Towards a complete DMT classification of division algebra codes
Laura Luzzi, Roope Vehkalahti, Alexander Gorodnik

To cite this version:

HAL Id: hal-01420952
https://hal.archives-ouvertes.fr/hal-01420952
Submitted on 21 Dec 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Towards a complete DMT classification of division algebra codes

Laura Luzzi
Laboratoire ETIS
CNRS - ENSEA - UCP
Cergy-Pontoise, France
laura.luzzi@ensea.fr

Roope Vehkalahti
Department of Mathematics and Statistics
University of Turku
Finland
roive@utu.fi

Alexander Gorodnik
School of Mathematics
University of Bristol
United Kingdom
a.gorodnik@bristol.ac.uk

Abstract—This work aims at providing new lower bounds for the diversity-multiplexing gain trade-off of a general class of lattice codes based on division algebras.

In the low multiplexing gain regime, some bounds were previously obtained from the high signal-to-noise ratio estimate of the union bound for the pairwise error probabilities. Here these results are extended to cover a larger range of multiplexing gains. The improvement is achieved by using ergodic theory in Lie groups to estimate the behavior of the sum arising from the union bound.

In particular, the new bounds for lattice codes derived from $\mathbb{Q}$-central division algebras suggest that these codes can be divided into two classes based on their Hasse invariants at the infinite places. Algebras with ramification at the infinite place seem to provide a better diversity-multiplexing gain trade-off.

I. INTRODUCTION

In [8] it was shown that the union bound can be used to analyze the diversity-multiplexing gain trade-off (DMT) of a large class of lattice codes based on division algebras. Using an upper bound for the pairwise error probability (PEP) in the high signal-to-noise ratio (SNR) regime, the behavior of the union bound was analyzed by combining information about the zeta function and about the distribution of units of the division algebra.

The choice to focus on the high SNR approximation of the PEP allowed to analyze the union bound using algebraic methods. However, it also implicitly restricted the analysis to be effective only for low multiplexing gain levels.

In this work we use a more accurate expression for the pairwise error and extend the earlier DMT analysis to cover a larger range of multiplexing gains. When we have enough receiving antennas, we can cover the whole multiplexing gain region. For fewer receive antennas, we have bounds up to a certain multiplexing gain threshold.

As in [8], the proofs rely heavily on the fact that the codes under analysis are coming from division algebras. This allows us to attack this question using analytic methods from the ergodic theory of Lie groups [3].

This work confirms that from the DMT point of view all the division algebra codes with complex quadratic center have equal (and optimal) diversity-multiplexing gain curve. When the center of the algebra is $\mathbb{Q}$, our work suggests that division algebra based lattice codes can be divided to two subclasses with respect to their DMT. The difference between these two subclasses is whether the Hasse invariant at the infinite place is ramified or not. In particular, division algebras with ramification lead to a better DMT.

Besides giving a new lower bound for the DMT of a general family of division algebra based lattice codes, this work also sheds some light on the applicability and limitations of the union bound approach in Rayleigh fading channels. In [9, Section III.D] the authors speculate that the union bound cannot be used to measure the DMT of a coding scheme accurately. Our work reveals that if we have good enough understanding of the spectrum of the pairwise error probabilities, and we have enough receive antennas, even a naive union bound analysis can be used to analyze the DMT of a space-time code.

II. NOTATION AND PRELIMINARIES

A. Central division algebras

Let $D$ be a degree $n$ $F$-central division algebra where $F$ is either $\mathbb{Q}$ or a quadratic imaginary field. Let $\Lambda$ be an order in $D$ and $\psi_{\text{reg}} : D \to M_n(\mathbb{C})$ the left regular representation of the algebra $D$. When the center $F$ is complex quadratic, $\psi_{\text{reg}}(\Lambda)$ is a $2n^2$-dimensional lattice and when $F = \mathbb{Q}$ it is $n^2$-dimensional. We are now interested in the diversity multiplexing gain trade-off of coding schemes based on the lattices $\psi_{\text{reg}}(\Lambda)$. When $F$ is complex quadratic, we can attack the question directly. However, in the case where the center is $\mathbb{Q}$ we will instead consider lattices $J\psi_{\text{reg}}(\Lambda)J^{-1}$, where $J$ is a certain matrix in $M_n(\mathbb{C})$. (The DMT of the lattices $\psi_{\text{reg}}(\Lambda)$ will be analyzed in an upcoming journal version.)

