Probability Bounds for an Eavesdropper's Correct Decision over a MIMO Wiretap Channel

David Karpuk
Dept. of Mathematics
and Systems Analysis
P.O. Box 11100
FI-00076 Aalto
Finland
Email: david.karpuk@aalto.fi

Iván Blanco-Chacón
Dept. of Mathematics
and Systems Analysis
P.O. Box 11100
FI-00076 Aalto
Finland
Email: ivan.blancochacon@aalto.fi

Camilla Hollanti
Dept. of Mathematics
and Systems Analysis
P.O. Box 11100
FI-00076 Aalto
Finland
Email: camilla.hollanti@aalto.fi

***Abstract*—In this paper, we establish probability bounds for the correct decision of the eavesdropper over a MIMO Wiretap Channel, when coding using cyclic division algebras is used. We focus in particular on codebooks constructed from natural orders in Q-central quaternion algebras, which allows the resulting expressions to take a more explicit form.**

***Index Terms*—MIMO, wiretap channel, cyclic division algebras, zeta functions, lattices, unit group**

I. Introduction

Space-time codes based on cyclic division algebras are ubiquitous in wireless communications, particularly over Gaussian and fading channels; see [1] for an introduction. For example, one can easily build codebooks satisfying the non-vanishing determinant (NVD) property, and perform analysis of the code's performance based on algebraic invariants.

Analysis of space-time codes for SISO and MIMO Gaussian and fading wiretap channels naturally leads one to consider inverse norm and inverse determinant sums [2], [3], which provide an upper bound on the probability of the correct decision of the eavesdropper. In [4] and [5] Vehkalahti and Lu showed how the unit group and diversity-multiplexing gain trade-off (DMT) of division algebra-based space-time codes are linked to each other through inverse determinant sums, and also demonstrated the connection to zeta functions. As a continuation of [4], [5], the authors later showed that the growth of the inverse determinant sum depends on the density of the unit group, see [6], [7]. Exact evaluation of such sums is infeasible, thus one hopes to provide methods to estimate it and understand its asymptotic growth.

In this paper, we study inverse determinant sums for $\mathbf{Q}$-central quaternion algebras. In short, the main contributions of this paper lie in

- applying number theoretic techniques to study the inverse determinant sums appearing in [3], allowing for explicit analysis of $\mathbf{Q}$-central quaternion algebra codes used in MIMO wiretap channels,
- applying results on the density of integer solutions to quadratic forms found in [8], [9], and using techniques similar to those found in [7], to obtain an asymptotic growth formula for the unit group of the natural order in a quaternion algebra, and
- presenting experimental evidence demonstrating the accuracy of approximating the inverse determinant sum by the unit group.

We conclude by discussing an analogous approach for the Golden Code, and present experimental results in that direction. While estimates similar to our main propositions have already appeared in [7], the novelty in our approach to studying the growth of the inverse determinant sum is that it relies on recent results concerning the density of solutions to quadratic forms.

II. The MIMO Wiretap Channel Model

In [3], the proposed model for a MIMO wiretap channel is

$$Y = H_bX + V_b \qquad (1)$$
$$Z = H_eX + V_e \qquad (2)$$

where X, the transmitted codeword, is an $n_t \times T$ complex matrix, H_b is an $n_b \times n_t$ complex matrix, H_e is an $n_e \times n_t$ complex matrix, and V_b and V_e are the corresponding zero mean noise matrices for Bob and Eve, respectively. The entries of the channel matrix are complex Gaussian i.i.d. random variables. The matrix Y is the signal that Bob receives, while Z is the signal that Eve receives.

To confuse Eve, Alice employs a coset coding strategy. Coset coding was originally introduced by Wyner in [10], but the technique has been under study recently [2], [3], [11] in the context of algebraic codes for fading channels. The basic ingredients are a lattice Λ_b consisting of codewords intended for Bob, and a sublattice $\Lambda_e \subset \Lambda_b$ consisting of random bits intended to confuse Eve.

