# MAXIMAL ORDER CODES OVER NUMBER FIELDS

*by*

Christian Maire & Frédérique Oggier

***Abstract.*** — We present constructions of codes obtained from maximal orders over number fields. Particular cases include codes from algebraic number fields by Lenstra and Guruswami, codes from units of the ring of integers of number fields, and codes from both additive and multiplicative structures of maximal orders in central simple division algebras. The parameters of interest are the code rate and the minimum Hamming distance. An asymptotic study reveals several families of asymptotically good codes.

## Contents

## 1. Preliminaries

Given

(i) a number field $\mathbb{K}$ and a maximal order $\Lambda$ defined on $\mathbb{K}$;
(ii) a locally compact group $\mathrm{G}$ and $\mathsf{K}$ a compact of $\mathrm{G}$;
(iii) an embedding $\Psi : \Lambda \hookrightarrow \mathrm{G}$ such that the image $\Psi(\Lambda)$ is a lattice of $\mathrm{G}$, *i.e.* a discrete subgroup with a fundamental domain of finite measure;

**2000** ***Mathematics Subject Classification.*** — 94B40, 11R52, 94B75.

***Key words and phrases.*** — Number Field Codes, Asymptotically Good Codes, Maximal Orders, Units.

(iv) a map $\Theta : \Lambda \to \mathcal{A}(\mathbb{F}_p)^N$ where $\mathcal{A}(\mathbb{F}_p)$ is an alphabet over the finite field $\mathbb{F}_p$, $p$ a prime, and $N \geq 1$ is an integer,

we consider the code $\mathcal{C} = \Theta\Big(\Psi^{-1}(z\mathsf{K} \cap \Psi(\Lambda))\Big)$, for some $z$ in a given fundamental domain of $\Psi(\Lambda)$.

$$\begin{tikzcd}
 & \mathsf{K}, \Psi(\Lambda) \subset \mathrm{G} \\
\Lambda \arrow[ur, hook, bend left, "\Psi"] \arrow[dr, bend right, "\Theta"] & \\
 & \mathcal{C} \subset \mathcal{A}(\mathbb{F}_p)^N
\end{tikzcd}$$

Codewords of the code $\mathcal{C}$ are elements of $\mathcal{A}(\mathbb{F}_p)^N$, and the parameters of interest are

- the rate $\frac{\log_q |\mathcal{C}|}{N}$ of the code, where $q = |\mathcal{A}(\mathbb{F}_p)|$, $N$ is the code length, and $\log_q(x) = \ln x / \ln q$;
- its minimum Hamming distance $d_H(\mathcal{C})$ which counts the minimum number of components in which any two distinct codewords differ.

The goal is to obtain both a high rate and a high minimum distance. The trade-off between both is characterized by the Singleton bound, which for nonlinear codes states that

$$\log_q |\mathcal{C}| \leq N - d_H(\mathcal{C}) + 1.$$

Asymptotically, the relative minimum distance $d_H(\mathcal{C})/N$ is considered, and families of codes $(\mathcal{C}_i)_i$ with length $N_i$ that satisfy

$$\liminf_i \frac{\log_q |\mathcal{C}_i|}{N_i} > 0, \ \liminf_i \frac{d_H(\mathcal{C}_i)}{N_i} > 0,$$

are called *asymptotically good codes*, e.g. [**30**, Chapter I, §1.3]. The alphabet size could more generally be allowed to grow with $i$, though we consider codes for which $q$ is constant, which are of special interest.

A first instance of the above principle is the code construction from algebraic number fields due to Lenstra [**12**] (and rediscovered independently by Guruswami [**3**]). An asymptotic analysis of this code instance was provided in both works, and asymptotically good codes were found.

***Example 1.1***. — [Lenstra [**12**], Guruswami [**3**]] Let $\mathbb{K}$ be a number field of degree $n$ with infinite places $\mathbb{P}_\infty$ and let $\mathcal{O}_\mathbb{K}$ be its ring of integers. Set $\Lambda = \mathcal{O}_\mathbb{K}$. Take $\Psi$ to be the embedding of $\mathbb{K}$ in its archimedean completions, so that $\mathrm{G} = \prod_{\sigma \in \mathbb{P}_\infty} \mathbb{K}_\sigma \simeq \mathbb{R}^n$, and $\Theta$ the reduction modulo $N$ distinct prime ideals of $\mathcal{O}_\mathbb{K}$ above $p$. Then $N \leq n$ and $\mathcal{A}(\mathbb{F}_p)$ is a finite extension of $\mathbb{F}_p$. In particular, $\mathcal{A}(\mathbb{F}_p) = \mathbb{F}_p$ when $N = n$.

***Remark 1.2***. — It is also possible to consider prime ideals above different primes $p$, as done in [**12, 3**], in which case $\Theta$ should be defined using $\prod_p \mathcal{A}(\mathbb{F}_p)$ rather than $\mathcal{A}(\mathbb{F}_p)^N$. This paper focuses on the case where all prime ideals are above the same prime, which is usually more standard[**20**, 1,§1-§2 (vi)] from a coding theory view point, even though the results that will be proven hold in the general case.

A natural extension of Lenstra's construction is the Arakelov construction of Goppa codes from function fields by Nakashima [**17, 18**]. Another extension of Goppa codes to division algebras in the function field situation can be found in a work by Morandi and Sethuraman [**16**]. Neither Nakashima nor Morandi and Sethuraman consider the asymptotic behavior of the codes.

This paper presents a generalization of the work by Lenstra and Guruswami, in the number field case. In particular, our framework gives rise to the following cases, whose details will be given later on in the paper.

***Example 1.3***. — Firstly, we use the multiplicative structure of the ring of integers $\mathcal{O}_{\mathbb{K}}$, where $\mathbb{K}$ is a number field of signature $(r_1, r_2)$. Take $\Lambda$ to be the units of $\mathcal{O}_K$, $\Lambda = \mathcal{O}_{\mathbb{K}}^{\times}$. Then $\Psi$ is the logarithmic embedding of $\mathbb{K}$ in $\mathrm{G} = \mathbb{R}^{r_1+r_2}$ and $\Theta$ is the reduction modulo some prime ideals of $\mathcal{O}_{\mathbb{K}}$ above the prime $p$. The term logarithmic embedding is used by abuse of language, since the kernel of $\Psi$ is finite, given by the roots of unity of $\mathbb{K}$.

Note that the logarithmic embedding of units $\mathcal{O}_{\mathbb{K}}^{\times}$ has been studied to obtain asymptotically good lattices, with respect to density, by Rosenbloom and Tsfasman [**27**].

***Example 1.4***. — Next, we give a construction using the additive structure of a central simple division algebra A of degree $d$ with center $\mathbb{K}$, where $\mathbb{K}$ has degree $n$. Let $\Lambda$ be a maximal $\mathcal{O}_{\mathbb{K}}$-order of A. Take $\Psi$ to be the embedding of A in its archimedean completions and $\Theta$ to be the reduction modulo some prime ideals of $\Lambda$. Then $\mathrm{G} = \prod_{\sigma \in \mathbb{P}_\infty} A_\sigma \simeq \mathbb{R}^{nd^2}$, where $\mathbb{P}_\infty$ is the set of infinite primes of $\mathbb{K}$. We will also focus on the case where all prime ideals of $\Lambda$ are above the same prime $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$, itself above $p$. The alphabet $\mathcal{A}(\mathbb{F}_p)$ is a simple algebra of finite dimension over $\mathcal{O}_K/\mathfrak{p}$, which is itself an extension of $\mathbb{F}_p$.

***Example 1.5***. — Consider the setting of Example 1.4, with $\Lambda$ a maximal order of a central simple division $\mathbb{K}$-algebra A of degree $d$. Consider the group $\Lambda^1$ of elements of $\Lambda$ of reduced norm 1. The map $\Psi$ is the embedding of $\Lambda^1$ in $\mathrm{G} = \prod\limits_{\sigma \in \mathbb{P}_{\mathbb{R}}^0 \cup \mathbb{P}_{\mathbb{C}}} \mathrm{Sl}_d(\mathbb{K}_\sigma)$, where $\mathbb{P}_{\mathbb{C}}$ is the set of complex places, and $\mathbb{P}_{\mathbb{R}}^0$ is the set of real places which do not ramify. As before, the map $\Theta$ corresponds to the reduction modulo some prime ideals of $\Lambda$ above the same prime.

As mentioned above, the code parameters to be studied are the Hamming distance $d_H(\mathcal{C})$ and the relative Hamming distance $d_H(\mathcal{C})/N$ for the asymptotic case, and the code rate $\log_q |\mathcal{C}|/N$. To understand $d_H(\mathcal{C})$ and $d_H(\mathcal{C})/N$, it is needed to study the volume of $\mathsf{K}$ via different norms appearing in G and $\Lambda$ respectively. For $|\mathcal{C}|$, the volume of interest is that of $\mathsf{K} \cap \Psi(\Lambda)$. As explained in [**12**], classical arithmetic estimations are typically not fine enough to guarantee that $\mathcal{C} = \Theta(\Psi^{-1}(\mathsf{K} \cap \Psi(\Lambda)))$ contains enough points. It is then needed to translate the initial code, for which the following lemma is essential.

***Lemma 1.6***. — *Let $G$ be a locally compact group equipped with the Haar measure $\mu$. Let $\Gamma \subset G$ be a lattice and let $\mathcal{D}$ be a fundamental domain respecting the action of $\Gamma$ on $G$. Let $\mathsf{K}$ be a compact of $G$. Then there exists $z \in \mathcal{D}$ such that*

$$\#\Big(z\mathsf{K} \cap \Gamma\Big) \geq \frac{\mu(\mathsf{K})}{\mu(\mathcal{D})}.$$

This lemma is a generalization of a critical point of the proof of Theorem 2.1 by Lenstra [**12**]. We provide a proof for the sake of completeness.

*Proof.* — We recall that a lattice of a locally compact group G is a discrete subgroup with a measurable fundamental domain of finite measure, in which case all fundamental domains are measurable with the same measure. Denote by $\chi$ the characteristic function on $\mathsf{K}$. Then $\mathsf{K} = \dot{\bigcup}_{y\in\Gamma}\Big(y\mathcal{D}\cap\mathsf{K}\Big)$, and

$$\begin{aligned}\mu(\mathsf{K}) &= \sum_{y\in\Gamma}\mu(y\mathcal{D}\cap\mathsf{K})\\ &= \sum_{y\in\Gamma}\int_{z\in\mathcal{D}}\chi(yz)d\mu\\ &= \int_{z\in\mathcal{D}}\sum_{y\in\Gamma}\chi(yz)d\mu\\ &= \int_{z\in\mathcal{D}}\#\Big(\mathsf{K}\cap z\Gamma\Big)d\mu.\end{aligned}$$

But $\mu(\mathsf{K}) = \mu(\mathsf{K})\int_{z\in\mathcal{D}}\frac{1}{\mu(\mathcal{D})}d\mu = \int_{z\in\mathcal{D}}\frac{\mu(\mathsf{K})}{\mu(\mathcal{D})}d\mu.$ Then, assume that for all $z\in\mathcal{D}$, $\#\Big(\mathsf{K}\cap z\Gamma\Big) < \frac{\mu(\mathsf{K})}{\mu(\mathcal{D})}$. As $\#\Big(\mathsf{K}\cap z\Gamma\Big)\in\mathbb{N}$ and $\frac{\mu(\mathsf{K})}{\mu(\mathcal{D})}$ is fixed, there exists $\lambda > 0$ such that for all $z\in\mathcal{D}$, $\frac{\mu(\mathsf{K})}{\mu(\mathcal{D})} - \#\Big(\mathsf{K}\cap z\Gamma\Big)\geq\lambda$. Hence,

$$0 = \int_{z\in\mathcal{D}}\left[\frac{\mu(\mathsf{K})}{\mu(\mathcal{D})} - \#\Big(\mathsf{K}\cap z\Gamma\Big)\right]d\mu \geq \lambda\mu(\mathcal{D}) > 0,$$

a contradiction, and there exists a $z\in\mathcal{D}$ for which

$$\#\Big(\mathsf{K}\cap z\Gamma\Big)\geq\frac{\mu(\mathsf{K})}{\mu(\mathcal{D})}.$$

The claim is then obtained by setting $z = z^{-1}$, since $\#\Big(\mathsf{K}\cap z^{-1}\Gamma\Big) = \#\Big(z\mathsf{K}\cap\Gamma\Big)$. □

For the codes obtained in this paper, the above lemma gives a lower bound $d_H(\mathcal{C})\geq f(t)$, while considerations on the volume of $\mathsf{K}$ lead to a lower bound of the type $\log_q|\mathcal{C}|\geq g(t)$, where $f$ and $g$ depend on the arithmetic context considered, and where $t\in\mathbb{R}_{>0}$ is a variable characterizing the compact $\mathsf{K}$. We will focus on two cases:

**Part I:** The number field case, which includes Example 1.1 for $\Lambda = \mathcal{I}\subset\mathcal{O}_{\mathbb{K}}$ an ideal of $\mathcal{O}_{\mathbb{K}}$, already studied in [**12, 3**] for $\Lambda = \mathcal{O}_{\mathbb{K}}$, and Example 1.3 for $\Lambda = \mathcal{O}_{\mathbb{K}}^{\times}$. For the former situation, with $\mathsf{K} = \mathsf{K}(t)$ a compact of $\mathbb{R}^n$, we get

$$d_H(\mathcal{C})\geq N - n\log_q(2t) + \log_q\mathsf{N}(\mathcal{I})$$

and assuming $N > n\log_q(2t) - \log_q\mathsf{N}(\mathcal{I})$,

$$\frac{\log_q|\mathcal{C}|}{N}\geq\frac{1}{N}\log_q(2^{r_1+r_2}\pi^{r_2}) + \frac{n}{N}\log_q(t) - \frac{1}{N}\log_q\mathsf{N}(\mathcal{I}) - \frac{1}{2N}\log_q|\mathrm{disc}_{\mathbb{K}}|.$$

For the latter, we have instead

$$d_H(\mathcal{C})\geq N - r_1\log_q(1+e^{2t}) - 2r_2\log_q(1+e^t).$$

If moreover $N > n\log_q(2e^{2t})$, then

$$\log_q|\mathcal{C}|\geq\log_q\frac{t^{r_1+r_2}}{2t+1} + \log_q(2^{r_1+r_2}) - \log_q(\mathrm{Reg}_{\mathbb{K}}) - \log_q(r_1+r_2).$$

**Part II:** The maximal order case includes Examples 1.4 and 1.5. In the former case, the additive one, consider a two-sided ideal $\mathcal{I}$ of a maximal order $\Lambda$ in a central simple division algebra A of degree $d$. The ideal $\mathcal{I}$ is chosen disjoint from the primes $\mathfrak{P}_1, \dots, \mathfrak{P}_N$ of $\Lambda$. We have

$$d_H(\mathcal{C}) \geq N - nd^2 \log_q \left(\frac{2t}{d^{1/2}}\right) + \log_q \mathsf{N}(\mathcal{I}).$$

Then assuming that $N + \log_q \mathsf{N}(\mathcal{I}) > nd^2 \log_q \left(\frac{2t}{d^{1/2}}\right)$, we get

$$\log_q |\mathcal{C}| \geq \log_q(\mathbb{V}^{r_1}_{d_2} \mathbb{V}^{r_2}_{2d^2}) + nd^2 \log_q(t) - \log_q \mathsf{N}(\mathcal{I}) - \frac{1}{2} \log_q \Delta_{\mathrm{A}},$$

where $\mathbb{V}_k$ is the volume of the ball of center 0 and radius 1 in $\mathbb{R}^k$, and $\Delta_{\mathrm{A}}$ is the absolute discriminant of A. In the latter multiplicative case, we get

$$d_H(\mathcal{C}) \geq N - \frac{nd}{2}(\log_q(2t||z||_\infty) + \log_q(\sqrt{d})),$$

and assuming that $N > \frac{nd}{2}(\log_q(2t||z||_\infty) + \log_q(\sqrt{d}))$, then

$$\log_q |\mathcal{C}| \geq n \log_q(t) - \log_q \zeta_{\mathbb{K}}(2) - \frac{3}{2} \log_q |\mathrm{disc}_{\mathbb{K}}| - \sum_{\mathfrak{p} \in S_0} (\mathsf{N}\mathfrak{p} - 1),$$

where $S_0$ is the set of finite primes of $\mathcal{O}_K$ that ramify in A, and $\zeta_{\mathbb{K}}$ is the Dedekind zeta function of $\mathbb{K}$. We note the presence of the element $z$ in the lower bound for $d_H(\mathcal{C})$.

For the resulting codes to be interesting, the above lower bounds should be nontrivial, in fact, we need to have ranges for the parameter $t$ such that $f(t) > 0$ and $g(t) > 0$. It turns out that

(i) for $q$ large enough, suitable ranges for $t$ always exist;

(ii) asymptotically, the requirements on the lower bounds become $f(t)/N = f(t, N)/N > 0$ and $g(t)/N = g(t, N) > 0$: in the number field and unit code cases, we let $\mathbb{K} = \mathbb{K}_n$ vary in an asymptotically good tower of extensions to obtain, as desired, families of codes $(\mathcal{C}_n)_n$ such that

$$\liminf_n \frac{1}{[\mathbb{K}_n : \mathbb{Q}]} d_H(\mathcal{C}_n) > 0 \quad \text{and} \quad \liminf_n \frac{1}{[\mathbb{K}_n : \mathbb{Q}]} \log_q |\mathcal{C}_n| > 0.$$

Similarly for additive codes in division algebras, we can associate to an asymptotically good tower of extensions a sequence of division algebras with center in this tower, to obtain asymptotically good codes. Among the four situations discussed above, multiplicative codes in division algebras are different in that one of the lower bound remains a function of $z$. This complicates the asymptotic study of the Hamming distance. Yet the other three situations give rise to families of asymptotically good codes.

## 2. Questions

The following questions are left open:

1. We obtain asymptotically good additive codes over division algebras with a matrix alphabet. The existence of such codes but over a finite field alphabet is open.
2. Asymptotically good multiplicative codes over division algebras are yet to be found.
3. It would be valuable to discuss the tightness of the proposed bounds.

4. The asymptotic case for division algebras over function fields is also an interesting open problem.
5. The decoding of Goppa codes has been well studied, it is natural to wonder whether it can be translated to the scenario considered in this paper. This question seems not easy, the reason behind is that there is no immediate analog for the encoding.

Numerical computations were performed using the softwares GP-Pari [**23**], KASH [**10**] and Octave [**19**].

# PART I<br>NUMBER FIELD CODES

Let $\mathbb{K}$ be a number field of degree $n$ over $\mathbb{Q}$, with signature $(r_1, r_2)$, and $n = r_1 + 2r_2$.

