A Noncommutative Analogue of the Odlyzko Bounds and Bounds on Performance for Space-Time Lattice Codes

Benjamin Linowitz, Matthew Satriano, and Roope Vehkalahti

***Abstract*— This paper considers space-time coding over several independently Rayleigh faded blocks. In particular, we will concentrate on giving upper bounds for the coding gain of lattice space-time codes as the number of blocks grow. This problem was previously considered in the single antenna case by Bayer-Fluckiger *et al.* in 2006. Crucial to their work was Odlyzko's bound on the discriminant of an algebraic number field, as this provides an upper bound for the normalized coding gain of number field codes. In the MIMO context natural codes are constructed from division algebras defined over number fields and the coding gain is measured by the discriminant of the corresponding (noncommutative) algebra. In this paper, we will develop analogues of the Odlyzko bounds in this context and show how these bounds limit the normalized coding gain of a very general family of division algebra based space-time codes. These bounds can also be used as benchmarks in practical code design and as tools to analyze asymptotic bounds of performance as the number of independently faded blocks increases.**

***Index Terms*— Space-time codes, algebra, MIMO, fading.**

I. Introduction

CONSIDER a lattice $L \subset \mathbb{C}^n$ having fundamental parallelotope of volume one and define a function $f_1 : \mathbb{C}^n \to \mathbb{R}$ by

$$f_1(x_1, \ldots, x_n) = |x_1|^2 + |x_2|^2 + \cdots + |x_n|^2. \tag{1}$$

The real number $h(L) = \inf_{x \in L,\, x \neq \mathbf{0}} f_1(x)$ is the *Hermite invariant* of the lattice L. In rough terms we may say that the greater the Hermite invariant of a lattice is, the higher the guaranteed protection against worst case pairwise error when a subset of the lattice is used as a code in the Gaussian or slow fading channel. Similarly, if we have a Rayleigh fast fading single antenna channel, the role of the function f_1 is played by the function

$$f_2(x_1, x_2, \ldots, x_n) = |x_1 x_2 \cdots x_n|. \tag{2}$$

Assuming that it is not zero, the real number $Nd_{p,min}(L) = \inf_{x \in L, x \neq \mathbf{0}} f_2(x)$ is the *normalized product distance* of the lattice L and can be used to identify the best lattice code for the fast fading channel on high signal-to-noise ratio (SNR) regime.

Let us now consider the main topic of this paper. Suppose that we have n transmit antennas and a *Rayleigh block fading channel* where the fading stays stable for n units of time and then changes independently for the next n units of time. The ability to encode and decode over m such independently faded blocks implies that our lattice code L lies in the space $M_{n \times mn}(\mathbb{C})$. Let us suppose that $(X_1, X_2, \ldots, X_m)$ is an element of $M_{n \times mn}(\mathbb{C})$, and define

$$f_3(X_1, X_2, \ldots, X_m) = \prod_{i=1}^{m} |det(X_i)|. \tag{3}$$

In analogy with the functions defined above, we can define the *normalized minimum determinant* of the lattice L by $\delta(L) = \inf_{X \in L, X \neq \mathbf{0}} |f_3(X)|$. Again, the number $\delta(L)$ can be seen as measuring the quality of the lattice L.

The following problems are natural to consider in all three cases.

1 Given the channel, find optimal lattices that maximize the corresponding function f_i.
2 Given a lattice, find upper and lower bounds for the maximal value obtained by the function f_i.

From a mathematical standpoint these problems can be seen as arising in the classical *geometry of numbers*, though good solutions for the problems in full generality do not appear to be in the literature.

The case in which one considers the function f_1, defined in (1), and the associated Hermite invariant, is known as the sphere packing problem. In this setting there exist a number of good constructions and general bounds.

In the case of the function f_2, defined in (2), and the associated real number $Nd_{p,min}(L)$, most of the known constructions are based on algebraic number fields and good general bounds are known only in the case where the lattice L is real [22, p. 615].

Manuscript received August 20, 2014; accepted February 5, 2015. Date of publication February 24, 2015; date of current version March 13, 2015. B. Linowitz was supported in part by the NSF RTG under Grant DMS-1045119 and in part by the NSF through the Mathematical Sciences Post-Doctoral Fellowship. M. Satriano was supported by the NSF through the Mathematical Sciences Post-Doctoral Fellowship. R. Vehkalahti was supported in part by the Suomen Akatemia through the Academy of Finland under Grant 252457 and in part by the Finnish Cultural Foundation.

B. Linowitz is with the Department of Mathematics, University of Michigan, Ann Arbor, MI 48109 USA (e-mail: linowitz@umich.edu).

M. Satriano is with the Division of Biostatistics and Bioinformatics, Sidney Kimmel Comprehensive Cancer Center, Department of Oncology, Johns Hopkins University School of Medicine, Baltimore, MD 21205 USA (e-mail: msatria2@jhu.edu).

R. Vehkalahti is with the Department of Mathematics and Statistics, University of Turku, Turku 20014, Finland (e-mail: roiive@utu.fi).

Communicated by B. S. Rajan, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2015.2406698

For the function f_3 defined in (3) and the associated real number $\delta(L)$, to the best of our knowledge there are no good general bounds.

For a general lattice $L \subset M_{n\times mn}(\mathbb{C})$ finding good bounds for $\delta(L)$ is an extremely difficult task. For this reason we restrict our attention to a broad class of lattices arising from central division algebras defined over number fields. For the lattices arising from this construction we can say a great deal more about $\delta(L)$.

In order to describe our results on $\delta(L)$, let us first briefly describe the general construction principle behind these algebraic lattices. There are many ways to construct lattice codes with good Hermite invariant. To build a lattice code with good product distance or minimum determinant, the task is more difficult. A usual method is to choose a central simple algebra or number field $\mathcal{A}$, a suitable subset $\Lambda \subset \mathcal{A}$ and then a faithful representation ψ which maps every element of $\mathcal{A}$ to a suitable matrix space $M_{m\times mn}(\mathbb{C})$. If the mapping ψ, the subset Λ, and the algebra $\mathcal{A}$ are well chosen then the set $\psi(\Lambda)$ will be a lattice in $M_{n\times mn}(\mathbb{C})$ and will have a good minimum determinant. This type of construction offers a rich selection of lattice codes. Assuming that this algebraic construction yields a k-dimensional lattice in the given matrix space $M_{n\times mn}(\mathbb{C})$, it is natural to ask for bounds on the size of the minimum determinant.

This problem was first considered in the context of number field codes in a fast fading SISO channel in [7] by using the Odlyzko bounds [13], and in [21] by using sphere packing bounds. In [19], [18], and [30] the problem was considered in the case in which $m = 1$ and $n \geq 1$. In [9] the authors concentrated on the case where $n = m = 2$.

In this work we will generalize and unify previous number field and division algebra constructions and relate the normalized minimum determinant to the *discriminant* of the corresponding algebra. We will then give completely general lower bounds for the discriminant of any division algebra and derive upper bounds for the minimum determinants of the corresponding lattices. The discriminant bounds given in this paper are a generalization of the Odlyzko bounds in number fields and are of independent interest.

We will begin by defining the channel model, lattice codes and finite codes associated to a lattice. We will then describe the suitability of the normalized minimum determinant as a design criterion in one shot MIMO channels and make some remarks on the limits of this criterion. In Section I-D we show how this criterion can be extended to the multi-block channel. In Section II we briefly review the known construction methods of lattice codes from division algebras. We then extend these methods so as to obtain a lattice code for a multiblock channel from any order in a central division algebra. The presented explicit methods follow [5], [8], and unify [4], [9]. The construction method given in Proposition 4 generalizes the previously used methods by allowing us to consider a larger array of centers.

Section VI contains the main results of our paper. In construction Sections II and III we did prove that in most cases the normalized minimum determinant of a division algebra code depends only on the discriminant of the algebra. Unlike the case of number fields however, the mathematical literature does not offer ready-to-use bounds for the discriminant of a central division algebra defined over a number field. The discriminant bounds in [30] do solve this problem, but only after the center is fixed. However, in the general case, where we are allowed to optimize our code over all number fields with a fixed degree (or even signature), these results do not apply. The problem is that the $\mathbb{Z}$-discriminant of a central division algebra $\mathcal{A}$ defined over a number field K is a product of terms depending on the discriminant of the center $d(\mathcal{O}_K/\mathbb{Z})$ and the K-discriminant $d(\Lambda/\mathcal{O}_K)$ of the algebra $\mathcal{A}$ and minimizing one term might implicitly make the other term bigger. This problem was first considered in [9], where the authors were able to solve the problem for division algebras of degree 2 over totally complex fields of degree 4.

In Section VI we will give completely general lower bounds which make no assumptions on the degree (or even signature) of the center or division algebra. The proofs of these results combine the bounds in [30] with an analysis of the proof of the original Odlyzko bounds for number fields. As described in [30], the discriminant $d(\Lambda/\mathcal{O}_K)$ depends only on the two prime ideals of $\mathcal{O}_K$ of smallest norm. In order to find lower bounds we make crucial use of the fact that the original proof of Odlyzko (and certainly its refinement due to Poitou [29]) describes the impact on $d(\mathcal{O}_K/Z)$ of the assumption that the field K has prime ideals with small norm. The proofs of our theorems are a result of balancing the effect of small primes on $d(\Lambda/\mathcal{O}_K)$ against their effect on making the field discriminant $d(\mathcal{O}_K/\mathbb{Z})$ bigger. The bounds we develop therefore form a non-commutative analogue of the Odlyzko bounds in algebraic number theory.

While Section VI is strongly mathematical, Section VII returns to the coding theoretic context. We first derive some easy-to-use corollaries of our main theorems and then show how it is possible to find algebras that are optimal for our bounds. We then show how these discriminant bounds can be used so as to deduce minimum determinant bounds. Finally, we compare the resulting bounds to the minimum determinants of some example codes.

As in the case of the traditional Odlyzko bounds, our non-commutative bounds seem to be very tight. Therefore the bounds can be used as a benchmark in code design and provide understanding of the asymptotic behavior of the worst case pairwise error probability. The weakness of our approach lies in the fact that while minimum determinant criteria (in one form or another) has been applied in a number of space-time coding papers it only considers pairwise error and not the actual error probability. We will discuss this issue in Section II and suggest a remedy to this problem.

A. Channel Model

In this paper we are considering the so called multiblock Rayleigh faded channel with minimal delay. In such a channel a codeword $X \in M_{n\times nm}(\mathbb{C})$ has the form $(X_1, X_2, \ldots, X_m)$, where $X_i \in M_n(\mathbb{C})$. The channel equation, for transmitting i'th block X_i, then has the form

$$Y_i = H_i X_i + N_i, \tag{4}$$

where $H_i \in M_{n_r \times n}(\mathbb{C})$ is the channel matrix and $N_i \in M_{n_r \times T}(\mathbb{C})$ is the noise; n_r denotes the number of receiving antennas. Here we assume that each of H_i are independently Rayleigh faded and the decoding is done after the receiver has received all m blocks. We will call such a channel an (n, n_r, m)-multiblock channel. We note that when $m = 1$ this is the usual one shot MIMO channel and when $n = 1$ we are dealing with the fast fading single antenna channel. Throughout the paper we assume that receiver has perfect channel state information.

A code C in a (n, n_r, m)-channel is a set of matrices in $M_{n \times nm}(\mathbb{C})$. This paper will discuss code design and performance limits of codes in this channel. In particular we will concentrate on finite codes that are drawn from lattices and we assume that the receiver has perfect channel state information.

B. Lattices and Spherical Shaping

Definition 1: A *matrix lattice* $L \subseteq M_{n \times T}(\mathbb{C})$ has the form

$$L = \mathbb{Z}B_1 \oplus \mathbb{Z}B_2 \oplus \cdots \oplus \mathbb{Z}B_k,$$

where the matrices $B_1, \ldots, B_k$ are linearly independent over $\mathbb{R}$, i.e., form a lattice basis, and k is called the *rank* or the *dimension* of the lattice.