Consider matrices

$$\begin{pmatrix} A & -B^* \\ B & A^* \end{pmatrix} \in M_{2n}(\mathbb{C}),$$

where $*$ refers to complex conjugation and $A, B \in M_n(\mathbb{C})$. We denote this set of matrices by $M_n(\mathbb{H})$.

The algebra $D$ is ramified at the infinite place if $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_{n/2}(\mathbb{H})$. If it is not, then $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_n(\mathbb{R})$.

Lemma 2.1: [8, Lemma 9.10] If the infinite prime is ramified in the algebra $D$, then there exists a matrix $A \in M_n(\mathbb{C})$ such that $A\psi_{\text{reg}}(\Lambda)A^{-1} \subset M_{n/2}(\mathbb{H})$. If $D$ is not ramified at
The infinite place, then there exists a matrix \( B \in M_n(\mathbb{C}) \) such that \( B\psi_{reg}(\Lambda)B^{-1} \subset M_n(\mathbb{R}) \).

From now on we will simply use the notation \( \psi \) for both embeddings of Lemma 2.1 when the center is \( \mathbb{Q} \) and for \( \psi_{reg} \), when the center is complex quadratic.

### B. System Model

We consider a multiple-input multiple output (MIMO) system with \( n \) transmit antennas and \( m \) receive antennas, and minimal delay \( T = n \). As in [9], the received signal is

\[
Y = \sqrt{\frac{P}{n}} H \bar{X} + W, 
\]

where \( \bar{X} \in M_n(\mathbb{C}) \) is the transmitted codeword, \( H, W \in M_{m,n}(\mathbb{C}) \) are respectively the channel matrix and additive noise, both with i.i.d. circularly symmetric complex Gaussian entries \( h_{ij}, w_{ij} \sim \mathcal{N}_C(0,1) \), and \( \rho \) is the signal-to-noise ratio. The channel is perfectly known at the receiver but not at the transmitter. In the DMT setting, we consider code sequences \( \mathcal{C}(\rho) \) whose size grows with SNR, with multiplexing gain

\[
r = \lim_{\rho \to \infty} \frac{\log |\mathcal{C}|}{\log \rho}.
\]

Let \( P_e \) denote the average error probability of the code under maximum likelihood decoding. Then the diversity gain is

\[
d(r) = -\lim_{\rho \to \infty} \frac{\log P_e(\rho)}{\log \rho}.
\]

Let \( \Lambda \) be an order in a degree \( n \) \( F \)-central division algebra \( D \) and \( \psi \) an embedding as defined in Section II-A.

Given \( M \), we consider the finite subset of elements with Frobenius norm bounded by \( M \):

\[
\Lambda(M) = \{ x \in \Lambda : \|\psi(x)\| \leq M \}.
\]

Let \( k \leq 2n^2 \) be the dimension of \( \Lambda \) as a \( \mathbb{Z} \)-module. As in [8], we choose \( M = \rho^{\frac{k}{2n}} \) and consider codes of the form

\[
\mathcal{C}(\rho) = M^{-1}\psi(\Lambda(M)) = \rho^{\frac{k}{2n}} \psi(\Lambda(\rho^{\frac{k}{2n}})).
\]

The multiplexing gain of this code sequence is indeed \( r \), and it satisfies the average power constraint

\[
\frac{1}{|\mathcal{C}|} \frac{1}{n^2} \sum_{X \in \mathcal{C}} \|X\|^2 \leq 1.
\]

The error probability is given by

\[
P_e = \int_{M_{m,n}(\mathbb{C})} p(H) \rho(H) d\lambda(H),
\]

where \( \lambda \) is the Lebesgue measure, and the density of \( H \) is

\[
p(H) = \frac{1}{\pi^{mn}} \prod_{i=1}^{m} \prod_{j=1}^{n} e^{-|h_{ij}|^2}.
\]

For fixed \( H \), the union bound for the error probability gives

\[
P_e(H) = \Pr \{ \hat{X} \neq \bar{X} | H \} \leq \sum_{X \in \mathcal{C}, X \neq \bar{X}} \Pr \{ \hat{X} \rightarrow X | H \}.
\]

The pairwise error probability is upper bounded by the Chernoff bound on the \( Q \)-function [6]:

\[
\Pr \{ \hat{X} \rightarrow X | H \} \leq e^{-\frac{\rho}{2n}\|H(\bar{X}-X)\|^2}
\]

By linearity of the code,

\[
P_e(H) \leq \sum_{X \in \mathcal{C}, X \neq \bar{X}} e^{-\rho\|H X\|^2}.
\]

By the dotted inequality we mean \( f(\rho) \leq g(\rho) \) if

\[
\lim_{\rho \to \infty} \frac{\log f(\rho)}{\log \rho} \leq \lim_{\rho \to \infty} \frac{\log g(\rho)}{\log \rho}.
\]

To simplify notation, we define \( c = \rho^{1-\frac{2n}{k}} \).