- The set $\mathbb{P}$ of places of $\mathbb{K}$ comprises the subset $\mathbb{P}_\infty$ of infinite places and the subset $\mathbb{P}_0$ of finite places, where $\mathbb{P}_\infty$ contains the $r_1$ embeddings of $\mathbb{K}$ into $\mathbb{R}$ and the $r_2$ embeddings of $\mathbb{K}$ into $\mathbb{C}$.
- Let $\mathcal{O}_\mathbb{K}$ be its ring of integers.
- For $\mathfrak{p}$ a maximal ideal of $\mathcal{O}_\mathbb{K}$, we identify $\mathfrak{p}$ and the place $v$ associated to $\mathfrak{p}$; we denote by $\iota_v : \mathbb{K} \hookrightarrow \mathbb{K}_\mathfrak{p}$ the embedding of $\mathbb{K}$ into its completion $\mathbb{K}_\mathfrak{p}$ (we may also write $\mathbb{K}_v$).
- Similarly, if $v \in \mathbb{P}_\infty$, we denote by $\iota_v$ the embedding of $\mathbb{K}$ into $\mathbb{K}_v$, where $\mathbb{K}_v \simeq \mathbb{R}$ or $\mathbb{K}_v = \mathbb{C}$.
- Let $\text{disc}_\mathbb{K}$ be the discriminant of $\mathbb{K}$ and $\text{rd}_\mathbb{K} = |\text{disc}_\mathbb{K}|^{1/n}$ be its root discriminant.
- Set $r = r_1 + r_2$. By Dirichlet's Unit Theorem, $\mathcal{O}_\mathbb{K}^\times \simeq \mu_\mathbb{K} \times \mathbb{Z}^{r-1}$, where $\mu_\mathbb{K}$ is the group of roots of unity of $\mathbb{K}$.
- Let $\text{Reg}_\mathbb{K}$ be the regulator of $\mathbb{K}$.
- If $x \in \mathcal{O}_\mathbb{K}$, $\mathsf{N}(x)$ denote its absolute norm *i.e.* $\mathsf{N}(x) = \#\mathcal{O}_\mathbb{K}/(x)$. More generally, if $\mathcal{I}$ is an integral ideal of $\mathcal{O}_K$, we have $\mathsf{N}(\mathcal{I}) = \#\mathcal{O}_K/\mathcal{I}$.

## 3. An Arakelov View Point of Number Field Codes

In this section, we recall Lenstra's construction of codes over algebraic number fields [**12**], while rephrasing it using the language of Arakelov divisors, which emphasizes the analogy and differences with the construction of Goppa codes in the context of function fields.

**3.1. Arakelov divisors and geometry of numbers.** — An Arakelov divisor $\mathbb{A}$ of $\mathbb{K}$ is a pair $(\mathcal{I}, (t_\sigma)_\sigma)$, where $\mathcal{I}$ is a fractional ideal of $\mathcal{O}_\mathbb{K}$ and where $\sigma \in \mathbb{P}_\infty$ and $t_\sigma \in \mathbb{R}_{>0}$. We also write the formal sum

$$\mathbb{A} = \sum_{\mathfrak{p} \in \mathbb{P}_0} v_\mathfrak{p}(\mathcal{I}) \cdot \mathfrak{p} + \sum_{\sigma \in \mathbb{P}_\infty} t_\sigma \cdot \sigma$$

where $v_\mathfrak{p}(\mathcal{I}) \in \mathbb{Z}$ is the valuation of $\mathcal{I}$ in $\mathfrak{p}$.

For $x \in \mathcal{O}_\mathbb{K}$, $x \neq 0$, its Arakelov divisor $(x)$ is given by

$$(x) = \sum_{\mathfrak{p} \in \mathbb{P}_0} v_\mathfrak{p}(x) \cdot \mathfrak{p} + \sum_{\sigma \in \mathbb{P}_\infty} -|\sigma(x)| \cdot \sigma,$$

where $(x) = x\mathcal{O}_\mathbb{K}$ is the fractional principal ideal generated by $x$.

***Definition 3.1.*** — Let $\mathbb{A}$ be an Arakelov divisor. Set

$$\mathcal{L}(\mathbb{A}) := \{x \in \mathcal{O}_{\mathbb{K}},\ (x) + \mathbb{A} \geq 0\} \cup \{0\}.$$

The inequality $(x) \geq -\mathbb{A}$ is an inequality between divisors. Thus $x \in \mathcal{L}(\mathbb{A})$ if and only if:

(i) for every prime $\mathfrak{p}$, $v_{\mathfrak{p}}(x) \geq -v_{\mathfrak{p}}(\mathcal{I})$; in particular, $x$ is $\mathfrak{p}$-integral for all $\mathfrak{p} \nmid \mathcal{I}$;

(ii) for every embedding $\sigma \in \mathbb{P}_\infty$, $|\sigma(x)| \leq t_\sigma$.

***Remark 3.2.*** — The set $\mathcal{L}(\mathbb{A})$ is never empty since it contains 0. When considering function fields, for constructing Goppa codes, adding 0 endows $\mathcal{L}(\mathbb{A})$ with a vector space structure, which is not necessarily the case here in the context of number fields. Unlike for curves over finite fields, the set $\mathcal{L}(\mathbb{A})$ loses the property of linearity, failing the formula of Riemann-Roch. It is possible to remedy this by modifying the definition of $\mathcal{L}(\mathbb{A})$ (see [**29**]).

*From now on, we assume that $\mathcal{I}^{-1} = \prod_{i=1}^{t} \mathfrak{p}_i^{-a_i}$, with $a_i < 0$, that $t_\sigma = t$ for every $\sigma \in \mathbb{P}_\infty$, and we consider the Arakelov divisor $\mathbb{A} = (\mathcal{I}^{-1}, (t)_\sigma)$. Then $\mathcal{L}(\mathbb{A})$ is a subset of the integral ideal $\mathcal{I}$.*

Take

$$\Psi : \mathcal{O}_{\mathbb{K}} \to \prod_{v \in \mathbb{P}_\infty} \mathbb{K}_\sigma \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n,$$

the natural embedding. The following is well known.

***Proposition 3.3.*** — *The subgroup $\Psi(\mathcal{I})$ of $\mathbb{R}^n$ is a discrete subgroup of covolume $2^{-r_2}\mathsf{N}(\mathcal{I})\sqrt{|\mathrm{disc}_{\mathbb{K}}|}$, where $\mathsf{N}(\mathcal{I}) = \#\mathcal{O}_{\mathbb{K}}/\mathcal{I}$. As a consequence, the set $\mathcal{L}(\mathbb{A})$ is finite.*

*Proof.* — See e.g. [**11**, Chapter V]. The embedding $\Psi(\mathcal{I})$ of $\mathcal{I}$ into the completions of $\mathbb{K}$ is discrete and thus the intersection of $\Psi(\mathcal{I})$ with any compact of $\mathbb{R}^n$ is finite. □

For $t \in \mathbb{R}_{>0}$, consider the compact $\mathsf{K}(t)$ of $\mathbb{R}^n$ given by

$$\mathsf{K}(t) = \{x \in \prod_{\sigma \in \mathbb{P}_\infty} \mathbb{K}_\sigma,\ |\sigma(x)| \leq t,\ \forall \sigma\}.$$

***Definition 3.4.*** — Let $\mathbb{A} = (\mathcal{I}^{-1}, (t)_\sigma)$ be an Arakelov divisor. Set

$$\mathsf{N}_\infty(\mathbb{A}) = 2^{r_1}\pi^{r_2}t^n.$$

This is the volume of the compact $\mathsf{K}(t)$ of $\mathbb{R}^n$, with respect to the Lebesgue measure.

A classical approach to the geometry of numbers gives a situation where $\mathcal{L}(\mathbb{A})$ contains at least one nonzero element.

***Proposition 3.5.*** — *If $\mathsf{N}_\infty(\mathbb{A}) \geq 2^r\mathsf{N}(\mathcal{I})\sqrt{|\mathrm{disc}_{\mathbb{K}}|}$, the set $\mathcal{L}(\mathbb{A})$ contains at least one nonzero element, with $r = r_1 + r_2$.*

*Proof.* — This is a consequence of the well known Minkowski Theorem, see e.g. [**11**, Chapter V]. □

This is where we use the extension of Lenstra's result, Lemma 1.6, which shows that if we translate the compact bounded by $\mathsf{N}_\infty(\mathbb{A})$, then $\mathcal{L}(\mathbb{A})$ contains at least $\frac{2^{r_2}\mathsf{N}_\infty(\mathbb{A})}{\mathsf{N}(\mathcal{I})\sqrt{|\mathrm{disc}_{\mathbb{K}}|}}$ elements.

***Proposition 3.6* (Lenstra).** — *Let $\mathcal{D}$ be a fundamental domain of $\Psi(\mathcal{I})$. There exists a $z \in \mathcal{D}$ such that $z + \mathsf{K}(t)$ contains at least $\frac{2^{r_2}\mathsf{N}_\infty(\mathbb{A})}{\mathsf{N}(\mathcal{I})\sqrt{|\mathrm{disc}_\mathbb{K}|}}$ elements of $\Psi(\mathcal{I})$. Such a $z$ is said $\mathbb{A}$-admissible.*

*Proof.* — This is Lemma 1.6 applied to our situation. □

***Definition 3.7.*** — For $z \in \mathbb{R}^n$, set $\mathcal{L}_z(\mathbb{A}) = \Psi^{-1}(z + \mathsf{K}(t)) \cap \mathcal{I}$.

***Remark 3.8.*** — As $\Psi$ is an embedding,

$$\Psi^{-1}((z + \mathsf{K}(t)) \cap \Psi(\mathcal{I})) = \Psi^{-1}(z + \mathsf{K}(t)) \cap \Psi^{-1}(\Psi(\mathcal{I})) = \Psi^{-1}(z + \mathsf{K}(t)) \cap \mathcal{I}.$$

**3.2. The code construction.** — Let $\mathcal{I}$ be an ideal of $\mathcal{O}_\mathbb{K}$ and let $T = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$ be a set of prime ideals of $\mathcal{O}_\mathbb{K}$, disjoint from $\mathcal{I}$. Consider

$$\Theta : \mathcal{O}_\mathbb{K} \to \prod_{i=1}^{N} \mathcal{O}_\mathbb{K}/\mathfrak{p}_i,\ x \mapsto (x \bmod \mathfrak{p}_1, \dots, x \bmod \mathfrak{p}_N).$$

As motivated in Remark 1.2, we assume that for $i = 1, \dots, N$, $\#\mathcal{O}_\mathbb{K}/\mathfrak{p}_i = q$, $q$ a power of some $p$.

Number field codes follow the principle given in the introduction:

$$\begin{tikzcd}
 & \mathrm{G} = \prod_{\sigma\in\mathbb{P}_\infty} \mathbb{K}_\sigma \simeq \mathbb{R}^n \\
\mathcal{O}_\mathbb{K} \arrow[ur, "\Psi"] \arrow[dr, "\Theta"'] & \\
 & \mathcal{A}(\mathbb{F}_p)^N = \prod_{\mathfrak{p}\in T} \mathcal{O}_\mathbb{K}/\mathfrak{p}
\end{tikzcd}$$

***Definition 3.9.*** — Suppose $z$ is $\mathbb{A}$-admissible for the Arakelov divisor $\mathbb{A}$. Set $\mathsf{K}_z(t) = z + \mathsf{K}(t)$. The number field code $\mathcal{C}_z(\mathbb{A})$ is obtained by

$$\mathcal{C}_z(\mathbb{A}) = \Theta\Big(\Psi^{-1}(\mathsf{K}_z(t)) \cap \mathcal{I}\Big) = \Theta(\mathcal{L}_z(\mathbb{A})).$$

When $I = \mathcal{O}_\mathbb{K}$, the code is said to be *integral*, which corresponds to the context of Lenstra and Guruswami.

**3.3. The parameters.** — We consider the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C} = \mathcal{C}_z(\mathbb{A})$ first.

***Proposition 3.10.*** — *For the number field code $\mathcal{C} = \Theta\Big(\Psi^{-1}(\mathsf{K}_z(t)) \cap \mathcal{I}\Big)$ of length $N$ constructed above as a subset of $\mathbb{F}_q^N$, its minimum distance $d_H(\mathcal{C})$ satisfies*

$$d_H(\mathcal{C}) \geq N - n\log_q(2t) + \log_q \mathsf{N}(\mathcal{I}).$$

*Proof.* — Take two distinct codewords which agree on the largest number $|I|$ of components, then by the surjectivity of $\Theta$, their difference has a preimage $y \in \mathcal{I}$ such that $y \in \bigcap_{i\in I} \mathfrak{p}_i = \prod_{i\in I} \mathfrak{p}_i$; $y \neq 0$. Hence $y \in \mathcal{J} := \mathcal{I}\prod_{i\in I}\mathfrak{p}_i$. But $\mathcal{O}_{\mathbb{K}}/(y) \twoheadrightarrow \mathcal{O}_{\mathbb{K}}/\mathcal{J}$ and $\#\mathcal{O}_{\mathbb{K}}/(y) \geq \#\mathcal{O}_{\mathbb{K}}/\mathcal{J}$. Then

$$\#\mathcal{O}_{\mathbb{K}}/\mathcal{J} = \mathsf{N}(\mathcal{I})\prod_{i\in I}\mathsf{N}(\mathfrak{p}_i) = \mathsf{N}(\mathcal{I})q^{|I|}$$

and $\#\mathcal{O}_{\mathbb{K}}/(y) = \mathsf{N}(y)$. Since $|I| = N - d_H(\mathcal{C})$, it follows that

$$N - d_H(\mathcal{C}) \leq \log_q \mathsf{N}(y) - \log_q \mathsf{N}(\mathcal{I}).$$

But for every $\sigma \in \mathbb{P}_\infty$, and for $x$, $x'$ the respective preimages of the two codewords at minimum distance,

$$|\sigma(y)| = |\sigma(x) - \sigma(x')| = |\sigma(x) - z_\sigma - \sigma(x') + z_\sigma| \leq |\sigma(x) - z_\sigma| + |\sigma(x') - z_\sigma| \leq 2t,$$

where $z = (z_\sigma)_\sigma \in G$, and consequently $\mathsf{N}(y) \leq (2t)^n$. □

***Corollary 3.11***. — *Let $\mathcal{C}_z(\mathbb{A})$ be a number field code as constructed above. If $N > n\log_q(2t) - \log_q \mathsf{N}(\mathcal{I})$, then $\Theta_{|\mathcal{L}_z(\mathbb{A})}$ is injective.*

*Proof.* — If $x \neq x'$, with $x, x' \in \mathcal{L}_z(\mathbb{A})$, then $d_H(\Theta(x), \Theta(x')) \geq d_H(\mathcal{C}) > 0$. □

Under the injectivity hypothesis, one has:

***Proposition 3.12***. — *Let $\mathcal{C} = \mathcal{C}_z(\mathbb{A})$ be an Arakelov code. Assume that $N > n\log_q(2t) - \log_q \mathsf{N}(\mathcal{I})$. Then*

$$\frac{\log_q |\mathcal{C}|}{N} \geq \frac{1}{N}\log_q(2^r\pi^{r_2}) + \frac{n}{N}\log_q(t) - \frac{1}{N}\log_q \mathsf{N}(\mathcal{I}) - \frac{n}{2N}\log_q \mathrm{rd}_{\mathbb{K}},$$

*where $r = r_1 + r_2$.*

*Proof.* — Indeed, in this case the map $\Theta_{|\mathcal{L}_z(\mathbb{A})}$ is injective. Then, the lower bound for $\log_q(\mathcal{C})$ results from Proposition 3.6. □

Number field code constructions have been proposed to obtain asymptotically good codes, which we will discuss in Section 5.

## 4. Unit Codes

**4.1. The code construction.** — Let us start with a number field $\mathbb{K}$ of degree $n = r_1 + 2r_2$. Let $\mathcal{O}_{\mathbb{K}}$ be its ring of integers and let $\mathcal{O}_{\mathbb{K}}^\times$ be the group of units of $\mathcal{O}_{\mathbb{K}}$. We write $\mathbb{P}_{\mathbb{C}}$ for the infinite complex places. By Dirichlet's Unit Theorem, $\mathcal{O}_{\mathbb{K}}^\times \simeq \mu_{\mathbb{K}} \times \mathbb{Z}^{r_1+r_2-1}$, where $\mu_{\mathbb{K}}$ it the roots of unity in $\mathbb{K}$ showing that $\mathcal{O}_{\mathbb{K}}^\times$ is a lattice. Let us be more precise. Set $r = r_1 + r_2$. Let

$$\begin{array}{rcl} \Psi : \mathcal{O}_{\mathbb{K}}^\times & \longrightarrow & \mathbb{R}^r \\ \varepsilon & \mapsto & (\delta_\sigma \log|\sigma(\varepsilon)|)_\sigma \end{array}$$

where $\sigma \in \mathbb{P}_\infty$ and where $\delta_\sigma = 2$ if $\sigma \in \mathbb{P}_{\mathbb{C}}$ and 1 otherwise. The homomorphism $\Psi$ is called the logarithmic embedding by abuse of language, since its kernel $\mu_{\mathbb{K}}$ is finite. This does not prevent this situation to fit our general framework.

Set $\mathbb{H}_0 = \Psi(\mathcal{O}_{\mathbb{K}}^\times)$ and take a $\mathbb{Z}$-basis $(\varepsilon_i)_{i=1,\cdots,r-1}$ of $\mathcal{O}_{\mathbb{K}}^\times$ (mod $\mu_{\mathbb{K}}$). Consider the lattice $\mathbb{H}$ of $\mathbb{R}^r$

$$\mathbb{H} := \mathbb{Z}x_0 \oplus \Big(\bigoplus_i \mathbb{Z}\Psi(\varepsilon_i)\Big) = \mathbb{Z}x_0 \oplus \mathbb{H}_0 \ \subset\ \mathbb{R}^r,$$

where $x_0 = (1, \dots, 1, \dots, 1)$. Then $x_0$ is orthogonal to $\mathbb{H}_0$.

***Proposition 4.1.*** — *$\mathbb{H}$ is a lattice of $\mathbb{R}^r$ of covolume $\mu(\mathbb{R}^r/\mathbb{H}) = r$ $\mathrm{Reg}_{\mathbb{K}}$, where $\mathrm{Reg}_{\mathbb{K}}$ is the regulator of the number field $\mathbb{K}$.*

*Proof.* — It is an easy computation. □

Let us restrict the map $\Psi$ to $\Lambda := \langle \varepsilon_1, \cdots, \varepsilon_{r-1} \rangle$ and consider the map $\Psi_\Lambda : \Lambda \to \mathbb{H}_0$, $\varepsilon \mapsto \Psi(\varepsilon)$, which is then an isomorphism of groups.
Consider the projection map: $\mathrm{Pr}_{\mathbb{H}_0} : \mathbb{H} \to \mathbb{H}_0$.

