $\mathsf{size}(f) = \|f\|$.[2] We thus need a different notion of size of an element, and to this end we first briefly review the theory of valuations of a number field.

3.2.1 Valuations of a Number Field

In order to define the "right" notion of size or absolute value of an element of a number field, we want to appeal to the valuation-theoretic point of view of the theory of number fields. One prominent advantage of the valuation-theoretic perspective (compared to the ideal-theoretic treatment) is that the "archimedean" valuations bring into the picture the points at infinity as the "primes at infinity", and in this way achieve a perfect analogy with the function field case of algebraic geometry. We refer the reader to the book by Neukirch [15] for an excellent exposition of the valuation-theoretic approach to algebraic number theory.

Definition 4 *A* **valuation** *(also called* **place***) of a field K is a function $|\ |: K \to \mathbb{R}$ with the properties:*[3]

1. $|x| \geq 0$, *and* $|x| = 0 \iff x = 0$
2. $|xy| = |x||y|$
3. *There exists a constant $c \geq 1$ such that for all $x, y \in K$, $|x+y| \leq c \cdot \max\{|x|, |y|\}$ ("triangle inequality").*

We tacitly exclude in the sequel the case where $|\ |$ is the trivial valuation of K that satisfies $|x| = 1$ for all $x \neq 0$. Also, when Condition (3) above is met with any $c \leq 2$, then it is an easy exercise to show that in fact $|x+y| \leq |x| + |y|$ for all x, y, which is the "familiar" triangle inequality. Two valuations $|\ |_1$ and $|\ |_2$ on K are said to be *equivalent* iff there exists a real number $s > 0$ such that $|x|_1 = |x|_2^s$ for all $x \in K$. (Whenever we refer to a valuation from now on, we implicitly mean any member of its equivalence class.)

Definition 5 *A* **place** *of K is an equivalence class of valuations of K.*

Definition 6 *A valuation (place) $|\ |$ is called* **non-archimedean** *(or* **ultrametric***) if $|n|$ stays bounded for all $n \in \mathbb{N}$. Otherwise it is called* **archimedean**. *Alternatively, a valuation $|\ |$ is non-archimedean if and only if it satisfies the triangle inequality of Condition (3) above with $c = 1$, i.e., if $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$.*

Examples: The absolute value defined on rational numbers is an example of an archimedean valuation on $\mathbb{Q}$. If $v_p(a/b)$ denotes the highest power of p that divided a rational number a/b, then $|x|_p = p^{-v_p(x)}$ is a non-archimedean valuation on $\mathbb{Q}$. The valuation $|h| = e^{\deg(h)}$ is a non-archimedean valuation on the field of rational functions $\mathbb{Q}(X)$ over $\mathbb{Q}$ (where the degree of a rational function $h(x) = f(x)/g(x)$ where $f, g \in \mathbb{Q}[X]$ is defined as $\deg(f) - \deg(g)$.

[2]For example, let $K = \mathbb{Q}(\alpha)$ where α is a root of $x^2 + Dx + 1 = 0$. Then one can easily see that $\|\alpha\| = 1$ (for example using Proposition 10) and of course $\|1\| = 1$, but $\|\alpha - 1\| = D + 2$, and thus $\|x - y\|$ can be arbitrarily larger than both $\|x\|$ and $\|y\|$ even for quadratic extensions.

[3]Several textbooks call a "valuation" with these properties as an absolute value.

One can define a non-archimedean valuation of the fraction field of any domain R based on any non-zero prime ideal of R (the trivial valuation $|x| = 1$ for all $x \neq 0$ corresponds to the zero ideal), similar to the valuation $|\ \ |_p$ defined on $\mathbb{Q}$ above. In fact the non-zero prime ideals of the ring of integers $\mathcal{O}_K$ of a number field K correspond precisely to the non-archimedean places of K, and are called the **finite places** of K. In addition, the archimedean valuations of K correspond to the **infinite places** of K. The infinite places are important objects in the study of number fields and we review them next.

Remark: Function fields (finite extensions of $\mathbb{F}_q(t)$ where t is transcendental over $\mathbb{F}_q$) have only non-archimedean valuations, and thus differ from number fields in this important respect. For purposes of defining AG-codes one does designate certain places of the function field as *infinite*, but these are non-archimedean places as well, and the distinction between finite and infinite places does not correspond to the dichotomy between non-archimedean and archimedean places.

3.2.2 Infinite places and a notion of "size"

Let $K/\mathbb{Q}$ be a field extension of degree $[K : \mathbb{Q}] = m$. Then there are n distinct field homomorphisms (called embeddings) $\tau_i : K \to \mathbb{C}$ of the field K into $\mathbb{C}$ which leave $\mathbb{Q}$ fixed. Out of these let r of the embeddings be into the reals, say $\tau_1, \ldots, \tau_r : K \to \mathbb{R}$, and let the remaining $2s = n - r$ embeddings be complex. We refer to this pair (r, s) as the *signature* of K. These $2s$ embeddings come in s pairs of complex conjugate non-real embeddings, say $\sigma_j, \bar{\sigma}_j : K \to \mathbb{C}$ for $1 \leq j \leq s$. The following fundamental result shows the correspondence between the archimedean valuations and the embeddings of K into $\mathbb{C}$.