The space $M_{n \times T}(\mathbb{C})$ is a $2nT$-dimensional real vector space with a real inner product

$$\langle X, Y \rangle = \Re(Tr(XY^{\dagger})),$$

where Tr is the matrix trace. This inner product also naturally defines a metric on the space $M_{n \times T}(\mathbb{C})$ by setting $||X|| = \sqrt{\langle X, X \rangle}$.

We now consider a spherical shaping scheme based on a k-dimensional lattice L inside $M_{n \times T}(\mathbb{C})$. Given a positive real number R we define

$$L(R) = \{X \in L : ||X|| \leq R, X \neq \mathbf{0}\}.$$

These codes $L(R)$ will be the finite codes we are considering.

C. Design Criterion for One Shot MIMO

Before presenting a design criterion for the multiblock channel we describe the minimum determinant criterion used in the usual MIMO Rayleigh fading channel. The concept of *normalized minimum determinant* we are going to define has appeared implicitly or in restricted forms in several papers in space-time coding. Early attempts to define it in generality were given in [23] and [24], but only in [11] was the normalized minimum determinant defined formally and in a manner completely analogous to the definition of the Hermite invariant. Despite various papers where it has been used as a code design criterion, the needed energy normalizations still seem to cause confusion. We will therefore try to give an improved explanation of the concept here.

Let us suppose that L is a k-dimensional lattice in $M_{n \times T}(\mathbb{C})$ and that we consider a finite code $L(R)$. Let θ be a positive constant with the property that

$$\frac{1}{|L(R)|} \sum_{X \in L(R)} ||\theta X||^2 = T.$$

Let us now consider transmission of codewords from $L(R)$ in the Rayleigh fading MIMO channel with $n = n_t$ transmit antennas and n_r receive antennas. The channel is assumed to be fixed for a block of T channel uses, but to vary in an independent and identically distributed (i.i.d.) fashion from one block to another. Thus, the channel input-output relation can be written as

$$Y = \sqrt{\rho} H \theta X + N, \tag{5}$$

where $H \in M_{n_r \times n}(\mathbb{C})$ is the channel matrix and $N \in M_{n_r \times T}(\mathbb{C})$ is the noise matrix. The entries of H and N are assumed to be i.i.d. zero-mean complex circular symmetric Gaussian random variables with variance 1. The matrix $X \in L(R)$ is the transmitted codeword, and the term ρ denotes the signal-to-noise ratio (SNR). It is assumed that the receiver has perfect channel state information.

Following [10], we can bound the pairwise error probability between two codewords $X \neq X' \in L(R)$ by above when transmitting with SNR ρ:

$$P(\rho, X \to X') \leq \frac{1}{(\det(I + \frac{\rho\theta^2}{4n}(X - X')(X - X')^*))^{n_r}}, \tag{6}$$

where $*$ denotes complex conjugate transpose.

Combining this expression with the union bound we can now deduce an upper bound for the average error probability when transmitting a codeword from $L(R)$ at SNR ρ:

$$P_e(\rho) \leq \sum_{\substack{X \in L, \\ 0 < ||X|| \leq 2R}} \frac{1}{(\det(I + \frac{\rho\theta^2}{4n} XX^*))^{n_r}}.$$

If we suppose that ρ is particularly large and the matrices X are invertible then we obtain the further bound

$$P_e(\rho) \leq \sum_{\substack{X \in L, \\ 0 < ||X|| \leq 2R}} \frac{1}{(\det(\frac{\rho\theta^2}{4n} XX^*))^{n_r}}. \tag{7}$$

In what follows, the matrices in our lattices will not only be invertible but have an even stronger property.

Definition 2: If the *minimum determinant* of the lattice $L \subseteq M_{n \times T}(\mathbb{C})$ is non-zero, i.e. satisfies

$$\det_{min}(L) := \inf_{\mathbf{0} \neq X \in L} \sqrt{|\det(XX^*)|} > 0,$$

we say that the lattice satisfies the *non-vanishing determinant* (NVD) property.

Assuming now that $\det_{min}(L) = c > 0$, we can further improve our inequality (7) with

$$P_e(\rho) \leq \sum_{\substack{X \in L, \\ 0 < ||X|| \leq 2R}} \frac{(4n)^{nn_r}}{c^{2n_r} \theta^{2nn_r} \rho^{nn_r}}. \tag{8}$$

This bound suggests that minimum determinant plays a crucial role in the code design. However, in order to compare two k-dimensional lattices L_1 and L_2, the comparison based on the minimum determinant is relevant only if both the needed constants θ_1, θ_2 and the number of codewords in $L_1(R)$ and $L_2(R)$ are close to one another. Therefore we need a normalization that guarantees a fair comparison.

Let us now suppose we have a k dimensional lattice $L \subset M_{n\times T}(\mathbb{C})$. The *Gram matrix* of the lattice L is defined as

$$G(L) = \left(\langle X_i, X_j\rangle\right)_{1\le i,j\le k},$$

where $\{X_i\}$ is a basis of L. The volume of the fundamental parallelotope of L is then defined as $vol(L) = \sqrt{|det(G(L))|}$.

The following lemma proves that if we have two k-dimensional lattices L_1 and L_2 in the same space $M_{n\times T}(\mathbb{C})$, then the scaling factors θ_1 and θ_2 needed for normalization are roughly the same and the finite codes $L_1(R)$ and $L_2(R)$ have roughly the same number of codewords.

Although both of the assertions in the following lemma are well known, we give a complete proof of the second as it seems to have caused some confusion within the space-time community.

Lemma 1: Let L be a k-dimensional lattice with a unit fundamental parallelotope in $M_{n\times T}(\mathbb{C})$ and $L(R)$ be defined as above. Then $|L(R)| = c_1R^k + O(R^{k-1})$ and

$$\sum_{X\in L(R)} ||X||^2 = c_2R^{k+2} + O(R^{k+1}),$$

where c_i are constants independent of R and the lattice L, and O is Landau's big O.

Proof: The first claim is well known. Let us denote the Voronoi cell of a point $x \in L$ by V_x, and let r be a real number such that for any $x \in L$ and for any $y \in V_x$ we have $||x - y|| < r$. We then have that for any $x \in L$ and for any $y \in V_x$,

$$||x||^2 - 2r||x|| - r^2 \le ||y||^2 \le ||x||^2 + 2r||x|| + r^2.$$

We can therefore write

$$\sum_{x\in L(R-r)} (||x||^2 - 2r||x|| - r^2)vol(V_x) \le \int_{B(R)} ||x||^2dx \le \sum_{x\in L(R+r)} (||x||^2 + 2r||x|| + r^2)vol(V_x),$$

where $B(R)$ is a closed ball of radius R about the origin and integral is done in the space $\mathbb{R}(L)$. As we have assumed that $vol(L) = 1$, we have that $vol(V_x) = 1$ for all x and

$$\sum_{x\in L(R-r)} ||x||^2 - \sum_{x\in L(R-r)} (2r||x|| + r^2) \le \int_{B(R)} ||x||^2dx \le \sum_{x\in L(R+r)} ||x||^2 + \sum_{x\in L(R+r)} (2r||x|| + r^2). \quad (9)$$

The integral in the middle grows like $cR^{k+2} + O(R^{k+1})$ and according to the first statement the sum $\sum_{x\in L(R)} 2r||x||+r^2$ is bounded above by CR^{k+1} for some C independent of R. Using again the first statement we have that $\sum_{x\in L(R)} ||x||^2 - \sum_{x\in L(R-r)} ||x||^2 \in O(R^{k+1})$ and $\sum_{x\in L(R+r)} ||x||^2 - \sum_{x\in L(R)} ||x||^2 \in O(R^{k+1})$. Taking all these into account and reorganizing (9) we get the claim. ■

We can now define the *normalized minimum determinant* $\delta(L)$, which is obtained by first scaling the lattice L to have a unit size fundamental parallelotope and then taking the minimum determinant of the resulting scaled lattice. A simple computation proves the following.

Lemma 2: Let L be a k-dimensional matrix lattice in $M_{n\times T}(\mathbb{C})$. We then have that

$$\delta(L) = \det_{min}(L)/(vol(L))^{n/k}.$$

Remark 1: Different forms of minimum determinant criteria have been used in numerous papers on space-time coding. While a crude tool, the concept has been quite effective in code design. However, the derivation of the minimum determinant criterion through the union bound as in Lemma 1 makes it clear that the *distribution* of the determinants in the lattice, and not just the minimum determinant, is quite relevant. This is particularly clear when the SNR compared to the code size is relatively small. This was already known in the very early work on number field codes [16], though the technical obstacles needed to analyze the question did not allow researchers at the time to attack this problem.

In the context of algebraic codes this problem was addressed in [25], where the distribution of determinants of number field and division algebra codes was analyzed. This work revealed that division algebra based codes can be divided into different classes with respect to their *signature* (defined below in Definition 9). However, as pointed out in [28], the normalized minimum determinant still plays a major role and is effective when we compare codes having the same signature. The bounds we will develop in this paper are sensitive to the signatures of the considered algebras, and can therefore be used to analyze the behavior of minimum determinants within the class of algebras having the same signature. We can conclude that while minimum determinant criteria are not a perfect measure of space-time codes, the bounds presented here will also be relevant to more refined analyses.

Remark 2: We also point out the recent work [14], which appeared after finishing this work. In this paper it is proved that the normalized minimum determinant has far more important role in the performance of lattice space-time codes than was believed earlier. It seem to play almost exactly analogous role to the Hermite invariant, which has had a crucial role in the design of lattice codes for the Gaussian single antenna channel.

D. Design Criterion for Multiblock Channel

Let us now show how the design criterion of the previous section can be used to define a design criterion for the multiblock channel. Let us suppose we have a multiblock code $L \subset M_{n\times mn}(\mathbb{C})$ and that $(X_1, X_2, \dots X_m)$ is a codeword in L. The channel equation

$$(H_1X_1, H_2X_2, \dots, H_mX_m) + (N_1, N_2, \dots, N_m),$$

can just as well be written in the form

$$(H_1, \dots, H_m)\text{diag}(X_1, \dots, X_m) + \text{diag}(N_1, \dots, N_m),$$

where the diag-operator places the ith $n \times n$ entry in the ith diagonal block of a matrix in $M_{mn}(\mathbb{C})$. This reveals that optimizing a code L for the (n, n_r, m)-multiblock channel is equivalent to optimizing $\text{diag}(L)$ for the usual one shot $nm \times mn_r$ MIMO channel, where $\text{diag}(L)$ is defined as $\{\text{diag}(X) \mid X \in L\}$.

Let us now suppose we have an (n, n_r, m)-multiblock code L.

Definition 3: By abusing notation we define the normalized minimum determinant for the code L by

$$\delta(L) := \delta(\mathrm{diag}(L)).$$

We are now interested in the extrema of the normalized minimum determinants of k-dimensional (n, n_r, m)-multiblock codes.

II. Algebraic Preliminaries and Lattice Codes for One Shot MIMO

Let us now describe how lattice codes from division algebras are typically built. We will follow the standard presentation (see [3], [15]), but with an order-theoretic perspective [20]. The general idea is to show how we can transform an abstract algebraic structure into a concrete lattice of matrices. This construction will form a basis for our construction of multiblock codes. We refer the reader to [15] for all proofs.

Definition 4: Let K be an algebraic number field of degree m and assume that E/K is a cyclic Galois extension of degree n with Galois group $Gal(E/K) = \langle \sigma \rangle$. We can define an associative K-algebra

$$\mathcal{A} = (E/K, \sigma, \gamma) = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

where $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in K^*$. We call the resulting algebra a *cyclic algebra*.