Now for $t \in \mathbb{R}_{>0}$, take the compact $\mathsf{K}(t)$ of $\mathbb{R}^r$ defined by

$$\mathsf{K}(t) = \{x \in \prod_{\sigma \in \mathbb{P}_\infty} \mathbb{K}_\sigma,\ |\sigma(x)| \le t,\ \forall \sigma\},$$

of volume $\mu(\mathsf{K}(t)) = (2t)^r$ (when taking the Lebesgue measure).

Similarly to the additive situation, the question is to estimate $\#(\mathbb{H} \cap \mathsf{K}_z(t))$. Let $\mathcal{D}$ be a fundamental domain of $\mathbb{H}$. By Lemma 1.6, there exists a $z \in \mathcal{D}$ such that

$$\#(\mathsf{K}_z(t) \cap \mathbb{H}) \ge \frac{\mu(\mathsf{K}(t))}{\mu(\mathbb{R}^r/\mathbb{H})} = \frac{2^r t^r}{r\mathrm{Reg}_{\mathbb{K}}}$$

where $\mathsf{K}_z(t) = (z + \mathsf{K}(t))$.

***Definition 4.2.*** — Set $\mathbb{H}_{0,z}(t) = \mathrm{Pr}_{\mathbb{H}_0}\Big(\mathsf{K}_z(t) \cap \mathbb{H}\Big)$.

***Lemma 4.3.*** — *One has $\#\Psi_\Lambda^{-1}\Big(\mathbb{H}_{0,z}(t)\Big) \ge \dfrac{2^r t^r}{(2t+1)r\mathrm{Reg}_{\mathbb{K}}}$.*

*Proof.* — Take $x_1, x_2 \in \mathsf{K}_z(t) \cap \mathbb{H}$ such that $\mathrm{Pr}_{\mathbb{H}_0}(x_1) = \mathrm{Pr}_{\mathbb{H}_0}(x_2)$. Write $x_i = \lambda_i x_0 + y$ with $y \in \mathbb{H}_0$, $\lambda_i \in \mathbb{Z}$, $i = 1, 2$. Then $|\lambda_1 - \lambda_2| \le 2t$. Now as $\lambda_i$ are integers, then given $x \in \mathsf{K}_z(t)$, there are at most $(2t+1)$ elements $x'$ in $\mathsf{K}_z(t)$ such that $\mathrm{Pr}_{\mathbb{H}_0}(x) = \mathrm{Pr}_{\mathbb{H}_0}(x')$. Thus

$$\#\Psi_\Lambda^{-1}\Big(\mathbb{H}_{0,z}(t)\Big) \ge \frac{\#\Big(\mathsf{K}_z(t) \cap \mathbb{H}\Big)}{2t+1} \ge \frac{2^r t^r}{(2t+1)r\mathrm{Reg}_{\mathbb{K}}}.$$

□

Let $T = \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$ be a set of prime ideals of $\mathcal{O}_{\mathbb{K}}$. Consider $\Theta$ the reduction map

$$\Theta : \mathcal{O}_{\mathbb{K}}^\times \to \prod_{i=1}^{N} \mathcal{O}_{\mathbb{K}}/\mathfrak{p}_i,\ x \mapsto (x \bmod \mathfrak{p}_1, \dots, x \bmod \mathfrak{p}_N).$$

***Definition 4.4.*** — The unit code $\mathcal{C}_{z,t}(\mathcal{O}_{\mathbb{K}}^\times)$ of the number field $\mathbb{K}$ is the code

$$\Theta\Big(\Psi_\Lambda^{-1}\Big(\mathbb{H}_{0,z}(t)\Big)\Big).$$

$$\begin{tikzcd} & \mathrm{G} = \mathbb{R}^r \\ \Lambda \subset \mathcal{O}_K^\times \arrow[ur, bend left, "\Psi"] \arrow[dr, bend right, "\Theta"] & \\ & \mathcal{A}(\mathbb{F}_p)^N = \prod_{\mathfrak{p}\in T} \mathcal{O}_\mathbb{K}/\mathfrak{p} \end{tikzcd}$$

**4.2. The parameters.** — We bound the minimum distance $d_H(\mathcal{C}_{z,t}(\mathcal{O}_\mathbb{K}^\times))$ and the rate $\log_q \mathcal{C}_{z,t}(\mathcal{O}_\mathbb{K}^\times)/N$. We start with an observation.

***Lemma 4.5.*** — *For $\varepsilon$ and $\varepsilon'$ in $\Psi_\Lambda^{-1}\Big(\mathrm{Pr}_{\mathbb{H}_0}(\mathsf{K}_z(t))\Big)$ one has:*

$$e^{-2t/\delta_\sigma} \leq \left|\frac{\sigma(\varepsilon)}{\sigma(\varepsilon')}\right| \leq e^{2t/\delta_\sigma}$$

*and*

$$\Big|\mathsf{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon - \varepsilon')\Big| \leq (1+e^{2t})^{r_1}(1+e^t)^{2r_2}.$$

*Proof.* — Let us write $\Psi_\Lambda(\varepsilon) = (a_1, \cdots, a_r)$ and $\Psi_\Lambda(\varepsilon') = (a'_1, \cdots, a'_r)$. Then $a_1 + \cdots + a_r = 0 = a'_1 + \cdots + a'_r$. Now there exist $\lambda, \lambda' \in \mathbb{Z}$ such that $x = \lambda x_0 + \Psi_\Lambda(\varepsilon) \in \mathsf{K}_z(t)$ and $x' = \lambda' x_0 + \Psi_\Lambda(\varepsilon') \in \mathsf{K}_z(t)$. Hence, $-t \leq \lambda - \lambda' + (a_i - a'_i) \leq t$ for all $i = 1, \cdots, r$. After summing for $i = 1$ to $r$, one obtains $-rt \leq r(\lambda - \lambda') \leq rt$ and then $|\lambda - \lambda'| \leq t$. Then

$$|a_i - a'_i| \leq |\lambda - \lambda' - (a_i - a'_i)| + |\lambda - \lambda'| \leq 2t.$$

One concludes thanks to the fact that $a_i = \delta_\sigma \log(\sigma(\varepsilon))$ for $\sigma \in \mathbb{P}_\infty$. Hence

$$\begin{aligned} \Big|\mathsf{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon - \varepsilon')\Big| &= \prod_{\sigma\in\mathbb{P}_\infty} \Big|\sigma(\varepsilon) - \sigma(\varepsilon')\Big|^{\delta_\sigma} \\ &= \prod_{\sigma\in\mathbb{P}_\infty} |\sigma(\varepsilon)|^{\delta_\sigma}\Big|1 - \sigma(\varepsilon')/\sigma(\varepsilon)\Big|^{\delta_\sigma} \leq (1+e^{2t})^{r_1}(1+e^t)^{2r_2}. \end{aligned}$$

□

Following the computations of Section 3.3, one obtains:

***Proposition 4.6.*** — *First*

$$d_H(\mathcal{C}_{z,t}(\mathcal{O}_\mathbb{K}^\times)) \geq N - r_1 \log_q(1+e^{2t}) - 2r_2 \log_q(1+e^t) \geq N - n\log_q(2e^{2t}).$$

*If moreover $N > n\log_q(2e^{2t})$, then*

$$\log_q |\mathcal{C}_{z,t}(\mathcal{O}_\mathbb{K}^\times)| \geq \log_q \frac{t^r}{2t+1} + \log_q(2^r) - \log_q(\mathrm{Reg}_\mathbb{K}) - \log_q r.$$

Note that

$$N > n\log_q(2e^{2t}) \iff \tfrac{1}{2}\Big((\ln q)\tfrac{N}{n} - \ln 2\Big) > t$$

for which a range of $t > 0$ always exists, by letting $q$ grow as needed. Furthermore, for the second lower bound to be nontrivial, we need

$$\log_q \tfrac{t^r}{2t+1} + \log_q(2^r) > \log_q \mathrm{Reg}_\mathbb{K} - \log_q r,$$

or equivalently

$$\ln \tfrac{t^r}{2t+1} + \ln(2^r) > \ln \mathrm{Reg}_{\mathbb{K}} - \ln r$$

and for $n > 1$, it is always possible to find a range of suitable $t$.

***Example 4.7***. — For number fields of degree $n = 8$, Proposition 4.6 gives the condition

$$\tfrac{1}{2}\left((\ln q)\tfrac{N}{8} - \ln 2\right) > t.$$

For a code of length $N = 8$, we need a prime that splits, in which case $q = p$. Alternatively, a code of length $N = 4$ can be obtained by considering a prime that splits into only four factors, with $q = p^2$. In both cases, the above condition becomes

$$\tfrac{1}{2}(\ln p - \ln 2) > t.$$

For $p = 541$, we get $t < 2.8001$ while for $p = 569$, we get $t < 2.8253$.

- Consider the totally complex number field $\mathbb{K}_1$ given by the polynomial $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$, with discriminant $\mathrm{disc}_{\mathbb{K}_1} = 3^4 \cdot 5^6$ and regulator $\mathrm{Reg}_{\mathbb{K}_1} = 4.661820$. This is a cyclotomic field, with a primitive 15th root of unity. Since $541 \equiv 1 \pmod{15}$, 541 splits in $\mathbb{K}_1$, and we have
$$541\mathcal{O}_{\mathbb{K}_1} = \prod_{i=1}^{8} \mathfrak{p}_i,\ 569\mathcal{O}_{\mathbb{K}_1} = \prod_{i=1}^{4} \mathfrak{q}_i.$$
- Consider the totally real number field $\mathbb{K}_2$ given by the polynomial $x^8 - 7x^6 + 14x^4 - 8x^2 + 1$, with discriminant $\mathrm{disc}_{\mathbb{K}_2} = 2^8 \cdot 3^4 \cdot 5^6$ and regulator $\mathrm{Reg}_{\mathbb{K}_2} = 24.388406$. We have
$$541\mathcal{O}_{\mathbb{K}_2} = \prod_{i=1}^{8} \mathfrak{p}_i,\ 569\mathcal{O}_{\mathbb{K}_2} = \prod_{i=1}^{4} \mathfrak{q}_i.$$

The lower bounds are shown in Figure 1, for $n = N = 8$ and values of $t$ varying between 1.4 and 2.8.

## 5. Asymptotic Code Behavior

We will address the design of asymptotically good unit codes, defined in Section 4. For asymptotically good number field codes (see Section 3), we refer to the works by Lenstra [**12**] and by Guruswami [**3**]. We will also consider the Singleton bound asymptotically.

The asymptotic study considered relies on the study of infinite extensions of number fields, in which root discriminants are bounded. When the extension is not ramified, the root discriminant is constant.
As noted in [**5**], the question of the nature of ramification in such extensions is linked to a deep conjecture of arithmetic geometry (the 5a conjecture) by Fontaine-Mazur.

### 5.1. Background on Number Field Towers.

— There is an abundant literature on infinite number field towers, e.g. [**26**], [**15**], [**28**], [**31**], [**6**], [**7**], [**14**].
We introduce now some basic notations concerning towers of number fields (see [**31**]).

***Definition 5.1***. — A sequence $(\mathbb{K}_n)_n$, $n \in \mathbb{N} \cup \{0\}$, of number fields, where $\mathbb{K}_0 = \mathbb{K}$, is called a tower of $\mathbb{K}$ if for all $n$, $\mathbb{K}_n \subsetneq \mathbb{K}_{n+1}$ so in particular $[\mathbb{K}_n : \mathbb{K}] \to \infty$ with $n$.

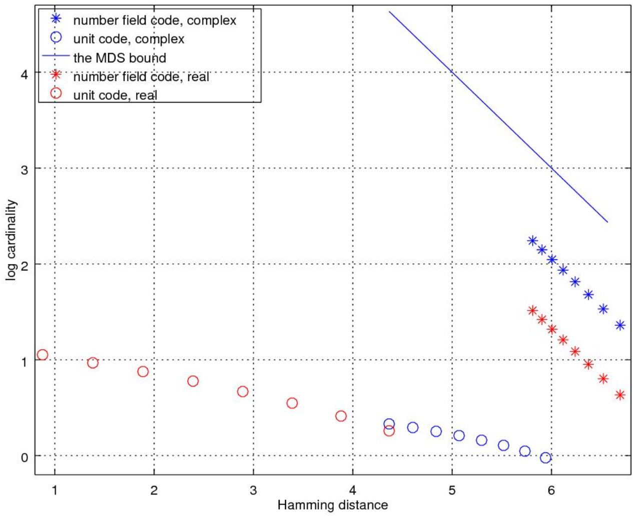

FIGURE 1. The trade-off between the lower bound on $d_H(\mathcal{C})$ and $\log_q(|\mathcal{C}|)$ are shown. The Singleton bound characterizes the optimal trade-off between $d_H(\mathcal{C})$ and $\log_q(|\mathcal{C}|)$, which corresponds to the maximum distance separable (MDS) case, shown as a reference.

Assuming *GRH* in a tower $\mathbb{L} = \bigcup_n \mathbb{K}_n$ of $\mathbb{K}$ means that every field in the tower satisfies its corresponding *Generalized Riemann Hypothesis*.
Then given a tower $(\mathbb{K}_n)_n$, set:

- $g_n = g_{\mathbb{K}_n} = \ln(\sqrt{|\mathrm{disc}(\mathbb{K}_n)|})$;
- $\mathsf{h}_n = |\mathrm{Cl}(\mathbb{K}_n)|$ the class number of $\mathbb{K}_n$;
- $\mathrm{Reg}_n = \mathrm{Reg}_{\mathbb{K}_n}$ the regulator of $\mathbb{K}_n$.

***Definition 5.2***. — Let $\mathbb{K}$ be a number field and let $\mathbb{L}/\mathbb{K}$ be an infinite algebraic extension (the real places remain real). Let $(\mathbb{K}_n)_n$ be a tower of number fields of $\mathbb{K}$ such that $\bigcup\limits_n \mathbb{K}_n = \mathbb{L}$. Set $\mathrm{rd}_{\mathbb{L}} := \limsup\limits_n \{\mathrm{rd}_{\mathbb{K}_n}\}$. The quantity $\mathrm{rd}_{\mathbb{L}}$ does not depend on the choice of $(\mathbb{K}_n)_n$. The extension $\mathbb{L}/\mathbb{K}$ is said to be asymptotically good if the quantity $\mathrm{rd}_{\mathbb{L}}$ is finite.

Let $p$ be a prime number. The $p$-towers of class fields provide natural examples of asymptotically good extensions. More precisely, let $\Sigma$ and $T$ be two finite sets of finite places of $\mathbb{K}$, with $T \cap \Sigma = \emptyset$. Let $\mathbb{K}_\Sigma^T/\mathbb{K}$ be the maximal pro-$p$-extension of $\mathbb{K}$ which is not ramified outside $\Sigma$ and totally split in the places of $T$ (the real places remain real). The extensions $\mathbb{K}_\Sigma^T/\mathbb{K}$ have been studied by numerous authors, see [**2**] for a tentatively exhaustive survey.
The following proposition is well known.

***Proposition 5.3***. — *If $(\Sigma, p) = 1$ and if $\mathbb{K}_\Sigma^T/\mathbb{K}$ is infinite, then $\mathbb{K}_\Sigma^T/\mathbb{K}$ is asymptotically good:*

$$\mathrm{rd}_{\mathbb{K}} \leq \mathrm{rd}_{\mathbb{K}_\Sigma^T} \leq \mathrm{rd}_{\mathbb{K}} \Big( \prod_{\mathfrak{p} \in \Sigma} \mathsf{N}(\mathfrak{p}) \Big)^{1/[\mathbb{K}:\mathbb{Q}]}.$$

*Furthermore, if $\Sigma = \emptyset$, then $\mathrm{rd}_{\mathbb{K}_\emptyset^T} = \mathrm{rd}_{\mathbb{K}}$.*

*Proof.* — This is a local computation, well known when $\Sigma = \emptyset$. For the general case, see e.g. [**7**] or [**14**]. □

When $\Sigma = \emptyset$, we say that the tower $\mathbb{K}_\emptyset^T$ is not ramified. This is the seminal case, see the article by Martinet [**15**].

Set $\mathrm{G}_\Sigma^T = \mathrm{Gal}(\mathbb{K}_\Sigma^T/K)$. Class field theory gives information on the maximal abelian quotient $\mathrm{G}_\Sigma^{T,ab}$ of the pro-$p$ group $\mathrm{G}_\Sigma^T$:

$$\mathrm{G}_\Sigma^{T,ab} \simeq \mathrm{Cl}_{\Sigma,p}^T(\mathbb{K}),$$

where $\mathrm{Cl}_{\Sigma,p}^T(\mathbb{K})$ is the $p$-Sylow of the $T$-class group of $\mathbb{K}$, for a given ray built over $\Sigma$ (the isomorphism is given by Artin's symbol [**2**]). When $\Sigma = \emptyset$, $\mathrm{Cl}_{\emptyset,p}^T = \mathrm{Cl}_p^T(\mathbb{K})$ is the $p$-Sylow of the $T$-class group of $\mathbb{K}$ which is by definition the $p$-Sylow of the quotient of the class group $\mathrm{Cl}(\mathbb{K})$ of $\mathbb{K}$ by the classes generated by $T$.

*5.1.1. Criteria.* — To simplify, we only consider unramified towers. For towers with ramification, see e.g. [**7**], [**6**], [**14**]. The Golod- Shafarevich Theorem [**26**] guarantees the existence of asymptotically good $p$-towers.

If $p$ is a prime number and $A$ an abelian $p$-group, we denote by $d_pA$ the $p$-rank of $A$ *i.e.*, $d_pA = \dim_{\mathbb{F}_p} A/A^p$.