Fact 7 *There are precisely $(r + s)$ infinite places (which we denote by $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{r+s}$ throughout) of a number field K that has signature (r, s) (with $r + 2s = [K : \mathbb{Q}]$). The r infinite places $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ corresponding to the r real embeddings $\tau_1, \ldots, \tau_r$ are given by the (archimedean) valuations $|x|_{\mathfrak{q}_i} \stackrel{\text{def}}{=} |\tau_i(x)|$ for $1 \leq i \leq r$ and the s infinite places $\mathfrak{q}_{r+1}, \ldots, \mathfrak{q}_{r+s}$ corresponding to the s pairs of complex conjugate embeddings σ_j are given by $|x|_{\mathfrak{q}_{r+j}} = |\sigma_j(x)|^2$.* □

We now come to our definition of the size of an element x in a number field K.

Definition 8 [Size]: *Let K be a number field with signature (r, s). Let Let $|\ \ |_{\mathfrak{q}_1}, |\ \ |_{\mathfrak{q}_2}, \ldots, |\ \ |_{\mathfrak{q}_r}$ be the archimedean valuations of x corresponding to the r real embeddings of K, and let $|\ \ |_{\mathfrak{q}_{r+1}}, \ldots, |\ \ |_{\mathfrak{q}_{r+s}}$ be the archimedean valuations of x corresponding to the s complex conjugate embeddings of K. The* size *of an element $x \in K$ is defined as*

$$\mathsf{size}(x) \stackrel{\text{def}}{=} \sum_{i=1}^{r} |x|_{\mathfrak{q}_1} + \sum_{i=1}^{s} 2\sqrt{|x|_{\mathfrak{q}_{r+s}}} \ . \tag{1}$$

The following shows an important property of the above definition of $\mathsf{size}(\cdot)$ (which was lacking in the attempted definition $\mathsf{size}(x) = \|x\|$):

Lemma 9 *Let K be a number field with signature (r, s) and let $a, b \in \mathcal{O}_K$. Then $\mathsf{size}(a - b) \leq \mathsf{size}(a) + \mathsf{size}(b)$.*

Proof: The proof follows from the definition of $\mathsf{size}(x)$ and the (easy to check) facts that $|x - y|_{\mathfrak{q}} \leq |x|_{\mathfrak{q}} + |y|_{\mathfrak{q}}$ for the real infinite places $\mathfrak{q}$ of K, and $\sqrt{|x - y|_{\mathfrak{q}}} \leq \sqrt{|x|_{\mathfrak{q}}} + \sqrt{|y|_{\mathfrak{q}}}$ for the complex (infinite) places of K. □

The following central and important result (see any textbook, eg. [15], for a proof), relates the norm of an element (recall Definition 2) to its size, and is crucial for lower bounding the distance of the our codes.

Proposition 10 *For a number field K and for any element $x \in \mathcal{O}_K$ in its ring of integers, we have*

$$\|x\| = |x|_{\mathfrak{q}_1} \cdot |x|_{\mathfrak{q}_2} \cdots |x|_{\mathfrak{q}_\ell},$$

where $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$ are the archimedean (infinite) places of K.

Using the above, we get the following useful upper bound on $\|x\|$ in terms of $\mathsf{size}(x)$.

Lemma 11 *For a number field K and any $x \in \mathcal{O}_K$, we have $\|x\| \le (\frac{\mathsf{size}(x)}{M})^M$.*

Proof: Let (r, s) be the signature of K. The claimed result follows using Equation (1), Proposition 10 and an application of the AM-GM inequality to the M numbers

$$(|x|_{\mathfrak{q}_1}, \ldots, |x|_{\mathfrak{q}_r}, \sqrt{|x|_{\mathfrak{q}_{r+1}}}, \sqrt{|x|_{\mathfrak{q}_{r+1}}}, \cdots, \sqrt{|x|_{\mathfrak{q}_{r+s}}}, \sqrt{|x|_{\mathfrak{q}_{r+s}}}) \ .$$

The arithmetic mean of these numbers equals $\frac{\mathsf{size}(x)}{M}$ and their geometric mean equals $\|x\|^{1/M}$. $\square$

Corollary 12 *Let K be a number field of degree $[K : \mathbb{Q}] = M$. If $a, b \in \mathcal{O}_K$ are such that $\mathsf{size}(a) \le B$ and $\mathsf{size}(b) \le B$, then $\|a - b\| \le \left(\frac{2B}{M}\right)^M$.*

Proof: By Lemma 9, we have $\mathsf{size}(a - b) \le 2B$, and using Lemma 11, we get $\|a - b\| \le (\frac{2B}{M})^M$. $\square$.

3.3 The code construction

For the rest of this section, let K be a number field of degree $[K : \mathbb{Q}] = M$ and signature (r, s). A number field code (NF-code for short) $\mathcal{C} = \mathcal{C}_K$, based on a number field K, has parameters $(n, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n;\ B)$ where n is the blocklength of the code, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ are distinct (non-zero) prime ideals of $\mathcal{O}_K$, and B is a positive real. The i^{th} position of the code $\mathcal{C}$ is defined over an alphabet of size $\|\mathfrak{p}_i\|$ for $1 \le i \le n$; let us assume w.l.o.g that $\|\mathfrak{p}_1\| \le \|\mathfrak{p}_2\| \le \cdots \le \|\mathfrak{p}_n\|$.