It is clear that the center of the algebra $\mathcal{A}$ is precisely the field K. That is, an element of $\mathcal{A}$ commutes with all other elements of $\mathcal{A}$ if and only if it lies in K.

Definition 5: We call $\sqrt{[\mathcal{A} : K]}$ the *degree* of the algebra $\mathcal{A}$. It is easily verified that the degree of $\mathcal{A}$ is equal to n.

We consider $\mathcal{A}$ as a right vector space over E and note that every element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following representation as a matrix

$$\psi(a) = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

This mapping allows us to embed any cyclic algebra into $M_n(\mathbb{C})$. Under such an embedding $\psi(\mathcal{A})$ forms an mn^2-dimensional $\mathbb{Q}$-vector space. The map ψ is called the *left regular representation* of $\mathcal{A}$ (see Remark 3).

We are particularly interested in algebras $\mathcal{A}$ for which $\psi(a)$ is invertible for all non-zero $a \in \mathcal{A}$.

Definition 6: A cyclic K-algebra $\mathcal{A}$ is a *division algebra* if every non-zero element of $\mathcal{A}$ is invertible.

The set $\psi(\mathcal{A})$ is an additive subgroup of $M_n(\mathbb{C})$ but is not discrete. This is obviously not a preferred property for a lattice code. A usual strategy to try to overcome this problem is to restrict one's attention to the image in $M_n(\mathbb{C})$ of a suitable subset of $\mathcal{A}$.

Definition 7: A $\mathbb{Z}$*-order* Λ in $\mathcal{A}$ is a subring of $\mathcal{A}$ having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over $\mathbb{Z}$ which generates $\mathcal{A}$ as a linear space over $\mathbb{Q}$.

Lemma 3: Let Λ be a $\mathbb{Z}$-order in a division algebra $\mathcal{A}$. We then have that $\psi(\Lambda)$ is a free group with mn^2 generators. In other words

$$\psi(\Lambda) = \mathbb{Z}B_1 \oplus \mathbb{Z}B_2 \oplus \cdots \oplus \mathbb{Z}B_{mn^2} \subset M_n(\mathbb{C}).$$

We also have that $det(X) \neq 0$ for every non-zero element $X \in \psi(\Lambda)$.

Although $\psi(\Lambda)$ is an additive group, it is not usually a lattice; indeed, if $m > 2$ then the matrices $\mathcal{B}_i$ cannot be linearly independent over $\mathbb{R}$, as $mn^2 > 2n^2$. Lattice theory then tells us that $\psi(\Lambda)$ is not a discrete set under such conditions.

It can be proven that if K is either $\mathbb{Q}$ or a complex quadratic field, then $\psi(\Lambda)$ is a lattice in $M_n(\mathbb{C})$ and will have the NVD property. For other division algebras, as we pointed out above, $\psi(\Lambda)$ is not a lattice in $M_n(\mathbb{C})$. However, this does not exclude the possibility that there is a *different* embedding ψ' of $\mathcal{A}$ into a matrix space that realizes Λ as an NVD lattice.

Algebraic existence results (particularly the short exact sequence of Brauer groups that appears in local class field theory [2, eq. (32.13)] show that, given an algebraic number field K of degree m and any integer $n \geq 1$, there exist infinitely many isomorphism classes of central division algebras of degree n having center equal to K. Furthermore, the Albert-Brauer-Hasse-Noether theorem implies that every central simple algebra defined over a number field is cyclic [2, Th. 32.20], and therefore of the form given in Definition 4. We will show in the following sections that for every order Λ in a division algebra $\mathcal{A}$, there is an embedding ψ' of $\mathcal{A}$ into a suitable matrix such that the resulting code $\psi'(\Lambda)$ is a multiblock code with the NVD property.

Remark 3: In order to state our constructions in Section III in full generality, we need a more general version of the left regular representation. Let $\mathcal{A}$ be a central division algebra of degree n over a number field K. Let us now suppose that E is a maximal subfield of $\mathcal{A}$. From the theory of central simple algebras, we know that $[\mathcal{A} : E] = n$. Let $\{d_1, \ldots, d_n\}$ be a right E-basis for $\mathcal{A}$. Multiplication on the left is an E-linear mapping of $\mathcal{A}$ into itself. In this manner we get a K-algebra embedding $\phi : \mathcal{A} \hookrightarrow M_n(E) \subseteq M_n(\mathbb{C})$. We call this embedding the *left regular representation*.

Lastly, given a division algebra $\mathcal{A}$ over a number field, to every $\mathbb{Z}$-order Λ in $\mathcal{A}$, we can associate a non-zero integer $d(\Lambda/\mathbb{Z})$ called the $\mathbb{Z}$*-discriminant of* Λ. Although we do not give the definition here, throughout the paper we give references for all propeties of $\mathbb{Z}$-discriminants that we use. We refer the reader to [2, Ch. 2] for a detailed treatment of the theory of orders in central simple algebras.

III. Multiblock Codes From Central Division Algebras

In this section we will describe how we can build multiblock lattice codes from division algebras and how it is possible to measure the normalized minimum determinants

of the constructed codes in terms of algebraic invariants of the corresponding division algebras. The main theme here is that we begin with an "idealized" abstract embedding ψ_{abs} that gives us an existence result where any order Λ of a division algebra $\mathcal{A}$ can be realized as a multiblock lattice code $\psi(\Lambda) \subset M_{n\times nk}(\mathbb{C})$ having the NVD property. The normalized minimum determinant of the corresponding code is directly related to the discriminant of the order Λ. We then try to find an explicit embedding ψ_{reg} that has many of the same properties of the abstract embedding and for which the connection between the discriminant and the minimum determinant still holds. Our presentation follows [4]. Only in Section III-B will we extend beyond [4].

We begin with a few definitions and preliminary results.

Let $K/\mathbb{Q}$ be an algebraic number field of degree m. We then have that

$$m = r_1 + 2r_2,$$

where r_1 is the number of real embeddings and r_2 the number of pairs of complex embeddings of K into $\mathbb{C}$.

Let us define the space $G(\mathbb{C})_n \subseteq M_{n\times 2n}(\mathbb{C})$ by

$$G(\mathbb{C})_n = \{(\overline{B}, B) \in M_{n\times 2n}(\mathbb{C}) : B \in M_n(\mathbb{C})\},$$

where * refers to complex conjugation and $\overline{B} = (b_{ij}^*)$.

Definition 8: The ring $\mathbf{H}$ of *Hamiltonian quaternions* is a subset in $M_2(\mathbb{C})$ consisting of matrices of type

$$\begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{pmatrix},$$

where $x_i \in \mathbb{C}$ are freely chosen. Each matrix in the matrix ring $M_n(\mathbf{H}) \subset M_{2n}(\mathbb{C})$ consists of n^2 freely chosen (2×2) blocks that have the inner structure of Hamiltonian quaternions.

There exists an isomorphism (see [1])

$$\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R} \cong M_{n/2}(\mathbf{H})^{\omega} \times M_n(\mathbb{R})^{r_1-\omega} \times G(\mathbb{C})_n^{r_2}. \quad (10)$$

The integer ω appearing in (10) is, by definition, the number of real places where $\mathcal{A}$ ramifies.

Definition 9: We call the triplet (ω, r_1, r_2) the *signature* of $\mathcal{A}$.

Each element in $\mathcal{A}$ can now be seen as a concatenation of ω matrices in $M_n(\mathbb{C})$, $r_1 - \omega$ matrices in $M_n(\mathbb{R})$ and r_2 pairs of conjugate matrices in $M_n(\mathbb{C})$. Equivalently, every element of $\mathcal{A}$ can be viewed as a matrix in $M_{n\times nm}(\mathbb{C})$, where as above $m = r_1 + 2r_2$.

The above isomorphism (10) implies the existence of an injection ψ_{abs}

$$\mathcal{A} \hookrightarrow (M_{n/2}(\mathbf{H})^{\omega} \times M_n(\mathbb{R})^{r_1-\omega} \times G(\mathbb{C})_n^{r_2}) \subset M_{n\times nm}(\mathbb{C}). \quad (11)$$

This will be our "idealized" abstract embedding.

A. Division Algebra Based mn^2-Dimensional Codes in $M_{n\times nm}(\mathbb{C})$

We will now finally show how any order inside of an arbitrary central division algebra $\mathcal{A}$ can be realized as a lattice in a suitable matrix space.

Let us first describe the codes and their properties we get by using the embedding (11).

Let $K/\mathbb{Q}$ be a number field of degree m and $\mathcal{A}$ a K-central division algebra of degree n.

Proposition 1 [4]: Let us suppose that Λ is a $\mathbb{Z}$-order in $\mathcal{A}$ and ψ_{abs} the embedding (11). Then $\psi_{abs}(\Lambda)$ is an n^2m-dimensional lattice in $M_{n\times nm}(\mathbb{C})$ and

$$\det_{min}(\psi_{abs}(\Lambda)) = 1, \quad vol(\psi_{abs}(\Lambda)) = \sqrt{|d(\Lambda/\mathbb{Z})|},$$
$$\text{and } \delta(\psi_{abs}(\Lambda)) = \left(\frac{1}{|d(\Lambda/\mathbb{Z})|}\right)^{1/2n}.$$

This result gives us the existence result. We now know that any order of a division algebra can be realized as a multiblock code. However, the embedding (11) is based on existence results and does not directly give us a method to find the lattices of Proposition 1. Yet it does give us a hint of how it can be imitated in an explicit way

Let K and $\mathcal{A}$ be as above, E be a maximal subfield of $\mathcal{A}$ and $\phi : \mathcal{A} \hookrightarrow M_n(E) \subseteq M_n(\mathbb{C})$ the left regular representation.

The field K has m distinct $\mathbb{Q}$-embeddings β_i from K into $\mathbb{C}$. For each β_i we can find an embedding $\alpha_i : E \hookrightarrow \mathbb{C}$ which extends β_i in the sense that $\alpha_i|_K = \beta_i$. We caution the reader that the embedding α_i will not in general be unique. Let us now suppose that $\{\alpha_1, \ldots, \alpha_m\}$ is collection of embeddings of E into $\mathbb{C}$ which extend all of the embeddings $\{\beta_1, \ldots, \beta_m\}$. Let a be an element of $\mathcal{A}$ and $A = \phi(a)$ the corresponding matrix in $M_n(E)$. We then get a mapping $\psi_{reg1} : \mathcal{A} \to M_{n\times nm}(\mathbb{C})$ given by

$$d \mapsto (\alpha_1(A), \ldots, \alpha_m(A)), \quad (12)$$

where each of the embeddings α_i have been extended to maps $\alpha_i : M_n(E) \hookrightarrow M_n(\mathbb{C})$.

Proposition 2 [4]: Let Λ be a $\mathbb{Z}$-order in $\mathcal{A}$ and ψ_{reg1} the previously defined embedding. Then $\psi_{reg1}(\Lambda)$ is an n^2m-dimensional lattice in $M_{n\times nm}(\mathbb{C})$ and $\det_{min}\left(\psi_{reg1}(\Lambda)\right) = 1$.

We are now interested in the values of $\delta(\psi_{reg1}(\Lambda))$. As we know that $\det_{min}\left(\psi_{reg1}(\Lambda)\right) = 1$, Lemma 2 implies that in order to measure $\delta(\psi_{reg1}(\Lambda))$ it suffices to know $vol(\psi_{reg1}(\Lambda))$. Unfortunately we cannot always relate this value to the algebraic invariants of $\mathcal{A}$. The following result describes conditions under which we can determine the normalized minimum determinant of the code from the discriminant of the associated order.

