CODES FROM UNIT GROUPS OF DIVISION ALGEBRAS OVER NUMBER FIELDS

by

Christian Maire & Aurel Page

Abstract. — Lenstra and Guruswami described number field analogues of the algebraic geometry codes of Goppa. Recently, the first author and Oggier generalised these constructions to other arithmetic groups: unit groups in number fields and orders in division algebras; they suggested to use unit groups in quaternion algebras but could not completely analyse the resulting codes. We prove that the noncommutative unit group construction yields asymptotically good families of codes for division algebras of any degree, and we estimate the size of the alphabet in terms of the degree.

1. Introduction

Number field codes, introduced by Lenstra [**9**] and independently rediscovered by Guruswami [**5**], are number field analogues of the geometric codes of Goppa [**4**] built from curves over finite fields. In these original constructions, the codes are constructed from the ring of integers of a number field.

In [**11**], the first author and Oggier extended these ideas: they explained how to construct codes from any arithmetic group, and they analysed the parameters of the resulting codes in the case of the unit group of the ring of integers of a number field, and in the case of an order in a division algebra. In every case, it is possible to obtain asymptotically good families of codes using towers of number fields with bounded root discriminant. The multiplicative group of an order in a quaternion algebra was also considered with a partial analysis and the question of constructing asymptotically good codes from these groups was left open, short of having adapted techniques, as explained in Remark 12 of [**11**].

We completely analyse the noncommutative unit group codes in any degree, by using a metric that is adapted to those groups. We also explain how to construct codes using columns $\mathbb{F}_p^d$ instead of matrices $\mathrm{M}_d(\mathbb{F}_p)$ as the alphabet. We analyse how the size of the alphabet varies with the degree of the algebra, and we prove the following theorem.

2000 ***Mathematics Subject Classification.*** — 11T71, 94B40, 11R52, 94B75.

Key words and phrases. — Number Field Codes, Division Algebras over Number Fields, Asymptotically Good Codes.

The authors would like to thank the Warwick Mathematics Department and the Department of Mathematics at Cornell University for providing a stimulating research atmosphere. Research of CM has been partially funded by the Region Bourgogne Franche-Comté. We also thank the EPSRC for financial support via the EPSRC Programme Grant EP/K034383/1 LMF: L-functions and modular forms.

Theorem. — *For all $d \geq 2$, there exists a family of asymptotically good number field codes, each obtained from the group of units of reduced norm* 1 *in a maximal order in a division algebra of degree d, over a fixed alphabet $\mathbb{F}_p^d$, where $\log p = c \log d + O(\log \log d)$ and $c > 0$ is a constant.*

We did not try to get the sharpest possible bounds, but the asymptotic of $\log p$ in terms of d is probably correct apart from the value of the constant c. Our analysis uses tools from the theory of arithmetic groups: the metric we use is closely related to the canonical metric on the associated symmetric space, and we use Macdonal's [**10**] and Prasad's [**16**] volume formulas. We also rely on a classical integration formula in KAK coordinates for the Haar measure of a semisimple Lie group (see for instance [**8**, Proposition 5.28]), but the analysis of the dependence on the degree required computing normalization factors that we could not find in the literature. Our method should generalize to arithmetic lattices in other semisimple groups.

One nice feature of the noncommutative case is that there are closed formulas for the covolume of the arithmetic group, contrary to the regulator of a number field. For fixed d, it is even possible to give closed formulas for the parameters of the code using our techniques, and we carry out these computations in the case $d = 2$. This is why we derive exact formulas whenever possible, and then deduce an asymptotic analysis of the interesting quantities.

For the sake of comparison, we revisit the additive case and carry out the analysis of the dependence on the degree. We obtain the following result.

Theorem. — *For all $d \geq 2$, there exists a family of asymptotically good number field codes, each obtained from the additive group of a maximal order in a division algebra of degree d, over a fixed alphabet $\mathbb{F}_p^d$, where $\log p = \frac{1}{2} \log d + O(\log \log d)$.*

The article is organized as follows. We first recall, in Section 2, the general construction of arithmetic group codes following Maire–Oggier, and we review the basic properties of central simple algebras over number fields in Section 3. In Section 4, we carry out the crucial volume computations that we need to estimate the parameters of the codes. We analyse the multiplicative construction in Section 5, where we prove our main theorem and give a detailed study of the quaternion case. Finally, we revisit the additive construction in Section 6.

2. The construction

We recall the principle of the construction as in [**11**]. Given

(i) a locally compact group G and a compact subset $\mathrm{B} \subset G$,
(ii) a lattice $\Gamma \subset G$, that is a discrete subgroup with a fundamental domain of finite Haar measure,
(iii) a map $\Theta\colon \Gamma \to \mathcal{A}^N$, where $\mathcal{A}$ is an alphabet (i.e. a finite set) and $N \geq 1$ is an integer,

we consider the code $\mathcal{C} = \Theta(\Gamma \cap c\mathrm{B})$, where $c \in G$ is such that $|\Gamma \cap c\mathrm{B}|$ is maximal. There may be more than one such c; we simply pick any one. Codewords of $\mathcal{C}$ are elements of $\mathcal{A}^N$. The main tool to estimate the rate of such codes is an idea of Lenstra, which we express in the following lemma.

Lemma 1. — *Let μ be a Haar measure on G. If $\Theta|_{\Gamma\cap c\mathrm{B}}$ is injective, then*

$$|\mathcal{C}| \geq \frac{\mu(\mathrm{B})}{\mu(G/\Gamma)}.$$

Proof. — This is [**11**, Lemma 1]. □

One natural way to construct such a code from an arithmetic group as follow. Given a number field F, a linear algebraic group $\mathbb{G}$ defined over F that has no nontrivial character and an arithmetic group $\Gamma \subset \mathbb{G}(\mathbb{Z}_F)$, we can consider $G = \mathbb{G}(F \otimes_{\mathbb{Q}} \mathbb{R})$ in which Γ is a lattice via the natural embedding $\Gamma \subset \mathbb{G}(F) \subset G$ (this theorem is due to Borel and Harish-Chandra [**1**]). Then define

$$\Theta \colon \Gamma \to \prod_{\mathfrak{p}\in S} \mathbb{G}(\mathbb{Z}_F/\mathfrak{p}) \to \mathcal{A}^N,$$

where S is a finite set of prime ideals of F and $\mathcal{A}$ is related to the groups $\mathbb{G}(\mathbb{Z}_F/\mathfrak{p})$. For instance, if for all $\mathfrak{p} \in S$ we have an embedding $\mathbb{G}(\mathbb{Z}_F/\mathfrak{p}) \hookrightarrow \mathrm{GL}_d(\mathbb{F}_{q_0})$, then we can take $\mathcal{A} = \mathbb{F}_{q_0}^d$. In this case the code length N is equal to $d \cdot |S|$, and the map Θ picks the columns of the corresponding matrices.

The parameters of interest of $\mathcal{C}$ are the *rate* $\dfrac{\log_q |\mathcal{C}|}{N}$, where $q = |\mathcal{A}|$ is the size of the alphabet, $\log_q(x) = \log x/\log q$, and the *minimum Hamming distance* $d_H(\mathcal{C})$ of $\mathcal{C}$, which is the minimum number of components in which any two distinct codewords differ. Asymptotically, families of codes $(\mathcal{C}_i)_i$ with length $N_i \to \infty$ that satisfy

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

are called *asymptotically good codes* (see for example [**18**] for a good explanation of the notion in the context of algebraic geometry codes).

We are going to consider two instances of this construction: one where $\mathbb{G}$ is the group of units of reduced norm one of a division algebra, and one where $\mathbb{G}$ is the additive group of a division algebra. The precise specification of the code in those cases is given in Section 5 for the multiplicative case and Section 6 for the additive case.

3. Central Simple Algebras: what we need

Our main references are [**15**] and [**17**], however the litterature is abundant. All our algebras will be finite-dimensional and associative.

3.1. Generalities.

— Let A be an algebra over a field F. The *center* of A is $\mathrm{Z}(A) = \{a \in A \mid \ xa = ax, \forall x \in A\}$. We say that A is *central* if $\mathrm{Z}(A) = F$, that A is a *division algebra* if $A^\times = A \setminus \{0\}$, and that A is *simple* if the only two-sided ideals of A are $\{0\}$ and A. Every division algebra is simple. The dimension of a central simple algebra over F is a square d^2, and d is called the *degree* of A over F.

Let A be a central simple algebra of degre d over a field F. There exists a finite extension L/F and an isomorphim $A \otimes_F L \cong \mathrm{M}_d(L)$ of algebras over L, where as usual $\mathrm{M}_d(R)$ denotes the matrix algebra with coefficients in R. Let φ be such an isomorphism. For all $x \in A$, the determinant $\det \varphi(x)$ (resp. the trace $\operatorname{tr} \varphi(x)$) is in F and is independent of L and φ; it is called the *reduced norm* $\operatorname{nrd}(x)$ (resp. *reduced trace* $\operatorname{trd}(x)$) of x. The map $\operatorname{trd}\colon A \to F$ is F-linear, the map $\operatorname{nrd}\colon A \to F$ is multiplicative, and $A^\times = \{x \in A \mid \operatorname{nrd}(x) \neq 0\}$.

Example 2. — *Let $\mathbb{H}$ be the algebra of Hamiltonian quaternions:*

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k \text{ with } i^2 = j^2 = k^2 = ijk = -1.$$

Then $\mathbb{H}$ is a central division algebra over $\mathbb{R}$. For all $x, y, z, t \in \mathbb{R}$ we have $\operatorname{nrd}(x + yi + zj + tk) = x^2 + y^2 + z^2 + t^2$ and $\operatorname{trd}(x + yi + zj + tk) = 2x$.

