JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Abdulaziz DEAJIM et David GRANT

On the classification of 3-dimensional non-associative division algebras over p-adic fields

Tome 23, n° 2 (2011), p. 329-346.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_2_329_0>

© Société Arithmétique de Bordeaux, 2011, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l'accord avec les conditions générales d'utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Journal de Théorie des Nombres
de Bordeaux **23** (2011), 329-346

On the classification of 3-dimensional non-associative division algebras over *p*-adic fields

par Abdulaziz DEAJIM et David GRANT

Résumé. Soient p un nombre premier et K un corps p-adique. On emploie les résultats de [12] et l'arithmétique des courbes elliptiques sur K pour réduire le problème de classification des algèbres à division non associatives de dimension 3 sur K à celui de la classification des formes cubiques ternaires H sur K sans zéros non-triviaux. On donne une solution explicite du dernier problème qu'on relie ensuite à la réduction de la jacobienne de H.

Ce résultat complète la classification des algèbres à division non associatives de dimension 3 sur les corps de nombres faite dans [12]. Ces algèbres sont utiles pour la construction des codes espace-temps utilisés pour une meilleure fiabilité des communications à travers les systèmes multi-antennes.

Abstract. Let p be a prime and K a p-adic field (a finite extension of the field of p-adic numbers $\mathbb{Q}_p$). We employ the main results in [12] and the arithmetic of elliptic curves over K to reduce the problem of classifying 3-dimensional non-associative division algebras (up to isotopy) over K to the classification of ternary cubic forms H over K (up to equivalence) with no non-trivial zeros over K. We give an explicit solution to the latter problem, which we then relate to the reduction type of the jacobian of H.

This result completes the classification of 3-dimensional non-associative division algebras over number fields done in [12]. These algebras are useful for the construction of space-time codes, which are used to make communications over multiple-transmit antenna systems more reliable.

1. Introduction

A finite-dimensional non-associative division algebra over a field k is a finite-dimensional vector space A over k along with a k-bilinear product that has no non-trivial zero divisors (see §2 for a fuller description). The associative algebras are included among the non-associative ones, but the

Manuscrit reçu le 1er mai 2010, révisé le 8 février 2011.
The second author was partially supported by NSF grant CCF 0434410.
Classification math. 17A35, 94B27, 11E76, 11G07.

first example of such a division algebra that was not associative was the octonions of Graves and Cayley over the real numbers [8]. Dickson constructed examples of non-associative division algebras over other fields [14], [15], as did Albert, who systematized the subject [1], [2], [3]. Since a semifield is a non-associative division algebra over its center, these algebras have been much researched and are important for the study of translation planes and finite geometries (see [7] for details and references).

Our interest in non-associative division algebras comes from an entirely different application. Recently, non-associative division algebras over number fields have proved useful in constructing "space-time codes," which are matrix codes of complex numbers designed to improve the reliability of radio communications in systems which have more than one transmit antenna (like cell towers). (See [29] for the fundamentals of space-time codes, and [13] for background and references for the application of non-associative division algebras to such codes.)

Recently the authors produced a categorization of 3-dimensional non-associative division algebras over number fields L (which we recall in §3), which included a category for such algebras which remain a division algebra when considered under extension of scalars as being defined over a completion K of L. Hence to complete the classification of all 3-dimensional non-associative division algebras over L, we have to do the same for such algebras over K. It is that task we complete in this paper in the form of Theorem 5.2.

The main tools employed are:

(1) results on linear matrices and their determinants (Proposition 3.2) derived by the first author from a general result of Beauville and made constructive in his thesis [11] and published in [12] (these results have also been obtained independently in unpublished work of Catherine O'Neil and Manjul Bhargava);

(2) the arithmetic of elliptic curves over p-adic fields;

(3) elementary considerations on ternary cubic forms (homogeneous polynomials) over p-adic and finite fields with no non-trivial rational zeroes; and

(4) the polynomials associated to ternary cubic forms H introduced in [5] to define the jacobian E of the curve defined by H when it is absolutely irreducible, which allow us to relate our classification types of H with no non-trivial zeroes over K in Theorem 5.1 to the reduction type of E in Theorem 5.2.

We note that although our classification result is for non-associative division algebras over p-adic fields, we expect our method can be modified so that the same results will hold for 3-dimensional non-associative division algebras over any non-archimedean local field of characteristic different from 3.

The paper is organized as follows. In §2 we recall preliminary results on non-associative division algebras, especially the important contributions of Albert and Menichetti. In §3 we recount what we need of [12] on 3-dimensional non-associative division algebras over perfect fields and their classification via their representations. In §4 we apply the arithmetic of elliptic curves over p-adic fields K to reduce the classification of 3-dimensional non-associative division algebras over K to that of classifying ternary cubic forms over K which have no non-trivial zeros over K. In the final §5, we recall what we need of the classical and modern theory of ternary cubic forms, and complete the classification.

We thank the referee for many helpful suggestions.

2. Preliminaries on non-associative division algebras

In this section we give the necessary background on non-associative division algebras and their representations.

Let n be a positive integer, k a field, and A an n-dimensional vector space over k, whose addition we denote by $+$ and whose scalar multiplication we denote by juxtaposition. We call a product $\circ$ on A *k-bilinear*, if for every $a, b, c \in A$ and $s \in k$ we have

$$a \circ (b+c) = a \circ b + a \circ c,\ (a+b) \circ c = a \circ c + b \circ c,\ s(a \circ b) = sa \circ b = a \circ sb.$$

Definition. An n-dimensional vector space A over a field k is said to be an n-dimensional non-associative algebra over k if it has a k-bilinear product $\circ$. By abuse of notation, we denote this algebra as $A = (A, \circ)$. If in addition A has no nontrivial zero divisors under $\circ$, we say that A is a non-associative division algebra.

In the definition above, *non-associative* simply means that associativity is not being assumed [25]. So examples of non-associative division algebras include the associative ones, the octonions over the real numbers, and the *twisted fields* of Albert, which he first introduced over a finite field. He later generalized his definition to what he called *generalized twisted fields* [3]. Menichetti [22] gave a definition of these over any field, which we state more generally here.