Proposition 3: Let us suppose that $\mathcal{A}$ has signature $(\omega, r_1 - \omega, r_2)$. If

$$\psi_{reg1}(\mathcal{A}) \subset (M_{n/2}(\mathbf{H})^{\omega} \times M_n(\mathbb{R})^{r_1-\omega} \times G(\mathbb{C})^{r_2}),$$

then

$$vol(\psi_{abs}(\Lambda)) = vol(\psi_{reg1}(\Lambda)) \text{ and}$$
$$\delta(\psi_{abs}(\Lambda)) = \delta(\psi_{reg1}(\Lambda)).$$

Remark 4: We note that the geometric structure of $\psi_{reg1}(\Lambda)$ will in general depend on the choice of E-basis of $\mathcal{A}$ and on the choice of the embeddings α_i.

B. Division Algebra Based $2mn^2$-Dimensional Codes in $M_{n\times nm}(\mathbb{C})$

In the previous section we gave a construction of space time lattice codes from division algebras and described a means of measuring their normalized minimum determinants. We are not yet using the whole signaling space however. The codes in the previous section are mn^2-dimensional lattices in $M_{n\times nm}(\mathbb{C})$, while the maximal rank a lattice can have in such a space is $2mn^2$. We now describe a construction of lattices with maximal rank. The usual strategies for code construction in this scenario can be found in [5] and [8]. Unfortunately these methods only allow us to realize some division algebras as lattice codes. In this section we show how it is possible to overcome these limitations.

Let us consider the case where the center K of the division algebra $\mathcal{A}$ is a totally complex number field. As the center K does not have real primes we simply have an embedding

$$\mathcal{A} \hookrightarrow G(\mathbb{C})^{r_2}. \tag{13}$$

The space $G(\mathbb{C})$ consists of pairs of $n \times n$ matrices, where the second matrix is the complex conjugate of the first. Projecting onto the first coordinate gives us an embedding

$$\psi_{abs2} : \mathcal{A} \hookrightarrow M_{n\times n}(\mathbb{C})^{r_2}. \tag{14}$$

Proposition 4: Let K be a totally complex number field of degree $2m$, $\mathcal{A}$ a K-central division algebra of degree n and Λ a $\mathbb{Z}$-order in $\mathcal{A}$. Then $\psi_{abs2}(\Lambda)$ is a $2mn^2$-dimensional lattice in $M_{n\times nm}(\mathbb{C})$ and the following hold:

$$\det_{min}(\psi_{abs2}(\Lambda)) = 1, \quad vol(\psi_{abs2}(\Lambda)) = 2^{-mn^2}\sqrt{|d(\Lambda/\mathbb{Z})|}$$

and

$$\delta(\psi_{abs2}(\Lambda)) = \left(\frac{2^{2mn^2}}{|d(\Lambda/\mathbb{Z})|}\right)^{1/4n}.$$

Proof: The part considering the dimension of the lattice follows directly from Proposition 1. Let us consider the claim $\det_{min}(\psi_{abs2}(\Lambda)) = 1$. If we use the mapping ψ_{abs}, the absolute value of the determinant of any codeword B is given by the formula $|det(\mathrm{diag}(\psi_{abs}(B)))| = \prod_{i=1}^{2r_2}|b_i|$, where the b_i are the determinants of $n \times n$ blocks B_i that appear in B. However, in this product each b_i can be paired with its complex conjugate. This shows that

$$|det(\psi_{abs2}(B))| = \sqrt{|det(\psi_{abs}(B))|} \geq 1.$$

Let us now consider the Gram matrix of $\psi_{abs2}(\Lambda)$. The elements in the matrix are of type $\Re(tr(\psi_{abs2}(a)\psi_{abs2}(b)^\dagger))$. But the relation between mappings ψ_{abs} and ψ_{abs2} already reveals that $\Re(tr(\psi_{abs}(a)\psi_{abs}(b)^\dagger)) = 2\Re(tr(\psi_{abs2}(a)\psi_{abs2}(b)^\dagger)$. As the Gram matrix is a $2mn^2 \times 2mn^2$ matrix we then have that

$$\begin{aligned} vol(\psi_{abs2}(\Lambda)) &= \sqrt{G(\psi_{abs2}(\Lambda))} = \sqrt{2^{-2mn^2}G(\psi_{abs}(\Lambda))} \\ &= 2^{-mn^2}vol(\psi_{abs}(\Lambda)). \end{aligned}$$

The final result now follows from Lemma 2 together with equation $vol(\psi_{abs}(\Lambda)) = \sqrt{|d(\Lambda/\mathbb{Z})|}$. ∎

Let us now see how these existence results can be realized as explicit codes.

The field K has $2m$ distinct $\mathbb{Q}$-embeddings $\beta_i : K \hookrightarrow \mathbb{C}$. As we assumed that K is totally complex, each of these embeddings is part of a complex conjugate pair. We will denote by $\overline{\beta_i}$ the embedding given by $x \mapsto \overline{\beta_i(x)}$.

For each β_i we can find an embedding $\alpha_i : E \hookrightarrow \mathbb{C}$ such that that $\alpha_i|_K = \beta_i$. This choice can be made in such away that $\overline{\alpha_i}|_K = \overline{\beta_i}$. Let us now suppose $\{\alpha_1, \ldots, \alpha_{2m}\}$ is a collection of such embeddings and that they have been ordered in such a way that $\alpha_i = \overline{\alpha_{i+m}}$, for $0 \leq i \leq m$.

With this notation we can now define the following. Let a be an element of $\mathcal{A}$ and $A = \phi(a)$. We then get a mapping $\psi_{reg2} : \mathcal{A} \mapsto M_{n\times nm}(\mathbb{C})$ by

$$a \mapsto (\alpha_1(A), \ldots, \alpha_{m/2}(A)), \tag{15}$$

where each α_i is extended to an embedding $\alpha_i : M_n(E) \hookrightarrow M_n(\mathbb{C})$.

Proposition 5: Let Λ be a $\mathbb{Z}$-order in $\mathcal{A}$ and ψ_{reg2} the previously defined embedding. Then $\psi_{reg2}(\Lambda)$ is a $2mn^2$-dimensional lattice in $M_{n\times nm}(\mathbb{C})$ which satisfies

$$\det_{min}\left(\psi_{reg2}(\Lambda)\right) = 1, \; vol(\psi_{reg2}(\Lambda)) = 2^{-mn^2}\sqrt{|d(\Lambda/\mathbb{Z})|}$$

and

$$\delta(\psi_{reg2}(\Lambda)) = \left(\frac{2^{2mn^2}}{|d(\Lambda/\mathbb{Z})|}\right)^{1/4n}.$$

Remark 5: The standard method to build multiblock codes with full rate as in [5] and [8] works only for algebras defined over number fields containing a complex quadratic field. The method described above works for any totally complex center.

IV. Algebraic and Coding Theoretic Motivation for Discriminant Bounds

In the previous section we saw that the normalized coding gain of a code derived from a division algebra depends on the discriminant of the algebra. In the rest of this paper we will concentrate on giving general lower bounds for the discriminants. These will in turn yield upper bounds for the normalized minimum determinants. Before giving these (purely algebraic) results, let us first examine these bounds and show the manner in which they extend the results of [7].

A. Connection to the Discriminant Bounds in Number Fields

In [7] the authors considered algebraic number field codes in the Rayleigh fast fading SISO channel. In our notation the fast fading SISO channel is simply a multiblock channel with $n = 1$. The codewords are then of type

$$(x_1, x_2, \ldots, x_m) \in \mathbb{C}^m,$$

where each of the elements x_i faces an independent fading.

In order to design a code in this scenario, we can apply the construction of Proposition 2. It calls for a number field K of degree m and a K-central division algebra $\mathcal{A}$ of degree 1; that is, $\mathcal{A} = K$.

Let us now suppose that $\alpha_1, \ldots, \alpha_m$ are the $\mathbb{Q}$-embeddings of the field K into $\mathbb{C}$. We then have that $\psi_{reg1}(\mathcal{O}_K)$ is an m-dimensional lattice in $\mathbb{C}^m$. This mapping is the usual Minkowski embedding that has been used in several coding theoretic works.

We can partition the embeddings $\alpha_1, \ldots, \alpha_m$ into r_1 real embeddings and $2r_2$ complex embeddings. It follows that $\psi_{reg_1}(K) \subset \mathbb{R}^{r_1} \times G_1(\mathbb{C})^{r_2}$. From the basic algebraic number theory we know that $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times G_1(\mathbb{C})^{r_2}$. According to Propositions 1 and 3 we now have that

$$\delta(\psi_{reg1}(\mathcal{O}_K)) = \frac{1}{\sqrt{|d(K/\mathbb{Q})|}}. \tag{16}$$

In the same manner we may choose a totally complex field K of degree $2m$ so that $\psi_{reg2}(\mathcal{O}_K))$ will be a $2m$-dimensional lattice in $\mathbb{C}^m$ satisfying

$$\delta(\psi_{reg2}(\mathcal{O}_K)) = \frac{2^{m/2}}{|d(K/\mathbb{Q}|^{1/4}}. \tag{17}$$

It is evident that the normalized minimum determinant depends only on the discriminant of the field K. In [7] the authors then posed the question: What are the limits for the normalized minimum determinant for a given m when one uses these algebraically defined codes? After all, there are infinitely many isomorphism classes of number fields of each degree m. Equations (16) and (17) transform this problem into finding bounds for discriminants of degree m algebraic number fields. While multiple number fields may have the same discriminant, it is known that there are only finitely many number fields with a given discriminant. It follows that for every degree m infinitely many discriminants are assumed by degree m number fields. In order to get some intuition for this scenario, the authors of [7] used known discriminant bounds of the form described below.

The Odlyzko bound $C_{(r_1,r_2)}$ is a lower bound for the discriminant of all number fields having signature (r_1, r_2).

As the degree $m \to \infty$ these bounds give

$$|d(K/\mathbb{Q})|^{1/m} \geq (60.8)^{r_1/m}(22.3)^{2r_2/m}. \tag{18}$$

By employing equations (16) and (17) the Odlyzko bounds can be transformed into minimum determinant bounds.

We now consider the same question, but in the setting in which we have n_t transmit antennas and employ a Rayleigh block fading channel. The codewords then have form

$$(X_1, X_2, \cdots, X_m),$$

where the X_i are $n \times n$ matrices. As we saw earlier, in order to build a code we need degree m number field K (resp. degree $2m$ totally complex number field) and a degree n division algebra. We will then have $\delta(\psi(\Lambda)) = \left(\frac{1}{|d(\Lambda/\mathbb{Z})|}\right)^{\frac{1}{2n}}$ and $\delta(\psi_2(\Lambda)) = \left(\frac{2^{2mn^2}}{|d(\Lambda/\mathbb{Z})|}\right)^{\frac{1}{4n}}$.

Now we can ask the same question as in the case of number fields. If we fix m and n, what are the limits for the normalized minimum determinant for codes in this setting. In the case of number fields the Odlyzko bound immediately implied an upper bound. In the case of division algebras however, the needed bounds do not appear in the mathematical literature. The bounds given in [30] answer to this question only in the case in which the center K is fixed. The bounds in [9] on the other hand consider only the case of totally complex quartic fields.

In this paper we will give completely general lower bounds. Given a center of degree m and a division algebra $\mathcal{A}$ of degree n we will produce lower bounds for the discriminant $d(\Lambda/\mathbb{Z})$, where Λ is any $\mathbb{Z}$-order of $\mathcal{A}$.

B. Scope and Implications of the Discriminant Bounds

The methods used in the previous sections made use of $\mathbb{Z}$-orders contained in division algebras. We would therefore like to determine lower bounds for the discriminants of these orders. Maximal orders have the smallest discriminant of all $\mathbb{Z}$-orders contained in a given division algebra $\mathcal{A}$. It is therefore sufficient to find lower bounds for the discriminants of maximal orders. This is an enormous help to us as any maximal $\mathbb{Z}$-order contained in a division algebra has an additional integral structure. In particular maximal $\mathbb{Z}$-orders are also $\mathcal{O}_K$-orders.

Proposition 6 [2, Th. 10.5]: Let $\mathcal{A}$ be a K-central division algebra. Then any maximal $\mathbb{Z}$-order in $\mathcal{A}$ is an $\mathcal{O}_K$-order.