As we will only be concerned with Eve's lattice from this point on, we will write Λ for Λ_e. We build a codebook carved from Eve's lattice in the following way. We identify $M_{n_t\times T}(\mathbf{C}) = \mathbf{C}^{n_tT} = \mathbf{R}^{2n_tT}$ in the natural way, by vectorizing the matrices and identifying a complex number with the vector consisting of its real and imaginary parts. To construct a codebook, we consider a lattice $\Lambda \subset \mathbf{R}^{2n_tT}$, a norm $||\cdot||$ on $\mathbf{R}^{2n_tT}$, and a positive number $R > 0$, and define our codebook by

$$\{X \in \Lambda : ||X|| < R\}. \tag{3}$$

We will concentrate on the cases $||\cdot|| = ||\cdot||_2$ or $||\cdot||_\infty$, i.e. spherical or cubic shaping, respectively. Recall that $||\cdot||_2$ is the usual norm on Euclidean space, and $||x||_\infty = \max_i\{|x_i|\}$.

In the setup, the authors of [3] show that measuring the probability of Eve's correct decision requires that we study the *inverse determinant sum*

$$S_R(s) := \sum_{\substack{X\in\Lambda-\{\mathbf{0}\}\\ ||X||<R}} \frac{1}{\det(XX^*)^s} \tag{4}$$

where in $\det(XX^*)$ we consider the matrix XX^* before vectorization. Towards that end, we study inverse determinant sums arising from central division algebras of the form $(\mathbf{Q}(\sqrt{d})/\mathbf{Q}, \sigma, -1)$, i.e. quaternion algebras with center $\mathbf{Q}$. In particular, we restrict ourselves to the case of $n_t = T = 2$. Our goals are to provide lower and upper bounds for $S_R(s)$, and study its asymptotic behavior as $R \to \infty$.

III. Algebraic Background

As a blanket reference for the necessary mathematical background concerning quaternion algebras, we recommend [12], and for an overview of their applications to space-time coding (and a summary of the relevant notation concerning cyclic division algebras) see [1].

We recall two definitions concerning cyclic division algebras that will be of particular importance for this paper. If $a \in \mathcal{A} = (K/\mathbf{Q}, \sigma, \gamma)$ has matrix $\phi(a)$ via the left regular representation, we define the *reduced norm* of a to be

$$\mathrm{nrd}(a) = \det(\phi(a)). \tag{5}$$

One can easily check that if $\mathcal{O}$ is a $\mathbf{Z}$-order in $\mathcal{A}$, then $\mathrm{nrd}(a) \in \mathbf{Z}$ for any $a \in \mathcal{O}$. Furthermore, the reduced norm of any unit $a \in \mathcal{O}^\times$ is ± 1.

If $\mathfrak{a}$ is a left ideal of a $\mathbf{Z}$-order $\mathcal{O}$, we define its norm to be $N(\mathfrak{a}) := |\mathcal{O}/\mathfrak{a}|$. The two definitions of norm coincide for principal ideals, in the sense that if $\mathfrak{a} = (a)$, then

$$N(\mathfrak{a}) = |\mathrm{nrd}(a)|^2. \tag{6}$$

If $\mathcal{O}$ is a $\mathbf{Z}$-order in $\mathcal{A}$, its *zeta function* is defined to be

$$\zeta_{\mathcal{O}}(s) = \sum_{\mathfrak{a}\subseteq\mathcal{O}} \frac{1}{N(\mathfrak{a})^s} \tag{7}$$

where the sum ranges over all *left* ideals of $\mathcal{O}$. We similarly define the *partial zeta function* $\zeta^1_{\mathcal{O}}(s)$ by the same formula, but the sum is restricted to *principal* left ideals. Such partial zeta functions are well-understood for rings of integers of number fields; see [13].

Consider the left regular representation of a cyclic division algebra $\mathcal{A} = (K/\mathbf{Q}, \sigma, -1)$ where $K = \mathbf{Q}(\sqrt{d})$ is a real quadratic field with $\mathrm{Gal}(K/\mathbf{Q}) = \langle\sigma\rangle$. To guarantee $\mathcal{A}$ is a division algebra (i.e. satisfies the NVD property), we assume that $d \equiv 3 \bmod 4$. To produce codeword matrices from $\mathcal{A}$, we restrict the left regular representation to an order Λ of $\mathcal{A}$.