Definition. Let F be a degree-n galois extension of a field k. Let c be an element of F whose norm to k is not 1. For fixed σ, τ in the galois group of F over k, define a product $\circ$ on F by

$$x \circ y = x\,y - c\,x^{\sigma}\,y^{\tau},$$

where the product in the right hand side of the equation is the field product. Then $(F, \circ)$ is an n-dimensional non-associative division algebra over k, which is called a generalized twisted field over k split by F.

An equivalence relation on non-associative algebras, weaker than isomorphism, also appears in the work of Albert [1].

Definition. Let $A = (A, \circ)$ and $B = (B, \star)$ be k-algebras which are isomorphic as k-vector spaces over a field k. We say that A and B are k-isotopic if there exist k-vector space isomorphisms α, β, γ from A to B such that

$$a_1 \circ a_2 = (a_1^{\alpha} \star a_2^{\beta})^{\gamma^{-1}}$$

for every $a_1, a_2 \in A$. We call the triplet (α, β, γ) a k-isotopism from A to B. Since k-isotopism is an equivalence relation, we will also say that A and B are k-isotopic, or are equivalent up to k-isotopy.

It can be easily checked that the property of not having zero divisors is invariant under isotopy. Therefore, an algebra that is isotopic to a division algebra must be a division algebra, too.

If $(A, \circ)$ is an n-dimensional non-associative algebra over a field k, and F is a field extension of k, then the tensor product of k-vector spaces $F \otimes A$ is an n-dimensional vector space over F, so can be given the structure of a non-associative F-algebra with product $\cdot \otimes \circ$, where $\cdot$ denotes multiplication in F. We call $F \otimes A = (F \otimes A, \cdot \otimes \circ)$ the *extension of scalars* of A by F. Note that if A is a non-associative division algebra over k, then $F \otimes A$ may or may not be a non-associative division algebra over F. (For example, the Hamiltonian quaternion algebra over the rational field $\mathbb{Q}$ obtains zero divisors when its scalars are extended over $\mathbb{Q}_p$ for any odd p.)

Let $\mathrm{Mat}_n(k)$ denote the ring of $n \times n$ matrices with entries in k.

Definition. Let m and n be positive integers. For any $P_1, \cdots, P_m \in \mathrm{Mat}_n(k)$ and indeterminates $z_1, \cdots, z_m$, we call $\sum_{i=1}^{m} z_i P_i$ a linear matrix over k.

Definition. Let f be a form over a field k. We call f a k-anisotropic form if it has no nontrivial solutions over k.

Let A be a finite dimensional non-associative algebra over a field k, and suppose that $\mathcal{B}$ is a basis for A over k. For $a \in A$, let $[a]_{\mathcal{B}}$ denote the column vector of its coordinates with respect to this basis.

Definition. Let $(A, \circ)$ be an n-dimensional non-associative algebra over a field k, and $\mathcal{B}$ a basis for A as a k-vector space. Then by the bilinearity of $\circ$, there are matrices $M_i, N_i \in \mathrm{Mat}_n(k)$, $1 \leq i \leq n$, such that for every $p, q \in A$, setting $r = p \circ q$ we have

$$[r]_{\mathcal{B}} = (\sum_{i=1}^{n} p_i M_i)[q]_{\mathcal{B}} = {}^t(\sum_{i=1}^{n} q_i N_i)[p]_{\mathcal{B}},$$

where $(p_i) = [p]_{\mathcal{B}}, (q_i) = [q]_{\mathcal{B}}$, and ^{t} denotes taking the transpose.

Let x_i and y_i, $1 \leq i \leq n$, be indeterminates, and x, y the column vectors whose entries are x_i and y_i. We call

$$\Lambda = \sum_{i=1}^{n} x_i M_i \text{ and } \Gamma = \sum_{i=1}^{n} y_i N_i,$$

the left and right representations of A with respect to $\mathcal{B}$, so $\Lambda y = {}^t\Gamma x$.

Let $f_\Lambda(x_1, ..., x_n)$, $f_\Gamma(y_1, ..., y_n)$ be the determinants of Λ and Γ. We call them the left and right determinants of A, and they are independent of the choice of $\mathcal{B}$.

Note that if A is isotopic to B, then there is an invertible linear change of variables taking the left determinant of A to a constant multiple of the left determinant of B. The left and right representations of a non-associative division algebra A over k are linear matrices whose determinants are k-anisotropic.

The following is well-known. See e.g., [12].

Lemma 2.1. *Let k be a field, and $z_1, ..., z_n$ be indeterminates. Let $P_i \in \mathrm{Mat}_n(k)$, $1 \leq i \leq n$, be such that the determinant of the linear matrix $P = \sum_{i=1}^{n} z_i P_i$ is k-anisotropic. Then P is the left-representation of an n-dimensional non-associative division algebra over k.*

From the above lemma, the following is evident.

Corollary 2.1. *To find all n-dimensional non-associative division algebras over a field k (up to isotopy), it suffices to find all degree-n anisotropic forms over k in n variables (up to invertible linear change of variables) that can be written as determinants of linear matrices over k, and then to find all the ways that such a form can be written as the determinant of a linear matrix over k.*

3. Three-dimensional non-associative division algebras over perfect fields

The classification of n-dimensional non-associative division algebras over fields k has only been accomplished for certain n and k. In the case $n = 2$, it is known that all non-associative division algebras over k are isotopic to quadratic field extensions of k (see e.g., [12] for references).

For the case $n = 3$, the classification depends on k. For instance, there are no 3-dimensional non-associative division algebras over an algebraically closed field or a real closed field since there are no anisotropic ternary cubic forms over such fields. Over finite fields $\mathbb{F}_q$, Menichetti [21] proved a conjecture of Kaplansky [19] that all 3-dimensional non-associative division algebras are isotopic to generalized twisted fields (Menichetti extended this in [22] for any prime n, and q sufficiently large depending on n.)

Over number fields we have the following theorem from [12] (for more details, see [11]).

Theorem 3.1. *Let L be a number field. Then every 3-dimensional non-associative division algebra A over L is one of the following types:*

(1) A is a generalized twisted field.

(2) $M \otimes A$ is a generalized twisted field over M, for some quadratic extension M of L.

(3) $L_\nu \otimes A$ is a 3-dimensional non-associative division algebra over some non-archimedean completion L_ν of L.