This result will play a crucial role in Section VI.

Discriminant bounds obviously give bounds for the normalized minimum determinants of the corresponding lattices in the case that we are using construction of Proposition 5 or 1. However, when using Proposition 2 the connection between the discriminant and normalized minimum determinant is more subtle. Even in this case however, our bounds are effective.

We also note that the discriminant bounds we give are dependent upon the signature of the algebra, much as the Odlyzko bounds depend on the signature of the number field whose discriminant is being bounded. The need for this dependency is clear as different signatures lead to different codes needed within different coding schemes. If we have a 2 transmit and receive antennas and we can decode and encode over 2-blocks of length 2 without any constraints in decoding complexity then it is a good idea to use the construction of Proposition 5, which leads to a 16-dimensional lattice in $M_{2\times 4}(\mathbb{C})$. The corresponding discriminant bound is then given by Theorem 2.

However, if we have the same scenario with only a single receiving antenna and we aim for low decoding complexity, then it is natural to use a code which is an 8-dimensional lattice in $M_{2\times 4}(\mathbb{C})$. Such code can be naturally be build from the construction of Proposition 2.

The other reason for this division is that, as suggested in [25], different signatures seem to lead to considerably different behaviors of the inverse determinant sum (7). Therefore even two codes having the same center can have very different performances.

V. Algebraic Preliminaries

Let K be a number field of degree d and signature (r_1, r_2). That is, $d = r_1 + 2r_2$ where r_1 is the number of real embeddings of K and r_2 is the number of complex-conjugate pairs of embeddings. Let $\mathcal{O}_K$ denote the ring of integers of K.

We impose an order relation on the set of ideals of $\mathcal{O}_K$ as follows. Given two ideals I_1 and I_2, we will write $I_1 \leq I_2$ if $|N_{\mathbb{Q}}^K(I_1)| \leq |N_{\mathbb{Q}}^K(I_2)|$.

Let $\mathcal{A}$ be a central division algebra over K of degree n. Given an $\mathcal{O}_K$-order Λ of A, we denote by $d(\Lambda/\mathcal{O}_K)$ the discriminant of Λ. An order of $\mathcal{A}$ is called *maximal* if it is maximal with respect to inclusion. It is well known that all maximal orders of $\mathcal{A}$ have the same discriminant. This quantity is the *discriminant of* $\mathcal{A}$.

The following theorem summarizes in [30, Th. 2.4.26 and Proposition 2.4.27].

Theorem 1: Let $\mathcal{A}$ be a central division algebra of degree n over a number field K. Let $P_1 \leq P_2$ be a pair of prime ideals of $\mathcal{O}_K$ having smallest norms.

1) If no real place of K ramifies in $\mathcal{A}$ then the discriminant of $\mathcal{A}$ is at least $(P_1 P_2)^{n(n-1)}$.
2) If K has a unique real place and $n = 2m$ with m odd, then the discriminant of $\mathcal{A}$ is at least $P_1^{n(n-1)} P_2^{m(m-1)}$.
3) If K has at least two real places and $n = 2m$ with m odd, then the discriminant of $\mathcal{A}$ is at least $(P_1 P_2)^{m(m-1)}$.

Remark 6: We note that Theorem 1 is exhaustive in the following sense. The only cases potentially not covered by this theorem are those in which K has no real places or those in which the algebra $\mathcal{A}$ has degree $n = 2^k m$ over K where $k > 1$ and m is odd. In both of these cases however, one may construct a central division algebra over K of degree n which is unramified at all real places (see [30, Remark 2.4.24]).

VI. Bounding the $\mathbb{Z}$-Discriminant of an Order

Let Λ be an $\mathcal{O}_K$-order of $\mathcal{A}$. The $\mathbb{Z}$-discriminant of Λ is defined by the formula

$$d(\Lambda/\mathbb{Z}) = N_{K/\mathbb{Q}}(d(\Lambda/\mathcal{O}_K))d(\mathcal{O}_K/\mathbb{Z})^{n^2},$$

[2, p. 223].

The following theorems provide lower bounds for the $\mathbb{Z}$-discriminant of Λ which depend only on the signatures of K and $\mathcal{A}$. Note that below, $\gamma = 0.577215664901532860\ldots$ is Euler's constant, and that C_h is the function defined below in Equation (20).

Parts (1)-(3) of Theorem 1 are used to prove Theorems 2-4, respectively.

Theorem 2: Let K be a number field of degree d and signature (r_1, r_2), $\mathcal{A}$ be a central division algebra over K of degree $n \geq 2$ and signature $(0, r_1, r_2)$, and Λ be a maximal order of $\mathcal{A}$. Let $y_0 \in \{0.1, 2\}$ and $y \leq y_0$ be a positive real number. Lastly, let $z(y) = \left[e^{r_1} e^{d(\gamma + \log 4\pi)} e^{-12\pi/5\sqrt{y}} e^{-I(y)}\right]^{n^2}$ and (p_1, p_2) be the relevant pair of prime powers from Table I.

1) If $y_0 = 0.1$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 4^{n(n-1)}(53.450)^{n^2} z(y), & n \geq 7 \\ (p_1 p_2)^{n(n-1)}(e^{C_h(p_1,0.1)+C_h(p_2,0.1)})^{n^2} z(y), & 2 \leq n \leq 6 \end{cases}$$

2) If $y_0 = 2$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 4^{n(n-1)}(8.134)^{n^2} z(y), & n \geq 7 \\ (p_1 p_2)^{n(n-1)}(e^{C_h(p_1,2)+C_h(p_2,2)})^{n^2} z(y), & 2 \leq n \leq 6 \end{cases}$$

TABLE I
Prime Powers (p_1, p_2) for Which $(x_1 x_2)^{1-\frac{1}{n}} e^{C_h(x_1,y)+C_h(x_2,y)}$ Is Minimized for $y \in \{0.1, 2\}$

y	n	(p_1, p_2)	y	n	(p_1, p_2)
0.1	2	(13, 13)	2	2	(7, 7)
0.1	3	(7, 7)	2	3	(4, 4)
0.1	4	(4, 4)	2	4	(3, 3)
0.1	5	(3, 3)	2	5	(3, 3)
0.1	6	(3, 3)	2	6	(3, 3)

TABLE II
Prime Powers (p_1, p_2) for Which $f_n(x_1, x_2) = x_1^{1-\frac{1}{n}} x_2^{\frac{1}{4}-\frac{1}{2n}} e^{C_h(x_1,0.1)+C_h(x_2,0.1)}$ Is Minimized

n	(p_1, p_2)
2	$(13, *)$[1]
6	(3, 64)
10	(2, 53)
14	(2, 47)
18	(2, 43)
22	(2, 43)
26	(2, 43)

Theorem 3: Let K be a number field of degree d and signature $(1, r_2)$, $\mathcal{A}$ be a central division algebra over K of degree $n = 2m$ (with m odd), and Λ be a maximal order of $\mathcal{A}$. Let $y_0 \in \{0.1, 2\}$ and $y \leq y_0$ be a positive real number. Lastly, let $z(y) = \left[e^{r_1} e^{d(\gamma + \log 4\pi)} e^{-12\pi/5\sqrt{y}} e^{-I(y)}\right]^{n^2}$ and (p_1, p_2) be the relevant pair of prime powers from Table II.

1) If $y_0 = 0.1$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 2^{n(n-1)} 41^{m(m-1)} (9.572)^{n^2} z(y), & n \geq 30 \\ p_1^{n(n-1)} p_2^{m(m-1)} (e^{C_h(p_1,y_0)+C_h(p_2,y_0)})^{n^2} z(y), & 2 \leq n \leq 26 \end{cases}$$

2) If $y_0 = 2$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 2^{n(n-1)} 41^{m(m-1)} (2.852)^{n^2} z(y), & n \geq 30 \\ p_1^{n(n-1)} p_2^{m(m-1)} (e^{C_h(p_1,2)+C_h(p_2,2)})^{n^2} z(y), & 2 \leq n \leq 26 \end{cases}$$

Theorem 4: Let K be a number field of degree d and signature (r_1, r_2) with $r_1 \geq 2$. Let $\mathcal{A}$ be a central division algebra over K of degree $n = 2m$ (with m odd), and Λ be a maximal order of $\mathcal{A}$. Let $y_0 \in \{0.1, 2\}$ and $y \leq y_0$ be a positive real number. Lastly, let $z(y) = \left[e^{r_1} e^{d(\gamma + \log 4\pi)} e^{-12\pi/5\sqrt{y}} e^{-I(y)}\right]^{n^2}$ and (p_1, p_2) be the relevant pair of prime powers from Table III.

1) If $y_0 = 0.1$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 37^{2m(m-1)} (1.803)^{n^2} z(y), & n \geq 118 \\ (p_1 p_2)^{m(m-1)} (e^{C_h(p_1,y_0)+C_h(p_2,y_0)})^{n^2} z(y), & 6 \leq n \leq 114 \end{cases}$$

2) If $y_0 = 2$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 9^{2m(m-1)} (1.189)^{n^2} z(y), & n \geq 14 \\ (11)^{2m(m-1)} (1.091)^{n^2} z(y), & n = 6, 10 \end{cases}$$

Remark 7: In stating Theorem 4 we excluded the case $n = 2$. The reason for this was that in this situation,

[1]The '*' in Table II indicates that when $n = 2$ the function $f_n(x_1, x_2)$ does not depend upon x_2 and will be minimized whenever $x_1 = 13$.

TABLE III
PRIME POWERS (p_1, p_2) FOR WHICH $(x_1x_2)^{\frac{1}{4}-\frac{1}{2n}} e^{C_h(x_1,0.1)+C_h(x_2,0.1)}$ IS MINIMIZED

n	(p_1, p_2)
6	$(64, 64)$
10	$(53, 53)$
14	$(47, 47)$
$18-26$	$(43, 43)$
$30-114$	$(41, 41)$

the hypotheses of the theorem allow for the existence of a quaternion division algebra ramified at precisely two real places of K and which is unramified at all finite primes of K. Given a maximal order Λ of such an algebra, we will have $d(\Lambda/\mathbb{Z}) = d(\mathcal{O}_k/\mathbb{Z})$, hence our desired bound is simply the Odlyzko bound.

Remark 8: As was the case with Theorem 1 (and pointed out in Remark 6), Theorems 2, 3 and 4 exhaust all possible central division algebras.

In order to obtain a lower bound for $d(\Lambda/\mathbb{Z})$, it of course suffices to obtain a lower bound for

$$|N_{\mathbb{Q}}^K(d(\Lambda/\mathcal{O}_K))|^{1/n^2}|d(\mathcal{O}_K/\mathbb{Z})|.$$

We have already seen, in Theorem 1, how to obtain lower bounds for $|N_{\mathbb{Q}}^K(d(\Lambda/\mathcal{O}_k))|$. We now focus on bounding $|d(\mathcal{O}_K/\mathbb{Z})|$ from below. To do so we will employ the Odlyzko bounds [13], as well as a refinement of these bounds due to Poitou [29] which takes into account the existence of primes of small norm. The precise formulation of these bounds which we will use is due to Brueggeman and Doud [12, Th. 2.4].