### III. A NEW UPPER BOUND ON THE ERROR PROBABILITY

We now consider a similar argument to our previous paper [8]. Let \( \mathcal{I} \) be a collection of elements in \( \Lambda \), each generating a different right ideal, and let \( \mathcal{I}(M) = \mathcal{I} \cap \Lambda(M) \). Thus, each nonzero element \( x \in \Lambda(M) \) can be written as \( x = vz, \) with \( v \in \Lambda^* \), \( z \in \mathcal{I}(M) \). Since by hypothesis the center \( F \) of the algebra is \( \mathbb{Q} \) or an imaginary quadratic field, the subgroup

\[
\Lambda^1 = \{ x \in \Lambda^* : \det(\psi(x)) = 1 \},
\]

of units of reduced norm 1 in \( \Lambda^* \) has finite index \( j = [\Lambda^* : \Lambda^1] \) [5, p. 211]. Let \( a_1, a_2, \ldots, a_j \) be coset leaders of \( \Lambda^1 \) in \( \Lambda^* \). We note that \( \Gamma = \psi(\Lambda^1) \) is an arithmetic subgroup of a Lie group \( G \). In our case \( G \) is one of the groups \( \text{SL}_n(\mathbb{C}) \), \( \text{SL}_n(\mathbb{R}) \) or \( \text{SL}_n(\mathbb{H}) \).

The previous sum can be rewritten as

\[
\sum_{x \in \mathcal{I}(M)} \sum_{i=1}^{j} \sum_{u \in \Gamma, \|\psi(xa_i)u\| \leq M} e^{-c\|H \psi(xa_i)u\|^2}.
\]

Since \( xa_i \in \Lambda \), we have \( |\det(\psi(xa_i))| = |\det(\psi(x))| \geq 1 \).

For \( i \in \{1, \ldots, j\} \), let’s consider

\[
g_i = \frac{\psi(xa_i)}{|\det(\psi(xa_i))|} \in G.
\]

With a slight abuse of notation, \( \forall a \in G \) we denote by \( B_a(M) \) the “shifted ball” in \( G \):

\[
B_a(M) = \{ g \in G : \|ag\| \leq M \}.
\]

Using the notation \( d_x = |\det(\psi(x))|^{\frac{1}{2n}} \), we find

\[
P_e(H) \leq \sum_{x \in \mathcal{I}(M)} \sum_{i=1}^{j} \sum_{u \in \Gamma, \|H g_i u\|^2} e^{-cd_x^2\|H g_i u\|^2}, \tag{1}
\]