We consider the natural order

$$\mathcal{O} = \mathcal{O}_K \oplus e\mathcal{O}_K$$

of $\mathcal{A}$. Then for $a \in \mathcal{O}$, our codeword matrices take the form

$$\phi(a) := \begin{pmatrix} x_0 + x_1\sqrt{d} & y_0 + y_1\sqrt{d} \\ -y_0 + y_1\sqrt{d} & x_0 - x_1\sqrt{d} \end{pmatrix} \tag{8}$$

for $x_i, y_i \in \mathbf{Z}$, since $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$. Then

$$\mathrm{nrd}(a) = x_0^2 - dx_1^2 + y_0^2 - dy_1^2, \tag{9}$$

a diagonal quadratic form with discriminant d^2.

Now we identify the order $\mathcal{O}$ with the lattice Λ obtained by vectorizing the matrices obtained from its left regular representation. In other words, Λ is the collection of all

$$\psi(a) := \mathrm{vec}(\phi(a)) = \begin{pmatrix} x_0 + x_1\sqrt{d} \\ -y_0 + y_1\sqrt{d} \\ y_0 + y_1\sqrt{d} \\ x_0 - x_1\sqrt{d} \end{pmatrix} \tag{10}$$

and has generator matrix

$$M_e = \begin{pmatrix} 1 & \sqrt{d} & 0 & 0 \\ 0 & 0 & -1 & \sqrt{d} \\ 0 & 0 & 1 & \sqrt{d} \\ 1 & -\sqrt{d} & 0 & 0 \end{pmatrix}. \tag{11}$$

Note that $\det(M_e) = 4d$. From now on, we will drop $\mathcal{O}$ from our notation, and simply refer to the lattice Λ as the natural order. Thus, for example, $\Lambda^\times$ refers to the units of $\mathcal{O}$ considered as a subset of the lattice Λ, and $||a|| < R$ for an element a of the natural order really means $||\psi(a)|| < R$.

Lastly, we observe that one often constructs codebooks (e.g. the Golden Code [14]) not from Λ, but from a principal ideal of Λ. However, this has the effect of multiplying the inverse norm sum (the principal object of study, defined in the following section) by the norm of the principal ideal. Thus we may as well consider only Λ, as multiplication by a constant will not change our estimates or asymptotic growth formulas.

IV. Inverse Determinant Sums

For a positive number R, we consider the following constellations:

$$\begin{aligned} \mathcal{S}_R &:= \{a \in \Lambda : ||a||_2 \le R\} \quad \text{(spherical shaping)} \\ \mathcal{C}_R &:= \{a \in \Lambda : ||a||_\infty \le R\} \quad \text{(cubic shaping)} \end{aligned}$$

In other words, $\mathcal{C}_R$ is the set of all elements of Λ inside a hypercube of side length $2R$, and $\mathcal{S}_R$ is the set of all elements of Λ inside a sphere of radius R. When the result is independent of the shaping region, we simply write Λ_R.

By combining (6) and the equation $\det(XX^*) = |\det(X)|^2$, one can see that the design criterion outlined in [3] now demands that we consider the inverse determinant sum

$$S^{\mathrm{s}}_R(s) := \sum_{a\in\mathcal{S}_R} \frac{1}{|\mathrm{nrd}(a)|^{2s}}, \tag{12}$$

and similarly for $S_R^{\mathrm{c}}(s)$, defined in the obvious way. Here s corresponds to the number of receiver antennas n_e available to Eve. More precisely, by [3], we have

$$s = n_e + 2 \tag{13}$$

due to our assumption that $T = 2$. Again, we simply write $S_R(s)$ when we are unconcerned with the precise shaping region.

V. First Upper Bounds for $S_R(s)$

In this section, we establish some basic upper bounds for $S_R(s)$, for both $\Lambda_R = \mathcal{S}_R$ and $\mathcal{C}_R$, i.e. for both spherical and cubic shaping. While these bounds are very loose, they underscore the drastic difference in estimating the asymptotic behavior of the size of the constellation and the unit group.