3.2. Over number fields. — Let F be a number field of degree n over $\mathbb{Q}$. Denote by $\mathbb{Z}_F$ the ring of integers of F, and by $\mathbb{P}_\infty$ the set of infinite places of F. Let A be a central simple algebra of degree d over F.

3.2.1. — Let $x \in A$. Then the *absolute norm* $\mathrm{N}(x) \in \mathbb{Q}$ of x is the absolute value of the determinant of the matrix of left multiplication by x on A, seen as a matrix in $\mathrm{M}_{d^2 n}(\mathbb{Q})$. We have $\mathrm{N}(x) = |N_{F/\mathbb{Q}}(\operatorname{nrd}(x))^d|$, where $N_{F/\mathbb{Q}}$ denotes the norm in $F/\mathbb{Q}$. Let us remark that when A is a division algebra, $\mathrm{N}(x) = 0$ if and only if $x = 0$.

3.2.2. — An *order* in A is a subring $\mathcal{O} \subset A$ that is finitely generated as a $\mathbb{Z}$-module and such that $\mathcal{O}F = A$. If $\mathcal{O}$ is an order and $x \in \mathcal{O}$ is such that $\mathrm{N}(x) \neq 0$, then $\mathrm{N}(x) = |\mathcal{O}/x\mathcal{O}|$.

Let $\mathcal{O}$ be a maximal order (i.e. not properly contained in a larger order), and let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_F$; put $q = |\mathbb{Z}_F/\mathfrak{p}|$. We say that

- $\mathfrak{p}$ is *unramified* in A if $\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathrm{M}_d(\mathbb{F}_q)$;
- $\mathfrak{p}$ is *ramified* in A otherwise.

The number of primes that ramify in A is finite. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_F$, and denote by $F_\mathfrak{p}$ the completion of F at $\mathfrak{p}$. Then there exists an isomorphism

$$A \otimes_F F_\mathfrak{p} \cong \mathrm{M}_{d_\mathfrak{p}}(D_\mathfrak{p}),$$

where $D_\mathfrak{p}$ is a central division algebra over $F_\mathfrak{p}$; let us write $[D_\mathfrak{p} : F_\mathfrak{p}] = e_\mathfrak{p}^2$. We then have $e_\mathfrak{p} d_\mathfrak{p} = d$, the prime $\mathfrak{p}$ is ramified if and only if $e_\mathfrak{p} > 1$, and more generally we have $\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathrm{M}_{d_\mathfrak{p}}(\mathbb{F}_{q^{e_\mathfrak{p}}})$.

Let $\sigma \in \mathbb{P}_\infty$ be an infinite place of F. If σ is complex, then there is an isomorphism

$$A \otimes_F F_\sigma \cong \mathrm{M}_d(\mathbb{C}),$$

and in this case, we say that σ is *unramified*. If σ is real, then there is an isomorphism

- $A \otimes_F F_\sigma \cong \mathrm{M}_d(\mathbb{R})$, in which case we say that σ is *unramified* in A, or
- $A \otimes_F F_\sigma \cong \mathrm{M}_{d/2}(\mathbb{H})$, in which case we say that σ is *ramified* in A.

In all cases, we fix an isomorphism extending σ as above, and still call it $\sigma\colon A \otimes_F F_\sigma \cong \mathrm{M}_{d_\sigma}(D_\sigma)$, where D_σ is a central division algebra of degree e_σ over F_σ, and we write $n_\sigma = [F_\sigma : \mathbb{R}]$.

3.2.3. — We denote by Δ_F the absolute value of the discriminant of F and by rd_F its *root discriminant* $\Delta_F^{1/n}$. Recall that if K/F is an unramified extension of number fields then $\mathrm{rd}_K = \mathrm{rd}_F$. The *reduced discriminant* δ_A of A is defined as

$$\delta_A = \prod_\mathfrak{p} \mathfrak{p}^{d(1-1/e_\mathfrak{p})}$$

where the product is over all prime ideals of $\mathbb{Z}_F$. The *absolute discriminant* Δ_A of A is defined as

$$\Delta_A = \Delta_F^{d^2} \mathrm{N}(\delta_A)^d.$$

Here as usual, if $I \subset \mathbb{Z}_F$ is an ideal of $\mathbb{Z}_F$, we denote by $\mathrm{N}(I) = |\mathbb{Z}_F/I|$ its absolute norm.

4. Volumes

4.1. Cartan decomposition. — Let D be a division algebra over $\mathbb{R}$, so that D is isomorphic to one of $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. We write $F = \mathrm{Z}(D)$ the center of D, e the degree of D over F, and $n = [F\colon \mathbb{R}]$. Hence: $e = n = 1$ if $R = \mathbb{R}$; $e = 1$, $n = 2$ if $R = \mathbb{C}$; and $e = 2$, $n = 1$ if $R = \mathbb{H}$. We will later apply the results of this section to the completion $\mathrm{M}_d(D)$ of a central simple algebra over a number field at a real or complex place σ, and the notations for those degrees will become e_σ, n_σ and d_σ. There exists a unique $\mathbb{R}$-linear and anti-multiplicative involution $x \mapsto \bar{x}$ on D such that for all $x \in D^\times$ we have $x\bar{x} \in \mathbb{R}_{>0} \subset D$: it is called the *canonical involution* of D. Explicitly, the canonical involution is the identity on $\mathbb{R}$, the complex conjugation on $\mathbb{C}$, and the quaternionic conjugation on $\mathbb{H}$. In this section, we fix $d \geq 1$.

Consider the semisimple Lie group:

$$G = \mathrm{SL}_d(D) = \{g \in \mathrm{M}_d(D) \mid \mathrm{nrd}(g) = 1\}.$$

Consider the following maximal compact subgroup of G:

$$K = \mathrm{SU}_d(D) = \{g \in G \mid g^t\bar{g} = \mathrm{Id}\},$$

and define

$$A = \left\{ \begin{pmatrix} \exp(a_1) & & 0 \\ & \ddots & \\ 0 & & \exp(a_d) \end{pmatrix} : a_1, \ldots, a_d \in \mathbb{R} \right\} \cap G.$$

Example 3. — *If $D = \mathbb{H}$ and $d = 2$, then*

$$\mathrm{SL}_d(D) = \mathrm{SL}_2(\mathbb{H}) = \{g \in \mathrm{M}_2(\mathbb{H}) \mid \mathrm{nrd}(g) = 1\},$$

where for $a, b, c, d \in \mathbb{H}$ we have

$$\mathrm{nrd} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} \mathrm{nrd}(ad) & \text{if } c = 0 \\ \mathrm{nrd}(ac^{-1}dc - bc) & \text{if } c \neq 0. \end{cases}$$

Note that the set $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{H}) \mid ad - bc = 1 \right\}$ *is not stable under multiplication. In this case we have*

$$K = \mathrm{SU}_d(D) = \mathrm{SU}_2(\mathbb{H}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{H}) \mid a\bar{a} + b\bar{b} = c\bar{c} + d\bar{d} = 1,\ a\bar{c} + b\bar{d} = 0 \right\}.$$

Let $\mathrm{Z}_K(A) = \{a \in A \mid \ ak = ka, \forall k \in K\}$ be the centralizer of A in K. Explicitly, we have

- if $D = \mathbb{R}$, then $\mathrm{Z}_K(A) \cong \{\pm 1\}^{d-1}$ is the group of diagonal matrices with coefficients ± 1 on the diagonal and determinant 1;
- if $D = \mathbb{C}$, then $\mathrm{Z}_K(A) \cong \mathrm{U}(1)^{d-1}$ is the group of diagonal matrices with coefficients in $\mathbb{C}$ of absolute value 1 on the diagonal and determinant 1;

- if $D = \mathbb{H}$, then $\mathrm{Z}_K(A) \cong \mathrm{SL}_1(\mathbb{H})^d \cong \mathrm{SU}_2(\mathbb{C})^d$ is the group of diagonal matrices with coefficients in $\mathbb{H}$ of reduced norm 1 on the diagonal.

Let us recall the Cartan decomposition of G that will be of great interest for the computation of the different volumes (see for example [**8**, Chapter V, §4]):

***Theorem 4* (Cartan decomposition).** — *Let $G = \mathrm{SL}_d(D)$, K and A be as above. Then we have $G = KAK$. In the decomposition $g = k_1 a k_2$ of an element $g \in G$ with $k_i \in K$ and $a = \mathrm{diag}(\exp(a_1), \dots, \exp(a_d)) \in A$, the a_i are unique up to permutation. Moreover, let $S \subset G$ be the subset of elements $g \in G$ such that the a_i are distinct. Then for all g in S, the pair (k_1, k_2) is uniquely determined up to changing (k_1, k_2) into $(k_1 z^{-1}, z k_2)$ with $z \in \mathrm{Z}_K(A)$.*

Remark 5. — *When $D = \mathbb{R}$ or $\mathbb{C}$, this is also known as the singular value decomposition. Note that $G \setminus S$ has zero measure, so that we can and will restrict to S when computing integrals.*

Define the function $\rho\colon G \to \mathbb{R}_{\geq 0}$ such that for all $g \in G$ with Cartan decomposition $g = k_1 a k_2$, where $a = \mathrm{diag}(\exp(a_1), \dots, \exp(a_d))$, we have

$$\rho(g) = \max_i |a_i|.$$

This is well-defined since the a_i are unique up to permutation. Note that we have $\rho(g^{-1}) = \rho(g)$ for all $g \in G$.

Let us give a series of corollaries of Theorem 4 that will be useful to estimate the minimal Hamming distance of the multiplicative codes.