Using a simplified argument inspired by the Strong Wavefront Lemma in [3], we will now show that the sum (1) can be
bounded by an integral over the corresponding ball in $G$.
Let $\mathcal{F}_T$ be the fundamental domain of $\Gamma$ in $G$, which is a compact polyhedron in $G$ containing the identity element $e$. Consequently, $R_T = \max_{g \in \mathcal{F}_T} \|g\|$ is finite (and greater than $n = \|e\|$). Suppose $g \in \mathcal{F}_T$. By submultiplicativity of the Frobenius norm, we have that $\forall a \in M_{m,n}(C),$
$$\|ag\| \leq \|a\| \|g\| \leq R_T \|a\|.$$
In particular, we have that $\forall g \in \mathcal{F}_T,$
$$\bigcup_{u \in \mathbb{B}_x(M)} d\mu(u) \leq \sum_{u \in \mathbb{B}_x(M)} e^{-c\|au\|^2} \leq \sum_{u \in \mathbb{B}_x(M)} e^{-\frac{c}{R_T} \|aug\|^2}.$$
By integrating both sides over $\mathcal{F}_T$, we find
$$\mu(\mathcal{F}_T) \sum_{u \in \mathbb{B}_x(M)} e^{-c\|au\|^2} \leq \mu(\mathcal{F}_T) \sum_{u \in \mathbb{B}_x(M)} \int_{\mathcal{F}_T} e^{-\frac{c}{R_T} \|aug\|^2} d\mu(g),$$
where $\mu$ is the Haar measure over $G$. The last equality follows from the invariance of $\mu$ under $G$-action.
Note that the images $u\mathcal{F}_T$ are disjoint. If $g = u\gamma$ with $\gamma \in \mathcal{F}_T$ and $u \in B_x(M)$,
$$\|xg\| = \|xu\gamma\| \leq \|xu\| \|\gamma\| \leq MR_T R_x.$$
We have
$$\bigcup_{u \in \mathbb{B}_x(M)} u\mathcal{F}_T \subset B_x(MR_T),$$
where the union is disjoint. We can conclude that
$$\sum_{u \in \Gamma, u \in \mathbb{B}_x(M)} e^{-c\|au\|^2} \leq \frac{1}{\mu(\mathcal{F}_T) R_T} \int_{B_x(MR_T)} e^{-\frac{ac}{R_T} \|aug\|^2} d\mu(g).$$
Let $M_x = \frac{R_x M}{dx}$. From (1), the error probability is upper bounded by
$$\int_{M_{m,n}(C)} \frac{1}{\mu(\mathcal{F}_T)} \sum_{x \in \mathcal{I}(M)} \sum_{i=1}^{\mathcal{J}} \int_{B_{x}(M)} e^{-\frac{c}{R_T} \|Hg\|^2} d\mu p(H) d\lambda = \frac{\mathcal{J}}{\mu(\mathcal{F}_T)} \sum_{x \in \mathcal{I}(M)} \int_{M_{m,n}(C)} \int_{B_{x}(M)} e^{-\frac{c}{R_T} \|Hg\|^2} d\mu p(H) d\lambda.$$ Since the integrand is a measurable and non-negative function, by Tonelli’s theorem we can exchange the two integrals. From the determinant bound in [6], we have that $\forall X \in M_n(C),$
$$\int_{M_{m,n}(C)} \int_{B_{x}(M)} e^{-\frac{c}{R_T} \|Hg\|^2} p(H) d\lambda(H) = \frac{1}{(\det(I + cXX^*))^m}. $$
Thus the error probability is bounded by
$$\frac{\mathcal{J}}{\mu(\mathcal{F}_T)} \sum_{x \in \mathcal{I}(M)} \int_{B_{x}(M)} e^{-\frac{c}{R_T} \|Hg\|^2} p(H) d\mu(g) = \frac{\mathcal{J}}{\mu(\mathcal{F}_T)} \sum_{x \in \mathcal{I}(M)} \int_{B_{x}(M)} \frac{1}{(\det(I + \frac{c}{R_T} \rho - \frac{c}{R_T} gg^*))} d\mu.$$ Our problem is now reduced to finding an asymptotic upper bound for the integral
$$I_x = \int_G \frac{1}{(\det(I + \frac{c}{R_T} \rho - \frac{c}{R_T} gg^*))^m} \chi_B(\frac{2}{R_T} g) d\mu(g) (2)$$
where $\chi_B$ is the indicator function of the set $B$, and where we define $\delta_x = \frac{2}{R_T}$ to simplify notation. Note that
$$P_T \leq \frac{\mathcal{J}}{\mu(\mathcal{F}_T)} \sum_{x \in \mathcal{I}(M)} I_x (3)$$
In the cases we’re interested in, $G$ is a connected noncompact semi-simple Lie group with finite center and admits a Cartan decomposition $G = K \exp(a^+)K$, where $K$ is a maximal compact subgroup of $G$, and $A^+ = \exp(a^+)$, with $a^+$ the positive Weyl chamber associated to a set of positive restricted roots $\Phi^+$. Given a root $\alpha \in \Phi^+$, we denote its multiplicity by $m_\alpha$. The highest weight is the sum of positive restricted roots with their multiplicities: $\beta = \sum_{\alpha \in \Phi^+} m_\alpha \alpha$. The following identity holds for any function $f \in L^1(G) [2]$: 
$$\int_G f d\mu = \int_{K \times a^+ \times K} f(k(\exp(a))k') \prod_{\alpha \in \Phi^+} (\sinh \alpha(a))^{m_\alpha} dk d\alpha k'$$
where $da$ and $dk$ are the Haar measures on $a^+$ and $K$ respectively.
Note that in (2), the integrand $f$ is invariant by $K$-action both on the left and on the right since it only depends on the singular values of $g$. So by definition of Haar measure,
$$\int_G f d\mu = \int_{a^+} f(\exp(a)) \prod_{\alpha \in \Phi^+} (\sinh \alpha(a))^{m_\alpha} da.$$ The dominant term (as a function of $\rho$) of the integral (2) corresponds to the highest term of the sum
$$\prod_{\alpha \in \Phi^+} (\sinh \alpha(a))^{m_\alpha} = \sum_{\xi \in \mathcal{I}(a)} h_\xi e^{\xi(a)}.$$ The highest term corresponds to $\xi = \beta$ [2]. Therefore the dominant term of the expression is
$$\int_G f(\exp(a)) e^{\beta(a)} da. (4)$$
IV. DMT BOUNDS FOR DIVISION-ALGEBRA BASED CODES
In this section we will prove the following DMT bounds for the three classes of codes introduced earlier.