(4) A has a left representation whose determinant defines a nontrivial element of order 3 in the Tate-Shafarevich group of some elliptic curve E over L with $E(L) \neq 0$.

In this paper we classify 3-dimensional non-associative algebras over p-adic fields, which will complete the picture in case (3) above. By Corollary 2.1, the classification of 3-dimensional non-associative division algebras over a field k (up to isotopy) comes down to finding (up to invertible linear change of variables) anisotropic ternary cubic forms over k, then seeing which of them can be written as determinants of linear matrices, and for such forms, finding all the ways they can be written as the determinants of linear matrices.

Let k be a perfect field, $\overline{k}$ an algebraic closure of k, and G_k the galois group of $\overline{k}$ over k.

Let us now go through a series of simplifications (as in [11]). Suppose that $f(x, y, z)$ is a cubic anisotropic form over k. If f were reducible over k, then the algebraic set C_f defined by the vanishing of f in $\mathbb{P}^2$ would contain a k-rational line and, thus, a k-rational point, a contradiction. So f must be irreducible over k. If f factors over $\overline{k}$, since G_k acts on the components of C_f, C_f cannot be the union of a line and a conic since the line would then be k-rational. So C_f is the union of three G_k-conjugate lines. On the other hand, if f stays irreducible over $\overline{k}$, then it has at most one singular point [18], which would then be a k-rational point. So C_f must be a nonsingular genus one curve in this case. We have just proved the following lemma.

Lemma 3.1. *Let k be a perfect field, f a ternary anisotropic cubic form over k, and C_f the algebraic set defined by f. Then either C_f is the union of three lines conjugate under G_k, or C_f is an absolutely irreducible curve of genus one.*

If A is a 3-dimensional generalized twisted field over k split by a cyclic cubic extension F, then each of its left and right determinants is a constant times the product of three G_k-conjugate lines defined over F. Menichetti has proved the converse.

Proposition 3.1. [22] *If k is a perfect field with a cyclic cubic extension F, and A is a 3-dimensional non-associative division algebra over k whose left and right determinants factor into linear forms over F, then A is isotopic to a generalized twisted field over k split by F.*

Remark. In fact, the left determinant of A factors over F if and only if the right determinant does, see [12]. If these determinants factor over $\overline{k}$, but not over a cyclic cubic extension, then they do so over an S_3-extension F' of k, which is a cyclic cubic extension of the unique quadratic extension of k contained in F' (here S_3 denotes the symmetric group on 3 letters.)

From Lemma 3.1 and Proposition 3.1, we see that a 3-dimensional non-associative division algebra over k is either isotopic to a generalized twisted field over k (or a quadratic extension of k), or the algebraic sets defined by its left or right determinant are absolutely irreducible so are genus one cubic curves with no k-rational points. Hence it suffices to classify these latter algebras.

Note that if H is an absolutely irreducible anisotropic ternary cubic form over k that is the determinant of a linear matrix, then in [12] a precise algorithm was given for finding all ways that such an H can be written as the determinant of a linear matrix over k. Therefore Corollary 2.1 implies that completing the classification of 3-dimensional non-associative division algebras over a perfect field k (up to isotopy) comes down to finding (up to invertible linear change of variables) all anisotropic ternary cubic forms over k, and then seeing which of them can be written as determinants of linear matrices.

So let f be an absolutely irreducible anisotropic ternary cubic form over k and C_f the plane curve defined by f. We will study C_f in terms of its jacobian E over k. Note that E is an elliptic curve over k and $C_f \in \mathrm{WC}(E/k)$, the Weil-Châtelet group of principal homogeneous spaces of E over k. Since C_f is a cubic plane curve, it must have index dividing 3 [27]. Since C_f is a nontrivial element of $\mathrm{WC}(E/k)$ (as it has no k-rational point), C_f is indeed of index 3 over k.

Conversely, if E is an elliptic curve over k whose Weil-Châtelet group has an element C of index 3 over k, C has an effective k-rational divisor D of degree 3, which gives a projective embedding of C defined by an absolutely irreducible anisotropic ternary cubic form over k.

It follows that in order to complete the classification of 3-dimensional non-associative division algebras over k, we need only find which elliptic curves E over k have index-3 elements C in their Weil-Châtelet groups over k, such that the defining ternary cubic forms for C can be written as determinants of linear matrices over k. (The finer classification of which classes in $\mathrm{WC}(E/k)$ of index 3 give rise to equivalent ternary cubic forms under linear change of variables is carried out in [16].)

The chief result we use is:

Proposition 3.2. *Let k be a perfect field and C_f a genus one curve defined by an absolutely irreducible anisotropic ternary cubic form f over k. Then f is the determinant of a linear matrix over k if and only if C_f has a k-rational divisor of degree zero which is not linearly equivalent to the zero divisor.*

This was proved in [11] by first deriving it from a general result of Beauville [6], and then by giving a constructive proof.

Our classification problem has now been reduced to determining which ternary cubics f over a p-adic field K are absolutely irreducible, anisotropic, and are such that C_f has a rational divisor D of degree 0 which is not linearly equivalent to 0. In the next section we will show that for absolutely irreducible forms f over K, such a D always exists.

4. Reducing the classification of 3-dimensional non-associative division algebras over p-adic fields to that of classifying absolutely irreducible anisotropic ternary cubic forms

For the remainder of the paper, let the field K be a finite extension of $\mathbb{Q}_p$, where p is a rational prime.

For a curve C over K, let $\mathrm{Div}^0(C)$ and $\mathrm{Pic}^0(C)$ respectively denote the group of divisors of degree 0 and the Picard group of divisor classes of degree 0 modulo linear equivalence over $\overline{K}$. We let $\mathrm{Div}^0_K(C)$ and $\mathrm{Pic}^0_K(C)$ denote the corresponding subgroups of divisors and divisor classes rational over K. For D in $\mathrm{Div}^0_K(C)$, we will let $[D]$ denote its class in $\mathrm{Pic}^0_K(C)$.