We are now almost in a position to define our code $\mathcal{C} = \mathcal{C}_K$, but for a technical reason that will become clear in Section 3.5, we will need to define the code with one extra "shift" parameter $\mathbf{z} \in \mathbb{R}^r \times \mathbb{C}^s$. Given such a $\mathbf{z} = \langle z_1, z_2, \ldots, z_{r+s}\rangle$ with $z_i \in \mathbb{R}$ for $1 \le i \le r$ and $z_j \in \mathbb{C}$ for $r < j \le r + s$, the $\mathbf{z}$-shifted size $\mathsf{size}_{\mathbf{z}}(x)$ of $x \in \mathcal{O}_K$ is defined as follows. Let $\tau_1, \ldots, \tau_r$ be the embeddings $K \to \mathbb{R}$, and let σ_j, $1 \le j \le s$, be the non-conjugate complex embeddings $K \to \mathbb{C}$. For $i = 1, 2, \ldots, r$, define $a_i^{(x)} = |\tau_i(x) - z_i|$, and for $1 \ge j \le s$, define $b_j^{(x)} = |\sigma_j(x) - z_{r+j}|^2$. (Thus the archimedean valuations are just "shifted" with respect to $\mathbf{z}$.) Now define

$$\mathsf{size}_{\mathbf{z}}(x) = \sum_{i=1}^{r} a_i^{(x)} + \sum_{j=1}^{s} 2\sqrt{b_j^{(x)}} \tag{2}$$

Lemma 13 *Let K be a number field of signature (r, s), with $[K : \mathbb{Q}] = r + 2s = M$, and $\mathbf{z} \in \mathbb{R}^r \times \mathbb{C}^s$. If $a, b \in \mathcal{O}_K$ are such that $\mathsf{size}_{\mathbf{z}}(a) \le B$ and $\mathsf{size}_{\mathbf{z}}(b) \le B$, then $\|a - b\| \le \left(\frac{2B}{M}\right)^M$.*

Proof: One can show, similarly to Lemma 9, that if $\mathsf{size}_{\mathbf{z}}(a) \le B$ and $\mathsf{size}_{\mathbf{z}}(b) \le B$, then $\mathsf{size}(a-b) \le 2B$. The proof then follows using Lemma 11. $\square$

We now formally specify our code construction with the "shift parameter" added in.

Definition 14 *The code $\mathcal{C} = \mathcal{C}_K$ based on a number field K with parameters $(n, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n;\ B;\ \mathbf{z})$ is defined as follows. The message set of $\mathcal{C}$ is $\{m \in \mathcal{O}_K : \mathsf{size}_{\mathbf{z}}(m) \le B\}$. The encoding function is $\mathsf{Enc}_{\mathcal{C}}(m) = \langle m/\mathfrak{p}_1, m/\mathfrak{p}_2, \ldots, m/\mathfrak{p}_n \rangle$.*

Remark: By our definition of size, the message space of our code corresponds to a high-dimensional "octahedron". This is a natural choice since it is amenable to a statement like Lemma 13, and also gives more messages than if we chose, say, a "cube" for the message space.

3.4 Distance of the code

We now estimate the distance of the code. If $\mathsf{Enc}_{\mathcal{C}}(m_1)$ and $\mathsf{Enc}_{\mathcal{C}}(m_2)$ agree in t places, say $1 \le i_1 < i_2 < \cdots < i_t \le n$, then $m_1 - m_2 \in \mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_t}$. By Fact 3 and the ordering of the $\mathfrak{p}_i$'s in increasing order of norm, we get $\|m_1 - m_2\| \ge \prod_{i=1}^{t} \|\mathfrak{p}_i\|$. On the other hand, by Lemma 13, we have $\|m_1 - m_2\| \le (2B/M)^M$. Thus if $\prod_{i=1}^{t} \|\mathfrak{p}_i\| > (2B/M)^M$, then we must have $m_1 = m_2$, and thus two distinct codewords can agree in at most $(t-1)$ places. We have thus shown the following:

Lemma 15 *For a number field code $\mathcal{C} = \mathcal{C}_K$ based on a field K with $[K : \mathbb{Q}] = M$ with parameters $(n, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n;\ B;\ \mathbf{z})$, if t $(1 \le t \le n)$ is such that $\|\mathfrak{p}_1\| \times \|\mathfrak{p}_2\| \cdots \times \|\mathfrak{p}_t\| > (2B/M)^M$, then the distance $d(\mathcal{C})$ of $\mathcal{C}$ is* at least $(n - t + 1)$. *In particular,*

$$d(\mathcal{C}) > n - \frac{M \log(2B/M)}{\log \|\mathfrak{p}_1\|} . \qquad \square$$

3.5 The Rate of the Code

To estimate the rate of the code we need a lower bound (or good estimate) of the number of elements x of $\mathcal{O}_K$ with $\mathsf{size}_{\mathbf{z}}(x) \le B$. The key quantity in such a lower bound is the discriminant of a number field.

Discriminant: Given a number field K of degree M with M embeddings $\zeta_1, \ldots, \zeta_M : K \to \mathbb{C}$, the *discriminant* of any M-tuple of elements $\alpha_1, \ldots, \alpha_M \in K$, denoted $\mathsf{disc}(\alpha_1, \ldots, \alpha_M)$, is defined as the square of the determinant of the $M \times M$ matrix having $\zeta_i(\alpha_j)$ as its $(i,j)^{\text{th}}$ entry. $\mathsf{disc}(\alpha_1, \ldots, \alpha_M) \in \mathbb{Q}$ and if $\alpha_i \in \mathcal{O}_K$, then $\mathsf{disc}(\alpha_1, \ldots, \alpha_M) \in \mathbb{Z}$. The discriminant of K, denoted D_K, is defined as $\mathsf{disc}(\beta_1, \ldots, \beta_M)$ where $\beta_1, \ldots, \beta_M$ is *any* integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$ ($\mathcal{O}_K$ is a free abelian group of rank M and one can show the choice of basis does not matter in the definition of the discriminant). Lastly, the root discriminant of K, denoted rd_K, is defined as $|D_K|^{1/M}$.