***Theorem 5.4***. — *Let $p$ be a prime number. Set $\delta_{\mathbb{K},p} = 1$ if $\mathbb{K}$ contains pth roots of unity, 0 else. Let $\mathbb{K}/\mathbb{K}_0$ be a cyclic extension of degree $p$. If*

$$d_p\mathrm{Cl}_p^T \geq 2 + 2\sqrt{r_1 + r_2 + |T| + \delta_{\mathbb{K},p}},$$

*then the extension $\mathbb{K}_\emptyset^T/\mathbb{K}$ is infinite.*

*Proof.* — See e.g. [**14**]. □

This results, together with a result of genus theory, lead to:

***Corollary 5.5***. — *Let $\mathbb{K}/\mathbb{K}_0$ be a cyclic extension of degree $p$. Let $\rho$ be the number of places finite or not) of $\mathbb{K}_0$ which ramify in $\mathbb{K}/\mathbb{K}_0$. If*

$$\rho \geq 2 + r_1(\mathbb{K}_0) + r_2(\mathbb{K}_0) + |T| + \delta_{\mathbb{K}_0,p} + 2\sqrt{r_1 + r_2 + |T| + \delta_{\mathbb{K},p}},$$

*then the extension $\mathbb{K}_\emptyset^T/\mathbb{K}$ is infinite.*

*Proof.* — Indeed, by genus theory (see e.g. [**2**, Corollary 4.5.1, Chapter IV, §4]), one has $d_p\mathrm{Cl}(\mathbb{K}) \geq \rho - (r_1(\mathbb{K}_0) + r_2(\mathbb{K}_0) + \delta_{\mathbb{K}_0,p})$ and obviously, $d_p\mathrm{Cl}_p \leq d_p\mathrm{Cl}_p^T + |T|$. □

*5.1.2. The Brauer-Siegel Inequality.* — The Brauer-Siegel Inequality is a well known inequality from algebraic number theory (see e.g. [**11**] Chapter XIII §4) : $\ln \mathrm{Reg}_{\mathbb{K}} \leq C \ln |\mathrm{disc}_{\mathbb{K}}|$, where $C$ is a universal constant. It tells that along an asymptotically good extension, the quantity $\frac{1}{[\mathbb{K}:\mathbb{Q}]} \log_q \mathrm{Reg}_{\mathbb{K}}$ remains bounded. In [**31**], Tsfasman and Vladut show how it is possible to give a good asymptotic estimation of the Brauer-Siegel inequality, by making explicit the quantity $C$. In fact, they even give a recipe to improve the universal constant $C$, depending on the context, see Section 5.1.3.

Assuming *GRH* in an asymptotically good extension $\mathbb{L}/\mathbb{K}$, Tsfasman and Vladut in [**31**] prove that $\lim\limits_{n} \frac{\log(\mathrm{Reg}_n \mathsf{h}_n)}{g_n}$ exists in the tower $\mathbb{L} = \bigcup_n \mathbb{K}_n$. We denote by $B(\mathbb{L}/\mathbb{K})$ this limit.

***Theorem 5.6*** **(Tsfasman-Vladut, Theorem G).** — *Given an asymptotic good tower $\mathbb{L} = \bigcup_n \mathbb{K}_n$ of $\mathbb{K}$.*

1. *Assuming GRH, the limit $B(\mathbb{L}/\mathbb{K}) := \lim_n \frac{\ln(\mathrm{Reg}_n \mathsf{h}_n)}{g_n}$ exists and depends only on $\mathbb{L}/\mathbb{K}$, not on the choice of tower $(\mathbb{K}_n)_n$ with limit $\mathbb{L}$. Without assuming GRH, one has the same conclusion if the tower of number fields $(\mathbb{K}_n)_n$ is Galois relatively to $\mathbb{K}$.*
2. *Assuming GRH, $B(\mathbb{L}/\mathbb{K}) \leq 1.0939$ for all $\mathbb{L}/\mathbb{K}$. If $\mathbb{K}$ is totally imaginary, then $B(\mathbb{L}/\mathbb{K}) \leq 1.0765$.*
3. *Without assuming GRH, one has $\limsup_n \frac{\ln(\mathrm{Reg}_n \mathsf{h}_n)}{g_n} \leq 1.1589$.*

As a consequence, one obtains

***Corollary 5.7.*** — *Given an asymptotic good tower $\mathbb{L} = \bigcup_n \mathbb{K}_n$ of $\mathbb{K}$, then*

$$\begin{aligned} \limsup_n \tfrac{1}{[\mathbb{K}_n:\mathbb{Q}]} \log_q \mathrm{Reg}_n &\leq \tfrac{B(\mathbb{L}/\mathbb{K})}{2} \log_q \mathrm{rd}_{\mathbb{L}} - \liminf_n \tfrac{1}{[\mathbb{K}_n:\mathbb{Q}]} \log_q \mathsf{h}_n \\ &\leq \tfrac{B(\mathbb{L}/\mathbb{K})}{2} \log_q \mathrm{rd}_{\mathbb{L}}. \end{aligned}$$

*5.1.3. Examples.* —

***Example 5.8.*** — A first illustration is the infinite Hilbert 2-tower of quadratic number fields $\mathbb{K}$ as soon as $\mathbb{K}/\mathbb{Q}$ is sufficiently ramified. Apply Corollary 5.5 to a quadratic extension $\mathbb{K}/\mathbb{Q}$ with $p = 2$. If $\rho \geq 4 + |T| + 2\sqrt{r_1 + r_2 + |T| + 1}$, the maximal 2-extension $\mathbb{K}_\emptyset^T$ of $\mathbb{K}$, totally split in $T$, is infinite. For $r_2 = 1$ and $|T| = 1$, the imaginary quadratic field $\mathbb{K}/\mathbb{Q}$ has an infinite 2-tower $\mathbb{K}_\emptyset^T$ which is $T$-split as soon as $\rho \geq 9$. For example, the field $\mathbb{K} = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$ has a 2-tower $\mathbb{K}_\emptyset^T = \bigcup_n \mathbb{K}_n$ which is $T = \{\mathfrak{p}\}$-split and infinite for every prime $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$. Furthermore,

$$\limsup_n \frac{1}{[\mathbb{K}_n : \mathbb{Q}]} \ln \mathrm{Reg}_{\mathbb{K}_n} \leq \frac{1.0765}{2} \ln(19399380^{1/2}) \simeq 4.5161\ldots$$

***Example 5.9.*** — These criteria have been refined (see e.g. [**28**], [**9**]). An immediate refinement relies on Chebotarev density Theorem. Suppose that $d_2\mathrm{Cl}(\mathbb{K}) \geq 2 + 2\sqrt{r_1 + r_2 + |T| + \delta_{\mathbb{K}}}$ and that the places of $T$ are totally split in the 2-field of Hilbert of $\mathbb{K}$. Then $d_2\mathrm{Cl}_2^T(\mathbb{K}) = d_2\mathrm{Cl}_2(\mathbb{K}) \geq 2 + 2\sqrt{r_1 + r_2 + |T| + \delta_{\mathbb{K}}}$ and the number field $\mathbb{K}$ has an infinite 2-tower $\mathbb{K}_\emptyset^T$, which is $T$-split (according to Theorem 5.4). By the Chebotarev density Theorem, the places of $T$ are of positive density. For example, $\mathbb{K} = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19})$ has a 2-tower which is $T = \{\ell\}$-split for every inert prime $\ell$ in $\mathbb{K}/\mathbb{Q}$: since $\ell$ is principal, it is totally split in the Hilbert field of $\mathbb{K}$. A computation shows that $\mathrm{Cl}_2(\mathbb{K}) \simeq (\mathbb{Z}/2\mathbb{Z})^6$. The condition on $\ell$ indicates that their density is 1/2. For example, $\ell = 23, 29, 37, 41, \ldots$ are suitable. Furthermore, under GRH,

$$\limsup_n \frac{1}{[\mathbb{K}_n : \mathbb{Q}]} \ln \mathrm{Reg}_n \leq \frac{1.0765}{2} \ln(1141140^{1/2}) \simeq 3.7536\ldots$$

***Example 5.10.*** — Following Martinet [**15**, Example 5.3], we consider $\mathbb{K}_0 = \mathbb{Q}(\sqrt{5}, \sqrt{17})$ and $\mathbb{K} = \mathbb{K}_0(\sqrt{-3 \cdot 19})$. The criterion of Corollary 5.5 is applied to the quadratic extension $\mathbb{K}/\mathbb{K}_0$, the number field $\mathbb{K}$ has an infinite non-ramified 2-tower. Since $\mathbb{K}/\mathbb{K}_0$ is not ramified, we deduce that the quadratic field $\mathbb{K}_0$ has an infinite 2-tower. A computation shows that $\mathrm{Cl}_2(\mathbb{K}) \simeq (\mathbb{Z}/8\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^5$. We then choose a prime $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ such that $\mathfrak{p}$ is totally split in the 2-field of Hilbert of $\mathbb{K}$, then $d_2\mathrm{Cl}_2^T(\mathbb{K}) = 7 \geq 2 + 2\sqrt{6}$ and the $T$-split 2-tower $\mathbb{K}_\emptyset^T$ of $\mathbb{K}$ is infinite, where here $T = \{\mathfrak{p}\}$. For this tower, one obtains, under GRH,

$$\limsup_n \frac{1}{[\mathbb{K}_n : \mathbb{Q}]} \ln \mathrm{Reg}_n \leq \frac{1.0765}{2} \ln(\mathrm{rd}_\mathbb{K}) \simeq 2.6561\ldots$$

We may take for example $T = \{\mathfrak{p}\}$ where $\mathfrak{p}|\ell$, with $\ell \in \{59, 101, 149, \ldots\}$ and $N(\mathfrak{p}) = \ell^2$; alternatively $T = \{\mathfrak{p}\}$ where $\mathfrak{p}|\ell$, with $\ell \in \{170701, 906601, \ldots\}$ and $\mathsf{N}(\mathfrak{p}) = \ell$.

***Example 5.11***. — Consider next Martinet's example [**15**]: $\mathbb{K} = \mathbb{Q}(\cos(2\pi/11), \sqrt{2}, \sqrt{-23})$. It is a totally imaginary number field of degree 20 over $\mathbb{Q}$. The 2-class group of $\mathbb{K}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^9$. Hence take a prime $\mathfrak{p} \in \mathcal{O}_\mathbb{K}$ such that $\mathfrak{p}$ splits totally in the 2-Hilbert class field of $\mathbb{K}$; set $T = \{\mathfrak{p}\}$. Then $d_2\mathrm{Cl}_2(\mathbb{K}) = d_2\mathrm{Cl}_2^T(\mathbb{K}) = 9 \geq 2 + 2\sqrt{12}$ and the 2-tower $\mathbb{K}_\emptyset^T/\mathbb{K}$ is infinite. For this tower, one obtains, under GRH,

$$\limsup_n \frac{1}{[\mathbb{K}_n : \mathbb{Q}]} \ln \mathrm{Reg}_n \leq \frac{1.0765}{2} \ln(\mathrm{rd}_\mathbb{K}) \simeq 2.4360\ldots$$

We may take for example $T = \{\mathfrak{p}\}$ where $\mathfrak{p}|\ell$, with $\ell \in \{3, 7, 13, 17, 29, 47, 59, 71, \ldots\}$ and $N(\mathfrak{p}) = \ell^{10}$; alternatively $T = \{\mathfrak{p}\}$ where $\mathfrak{p}|\ell$, with $\ell \in \{47, 71\ldots\}$ and $N(\mathfrak{p}) = \ell^5$; a third possibility is $T = \{89, 199, 241, \ldots\}$, with $\mathsf{N}(\mathfrak{p}) = \ell^2$, or finally $T = \{294799, 583351, 689063, 693727 \cdots\}$ with $\mathsf{N}(\mathfrak{p}) = \ell$.

***Example 5.12***. — We conclude by looking at Example 3.4 in [**8**].
Set $\mathbb{K} = \mathbb{Q}(\sqrt{130356633908760178920}, \sqrt{-80285321329764931})$.
Then $\mathbb{K}$ has one infinite extension $\mathbb{L}/\mathbb{K}$, contained in the 2-tower $\mathbb{K}_\emptyset^\emptyset$, in which the places dividing $\{71, 79, 83, 97, 101, 59, 61, 67, 73\}$ are totally split. Also $B(\mathbb{L}/\mathbb{K}) \leq 0.951\ldots$. Furthermore, there exists a tower $(K_n)_n$ of $\mathbb{K}$, with limit $\mathbb{L}$ such that $\mathsf{h}(\mathbb{K}_n) \geq 2^{13[\mathbb{K}_n:\mathbb{K}]-1}$. Thus

$$\begin{aligned} \limsup_n \frac{1}{[\mathbb{K}_n : \mathbb{Q}]} \ln \mathrm{Reg}_{\mathbb{K}_n} &\leq \frac{0.951}{2} \ln \mathrm{rd}_\mathbb{K} - \frac{13}{2} \ln(2) \\ &\leq 15.7606\ldots \end{aligned}$$

For other examples, see e.g. [**31**], [**15**], [**28**], [**7**], [**6**], [**4**].

**5.2. Number Field Codes.** — Consider again the strategy of Lenstra [**12**] and Guruswami [**3**]. Start with an infinite tower $(\mathbb{K}_n)_n$ which is asymptotically good, $\mathbb{L} = \bigcup_n \mathbb{K}_n$. To simplify, we assume that $\mathbb{L}/\mathbb{K}$ is unramified. Fix a set $T$ of places of $\mathbb{K}$, which are totally split in $\mathbb{L}/\mathbb{K}$ ; $N = \#T$. Suppose that for every place $\mathfrak{p} \in T$, $\#\mathcal{O}_\mathbb{K}/\mathfrak{p} = q$. Set $t \in \mathbb{R}_{>0}$. As explained in Section 3, consider the sequence of number fields $\mathcal{C}_n := \mathcal{C}_{z_n}(\mathcal{O}_{\mathbb{K}_n})$, where to simplify, the codes $\mathcal{C}_n$ are integers. Codewords of $\mathcal{C}_n$ belong to $(\mathbb{F}_q)^{N[\mathbb{K}_n:\mathbb{K}]}$.
As noticed by Lenstra and Guruswami, the code family $(\mathcal{C}_n)_n$ is asymptotically good for a large enough $q$ and for an appropriate $t$.

Recall that the Singleton bound for nonlinear codes states that

$$\log_q |\mathcal{C}| \leq N - d_H(\mathcal{C}) + 1.$$

In our context, we get

$$\begin{aligned}
& \frac{1}{\mathbb{K}:\mathbb{Q}]}\log_q(2^r\pi^{r_2})+\log_q(t)-\frac{1}{2}\log_q \mathrm{rd}_{\mathbb{K}_n} \\
\leq \; & \frac{1}{[\mathbb{K}_n:\mathbb{Q}]}\log_q|\mathcal{C}_n| \\
\leq \; & \frac{N}{[\mathbb{K}_n:\mathbb{Q}]}-\frac{1}{[\mathbb{K}_n:\mathbb{Q}]}d_H(\mathcal{C}_n)+\frac{1}{[\mathbb{K}_n:\mathbb{Q}]} \\
\leq \; & \log_q(2t)+\frac{1}{[\mathbb{K}_n:\mathbb{Q}]}
\end{aligned}$$

and we are looking at how close to equality the following inequality is:

$$\frac{1}{[\mathbb{K}:\mathbb{Q}]}\log_q(2^r\pi^{r_2})-\frac{1}{2}\log_q \mathrm{rd}_{\mathbb{K}}-\log_q 2\leq\frac{1}{[\mathbb{K}_n:\mathbb{Q}]}$$

where we recall that $\mathrm{rd}_{\mathbb{K}_n}=\mathrm{rd}_{\mathbb{K}}$. Its limit when $n$ grows is

$$\frac{1}{[\mathbb{K}:\mathbb{Q}]}\log_q(2^r\pi^{r_2})-\frac{1}{2}\log_q \mathrm{rd}_{\mathbb{K}}-\log_q 2\leq 0$$

For $q$ large enough, the inequality is close to be tight.
For the sake of completeness, we recall Odlyzko's asymptotic estimations [**21**]: for $[\mathbb{K}:\mathbb{Q}]=n\gg 0$ (under GRH)

$$\mathrm{rd}_{\mathbb{K}}\geq(8\pi e^{\gamma+\pi/2})^{r_1/n}(8\pi e^{\gamma})^{2r_2/n}.$$

**5.3. Unit Codes.** — Our goal next is to study asymptotically the inequalities of Proposition 4.6 for unit codes $\mathcal{C}:=\mathcal{C}_{z,t}(\mathcal{O}_{\mathbb{K}}^{\times})$ built over units of the ring of integers of the number field $\mathbb{K}$ in Section 4.
As in Section 5.2, start with an infinite asymptotically good tower $(\mathbb{K}_n)_n$, $\mathbb{L}=\bigcup_n\mathbb{K}_n$ (we still assume $\mathbb{L}/\mathbb{K}$ unramified). Let $T$ be a set of places of $\mathbb{K}$, which are totally split in $\mathbb{L}/\mathbb{K}$; $N=\#T$. Suppose that for every place $\mathfrak{p}\in T$, $\#\mathcal{O}_{\mathbb{K}}/\mathfrak{p}=q$. Set $t\in\mathbb{R}_{>0}$ and consider the sequences of codes $\mathcal{C}_n:=\mathcal{C}_{z_n,t}(\mathcal{O}_{\mathbb{K}_n}^{\times})$. Codewords in $\mathcal{C}_n$ are in $(\mathbb{F}_p)^{N[\mathbb{K}_n:\mathbb{K}]}$.
Since $\mathbb{L}/\mathbb{K}$ is asymptotically good,

$$\limsup_n\frac{1}{[\mathbb{K}_n:\mathbb{Q}]}\mathrm{Reg}_n\leq\frac{B(\mathbb{L}/\mathbb{K})}{2}\log_q \mathrm{rd}_{\mathbb{L}},$$

where we may upper bound $\mathbb{B}(\mathbb{L}/\mathbb{K})$, the universal constant given by Tsfasman and Vladut (see Theorem 5.6).
The code family $(\mathcal{C}_n)_n$ will be asymptotically good as soon as

$$\frac{N}{[\mathbb{K}:\mathbb{Q}]}>\log_q(2e^{2t})$$

and for $n$ large enough:

$$\log_q t>\frac{[\mathbb{K}:\mathbb{Q}]B(\mathbb{L}/\mathbb{K})}{2r}\log_q \mathrm{rd}_{\mathbb{L}}-\log_q 2.$$

Thus it is always possible to find a real $t$ for which these conditions are satisfied as soon as $q$ is large enough.

***Example 5.13* (Continuation of Example 5.9).** — As an illustration, consider $\mathbb{K} = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19})$ and its 2-tower $\mathbb{K}_\emptyset^T = \mathbb{L}$ which is not ramified, with $N = 1$ and $B(\mathbb{L}/\mathbb{K}) = 1.0765$. Then $\mathrm{rd}_\mathbb{L} = \mathrm{rd}_\mathbb{K} = 1141140^{1/2}$.
It is enough to take $t$ and $q$ satisfying

$$\ln q > 2\ln(1+e^t) \quad \text{and} \quad \ln t > 7.5072\ldots - \ln 2 \approx 6.8141\ldots$$

For $\ln t = 6.8141\ldots$, we obtain $\ln q \geq 1821.2211\ldots$. It is enough to then choose $\ell$ inert in $\mathbb{K}/\mathbb{Q}$ such that $q = \ell^2 \geq e^{1821.2211\cdots}$.
In summary, consider the Hilbert 2-tower $\bigcup\limits_n \mathbb{K}_n$ of $\mathbb{K}$ which is $\{\ell\}$-split: this is an asymptotically good tower. Take $\ell$ as aforementioned. For all $n$, we choose an element $\mathcal{O}_{\mathbb{K}_n}^\times$-admissible $z_n$; we take $t = e^{6.8141\cdots}$; the family of codes $\Big(\mathcal{C}_{z_n,t}(\mathcal{O}_{\mathbb{K}_n}^\times)\Big)$ has codewords in $\Big(\mathbb{F}_{\ell^2}\Big)^{[\mathbb{K}_n:\mathbb{K}]}$ and is asymptotically good.