Proposition 4.1. *Let f be an absolutely irreducible ternary cubic form over K, so C_f is a curve of genus 1 over K. Then C_f has a K-rational divisor D of degree 0 such that $[D] \neq 0$.*

Proof. Let $C = C_f$, and E be the jacobian of C. We will identify $E(K)$ with $\mathrm{Pic}^0_K(C)$. The Proposition requires us to find a non-trivial divisor class in $\mathrm{Pic}^0_K(C)$ which contains a K-rational divisor. The exact sequence of G_K-modules,

$$1 \to \overline{K}^* \to \overline{K}(C)^* \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0,$$

where the maps are in turn, the natural injection, the map taking a function to its divisor, and the natural surjection, breaks into two short exact sequences

$$1 \to \overline{K}^* \to \overline{K}(C)^* \to \overline{K}(C)^*/\overline{K}^* \to 1, \tag{1}$$

$$1 \to \overline{K}(C)^*/\overline{K}^* \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0. \tag{2}$$

Since G_K is the galois group of $\overline{K}(C)/K(C)$, using Hilbert's Theorem 90, the long exact sequence of Galois cohomology attached to (1) gives an injection

$$\epsilon : H^1(G_K, \overline{K}(C)^*/\overline{K}^*) \to H^2(G_K, \overline{K}^*) = Br(K),$$

the Brauer group of K. The long exact sequence attached to (2) gives a map

$$\delta : E(K) = \mathrm{Pic}^0_K(C) \to H^1(G_K, \overline{K}(C)^*/\overline{K}^*),$$

whose kernel is non-trivial if and only if a D as in the statement of the proposition exists. The composite map $\phi = \epsilon \circ \delta$ maps $E(K)$ into $Br(K)$, and the kernel is the image of $\mathrm{Div}^0_K(C)$ in $E(K)$. Now the theory of formal groups shows that $E(K)$ has a subgroup isomorphic to the ring of integers of K [27], which is torsion free. Since K is a p-adic field, $Br(K) = \mathbb{Q}/\mathbb{Z}$ [26], a torsion group. Hence the kernel of ϕ — and therefore the kernel of δ — is non-trivial, so a D as in the statement of the proposition exists. □

Since K is a p-adic field, a theorem of Lichtenbaum [20] shows that the index of a principal homogeneous space for E is equal to its order in $\mathrm{WC}(E/K)$ (Milne showed the same over any local field [23]). Combining this with the results from the last section, we see that to each isotopy class of 3-dimensional non-associative division algebras over K which are not twisted fields over K or over a quadratic extension of K, there corresponds an elliptic curve E/K that has an element C in $\mathrm{WC}(E/K)$ of order 3, and for which there exists a divisor $D \in \mathrm{Div}_K 0(C)$ with $[D] \neq 0$ in $E(K)$. The proposition implies that finding all such C is the same as finding all absolutely irreducible anisotropic ternary cubics over K. It is this problem that we tackle in the next section.

5. Classifying absolutely irreducible anisotropic ternary cubic forms over *p*-adic fields

We now complete the classification up to isotopy of 3-dimensional non-associative division algebras over a p-adic field K, which by the results of §4 comes down to classifying (up to invertible linear change of variables) absolutely irreducible anisotropic ternary cubic forms over K. This can be done in three steps:

(1) determining the set of ternary cubic forms which are absolutely irreducible;

(2) determining the set of which ternary cubic forms are anisotropic;

(3) taking the intersection of the two sets.

For cubic forms f over the complex numbers, there is a specific set of polynomials in the coefficients of f described in [24] §240 (and verified and clarified in [9]) which vanish if and only if f factors. By the Lefschetz Principle, the vanishing of these polynomials will determine the absolute

reducibility of ternary cubics over any field of characteristic 0. Hence it suffices to solve step (2), i.e. to find all anisotropic ternary cubics over K, which we do in Theorem 5.1. A set of polynomials in the coefficients of a ternary cubic form due to Artin, Rodriguez-Villegas, and Tate [5] will play a significant role in interpreting the results (see Theorem 5.2).

In [5], for the ternary cubic form over K, $f(x,y,z) =$
$Ax^3+By^3+Cz^3+Px^2y+Qy^2z+Rz^2x+Txy^2+Uyz^2+Vzx^2+Mxyz$,
they give the following polynomials in the coefficients of f:

$$
\begin{gathered}
a_1 = M, \qquad (3)\\
a_2 = -(PU+QV+RT),\\
a_3 = 9ABC-(AQU+BRV+CPT)-(TUV+PQR),\\
a_4 = (ARQ^2+BPR^2+CQP^2+ATU^2+BUV^2+CVT^2)+\\
(PQUV+QRVT+RPTU)-3(ABRU+BCPV+CAQT),\\
a_6 = -27A^2B^2C^2+9(A^2BCQU+B^2CARV+C^2ABPT)\\
+3ABC(TUV+PQR)-(ABQRUV+BCRVPT+CAPQTU)\\
-(A^2CQ^3+B^2AR^3+C^2BP^3+A^2BU^3+B^2CV^3+C^2AT^3)\\
-PQRTUV+2(ACQ^2TV+BAR^2UT+CBP^2VU\\
+ACQRT^2+BARPU^2+CBPQV^2)-(AQTVU^2+BRUTV^2\\
+CPVUT^2+APQ^2RU+BQR^2PV+CRP^2QT)\\
-(AQ^2R^2T+BR^2P^2U+CP^2Q^2V+ART^2U^2+BPU^2V^2+CQV^2T^2)\\
+M(ABU^2V+BCV^2T+CAT^2U+ABR^2Q+BCP^2R+CAQ^2P)\\
+M(AQRTU+BRPUV+CPQVT-3ABC(QV+RT+PU))\\
-M^2(ABRU+BCPV+CAQT)+M^3ABC.
\end{gathered}
$$

We will call

$$(a_1,a_2,a_3,a_4,a_6) = (a_1(f),a_2(f),a_3(f),a_4(f),a_6(f))$$

the *vector of polynomials associated* to f.