Proposition 16 ([9]) *For any number field K with signature (r, s) and discriminant D_K, and any $B \in \mathbb{R}_+$, there exists a $\mathbf{z} \in \mathbb{R}^r \times \mathbb{C}^s$, such that*

$$\Big|\{x \in \mathcal{O}_K : \mathsf{size}_{\mathbf{z}}(x) \le B\}\Big| \ge \frac{2^r \pi^s}{\sqrt{|D_K|}} \frac{B^M}{M!} . \tag{3}$$

Proof: A proof of a similar result appears in [9]; we reproduce the proof here for completeness. The proof uses geometric arguments. Let $M = r + 2s$ be the degree $[K : \mathbb{Q}]$. Consider the mapping $\rho : K \to \mathbb{R}^M$ defined by $\alpha \mapsto (\tau_1(\alpha), \ldots, \tau_r(\alpha), \mathsf{Re}[\sigma_1(\alpha)], \mathsf{Im}[\sigma_1(\alpha)], \ldots, \mathsf{Re}[\sigma_s(\alpha)], \mathsf{Im}[\sigma_s(\alpha)])$. This maps $\mathcal{O}_K$ onto an n-dimensional lattice $\Lambda_{\mathbb{R}}$ whose fundamental parallelotope, denote it by F, has volume $\mathrm{vol}(F) = 2^{-s}\sqrt{|D_K|}$ (cf. [13]). For convenience let us identify $\mathcal{O}_K$ with its image $\Lambda_{\mathbb{R}} \subset \mathbb{R}^M$. The image of the set $S = \{x \in \mathcal{O}_K : \mathsf{size}(x) \le B\}$ under the mapping ρ lies within a set $U \subset \mathbb{R}^M$ where $U = \{(x_1, \ldots, x_M) : |x_1| + \ldots |x_r| + \sum_{i=1}^{s} 2\sqrt{x_{r+2i-1}^2 + x_{r+2i}^2} \le B\}$. The volume of U, $\mathrm{vol}(U)$, equals $2^r(\frac{\pi}{2})^s \frac{B^M}{M!}$ (see for example [13]), and thus we expect roughly $\frac{\mathrm{vol}(U)}{\mathrm{vol}(F)} = \frac{1}{\sqrt{|D_K|}} \cdot 2^r \pi^s \frac{B^M}{M!}$ elements in the set S. However the error term can dominate, and thus we use an averaging argument from [9] by allowing a "shift" $\mathbf{y} \in \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^M$.

Let $\chi : \mathbb{R}^M \to \{0, 1\}$ denote the characteristic function of U. We then have:

$$\begin{aligned}
\int_{\mathbf{y} \in F} |(\mathbf{y} + U) \cap \mathcal{O}_K| d\mathbf{y} &= \sum_{\mathbf{x} \in \mathcal{O}_K} \int_{\mathbf{y} \in F} \chi(\mathbf{x} - \mathbf{y}) d\mathbf{y} = \sum_{\mathbf{x} \in \mathcal{O}_K} \int_{\mathbf{y} \in \mathbf{x} - F} \chi(\mathbf{y}) d\mathbf{y} \\
&= \int_{\mathbf{y} \in \mathbb{R}^M} \chi(\mathbf{y}) d\mathbf{y} = \mathrm{vol}(U) \\
&= \int_{\mathbf{y} \in F} \frac{\mathrm{vol}(U)}{\mathrm{vol(F)}} d\mathbf{y} ,
\end{aligned}$$

where we have used the fact that $\mathbb{R}^M$ is the disjoint union of the sets $\mathbf{x} - F$, for $\mathbf{x} \in \mathcal{O}_K$. Hence there must exist a $\mathbf{y} \in F$ such that $|(\mathbf{y} + U) \cap \mathcal{O}_K| \ge \frac{\mathrm{vol}(U)}{\mathrm{vol(F)}} = \frac{2^r(\pi)^s B^M}{M!\sqrt{|D_K|}}$, as desired. □

The following proposition records the quantitative parameters (rate and distance) of the NF-code construction we gave in Section 3.3. (All logarithms are to the base 2.)

Proposition 17 *Let K be a number field of degree $[K : \mathbb{Q}] = M$ and signature (r, s). Let $\mathcal{C} = \mathcal{C}_K$ be a number field code defined with parameters $(n, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n;\ B;\ \mathbf{z})$ with $\|\mathfrak{p}_1\| \le \cdots \le \|\mathfrak{p}_n\|$. Then there exists a choice of the "shift" $\mathbf{z}$ for which the rate $R(\mathcal{C})$ of $\mathcal{C}$ is at least*

$$\frac{\log(2^r \pi^s B^M) - \log M! - \log\sqrt{|D_K|}}{\log\|\mathfrak{p}_n\|}$$

and the distance $d(\mathcal{C})$ of $\mathcal{C}$ is greater than $n - \frac{M\log(2B/M)}{\log\|\mathfrak{p}_1\|}$. In particular we have

$$R(\mathcal{C}) > \frac{(n-d)\log\|\mathfrak{p}_1\| + s\log(\pi/4) + M\log e - M\log\sqrt{\mathrm{rd}_K} - \log 3M}{\log\|\mathfrak{p}_n\|} .$$

Proof: The proof follows easily from Lemma 15 and Proposition 16, and using Stirling's approximation that $M! \simeq \sqrt{2\pi M}(\frac{M}{e})^M \le 3M(\frac{M}{e})^M$ for all $M \ge 1$. □