***Example 5.14* (Continuation of Example 5.10).** — As a second illustration, take $\mathbb{K} = \mathbb{Q}(\sqrt{5}, \sqrt{17}, \sqrt{-3 \cdot 19})$ and its 2-tower $\mathbb{K}_\emptyset^T = \mathbb{L}$, with $T = \{\mathfrak{p}\}$ and where $\mathfrak{p}$ splits totally in the 2-Hilbert class field of $\mathbb{K}$. It is enough to take $t$ and $q$ satisfying

$$\ln q > 8\ln(1+e^t) \quad \text{and} \ln t \geq 4.6204\ldots$$

For $\ln t = 4.6204\ldots$, we obtain $\ln q \geq 8\ln(1+e^{e^{4.6204\cdots}}) \geq 812.3218\ldots$. In summary, take $T = \{\mathfrak{p}\}$ with $\mathfrak{p}$ totally split in the 2-Hilbert field of $\mathbb{K}$ and $\mathsf{N}(\mathfrak{p}) \geq e^{812.3218\cdots}$.

***Example 5.15* (Continuation of Example 5.11).** — As a third illustration, take again Martinet's example $\mathbb{K} = \mathbb{Q}(\cos(2\pi/11), \sqrt{2}, \sqrt{-23})$ and its 2-tower $\mathbb{K}_\emptyset^T = \mathbb{L}$, with $T = \{\mathfrak{p}\}$ and where $\mathfrak{p}$ splits totally in the 2-Hilbert class field of $\mathbb{K}$. It is enough to take $t$ and $q$ satisfying

$$\ln q > 20\ln(1+e^t) \quad \text{and} \quad \ln t > 4.1788\ldots$$

For $\ln t = 4.1788\ldots$, we obtain $\ln q \geq 1305.8267\ldots$.

# PART II
# MAXIMAL ORDERS CODES

## 6. Background on Central Simple Algebras

The book by Reiner [**25**] is a major reference. We also refer to the book by Gille and Szamuely [**1**].

Let A be a central simple algebra over $\mathbb{K}$, which is *division*: this hypothesis is necessary for our code constructions. We may speak of a division algebra A for short, to mean a central simple division $\mathbb{K}$-algebra.

**6.1. Central simple algebras.** — Our reference is [**25**, §32].
- Let $d^2$ be the dimension of A over $\mathbb{K}$, then $d$ is the degree of A over $\mathbb{K}$.
- For A a central simple algebra of degree $d$, we have $\mathrm{A} = \mathsf{M}_r(\mathsf{D})$ for $\mathsf{D}$ a skewfield and $d = re$ where $e^2 = [\mathsf{D} : \mathbb{K}]$. In particular if $d$ is prime, either $r = 1$ or $e = 1$.
- Let $v \in \mathbb{P}$ be a place of $\mathbb{K}$ and consider the algebra $\mathrm{A}_v = \mathrm{A} \otimes_{\mathbb{K}} \mathbb{K}_v$. Then $\mathrm{A}_v \simeq \mathsf{M}_{f_v}(\mathsf{D}_v)$, where $\mathsf{D}_v$ is a skewfield of center $\mathbb{K}_v$. We then have $f_v e_v = d$, with $e_v^2 = [\mathsf{D}_v : \mathbb{K}_v]$.
- The integer $e_v$ (or $e_{\mathfrak{p}}$ if $v = \mathfrak{p}$) is the ramification index of $v$ (or of $\mathsf{D}_v$) and $f_v$ (or $f_{\mathfrak{p}}$ if $v = \mathfrak{p}$) is the residual degree of $v$ (or of $\mathsf{D}_v$).
- The algebra is said to be ramified in $v$ if $[\mathsf{D}_v : \mathbb{K}_v] > 1$, and totally ramified if $[\mathsf{D}_v : \mathbb{K}_v] = d^2$ ($\Longleftrightarrow e_v = d$). If $v$ is not ramified, we say that A is split in $v$.
- For almost every place $v$ in $\mathbb{K}$, A is split in $v$, *i.e.* $e_v = 1$.

Let $S_0$ be the set of primes $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ which ramify in A and let $S_\infty$ be the set of ramified archimedean places. Set $S = S_0 \cup S_\infty$. The set $S$ is thus finite.

**6.2. Local symbols.** — Our references are [**25**, §12, §13, §14], [**1**, chapter 4]. We recall the notation $\mathbb{P}_\infty$ for infinite primes and $\mathbb{P}_0$ for the finite ones.
- For every division algebra A and every place $v \in \mathbb{P}$, we associate the invariant $\alpha_v \in \mathbb{Q}/\mathbb{Z}$ obtained as follows. If $v$ is not ramified, then $\alpha_v = 0$. Suppose now that $v$ is ramified *i.e.* $e_v > 1$. If $v \in \mathbb{P}_\infty$ then $\alpha_v = 1/2$. Suppose $v \in \mathbb{P}_0$ (and ramifies). As recalled above, $\mathrm{A}_v \simeq \mathsf{M}_{f_v}(\mathsf{D}_v)$, where $\mathsf{D}_v$ is a division algebra of center $\mathbb{K}_v$, with $e_v^2 = [\mathsf{D}_v : \mathbb{K}_v]$. Let $q_0$ be the cardinality of the residual field of $\mathbb{K}_v$. Let $\mathbb{K}_v(\omega)/\mathbb{K}_v$ be the unique non-ramified extension of degree $e_v$ of $\mathbb{K}_v$ where $\omega$ is a primitive $q_0^{e_v} - 1$ root of unity. It is a cyclic extension of Galois group generated by a lifting $\sigma$ of the Frobenius automorphism on the residual field. There exists an integer $r_v$, $1 \leq r_v \leq e_v$, $(r_v, e_v) = 1$, such that $\mathsf{D}_v$ is isomorphic to the cyclic algebra $(\mathbb{K}_v(\omega)/\mathbb{K}_v, \sigma, \pi^{r_v})$, where $\pi$ is a uniformizer of $\mathbb{K}_v$. The invariant is defined by $\alpha_v = \frac{r_v}{e_v} \in \mathbb{Q}/\mathbb{Z}$.
- Globally, we get $\sum_v \alpha_v = 0 \in \mathbb{Q}/\mathbb{Z}$: this is Hasse's product formula. Thus, if A is a quaternion algebra *i.e.* of dimension 4, then $|S|$ is even.
- Conversely, given a family $(\alpha_v)$ such that
  (i) $\alpha_v \in \mathbb{Q}/\mathbb{Z}$;
  (ii) $\alpha_v = 0$ for almost every $v$
  (iii) for $v \in \mathbb{P}_{\mathbb{C}}$, $\alpha_v = 0$, and for $v \in \mathbb{P}_{\mathbb{R}}$, $\alpha_v \in \{0, 1/2\}$;
  (iv) $\sum_v \alpha_v = 0$;

then there exists a division algebra over $\mathbb{K}$ whose local symbols are $(\alpha_v)_{v \in \mathbb{P}}$. In that case, the division algebra A is of degree the *lcm* of the denominators of the $\alpha_v$.

**6.3. Discriminant.** — The reference is [**25**, §25].
- By a full $\mathcal{O}_{\mathbb{K}}$-lattice $\Lambda$ of A, we mean a finitely generated $\mathcal{O}_{\mathbb{K}}$-submodule in $A$ such that $\mathbb{K}\Lambda = \{\sum_{\text{finite}} x_i \lambda_i,\ x_i \in \mathbb{K}, \lambda_i \in \Lambda\} = \mathrm{A}$.
- Let $\Lambda$ be an $\mathcal{O}_{\mathbb{K}}$-order of A, that is, $\Lambda$ is a subring of A, having the same identity element as A, which is also a full $\mathcal{O}_{\mathbb{K}}$-lattice in A.
- The discriminant $\mathrm{disc}_\Lambda$ of $\Lambda$ is the ideal of $\mathcal{O}_{\mathbb{K}}$ generated by the determinant of the reduced trace form Trd.
- If $\Lambda$ has a basis $\{b_1, \cdots, b_{d^2}\}$ over $\mathcal{O}_{\mathbb{K}}$, then $\mathrm{disc}_\Lambda$ is the principal ideal generated by $\det(\mathrm{Trd}(b_i b_j))$.
- Let $\Lambda$ and $\Lambda'$ be two *maximal* orders, meaning that they are not properly contained in any other $\mathcal{O}_{\mathbb{K}}$-order in A. Then $\mathrm{disc}_\Lambda = \mathrm{disc}_{\Lambda'}$.

• By definition, the discriminant $\mathrm{disc}_{\mathrm{A}}$ of A is equal to $\mathrm{disc}_{\Lambda}$ for a maximal order $\Lambda$ of A.
• We have $\mathrm{disc}_{\mathrm{A}} = \prod_{\mathfrak{p}\in S_0} \mathfrak{p}^{f_{\mathfrak{p}} d(e_{\mathfrak{p}}-1)} = \prod_{\mathfrak{p}\in S_0} \mathfrak{p}^{d^2(1-1/e_{\mathfrak{p}})}$ for $\mathfrak{p}$ finite primes of $\mathcal{O}_{\mathbb{K}}$ that ramify in A.
• An order $\Lambda$ is maximal if and only if $\mathrm{disc}_{\Lambda} = \mathrm{disc}_{\mathrm{A}}$ (cf [**25**, Theorem 32.1]).
• We define the absolute discriminant $\Delta_{\mathrm{A}}$ of A as the determinant of the form $\mathsf{T} = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}} \circ \mathrm{Trd}$. We have

$$\Delta_{\mathrm{A}} = |\mathrm{disc}_{\mathbb{K}}|^{d^2}\ \mathsf{N}_{\mathbb{K}/\mathbb{Q}} \mathrm{disc}_{\mathrm{A}}.$$

Recall that $\dim_{\mathbb{Q}} \mathrm{A} = nd^2$.

***Definition 6.1***. — The quantity $\mathrm{rd}_{\mathrm{A}} := \Big(\Delta_{\mathrm{A}}\Big)^{1/nd^2} = \mathrm{rd}_{\mathbb{K}} \Big(\prod_{\mathfrak{p}\in S_0} \mathsf{N}(\mathfrak{p})^{(1-1/e_{\mathfrak{p}})}\Big)^{1/[\mathbb{K}:\mathbb{Q}]}$ is the root discriminant of the division algebra A.
Recall that $\mathrm{rd}_{\mathbb{K}} = |\mathrm{disc}_{\mathbb{K}}|^{1/[\mathbb{K}:\mathbb{Q}]}$ is the root discriminant of $\mathbb{K}$.

***Remark 6.2***. — Given $\mathbb{K}$, to determine division algebras A which are not ramified in infinite places with a small root discriminant reduces to look for prime ideals of $\mathbb{K}$ of smallest norms (this is a consequence of the product formula for symbols).

***Remark 6.3***. — Let $\Big(\bigcup_n \mathbb{K}_n\Big)/\mathbb{K}$ be an infinite non-ramified extension in which the prime ideal $\mathfrak{p}$ splits totally. For every number field $\mathbb{K}_n$, take $\mathfrak{p}_n$ and $\mathfrak{p}'_n$ two ideals of $\mathcal{O}_{\mathbb{K}_n}$ above $\mathfrak{p}$. Consider the quaternion algebra $\mathrm{A}_n$ of center $\mathbb{K}_n$ ramified only at $\mathfrak{p}_n$ and $\mathfrak{p}'_n$. Then

$$\mathrm{rd}_{\mathrm{A}_n} = \mathrm{rd}_{\mathbb{K}} \Big(\mathsf{N}_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p})\Big)^{1/[\mathbb{K}_n:\mathbb{Q}]} \xrightarrow[n\to\infty]{} \mathrm{rd}_{\mathbb{K}}.$$

**6.4. Ideals.** — The reference is [**25**, §22-24].
• Let $\Lambda$ be an $\mathcal{O}_{\mathbb{K}}$-order of A.

***Lemma 6.4***. — *Let* A *be a division algebra. Then for $x \in \Lambda$, $x \neq 0$, the $\mathcal{O}_{\mathbb{K}}$-module $\Lambda x$ (resp. $x\Lambda$) is a full lattice.*

*Proof*. — Since $x \neq 0$ and A is division, we denote by $x^{-1}$ the inverse of $x$. Since $\mathbb{K}\Lambda = \mathrm{A}$, there exists $a \in \mathbb{K}$, $\lambda \in \Lambda$ such that $a\lambda = x^{-1}$. Set now $z = a_0\lambda_0 \in \mathrm{A}$, $a_0 \in \mathbb{K}$, $\lambda_0 \in \Lambda$. Then $a_0 a \lambda_0 \lambda x = z$. □

*We further assume that* $\Lambda$ *is* maximal.

• A two-sided ideal $\mathcal{I}$ of $\Lambda$ is a full $\mathcal{O}_{\mathbb{K}}$-lattice such that $\Lambda_l(\mathcal{I}) = \Lambda_r(\mathcal{I}) = \Lambda$, where $\Lambda_l(\mathcal{I}) = \{x \in \mathrm{A},\ x\mathcal{I} \subset \mathcal{I}\}$ (resp. $\Lambda_r(\mathcal{I}) = \{x \in \mathrm{A},\ \mathcal{I}x \subset \mathcal{I}\}$).
• A prime ideal $\mathfrak{P}$ of $\Lambda$ is a proper two-sided ideal in $\Lambda$ such that $\mathbb{K}\mathfrak{P} = \mathrm{A}$, and such that for any two-sided ideal $S, T \subset \Lambda$, $ST \in \mathfrak{P}$ implies $S \subset \mathfrak{P}$ or $T \subset \mathfrak{P}$.
The prime ideals of $\Lambda$ coincide with the maximal two-sided ideal of $\Lambda$ (Theorem 22.3 of [**25**]).
• There is a bijective correspondence between the nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ and the prime ideals $\mathfrak{P}$ of $\Lambda$: $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{\mathbb{K}}$.
• We have $\mathfrak{p}\Lambda = \mathfrak{P}^{e_{\mathfrak{P}}}$, where $e_{\mathfrak{P}} = e_v$ is the ramification index of $v$ in A (see [**25**, Theorem 32.1]).
• Prime ideals of $\Lambda$ satisfy the following two properties:

- For $\mathfrak{P}_1, \mathfrak{P}_2$ distinct prime ideals of $\Lambda$, $\mathfrak{P}_1 + \mathfrak{P}_2 = \Lambda$.
- For $\mathfrak{P}_1, \mathfrak{P}_2$ distinct prime ideals of $\Lambda$, $\mathfrak{P}_1\mathfrak{P}_2 = \mathfrak{P}_1 \cap \mathfrak{P}_2$.

• If $\mathcal{I}$ is a two-sided ideal of $\Lambda$, we recall the unique decomposition $\mathcal{I} = \prod_{i=1}^{t} \mathfrak{P}_i^{a_i}$, where $v_{\mathfrak{P}}(\mathcal{I}) = a_i \in \mathbb{N}$ (cf [**25**, Theorem 22.10]).

**6.5. Reduction.** —
• Let $\mathcal{I}$ be a right ideal of $\Lambda$. We denote by $\mathsf{N}(\mathcal{I}) = \#\Lambda/\mathcal{I}$ the absolute norm of $\mathcal{I}$. If $\mathcal{I}$ is two-sided, the quantity $\#\Lambda/\mathcal{I}$ does not depend on whether the ideal is a right or left ideal [**25**, Theorem 24.3].
• Set $\mathsf{N}(x) = \mathsf{N}(x\Lambda)$. Then $\#\Lambda/x\Lambda = \#\Lambda/\Lambda x$ (see [**25**, exercice 10.7 §10]). In particular $\mathsf{N}(x) = \#\Lambda/x\Lambda = |\mathsf{N}_{\mathbb{K}/\mathbb{Q}}\mathrm{Nrd}(x)|^d$.
• Let $\mathfrak{P}$ be a maximal ideal of the maximal order $\Lambda$ and let $v$ be the place of $\mathbb{K}$ corresponding to $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{\mathbb{K}}$. The quotient $\Lambda/\mathfrak{P}$ is a simple algebra of finite dimension over $\mathbb{F}_{q_0} = \mathcal{O}_K/\mathfrak{p}$ and the determination of its structure is a local computation.
Indeed, one has $\mathrm{A}_v \simeq \mathsf{M}_{f_v}(\mathsf{D}_v)$, with $e_v^2 = [\mathsf{D}_v : \mathbb{K}_v]$.
The skewfield $\mathsf{D}_v$ has a unique maximal order $\mathrm{R}_v$ with a prime ideal $\pi_v\mathrm{R}_v$. Then $\Lambda_v = \mathsf{M}_{f_v}(\mathrm{R}_v)$ is a maximal order of $\mathrm{A}_v$ with unique two-sided maximal ideal $\pi_v\Lambda_v$ (see [**25**, Theorem 17.3]). Hence, as $\mathrm{R}_v/(\pi_v) \simeq \mathbb{F}_{q_0^{e_v}}$ (see [**25**, Theorem 14.3]), one has

$$\Lambda/\mathfrak{P} \simeq \Lambda_v/\pi_v\Lambda_v \simeq \mathsf{M}_{f_v}(\mathbb{F}_{q_0^{e_v}})$$

and then $|\Lambda/\mathfrak{P}| = q_0^{f_v^2 e_v} = q_0^{df_v}$.
• When A is a quaternion algebra, $\Lambda/\mathfrak{P} \simeq \mathsf{M}_2(\mathbb{F}_{q_0})$ if $\mathfrak{P}$ is unramified, and $\Lambda/\mathfrak{P} \simeq \mathbb{F}_{q_0^2}$ if $\mathfrak{P}$ is ramified.
• Let $\mathcal{I}$ be a two-sided ideal of $\Lambda$. We write $\mathcal{I} = \prod_{i=1}^{t} \mathfrak{P}_i^{a_i}$ and for $i = 1, \cdots, t$, let $\mathfrak{p}_i \subset \mathcal{O}_{\mathbb{K}}$, with $\mathfrak{p}_i | \mathfrak{P}_i$. Let $f_{\mathfrak{P}_i} = f_v$ be the residual degree of $\mathfrak{P}_i$. Then

$$\mathsf{N}(\mathcal{I}) = \prod_{i=1}^{t} \mathsf{N}(\mathfrak{p}_i)^{df_{\mathfrak{P}_i}},$$

where $\mathsf{N}(\mathfrak{p}_i) = \#\mathcal{O}_{\mathbb{K}}/\mathfrak{p}_i$.