Let $y > 0$ be a real number, γ be Euler's constant, and $I(y)$ be as in [12, Th. 2.4]. Let

$$f(x) := (3x^{-3}(\sin x - x\cos x))^2,$$

and

$$C_f(x, y) := 4\sum_{j=1}^{\infty}\frac{\log x}{1+x^j} f(j\sqrt{y}\log x).$$

[12, Th. 2.4] shows that for any prime ideals P_1, P_2 of k and all $y > 0$

$$|d(\mathcal{O}_K/\mathbb{Z})| \geq e^{r_1}e^{d(\gamma+\log 4\pi)}e^{-12\pi/5\sqrt{y}}\cdot e^{-I(y)}e^{C_f(N_{\mathbb{Q}}^K(P_1),y)}e^{C_f(N_{\mathbb{Q}}^K(P_2),y)}. \quad (19)$$

We further define functions

$$h(x) = \begin{cases} f(x), & x \leq 4 \\ 0, & x > 4 \end{cases}$$

and

$$C_h(x, y) := 4\sum_{j=1}^{\infty}\frac{\log x}{1+x^j} h(j\sqrt{y}\log x). \quad (20)$$

The next lemma follows immediately from the fact that for all $x \geq 0$ we have $f(x) \geq h(x) \geq 0$ and the fact that $h(x)$ is decreasing.

Lemma 4: For all real numbers $x, y, y_0 > 0$ with $y \leq y_0$ the following properties hold:

(i) We have $C_f(x, y) \geq C_h(x, y)$.

(ii) We have $C_h(x, y) \geq C_h(x, y_0)$.

It follows that for all $y > 0$

$$|d(\mathcal{O}_K/\mathbb{Z})| \geq e^{r_1}e^{d(\gamma+\log 4\pi)}e^{-12\pi/5\sqrt{y}}e^{-I(y)}\cdot e^{C_h(N_{\mathbb{Q}}^K(P_1),y)}e^{C_h(N_{\mathbb{Q}}^K(P_2),y)}. \quad (21)$$

Since we are viewing the signatures of $\mathcal{A}$ and K as being fixed, and since the term $e^{r_1}e^{d(\gamma+\log 4\pi)}e^{-12\pi/5\sqrt{y}}e^{-I(y)}$ is determined by the signature of K, it suffices (by Theorem 1) to determine the rational prime powers $p_1, p_2 > 1$ for which each of the following functions are minimized:

1) $(p_1p_2)^{(n-1)/n}e^{C_h(p_1,y)}e^{C_h(p_2,y)} = (p_1p_2)^{1-\frac{1}{n}}e^{C_h(p_1,y)}e^{C_h(p_2,y)}$,
2) $p_1^{(n-1)/n}p_2^{m(m-1)/n^2}e^{C_h(p_1,y)}e^{C_h(p_2,y)} = p_1^{1-\frac{1}{n}}p_2^{\frac{1}{4}-\frac{1}{2n}}e^{C_h(p_1,y)}e^{C_h(p_2,y)}$,
3) $(p_1p_2)^{m(m-1)/n^2}e^{C_h(p_1,y)}e^{C_h(p_2,y)} = (p_1p_2)^{\frac{1}{4}-\frac{1}{2n}}e^{C_h(p_1,y)}e^{C_h(p_2,y)}$.

We will determine the minima of these three functions with respect to the parameters $y = 0.1$ and $y = 2$.

In order to obtain a good bound for $\delta(\Lambda)$, we will take advantage of the fact that both $d(\Lambda/\mathcal{O}_k)$ and $d(\mathcal{O}_k/\mathbb{Z})$ are affected by the existence of primes of small norm. To do so we will need a few technical results, which are the subject of Section VI-A.

A. Three Technical Propositions

Proposition 7: Let $n \geq 2$ and define $f_n(x_1, x_2) = (x_1x_2)^{1-\frac{1}{n}}e^{C_h(x_1,y)+C_h(x_2,y)}$.

1) If $y = 0.1$ and $n \geq 7$ then for all prime powers p_1, $p_2 > 1$ we have $f_n(p_1, p_2) \geq f_n(2, 2)$. For $2 \leq n \leq 6$ the prime powers for which $f_n(x_1, x_2)$ is minimized are given in Table I.
2) If $y = 2$ and $n \geq 7$ then for all prime powers $p_1, p_2 > 1$ we have $f_n(p_1, p_2) \geq f_n(2, 2)$. For $2 \leq n \leq 6$ the prime powers for which $f_n(x_1, x_2)$ is minimized are given in Table I.

Proof: We will prove the proposition in the case that $y = 0.1$. The case in which $y = 2$ is completely analogous.

Fix an integer $n \geq 2$ and define an auxiliary function $g(x_1, x_2) = (x_1x_2)e^{C_h(x_1,0.1)+C_h(x_2,0.1)}$. Note that for all $x_1, x_2 \geq 0$ we have $g(x_1, x_2) \geq f_n(x_1, x_2)$. An easy calculation shows that $214 > g(2, 2)$. As $g(2, 2) \geq f_n(2, 2)$, we conclude that $214 \geq f_n(2, 2)$. Observe that $f_n(x_1, x_2) \geq \sqrt{x_1x_2}$. It follows that if p_1, p_2 are prime powers and $f_n(p_1, p_2) < f_n(2, 2)$, then $f_n(p_1, p_2) < 214$ and so $2 \leq p_1, p_2 \leq \frac{214^2}{2}$.

By virtue of the previous paragraph we can check, for any fixed value of $n \geq 2$, to see which values of (p_1, p_2) minimize the function $f_n(x_1, x_2)$ when restricted to prime powers. The assertion of the proposition for $2 \leq n \leq 6$ therefore follows immediately. Similarly, an easy computation shows that $f_n(p_1, p_2) \geq f_n(2, 2)$ for all prime powers p_1, p_2 when $7 \leq n \leq 1000$. Suppose now that $n > 1000$. Since $f_n(x_1, x_2) = g(x_1, x_2)/(x_1x_2)^{\frac{1}{n}}$, we have $f_n(2, 2) > f_n(p_1, p_2)$ if and only if $g(2, 2) > (\frac{4}{p_1p_2})^{\frac{1}{n}}g(p_1, p_2)$. As we are assuming that $n > 1000$ it is clear that if $(p_1, p_2) \neq (2, 2)$

then $(\frac{4}{p_1p_2})^{\frac{1}{n}} > 0.990707126780213$. The proposition now follows from a computation which shows that $g(2,2) < 0.990707126780213 \cdot g(p_1,p_2)$ for all prime powers $p_1, p_2 \leq \frac{214^2}{2}$. ∎

Proposition 8: Let $n = 2m \geq 2$ with m odd and define $f_n(x_1,x_2) = x_1^{1-\frac{1}{n}} x_2^{\frac{1}{4}-\frac{1}{2n}} e^{C_h(x_1,y)+C_h(x_2,y)}$.

1) If $y = 0.1$ and $n \geq 30$ then for all prime powers p_1, $p_2 > 1$ we have $f_n(p_1,p_2) \geq f_n(2,41)$. If $2 \leq n \leq 26$, the prime powers for which $f_n(x_1,x_2)$ is minimized are given in Table II.
2) If $y = 2$ and $n \geq 14$ then for all prime powers $p_1, p_2 > 1$ we have $f_n(p_1,p_2) \geq f_n(2,9)$. If $n \in \{2,6,10\}$, the prime powers for which $f_n(x_1,x_2)$ is minimized are $\{(7,17),(3,11),(2,11)\}$.

Proof: We will prove the proposition in the case that $y = 0.1$. The case in which $y = 2$ is similar and is left to the reader.

Fix an integer $n \geq 30$ as in the statement of the proposition and define an auxiliary function $g(x_1,x_2) = x_1 x_2^{\frac{1}{4}} e^{C_h(x_1,y)+C_h(x_2,y)}$. Then for all $x_1, x_2 > 0$ we see that $g(x_1,x_2) > f_n(x_1,x_2)$. An easy calculation shows that $49 > g(2,41) > f_n(2,41)$. As $n \geq 30$ we see that $49 > f_n(2,41) > x_1^{\frac{29}{30}} x_2^{\frac{7}{30}}$. It follows that if p_1, p_2 are prime powers for which $f_n(2,41) > f_n(p_1,p_2)$ then $49^{\frac{30}{7}} \geq p_1^{\frac{29}{7}} p_2$. In particular we must have $p_1 \leq 47$ and $p_2 \leq 992129$.

By virtue of the previous paragraph we can check, for any fixed value of $n \geq 30$, to see which values of (p_1,p_2) minimize the function $f_n(x_1,x_2)$ when restricted to prime powers. Similarly, an easy computation shows that $f_n(p_1,p_2) \geq f_n(2,41)$ for all prime powers p_1, p_2 when $30 \leq n = 2m \leq 7000$.

We now assume that $n > 7000$. Since $f_n(x_1,x_2) = g(x_1,x_2)/x_1^{\frac{1}{n}} x_2^{\frac{1}{2n}}$, we have $f_n(2,41) > f_n(p_1,p_2)$ if and only if $g(2,41) > (\frac{2}{p_1})^{\frac{1}{n}} (\frac{41}{p_2})^{\frac{1}{2n}} g(p_1,p_2)$. In this case we see that $(\frac{2}{p_1})^{\frac{1}{n}} (\frac{41}{p_2})^{\frac{1}{2n}} \geq (\frac{2}{47})^{\frac{1}{7000}} (\frac{41}{992129})^{\frac{1}{14000}} = 0.998828683870189$ for all prime powers p_1, p_2 in the ranges specified above. A computation shows that $g(2,41) < 0.998828683870189 \cdot g(p_1,p_2)$ for all prime powers $2 \leq p_1 \leq 47$ and $2 \leq p_2 \leq 992129$ with $(p_1,p_2) \neq (2,41),(2,37),(2,43)$. The case of the proposition in which $y = 0.1$ and $n \geq 30$ now follows from demonstrating that for $n > 7000$ and $(p_1,p_2) = (2,37),(2,43)$ we have $f_n(p_1,p_2) \geq f_n(2,41)$. The case in which $y = 0.1$ and $2 \leq n \leq 26$ can be handled similarly. ∎

Proposition 9: Let $n = 2m \geq 2$ with m odd and define $f_n(x_1,x_2) = (x_1x_2)^{\frac{1}{4}-\frac{1}{2n}} e^{C_h(x_1,y)+C_h(x_2,y)}$.

1) If $y = 0.1$ and $n \geq 118$ then for all prime powers $p_1, p_2 > 1$ we have $f_n(p_1,p_2) \geq f_n(37,37)$. If $6 \leq n \leq 114$, the prime powers for which $f_n(x_1,x_2)$ is minimized are given in Table III.
2) If $y = 2$ and $n \geq 14$ then for all prime powers $p_1, p_2 > 1$ we have $f_n(p_1,p_2) \geq f_n(9,9)$. If $n = 6, 10$ then for all prime powers $p_1, p_2 > 1$ we have $f_n(p_1,p_2) \geq f_n(11,11)$.

Proof: We will prove the proposition in the case that $y = 0.1$. The case in which $y = 2$ is similar and is left to the reader.

Fix an integer $n \geq 114$ as in the statement of the proposition and define an auxiliary function $g(x_1,x_2) = (x_1x_2)^{\frac{1}{4}} e^{C_h(x_1,y)+C_h(x_2,y)}$. Then for all $x_1, x_2 > 0$ we see that $g(x_1,x_2) > f_n(x_1,x_2)$. An easy calculation shows that $11 > g(37,37) > f_n(37,37)$. As $f_n(x_1,x_2) > (x_1x_2)^{\frac{14}{57}}$ for n in this range, we see that if p_1, p_2 are prime powers for which $f_n(p_1,p_2) < f_n(37,37)$ then $(p_1p_2) < 11^{\frac{57}{14}}$.

By virtue of the previous paragraph we can check, for any fixed value of $n \geq 114$, to see which values of (p_1,p_2) minimize the function $f_n(x_1,x_2)$ when restricted to prime powers. Similarly, an easy computation shows that $f_n(p_1,p_2) \geq f_n(37,37)$ for all prime powers p_1, p_2 when $116 \leq n = 2m \leq 20000$. Suppose now that $n > 20000$. Since $f_n(x_1,x_2) = g(x_1,x_2)/(x_1x_2)^{\frac{1}{2n}}$, we have $f_n(37,37) > f_n(p_1,p_2)$ if and only if $g(37,37) > (\frac{37}{\sqrt{p_1p_2}})^{\frac{1}{n}} g(p_1,p_2)$.