4 Constructing an asymptotically good code

By Proposition 17, in order to have good rate, one would like to define codes based on number fields K with small root discriminant rd_K. In addition, in order to define a code of blocklength n over a alphabet of size q, we need $\mathcal{O}_K$ to have n prime ideals of norm at most q. In particular, if one hopes to construct a family of asymptotically good codes over an alphabet of size q based on this approach, then one needs a family of number fields $\{K_n\}$ such that K_n has small root discriminant (the best one can hope for is of the form c for some constant c by existing lower bounds on the discriminant, see the survey [16]) and has $\Omega([K_n : \mathbb{Q}])$ prime ideals of norm at most q. Constructions of sequences of number fields with bounded root discriminant are obtained in the literature using the existence of infinite Hilbert class field towers for some number fields, and we next review some results and terminology from class field theory that will be necessary for our number field constructions.

4.1 Class Fields: Definitions

We will quickly review the basic notation: a finite extension K/k of number fields is (i) *unramified* if no place (including the infinite ones: i.e. real places stay real) of k is ramified in K (this implies $\mathsf{disc}(K/k) = (1)$); (ii) *abelian* if K/k is Galois with abelian Galois group; (iii) a p-extension if K/k is Galois with $[K : k]$ a power of p.

Definition 18 [p-Hilbert class field]: *For any number field k, the maximal unramified abelian extension k^1 of k is known to be finite and is called the* Hilbert class field *(or simply class field) of k. For a prime p, the maximal p-extension of k contained in k^1 is called the* Hilbert p-class field *(or simply p-class field) of k.*

Definition 19 [p-Class field tower]: *For any number field k, the (Hilbert) class field tower of k is the sequence of fields: $k_0 = k$; $k_1 = k^1$ is the class field of k; and for $i \geq 2$, $k_i = (k_{i-1})^1$ is the class field of k_{i-1}. The tower terminates at i if k_i has trivial class group (and thus has as class field k_i itself); the tower is* infinite *if it does not terminate at any i. The p-class field tower of k is defined similarly by repeatedly taking p-class fields starting at k.*

Remark: Each k_i in the tower will be an unramified Galois extension of k but need not be an abelian extension of k.

4.2 Class field towers with specified primes splitting completely

An important property of class field towers (or p-class field towers) is that root discriminant $\mathrm{rd}(k_i)$ remains fixed all the way up the tower (since all extensions are unramified) and thus an infinite tower gives us an infinite sequence of function fields with bounded root discriminant, which is useful for us in constructing an infinite family of good number field codes. But we also need an infinite tower of number fields which have several prime ideals of small norm, and this can be achieved if K has an infinite class field tower in which certain prime ideals of K of small norm that split completely all the way up the tower. To study the existence of such towers we now define the notion of class field towers with the added constraint that a set of specified primes split completely.

Definition 20 [T-decomposing p-Class Field]: *For any number field k and a set of primes T (of $\mathcal{O}_k$), the maximal unramified abelian p-extension of k in which every prime in T splits completely, denoted k_p^T, is called the T-decomposing p-class field of k.*

Definition 21 [T-decomposing p-Class Field Tower]: *For any number field k and a set of primes T, the T-decomposing p-class field tower of k is obtained by repeatedly taking T-decomposing p-class fields: It is the sequence of fields $k_0 = k$, $k_1 = k_p^T$ and for $i \geq 2$, $k_i = (k_{i-1})_p^{T_{i-1}}$, where T_i is the set of primes in k_i lying above T. We say that k has an infinite T-decomposing p-class field tower if*

Our goal is now to find a number field K (with a not too large root discriminant) and a set of primes T of small norm in K, such that K has an infinite T-decomposing p-class field tower. We now review the basic approach behind construction of such class field towers, and will then plug in values to get a specific construction.

4.3 The Construction Approach

The basic approach behind constructing number fields K with infinite class field towers is the Golod-Šafarevič theory [4] (cf. [17]) which gives a sufficient condition for the infinitude of the p-class field tower of a number field based on lower bounds on the p-rank of the ideal class group of K. For our purposes, it suffices to use the following result which gives a specific sufficient condition for quadratic extensions to have infinite 2-class field towers with certain added splitting constraints. This result appears as Corollary 6.2 in [21] and is proved using techniques which also appear in related works like [11, 8].

Proposition 22 ([21]) *Let $P = \{p_1, \ldots, p_s\}$ and $Q = \{q_1, \ldots, q_r\}$ be disjoint sets of primes. Consider a imaginary quadratic extension $K/\mathbb{Q}$ that is ramified exactly at those primes in Q. Let T be the set of primes ideals of $\mathcal{O}_K$ that lie above the primes in P, and let $|T| = t$. Suppose further that*

$$r \geq 3 + t - s + 2\sqrt{2 + t}\,. \tag{4}$$

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

The above is a very useful proposition and we believe plugging in specific values into it will lead to many asymptotically good number field code constructions. In the next two subsections, our aim is to present concrete examples of code constructions based on the above proposition and we therefore focus on a specific setting of parameters which will lead to an asymptotically good code over a reasonably small alphabet.

4.4 Specific Constructions

We now apply Proposition 22 to get a specific construction of a number field with an infinite 2-class field tower.

Lemma 23 *Let $d = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 4849845$, and let $K = \mathbb{Q}(\sqrt{-d})$. Then:*

(i) $\mathrm{rd}_K = \sqrt{4d} \simeq 4404.4727$

(ii) $\mathcal{O}_K$ has a set T of two prime ideals of norm 29.

(iii) K has an infinite T-decomposing 2-class field tower.