**6.6. Euclidean Embeddings.** — Here the reference is the thesis by Page [**22**, Chapter 2, §3].
Let A be a division algebra of center $\mathbb{K}$ and dimension $d^2$.

Set $\mathbb{P}_{\mathbb{R}}^1 = \mathbb{P}_{\mathbb{R}} \cap S_\infty$ and $\mathbb{P}_{\mathbb{R}}^0 = \mathbb{P}_{\mathbb{R}} - \mathbb{P}_{\mathbb{R}}^1$.
We recall that

(*i*) if $\sigma \in \mathbb{P}_{\mathbb{C}}$, then $\mathrm{A}_\sigma \simeq \mathsf{M}_d(\mathbb{C})$,
(*ii*) if $\sigma \in \mathbb{P}_{\mathbb{R}}^0$, then $\mathrm{A}_\sigma \simeq \mathsf{M}_d(\mathbb{R})$,
(*iii*) if $\sigma \in \mathbb{P}_{\mathbb{R}}^1$, then $\mathrm{A}_\sigma \simeq \mathsf{M}_{d/2}(\mathbb{H})$, where $\mathbb{H}$ is Hamilton's quaternion algebra.

Take $\sigma \in \mathbb{P}_\infty$. For $\mathbb{K}_\sigma = \mathbb{R}$ or $\mathbb{C}$, we endow $\mathsf{M}_\bullet(\mathbb{K}_\sigma)$ with the norm

$$\|M\|_2 = \sqrt{\mathrm{Tr}(M\overline{M}^t)}.$$

***Remark 6.5***. — If $\mathrm{A}_\sigma \simeq \mathbb{H}$, for $x \in \mathrm{A}_\sigma$, $\|x\|_2 = \mathrm{Nrd}(x)$.

Consider the embedding

$$\Psi : \mathrm{A} \longrightarrow \prod_{\sigma \in \mathbb{P}_\infty} \mathrm{A}_\sigma \simeq \mathbb{R}^{nd^2}.$$

We endow the product $\prod_{\sigma \in \mathbb{P}_\infty} \mathrm{A}_\sigma$ with the Lebesgue measure and with the norm inherited from the positive definite form

$$\mathsf{T}_2 = \sum_{\sigma \in \mathbb{P}_\infty} [\mathbb{K}_\sigma : \mathbb{R}](\|\sigma(\cdot)\|_2)^2.$$

The following volume computation is well known ([**22**, Chapter 2 §3]):

***Proposition 6.6***. — *The embedding $\Psi(\Lambda)$ is a lattice of $\mathbb{R}^{nd^2}$ of covolume $\sqrt{\Delta_{\mathrm{A}}}$.*

Noticing that $\sigma \in \mathbb{P}_\infty$ and $x \in \mathrm{A}$, we have $\mathrm{Nrd}(\iota_v(x)) = \iota_v(\mathrm{Nrd}(x))$, it then follows that $\mathsf{N}_{\mathbb{K}/\mathbb{Q}}(\mathrm{Nrd}(x)) = \prod_{v \in \mathbb{P}_\infty} \mathrm{Nrd}(\iota_v(x))$. The next proposition is a consequence of the inequality of arithmetic and geometric means.

***Proposition 6.7***. — *For every $x \in \mathrm{A}^\times$, we have*

$$\mathsf{N}(x) = \left|\mathsf{N}_{\mathbb{K}/\mathbb{Q}}\mathrm{Nrd}(x)\right|^d \leq \left(\frac{\mathsf{T}_2(x)}{nd}\right)^{\frac{nd^2}{2}}.$$

*Proof.* — See [**22**, Chapter 2 §3]. □

***Remark 6.8***. — It is possible, and in some cases, simpler to endow $\mathsf{M}_\bullet(\mathbb{K}_\sigma)$ with the infinite norm by setting $\|(a_{i,j})_{i,j}\|_\infty = \max_{i,j} |a_{i,j}|$, and similarly for $x \in \mathrm{A}, \|x\|_\infty = \max_{\sigma \in \mathbb{P}_\infty} \|\sigma(x)\|_\infty$. Typically, if $\mathbb{P}^1_{\mathbb{R}} = \emptyset$ it follows that $\mathsf{N}(x) \leq \left(d!\|x\|_\infty^{d^2}\right)^{d(r_1+r_2)}$.
For Example 1.5, the norm $\mathsf{T}_2$ is natural. For the sake of coherence, we will thus privilege the norm $\mathsf{T}_2$.

## 7. Additive Codes

**7.1. The context.** — The goal is to build codes, exploiting the additive structure of division algebras. The principle is similar to that of Section 3. In the context of function fields, more precisely Goppa codes built from division algebras over function fields, a similar idea has been developed by Morandi and Sethuraman [**16**], without an asymptotic study.

Let $\mathbb{K}$ be a number field of degree $n$ over $\mathbb{Q}$ and let A be a division algebra of center $\mathbb{K}$. Let $\Lambda$ be a maximal order of A.
In this context, an Arakelov divisor $\mathbb{A}$ is a pair $(\mathcal{I}, t)$, where $\mathcal{I}$ is a two-sided ideal of $\Lambda$ and where $t \in \mathbb{R}_{>0}$. It is then possible to develop a language similar to that of Section 3, but we will be more concise.
Here the locally compact group is the group $G = \prod_{\sigma \in \mathbb{P}} \mathrm{A}_\sigma \simeq \mathbb{R}^{nd^2}$ and $\Psi$ is the natural embedding

$$\Psi : \mathrm{A} \longrightarrow \prod_{\sigma \in \mathbb{P}} \mathrm{A}_\sigma \simeq \mathbb{R}^{nd^2}.$$

As mentioned in the previous section, we endow $\mathbb{R}^{nd^2}$ with the Lebesgue measure and with the norm $\mathsf{T}_2$.

***Proposition 7.1***. — *The subset* $\Psi(\mathcal{I})$ *of* $\mathbb{R}^{nd^2}$ *is discrete of covolume*

$$\mathsf{N}(\mathcal{I})\sqrt{\Delta_{\mathrm{A}}},$$

*where* $\mathsf{N}(\mathcal{I}) = \#\Lambda/\mathcal{I}$.

*Proof.* — See [**22**, Chapter 2 §3]. □

Set $t \in \mathbb{R}_{>0}$. Consider the compact $\mathsf{K}(t)$ of $\prod\limits_{\sigma\in\mathbb{P}_\infty} \mathrm{A}_\sigma \simeq \mathbb{R}^{nd^2}$:

$$\mathsf{K}(t) = \{x \in \prod_{\sigma\in\mathbb{P}_\infty} \mathrm{A}_\sigma,\ \|\sigma(x)\|_2 \leq t,\ \forall\sigma\}.$$

***Definition 7.2***. — Set

$$\mathsf{N}_\infty(t) = \mathbb{V}_{d^2}^{r_1}\mathbb{V}_{2d^2}^{r_2}t^{d^2n},$$

where $\mathbb{V}_k$ is the volume of the ball of center 0 and of radius 1 of $\mathbb{R}^k$ for the norm $\|\cdot\|_2$. This is the volume of the compact $\mathsf{K}(t)$ of $\mathbb{R}^{nd^2}$. We set $\mathbb{V}_{r_1,r_2,d} = \mathbb{V}_{d^2}^{r_1}\mathbb{V}_{2d^2}^{r_2}$.

***Remark 7.3***. — For $x \in \mathsf{K}(t)$, we have $\mathsf{T}_2(x) \leq [\mathbb{K}:\mathbb{Q}]t^2 = nt^2$.

As for the commutative case, we need Lenstra's result.

***Proposition 7.4***. — *Let* $\mathcal{D}$ *be a fundamental domain of* $\Psi(\mathcal{I})$*. There exists a* $z \in \mathcal{D}$ *such that* $z + \mathsf{K}(t)$ *contains at least* $\mathsf{N}_\infty(t)/\mathsf{N}(\mathcal{I})\sqrt{\Delta_A}$ *elements of* $\mathcal{I}$*. Such an element* $z$ *is called* $\mathcal{I}$*-admissible.*

*Proof.* — This is Lemma 1.6 applied to our setting. □

***Remark 7.5***. — Here, the quotient $\mathbb{R}^{nd^2}/\Psi(\mathcal{I})$ is compact.

***Definition 7.6***. — If $z \in \mathbb{R}^{nd^2}$ is $\mathcal{I}$-admissible, we set $\mathsf{K}_z(t) = z + \mathsf{K}(t)$.

**7.2. The construction.** — Let $\mathbb{K}$ be a number field of degree $[\mathbb{K}:\mathbb{Q}] = n$, with ring of integers $\mathcal{O}_\mathbb{K}$. Let A be a central simple division $\mathbb{K}$-algebra, and let $\Lambda$ be a maximal $\mathcal{O}_\mathbb{K}$-order of $A$. The algebra A is ramified at $S$.
Let $\mathcal{I}$ be a two-sided ideal of $\Lambda$ and let $T = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_N\}$ be a set of prime ideals of $\Lambda$, disjoint from $\mathcal{I}$. Consider

$$\Theta : \Lambda \to \prod_{i=1}^{N} \Lambda/\mathfrak{P}_i,\ x \mapsto (x \bmod \mathfrak{P}_1, \ldots, x \bmod \mathfrak{P}_N).$$

The proposed code is built using the embeddings $\Psi$ and $\Theta$ :

$$\begin{tikzcd}
 & \prod\limits_{\sigma\in\mathbb{P}_\infty} \mathrm{A}_\sigma \simeq \mathbb{R}^{nd^2} \\
\mathcal{I} \subseteq \Lambda \arrow[ur, bend left, "\Psi"] \arrow[dr, bend right, "\Theta"] & \\
 & \prod\limits_{\mathfrak{P}\in T} \Lambda/\mathfrak{P}
\end{tikzcd}$$

***Definition 7.7.*** — Let $z$ be an $\mathcal{I}$-admissible element. The code $\mathcal{C}_z(\mathcal{I})$ is obtained as

$$\mathcal{C}_{z,t}(\mathcal{I}) = \Theta\Big(\Psi^{-1}(\mathsf{K}_z(t)) \cap \mathcal{I}\Big).$$

When $\mathcal{I} = \Lambda$, the code $\mathcal{C}_{z,t}(\mathcal{I})$ is called a maximal order code.

**7.3. The parameters.** — To simplify, we assume that for $i = 1, \cdots, N$, $\#\Lambda/\mathfrak{P}_i = q$.

***Proposition 7.8.*** — *For the code $\mathcal{C} := \mathcal{C}_{z,t}(\mathcal{I})$ constructed above as a subset of $\prod_{i=1}^{N} \Lambda/\mathfrak{P}_i$, its minimum distance $d_H(\mathcal{C})$ satisfies*

$$d_H(\mathcal{C}) \geq N - nd^2 \log_q\left(\frac{2t}{d^{1/2}}\right) + \log_q \mathsf{N}(\mathcal{I}).$$

*Proof.* — This proof is similar to that of Proposition 3.10. Take two distinct codewords which agree on the largest number $|I|$ of components, then by the surjectivity of $\Theta$, their difference has a preimage $y \in \mathcal{I}$ such that $y \in \bigcap_{i\in I} \mathfrak{P}_i = \prod_{i\in I} \mathfrak{P}_i$. Thus $y \in \mathcal{J} := \mathcal{I}\prod_{i\in I} \mathfrak{P}_i \subset \Lambda$. Hence

$$\Lambda/y\Lambda \twoheadrightarrow \Lambda/\mathcal{J}.$$

As $y\Lambda$ and $\mathcal{J}$ are full $\mathcal{O}_{\mathbb{K}}$-lattices (because $y \neq 0$), the quotients $\Lambda/y\Lambda$ and $\Lambda/\mathcal{J}$ are finite (as left $\Lambda$-modules). Hence $\#\Lambda/y\Lambda \geq \#\Lambda/\mathcal{J}$. Then

$$\#\Lambda/\mathcal{J} = q^{|I|}\mathsf{N}(\mathcal{I})$$

and $\#\Lambda/y\Lambda = \mathsf{N}(y)$. Since $|I| = N - d_H(\mathcal{C})$, we get

$$N - d_H(\mathcal{C}) \leq \log_q \mathsf{N}(y) - \log_q \mathsf{N}(\mathcal{I}).$$

But for every $\sigma \in \mathbb{P}_\infty$, and for $x, x'$ the respective preimages of the two codewords at minimum distance, $\|\sigma(y)\|_2 \leq \|\sigma(x)\|_2 + \|\sigma(x')\|_2 \leq 2t$. Consequently, and using Proposition 6.7 and Remark 7.3, we obtain $\mathsf{N}(y) \leq \left(\frac{2t}{d^{1/2}}\right)^{nd^2}$. □

***Corollary 7.9.*** — *Let $\mathcal{C} := \mathcal{C}_{z,t}(\mathcal{I})$ be an additive code over a two-sided ideal $\mathcal{I}$ of the maximal order $\Lambda$. If $N + \log_q \mathsf{N}(\mathcal{I}) > nd^2 \log_q(\frac{2t}{d^{1/2}})$, the map $\Theta_{|\Psi^{-1}(\mathsf{K}_z(t))\cap\mathcal{I}}$ is injective.*

*Proof.* — If $x \neq x'$, with $x, x' \in \Psi^{-1}(\mathsf{K}_z(t)) \cap \mathcal{I}$, then $d_H(\Theta(x), \Theta(x')) \geq d_H(\mathcal{C}) > 0$. □

Under the injectivity hypothesis, one has:

***Proposition 7.10.*** — *Let $\mathcal{C} = \mathcal{C}_{z,t}(\mathcal{I})$ be an additive code over a two-sided ideal $\mathcal{I}$ of the maximal order $\Lambda$.*
*Assume that $N + \log_q \mathsf{N}(\mathcal{I}) > nd^2 \log_q(\frac{2t}{d^{1/2}})$. Then*

$$\log_q(|\mathcal{C}|) \geq \log_q \mathbb{V}_{r_1,r_2,d} + d^2 n \log_q(t) - \log_q \mathsf{N}(\mathcal{I}) - \frac{nd^2}{2} \log_q \mathrm{rd}_{\mathrm{A}}.$$

*Proof.* — Indeed, in this case the map $\Theta_{|\Psi^{-1}(\mathsf{K}_z(t))\cap\mathcal{I}}$ is injective. Then, the lower bound for $\log_q(|\mathcal{C}|)$ results from Proposition 7.1 and Proposition 7.4. □

**7.4. Example.** — If $\mathfrak{P}$ is not ramified, then the code alphabet is $\mathcal{A}(\mathbb{F}_p) = \mathsf{M}_d(\mathbb{F}_{q_0})$.
A natural way to produce codes over an alphabet $\mathcal{A}(\mathbb{F}_p) = \mathbb{F}_q$ is to take $\Theta$ the reduction modulo some primes $\mathfrak{P}$ that are *totally ramified*: in particular, $T \subset S$. In this case, for every $\mathfrak{p} \in T$, $f_\mathfrak{p} = 1$, $e_\mathfrak{p} = d$ and, $\mathsf{N}(\mathfrak{p}) = q_0$, $\mathcal{A}(\mathbb{F}_p) = \mathbb{F}_{q_0^d}$ and $q = q_0^d$.
(1) Let $p > 2$ be a prime number and consider the $\mathbb{Q}$-algebra $\mathrm{A} = \left(\frac{-1,-p}{\mathbb{Q}}\right)$ which is a division algebra. Indeed, as recalled in Subsection 6.1, since $d = 2$ is prime, either A is a skewfield and $e = 2$, or $\mathrm{A} = \mathsf{M}_2(\mathbb{Q})$ and $e = 1$. But since $\mathrm{A}_\mathbb{Q}$ is ramified in $\mathbb{P}_\mathbb{R}$, that is, $\left(\frac{-1,-p}{\mathbb{R}}\right) \simeq \mathbb{H}$, it cannot be that $\mathrm{A}_\mathbb{Q} = \mathsf{M}_2(\mathbb{Q})$.
Furthermore $\mathrm{disc}_\mathrm{A} = p^2$. Indeed, the reduced norm $x_1^2 + px_2^2 + px_3^2$ is isotropic over $\mathbb{Q}_\nu$ for $\nu \neq p$. Then, by the product formula, A is necessarily ramified in $p$.
Consider the order $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\frac{1+j}{2} \oplus \mathbb{Z}i \oplus \mathbb{Z}i\frac{1+j}{2}$, with $i^2 = -1, j^2 = -p, ij = -ji$. It has discriminant $\mathrm{disc}_\Lambda = p^2\mathbb{Z}$ since

$$\det \begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & \frac{1+b}{2} & 0 & 0 \\ 0 & 0 & 2a & a \\ 0 & 0 & a & \frac{a-ab}{2} \end{bmatrix} = -p^2.$$

Hence $\Lambda$ is maximal since $\mathrm{disc}_\Lambda = \mathrm{disc}_\mathrm{A}$.
(2) Let $n \in \mathbb{N}$, $(n,3) = 1$. Consider the cyclotomic field $\mathbb{Q}(\zeta_n)$, and let $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ be its maximal real subfield of degree $\varphi(n)/2$.
Assume moreover that $p \equiv 1 \pmod{n}$. Hence the two places of $\mathbb{Q}$ in which A is ramified, split totally in $\mathbb{K}/\mathbb{Q}$. Then consider $\mathrm{A}_\mathbb{K} = \mathrm{A} \otimes \mathbb{K}$, by Proposition 7.12, it is a division algebra and $\Lambda_\mathbb{K} := \Lambda \otimes \mathcal{O}_\mathbb{K}$ is a maximal order.
For $\Theta$ the reduction modulo the $N = \varphi(n)/2$ primes above $p$, we get a code over $\mathbb{F}_p^N$.
Take $p'$ a prime different from $p$ such that $p' \equiv 1 \pmod{n}$ so that $p'$ splits in $\mathbb{K}$. For $\Theta$ the reduction modulo the $N = \varphi(n)/2$ primes above $p'$, we thus get a code of length $N = \varphi(n)/2$ over $\mathsf{M}_2(\mathbb{F}_{p'})$.

### 7.5. Asymptotic Behavior. —

*7.5.1. The construction.* — Let A be a division algebra of degree $d > 1$ over $\mathbb{K}$. Let $S$ be the set of places of $\mathbb{K}$ in which A is ramified. Let $T$ be a finite set of primes of $\mathbb{K}$.