Let $\|\cdot\|_2\colon D^d \to \mathbb{R}$ be the norm on D^d defined by $\|x\|_2 = \left(\sum_{i=1}^d x_i \bar{x}_i\right)^{1/2}$ for all $x \in D^d$, and let $|||\cdot|||\colon \mathrm{M}_d(D) \to \mathbb{R}_{\geq 0}$ be the corresponding operator norm, that is:

$$|||g||| = \sup_{x \neq 0} \frac{\|g \cdot x\|_2}{\|x\|_2} \text{ for all } g \in \mathrm{M}_d(D).$$

Corollary 6. — *For all $g \in G$, we have*

$$\rho(g) = \log \max(|||g|||, |||g^{-1}|||).$$

Proof. — As $\|\cdot\|_2$ is bi-invariant by K, in Cartan decomposition (Theorem 4) we have $|||g||| = \max_i \exp(a_i)$. Applying this to g and g^{-1} gives the result. □

Corollary 7. — *For all $g, h \in G$, we have $\rho(gh) \leq \rho(g) + \rho(h)$.*

Proof. — This follows from Corollary 6 and the submultiplicativity of operator norms. □

Corollary 8. — *For all $g \in G$, we have*

$$|\mathrm{nrd}(g-1)| \leq 2^d \exp(d\rho(g)).$$

Proof. — Let $x = g - 1$. We claim that we have $|\mathrm{nrd}(x)| \leq |||x|||^d$. To see this, let $V = D^d$ viewed as an $\mathbb{R}$-vector space of dimension $de^2 n$. The absolute value of the determinant of x viewed as an endomorphism of V is $|\mathrm{nrd}(x)|^{ne^2}$. So multiplication by x scales volumes by $|\mathrm{nrd}(x)|^{ne^2}$; applying this to a ball for the norm $\|\cdot\|_2$, noting that the volume of the

ball of radius R is proportionnal to R^{de^2n} and using the definition of the operator norm proves the claim.
On the other hand we have

$$|||x||| \leq |||g||| + 1 \leq 2\max(1, |||g|||) \leq 2\exp(\rho(g)),$$

where the last inequality follows from Corollary 6. $\square$

4.2. Haar measure on $\mathrm{SL}_d(D)$. — If $M, N \in \mathrm{M}_d(D)$, we write $[M, N]$ for the Lie bracket $MN - NM$, and if $g \in \mathrm{GL}_d(D)$, we write $\mathrm{Ad}(g)M = gMg^{-1}$. The Lie algebra of $\mathrm{SL}_d(D)$ is $\mathfrak{sl}_d(D) = \{X \in \mathrm{M}_d(D) \mid \mathrm{trd}(X) = 0\}$. We equip the $\mathbb{R}$-vector space $\mathfrak{sl}_d(D)$ with the positive definite inner product $(X, Y) \mapsto \mathrm{tr}_{R/\mathbb{R}}\,\mathrm{trd}({}^t\overline{X}Y)$, with corresponding norm $\|X\|^2 = n\,\mathrm{trd}({}^t\overline{X}X)$. This gives $G = \mathrm{SL}_d(D)$ the structure of a Riemannian manifold with a metric on G that is invariant under left translations by arbitrary elements of G and under right translation by elements of K. In particular, this defines a volume form $d\mu$ on G, on K and on $\mathrm{Z}_K(A)$.
Let us start with the computation of the volume of $\mathrm{Z}_K(A)$ with respect to $d\mu$.

Lemma 9. — *Let $G = \mathrm{SL}_d(D)$ and K, A as above. Then $\mu(\mathrm{Z}_K(A))$ equals*
- 2^{d-1} *when $D = \mathbb{R}$,*
- $(2\sqrt{2}\pi)^{d-1}\sqrt{d}$ *when $D = \mathbb{C}$,*
- $(4\sqrt{2}\pi^2)^d$ *when $D = \mathbb{H}$.*

Proof. —
- If $D = \mathbb{R}$, the group $\mathrm{Z}_K(A) \cong \{\pm 1\}^{d-1}$ is finite and the corresponding measure is the counting measure.
- If $D = \mathbb{C}$, the group $\mathrm{Z}_K(A)$ is a product of circles $U(1)^{d-1}$, which we parametrize as the image of $[0, 2\pi]^{d-1}$ under the map

$$(\theta_1, \ldots, \theta_{d-1}) \mapsto \mathrm{diag}\left(\exp(i\theta_1), \ldots, \exp(i\theta_{d-1}), \exp\left(-i\sum_{k=1}^{d-1}\theta_k\right)\right).$$

The Gram matrix of the corresponding tangent vectors is the $(d-1)\times(d-1)$ matrix

$$\begin{pmatrix} 4 & 2 & \ldots & 2 \\ 2 & 4 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 2 \\ 2 & \ldots & 2 & 4 \end{pmatrix},$$

which has determinant $2^{d-1}d$. So the corresponding volume is $(2\pi)^{d-1}\sqrt{2^{d-1}d}$.
- If $D = \mathbb{H}$, the group $\mathrm{Z}_K(A)$, as a Riemannian manifold, is a direct product of d copies of $\mathrm{SU}(2)$, which is a 3-dimensional sphere of radius $\sqrt{2}$ with our normalization. It is well-known that the volume of a 3-dimensional sphere of radius R is $2\pi^2R^3$, giving the formula.

$\square$

For the general situation, we have:

Proposition 10. — *Let $G = \mathrm{SL}_d(D)$ and K, A as above, and let $f \in L^1(G)$. Then the integral $\int_G f\, d\mu$ equals*

$$\frac{(ne)^{\frac{d-1}{2}}\sqrt{d}}{\mu(\mathrm{Z}_K(A))}\int_{K\times K}\int_{a_i}\prod_{1\leq i<j\leq d}\sinh(a_i-a_j)^{ne^2}f(k_1ak_2)da_idk_1dk_2,$$

where:

- $a = \mathrm{diag}(\exp(a_1), \ldots, \exp(a_d))$, *and*
- *the integral is over the set*

$$\left\{(a_1, \ldots, a_{d-1}) \in \mathbb{R}^{d-1} \mid a_1 > a_2 > \cdots > a_{d-1} > -\sum_{i=1}^{d-1} a_i\right\}$$

and $a_d = -\sum_{i=1}^{d-1} a_i$.

Proof. — We will obtain the formula by pulling back the metric along the map

$$\Psi\colon K \times A \times K \to G,$$

and computing the pullback by using the decomposition of $\mathfrak{sl}_d(D)$ according to restricted roots of A, as in [**7**], keeping track of all constants.
First we compute the differential of Ψ. Let $x = (k_1, a, k_2) \in K \times A \times K$, where $a = \mathrm{diag}(\exp(a_i))$. Using the canonical isomorphism between the tangent space of a Lie group at an arbitrary point and its Lie algebra, we obtain that the differential of Ψ at (k_1, a, k_2) is the map $d\Psi_x\colon \mathfrak{k} \times \mathfrak{a} \times \mathfrak{k} \to \mathfrak{g}$ that sends

$$(X_1, Y, X_2) \mapsto \mathrm{Ad}(k_2^{-1})\,\mathrm{Ad}(a^{-1})X_1 + Y + X_2.$$

To compute the pull-back of the volume form to $K \times A \times K$, it is enough to compute $\Delta_x = \det\left(d\Psi_x{}^t(d\Psi_x)\right)^{1/2}$. We compute this determinant by blocks. The term in $\mathfrak{a}$ does not contribute. We compute the other terms by decomposing $\mathrm{M}_d(D)$ in 2×2 blocks corresponding to rows and columns i and j. Consider the matrices

$$F_+ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } F_- = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{M}_2(D).$$

We have $\mathrm{Ad}(a)F_+ = \cosh(a_i - a_j)F_+ + \sinh(a_i - a_j)F_-$ and $\mathrm{Ad}(a)F_- = \cosh(a_i - a_j)F_- + \sinh(a_i - a_j)F_+$. In addition, let $D^0 = \{z \in D \mid \bar{z} + z = 0\}$. Then $\mathfrak{k}$ is the sum over all the blocks of $F_-\mathbb{R} \oplus F_+D^0$, and of $Z_{\mathfrak{k}}(\mathfrak{a})$, and those are orthogonal to $F_+\mathbb{R}$ and F_-D^0. Using this, we see that the matrix of $d\Psi_x$ is a direct sum of blocks of the form

$$\begin{pmatrix} \sinh(a_i - a_j) & 0 \\ \cosh(a_i - a_j) & 1 \end{pmatrix}$$

each appearing with multiplicity $\dim_{\mathbb{R}} D = ne^2$, and of blocks $(1\ 1)$ appearing with multiplicity $(e^2 - 1)d$. We therefore have

$$\Delta_x = 2^{\frac{(e^2-1)d}{2}} \prod_{1\leq i<j\leq d} \sinh(a_i - a_j)^{ne^2}.$$