Proof: Since $-d \equiv 3 (\mathrm{mod} 4)$, the discriminant of K equals $4d$ (see for example [13]), and thus $\mathrm{rd}_K = \sqrt{|D_K|} = \sqrt{4d}$ proving Part (i). Part (ii) follows since one can check that $-d$ is a quadratic residue modulo 29 and therefore the prime 29 splits into two prime ideals (each of which has norm 29) in the quadratic extension $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$.

To prove Part (iii), note that there are 8 primes (namely those dividing $|D_K| = 4d$) that are ramified in the extension $K/\mathbb{Q}$. Let us apply Proposition 22 to $K/\mathbb{Q}$ with $Q = \{2, 3, 5, 7, 11, 13, 17, 19\}$ and $P = \{29\}$. The prime 29 splits into a set T of two primes in $K/\mathbb{Q}$, we thus have $r = 8$, $s = 1$ and $t = 2$ in Proposition 22. Since these values satisfy Condition (4), we conclude that K has an infinite T-decomposing 2-class field tower. □

4.5 Obtaining an asymptotically good number field code

Let $K_0 = K$ be the number field from the previous section. Let $K_0 \subset K_1 \subset K_2 \subset \cdots$ be the (infinite) T-decomposing 2-class field tower of K_0. We construct a family of codes $\mathcal{C}_n$ based on the number fields K_n below.

Fix an n and let $[K_n : \mathbb{Q}] = M$ (note that M will be a power of 2 but this will not be important for us). Since K_n is totally complex, the signature of K_n is $(0, M/2)$. By Lemma 23, the prime 29 *splits completely* in the extension $K_n/\mathbb{Q}$, and thus $\mathcal{O}_{K_n}$ has M prime ideals, say $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_M$, each of norm 29.

Now consider the code $\mathcal{C}_n$ (defined as in Section 3.3) based on K_n with parameters $(M, \mathfrak{p}_1, \ldots, \mathfrak{p}_M;\ B;\ \mathbf{z})$ where $B = c_0 M$ for some some constant $c_0 > 0$ to be specified later, and $\mathbf{z} \in \mathbb{C}^{M/2}$ is a "shift parameter" as guaranteed by Proposition 16. Now let us analyze the parameters of this code family $\{\mathcal{C}_n\}_{n \geq 0}$. Define the *designed distance* of the code $\mathcal{C}_n$ to be

$$d'(\mathcal{C}_n) = M - \frac{M \log(2c_0)}{\log 29} . \tag{5}$$

Then, by Proposition 17, the distance of the code $d(\mathcal{C}_n)$ is at least $d'(\mathcal{C}_n)$, and the rate of the code $R(\mathcal{C}_n)$ is greater than

$$M - d'(\mathcal{C}_n) - \frac{M}{\log 29} \cdot \log\left(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_{K_n}}{\pi}}\right) - \frac{\log 3M}{\log 29} . \tag{6}$$

Combining Equations (5) and (6) above and using $\mathrm{rd}_{K_n} = \mathrm{rd}_K = 4404.4727$, we obtain, in the limit of large $M \to \infty$,

$$\frac{R(\mathcal{C}_n)}{M} \geq 1 - \frac{d'(\mathcal{C}_n)}{M} - \frac{\log 27.55}{\log 29} > 0.015 - \frac{d'(\mathcal{C}_n)}{M} . \tag{7}$$

Thus if $\frac{d'(\mathcal{C}_n)}{M} \leq 0.015$, we can get asymptotically good codes. By Equation (5) this will be the case if $c_0 > 29^{0.985}/2$, or if $c_0 \geq 13.79$. Also we must have $c_0 < 29/2 = 14.5$ in order to have $d'(\mathcal{C}_n)/M > 0$. By varying c_0 in this range ($13.79 \leq c_0 < 14.5$), we can achieve asymptotically good codes over an alphabet of size 29 for any value of relative distance δ in the range $0 < \delta \leq 0.015$. We have thus proved the following:

Theorem 24 *There exist asymptotically good families of number field codes. In particular, such codes exist over* $\mathrm{GF}(29)$. □

By allowing larger alphabet sizes, we can construct asymptotically codes using class field towers of the above field $\mathbb{Q}(\sqrt{-d})$, for much larger relative distances than the 0.015 we achieve above. In fact, we can get arbitrarily close to the singleton bound $(1 - \delta)$ by picking a sufficiently large alphabet size. Our goal above was mainly to minimize the alphabet size for which we could get asymptotically good number field codes.

4.6 Asymptotically good codes over a smaller alphabet

If we stick to encoding using only prime ideals that lie above a single prime integer, then it appears that reducing the alphabet size further will be difficult (see, however, the remark following Theorem 26). This is because to have an infinite class field tower in which a prime (in $\mathbb{Z}$) splits all the way up, current techniques seem to require ramification of at least 8 places and the resulting discriminant is then at least as large as our choice in Lemma 23, which in turn seems to necessitate an alphabet size of at least 29. However, since NF-codes are not linear in general, there is no reason to avoid codes defined by using prime ideals of different norms, and indeed this way we are able to get asymptotically good codes over an even smaller alphabet (specifically $\mathrm{GF}(19)$). We sketch this construction below.