When C_f is a curve of genus 1,

$$E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4+a_6,$$

is the jacobian of C_f [5]. This model for the jacobian works in all characteristics (extending the results of [4] to characteristics 2 and 3). From the a_i we define the other polynomials standardly attached to Weierstrass equations [27]:

$$
\begin{gathered}
b_2 = a_1^2+4a_2,\ b_4 = 2a_4+a_1a_3,\ b_6 = a_3^2+4a_6,\\
b_8 = a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2,\\
c_4 = b_2^2-24b_4,\ c_6 = -b_2^3+36b_2b_4-216b_6,\\
\Delta = -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6.
\end{gathered}
$$

For any $c \in K$ the polynomials satisfy

$$a_i(cf) = c^i a_i(f), \tag{4}$$

and more generally, if m is a 3×3 permutation matrix or diagonal matrix over K,

$$a_i(f((x,y,z)m)) = \det(m)^i a_i(f(x,y,z)). \tag{5}$$

On the other hand, c_4 and c_6 (and hence Δ) are *invariants* of f, that is, for any invertible 3×3 matrix m over K,

$$\begin{aligned} c_4(f((x,y,z)m)) &= \det(m)^4 c_4(f(x,y,z)), \\ c_6(f((x,y,z)m)) &= \det(m)^6 c_6(f(x,y,z)), \\ \Delta(f((x,y,z)m)) &= \det(m)^{12} \Delta(f(x,y,z)). \end{aligned} \tag{6}$$

From now on we let R denote the ring of integers of K, let π be a generator of the maximal ideal in R, and let $\mathbb{F}_q$ be the finite residue field $R/\pi R$.

A lot of information about anisotropic ternary cubic forms over K can be gleaned from studying their reduction over the residue field $\mathbb{F}_q$. Towards this end we need to discuss the minimality of a form, and to do that we need a notion of equivalence.

We say two forms f and g (of any degree and number of variables) over K are *equivalent over* K if g is a non-zero element in K times an invertible change of variables of f over K. Likewise, we say two forms over R are *equivalent over* R if one is gotten from the other by multiplying by a unit in R after applying an invertible linear change of variables over R. In addition, we will call a form over K *normalized* if all its coefficients lie in R and not all its coefficients vanish mod π. For a normalized ternary cubic form, a_1, a_2, a_3, a_4, a_6 all lie in R.

We will call a ternary cubic form over K *minimal* if it is a normalized form, and among all the normalized forms K-equivalent to it, its Δ-invariant has minimal valuation. It follows from the theory of elliptic curves that every absolutely irreducible anisotropic ternary cubic form over K is K-equivalent to a minimal one. However, it is not necessarily equivalent over R to a unique such one.

Let v denote the valuation of K, normalized so $v(\pi) = 1$. It is then clear from (6) that if for a ternary cubic form f over R, either $v(c_4) < 4$ or $v(c_6) < 6$ holds, then f is minimal.

Example. Suppose $p \neq 2, 3$, and let $\alpha \in R$ reduce to a cubic non-residue mod π. It follows that

$$f(x,y,z) = x^3 + \pi(y^3 + \alpha z^3)$$

is anisotropic over K, absolutely irreducible, and has vector of associated polynomials

$$(0, 0, 9\pi^2\alpha, 0, -27\pi^4\alpha^2),$$

so $b_2 = b_4 = b_8 = c_4 = 0$, $b_6 = -27\pi^4\alpha^2$, and $c_6 = 2^3 3^6 \pi^4 \alpha^2$, so f is minimal (the proof of Theorem 5.2 will show that f is minimal if $p = 2$ or 3 as well). Now f is K-equivalent to $g(x, y, z) = f(\pi x, y, z)/\pi$, which is normalized, and by (4) and (5) has the same associated polynomials, so is also minimal. But since the reductions mod π of C_f and C_g have different geometries (the former is a tripled line and the latter is 3 distinct lines), f and g cannot be equivalent over R. That is to say, f and g define non-isomorphic schemes over R.

Let f be a normalized anisotropic ternary cubic form over K. Let $\overline{f}$ be the reduction of f modulo π. By Hensel's Lemma, if $C_{\overline{f}}$ (the algebraic set defined by $\overline{f}$ over $\mathbb{F}_q$) has a non-singular $\mathbb{F}_q$-rational point, it will lift to a non-trivial R-rational point of C_f, violating the assumption that f is anisotropic. So all the $\mathbb{F}_q$-rational points of $C_{\overline{f}}$ must be singular.

Lemma 5.1. *Suppose that g is a ternary cubic form over $\mathbb{F}_q$, such that all of the $\mathbb{F}_q$-rational points of C_g are singular. Then either:*

i) g is a constant times the product of 3 conjugate linear forms ℓ_1, ℓ_2, ℓ_3 defined over $\mathbb{F}_{q^3}$ but not over $\mathbb{F}_q$, where the 3 points $P_{ij} = C_{\ell_i} \cap C_{\ell_j}$, $1 \leq i < j \leq 3$, are distinct.

ii) g is a constant times the product of 3 conjugate linear forms ℓ_1, ℓ_2, ℓ_3 defined over $\mathbb{F}_{q^3}$ but not over $\mathbb{F}_q$, and all C_{ℓ_i}, $i = 1, 2, 3$, intersect at an $\mathbb{F}_q$-rational point.

iii) g is a constant times the cube of an $\mathbb{F}_q$-rational linear form.

Proof. We first claim that g cannot be absolutely irreducible over $\mathbb{F}_q$. By way of contradiction, assume it is. On the one hand, if C_g is non-singular, it is a curve of genus 1, so has a nonsingular $\mathbb{F}_q$-rational point by the Hasse-Weil bound [27], contradicting the assumption on g. On the other hand, if C_g is singular, then, g being an absolutely irreducible plane cubic, C_g has precisely one singular point, which must be a cusp or a node [18]. In either case, the singular point is $\mathbb{F}_q$-rational, so can be used to project the nonsingular points of g isomorphically over $\mathbb{F}_q$ onto the projective line over $\mathbb{F}_q$ minus 1 or 2 points (see [27]). Hence C_g has a non-singular $\mathbb{F}_q$-rational point, again a contradiction. Thus g is not absolutely irreducible and so factors non-trivially over $\overline{\mathbb{F}}_q$.