The map Ψ is not injective, and by Theorem 4, outside of a set of zero measure, the fiber of k_1ak_2 is $\{(k_1z, a, z^{-1}k_2) : z \in Z_K(A)\}$. With the same computation we obtain that the volume of this fiber is $2^{\frac{(e^2-1)d}{2}}\mu(Z_K(A))$. This gives

$$\int_G f\ d\mu = \frac{1}{\mu(\mathrm{Z}_K(A))}\int_{K\times K}\int_{a\in A^+}\prod_{1\leq i<j\leq d}\sinh(a_i-a_j)^{ne^2} f\left(k_1 a k_2\right) dadk_1dk_2,$$

where $A^+\subset A$ is the subset of diagonal matrices with decreasing entries. We parametrise

$$A^+ = \left\{\mathrm{diag}(\exp(a_i)) : (a_1,\dots,a_{d-1})\in\mathbb{R}^{d-1} \mid a_1>a_2>\dots>a_d \text{ and } a_d = -\sum_{i=1}^{d-1} a_i\right\},$$

and the factor corresponding to this second change of variables is the square root of the determinant of the Gram matrix of the tangent vectors $\mathrm{diag}(0,\dots,1,0,\dots,0,-1)\in\mathfrak{g}$. This Gram matrix is the $(d-1)\times(d-1)$ matrix

$$ne\begin{pmatrix} 2 & 1 & \dots & 1\\ 1 & 2 & \ddots & \vdots\\ \vdots & \ddots & \ddots & 1\\ 1 & \dots & 1 & 2\end{pmatrix},$$

and it has determinant $(ne)^{d-1}d$. □

Proposition 11. — *Let K be as above. Then we have*

$$\mu(K) = \kappa\prod_{k=1}^{r}\frac{\pi^{m_k+1}}{m_k!},$$

where

(i) if $D=\mathbb{R}$:

- *if d is even, then $r=d/2$, $\kappa = 2^{d^2/2-d/4}$ and*
$$m_k = 2k-1 \text{ for } k\leq r-1 \text{ and } m_r = r-1;$$
- *if d is odd, then $r=(d-1)/2$, $\kappa = 2^{d^2/2+d/4-3/4}$ and*
$$m_k = 2k-1 \text{ for all } k\leq r;$$

(ii) if $D=\mathbb{C}$, then $r=d-1$, $\kappa = 2^{d^2+d/2-3/2}\sqrt{d}$ and
$$m_k = k \text{ for all } k\leq r;$$

(iii) if $D=\mathbb{H}$, then $r=d$, $\kappa = 2^{2d^2+d/2}$ and
$$m_k = 2k-1 \text{ for all } k\leq r.$$

Proof. — We apply Macdonald's formula [**10**]. Recall (see [**3**, Part II, §19]) that the roots of $\mathfrak{k}$ with respect to $\mathfrak{t}$ are the nonzero morphisms $\alpha\in\mathrm{Hom}_{\mathbb{R}}(\mathfrak{t},\mathbb{C})$ such that there exists a nonzero $X_\alpha\in\mathfrak{k}\otimes\mathbb{C}$ such that $[t,X_\alpha]=\alpha(t)X_\alpha$ for all $t\in\mathfrak{t}$; for each root α, the attached coroot $\alpha^\vee\in\mathfrak{t}\otimes\mathbb{C}$ is the unique element $\alpha^\vee\in\mathbb{C}\cdot[X_\alpha,X_{-\alpha}]$ such that $[\alpha^\vee,X_\alpha]=2X_\alpha$ and $[\alpha^\vee,X_{-\alpha}]=-2X_{-\alpha}$. In each case, we give the Lie algebra $\mathfrak{k}$ of K, and in Macdonald's notations, $\mathfrak{t}\subset\mathfrak{k}$, $\mathfrak{t}_{\mathbb{Z}}\subset\mathfrak{t}$, and the list of roots α, their corresponding root vectors X_α and coroots $\alpha^\vee\in\mathfrak{k}\otimes\mathbb{C}$. The list of m_k is standard (see [**16**, §1.5] or [**2**, Chap. VIII, §13 (VI)]).

(i) When $D = \mathbb{R}$, $K = \mathrm{SO}_d(\mathbb{R})$ and $\mathfrak{k} = \mathfrak{so}_d(\mathbb{R})$ is the Lie algebra of antisymmetric matrices (which all have trace 0), and we have $\mathfrak{k}_\mathbb{C} \cong \mathfrak{so}_d(\mathbb{C})$. We choose $\mathfrak{t} \subset \mathfrak{k}$ to be the space of matrices that are block-diagonal with 2×2 blocks of the form $\begin{pmatrix} 0 & \theta_k \\ -\theta_k & 0 \end{pmatrix}$ for $k = 1, \dots, r$. Then $\mathfrak{t}_\mathbb{Z} \subset \mathfrak{t}$ is the lattice of elements with $\theta_k \in \mathbb{Z}$ for all k. We will also write θ_k the corresponding linear form on $\mathfrak{t}$. For $k < \ell \leq r$ and $M \in \mathrm{M}_2(\mathbb{R})$, let $R_{k,\ell}(M)$ be the block matrix $\begin{pmatrix} 0 & M \\ -{}^tM & 0 \end{pmatrix}$ embedded in the $(2k-1, 2k, 2\ell-1, 2\ell)$-th block of a $d \times d$ matrix. For $k \leq r$ and $v \in \mathbb{R}^2$ a column vector, let $R_k(v)$ be the block matrix $\begin{pmatrix} 0 & v \\ -{}^tv & 0 \end{pmatrix}$, embedded in the $(2k-1, 2k, d)$-th block of a $d \times d$ matrix. For $k \leq r$, let $F_k \in \mathfrak{t}$ be the matrix with $\theta_k = 1$ and all other coefficients 0. Then the roots of $\mathfrak{k}$ with respect to $\mathfrak{t}$ are:

(a) For $1 \leq k < \ell \leq r$, the $\alpha = \pm(\theta_k - \theta_\ell)i$, with corresponding

$$X_\alpha = R_{k,\ell}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pm R_{k,\ell}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes i \in \mathfrak{k} \otimes \mathbb{C}$$

and coroots $\alpha^\vee = \pm(F_k - F_\ell) \otimes i \in \mathfrak{t} \otimes \mathbb{C}$.

(b) For $1 \leq k < \ell \leq r$, the $\alpha = \pm(\theta_k + \theta_\ell)i$, with corresponding

$$X_\alpha = R_{k,\ell}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \pm R_{k,\ell}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes i$$

and coroots $\alpha^\vee = \pm(F_k + F_\ell) \otimes i$.

(c) If d is odd, for $1 \leq k \leq r$, the $\alpha = \pm\theta_k i$, with corresponding

$$X_\alpha = R_k\begin{pmatrix} 1 \\ 0 \end{pmatrix} \pm R_k\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes i$$

and coroots $\alpha^\vee = \pm 2F_k \otimes i$.

(ii) When $D = \mathbb{C}$, $K = \mathrm{SU}_d(\mathbb{C})$ and $\mathfrak{k} = \mathfrak{su}_d(\mathbb{C})$ is the Lie algebra of anti-Hermitian matrices with trace 0, and we have $\mathfrak{k} \otimes \mathbb{C} \cong \mathfrak{sl}_d(\mathbb{C})$. We choose $\mathfrak{t} \subset \mathfrak{k}$ to be the space of diagonal matrices with coefficients $i\theta_k$ where $\theta_k \in \mathbb{R}$ and $\sum_{k=1}^d \theta_k = 0$. Then $\mathfrak{t}_\mathbb{Z} \subset \mathfrak{t}$ is the lattice of elements with $\theta_k \in \mathbb{Z}$ for all k. We will again write θ_k the corresponding linear form on $\mathfrak{t}$. For $k < \ell \leq r$ and $z \in \mathbb{C}$, let $R_{k,\ell}(z)$ be the matrix $\begin{pmatrix} 0 & z \\ -\bar{z} & 0 \end{pmatrix}$, embedded in the (k, ℓ)-th block of a $d \times d$ matrix. For $k \leq d$, let F_k be the matrix with $\theta_k = 1$ and all other coefficients 0. Then the roots of $\mathfrak{k}$ are, for $1 \leq k < \ell \leq d$, the $\alpha = \pm(\theta_k - \theta_\ell)i$, with corresponding

$$X_\alpha = R_{k,\ell}(1) \pm R_{k,\ell}(i) \otimes i$$

and coroots $\alpha^\vee = \pm(F_k - F_\ell) \otimes i$.

(iii) When $D = \mathbb{H}$, $K = \mathrm{SU}_d(\mathbb{H})$ and $\mathfrak{k} = \mathfrak{su}_d(\mathbb{H})$ is the Lie algebra of quaternion-anti-Hermitian matrices (which automatically have reduced trace 0), and we have $\mathfrak{k} \otimes \mathbb{C} \cong \mathfrak{sp}_{2d}(\mathbb{C})$. We choose $\mathfrak{t} \subset \mathfrak{k}$ to be the space of diagonal matrices with coefficients $i\theta_k$ where $\theta_k \in \mathbb{R}$. Then $\mathfrak{t}_\mathbb{Z} \subset \mathfrak{t}$ is the lattice of elements with $\theta_k \in \mathbb{Z}$ for all k. We will again write θ_k the corresponding linear form on $\mathfrak{t}$. For $k < \ell \leq r$ and $w \in \mathbb{H}$, let $R_{k,\ell}(w)$ be the matrix $\begin{pmatrix} 0 & w \\ -\bar{w} & 0 \end{pmatrix}$, embedded in the (k,ℓ)-th block of a $d\times d$ matrix. For $k\le r$, let F_k be the matrix with $\theta_k=1$ and all other coefficients 0. Then the roots of $\mathfrak{k}$ are

(a) For $1\le k<\ell\le d$, the $\alpha=\pm(\theta_k-\theta_\ell)i$, with corresponding
$$X_\alpha = R_{k,\ell}(1)\pm R_{k,\ell}(i)\otimes i$$
and coroots $\alpha^\vee=\pm(F_k-F_\ell)\otimes i$.

(b) For $1\le k<\ell\le d$, the $\alpha=\pm(\theta_k+\theta_\ell)i$, with corresponding
$$X_\alpha = R_{k,\ell}(j)\pm R_{k,\ell}(ij)\otimes i$$
and coroots $\alpha^\vee=\pm(F_k+F_\ell)\otimes i$.