Suppose that $\mathbb{K}$ has an infinite tower $\mathbb{L} = \bigcup_n \mathbb{K}_n$ of number fields such that:

(A) archimedean places and places of $T$ are totally split in $\mathbb{L}/\mathbb{K}$ ;
(B) for every integer $n$ and number field $\mathbb{K}_n$, we associate a division algebra $\mathrm{A}_n$ of center $\mathbb{K}_n$ and of fixed degree $d$ over $\mathbb{K}_n$ such that the sequence $(\mathrm{rd}_{\mathrm{A}_n})_n$ is bounded by $\mathsf{B} \in \mathbb{R}$.

In particular $(\mathrm{rd}_{\mathbb{K}_n})_n$ is bounded and $\mathbb{L}/\mathbb{K}$ is asymptotically good.

For every $n \geq 0$, fix a maximal $\mathcal{O}_{\mathbb{K}_n}$-order $\Lambda_n$ of $\mathrm{A}_n$.
Set $N = \#T$. Then $T(\mathbb{K}_n)$ contains $N_n := N[\mathbb{K}_n : \mathbb{K}]$ places $\mathfrak{p}$, all of which have residual field of cardinality $q_0$. Thus $N \leq [\mathbb{K} : \mathbb{Q}]$.

Let $\{\mathfrak{P}_1^{(n)}, \ldots, \mathfrak{P}_{N_n}^{(n)}\}$ be the nonzero prime ideals of $\Lambda_n$ above the primes of $T(\mathbb{K}_n)$ and consider the map $\Theta_n$ :

$$\Theta_n : \Lambda_n \to \prod_{i=1}^{N_n} \Lambda/\mathfrak{P}_i^{(n)},\ x \mapsto (x \bmod \mathfrak{P}_1^{(n)}, \ldots, x \bmod \mathfrak{P}_{N_n}^{(n)}).$$

To simplify, we suppose that for $i = 1, \cdots N_n$, $\#\Lambda_n/\mathfrak{P}_i^{(n)} = q$, where $q_0|q$. For example, this will always be the case if for the primes of $T(\mathbb{K})$, we have $\#\Lambda/\mathfrak{P}_i = q$ and if the algebras $\mathrm{A}_n$ are not ramified in $T(\mathbb{K}_n)$, or if the algebras $\mathrm{A}_n$ are totally ramified in $T(\mathbb{K}_n)$.

We thus start with codes built in Section 7 as follows. For every integer $n$ and number field $\mathbb{K}_n$ from the tower $\mathbb{L} = \bigcup_n \mathbb{K}_n$, we fix the compact $\mathsf{K}_n(t)$ of $\prod_{v\in\mathbb{P}_\infty(\mathbb{K}_n)} \mathrm{A}_{n,v} \simeq \mathbb{R}^{[\mathbb{K}_n:\mathbb{K}]d^2}$ given by

$$\mathsf{K}_n(t) = \{x \in \prod_{v\in\mathbb{P}_\infty(\mathbb{K}_n)} \mathrm{A}_{n,\sigma}, \|x\|_2 \leq t, \forall\sigma\}.$$

Consider then the embedding $\Psi_n : \mathrm{A}_n \to \prod\limits_{v\in\mathbb{P}_\infty(\mathbb{K}_n)} \mathrm{A}_{n,\sigma}$.

We then have the family of codes $\mathcal{C}_n$ from maximal orders defined by

$$\mathcal{C}_n := \mathcal{C}_{z_n,t}(\Lambda_n) = \Theta_n(\Psi^{-1}(\mathsf{K}_{z_n}(t)) \cap \Lambda_n),$$

where $\mathsf{K}_{z_n}(t) = z_n + \mathsf{K}_n(t)$, and the element $z_n$ is $\Lambda_n$-admissible.

For a fixed $n$, if the algebra $\mathrm{A}_n$ is not ramified at $\mathfrak{P}_i^{(n)} \in T(\mathbb{K}_n)$, $i = 1, \cdots, N_n$, codewords from $\mathcal{C}_n$ are found in $\Big(\mathsf{M}_d(\mathbb{F}_{q_0})\Big)^{N_n}$, they are of length $N_n = N[\mathbb{K}_n : \mathbb{K}] \longrightarrow \infty$ when $n \to \infty$. In this case $q = q_0^{d^2}$.
On the contrary, if $\mathrm{A}_n$ is totally ramified in $\mathfrak{P}_i^{(n)} \in T(\mathbb{K}_n)$, then codewords are in $\Big(\mathbb{F}_{q_0^d}\Big)^{N_n}$.

*7.5.2. Parameters.* — We give bounds on the relative minimum distance and the rate of additive codes, which have consequences on the code alphabet we are able to obtain asymptotically.

***Proposition 7.11.*** — *Suppose that*

$$N > d^2[\mathbb{K} : \mathbb{Q}] \log_q\Big(\frac{2t}{d^{1/2}}\Big).$$

*Then the obtained codes have parameters :*

(*i*) $\dfrac{1}{N[\mathbb{K}_n : \mathbb{K}]} d_H(\mathcal{C}_n) \geq 1 - \dfrac{[\mathbb{K} : \mathbb{Q}]d^2}{N} \log_q\Big(\dfrac{2t}{d^{1/2}}\Big)$.

(*ii*) $\dfrac{1}{[\mathbb{K}_n : \mathbb{K}]} \log_q(|\mathcal{C}_n|) \geq \log_q \mathbb{V}_{r_1,r_2,d} + d^2[\mathbb{K} : \mathbb{Q}] \log_q t - \dfrac{[\mathbb{K} : \mathbb{Q}]d^2}{2} \log_q \mathsf{B}$.

*Proof.* — This is a consequence of Propositions 7.8 and 7.10, noting that $\mathbb{V}_{r_1(\mathbb{K}_n),r_2(\mathbb{K}_n),d} = [\mathbb{K}_n : \mathbb{K}]\mathbb{V}_{r_1,r_2,d}$, since infinite places are totally split in $\mathbb{L}/\mathbb{K}$. □

*7.5.3. Discussion.* — Given the arithmetic context of Section 7.5.1, we see that for $q$ large enough, we can find a parameter $t$ for which $\log_q(|\mathcal{C}_n|) > 0$ and $d_H(\mathcal{C}_n) > 0$. Indeed the proposed construction gives rise to asymptotically good codes, as long as we can find a parameter $t \in \mathbb{R}_{>0}$ satisfying the double inequality:

$$\frac{1}{2}\log_q \mathsf{B} - \frac{1}{d^2[\mathbb{K} : \mathbb{Q}]} \log_q \mathbb{V}_{r_1,r_2,d} \leq \log_q(t) \leq \frac{N}{d^2[\mathbb{K} : \mathbb{Q}]} + \log_q\Big(\frac{d^{1/2}}{2}\Big).$$

The parameter $t$ exists as long as

$$\frac{N}{d^2[\mathbb{K} : \mathbb{Q}]} \geq \frac{1}{2}\log_q \mathsf{B} - \log_q\Big(\frac{d^{1/2}}{2}\Big) - \frac{1}{d^2[\mathbb{K} : \mathbb{Q}]} \log_q \mathbb{V}_{r_1,r_2,d}. \tag{1}$$

Since the left hand side term does not depend on $q$, we conclude that this will be true for $q$ large enough.

A natural way to produce codes over an alphabet $\mathcal{A}(\mathbb{F}_p) = \mathbb{F}_q$ would be to take $\Theta_n$ the reduction modulo some primes $\mathfrak{P}_i^{(n)}$ that are *totally ramified*: in particular, $T(\mathbb{K}_n) \subset S(\mathbb{K}_n)$. In this case, for every $\mathfrak{p} \in \mathsf{T}(\mathbb{K}_n)$, $f_\mathfrak{p} = 1$, $e_\mathfrak{p} = d$ and $q = \mathsf{N}(\mathfrak{p})^d$.
Hence

$$\log_q \mathrm{rd}_{\mathrm{A}_n} \geq \log_q \mathrm{rd}_{\mathbb{K}_n} + \frac{N(d-1)}{d^2[\mathbb{K}:\mathbb{Q}]}.$$

The condition (1) becomes (for $d \geq 2$):

$$(2) \qquad \frac{1}{2}\log_q \mathrm{rd}_{\mathbb{K}_n} \leq \frac{N}{d^2[\mathbb{K}:\mathbb{Q}]}\Big(\frac{3-d}{2}\Big) + \frac{1}{d^2[\mathbb{K}:\mathbb{Q}]}\log_q \mathbb{V}_{r_1,r_2,d} + \frac{1}{2}\log_q \frac{d}{4}.$$

In particular, this implies

$$\begin{aligned}\frac{1}{2}\log_q \mathrm{rd}_{\mathbb{K}_n} &\leq \frac{3}{2d^2} + \frac{1}{d^2[\mathbb{K}:\mathbb{Q}]}\log_q \mathbb{V}_{r_1,r_2,d} + \frac{1}{2}\log_q \frac{d}{4}\\ &\leq \frac{1}{d^2}\Big(\frac{3}{2} + \log_q \mathbb{V}_4\Big) + \frac{1}{2}\log_q \frac{d}{4}\\ &\leq \frac{3}{8} + \frac{1}{4}\log_q \mathbb{V}_4 + \frac{1}{2}\log_q \frac{d}{4},\end{aligned}$$

which implies $d \geq 48$ by asymptotic estimates of the lower bounds of the root discriminant of number fields (under GRH, $\mathrm{rd}_{\mathbb{K}_n} \geq 44.7$) and by the behavior of $\mathbb{V}_k$ when $k$ varies. However for $d$ large,

$$\frac{1}{d^2[\mathbb{K}:\mathbb{Q}]}\log_q \mathbb{V}_{r_1,r_2,d} \sim_{d\to\infty} -2\log_d d$$

and the condition (2) shows that this construction does not given a favorable situation. We leave the question of building asymptotic codes from maximal order codes over $\mathbb{F}_q$ open, and focus on matrix alphabet.

*7.5.4. By tensor product.* — When studying the asymptotic behavior of codes, we will need the stability of the property of being division after scalar extension.

***Proposition 7.12.*** — *Let* A *be a division algebra of dimension* $d^2$ *over the number field* $\mathbb{K}$. *Denote by* $S$ *the set of ramification of* A. *Let* $\Lambda$ *be a maximal order of* A. *Let* $\mathbb{L}/\mathbb{K}$ *be a finite extension. Suppose that for all* $v \in S$, *and* $w|v$, $w \in \mathbb{P}_\mathbb{L}$, $(e_v, [\mathbb{L}_w : \mathbb{K}_v]) = 1$. *Then* $\mathrm{A}_\mathbb{L} := \mathrm{A} \otimes \mathbb{L}$ *is a division algebra. Moreover, if for all* $v \in S_0$, $v$ *is unramified in* $\mathbb{L}/\mathbb{K}$, *then* $\Lambda_\mathbb{L} := \Lambda \otimes \mathcal{O}_\mathbb{L}$ *is a maximal order of* $\mathrm{A}_\mathbb{L}$ *and*

$$\mathrm{rd}_{\mathrm{A}_\mathbb{L}} = \mathrm{rd}_\mathbb{L}\Big(\prod_{\mathfrak{p}\in S_0}(\mathsf{N}_{\mathbb{K}/\mathbb{Q}}\mathfrak{p})^{1-1/e_\mathfrak{p}}\Big)^{\frac{1}{[\mathbb{K}:\mathbb{Q}]}} \leq \mathrm{rd}_\mathbb{L}\Big(\prod_{\mathfrak{p}\in S_0}\mathsf{N}_{\mathbb{K}/\mathbb{Q}}\mathfrak{p}\Big)^{\frac{d-1}{d[\mathbb{K}:\mathbb{Q}]}}.$$

*Proof.* — Let $S'$ be the set of ramification of $\mathrm{A}_\mathbb{L}$. First, thanks to [**1**], Corollary 4.5.11, one has $S' = S(\mathbb{L})$ and for all $w|v \in S$, $e_w = e_v$. Moreover for $w|v$, $\alpha_w = [\mathbb{L}_w : \mathbb{K}_v]\alpha_v$ (the local symbol is "multiplied" by the local degree). Consequently $\mathrm{A}_\mathbb{L} \simeq \mathsf{M}_m(\mathsf{D})$, where $\mathsf{D}$ is a division algebra of degree the lcm of $\alpha_w$ which is equal to the lcm of $\alpha_v$, *i.e.* of degree $d$. Comparing the dimensions, we have $m = 1$.
Now take an $\mathcal{O}_\mathbb{K}$-basis $\{b_1, \cdots, b_{d^2}\}$ of $\Lambda$. Then $\mathrm{disc}_\Lambda$ is the principal ideal generated by $\det(\mathrm{Trd}(b_ib_j))$. Now remark that $\{b_1, \cdots, b_{d^2}\}$ is an $\mathcal{O}_\mathbb{L}$-basis of $\Lambda_\mathbb{L}$. Hence, $\mathrm{disc}(\Lambda_\mathbb{L}) = \mathrm{disc}_\Lambda\mathcal{O}_\mathbb{L}$. But if we assume moreover that every prime $\mathfrak{p} \in S_0$ is unramified in $\mathbb{L}/\mathbb{K}$, then as $e_v = e_w$, one has $\mathrm{disc}_\Lambda\mathcal{O}_\mathbb{L} = \mathrm{disc}_{\mathrm{A}_\mathbb{L}}$ and then the order $\Lambda_\mathbb{L}$ is maximal.

The computation of the discriminant is then obvious. □

Let $\mathbb{L} = \bigcup_n \mathbb{K}_n$ be a tower of $\mathbb{K}$. If A is a division algebra over A, and $\Lambda$ a maximal order of A, for every integer $n$, denote by $\mathrm{A}_n := \mathrm{A} \otimes \mathbb{K}_n$ and $\Lambda_n = \Lambda \otimes \mathcal{O}_{\mathbb{K}_n}$.

***Corollary 7.13***. — *Let* A *be a division algebra over* $\mathbb{K}$ *ramified at* $S$. *Let* $\mathbb{L} = \bigcup_n \mathbb{K}_n$ *be an asymptotically good tower of* $\mathbb{K}$. *Suppose that* $\mathbb{L}/\mathbb{K}$ *is unramified at* $S_0$ *and that for all* $v \in S$, *and for all integer* $n$, $(e_v, [\mathbb{K}_n : \mathbb{K}]) = 1$ *(which is the case if* $(d, [\mathbb{K}_n : \mathbb{K}]) = 1$*). Then for every integer* $n$, *the central simple algebra* $\mathrm{A}_n$ *is a division algebra over* $\mathbb{K}_n$ *with root discriminant* $\mathrm{rd}_{\mathrm{A}_n}$ *bounded by* $\mathrm{rd}_{\mathbb{L}}\Big(\prod_{\mathfrak{p}\in S_0} \mathsf{N}_{\mathbb{K}/\mathbb{Q}}\mathfrak{p}\Big)^{\frac{d-1}{d[\mathbb{K}:\mathbb{Q}]}}$. *Moreover* $\Lambda_n$ *is a maximal order of* $\mathrm{A}_n$.

*7.5.5. By symbol reciprocity.* — We consider Remark 6.3 in the current context. We start from an asymptotically good extension $\mathbb{L}/\mathbb{K}$ such that

($i$) the primes in $T$ are totally split in $\mathbb{L}/\mathbb{K}$;
($ii$) there exists a place $v \in \mathbb{P}_{\mathbb{K}}$, $v \notin T$, with $v$ totally split in $\mathbb{L}/\mathbb{K}$.

Let $\mathbb{L} = \bigcup_n \mathbb{K}_n$ be a tower of $\mathbb{L}$. For every $n > 1$, choose $v_n^{(1)}$ and $v_n^{(2)}$ two places of $\mathbb{K}_n$ above $v$ and consider the division algebra $\mathrm{A}_n$ with center $\mathbb{K}_n$, ramified only in $v_i^{(n)}$, $i = 1, 2$, with local symbols $1/d$ and $1 - 1/d$.
As noted in Remark 6.3, we have $\mathrm{rd}_{\mathrm{A}_n} \longrightarrow \mathrm{rd}_{\mathbb{K}}$ when $n \to \infty$.

A particularly favorable context is that of quaternion algebras over number fields which are not totally imaginary. In that case, the $p$-tower $\mathbb{K}_\emptyset^T/\mathbb{K}$ is a natural candidate (in particular for $p = 2$): indeed, it suffices to then take for $v$ an infinite real place of $\mathbb{K}$.

*7.5.6. Examples.* — • Apply infinity criteria to 2-towers of real quadratic fields.
The field $\mathbb{K} = \mathbb{Q}(\sqrt{3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23})$ has a 2-class group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^7$. We take $T = \{\mathfrak{p}\}$ with an arbitrary $\mathfrak{p}$. Then the 2-tower $\mathbb{K}_\emptyset^T$ of $\mathbb{K}$, *i.e.* the 2-extension which is not ramified anywhere and totally split in $\mathfrak{p}$, is infinite. We note that real places remain real. Set $\mathbb{K}_\emptyset^T = \bigcup_n \mathbb{K}_n$. Let A be a quaternion algebra ramified in infinite places over $\mathbb{K}$ and set $\mathrm{A}_n = \mathrm{A} \otimes \mathbb{K}_n$. According to Corollary 7.13, the algebra $\mathrm{A}_n$ is division, of center $\mathbb{K}_n$, and of root discriminant $\mathrm{rd}_{\mathrm{A}_n} = \mathrm{rd}_{\mathbb{K}_n} = \mathrm{rd}_{\mathbb{K}}$.
We set $q_0 = \mathcal{O}_{\mathbb{K}}/\mathfrak{p}$; then here $\mathcal{A}(\mathcal{C}_n) = \mathsf{M}_2(\mathbb{F}_{q_0})$ and $q = q_0^4$. Also $\mathbb{V}_{2,0,2} = \mathbb{V}_4^2 = (\frac{\pi^2}{2})^2$.
By (1), the proposed codes will be asymptotically good as soon as

$$q_0^4 = q \geq \Big(2^{1/2}\mathrm{rd}_{\mathbb{K}}^{1/2}\Big(\frac{2}{\pi^2}\Big)^{1/4}\Big)^8,$$

or $q_0 \geq 401708303$. For example, $\mathfrak{p}$ one of the two primes above $p = 401708303$ suits. Alternatively $\mathfrak{p} = 20047\mathcal{O}_{\mathbb{K}}$ suits (it is inert here), in which case $q_0 = 20047^2 = 401882209$. In all cases, codewords belong to $\Big(\mathsf{M}_2(\mathbb{F}_{q_0})\Big)^{[\mathbb{K}_n:\mathbb{K}]}$.