Now, if g factors over $\overline{\mathbb{F}}_q$ into the product of an irreducible quadratic form q and a linear form ℓ, then the line C_ℓ would be $\mathbb{F}_q$-rational, and by Bezout's Theorem, C_g would have at most 2 singular points where C_q and C_ℓ intersect. Since an $\mathbb{F}_q$-line has at least three $\mathbb{F}_q$-rational points, one of them would have to be nonsingular, a contradiction. So, g must be

the product over $\overline{\mathbb{F}}_q$ of 3 linear forms ℓ_1, ℓ_2, ℓ_3. The same argument shows that if ℓ_1 were rational and ℓ_2 and ℓ_3 were not, but were conjugate over $\mathbb{F}_{q^2}$, then C_g would have a nonsingular $\mathbb{F}_q$-rational point. We conclude that either ℓ_1, ℓ_2, ℓ_3 are all defined over $\mathbb{F}_q$, or ℓ_1, ℓ_2, ℓ_3 are galois-conjugate linear forms defined over $\mathbb{F}_{q^3}$ but not defined over $\mathbb{F}_q$.

If the former possibility held, C_g would have a nonsingular $\mathbb{F}_q$-rational point if any of the ℓ_i were distinct (again, a rational line has at least three rational points), so all C_{ℓ_i} must coincide. This accounts for case (iii) in the statement of the lemma. On the other hand, if the latter possibility holds, all C_{ℓ_i} are distinct, so $C_{\ell_1} \cap C_{\ell_2} \cap C_{\ell_3}$ consists of 3 points or 1 point, giving rise to cases (i) and (ii). □

The following is derived easily from Lemma 3.1.

Lemma 5.2. *Let K be a p-adic field and f a ternary anisotropic cubic form over K. Then either C_f is an absolutely irreducible curve of genus one, or there is a cubic extension U of K such that f is K-equivalent to the norm from U to K of a linear form normalized over U.*

Now we can give a description (up to equivalence over K) of all anisotropic ternary cubic forms over K.

Theorem 5.1. *Let f be an anisotropic ternary cubic form over K. Let F be the cubic unramified extension of K, S its ring of integers, and N denote the norm from F to K. Up to equivalence over K, f can be written as a polynomial over R of one of the following types:*

A) $N(\alpha x + \beta y + \gamma z) + \pi c(x, y, z)$, where c is a cubic form over R, and $\alpha, \beta, \gamma \in S$ reduce mod π to a basis of $S/\pi S$ over $R/\pi R$.

B)(1) $N(\alpha x + \beta y) + \pi z^3 + (\pi z) q(x, y, z)$,

B)(2) $\pi N(\alpha x + \beta y) + z3 + (\pi z) q(x, y, z)$,

where $q(x, y, z)$ is a quadratic form over R with no $z2$ term, and $\alpha, \beta \in S$ reduce mod π to elements which are linearly independent over $R/\pi R$.

C) $x^3 + \pi u y^3 + \pi^2 v z^3 + \pi x q(x, y, z) + \pi^2 w x z^2 + \pi^2 y z \ell(y, z)$, where u, v are units in R, and $q(x, y, z)$ is a quadratic form over R with no x^2 or z^2 term, $w \in R$, and ℓ is a linear form over R.

Conversely, any polynomial of one of these types is anisotropic over K.

Proof. The converse of the theorem is an easy exercise gotten by assuming that f has a non-trivial solution over K, where each coordinate is in R but not all are in πR, and then using valuation arguments to derive a contradiction. We now proceed with the proof of the forward direction.

CASE I: f factors over $\overline{K}$.

By Lemma 5.2, since f is anisotropic, it is K-equivalent to the norm of a normalized linear form ℓ from a cubic extension U of K. If $U = F$, then one can easily check that f is of type A. If U is ramified, with uniformizer Π,

then we can change coordinates over K so that ℓ is of the form $x + u\Pi y + v\Pi^2 z$, where u, v are units in the ring of integers of U, so then f is K-equivalent to a form of type C.

CASE II: C_f is absolutely irreducible.

Since f is anisotropic over K, Lemma 5.2 shows that C_f is a non-singular curve of genus 1. Hence $\Delta \neq 0$, and we can assume that f is minimal. In particular, $\overline{f}$ satisfies the hypotheses of Lemma 5.1.

CASE II(i): $\overline{f}$ satisfies condition (i) of Lemma 5.1.

Since the norm from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$ is surjective, $\overline{f}$ is the norm from $\mathbb{F}_{q^3}(x, y, z)$ to $\mathbb{F}_q(x, y, z)$ of a linear form ℓ which has no non-trivial $\mathbb{F}_q$-rational zeroes. It follows that ℓ is of the form $\delta x + \epsilon y + \zeta z$, where δ, ϵ, ζ form a basis for $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$. The residue field of F is $\mathbb{F}_{q^3}$, so we can lift δ, ϵ, ζ arbitrarily to elements α, β, γ of S, which reduce mod π to a basis of $S/\pi S$ over $R/\pi R$. Noting that N reduces mod π to the norm from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$, it follows that f is of Type (A).

CASE II(ii): $\overline{f}$ satisfies condition (ii) of Lemma 5.1 .

Now $\overline{f}$ is the product of 3 linear forms, each defined over $\mathbb{F}_{q^3}$ but not over $\mathbb{F}_q$, with an $\mathbb{F}_q$-rational point in common. There is an invertible linear change of variables of f over R that moves the intersection point of these 3 lines to $(0, 0, 1) \mod \pi$. Therefore without loss of generality, we can assume as above that $\overline{f}$ is the norm from $\mathbb{F}_{q^3}(x, y, z)$ to $\mathbb{F}_q(x, y, z)$ of the line $\gamma x + \delta y$, where $\gamma, \delta \in \mathbb{F}_{q^3}$ are linearly independent over $\mathbb{F}_q$. Applying Hensel's Lemma over F we can lift γ and δ to elements α and β of S so that $f(x, y, 0) = N(\alpha x + \beta y)$, and α, β reduce mod π to elements which are linearly independent over $R/\pi R$. Hence we can now write

$$f = N(\alpha x + \beta y) + \pi^{n_1} z q(x, y) + \pi^{n_2} z^2 \ell(x, y) + \pi^{n_3} v z^3,$$