(c) For $1\le k\le d$, the $\alpha=\pm 2\theta_k i$, with corresponding
$$X_\alpha = jF_k \pm ijF_k\otimes i$$
and coroots $\alpha^\vee=\pm F_k\otimes i$.

Computing $\mu(\mathfrak{t}/\mathfrak{t}_{\mathbb{Z}})$ and the norms of the coroots in each case gives the result from Macdonald's formula: in his notation we have
$$\lambda=\mu(\mathfrak{t}/\mathfrak{t}_{\mathbb{Z}})\prod_\alpha \|\alpha^\vee\|,$$
and we finally let $\kappa=2^r\lambda$. □

Corollary 12. — *Let K be as above. We have*
$$\log\mu(K)=-\frac{n}{4}(ed)^2\log d+O(d^2).$$

Proof. — Use Proposition 11 and $\sum_{k=1}^r k\log k=\frac{r^2}{2}\log r+O(r^2)$. □

4.3. Volume of a ball. — In order to find a lower bound for the volume of certain balls $\mathrm{B}(t)$, we will need to compute a lower bound for an integral of the form
$$\int\prod_{i<j}\sinh(a_i-a_j)^m da_i,$$
where the integral is over the $(a_i)_i$ with $|a_i|\le t$ and $\sum_i a_i=0$. The domain for the a_i is the intersection of a hypercube with the hyperplane $\sum a_i=0$, i.e. a simplex. On the other hand, the integrand is small when some $|a_i-a_j|$ is small, that is when (a_i) is close to one of the hyperplanes $a_i=a_j$. To find a lower bound, we will restrict to a subset of the simplex that is far from those hyperplanes, and where the a_i vary independently, so we can compute the integral. Moreover, the integrand increases exponentially, so the size of the subset does not contribute significantly to the value of the integral, while the values of the integrand do; so we need a subset where many of the a_i are close to t. This is achieved using the following technical lemma.

Lemma 13. — *Let $k\ge 1$ be an integer. Then there exists k intervals $[\alpha_i,\beta_i]$ such that for all $a_i\in[\alpha_i,\beta_i]$ we have:*
(1) $|a_i|\le 1$;
(2) $|\sum_{j=1}^k a_j|\le 1$;
(3) $\beta_i-\alpha_i\ge\frac{1}{4(k+1)^2}$;
(4) $|a_i-a_j|\ge\frac{1}{4(k+1)^2}$;
(5) $|a_i+\sum_{j=1}^k a_j|\ge\frac{1}{4(k+1)^2}$;

(6) $|\{j\colon a_j \geq \frac{1}{4}\}| \geq \frac{k+1}{5}$.

Proof. — Let $c_1, \dots, c_k$ be defined by $c_i = \frac{2i}{k+1} - 1$, except when k is odd, where $c_{\frac{k+1}{2}} = \frac{1}{k+1}$. Let $\alpha_i = c_i - \frac{1}{8(k+1)^2}$ and $\beta_i = c_i + \frac{1}{8(k+1)^2}$. We claim that they satisfy the required properties.

(1) In absolute value, the extremal points of the intervals are $\frac{k-1}{k+1} + \frac{1}{8(k+1)^2} \leq 1$.
(2) The sum $\sum_{j=1}^k c_j$ is 0 if k is even, and $\frac{1}{k+1}$ if k is odd. The required inequalities become $|\frac{k}{8(k+1)^2}| \leq 1$ and $|\frac{1}{k+1} + \frac{k}{8(k+1)^2}| \leq 1$, which are true.
(3) By definition we have $\beta_i - \alpha_i = \frac{1}{4(k+1)^2}$.
(4) The minimum separation between the centers c_i is $\frac{1}{k+1}$, and we have $\frac{1}{k+1} - \frac{1}{4(k+1)^2} \geq \frac{1}{4(k+1)^2}$.
(5) The minimum separation between a c_i and $-\sum_{j=1}^k c_j$ is at least $\frac{1}{k+1}$, and we have $\frac{1}{k+1} - \frac{1}{8(k+1)^2} - \frac{k}{8(k+1)^2} \geq \frac{1}{4(k+1)^2}$.
(6) If $k \leq 4$ it is obvious, and when $k \geq 5$ we have $\alpha_i \geq \frac{1}{4}$ if and only if $i \geq \frac{k+1}{8}(5 + \frac{1}{2(k+1)^2})$, and the number of such i is at least $\frac{k+1}{5}$.

□

We can now give a lower bound for the volume of a certain ball $\mathrm{B}(t) \subset G$ with the above Haar measure $d\mu$.

Proposition 14. — *Let $t \geq 1$, and let $\mathrm{B}(t) = \{g \in G \mid \rho(g) \leq t\}$. Assume $d \geq 2$. Then*

$$\log \mu(\mathrm{B}(t)) \geq -\frac{3n(de)^2}{2} \log d + \frac{n(de)^2}{200} t + O(d^2)\cdot$$

Proof. — We apply Proposition 10 with f the indicator function of $\mathrm{B}(t)$. The formula reads

$$\mu(\mathrm{B}(t)) = \frac{(ne)^{\frac{d-1}{2}}\sqrt{d}}{\mu(\mathrm{Z}_K(A))} \mu(K)^2 I, \text{ where } I = \int_{a_i} \prod_{i<j} \sinh(a_i - a_j)^{ne^2} da_i,$$

where the integral is over the $a_i \in [-t, t]$ with $(a_i)_i$ decreasing and $\sum_i a_i = 0$. To compute a lower bound for the integral, we apply Lemma 13 to $k = d-1$. We have intervals $[\alpha_i, \beta_i]$, and after reordering the intervals and scaling them by t, we obtain that

$$I \geq \int \prod_{i<j} \sinh(a_i - a_j)^{ne^2} da_i,$$

where for $i \leq d$, a_i ranges over one of the intervals, and $a_d = -\sum_{i=1}^{d-1} a_i$. Since $x \mapsto \sinh(x)\exp(-x) = \frac{1-\exp(-2x)}{2}$ is increasing, for all $x \geq \dfrac{t}{4d^2}$ we have

$$\sinh(x) \geq \frac{1 - \exp(-t/2d^2)}{2} \exp(x) \geq \frac{1 - \exp(-1/2d^2)}{2} \exp(x) \geq \frac{1}{4d^2} \exp(x)\cdot$$

We get

$$I \geq \left(\frac{1}{4d^2}\right)^{ne^2 d(d-1)/2} \int \prod_{i<j} \exp(a_i - a_j)^{ne^2} da_i.$$

We compute the term β that appears in the exponential. For all (a_i) such that $\sum_{i=1}^{d} a_i = 0$, we have

$$\begin{aligned}
\beta &= \sum_{1\leq i<j\leq d} (a_i - a_j) = \sum_{i<j} a_i - \sum_{i<j} a_j \\
&= \sum_i (d-i)a_i - \sum_j (j-1)a_j = \sum_{i=1}^{d} (d+1-2i)a_i \\
&= -2\sum_{i=1}^{d} i a_i\cdot
\end{aligned}$$

Now since $a_d = -\sum_{i=1}^{d-1} a_i$, we have $\beta = 2\sum_{i=1}^{d-1}(d-i)a_i$. This gives

$$I \geq (2d)^{-d(d-1)ne^2} \int \exp\Big(2ne^2 \sum_{i=1}^{d-1}(d-i)a_i\Big) da_i\cdot$$

By properties (3) and (6) of Lemma 13, we obtain

$$I \geq (2d)^{-d(d-1)ne^2} \exp\left(2ne^2 \sum_{i=1}^{\lfloor d/5\rfloor} i\frac{t}{4}\right)\left(\frac{1}{4d^2}\right)^{(d-1)ne^2} \geq (2d)^{-(d-1)(d+2)ne^2} \exp\left(\frac{d^2ne^2}{200}t\right)\cdot$$

In particular,

$$\log I \geq -n(de)^2 \log d + \frac{n(de)^2}{200}t + O(d^2)\cdot$$

We conclude by using Corollary 12 and Lemma 9.

□

5. Multiplicative construction

We consider the following arithmetic group code. Let F be a number field of degree n over $\mathbb{Q}$, and let A be a central division algebra of degree $d \geq 2$ over F that is not a totally definite quaternion algebra. Let $\mathcal{O}$ be a maximal order in A. We let $\mathbb{G}$ be the algebraic group defined by the reduced norm 1 subgroup $A^1 \subset A^\times$, and $\Gamma = \mathcal{O}^1 = \{x \in \mathcal{O} \mid \mathrm{nrd}(x) = 1\}$.

Let S be a set of prime ideals of $\mathbb{Z}_F$ that are unramified in A and such that for all $\mathfrak{p} \in S$, the residue field $\mathbb{Z}_F/\mathfrak{p}$ is isomorphic to a common finite field $\mathbb{F}_{q_0}$. For all $\mathfrak{p} \in S$, we fix an isomorphism $\iota_\mathfrak{p} \colon \mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathrm{M}_d(\mathbb{F}_{q_0})$.

Let $\mathcal{A} = \mathbb{F}_{q_0}^d$, $s = |S|$ and $N = ds$, and define $\Theta \colon \Gamma \to \mathcal{A}^N$ to be the map sending $\gamma \in \Gamma$ to the word formed by the columns of the $\iota_\mathfrak{p}(\gamma)$ for $\mathfrak{p} \in S$.

Let us write $n = r_1 + 2r_2$ and $r_1 = u + r$, where (r_1, r_2) is the signature of F, and where u is the number of real places σ that are unramified in A, and r is the number of real places σ that ramify in A.