Proposition 1: We have the following upper bounds:

$$S_R^{\mathrm{s}}(s) \leq \#\mathcal{S}_R = \frac{\pi^2}{8d}R^4 + O(R^3) \tag{14}$$

$$S_R^{\mathrm{c}}(s) \leq \#\mathcal{C}_R = \frac{4}{d}R^4 + O(R^3) \tag{15}$$

Proof: We recall that if $\mathcal{B}$ is a hypercube or a sphere, and L a full lattice in n-dimensional Euclidean space, then

$$\#(L \cap \mathcal{B}) = \frac{\mathrm{vol}(\mathcal{B})}{\mathrm{vol}(L)}R^n + O(R^{n-1}). \tag{16}$$

Our lattice has generator matrix M_e, and hence volume $\det(M_e) = 4d$. In the case of spherical shaping, $\mathcal{B}$ is a ball with radius R in $\mathbf{R}^4$, we have $\mathrm{vol}(\mathcal{B}) = \frac{1}{2}\pi^2 R^4$. In the case of cubic shaping, our hypercube has side length $2R$, thus $\mathrm{vol}(\mathcal{B}) = 16R^4$. Now note that $S_R(s) \leq \#(L \cap \mathcal{B})$, since the reduced norm of every non-zero element in an order is a non-zero integer. The results follow easily. ■

VI. Bounds on $S_R(s)$ from Units

The bounds in the previous section show that $S_R(s)$ grows at most quartically with respect to R. However, we now establish lower and upper bounds in terms of the group $\Lambda^\times$, which combined with the results of the next section, provide a better estimate for the asymptotic growth of $S_R(s)$.

First, we define

$$b_{k,R}^{\mathrm{s}} := \#\{a \in \mathcal{S}_R : |\mathrm{nrd}(a)| = k\} \tag{17}$$

so that $b_{1,R}^{\mathrm{s}}$ is the number of units u in the natural order such that $||\psi(u)||_2 \leq R$, and similarly for cubic constellations. Again, when we are unconcerned with the precise bounding region, we will write simply $b_{k,R}$.

Proposition 2: (see also Propositions 6.7 and 6.11 of [7]) We have the bounds

$$b_{1,R}^{\mathrm{s}} \leq S_R^{\mathrm{s}}(s) \leq Cb_{1,R}^{\mathrm{s}}\zeta_\Lambda^1(s), \tag{18}$$

$$b_{1,R}^{\mathrm{c}} \leq S_R^{\mathrm{c}}(s) \leq Cb_{1,2R}^{\mathrm{c}}\zeta_\Lambda^1(s). \tag{19}$$

for an absolute constant C.

Proof: For $a \in \Lambda$ we have that $\mathrm{nrd}(a) = \pm 1$ if and only if $a \in \Lambda^\times$. Therefore every unit of Λ with norm bounded above by R contributes 1 to $S_R(s)$, providing us with the lower bound $b_{1,R} \leq S_R(s)$.

Now we treat the cases of spherical and cubic shaping separately. Fix $a \in \mathcal{S}_R$. By Lemma 9.3 of [7], we have that

$$\#\{u \in \Lambda^\times : ||au||_2 \leq R\} \leq Cb_{1,R}^{\mathrm{s}} \tag{20}$$

for an absolute constant C. Grouping elements of absolute norm k by the principal ideal they generate, and noting that two elements generate the same ideal exactly when they differ (multiplicatively) by a unit, one sees that if a_k^1 is the number of left principal ideals of Λ of norm k, then $b_{k,R}^{\mathrm{s}} \leq Cb_{1,R}^{\mathrm{s}}a_k^1$. Hence

$$S_R^{\mathrm{s}}(s) = \sum_{k\geq 1}\frac{b_{k,R}^{\mathrm{s}}}{k^{2s}} \leq Cb_{1,R}^{\mathrm{s}}\sum_{k\geq 1}\frac{a_k^1}{k^{2s}} = Cb_{1,R}^{\mathrm{s}}\zeta_\Lambda^1(s). \tag{21}$$

For the case of cubic shaping, note that for $x \in \mathbf{R}^n$, we have that $||x||_2 \leq R \Rightarrow ||x||_\infty \leq R$, and that $||x||_\infty \leq R \Rightarrow ||x||_2 \leq n^{1/2}R$. Thus, again fixing $a \in \Lambda_R$, we have

$$\begin{aligned}
& \#\{u \in \Lambda^\times : ||au||_\infty \leq R\} && (22)\\
\leq\ & \#\{u \in \Lambda^\times : ||au||_2 \leq 2R\} && (23)\\
\leq\ & C \cdot \#\{u \in \Lambda^\times : ||u||_2 \leq 2R\} && (24)\\
\leq\ & C \cdot \#\{u \in \Lambda^\times : ||u||_\infty \leq 2R\} && (25)\\
=\ & Cb_{1,2R}^{\mathrm{c}} && (26)
\end{aligned}$$

and the same argument as in the previous paragraph completes the proof. ■

While the above bounds reduce our task, in large part, to computing $b_{1,R}$, this is still a difficult problem.