• We can use a refined criterion with the field $\mathbb{K} = \mathbb{Q}(\sqrt{3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 19\cdot 23})$. Here $\mathrm{Cl}_2(\mathbb{K}) \simeq \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^5$. If we take $T = \{\mathfrak{p}\}$ with $\mathfrak{p}$ inert in $\mathbb{K}/\mathbb{Q}$, then $d_2\mathrm{Cl}_2^T(\mathbb{K}) = d_2\mathrm{Cl}_2(\mathbb{K}) \geq 6$ and thus the 2-tower $\mathbb{K}_\emptyset^T/\mathbb{K}$ is infinite. We get $q_0 \geq 23629901$ and may take $\mathfrak{p} = 4871\mathcal{O}_{\mathbb{K}}$.

• Take the field $\mathbb{K} = \mathbb{Q}(\cos(2\pi/11), \sqrt{2}, \sqrt{-23})$. We have seen that $\mathbb{K}$ has a 2-tower $S$ which is split for $S = \{\mathfrak{p}\}$ as soon as $\mathfrak{p}$ is totally split in the 2-Hilbert field of $\mathbb{K}$. See §5.1.3. Consider a quadratic extension $\mathbb{K}'/\mathbb{K}$ in the tower. The field $\mathbb{K}'$ is of degree 40 over $\mathbb{Q}$. There are two primes $\mathfrak{p}_i$ in $\mathcal{O}_{\mathbb{K}'}$ above $\mathfrak{p}$. The prime $\mathfrak{p}_1$ governs the ramification of algebras to come. The prime $\mathfrak{p}_2$ governs the code alphabet. More precisely, for $n \geq 1$, we set $T(\mathbb{K}_n) = \{\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}_n}, \mathfrak{p}|\mathfrak{p}_2\}$. We have $\#T(\mathbb{K}_n) = [\mathbb{K}_n : \mathbb{K}']$. For every integer $n \geq 1$, let then $\mathrm{A}_n$ be the quaternion algebra ramified in $\mathfrak{p}'_{1,n}$ and $\mathfrak{p}''_{1,n}$, where $\mathfrak{p}'_{1,n}$ and $\mathfrak{p}''_{1,n}$ are primes of $\mathcal{O}_{\mathbb{K}_n}$ dividing $\mathfrak{p}_1$.

As noted in Remark 6.3, we have $\mathrm{rd}_{\mathrm{A}_n} \longrightarrow \mathrm{rd}_{\mathbb{K}} = 11^{4/5}2^{3/2}23^{1/2} = 92.368\ldots$ when $n \to \infty$. Here $\mathbb{V}_{r_1,r_2,d} = (\frac{\pi^4}{24})^{20}$. We find

$$q_0^4 = q \geq \Big(2^{1/2}\mathrm{rd}_{\mathbb{K}}^{1/2}\Big(\frac{24}{\pi^4}\Big)^{1/8}\Big)^{160}.$$

For example, we may take $q_0 = 16943^{10}$ and $\mathcal{A}(\mathcal{C}_n) = \mathsf{M}_2(\mathbb{F}_{q_0})$.

## 8. Multiplicative codes

**8.1. Units of a maximal order of a skewfield.** — We remain in the context of division algebras. To simplify, we propose a construction when $d = 2$, *i.e.* in the context of quaternion algebras. The principal references here are [**32**], [**13**, Chapters 8 and 11], [**24**, Chapters 3 and 4].

Let $\mathbb{K}$ be a number field. Let $\mathrm{A} = \mathrm{A}_{\mathbb{K}}$ be a division quaternion algebra ramified in $S$. We suppose that A is not ramified in at least one infinite place $v \in \mathbb{P}_\infty$: the algebra A satisfies Eichler's condition. In other terms, following the notations of Section 6, $S_\infty \neq \mathbb{P}_\infty$.

Let us fix $\Lambda$ a maximal order of A. Let

$$\Lambda^1 = \{x \in \Lambda, \mathrm{Nrd} x = 1\},$$

be the group of of elements of $\Lambda$ of reduced norm equal to 1. It is also the subgroup of units $\Lambda^\times$ of $\Lambda$ of reduced norm 1.

Let $v \in \mathbb{P}_{\mathbb{R}}^0 \cup \mathbb{P}_{\mathbb{C}}$ and consider $\Psi_v$ the embeddings of $\Lambda^1$ in the completions $\mathrm{A}_v = \mathsf{M}_2(\mathbb{K}_v)$, where $\mathbb{K}_v = \mathbb{R}$ or $\mathbb{K}_\sigma = \mathbb{C}$. Take $x \in \Lambda^1$. As $\mathrm{Nrd}(x) = 1$, $\det(\sigma(x)) = 1$ hence $\sigma(x) \in \mathrm{Sl}_2(\mathbb{K}_\sigma)$.

Set $\mathrm{G} = \prod_{v \in \mathbb{P}_{\mathbb{R}}^0 \cup \mathbb{P}_{\mathbb{C}}} \mathrm{Sl}_2(\mathbb{K}_\sigma)$: it is a locally compact group. Endow G with the Tamagawa measure $\mu$. Hence, let

$$\Psi : \Lambda^1 \to \mathrm{G}$$

be the natural embedding of $\Lambda^1$ in G, corresponding to the the completions at unramified archimedean places (we still denote by abuse $\Psi$ the restriction of $\Psi$ to $\Lambda^1$). The map $\Psi$ is a homomorphism. In fact, one has more:

***Theorem 8.1.*** — *Assume that $S_\infty \neq \mathbb{P}_\infty$. Then the group $\Psi(\Lambda^1)$ is a lattice of* G, *isomorphic to $\Lambda^1$, with covolume*

$$\mu(\mathrm{G}/\Psi(\Lambda^1)) = \zeta_{\mathbb{K}}(2)(4\pi^2)^{-s}|\mathrm{disc}_{\mathbb{K}}|^{3/2} \prod_{\mathfrak{p} \in S_0} (\mathsf{N}\mathfrak{p} - 1),$$

*where $s = |\mathbb{P}_{\mathbb{R}}^1| = |S_\infty|$.*

*Proof.* — See for example Vigneras [**32**, Chapitre IV, Corollary 1.8]. □

***Remark 8.2.*** — Here the quotient $\mathrm{G}/\Psi(\Lambda^1)$ is compact.

**8.2. Volume Estimation.** — We recall how to obtain the Tamagawa measure of the locally compact group $\mathrm{Sl}_2(\mathbb{R})$. It is a normalized Haar measure, which allows to obtain naturally the computation of Theorem 8.1. We rely on Iwasawa's decomposition $\mathrm{Sl}_2(\mathbb{R}) = KAN$ where

$$\begin{aligned} K &= \mathrm{SO}_2(\mathbb{R}) = \{\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix},\ \varphi \in [0, 2\pi]\}, \\ A &= \{\begin{pmatrix} y & 0 \\ 0 & 1/y \end{pmatrix},\ y \in \mathbb{R}^\times\},\ \text{and } N = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R}\}. \end{aligned}$$

The Tamagawa measure $\mu$ over $\mathrm{Sl}_2(\mathbb{R})$ is equal to $yd\varphi dxdy$ (see [**24**, Example §4.6, Chapter 4]). We recall how it is obtained. By compatibility, the Tamagawa measure $\mu$ over $\mathrm{Sl}_2(\mathbb{R})$ verifies $\mu = \mu'\mu_{AN}$, where $\mu'$ is the Tamagawa measure over $\mathrm{SO}_2(\mathbb{R})$. Then, still by compatibility, $\mu_{AN} = y^2\mu_A\mu_N$. It then suffices to recall that the Tamagawa measure $\mu_N$ over $N$ is the Lebesgue measure $dx$, here $N \simeq (\mathbb{R}, +)$, and then the Tamagawa measure $\mu_A$ over $A$ is the measure $\dfrac{1}{y}dy$, here $A \simeq (\mathbb{R}^\times, \cdot)$; finally $\mu_{AN} = ydxdy$. Recall that $\mu_K(\mathrm{SO}_2(\mathbb{R})) = \pi$ (see [**32**, Corollary 2.6, chapter IV]).
Let $\mathbb{B}(0, t)$ be the sphere of $\mathsf{M}_2(\mathbb{R})$ of center 0 and radius $t$ for the norm $\|\cdot\|_2$.

***Lemma 8.3.*** — *For every $t \in \mathbb{R}_{>2.35}$, $\mu\Big(\mathbb{B}(0,t) \cap \mathrm{Sl}_2(\mathbb{R})\Big) \geq\ t$.*

*Proof.* — Every element $X \in \mathrm{Sl}_2(\mathbb{R})$ is uniquely written as $X = kan$, with $k \in K$, $a = \begin{pmatrix} y & 0 \\ 0 & 1/y \end{pmatrix}$ and $n = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.
Set $B(t) = \{(x, y) \in \mathbb{R}^2,\ y^2 + 1/y^2 + y^2x^2 \leq t\}$ and

$$B_\infty(t) = \{(x, y) \in \mathbb{R}^2,\ \sqrt{3}/\sqrt{t} \leq |y| \leq \frac{\sqrt{t}}{\sqrt{3}},\ |x| \leq 1\}.$$

Then $B_\infty(t) \subset B(t)$ and hence

$$\begin{aligned} \mu\Big(\mathbb{B}(0,t) \cap \mathrm{Sl}_2(\mathbb{R})\Big) &= \mu_K(\mathrm{SO}_2(\mathbb{R}))\mu_{AN}(B(t)) \\ &\geq \mu(\mathrm{SO}_2(\mathbb{R}))\mu_{AN}(B_\infty(t)) = \pi\int_{B_\infty(t)} ydxdy. \end{aligned}$$

It then suffices to note that

$$\int_{B_\infty(t)} ydxdy = \frac{2}{3}t - \frac{6}{t}.$$

Thus $\mu\Big(\mathbb{B}(0,t) \cap \mathrm{Sl}_2(\mathbb{R})\Big) \geq t$ as soon as $t \geq \sqrt{\frac{18}{2\pi - 3}} \simeq 2.3414\ldots$. □

***Remark 8.4.*** — The computation of this lemma privileges the choice of the norm $\|\cdot\|_2$ with respect to the norm $\|\cdot\|_\infty$.

**8.3. The code and its parameters (the totally real case).** — There are various contexts, we will develop the totally real case. Start with a totally real number field $\mathbb{K}$ of degree $n$ over $\mathbb{Q}$ and with a division algebra A for which $S_\infty = \emptyset$, *i.e.* A is not ramified in infinite places. Then for a place $v \in \mathbb{P}_\infty$, we have $\mathrm{Sl}_2(\mathbb{K}_\sigma) = \mathrm{Sl}_2(\mathbb{R})$.

The locally compact group here is the group $\mathrm{G} = \prod_{\sigma \in \mathbb{P}_\infty} \mathrm{A}_\sigma \simeq \mathrm{Sl}_2(\mathbb{R})^{r_1}$, with $r_1 = n = [\mathbb{K} : \mathbb{Q}]$.

Set $\mathsf{K}(t) = \{x \in \prod_{\sigma \in \mathbb{P}_\infty} \mathrm{A}_\sigma, \|\sigma(x)\|_2 \leq t, \forall \sigma\}$.

Fix then $\Lambda$ a maximal order of A. We take as lattice of G the group $\Psi(\Lambda^1)$.
As for the additive case, we need to translate the original code to have enough points.

***Lemma 8.5***. — *Suppose* $t \geq 2.35$.
*There exists* $z \in \mathrm{G}$ *such that* $\#\Psi(\Lambda^1) \cap z\mathsf{K}(t) \geq \dfrac{t^n}{\mu(\Psi(\Lambda^1)\backslash \mathrm{G})}$. *Such an element* $z$ *is called* $\Lambda^1$*-admissible.*

*Proof.* — This is a consequence of Lemma 1.6 and 8.3. □

As for the additive case, let $T = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_N\}$ be a set of prime ideals of $\Lambda$. Consider

$$\Theta : \Lambda \to \prod_{i=1}^{N} \Lambda/\mathfrak{P}_i, \ x \mapsto (x \pmod{\mathfrak{P}_1}, \ldots, x \pmod{\mathfrak{P}_N}).$$

The code $\mathcal{C}_{z,t}(\Lambda^1)$ is defined by

$$\Theta\Big(\Psi^{-1}(\mathsf{K}_z(t) \cap \Lambda^1)\Big),$$

where $\mathsf{K}_z(t) = z\mathsf{K}(t)$ for an element $\Lambda^1$-admissible $z$.

***Proposition 8.6***. — *(i)* $d_H(\mathcal{C}_{z,t}(\Lambda^1) \geq N - \dfrac{nd}{2}\Big(\log_q(2t\|z\|_\infty) + \log_q(\sqrt{d})\Big)$.
*(ii) If furthermore,* $N > \frac{nd}{2}\Big(\log_q(2t\|z\|_\infty) + \log_q(\sqrt{d})\Big)$ *then*

$$\log_q(|\mathcal{C}_{z,t}(\Lambda^1)|) \geq n\log_q(t) - \log_q \zeta_{\mathbb{K}}(2) - \frac{3}{2}\log_q|\mathrm{disc}_{\mathbb{K}}| - \sum_{\mathfrak{p} \in S_0} \log_q(\mathsf{N}\mathfrak{p} - 1).$$

*Proof.* — *(i)* We follow the proof of Proposition 7.8. Consequently, for every $\sigma \in \mathbb{P}_\infty$,

$$\|\sigma(y)\|_2 = \|\sigma(z)(\sigma(x) - \sigma(x'))\|_2 \leq 2\|z\|_\infty t.$$

Then $\mathsf{N}(y) \leq \Big(\dfrac{2t\|z\|_\infty}{\sqrt{d}}\Big)^{nd^2}$ and the inequality is immediate. □

***Remark 8.7***. — We notice a mix of multiplicative and additive contexts, which causes a problem to an asymptotic study which comes from the element $z$. This problem did not happen for unit codes, because of the logarithm. We note that the formula for the dimension is well understood asymptotically.

## Acknowledgement

The authors would like to thank Aurel Page for his careful reading and for his interest in this work. The research of F. Oggier is supported in part by the Nanyang Technological University under Research Grant M58110049 and M58110070. Part of this work was done while C. Maire was visiting the Division of Mathematical Sciences, Nanyang Technological University, Singapore. C. Maire thanks the Région Franche-Comté and the Division of Mathematical Sciences, NTU, Singapore for the financial support of these visits.

# References

[1] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge studies in advanced mathematics 101, Cambridge University Press, 2006.

[2] G. Gras, *Class Field Theory*, SMM, Springer 2003.

[3] V. Guruswami, *Construction of codes from number fields*, IEEE Transactions on Information Theory **49** (3) (2003), 594-603.

[4] F. Hajir and C. Maire, *Asymptotically good towers of global fields*, Proceedings of the European Congress of Mathematics, Barcelona 2000, Progress in Math. 202, 207-218.

[5] F. Hajir and C. Maire, *Extensions of number fields with wild ramification of bounded depth*, International Math. Research Notices **13** (2002), 667-696.

[6] F. Hajir and C. Maire, *Tamely ramified towers and discriminant bounds for number fields II*, Journal of Symbolic Computation **33** (2002), 415-423.

[7] F. Hajir and C. Maire, *Tamely ramified towers and discriminant bounds for number fields*, Compositio Math. **128** (2001), 35-53.

[8] F. Hajir and C. Maire, *On the invariant factors of Class Groups in towers of number fields*, Canadian Journal of Math., to appear.

[9] H. Koch, *Galoissche Theorie der p-Erweiterungen*, Springer-Verlag, 1970.

[10] KANT/KASH, Computational Algebraic Number Theory/KAnt SHell, version 2.5., `http://page.math.tu-berlin.de/~kant/kash.html`.

[11] S. Lang, *Algebraic Number Theory*, Addison-Wesley Publishing Company, INC., 1970.

[12] H.W. Lenstra, *Codes from algebraic number fields*, In: M. Hazewinkel, J.K. Lenstra, L.G.C.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.

[13] C. Maclachlan and A. W. Reid, *The arithmetic of hyperbolic* 3*-manifolds*, GTM 219, Springer, 2003.

[14] C. Maire, *Finitude de tours et p-tours $T$-ramifiées modérées, $S$-décomposées*, J. Th. des Nombres de Bordeaux **8** (1996), 47-73.

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

[16] P.J. Morandi and B.A. Sethuraman, *Divisor on Division Algebras and Error Correcting Codes*, Communications in Algebra **26** (1998), 3211-3221.

[17] T. Nakashima, *Construction of Codes from Arakelov Geometry*, Des. Codes Cryptogr. **73** (2014), 47-54.

[18] T. Nakashima, *AG Codes and Vector Bundles on Rational Surfaces*, International Journal of Pure and Applied Mathematics **96** no 3 (2014), 329-342.

[19] GNU Octave, `https://www.gnu.org/software/octave/`.

[20] F.J. Mac Williams, N.J.A Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 3rd edition, 1981.

[21] 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 **2** (1990), 119-141.

[22] A. Page, *Méthodes explicites pour les groupes arithmétiques*, PhD Thesis, Bordeaux (France), 2014.

[23] The PARI Group, PARI/GP version 2.6.1, `http://pari.math.u-bordeaux.fr/`.

[24] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure and Applied Math. Series **139**, Academic Press Inc, Harcourt Brace and Compagny Publishers, 1994.

[25] I. Reiner, *Maximal Orders*, London Math. Society Monographes New Series **28**, Oxford Science Publications, 2003.

[26] P. Roquette, *On class field towers*, In J.-W.-S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press London, 1967.

[27] M.Y. Rosenbloom and M. Tsfasman, *Multiplicative lattices in global fields*, Invent. Math. **101** (1990), no. 3, 687–696.

[28] R. Schoof, *Infinite class field towers of quadratic fields*, J. reine angew. Math. **372** (1986), 209-220.

[29] R. Schoof and V. Der Geer, *Effectivity of Arakelov divisors and the analogue of the theta divisor of a number field*, Selecta Math. New Ser. **6** (2000), 377-398.

[30] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic Geometric Codes: Basic Notions*, Mathematical Surveys and Monographs 139, AMS, 2007.

[31] M. Tsfasman and S. Vladut, *Infinite global fields and the generalized Brauer-Siegel theorem*, Dedicated to Yuri I. Manin on the occasion of his 65th birthday, Mosc. Math. Journal **2** (2002), no.2, 329-402.

[32] M.-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lectures Notes Math. **800**, Springer, 1980.

*July 18, 2017*

Christian Maire, Laboratoire de Mathématiques de Besançon, Université Bourgogne Franche-Comté et CNRS (UMR 6623), 16 route de Gray, 25030 Besançon cédex, France.
*E-mail :* christian.maire@univ-fcomte.fr

Frédérique Oggier, Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. • *E-mail :* frederique@ntu.edu.sg