We let $G = \prod_{\sigma\in\mathbb{P}_\infty} \mathrm{SL}_{d_\sigma}(D_\sigma) \cong \Big(\mathrm{SL}_d(\mathbb{R})\Big)^u \times \Big(\mathrm{SL}_{d/2}(\mathbb{H})\Big)^r \times \Big(\mathrm{SL}_d(\mathbb{C})\Big)^{r_2}$.

Following the notations of Section 4, we define $\rho \colon G \to \mathbb{R}_{\geq 0}$ componentwise: for all $g = (g_\sigma)_{\sigma\in\mathbb{P}_\infty} \in G$, let

$$\rho(g) = \max_{\sigma\in\mathbb{P}_\infty} \rho(g_\sigma).$$

For $t > 0$, we define the following compact subset $\mathrm{B}(t) \subset G$:

$$\mathrm{B}(t) = \{g \in G \mid \rho(g) \leq t\}.$$

Note that for all $g, h \in \mathrm{B}(t)$, we have $h^{-1} \in \mathrm{B}(t)$ and $\rho(h^{-1}g) \leq 2t$, by Corollary 7.

Let $\mathcal{C}$ be the code attached to $(\mathrm{B}(t), \Gamma, \Theta)$ as in Section 2. The goal of this section is to analyse the code $\mathcal{C}$, and to obtain aymptotically good families of codes from this construction.

5.1. Minimal distance. — Let us start with the following lemma:

Lemma 15. — *Let A be a central simple algebra of degree d over a number field F, and let $\mathcal{O}$ be an order in A. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_F$ such that there is an isomorphism $\iota_{\mathfrak{p}} \colon \mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathrm{M}_d(\mathbb{F}_q)$. Let $x \in \mathcal{O}$, and let r be the rank of the matrix $\iota_{\mathfrak{p}}(x)$. Then $|\mathcal{O}/(\mathfrak{p}\mathcal{O} + x\mathcal{O})| = q^{d(d-r)}$.*

Proof. — Let $m = \iota_{\mathfrak{p}}(x)$. We have $\mathcal{O}/(\mathfrak{p}\mathcal{O}+x\mathcal{O}) \cong \mathrm{M}_d(\mathbb{F}_q)/(m\cdot\mathrm{M}_d(\mathbb{F}_q))$. Since $\dim_{\mathbb{F}_q}(m\cdot\mathbb{F}_q^d) = r$ by definition, we have $\dim_{\mathbb{F}_q}(m\cdot\mathrm{M}_d(\mathbb{F}_q)) = dr$, and therefore $\dim_{\mathbb{F}_q}\mathrm{M}_d(\mathbb{F}_q)/(m\cdot\mathrm{M}_d(\mathbb{F}_q)) = d(d-r)$, proving the result. □

Concerning the minimum Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$, we obtain:

Proposition 16. — *We have*

$$d_H(\mathcal{C}) \geq N - nd^2\log_q(2) - \frac{2nd^2t}{\log q}\cdot$$

Proof. — Denote by $d_{\mathcal{C}}$ the minimal distance of the code $\mathcal{C}$. Let $x \neq y$ be elements of $\Gamma \cap c\mathrm{B}(t)$ such that $d_H(\Theta(x), \Theta(y)) = d_{\mathcal{C}}$. Let $z = y^{-1}x - 1 \in \mathcal{O}$; the element z is nonzero and therefore $\mathrm{N}(z) \neq 0$ since A is a division algebra. For each $\mathfrak{p} \in S$, let $k_{\mathfrak{p}}$ be the number of zero columns of $\iota_{\mathfrak{p}}(z)$. Since multiplying a matrix by $\iota(y)^{-1}$ on the left does not change which columns are zero, we get $\sum_{\mathfrak{p}\in S} k_{\mathfrak{p}} = N - d_{\mathcal{C}}$. Moreover, for all $\mathfrak{p} \in S$ the rank of $\iota_{\mathfrak{p}}(z)$ is at most $d - k_{\mathfrak{p}}$, so by Lemma 15 we have $|\mathcal{O}/(\mathfrak{p}\mathcal{O} + z\mathcal{O})| \geq q_0^{dk_{\mathfrak{p}}}$. We obtain

$$\mathrm{N}(z) = |\mathcal{O}/z\mathcal{O}| \geq \prod_{\mathfrak{p}\in S} q_0^{dk_{\mathfrak{p}}} = q_0^{d(N-d_{\mathcal{C}})} = q^{N-d_{\mathcal{C}}}.$$

On the other hand, let us write $x = cx_0$ and $y = cy_0$, with $x_0, y_0 \in \mathrm{B}(t)$ and where $c \in G$ is as in Section 2. Since $\rho(y^{-1}x) = \rho(y_0^{-1}x_0) \leq 2t$, by Corollary 8 we obtain

$$\mathrm{N}(z) = \prod_{\sigma\colon F\hookrightarrow\mathbb{C}} |\sigma(\mathrm{nrd}(z))|^d \leq 2^{nd^2}\exp(nd^2\rho(y^{-1}x)) \leq 2^{nd^2}\exp(2nd^2t).$$

Taking logarithms and dividing by $\log q$ gives the result. □

As consequence, we have:

Corollary 17. — *Suppose that $t > 0$ is such that $2t \leq \dfrac{N\log q}{nd^2} - \log 2$. Then $\Theta|_{\Gamma\cap c\mathrm{B}(t)}$ is injective.*

5.2. Number of codewords. — Recall that $G = \prod_{\sigma\in\mathbb{P}_\infty} \mathrm{SL}_{d_\sigma}(D_\sigma)$. Then G inherits the topology product and the product measure $\otimes_\sigma d_{\mu_\sigma}$, where the volume form d_{μ_σ} is normalized as in Section 4.2. Let us start with Prasad's formula for the volume $G/\mathcal{O}^1$.

Proposition 18. — *We have*

$$\mu(G/\mathcal{O}^1) = d^{\frac{n}{2}} \left(\frac{\Delta_A}{\Delta_F}\right)^{1/2} \prod_{j=2}^{d} \zeta_F(j) \cdot \Phi,$$

where

$$\Phi = \prod_{\mathfrak{p}} \prod_{0<i<d, e_\mathfrak{p} \nmid i} (1 - N(\mathfrak{p})^{-i}).$$

Proof. — We use Prasad's formula [**16**, Theorem 3.7] where the normalisation of the volume is defined as follows. On each factor $\mathfrak{g}_\sigma = \mathfrak{sl}_{d_\sigma}(D_\sigma)$, the choice of a volume form determines one on $\mathfrak{g}_\sigma \otimes_\mathbb{R} \mathbb{C}$. Prasad chooses the volume form that gives volume 1 to a maximal compact subgroup $K' \cong \mathrm{SU}_d(\mathbb{C})^n$ of $\mathbb{G}(\mathbb{C}) = (A \otimes_\mathbb{R} \mathbb{C})^1$. For this normalisation, Prasad's formula yields

$$\mu_{\mathrm{Pras}}(G/\mathcal{O}^1) = \left(\frac{\Delta_A}{\Delta_F}\right)^{1/2} \left(\prod_{k=1}^{d-1} \frac{k!}{(2\pi)^{k+1}}\right)^n \prod_{j=2}^{d} \zeta_F(j) \cdot \Phi$$

(for details, the reader can refer to [**13**, Theorem 2.4.1.10]). To relate our normalisation to the one of Prasad, we relate the norm $\|\cdot\|$ on $\mathfrak{sl}_{d_\sigma}(D_\sigma) \otimes_\mathbb{R} \mathbb{C} \cong \mathfrak{sl}_d(\mathbb{C})^{[F_\sigma : \mathbb{R}]}$ that we defined previously, to the norm $\|\cdot\|_\mathbb{C}$ on the same Lie algebra, induced by the one on $\mathfrak{sl}_{d_\sigma}(D_\sigma)$. We find $\|\cdot\|_\mathbb{C} = \frac{1}{\sqrt{2}}\|\cdot\|$. Denoting $\mu_\mathbb{C}$ the measure induced by the metric $\|\cdot\|_\mathbb{C}$, we have

$$\mu_\mathbb{C}(K') = 2^{-\frac{n(d^2-1)}{2}} \left(2^{d^2+d/2-3/2}\sqrt{d} \prod_{k=1}^{d-1} \frac{\pi^{k+1}}{k!}\right)^n,$$

thanks to $\mu_\mathbb{C}(\mathrm{SU}_d(\mathbb{C})) = 2^{d^2+d/2-3/2}\sqrt{d} \prod_{k=1}^{d-1} \frac{\pi^{k+1}}{k!}$ by Proposition 11(ii). Finally, we get the formula since

$$\mu(G/\mathcal{O}^1) = \mu_{\mathrm{Pras}}(G/\mathcal{O}^1)\mu_\mathbb{C}(K').$$

□

Corollary 19. — *We have*

$$\log \mu(G/\mathcal{O}^1) \leq \frac{1}{2} \log \left(\frac{\Delta_A}{\Delta_F}\right) + O(n \log d).$$

Proof. — It follows from $\zeta_F(j) \leq \zeta(j)^n \leq (1 + O(2^{-j}))^n$ for $j \geq 2$ and $\Phi \leq 1$. □

This estimation allows us to obtain the following estimation on the rate of $\mathcal{C}$:

Proposition 20. — *Assume that $s = |S| = n$. For all $t \geq 1$ as in Corollary 17, we have*

$$\frac{1}{N} \log |\mathcal{C}| \geq \frac{d}{200}t - \frac{d^2-1}{2d} \log \mathrm{rd}_F - \frac{1}{2n} \log \mathrm{N}(\delta_A) - \frac{3d}{2} \log d + O(d).$$

Proof. — We have $N = dn$, and by Lemma 1, $|\mathcal{C}| \geq \dfrac{\mu(\mathrm{B}(t))}{\mu(G/\mathcal{O}^1)}$. Since $\mathrm{B}(t)$ is a product of balls on each of the factors, Proposition 14, together with Corollary 19 and the relation $\Delta_A = N(\delta_A)^d \Delta_F^{d^2}$, give the result. □

5.3. Analysis of the code. — Let us start with the existence of unramified towers of number fields with splitting conditions.