VII. Asymptotic Growth of $b_{1,R}$ and $S_R(s)$

Here we present results on the asymptotic behavior of $b_{1,R}$ as $R \to \infty$, for natural orders of cyclic division algebras of the form $(\mathbf{Q}(\sqrt{d})/\mathbf{Q}, \sigma, -1)$. We remark that while these results apply directly only to these specific orders, the theoretical tools can likely be generalized to natural orders of arbitrary cyclic division algebras over number fields.

Proposition 3: We have

$$b_{1,R} = O(R^2\log(R)) \tag{27}$$

and therefore

$$S_R(s) = O(R^2\log(R)) \tag{28}$$

as well, as $R \to \infty$, for both spherical and cubic constellations.

Proof: Note that it suffices to prove the result for cubic constellations. To see this, observe that a solid ball of radius R is a subset of a solid cube of side length $2R$, and thus $b_{1,R}^{\mathrm{s}} \leq b_{1,R}^{\mathrm{c}}$. Thus we may restrict our attention to cubic constellations. Let $a \in \Lambda^\times$, with

$$\psi(a) = \begin{pmatrix} x_0 + x_1\sqrt{d} & y_0 + y_1\sqrt{d} \\ -y_0 + y_1\sqrt{d} & x_0 - x_1\sqrt{d} \end{pmatrix} \tag{29}$$

where $x_i, y_i \in \mathbf{Z}$. The condition $||\psi(a)||_\infty \leq R$ implies easily that $|x_i|, |y_i| \leq R$. We must now estimate the number of solutions to the quadratic forms

$$\mathrm{nrd}(a) = x_0^2 + y_0^2 - d(x_1^2 + y_1^2) = \pm 1 \tag{30}$$

under the constraint $|x_i|, |y_i| \leq R$.

Let us write $b^{c+}_{1,R}$ for the quantity

$$\#\{(z_i) \in \mathbf{Z}^4 : z_0^2 + z_1^2 - d(z_2^2 + z_3^2) = \pm 1, |z_i| \leq R\} \quad (31)$$

so that $b^{c}_{1,R} \leq b^{c+}_{1,R}$. Theorem 7 of [9], on the density of solutions to diagonal quadratic forms in four variables (summarized in the introduction of [8]), implies that

$$b^{c+}_{1,R} = O(R^2 \log(R)) \quad (32)$$

as $R \to \infty$, which completes the proof. ■

Remark 1: The authors would like to thank R. Vehkalahti for pointing out that by combining Lemma 6.16, Theorem A.1, Theorem 8.1, and Theorem 8.2 of [7], one can actually prove that $b_{1,R} = O(R^2)$. However, we present the above approach to highlight the utility and novelty of using the quadratic form attached to the reduced norm of the quaternion algebra to estimate the growth of the units.

VIII. Experimental Results

Here we present experimental results for cubic constellations. As a measure of the accuracy of our approximation, let us define the relative error by

$$e^{c}_{R}(s) := 100 * |S^{c}_{R}(s) - b_{1,R}|/S^{c}_{R}(s). \quad (33)$$

The results presented below are intended to measure the accuracy of approximating $S^{c}_{R}(s)$ by $b^{c}_{1,R}$, for the algebras $\mathcal{A} := (\mathbf{Q}(\sqrt{d})/\mathbf{Q}, \sigma, -1)$, $d = 3, 7$. The case $s = 3$ corresponds to the situation where Eve has 1 receiver antenna, and the case $s = 4$ to the case of 2 receiver antennas. We have rounded $S_R(s)$ to the nearest integer for the sake of presentation.