where all $n_1, n_2, n_3 \geq 1$, q is a quadratic form and ℓ is a linear form over R. Note that $v \neq 0$ (since $(0, 0, 1)$ cannot be a K-rational point on f), so we can assume that n_3 is chosen so that v is a unit. Hence v is a norm from F, so dividing f by v and adjusting α and β we can assume without loss of generality that v is 1. We can assume that ℓ is normalized if it does not vanish. We will say that n_2 "does" or "does not" exist depending on whether ℓ is or is not non-vanishing. By minimality, (4) and (5) show that $h(x, y, z) = f(\pi x, \pi y, z)/\pi^3$ cannot be in $R[x, y, z]$. In other words, $n_3 < 3$, or n_2 exists and $n_2 = 1$. If $n_3 = 1$, f is of type (B)(1). So without loss of generality, now assume $n_3 \geq 2$, and let $i(x, y, z) = f(\pi x, \pi y, z)/\pi^2$. Then $\overline{i} \neq 0$ meets the hypotheses of Lemma 5.1. If $n_2 = 1$, then $\overline{i}$ is divisible by the rational line z, so by Lemma 5.1, must be a multiple of z^3. Hence $n_2 > 1$ (or does not exist), and $n_3 = 2$. Replacing f by the K-equivalent $i(x, y, z)$ makes it of type (B)(2).

CASE II(iii): $\overline{f}$ satisfies condition (iii) of Lemma 5.1.

Moreover, we will assume without loss of generality that there is no minimal form g over R which is K-equivalent to f such that $\overline{g}$ satisfies conditions (i) or (ii) of Lemma 5.1. Since $\overline{f}$ satisfies condition (iii) of Lemma 5.1, after multiplying f by a unit in R, there is an invertible linear change of variables over R such that we can write

$$f = x^3 + \pi^{n_1}x^2\ell(y,z) + \pi^{n_2}xq(y,z) + \pi^{n_3}c(y,z),$$

where all $n_i \geq 1$, and ℓ, q and c are respectively a linear, quadratic, and cubic form over R. If $c = 0$, C_f has a K-rational point, so $c \neq 0$ and we can assume n_3 has been chosen so that c is normalized.

By minimality, (4) and (5) show that $h = f(\pi x, y, z)/\pi^2$ cannot be in $R[x, y, z]$. Hence $n_3 = 1$. Then if $i = f(\pi x, y, z)/\pi$, $\overline{i}$ meets the hypotheses of Lemma 5.1, and by our assumptions, must satisfy condition (iii). Therefore $\overline{c}$ is a constant times the cube of a linear form over $\mathbb{F}_q$ in y and z.

Hence we can make an invertible linear change of the variables y and z over R after which we can assume without loss of generality that $\overline{c} = \overline{u}y^3$ for some unit u in R. Hence up to R-equivalence, f is of the form

$$x^3 + \pi uy^3 + \pi^{m_0}xy\lambda(x,y) + \pi^{m_1}xz\mu(x,y) + \pi^{p_1}yz\ell(y,z) + \pi^{m_2}txz^2 + \pi^{p_2}vz^3,$$

where each $m_i, p_i \geq 1$, u is a unit in R, $t, v \in R$, and λ, μ, ℓ are linear forms over R, which we may assume are normalized or vanish. Since $f(\pi x, y, z)/\pi$ is $\overline{u}y^3 \bmod \pi$, in fact we can take $p_1, p_2 \geq 2$. If t or v does not vanish, we can assume that it is a unit. Depending on whether either is or is not non-zero, we will say that the corresponding m_2 or p_2 "does" or "does not" exist.

Now let $h = f(\pi x, \pi y, z)/\pi^3$. As above, by minimality, (4) and (5) show we have $h \notin R[x, y, z]$, i.e., either m_2 exists and $m_2 = 1$, or p_2 exists and $p_2 = 2$. Then if $j = f(\pi x, \pi y, z)/\pi^2$, $\overline{j}$ meets the hypotheses of Lemma 5.1, so by our assumption must satisfy condition (iii) and be a constant times a cube, so must be $\overline{v}z^3$. Hence $p_2 = 2$, and $m_2 \geq 2$ or does not exist. Therefore v is a unit and f is of type (C). □

Note that Theorem 5.1 and its proof do not show that a given anisotropic ternary cubic form over K cannot be K-equivalent to two different types given in the classification (except for forms which factor non-trivially over $\overline{K}$, which we've seen are of type (A) or (C), depending whether they are constant multiples of norms of linear forms defined over unramified or ramified cubic extensions of K). For absolutely irreducible anisotropic ternary cubic forms, we can give a more canonical description of the types (A), (B)(1), (B)(2) and (C) in Theorem 5.1 that will make it clear that no such form is K-equivalent to two different types given in the classification.

We first note that forms of type (C) remain anisotropic over F, whereas by Hensel's Lemma, forms of type (A) do not. Furthermore, taking $z = 0$

and applying Hensel's Lemma show that forms of type (B)(1), and (B)(2) do not remain anisotropic over F. This gives a way to see that forms of type (C) cannot be K-equivalent to forms of other types. We now need a canonical way to distinguish between forms of types (A), (B)(1), and (B)(2).

We will use the vector of associated polynomials to do this. For an absolutely irreducible anisotropic ternary cubic form f over K, via Tate's algorithm [28], they will allow us to compute the Kodaira symbol of the reduction type of a minimal Weierstrass model for the jacobian E of C_f, and we will show that E has a different reduction type depending on whether f is of the form (A), (B)(1), or (B)(2). We conclude that the absolutely irreducible forms of types (A), (B)(1), (B)(2), and (C) are all K-inequivalent.

We now arrive at our final classification theorem.