Proposition 21. — *There exist an integer M_0 and a real number $C > 0$ such that for all primes p satisfying $\left(\frac{M_0}{p}\right) = 1$, there exists a sequence of number fields $(F_k)_k$ such that: (i) $[F_k\colon \mathbb{Q}] \to \infty$, (ii) the prime p splits totally in $F_k/\mathbb{Q}$, and (iii) $\mathrm{rd}_{F_k} \leq C$.*

Proof. — This follows from well-known methods in the study of towers of bounded root discriminant, using a tower above a quadratic field. The reader may refer to [**11**, Section 5]. □

We now prove the main result of this work.

Theorem 22. — *For all $d \geq 2$, there exists a family of asymptotically good number field codes, each obtained from the group of units of reduced norm 1 in a maximal order in a division algebra of degree d, over a fixed alphabet $\mathbb{F}_p^d$, where $\log p = c \log d + O(\log\log d)$ and $c > 0$ is a constant.*

Proof. — Let $d \geq 2$. We pick a family of number fields F_k with $\mathrm{rd}_{F_k} \leq C$ as in Proposition 21, leaving $p \geq 5$ to be chosen later. Fix F_k and put $n = [F_k : \mathbb{Q}]$. We choose A a central division algebra of degree d over F_k ramified exactly at one prime $\mathfrak{p}_2$ above 2 and one prime $\mathfrak{p}_3$ above 3; by Class Field Theory such an algebra does exist. This implies $\mathrm{N}(\delta_A)^{\frac{1}{nd}} \leq 6$. We choose S to be the set of primes of F_k above p, so that $q_0 = p$, $q = p^d$, $s = n = [\mathbb{F}_k : \mathbb{Q}]$ and $N = nd$. Let $\mathcal{C}$ be the unit group code constructed from A. The quantity of Proposition 20

$$\frac{d}{200}t - \frac{d^2-1}{2d}\log \mathrm{rd}_F - \frac{1}{2n}\log \mathrm{N}(\delta_A) - \frac{3d}{2}\log d + O(d)$$

can be written as

$$\frac{d}{200}t - \frac{3d}{2}\log d + O(d)\cdot$$

We pick $t \geq 1$ such that $\dfrac{d}{200}t - \dfrac{3d}{2}\log d + O(d) \geq 1$, so that $t = 300\log d + O(1)$. By Proposition 16 we have

$$\frac{d_H(\mathcal{C})}{N} \geq 1 - \frac{\log 2}{\log p} - \frac{2t}{\log p}\cdot$$

We pick p such that $\log p \geq \dfrac{1}{1-d^{-1}}(\log 2 + 2t)$, so that $\dfrac{d_H(\mathcal{C})}{N} \geq \dfrac{1}{d}$. By Proposition 20 and by the choice of t, we have

$$\frac{1}{N}\log|\mathcal{C}| \geq 1.$$

Since any $p \geq 5$ such that $(\frac{M_0}{p}) = 1$ can be used, by the Dirichlet arithmetic progression theorem, there exists such p with $\log p = 2t + O(\log t)$, i.e. $\log p = 600\log d + O(\log\log d)$. □

Remark 23. — *The main contributions come from the volume of K and from the exponential growth rate of the volume of* $\mathrm{B}(t)$. *We obtain $c = 600$ as an admissible value. We did not try to optimise this constant. It would be interesting to find families of unit group codes with a better asymptotic behaviour of* $\log p$ *as $d \to \infty$.*

5.4. Quaternion case. — In this section, A is a quaternion algebra, i.e. $d = 2$. First, it is easy to give a closed formula for the volume of $\mathrm{B}(t)$.

Proposition 24. — *We have*

$$\mu(\mathrm{B}(t)) = 2^{\frac{3}{2}u+\frac{5}{2}r+4r_2}\pi^{2r_1+3r_2}(\cosh(2t)-1)^u(\sinh(4t)-4t)^{r_2}.$$

Proof. — We compute the volume on each factor.
By Proposition 11, we have $\mu(\mathrm{SO}_2(\mathbb{R})) = 2\sqrt{2}\pi$, $\mu(\mathrm{SU}_2(\mathbb{C})) = 16\pi^2$ and $\mu(\mathrm{SL}_1(\mathbb{H})) = 4\sqrt{2}\pi^2$. In the $\mathrm{SL}_2(\mathbb{R})$ case, the integral to compute is

$$\int_0^t \sinh(2a)da = \frac{1}{2}(\cosh(2t)-1).$$

In the $\mathrm{SL}_2(\mathbb{C})$ case, the integral involved is

$$\int_0^t \sinh(2a)^2 da = \frac{1}{8}(\sinh(4t)-4t).$$

Putting these together gives the result. □

In the quaternion case, Prasad's formula allows us to obtain:

Proposition 25. — *We have*

$$\mu(G/\mathcal{O}^1) = 2^{n/2}(\Delta_F)^{\frac{3}{2}}\zeta_F(2)\prod_{\mathfrak{p}|\delta_A}(N(\mathfrak{p})-1).$$

To finish, let us give now an explicit example. Let $F = \mathbb{Q}(\cos(2\pi/11), \sqrt{2}, \sqrt{-23})$ (from [**12**]). The 2-class group of F is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^9$. Let F_1 be the 2-Hilbert class field of F. Let p be prime number such that every prime ideals above p in F splits completely in F_1/F; take a such prime $\mathfrak{p}$. Then there exists an unramified infinite extension L/F such that $\mathfrak{p}$ splits completely in L (see [**11**, Example 9]). Let $F_1 \subset F_k \subset L$ be an intermediate field, of degree n over $\mathbb{Q}$. By construction there exists $n/20$ primes of F_k above $\mathfrak{p}$ of residue degree f_p, where $f_p g_p = 20$. Let A be the quaternion algebra over F_k ramified at exactly two of these primes, and let S be the set of the remaining ones, which has size $s = \dfrac{n}{20} - 2$; $N = ds$. Let $\mathcal{C}$ be the unit group code constructed from A. Then

$$\frac{\mu(\mathrm{B}(t))}{\mu(G/\mathcal{O}^1)} = \frac{\left(2^2\pi^{3/2}(\sinh(4t)-4t)^{1/2}\right)^n}{2^{n/2}\,\mathrm{rd}_{F_k}^{3n/2}\,\zeta_{F_k}(2)(p^{f_p}-1)^2},$$

in particular

$$\left(\frac{\mu(\mathrm{B}(t))}{\mu(G/\mathcal{O}^1)}\right)^{1/n} \geq \frac{(2\pi)^{3/2}(\sinh(4t)-4t)^{1/2}}{\mathrm{rd}_F^{3/2}\,\zeta_F(2)^{1/20}(p^{f_p}-1)^{2/n}}.$$

We have $\mathrm{rd}_F \approx 92.37$ and $\zeta_F(2) \approx 1.02$. For $t = 2.2$ we have

$$\frac{(2\pi)^{3/2}(\sinh(4t)-4t)^{1/2}}{\mathrm{rd}_F^{3/2}\,\zeta_F(2)^{1/20}} > 1,$$

so this is an admissible value for an asymptotically good code. From the minimal distance formula, we need to choose p such that $q_0 = p^{f_p}$ satisfies

$$\log q_0 > \frac{n}{s}(\log 2 + 2t).$$

Asymptotically we can take any p such that $\dfrac{1}{20}\log q_0 > 5.09$, i.e. $p^{f_p/20} \geq 163$.

6. Complement: the additive construction

6.1. The construction (following [11]). — Let us recall the additive construction. Let F be a number field of degree n over $\mathbb{Q}$, and let A be a central division algebra of degree d over F. Consider the locally compact group $G = \prod_{\sigma\in\mathbb{P}_\infty} \mathrm{M}_{d_\sigma}(D_\sigma)$, equipped with

- the Euclidean norm $\mathsf{T}_2(g) = \sum\limits_{\sigma\in\mathbb{P}_\infty} n_\sigma \|\sigma(g)\|_2^2$, where $\|(m_{i,j})\|_2 = \sqrt{\sum_{i,j} e_\sigma |m_{i,j}|^2}$;
- the Lebesque measure $d\mu$ relative to an orthonormal basis of G with respect to T_2.

Let $\mathbb{G} = A$ be the algebraic additive group, and $\Gamma = \mathcal{O}$, where $\mathcal{O}$ is a maximal order of A.

As for the multiplicative group code, let S be a finite set of ideal primes of $\mathbb{Z}_F$ that are unramified in A and such that for all $\mathfrak{p} \in S$, the residue field $\mathbb{Z}_F/\mathfrak{p}$ is isomorphic to a common finite field $\mathbb{F}_{q_0}$. For all $\mathfrak{p} \in S$, we fix an isomorphism $\iota_\mathfrak{p} \colon \mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathrm{M}_d(\mathbb{F}_{q_0})$.

Let $\mathcal{A} = \mathbb{F}_{q_0}^d$, $s = |S|$ and $N = ds$, and define $\Theta\colon \Gamma \to \mathcal{A}^N$ be the map sending $\gamma \in \Gamma$ to the columns of the $\iota_\mathfrak{p}(\gamma)$ for $\mathfrak{p} \in S$.