Proposition 4.1: Case $F = \mathbb{Q}(\sqrt{-d})$, $G = SL_n(C)$. Let $d^*(r)$ be the piecewise linear function taking values $\lceil n - (m - r) \rceil$ when $r$ is a positive integer, with equation
$$d^*(r) = -(m + n - 2 \lceil r \rceil - 1) + m n - \lfloor r \rfloor \lfloor r \rfloor + 1. (5)$$
The DMT for space-time codes arising from $2n^2$-dimensional division algebras with center $F = \mathbb{Q}(\sqrt{-d})$ is $d^*(r)$ if $m \geq 2 \lceil r \rceil - 1$.
The DMT $d^*(r)$ is optimal for space-time codes [9], and Proposition 4.1 is well-known [1], but an alternative proof is included here for the sake of completeness.
Proposition 4.2: Case $F = \mathbb{Q}$, $G = \text{SL}_n(\mathbb{R})$. Let $d_1(r)$ be the line segment connecting the points $(r, [(m-r)(n-r)]^+)$ where $2r \in \mathbb{Z}$, with equation

$$d_1(r) = (-n-2m+2[2r]+1)r + mn - \frac{[2r]}{2}([2r]+1).$$

The DMT for space-time codes arising from $k = n^2$-dimensional division algebras with center $\mathbb{Q}$ not ramified at the infinite place is $d_1(r)$ if $m \geq [2r] - \frac{1}{2}$.

Proposition 4.3: Case $F = \mathbb{Q}$, $G = \text{SL}_n(\mathbb{H})$. Suppose that $n$ is even. Let $d_2(r)$ be the piecewise linear function connecting the points $(r, [(n-2r)(m-r)]^+)$ for $r \in \mathbb{Z}$. The DMT for space-time codes from $n^2$-dimensional division algebras with center $\mathbb{Q}$ which are ramified at the infinite place is $d_2(r)$ provided that $m \geq 2[r] - 1$.

Remark 4.4: The results in Propositions 4.2 and 4.3 are new. Although this proof only provides a lower bound, we conjecture that $d_1(r)$ and $d_2(r)$ are actually the DMTs for these space-time codes for all values of $r$.

Before proceeding with the proofs, we describe the Lie group structures associated to the three main types of codes considered in this paper. Due to lack of space, we omit definitions and details, and refer to [8, Appendix A].

Example 1: $F = \mathbb{Q}(\sqrt{-d})$, $G = \text{SL}_n(\mathbb{C})$. We have $\Phi^+ = \{e_1, \ldots, e_k \}_{1 \leq k}$, with multiplicity $m_\alpha = 2$ for all $\alpha \in \Phi^+$. Consider the algebra $\mathfrak{a} = \{a = \text{diag}(a_1, \ldots, a_n) : \sum_{i=1}^n a_i = 0\}$. The positive Weyl chamber associated to $\Phi^+$ is $\mathfrak{a}^+ = \{a \in \mathfrak{a} : a_1 \geq a_2 \geq \cdots \geq a_n\}$. We have the Cartan decomposition $\text{SL}_n(\mathbb{C}) = K \times A^+ \times K$, where $K = \text{SU}_n$ and $A^+ = \exp(\mathfrak{a}^+)$. The highest weight is $\beta(\mathfrak{a}) = \sum_{i=1}^n 4(n-i)a_i$.