For the algebra $\mathcal{A} := (\mathbf{Q}(\sqrt{3})/\mathbf{Q}, \sigma, -1)$:

R	$b^{c}_{1,R}$		$S^{c}_{R}(3)$	$e^{c}_{R}(3)$		$S^{c}_{R}(4)$	$e^{c}_{R}(4)$
10	300		308	2.5659		302	0.6428
20	1284		1316	2.4025		1292	0.6002
30	3132		3202	2.1872		3149	0.5452
40	5116		5242	2.4106		5147	0.6018
50	8220		8419	2.3594		8269	0.5888
60	11636		11918	2.3674		11705	0.5908
70	15652		16033	2.3734		15745	0.5922
80	21012		21516	2.3416		21135	0.5840
90	26340		26975	2.3532		26496	0.5872

For the algebra $\mathcal{A} := (\mathbf{Q}(\sqrt{7})/\mathbf{Q}, \sigma, -1)$:

R	$b^{c}_{1,R}$		$S^{c}_{R}(3)$	$e^{c}_{R}(3)$		$S^{c}_{R}(4)$	$e^{c}_{R}(4)$
10	124		126	1.819		125	0.4337
20	388		400	2.9023		391	0.7118
30	996		1021	2.4144		1002	0.5843
40	1764		1809	2.4997		1775	0.6047
50	2772		2846	2.6154		2790	0.6354
60	4084		4182	2.3381		4107	0.5643
70	5348		5477	2.3568		5379	0.5693
80	7108		7280	2.3685		7149	0.5739
90	8916		9142	2.4760		8970	0.6003

One can see from experiment that $b_{1,R}$ provides a good estimate of $S_R(s)$, in the sense that the relative error is quite small. This underscores the necessity of understanding the asymptotic growth of the unit group.

IX. The Golden Code

Many of the same theoretical tools presented here also allow one to analyze lattice codes coming from orders over division algebras of the form $(K/\mathbf{Q}(i), \sigma, \gamma)$, where $K/\mathbf{Q}(i)$ is a quadratic extension with Galois group generated by σ, and γ is not a norm from K. For example, the Golden Code is built from (an ideal of) the natural order of the algebra $\mathcal{A} = (\mathbf{Q}(\sqrt{5}, i)/\mathbf{Q}(i), \sigma, i)$.

If $\mathcal{O}_K = \mathbf{Z}[i, \omega]$, and we consider the left regular representation of the natural order, then codeword matrices take the form

$$\begin{pmatrix} x_0 + x_1\omega & y_0 + y_1\omega \\ i(y_0 + y_1\sigma(\omega)) & x_0 + x_1\sigma(\omega) \end{pmatrix} \quad (34)$$

for $x_i, y_i \in \mathbf{Z}[i]$. We carve spherical and cubic constellations by identify $\mathbf{C}^4$ with $\mathbf{R}^8$ in the natural way, and bounding the coordinates as before.

Proposition 4: We have the bounds

$$b^{s}_{1,R} \leq S^{s}_{R} \leq C b^{s}_{1,R} \zeta^{1}_{\Lambda}(s), \quad (35)$$

$$b^{c}_{1,R} \leq S^{c}_{R} \leq C b^{c}_{1,2\sqrt{2}R} \zeta^{1}_{\Lambda}(s) \quad (36)$$

for an absolute constant C.

Proof: This is the same proof as for Proposition 2, again using the results of [7]. ■

To give some idea of how the accuracy of the proposed bounds changes with the dimension of the underlying lattice, we present experimental results for the natural order of the cyclic division algebra $\mathcal{A} := (\mathbf{Q}(\sqrt{5}, i)/\mathbf{Q}(i), \sigma, i)$, from which the Golden Code is built.

R	$b^{c}_{1,R}$		$S^{c}_{R}(3)$	$e^{c}_{R}(3)$		$S^{c}_{R}(4)$	$e^{c}_{R}(4)$
1	24		26	8.3207		25	4.1441
2	392		452	13.2367		420	6.5912
3	1464		1751	16.3804		1595	8.2193
4	3896		4860	19.8421		4335	10.1249
5	10216		12648	19.2306		11321	9.7606
6	21864		26891	18.6950		24134	9.4051
7	38792		47808	18.8582		42859	9.4890
8	65384		80201	18.4753		72050	9.2516
9	105832		129422	18.2274		116449	9.1174

It is clear from this experiment that approximating the inverse determinant sum by the size of the unit group leads is less accurate, for the higher-dimensional lattice associated with the Golden Code. Again, we point out that it is possible to deduce from the theorems of [7] that $b_{1,R} = O(R^4)$ for the Golden Code algebra.