Lemma 25 *Let* $d' = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 37 \cdot 41$, *and let* $K' = \mathbb{Q}(\sqrt{-d'})$. *Then:*

(i) $\mathrm{rd}_{K'} = \sqrt{4d'} \simeq 246515.72$

(ii) $\mathcal{O}_{K'}$ *has a set* T' *of four prime ideals, two of which lie above* 17 *(and have norm* 17*) and two of which lie above* 19 *(and have norm* 19*).*

(iii) K' *has an infinite* T'*-decomposing* 2*-class field tower.*

Proof: The proof of this result is similar to that of Lemma 23 and uses Propostion 22 with $Q = \{2, 3, 5, 7, 11, 13, 23, 29, 37, 41\}$ and $P = \{17, 19\}$ (so we have $r = 10$, $s = 2$ and $t = 4$, and Condition (4) is satisfied). The details are omitted. □

One can now construct a family of codes from the infinite T'-decomposing 2-class field tower $K'_0 = K' \subset K'_1 \subset K'_2 \subset \dots$ of K', similar to the construction in Section 4.5. The code $\mathcal{C}'_n$ based on K'_n will have parameters $(N, \mathfrak{p}_1, \dots, \mathfrak{p}_M, \mathfrak{q}_1, \dots, \mathfrak{q}_M;\ B;\ \mathbf{z})$. Here the $\mathfrak{p}_i$'s (resp. $\mathfrak{q}_i$'s) are the M primes in K'_n that lie above the prime integer 17 (resp. 19), $N = 2M$ is the blocklength of the code, $B = c'_0 M$ for some some constant $c'_0 > 0$, and $\mathbf{z} \in \mathbb{C}^{M/2}$ is an appropriate "shift parameter". Now using Proposition 17 and arguments similar to those in Section 4.5, we obtain in the limit of large $M \to \infty$,

$$\frac{R(\mathcal{C}'_n)}{M} \geq \Big(1 - \frac{d(\mathcal{C}'_n)}{N}\Big)\frac{\log 17}{\log 19} - \frac{1}{2}\frac{\log\big(\frac{2}{e}\sqrt{\frac{\mathrm{rd}_{K'}}{\pi}}\big)}{\log 19} > \frac{\log 17}{\log 19}\Big(1 - \frac{d(\mathcal{C}'_n)}{N} - \frac{\log 14.5}{\log 17}\Big)\,. \tag{8}$$

Thus we can get asymptotically good codes for any value of relative minimum distance that is at most $(1 - \frac{\log 14.5}{\log 17}) \simeq 0.056$. We therefore conclude the following strengthening of Theorem 24.

Theorem 26 *There exist asymptotically good number field codes over an alphabet of size* 19. □

Remark: One can show a result similar to above using only prime ideals of norm 17 (i.e. no primes of any other norm like the norm 17 primes we used above) *if* one also uses the archimedean places for encoding as in [9]. We do not elaborate on this in detail since we did not discuss how to use archimedean places for encoding, but we just mention the number field upon which this code is based. The field is $\mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29})$ which has an infinite 2-class field tower in which the prime 17 splits completely all the way up the tower. Thus, the alphabet size in Theorem 26 can be brought down slightly to 17 if one uses archimedean places also for the encoding.

4.7 Beating the Gilbert-Varshamov bound: a discussion

Lower bounds on the discriminant of number fields [16] imply that the parameters guaranteed by Proposition 17 are worse than, or at best comparable to, the Gilbert-Varshamov bound (GV bound) *if* we use primes $\mathfrak{p}_1, \dots, \mathfrak{p}_M$ all of the same norm q. Indeed, by Proposition 17, the rate $r = R/n$ and distance $\delta = d/n$ of such codes can at best satisfy $r = 1 - \delta - A/\log_2 q$ for a constant A which is definitely at least 2, and this is weaker than what random codes can achieve. Thus in order to beat the GV bound, one must use primes of varying norms, say in the range $(q/2, q]$ as was done in [9]. Of course, guaranteeing that a number field has an infinite class field tower in which primes of several different small norms all split completely tends to increase its root discriminant very rapidly. We believe that an approach based on Proposition 22 might also yield codes that lie above the GV bound, though the alphabet size in such a construction is likely to be extremely large. It seems to be a tricky task to construct codes over a reasonably small alphabet that lie above the GV bound. Assuming the GRH, it is shown in [9] that, in the limit of large q, NF-codes that beat the GV bound exist, though proving such a result unconditionally appears to be a significant challenge.

5 Concluding Remarks

We should remark that a result similar to the Theorem 24 above also appears in the work of Lenstra [9]. As detailed in the introduction the similar (unconditional) result from [9] also used the infinite places for encoding, and then followed by appealing to the existence of number fields with infinite class field towers (without any "prime splitting" constraints). Our focus was on constructing number field codes within the spirit of other algebraic "ideallic" codes like Reed-Solomon codes, AG codes and Chinese Remainder codes, and investigating how well one can do with such constructions. In addition, we were interested in good codes over a reasonably small alphabet, and indeed we are able achieve this for an alphabet size of 19.

Our work opens up interesting questions in two main directions. One is to investigate whether the decoding paradigm developed in [5, 6] for algebraic codes have efficient implementations for number field codes as well. This line of research will inevitably boil down to tackling some fundamental questions in algorithmic algebraic number theory. [4]

Another direction for future work will be to give improved constructions of number field codes, possibly over even smaller alphabet sizes than we achieve, by investigating other constructions of infinite T-decomposing class field towers. For example, one possibility could be to allow tame ramification at a few places and see if this could lead to an improved version of Proposition 22 and consequently to improved codes (for example, recently Hajir and Maire [7] allowed tame ramification and obtained infinite class field towers with better bounds on the root discriminant than the earlier long standing ones due to Martinet [14]). Also, results on potential limits of the best (smallest) alphabet size one can achieve for asymptotically good codes using this class field tower approach could be interesting. One approach which is useful for such a pursuit is to use the improved lower bounds on the discriminant that are possible if one knows the splitting behavior of small primes [8] (see also the survey by Odlyzko [16] and the pointers therein). This has been used by Lenstra [9] to prove, assuming the GRH, that number field codes *cannot* achieve parameters that are beyond the reach of algebraic-geometric codes.