Example 2: $F = \mathbb{Q}$, $G = \text{SL}_n(\mathbb{R})$. We have $\Phi^+ = \{e_1, \ldots, e_k \}_{1 \leq k}$, with multiplicity $m_\alpha = 1$ for all $\alpha \in \Phi^+$. The positive Weyl chamber associated to $\Phi^+$ is again $\mathfrak{a}^+ = \{a \in \mathfrak{a} : a_1 \geq a_2 \geq \cdots \geq a_n\}$, and $\beta(\mathfrak{a}) = \sum_{i=1}^n 2(n-i)a_i$. We have $\text{SL}_n(\mathbb{R}) = K \times A^+ \times K$, where $K = \text{SO}_n$ and $A^+ = \exp(\mathfrak{a}^+)$.\n
Example 3: $F = \mathbb{Q}$, $G = \text{SL}_n(\mathbb{H})$. Let $n = 2p$. Consider $\mathfrak{a} = \{a = \text{diag}(a_1, \ldots, a_p, a_{p+1}, \ldots, a_n) : \sum_{i=1}^p a_i = 0\}$. We have $\Phi^+ = \{e_1, \ldots, e_k \}_{1 \leq k \leq 2p}$, with $m_\alpha = 1$ for all $\alpha \in \Phi^+$, and $\beta(\mathfrak{a}) = 8 \sum_{i=1}^p (p-i)a_i$. The positive Weyl chamber associated to $\Phi^+$ is $\mathfrak{a}^+ = \{a \in \mathfrak{a} : a_1 \geq a_2 \geq \cdots \geq a_p\}$.

In all three cases, $\mathfrak{a}^+$ is a set of diagonal $n \times n$ matrices.

Proof of Propositions 4.1, 4.2, 4.3: For the integral (2), the dominant term (4) is given by

$$\int_{\mathfrak{a}^+} \int_{\Pi_n=1} \frac{e^{\beta(\mathfrak{a})}}{\prod_{i=1}^n (1 + \delta x_\mathfrak{b}^1 e^{2\mathfrak{a}_i})} \frac{\chi_{\mathfrak{a}}(\sum_{i=1}^n e^{2\mathfrak{a}_i} \leq \frac{2\mathfrak{x}}{\mathfrak{a}})}{\mathfrak{a}_1 \leq \log \frac{\mathfrak{x}}{\mathfrak{a}} \delta_{\mathfrak{a}}} \, d\mathfrak{a}_1 \cdots d\mathfrak{a}_{n-1}$$

Note that the integral is only in $n-1$ variables and $a_n$ is just a dummy variable since $a_1 + a_2 + \cdots + a_n = 0$.

Now consider the change of variables $a_i = b_i \log \left( \frac{\mathfrak{x}_i}{\mathfrak{a}} \right)$. Giving that $\delta_a \geq 1/\mathfrak{R}_\mathfrak{a}$, this integral is bounded by

$$\left( \frac{\mathfrak{R}_\mathfrak{a}}{\mathfrak{k}} \right) \int_{\mathbb{B}} \int_{\Pi_n=1} \frac{e^{\beta(\mathfrak{a})}}{\prod_{i=1}^n (1 + e^{2\mathfrak{b}_i-1} \mathfrak{x}_i \delta_{\mathfrak{a}})} \, db$$

where $\mathbb{B} = \{b \in \mathbb{a}^+ : b_1 \leq 1\}$. We neglect logarithmic factors of $\rho$ in the sequel.

Let $(x^+) = \max(0, x)$. From the inequality $(1 + e^-x) \leq 1$, we find the upper bound

$$\int_{\mathbb{B}} e^{\beta(\mathfrak{b})} \log \frac{x^{n/k}}{\mathfrak{k}} \sum_{i=1}^n \left( 2(b_i-1) \log \frac{x^{n/k}}{\mathfrak{k}} + \log \rho \right)^+ \, db$$

$$\int_{\mathbb{B}} e^{-\log \rho} \left( \frac{x^{n/k}}{\mathfrak{k}} \beta(b) - m \sum_{i=1}^n (2(b_i-1)(\frac{x^{n/k}}{\mathfrak{k}} + \log \rho)) + 1 \right)^+ \, db$$

$$\int_{\mathbb{B}} e^{-\log \rho} \left( -\frac{x^{n/k}}{\mathfrak{k}} \beta(b) + m \sum_{i=1}^n 1(2(b_i-1)+1)^+ \right) db_1 \cdots db_{n-1}$$

where $\frac{x^{n/k}}{\mathfrak{k}} = \frac{\mathfrak{x}}{\mathfrak{k}} - \frac{\mathfrak{x}_a}{\mathfrak{k}} - \frac{\mathfrak{x}_n}{\mathfrak{k}} \leq \frac{\mathfrak{x}}{\mathfrak{k}}$. Note that $\mathbb{B}$ is contained in an $(n-1)$-dimensional cube with Lebesgue measure 1. So our integral can be upper bounded by