X. Conclusions and Future Work

We have provided lower and upper bounds on the value of the inverse determinant sum associated with a $\mathbf{Q}$-central quaternion algebra. Experimental evidence shows that approximating the inverse determinant sum by the unit group provides a good estimate. Hence we have also provided a precise statement regarding the asymptotic growth of the unit group of the natural order.

One can see from experiment that our approximations are worse for the higher-dimensional Golden Code, which exhibits the need for tighter lower and upper bounds on $S_R(s)$. This will require a more detailed approximation of the number of units of the order inside the bounding region, and an explicit expression for the constant C appearing in the bound $S_R^{\mathrm{c}}(s) \leq Cb_{1,R}^{\mathrm{c}}\zeta_\Lambda^1(s)$.

Measuring the asymptotic growth of the units of orders in $\mathbf{Q}(i)$-central quaternion algebras, as we did for $\mathbf{Q}$-central quaternion algebras, would depend on understanding the density of the solutions to the quadratic forms

$$\mathrm{nrd}(a) = x_0^2 + x_0x_1 - x_1^2 - i(y_0^2 + y_0y_1 - y_1^2) = \pm 1, \pm i \quad (37)$$

where the variables take values in $\mathbf{Z}[i]$. As far as the authors are aware, theoretical results on the density of such solutions are not in the literature. However, such questions are an active area of research in Number Theory.

Acknowledgement

The authors would like to acknowledge funding from the Academy of Finland grant #131745, which partially supported this research. The first author would also like to thank the Max-Planck-Institut für Mathematik, Bonn, Germany, where part of this research was completed, for its hospitality.

References

[1] Frédérique E. Oggier, Jean-Claude Belfiore, and Emanuele Viterbo, “Cyclic division algebras: A tool for space-time coding”, *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 1, pp. 1–95, 2007.

[2] J.-C. Belfiore and F. Oggier, “Lattice code design for the rayleigh fading wiretap channel”, in *ICC 2011*, `arxiv.org/pdf/1012.4161`.

[3] J.-C. Belfiore and F. Oggier, “An error probability approach to MIMO wiretap channels”, January 2013, `http://arxiv.org/abs/1109.6437`.

[4] H.-F. Lu, J. Lahtonen, R. Vehkalahti, and C. Hollanti, “Remarks on the criteria of constructing MAC-DMT optimal codes”, in *Proc. ITW 2010, Cairo, Egypt*, 2010.

[5] R. Vehkalahti and H.-F. (F.) Lu, “Diversity-multiplexing gain tradeoff: a tool in algebra?”, in *IEEE ITW*, 2011.

[6] R. Vehkalahti and L. Luzzi, “Connecting dmt of division algebra space-time codes and point counting in lie groups”, in *Proc. IEEE ISIT 2011*, 2012.

[7] R. Vehkalahti, H.-F. (F.) Lu, and L. Luzzi, “Inverse determinant sums and connections between fading channel information theory and algebra”, December 2012, `http://arxiv.org/abs/1111.6289`.

[8] T.D. Browning, “Density of integer solutions to diagonal quadratic forms”, *Monatschefte für Mathematik*, vol. 152, pp. 13–38, September 2007.

[9] D.R. Heath-Brown, “A new form of the circle method, and its application to quadratic forms.”, *Journal fr die reine und angewandte Mathematik*, vol. 481, pp. 149–206, 1996.

[10] A. Wyner, “The wire-tap channel”, *Bell. Syst. Tech. Journal*, vol. 54, 1975.

[11] C. Hollanti, E. Viterbo, and D. Karpuk, “Nonasymptotic Probability Bounds for Fading Channels Exploiting Dedekind Zeta Functions”, September 2012, submitted, available at `http://arxiv.org/abs/1303.3475`.

[12] M. Alsina and P. Bayer, *Quaternion Orders, Quadratic Forms, and Shimura Curves*, American Mathematical Society, 2004.

[13] S. Lang, *Algebraic number theory*, Springer-Verlag New York Inc., 1986.

[14] J.-C. Belfiore, G. Rekaya, and E.Viterbo, “The Golden code: a 2×2 full-rate space-time code with non-vanishing determinants”, in *Proc. 2004 IEEE Int. Symp. Inform. Theory*, Chicago, IL, June 27-July 2 2004, p. 308.