We conclude with some specific questions: Can one prove unconditionally, without assuming the GRH, that there exist codes that beat the Gilbert-Varshamov bound for a *not too large* alphabet size? If so, what is the smallest alphabet size one can achieve for such a result, and what is the best asymptotic performance one can achieve in the limit of large (but constant) alphabet size?

[4] One point worth mentioning here is that our code constructions, as are the ones in [9], are not "explicit" in the sense that there is an existential "shift" parameter involved in the construction. But we believe it still makes sense to raise algorithmic questions for these codes: we need the non-constructive shift only to get a good lower bound on the rate, and even with a fixed shift, the code is likely to have good rate (even though we do not know how to prove this). And even if the rate of a particular code is not that great, the decoding problem is still a clean algebraic question worth studying!

Acknowledgments

I am extremely grateful to Farshid Hajir for several useful discussions on these topics early on during this work. I thank Amin Shokrollahi for crucial pointers to prior work on number field codes. My sincere thanks to Hendrik Lenstra for bringing to my attention the necessity to use the averaging argument in the proof of Proposition 16, for the suggestion to use the Minkowski "octahedron" and numerous other useful discussions, and for sending me a copy of his paper [9]. I am grateful to Michael Tsfasman and Serge Vlăduţ for pointers to [20, 21] and for sending me a copy of their paper [21] (which was crucial in simplifying some of my asymptotically good code constructions). I would like to thank Andrew Odlyzko and Madhu Sudan for useful discussions.

References

[1] D. Boneh. Finding Smooth integers in short intervals using CRT decoding. *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, Portland, Oregon, May 2000, pp. 265-272.

[2] A. Garcia and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent. Math.*, 121 (1995), pp. 211-222.

[3] O. Goldreich, D. Ron and M. Sudan. Chinese Remaindering with errors. *IEEE Trans. on Information Theory*, to appear. Preliminary version appeared in *Proc. of the 31st Annual ACM Symposium on Theory of Computing*, Atlanta, Georgia, May 1999, pp. 225-234.

[4] E. S. Golod and I. R. Šafarevič. On class field towers. (Russian), Izv. Akad Nauk SSSR, 28 (1964), 261-272; (English translation) Amer. Math. Soc. Transl. Ser 2, 48 (1965), pp. 91-102.

[5] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and Algebraic-geometric codes. *IEEE Trans. on Information Theory*, 45 (1999), pp. 1757-1767.

[6] V. Guruswami, A. Sahai and M. Sudan. "Soft-decision" decoding of Chinese Remainder codes. *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science (FOCS)*, Redondo Beach, California, November 12-14,2000.

[7] F. Hajir and C. Maire. Tamely ramified towers and discriminant bounds for number fields. *Compositio Math.*, to appear.

[8] Y. Ihara. How many primes decompose completely in an infinite unramified Galois extension of a global field? *J. Math. Soc. Japan*, 35 (1983), pp. 693-709.

[9] H. W. Lenstra. Codes from algebraic number fields. In: M. Hazewinkel, J.K. Lenstra, L.G.L.T. Meertens (eds), *Mathematics and computer science II, Fundamental contributions in the Netherlands since 1945*, CWI Monograph 4, pp. 95-104, North-Holland, Amsterdam, 1986.

[10] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-correcting Codes.* North-Holland, Amsterdam, 1981.

[11] C. Maire. Finitude de tours et p-pours T-ramifiées moderées, S-décomposées. *J. de Théorie des Nombres de Bordeaux*, **8** (1996), pp. 47-73.

[12] D. M. Mandelbaum. On a class of arithmetic codes and a decoding algorithm. *IEEE Trans. on Information Theory*, 21 (1976), pp. 85-88.

[13] B. A. Marcus. *Number Fields*. Universitext, Springer-Verlag.

[14] J. Martinet. Tours de corps de classes et estimations de discriminants. *Invent. Math.*, 44 (1978), pp. 65-73.

[15] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften, Volume 322, Springer-Verlag, 1999.

[16] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Séminaire de Théorie des Nombres, Bordeaux*, pp. 1-15, 1989.

[17] P. Roquette. *On class field towers*. In: Algebraic Number Theory (Eds. J.W.S. Cassels, A. Frölich). Acad. Press, 1967, pp. 231-249.

[18] M. A. Shokrollahi and H. Wasserman. List decoding of algebraic-geometric codes. *IEEE Trans. on Information Theory*, Vol. 45, No. 2, March 1999, pp. 432-437.

[19] H. Stichtenoth. *Algebraic Number Fields and Codes*. Springer-Verlag, Berlin, 1993.

[20] M. A. Tsfasman. Global fields, codes and sphere packings. *Journees Arithmetiques 1989, - "Asterisque", 1992*, v.198-199-200, pp.373-396.

[21] M. A. Tsfasman and S. G. Vlădut. *Asymptotic properties of global fields and generalized Brauer-Siegel Theorem*. Preprint IML-98-35 (Marseille), 1998

[22] M. A. Tsfasman, S. G. Vlădut and T. Zink. Modular curves, Shimura curves, and codes better than the Varshamov-Gilbert bound. *Math. Nachrichten*, 109:21-28, 1982.