$$\min_{\mathbb{P}} \left( -\frac{x^{n/k}}{\mathfrak{k}} \beta(b) + m \sum_{i=1}^n 1(2(b_i-1)+1)^+ \right)$$

$$\min_{\mathbb{P}} \left( -\frac{x^{n/k}}{\mathfrak{k}} \beta(b) + m \sum_{i=1}^n (a_i+1-2s/k)^+ \right)$$

where $\mathbb{P} = \left\{ \frac{n}{k} \mathfrak{a} \leq \mathfrak{a} \leq \mathfrak{a} + \frac{r}{k} \right\}$. Thus, we need to find

$$\tilde{d}(s) = \min_{\mathbb{P}} g(\alpha), \text{ where}$$

$$g(\alpha) = -\beta(\alpha)/2 + m \sum_{i=1}^n (a_i+1-2s/n)^+ \text{.}$$

The proof of the following two Remarks is elementary but rather tedious and is omitted due to lack of space.

Remark 4.5: (Case $G = \text{SL}_n(\mathbb{C})$). On $\mathfrak{a}^+$, $\beta(\mathfrak{a}) = -\sum_{i=1}^n 4i\alpha_i$. In this case

$$g(\alpha) = \sum_{i=1}^n \left( 2i\alpha_i + m(\alpha_i+1-2s/n)^+ \right)$$

$$\mathbb{P} = \left\{ s/n \geq \max_{i} \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n, \sum_{i=1}^n \alpha_i = 0 \right\}.$$
Remark 4.6: (Case $G = SL_n(\mathbb{R})$). On $a^+, \beta(\alpha) = -\sum_{i=1}^{n} 2\alpha_i$. In this case we have

$$g(\alpha) = \sum_{i=1}^{n} \left( i\alpha_i + m(\alpha_i + 1 - 2s/n)^+ \right),$$

$$\mathcal{P} = \left\{ \sum_{i=1}^{n} \left( i\alpha_i + m(\alpha_i + 1 - 2s/n)^+ \right) \geq 0 \right\}.$$

If $m \geq [2s] - 1$, then $\min_{\alpha \in \mathcal{P}} g(\alpha) = d_1(s)$. The following Remark is more immediate.

Remark 4.7: (Case $G = SL_{n/2}(\mathbb{H})$). Let $n = 2p$. Recall that $a = \{a = \text{diag}(a_1, \ldots, a_p, a_1, \ldots, a_p) : \sum_{i=1}^{p} a_i = 0 \}$, and $\beta(\alpha) = -8\sum_{i=1}^{n} i\alpha_i$ on $a^+$. We have that $g(\alpha) = 2\sum_{i=p+1}^{n} i\alpha_i$ on $a^+$. The diversity order $d(s)$ is lower bounded by the piecwise linear function connecting the points $(s, 2(p-s)(m-s))$ for $s \in \mathbb{Z}$, if $m \geq 2(s/2) - 1$. We can conclude that (neglecting logarithmic factors) the dominant term in $\rho$ in (2) is of the order $f(\delta_x)$,

$$f(t) = \rho^{-d(s)} = \rho^{-d\left(r - \frac{k \log t}{n \log \rho}\right)}.$$

Consequently, the dominant term in (3) is bounded by

$$\frac{j}{\mu(F)} C(\log \rho R_{t})^{n-1} \sum_{x \in \mathcal{P}(\rho R_{t})} \rho^{-d\left(r - \frac{k \log t}{n \log \rho}\right)},$$

where $C$ is a constant independent of $\rho$ and $x$. We have

$$\sum_{x \in \mathcal{P}(\rho R_{t})} f(\delta_x) \leq \sum_{x \in \mathcal{P}(\rho R_{t})} f(\delta_x) \leq \sum_{x \in \mathcal{P}_t} f(\delta_x) \leq \sum_{x \in \mathcal{P}(\rho R_{t})} f(\delta_x),$$

where the arithmetic-geometric mean inequality, $d_x = |\det(\psi(x))|^{\frac{1}{2}} \leq \lVert \psi(x) \rVert$. Given $t \in \mathbb{N}$, define $s_t = \{x \in \mathcal{P} : \delta_x < t+1\}$, and $\forall t > 0$, let $S_t = \sum_{\delta_x \leq t} S_t$. Since $j$ is decreasing and $\delta_x = d_x/R_t \leq d_x$,

$$\sum_{x \in \mathcal{P}(\rho R_{t})} f(\delta_x) \leq \sum_{x \in \mathcal{P}(\rho R_{t})} s_t f(t).$$