Note that 8681 is the largest prime power less than $\lfloor \frac{11^{\frac{57}{14}}}{2} \rfloor$. As we are assuming that $n > 20000$ it is clear that $(\frac{37}{\sqrt{p_1p_2}})^{\frac{1}{n}} \geq (\frac{37}{8681})^{\frac{1}{20000}} = 0.999727138528677$ for all prime powers $2 \leq p_1, p_2 \leq \lfloor \frac{11^{\frac{57}{14}}}{2} \rfloor$. The proof of the $y = 0.1$, $n \geq 114$ case of the proposition now follows from a computation which shows that $g(37,37) < 0.999727138528677 \cdot g(p_1,p_2)$ for all prime powers p_1, p_2 in the aforementioned range. The proof when $y = 0.1$ and $6 \leq n \leq 110$ is virtually identical. ∎

B. Proof of Theorems 2, 3 and 4

We will now prove Theorem 2. The proofs of Theorems 3 and 4 are similar and will be left to the reader.

Let $y_0 \in \{0.1, 2\}$ and $y \leq y_0$ be any positive real number. We have already seen, by combining Theorem 1, equation (21) and Lemma 4, that

$$|d(\Lambda/\mathbb{Z})| \geq N_{\mathbb{Q}}^K(P_1P_2)^{n(n-1)} \cdot \left[e^{C_h(N_{\mathbb{Q}}^K(P_1),y_0)} e^{C_h(N_{\mathbb{Q}}^K(P_2),y_0)}\right]^{n^2} \cdot \left[e^{r_1} e^{d(\gamma+\log 4\pi)} e^{-12\pi/5\sqrt{y}} e^{-I(y)}\right]^{n^2}. \quad (22)$$

We begin by obtaining a lower bound for the related quantity

$$N_{\mathbb{Q}}^K(P_1P_2)^{1-\frac{1}{n}} \cdot e^{C_h(N_{\mathbb{Q}}^K(P_1),y_0)} e^{C_h(N_{\mathbb{Q}}^K(P_2),y_0)} \cdot e^{r_1} e^{d(\gamma+\log 4\pi)} e^{-12\pi/5\sqrt{y}} e^{-I(y)}. \quad (23)$$

Because we are viewing the signature of K as being fixed, it suffices to simply determine the prime powers p_1, p_2 for which

$$(p_1p_2)^{1-\frac{1}{n}} e^{C_h(p_1,y_0)+C_h(p_2,y_0)}$$

is minimized. This was done in Proposition 7. The theorem follows by substituting these values into (22) and performing simple algebraic manipulations.

VII. A User's Guide to Discriminant Bounds

In this section we will discuss how to use the bounds of the previous section and will compare them to certain naive bounds defined below. We give the construction of the naive bound only for the case considered in Theorem 2, although analogous bounds can be deduced for the other cases a virtually identical manner.

Let K be a number field of degree d and P_1, P_2 be the smallest prime ideals of K (with respect to the order relation on the prime ideals of K given in the first paragraph of Section V). If we suppose that no infinite place of K is ramified in the degree n central division algebra $\mathcal{A}$ (this is the case when K is totally complex for instance), then for any order $\Lambda \subset \mathcal{A}$ we have that by Theorem 1

$$|d(\Lambda/\mathbb{Z})| \geq |(N_{K/\mathbb{Q}}(P_1)N_{K/\mathbb{Q}}(P_2))^{n(n-1)}d(\mathcal{O}_K/\mathbb{Z})^{n^2}|. \quad (24)$$

This equation suggests a trivial bound that can be used to gauge the quality of the bounds proven in the previous section. Denote by $C_{r_1,d}$ the best known Odlyzko discriminant bound for a degree d number field K containing precisely r_1 real primes.

Proposition 10: Suppose that K is a totally complex number field of degree d and $\mathcal{A}$ is a central division algebra defined over K which has degree n. If Λ is a $\mathbb{Z}$-order contained in $\mathcal{A}$ then

$$|d(\Lambda/\mathbb{Z})| \geq 4^{n(n-1)}(C_{0,d})^{n^2}.$$

Proof: It is clear that $C_{0,d} \leq |d(\mathcal{O}_K/\mathbb{Z})|$. As the norm of any prime of K must be at least 2, the result follows from Equation (24). ∎

Let us now see how our bounds in Section VI stack up against this naive bound. In order to compare them, we will transform the main theorems in Section VI to an easy-to-use form involving classical Odlyzko bounds $C_{r_1,d}$. This is done in Corollaries 1-3.

The function $I(y)$ that appeared in (19) depends on the degree d of the field extension K and the number of real embeddings from K into $\mathbb{R}$. More precisely,

$$I(y) = I_{r_1,d}(y) = \int_{x=0}^{\infty} d\frac{1-f(x\sqrt{y})}{\sinh(x)} + r_1\frac{1-f(x\sqrt{y})}{\cosh(x/2)}dx,$$

where d is the degree of K and r_1 is the number of real embeddings from K to $\mathbb{R}$. Let $y_{r_1,d}$ the value of y which maximizes

$$e^{r_1}e^{d(\gamma+\log 4\pi)}e^{-12\pi/5\sqrt{y}}e^{-I_{r_1,d}(y)} \quad (25)$$

over all real $y > 0$. According to [27], we have

$$C_{r_1,d} = e^{r_1}e^{d(\gamma+\log 4\pi)}e^{-12\pi/5\sqrt{y_{r_1,d}}}e^{-I_{r_1,d}(y_{r_1,d})}.$$

Proposition 11: There exist integers $1 \leq N_1 \leq N_2$ such that when $d > N_1$ we have that $y_{r_1,d} < 2$ and when $d > N_2$ we have $y_{r_1,d} < 0.1$.

Proof: Let y_c be a positive real number. We will now prove that when d is large enough the optimal y will be smaller than y_c. Through elementary analysis we can see that there exists a positive constant C such that $I_{r_1,d}(y) \geq dC$, for all $y \geq y_c$. Therefore $\frac{12\pi}{5\sqrt{y}} + I_{r_1,d}(y) \geq dC$, for all $y \geq y_c$.

It is now enough to prove that there exists such y that

$$\frac{12\pi}{5\sqrt{y}} + I_{r_1,d}(y) < dC, \quad (26)$$

as in this case the y must be smaller than y_c.

Poitou [29, p. 6] proves that for a certain constant l (which is independent of r_1 and d) we have that

$$I_{r_1,d}(y) \leq ly. \quad (27)$$

Combining (26) and (27) we can see that it is now enough to prove that when d is large enough we have such y that

$$\frac{12\pi}{5} + d\sqrt{y}(yl - C) < 0,$$

which, for large enough d, is obviously true when $y = C/(l+1)$. ∎

Remark 9: This proposition proves that for sufficiently large d our discriminant bounds are effective. Explicitly, calculations in [27] show already that when $d > 7$, we have $y_{r_1,d} < 2$.

Remark 10: The bounds in [27] are actually calculated by using a simple approximation of the function $I_{r_1,d}(y)$ (see [29, p. 16]), which gives slightly weaker bounds. The differences between these weaker bounds and those obtained by optimizing (25) are very small and the loss arising from using the tables in [27] is irrelevant for practical purposes.

We next state the easy-to-use versions of our bounds in Section VI. Corollaries 1, 2, and 3 follow immediately from Proposition 11 and Theorems 2, 3, and 4, respectively.

Corollary 1: Let K be a number field of degree d and signature (r_1, r_2), $\mathcal{A}$ be a central division algebra over K of degree $n \geq 2$ and signature $(0, r_1, r_2)$, and Λ be a maximal order of $\mathcal{A}$. Lastly, let (p_1, p_2) be the relevant pair of prime powers from Table I.

1) If $d > N_2$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 4^{n(n-1)}(53.450)^{n^2}(C_{r_1,d})^{n^2}, & n \geq 7 \\ (p_1p_2)^{(n^2-n)}(e^{C_h(p_1,0.1)+C_h(p_2,0.1)}C_{r_1,d})^{n^2}, & 2 \leq n \leq 6 \end{cases}$$

2) If $d > N_1$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 4^{n(n-1)}(8.134)^{n^2}(C_{r_1,d})^{n^2}, & n \geq 7 \\ (p_1p_2)^{(n^2-n)}(e^{C_h(p_1,2)+C_h(p_2,2)}C_{r_1,d})^{n^2}, & 2 \leq n \leq 6 \end{cases}$$

Corollary 2: Let K be a number field of signature $(1, r_2)$, $\mathcal{A}$ be a central division algebra over k of degree $n = 2m$ (with m odd) and Λ be a maximal order of $\mathcal{A}$. Lastly, let (p_1, p_2) be the relevant pair of prime powers from Table II.

1) If $d > N_2$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 2^{n(n-1)}41^{m(m-1)}(9.572)^{n^2}(C_{r_1,d})^{n^2}, & n \geq 30 \\ p_1^{n^2-n}p_2^{m^2-m}(e^{C_h(p_1,0.1)+C_h(p_2,0.1)}C_{r_1,d})^{n^2}, & 2 \leq n \leq 26 \end{cases}$$

2) If $d > N_1$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 2^{n(n-1)}41^{m(m-1)}(2.852)^{n^2}(C_{r_1,d})^{n^2}, & n \geq 30 \\ p_1^{(n^2-n)}p_2^{(m^2-m)}(e^{C_h(p_1,2)+C_h(p_2,2)}C_{r_1,d})^{n^2}, & 2 \leq n \leq 26 \end{cases}$$

Corollary 3: Let K be a number field of signature (r_1, r_2) with $r_1 \geq 2$, $\mathcal{A}$ be a central division algebra over k of degree $n = 2m$ (with m odd) and Λ be a maximal order of $\mathcal{A}$. Lastly, let (p_1, p_2) be the relevant pair of prime powers from Table III.

1) If $d > N_2$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 37^{2m(m-1)}(1.803)^{n^2}(C_{r_1,d})^{n^2}, & n \geq 118 \\ (p_1 p_2)^{m^2-m}(e^{C_h(p_1,0.1)+C_h(p_2,0.1)}C_{r_1,d})^{n^2}, & 6 \leq n \leq 114 \end{cases}$$

2) If $d > N_1$, then

$$|d(\Lambda/\mathbb{Z})| \geq \begin{cases} 9^{2m(m-1)}(1.189)^{n^2}(C_{r_1,d})^{n^2}, & n \geq 14 \\ (11)^{2m(m-1)}(1.091)^{n^2}(C_{r_1,d})^{n^2}, & n = 6, 10 \end{cases}$$

We can now immediately see the difference between our bounds and the trivial ones. Both involve $(C_{r_1,d})^{n^2}$, but while the naive bound uses the multiplicative term $4^{n(n-1)}$, we have a considerably larger term. Our bounds are therefore much stronger when the degree n of the algebra is large.

A. Finding Optimal Algebras

Through computer simulations we see that when the degree of the center is less than 7 the value of $y_{r_1,d}$ that maximizes (25) is larger than 2 and therefore our bounds do not apply. However, for these cases we do not need discriminant bounds as we can simply perform brute force searches for optimal algebras. Let us now explain how these searches can be carried out.

Suppose that K is a totally complex field of degree d, and that P_1 and P_2 are a pair of smallest prime ideals in K. Then there exists a degree n division algebra $\mathcal{A}$ with maximal $\mathbb{Z}$-order Λ having discriminant

$$d(\Lambda/\mathbb{Z}) = (N_{k/\mathbb{Q}}(P_1)N_{K/\mathbb{Q}}(P_2))^{n(n-1)}d(\mathcal{O}_K/\mathbb{Z})^{n^2}. \quad (28)$$

Moreover, this is the smallest possible discriminant of a maximal $\mathbb{Z}$-order given that the center of $\mathcal{A}$ is K [30, Th. 2.4.26].