Take the ball $\mathrm{B}(t) = \{(x_\sigma)_\sigma \in \mathbb{G} \mid \|x_\sigma\|_2 \leq t\}$. Let $\mathcal{C}$ be the code attached to $(\mathrm{B}(t), \Gamma, \Theta)$ as in Section 2. Note that there codewords are columns in $\mathbb{F}_{q_0}^d$, instead of matrices in $\mathrm{M}_d(\mathbb{F}_{q_0})$ as in [**11**]. In other words, here $q = q_0^d$ instead of $q_0^{d^2}$.

Proposition 26. — *We have*

$$d_H(\mathcal{C}) \geq N - d^2 n \log_q(2t) + \frac{d^2 n}{2}\log_q d.$$

Proof. — We follow the proof of Proposition 16. Denote by $d_\mathcal{C}$ the minimal distance of the code $\mathcal{C}$. Let us choose $x \neq y$ in $\Gamma \cap (c + \mathrm{B}(t))$ such that $d_H(\Theta(x), \Theta(y)) = d_\mathcal{C}$, where $c \in G$ is as in Section 2. Let $z = x - y \in \mathcal{O}$; the element z is nonzero and therefore $\mathrm{N}(z) \neq 0$. As for the multiplicative case, we obtain $\mathrm{N}(z) \geq q^{N-d_\mathcal{C}}$. On the other hand, let us write $x = c + x_0$ and $y = c + y_0$, with $x_0, y_0 \in \mathrm{B}(t)$. As $\|\sigma(x-y)\|_2 \leq 2t$, and $\mathsf{T}_2(z) \leq n(2t)^2$, then we obtain

$$\mathrm{N}(z) = \prod_{\sigma\colon F\hookrightarrow\mathbb{C}} |\sigma(\mathrm{nrd}(z))|^d \leq \left(\frac{2t}{d^{1/2}}\right)^{d^2 n},$$

thanks to the estimate (see [**13**, Chapter 2, §3]): $|N_{F/\mathbb{Q}}\,\mathrm{nrd}(x)|^d \leq \left(\frac{\mathsf{T}_2(x)}{dn}\right)^{d^2n/2}$. Taking logarithms and dividing by $\log q$ gives the result. □

Concerning the number of codewords, we have:

Proposition 27. — *Suppose that $\Theta|_{\Gamma\cap(c+\mathrm{B}(t))}$ is injective. Then we have*

$$|\mathcal{C}| \geq \frac{2^{r_2 d^2}\ \mathbb{V}_{d^2}^{r_1}\ \mathbb{V}_{2d^2}^{r_2}\ t^{d^2 n}}{\sqrt{\Delta_A}},$$

where $\mathbb{V}_n$ denotes the volume of the unit ball of the space $\mathbb{R}^n$ equipped with the Lebesgue volume form.

Proof. — Here $\mu(\mathrm{B}(t)) = 2^{r_2 d^2} \mathbb{V}_{d^2}^{r_1} \mathbb{V}_{2d^2}^{r_2} t^{d^2 n}$, and $\mu(G/\mathcal{O}) = \sqrt{\Delta_A}$ (1). Then apply Lemma 1. $\square$

Corollary 28. — *Suppose that $\Theta|_{\Gamma \cap (c+\mathrm{B}(t))}$ is injective. Then we have*

$$\log |\mathcal{C}| \geq nd^2 \log t - \frac{1}{2} \log \Delta_A - nd^2 \log d + O(nd^2).$$

Proof. — Use $\mathbb{V}_n = -\frac{n}{2} \log n + O(n)$. $\square$

6.2. Asymptotic analysis. — We follow now the case of the multiplicative group of Section 5.3 to obtain the following

Theorem 29. — *For all $d \geq 2$, there exists a family of asymptotically good number field codes, each obtained from the additive group of a maximal order in a division algebra of degree d, over a fixed alphabet $\mathbb{F}_p^d$, where $\log p = \frac{1}{2} \log d + O(\log \log d)$.*

Proof. — Let $d \geq 2$. As in the proof of Theorem 22, we pick a family of number fields F_k, a prime number p, a central division algebra A ramified exactly at one prime $\mathfrak{p}_2$ above 2 and at one prime $\mathfrak{p}_3$ above 3, and a set S of prime, so that $q_0 = p$, $q = p^d$, $s = n = [\mathbb{F}_k : \mathbb{Q}]$ and $N = nd$. Let $\mathcal{C}$ be the additive group code constructed from A and S. Then by Corollary 28 we have

$$\frac{1}{N} \log |\mathcal{C}| \geq d \log t - \frac{1}{2nd} \log \Delta_A - d \log d + O(d) = d \log t - d \log d + O(d).$$

We pick $t \geq 1$ such that $-d \log d + d \log t + O(d) \geq 1$, so that

$$\log t = \log d + O(1).$$

By Proposition 26 we have

$$\frac{d_H(\mathcal{C})}{N} \geq 1 - \frac{\log 2t}{\log p} + \frac{\log d}{2 \log p}.$$

We pick p such that $\log p \geq \dfrac{1}{1 - d^{-1}} \left(\dfrac{1}{2} \log d + O(1) \right)$, so that $\dfrac{d_H(\mathcal{C})}{N} \geq \dfrac{1}{d}$. By Proposition 27 (and by the choice of t), we have $\dfrac{1}{N} \log |\mathcal{C}| \geq 1$. As before, by the Dirichlet arithmetic progression theorem, there exists such p with $\log p = \frac{1}{2} \log d + O(\log \log d)$. $\square$

6.3. Codes over finite fields. — In this section, we explain how to construct codes from quaternion orders, with alphabet naturally given as a finite field.

Theorem 30. — *Let M_0 and C as in Proposition 21, and let $\alpha = -\frac{1}{4} \log \frac{\pi^4}{24}$. For all prime p such that $\left(\frac{M_0}{p}\right) = 1$ and $\log p > \log C + \alpha$, there exists a family of asymptotically good codes over $\mathbb{F}_{p^2}$ obtained from maximal order groups of quaternions algebras.*

1. A factor $2^{-r_2 d^2}$ is missing in [**11**, Proposition 9], but this does not affect the results of the paper.

Proof. — Let F_k be as in Proposition 21. Let p be a prime number that splits totally in $F_k/\mathbb{Q}$, and let S be a maximal subset of primes of F_k above p such that $|S|$ is even.
Let A be a central division algebra of degree d over F_k ramified exactly at each prime ideal $\mathfrak{p}$ of S and with common ramification index $e > 1$. Consider the additive codes as in the previous section. Writing $d = ef$, then $\mathcal{O}/\mathfrak{p}\mathcal{O} \simeq \mathrm{M}_f(\mathbb{F}_{p^e})$, hence codewords are columns $\mathbb{F}_{p^e}^f$. We have $N = f \cdot |S| \geq f \cdot ([F_k : \mathbb{Q}] - 1)$, and $q = p^d$ as before. The only difference with the unramified case concerns the quantity $(\Delta_A)^{1/([F_k:\mathbb{Q}]d)}$ which is not bounded along $F_k/\mathbb{Q}$. Put $n = [F_k : \mathbb{Q}]$. We have

$$\frac{1}{dn} \log \Delta_A = d \log \mathrm{rd}_F + \frac{|S|}{n} f(e-1) \log p.$$

Then, a good parameter $t > 0$ does exist when

$$\log p > (e - \frac{1}{2}) \log d + \frac{1}{2}(e-1) \log p + O(e),$$

i.e when $e < 3$. Although there is no room when $e \geq 3$ (as noted in [**11**, §7.5.3]), we may construct maximal orders good codes over finite fields by using quaternions algebras. $\square$

Remark 31. — *The existence of unramified towers with splitting conditions and* small root discriminant *is then central in the asymptotic analysis of number field codes, especially when we look for codes over $\mathbb{F}_{p^2}$ with p as small as possible (see for example* [**5**]*). For towers of number fields of small root discriminant see for example* [**6**].

Remark 32. — *When d is* even*, our last computation shows how to construct asymptotically good additive codes from algebras of degree d where codewords are columns $\mathbb{F}_{p^2}^{d/2}$.*

References

[1] A. Borel, Harish-Chandra, *Arithmetic subgroups of algebraic groups.* Ann. of Math. (2) **75** (1962) 485–535.

[2] N. Bourbaki, *Groupes et Algèbres de Lie, Chapitres 7 et 8*, Springer, 2017.

[3] D. Bump, *Lie Groups*, Graduate Texts in Math. 225, Springer, 2013.

[4] V.D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. **24** (1981), 170-172.

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

[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] Z.-G. Hu and K.-H. Yan, *The Weyl Integration Model for KAK decomposition od Reductive Lie Group*, Arxiv, 2015.

[8] A.W. Knapp, *Representation Theory of semisimple Groups*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 2001.

[9] 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.

[10] I.G. Macdonald, *The volume of a compact Lie group*, Inventiones Math. **56** (1980), 93-95.

[11] C. Maire and F. Oggier, *Maximal order codes over number fields*, Journal of Pure and Applied Algebra **227** (7) (2018), 1827-1858.

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

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

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

[15] 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.

[16] G. Prasad, *Volumes of S-arithmetic quotients of semi-simple groups*, Publ. Math. IHES **69** (1989), 91-114.

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

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

April 18, 2018

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

Aurel Page, INRIA, Univ. Bordeaux, CNRS, IMB, UMR 5251, F-33400 Talence, France
E-mail : `aurel.page@inria.fr`