Using summation by parts [7, Theorem 1], we have

$$\sum_{t \leq \rho R_{t}} s_t f(t) = S(\rho R_{t}) f(\rho R_{t}) - \int_{\rho R_{t}}^{\rho R_{t+n}} S(t) f'(t) dt.$$

It is known [4, Theorem 29] that given a central simple algebra $D$ over $\mathbb{Q}$ and an order $\Delta$ in $D$, $\exists c, \delta > 0$ such that

$$\sum_{x \in \mathcal{P}} \left| \det(\psi(x)) \right|^{\frac{1}{2}} \leq \lVert \psi(x) \rVert.$$

Similarly, for a central simple algebra $\mathcal{A}$ over an imaginary quadratic field $F$ and an order $\Delta$ in $\mathcal{A}$, $\exists c, \delta > 0$ such that

$$\sum_{x \in \mathcal{P}} \left| \det(\psi(x)) \right|^{\frac{1}{2}} \leq \lVert \psi(x) \rVert.$$

In both cases, the exponent of $A$ is equal to $k/n$. Thus,

$$S(t) = \left\{ x \in \mathcal{P} : 1 \leq \left| \det(\psi(x)) \right| \leq R_{t}^{\frac{1}{n}} \rceil n \rceil \right\} \sim t^k.$$

Since $f(\rho R_{t}) = \rho^{-d(0)} = \rho^{-m+n}$, the first term in (8) is of the order $S(\rho R_{t}) f(\rho R_{t}) \sim \rho^{-m+n}$, which is smaller than $\rho^{-d(r)}$ in the three cases. The second term in (8) is

$$- \int_{1}^{\rho R_{t}} t^{k} \rho^{-d\left(r - \frac{k \log t}{n \log \rho}\right)} (\rho R_{t}) f'(t) dt$$

$$= - \int_{0}^{\rho R_{t}} t^{k} \rho^{-d\left(r - \frac{k \log t}{n \log \rho}\right)} (\rho R_{t}) dv$$

$$\leq C \log \rho \int_{0}^{\rho R_{t}} t^{k} \rho^{-d(v)} dv$$

after the change of variables $v = r - \frac{k \log t}{n \log \rho}$, since $(\rho R_{t})' \leq 0$. Let $d^*(v) = \nu v + d(v)$.

a) Case $G = SL_n(\mathbb{C})$: $d^*(v) = \nu v + d(v)$ is a piecewise linear function interpolating the points of the parabola $v^2 - \nu v + m$ for $v \in \mathbb{Z}$, $v \leq \min(m, n)$. It is decreasing in $[0, \nu]$ provided that $d^*([\nu] - 1) \geq d^*([\nu])$, or equivalently if $\nu \geq 2|\nu| - 1$. If $m \geq 2|R| - 1$, then

$$\int_{0}^{\rho R_{t}} t^{k} \rho^{-d^*(v)} dv \leq \nu \rho^{-d^*(r)}.$$

and so $P_\rho(\rho) \leq \rho^{-d\rho}$. For $\rho R_{t}$.

b) Case $G = SL_n(\mathbb{R})$: $d^*(v) = \nu v + d(v)$ interpolates the points $v^2 - \nu v + m$ for $v \in \mathbb{Z}$, $v \leq \min(m, n)$. It is decreasing in $[0, \nu]$ provided that $d^*([\nu] - 1) \geq d^*([\nu])$, or equivalently if $\nu \geq 2|\nu| - 1$. With the same reasoning as before we find $P_\rho(\rho) \leq \rho^{-d\rho}$. For $\rho R_{t}$.

c) Case $G = SL_{n/2}(\mathbb{H})$: $d^*(v) = \nu v + d(v)$ is a piecewise linear function interpolating the points $v^2 - \nu v + m$ for $v \in \mathbb{Z}$, $v \leq \min(m, n)$. It is decreasing in $[0, \nu]$ provided that $\nu \geq 2|\nu| - 1$. If $m \geq 2|R| - 1$, then we obtain $P_\rho(\rho) \leq \rho^{-d\rho}$.

\textbf{Acknowledgements}

The research of R. Vehkalahti is funded by the Academy of Finland grant #283135 and the Finnish Cultural Foundation. The research of A. Gorodnik was funded by ERC grant #239066.

\textbf{REFERENCES}