This formula allows us to perform a brute force search for optimal algebras. The key point is that given a degree d and a real number M, there are only finitely many number fields of degree d with discriminant smaller than M. We may therefore limit ourselves to the finite search space of degree d fields K with discriminant smaller than

$$|(N_{K/\mathbb{Q}}(P_1)N_{K/\mathbb{Q}}(P_2))^{(1-1/n)}d(\mathcal{O}_K/\mathbb{Z})|, \quad (29)$$

and make use of existing tables which contain all number fields of sufficiently small degree and discriminant [17]. For each such field, we find the smallest primes and compute the value of the $\mathbb{Z}$-discriminant given in equation (28). We then simply choose the center which minimizes this value.

Example 1: Let us demonstrate how this search can be performed in the case of degree n central division algebras defined over a totally complex number field of degree 4.

When $n = 2$ a search through the tables of number fields with signature $(0, 2)$ yields a field K of discriminant $d(K) = 3^2 \cdot 13$ with primitive element having minimal polynomial $x^4 - x^3 - x^2 + x + 1$. The field K has primes P_1 and P_2 both of norm 7. Hence, there is a degree 2 division algebra $\mathcal{A}$ containing an order Λ such that

$$d(\Lambda/\mathbb{Z}) = 7^4(3^2 \cdot 13)^4 = 449920319121.$$

TABLE IV
THE OPTIMAL ALGEBRAS WITH DEGREE 4 TOTALLY COMPLEX CENTERS

degree	$(N_{K/\mathbb{Q}}(P_1), N_{K/\mathbb{Q}}(P_2)))$	$d(\mathcal{O}_K/\mathbb{Z})$	$(d(\Lambda/\mathbb{Z}))^{1/n}$
$n = 2$	$(7, 7)$	$3^2 \cdot 13$	$49 \cdot 3^2 \cdot 13^2$
$n = 3$	$(4, 4)$	$3^2 \cdot 5^2$	$16^2(3^2 \cdot 5^2)^3$
$n = 4$	$(3, 3)$	$3^2 \cdot 37$	$9^3(3^2 \cdot 37)^4$
$n = 5$	$(3, 3)$	$3^2 \cdot 37$	$9^4(3^2 \cdot 37)^5$
$n = 6$	$(3, 3)$	$3^2 \cdot 37$	$9^5 \cdot (3^2 \cdot 37)^6$
$n = 7$	$(3, 3)$	$3^2 \cdot 37$	$9^6 \cdot (3^2 \cdot 37)^7$
$n > 7$	$(2, 2)$	$2^4 \cdot 41$	$4^{n-1}(2^4 \cdot 41)^n$

We can similarly find the optimal centers for every n. The results appear in the following table.

Here we can see that the optimal center varies as a function of n and the degree of the algebra, but stabilizes to the field K of discriminant $2^4 \cdot 41$ which has two prime ideals with norm 2.

Remark 11: If we use the algebra described in the first line of Table IV together with the construction of Proposition 5, we obtain a 16-dimensional lattice code for the $(2, 2, 2)$-multiblock channel.

Previously the best discriminant achieved [9] corresponded to the center K of discriminant $d(K) = 2^4 \cdot 3^2$ and primitive element of minimal polynomial $x^4 - x^2 + 1$. The minimal primes in this field have norms 4 and 9. The corresponding discriminant therefore is of the form

$$(4 \cdot 9)^2 \cdot (2^4 \cdot 3^2)^4 = 557256278016,$$

revealing that we managed to find an algebra with the smallest known discriminant and therefore also the multiblock code with the largest possible minimum determinant. However, we point out that in [9] the authors were concentrating only on fields K that have $\mathbb{Q}(i)$ as a subfield, while we optimized over all totally complex fields.

B. Minimum Determinant Bounds From Discriminant Bounds

We conclude the paper by showing how discriminant bounds can be transformed into minimum determinant bounds. As a concrete example, we concentrate on the $(2, 2, k)$-multiblock channel. To apply the construction given in Proposition 5, we need a $d = 2k$-dimensional totally complex field and a degree 2 division algebra $\mathcal{A}$. The minimum determinant of any $\mathbb{Z}$-order Λ in $\mathcal{A}$ is then given by

$$\delta(\psi_{reg2}(\Lambda)) = \left(\frac{2^{4d}}{|d(\Lambda/\mathbb{Z})|}\right)^{1/8}.$$

By Corollary 1, we have

$$\begin{aligned} |d(\Lambda/\mathbb{Z})| &\geq (p_1 p_2)^{n(n-1)}(e^{C_h(7,2)+C_h(7,2)})^{n^2}(C'_{r_1,d})^{n^2} \\ &\geq (7)^4(1.4121)^4(C'_{0,d})^4. \end{aligned}$$

Combining the two previous formulas we see

$$\delta(\psi_{reg2}(\Lambda)) \leq \frac{2^{d/2}}{\sqrt{(9.8847)(C'_{0,d})}}.$$

According to tables in [27] we find that $(C'_{0,8}) \geq 5.6^8$ and $(C'_{0,10}) \geq 6.6^{10}$.

In the following table we consider example algebras. When $d \leq 6$ our example algebras are already optimal. When $d = 8$ or $d = 10$ the algebras were found through experimentation and we do not make any claims of their optimality.

k	d	$N(p_1)N(p_2)$	$\lvert d(\mathcal{O}_k/\mathbb{Z})\rvert$	$\delta(\psi_{reg2}(\Lambda))^{1/d}$
1	2	$(3,4)$	3	$0.78..$
2	4	$(7,7)$	$3^2 \cdot 13$	$0.61..$
3	6	$(13,13)$	$3^2 \cdot 19^2$	$0.63..$
4	8	$(5,9)$	$5 \cdot 17^2 \cdot 43^2$	$0.49..$
5	10	$(11,23)$	11^9	$0.42..$

As stated earlier, our bounds are only relevant for degrees $d > 7$. When $d = 8$ we have an upper bound 0.52 for $\delta(\psi_{reg2}(\Lambda))^{1/d}$. When $d = 10$ the corresponding upper bound is 0.50. Assuming that our bounds are quite tight, the suggested algebra for $d = 8$ is quite close to optimal, but when $d = 10$ there likely exists a better option.

ACKNOWLEDGEMENT

The third author would like to thank Jyrki Lahtonen for pointing out the short proof of Lemma 1.

REFERENCES

[1] E. Bayer-Fluckiger, J.-P. Cerri, and J. Chaubert, "Euclidean minima and central division algebras," *Int. J. Number Theory*, vol. 5, no. 7, pp. 1155–1168, Nov. 2009.
[2] I. Reiner, *Maximal Orders*. New York, NY, USA: Academic, 1975.
[3] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.
[4] R. Vehkalahti, C. Hollanti, and F. Oggier, "Fast-decodable asymmetric space-time codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2362–2385, Apr. 2012.
[5] S. Yang and J.-C. Belfiore, "Optimal space–time codes for the MIMO amplify-and-forward cooperative channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 647–663, Feb. 2007.
[6] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–595, Nov./Dec. 1999.
[7] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "Algebraic lattice constellations: Bounds on performance," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 319–327, Jan. 2006.
[8] H.-F. Lu, "Constructions of multiblock space–time coding schemes that achieve the diversity–multiplexing tradeoff," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3790–3796, Aug. 2008.
[9] C. Hollanti and H.-F. Lu, "Construction methods for asymmetric and multiblock space–time codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1086–1103, Mar. 2009.
[10] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744–765, Mar. 1998.
[11] J. Lahtonen and R. Vehkalahti, "Dense MIMO matrix lattices—A meeting point for class field theory and invariant theory," in *Proc. 7th Int. Symp. Appl. Algebra, Algebraic Algorithms, Error Correcting Codes (AAECC)*, Bengaluru, India, 2007, pp. 247–256.
[12] S. Brueggeman and D. Doud, "Local corrections of discriminant bounds and small degree extensions of quadratic base fields," *Int. J. Number Theory*, vol. 4, no. 3, pp. 349–361, 2008.
[13] A. M. Odlyzko, "Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: A survey of recent results," *J. Théorie Nombres Bordeaux*, vol. 2, no. 1, pp. 119–141, 1990.
[14] L. Luzzi and R. Vehkalahti. "Division algebra codes achieve MIMO block fading channel capacity within a constant gap." [Online]. Available: http://arxiv.org/abs/1412.7650
[15] F. E. Oggier, J.-C. Belfiore, and E. Viterbo, "Cyclic division algebras: A tool for space-time coding," *Found. Trends Commun. Inf. Theory*, vol. 4, no. 1, pp. 1–95, 2007.
[16] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 502–518, Mar. 1996.
[17] *LMFDB—The Database of L-Functions, Modular Forms, and Related Objects*. [Online]. Available: http://www.lmfdb.org/NumberField/
[18] R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto, "On the densest MIMO lattices from cyclic division algebras," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3751–3780, Aug. 2009.
[19] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space–time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885–3902, Sep. 2006.
[20] C. Hollanti, J. Lahtonen, and H.-F. Lu, "Maximal orders in the design of dense space-time lattice codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4493–4510, Oct. 2008.
[21] C. Xing, "Diagonal lattice space–time codes from number fields and asymptotic bounds," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3921–3926, Nov. 2007.
[22] H. Hasse, *Number Theory*. Berlin, Germany: Springer-Verlag, 1980.
[23] G. Wang, H. Liao, H. Wang, and X.-G. Xia, "Systematic and optimal cyclotomic lattices and diagonal space-time block code designs," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3348–3360, Dec. 2004.
[24] G. Wang and X.-G. Xia, "On optimal multilayer cyclotomic space-time code designs," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1102–1135, Mar. 2005.
[25] R. Vehkalahti, H.-F. Lu, and L. Luzzi, "Inverse determinant sums and connections between fading channel information theory and algebra," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 6060–6082, Sep. 2013.
[26] (2005). *PARI/GP, Version 2.2.12*. [Online]. Available: http://pari.math.u-bordeaux.fr
[27] F. Diaz y Diaz, "Tables minorant la Racine n-ième du discriminant d'un corps de degré n," *Pub. Math. d'Orsay*, to be published.
[28] L. Luzzi and R. Vehkalahti, "A new design criterion for spherically-shaped division algebra-based space-time codes," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Seville, Spain, Sep. 2013, pp. 1–5.
[29] G. Poitou, "Sur les petits discriminants," *Séminaire Delange-Pisot-Poitou, Théorie Nombres*, vol. 18, no. 1, pp. 1–17, 1977.
[30] R. Vehkalahti, "Class field theoretic methods in the design of lattice signal constellations," Ph.D. dissertation, Univ. Turku, Turku, Finland, 2008.

Benjamin Linowitz received his M.Sc. and Ph.D. degrees from Dartmouth College, New Hampshire, USA, in 2009 and 2012, respectively, both in pure mathematics.

Since September 2012, he has been with the Department of Mathematics, University of Michigan, Ann Arbor, Michigan, USA. His research interests include the theory of orders in central simple algebras and their applications to other fields.

Matthew Satriano received his Ph.D. degree from the University of California, Berkeley, USA, in 2010 in pure mathematics.

Since July 2014, he has been with the Department of Oncology and Biostatistics at Johns Hopkins University, Baltimore, Maryland, USA. From 2010-14, he was with the Department of Mathematics, University of Michigan, Ann Arbor, Michigan, USA. His research interests include algebraic geometry and mathematical cancer modeling.

Roope Vehkalahti received the M.Sc. and Ph.D. degrees from the University of Turku, Finland, in 2003 and 2008, respectively, both in pure mathematics.

Since September 2003, he has been with the Department of Mathematics, University of Turku, Finland. In 2011-2012 he was visiting Swiss Federal Institute of Technology, Lausanne (EPFL). His research interest include applications of algebra and number theory to information theory.