Theorem 5.2. *Let the field K be a finite extension of $\mathbb{Q}_p$, and F the cubic unramified extension of K. Then a 3-dimensional non-associative division algebra over K is either isotopic to a generalized twisted field over K or over a quadratic extension of K, or has a left (and right) determinant which is an absolutely irreducible anisotropic ternary cubic form f over K. This form is K-equivalent to one of type (C) of Theorem 5.1 if it remains anisotropic over F, and if not, is K-equivalent to one of type (A), (B)(1), or (B)(2) of Theorem 5.1, depending on whether the reduction type of the Néron model of the jacobian of C_f is respectively of (split) multiplicative type, or additive type with Kodaira symbols IV or IV*.*

Proof. We've shown everything except the last sentence. Let R and S be as in Theorem 5.1. Let f be an absolutely irreducible anisotropic ternary cubic form over K, and E be the jacobian of C_f. Since the reduction type of E is unchanged under unramified field extension, and is invariant under change of variables for f, we can use the fact that over F a form of type (A) is equivalent to one of the shape

$$xyz + \pi c(x, y, z),$$

where c is a cubic form over S. Likewise, over F we see that forms of type (B)(1) and (B)(2) are respectively equivalent to those of the shape

$$xy(ux + vy) + \pi z^3 + \pi z q(x, y, z),$$

and

$$z^3 + \pi xy(ux + vy) + \pi z q(x, y, z),$$

where u, v are units in S, and q is a quadratic form over S. Computing associated polynomials and applying Tate's Algorithm, we get the following table of Kodaira symbols of E:

Type of F	$v(a_1)$	$v(a_2)$	$v(a_3)$	$v(a_4)$	$v(a_6)$	$v(\Delta)$	Kodaira symbol
(A)	1	≥ 2	≥ 3	≥ 4	≥ 3	$n \geq 3$	I_n
(B)(1)	≥ 1	≥ 1	1	≥ 2	≥ 3	> 0	IV
(B)(2)	≥ 1	≥ 2	2	≥ 3	≥ 5	>0	IV^*

Note that for f of type (A), the polynomial $T^2+a_1T-a_2$ has two distinct roots mod π, so by Hensel's Lemma, has two distinct roots in R. Hence E has split multiplicative reduction. For f of type (B)(1) or (B)(2), E has additive reduction. □

Remark.

1) The proof of Theorem 5.2 is computational. It would be nice to have a conceptual explanation of how the geometry of C_f as a scheme over R is reflected in the reduction type of the Néron model of E over R.

2) Fisher ([17], Theorem 4.7) gives an algorithm for computing a minimal model for any ternary cubic form over K with a non-trivial point over K. See also the comprehensive [10].

References

[1] A. A. Albert, *Non-associative algebras I: Fundamental concepts and Isotopy.* Ann. of Math. **43** (1942), 685–707.

[2] A. A. Albert, *On Nonassociative Division Algebras.* Trans. Amer. Math. Soc. **72** (1952), 296–309.

[3] A. A. Albert, *Generalized Twisted Fields.* Pac. J. Math. **11** (1961), 1–8.

[4] S. An, S. Kim, D. Marshall, S. Marshall, W. McCallum, and A. Perlis, *Jacobians of Genus One Curves.* J. Number Theory **90** (2001), 304–315.

[5] M. Artin, F. Rodriguez-Villegas, and J. Tate, *On the jacobians of plane cubics.* Adv. Math. **198** (2005), 366–382.

[6] A. Beauville, *Determinental hypersurfaces.* Mich. Math. J. **48** (2000), 39–64.

[7] M. Bilioti, V. Jha, and N. L. Larson, *Foundations of Translation Planes.* Marcel Dekker, New York, 2001.

[8] Jeff Biggus, *Sketching the history of hypercomplex numbers.* Available at `http://history.hyperjeff.net/hypercomplex`

[9] J. V. Chipalkatti, *Decomposable ternary cubics.* Experiment. Math. **11** (2002), 69–80.

[10] J. E. Cremona, T. A. Fisher, and M. Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves.* J. Algebra & Number Theory. **4** (2010), 763–820.

[11] A. Deajim, *On Non-Associative Division Algebras Arising from Elliptic Curves.* Ph.D. thesis, University of Colorado at Boulder, 2006.

[12] A. Deajim and D. Grant, *Space Time Codes and Non-Associative Division Algebras Arising from Elliptic Curves.* Contemp. Math. **463** (2008), 29–44.

[13] A. Deajim, D. Grant, S. Limburg, and M. K. Varanasi, *Space-time codes constructed from non-associative division algebras.* in preparation.

[14] L. E. Dickson, *Linear algebras in which division is always uniquely possible.* Trans. Amer. Math. Soc. **7** (1906), 370–390.

[15] L. E. Dickson, *On triple algebras and ternary cubic forms.* Bull. Amer. Math. Soc. **14** (1908), 160–168.

[16] T. A. Fisher, *Testing equivalence of ternary cubics.* in "Algorithmic number theory," F. Hess, S. Pauli, M. Pohst (eds.), Lecture Notes in Comput. Sci., Springer, **4076** (2006), 333-345.

[17] T. A. Fisher *A new approach to minimising binary quartics and ternary cubics*. Math. Res. Lett. **14** (2007), 597–613.
[18] W. Fulton, *Algebraic Curves*. W. A. Benjamin, New York, 1969.
[19] I. Kaplansky, *Three-Dimensional Division Algebras II*. Houston J. Math. **1**, No. 1 (1975), 63–79.
[20] S. Lichtenbaum, *The period-index problem for elliptic curves*. Amer. J. Math. **90**, No. 4 (1968), 1209–1223.
[21] G. Menichetti, *On a Kaplansky Conjecture Concerning Three-Dimensional Division Algebras over a Finite Field*. J. Algebra **47**, No. 2 (1977), 400-410.
[22] G. Menichetti, *n-Dimensional Algebras over a Field with Cyclic Extension of Degree n*. Geometrica Dedicata **63** (1996), 69–94.
[23] J. S. Milne, *Weil-Châtelet groups over local fields*. Ann. scient. Éc. Norm. Sup., 4th series. **3**, (1970), 273–284.
[24] G. Salmon, *Higher Plane Curves*. 3rd ed., reprinted by Chelsea, New York, 1879.
[25] R. Schafer, *An Introduction to Nonassociative Division Algebras*. Dover Publications, New York, 1995.
[26] J-P. Serre, *Local Fields*. GTM **67**, Springer-Verlag, New York, 1979.
[27] J. Silverman, *The Arithmetic of Elliptic Curves*. GTM **106**, Springer-Verlag, New York, 1986.
[28] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. GTM **151**, Springer-Verlag, New York, 1994.
[29] V. Tarokh, N. Seshadri, and A. Calderbank, *Space-time block codes for high data rate wireless communications*. IEEE Trans. Inf. Theory **44**, No. 2 (1998), 744–765.

Abdulaziz Deajim
Department of Mathematics
King Khalid University
P.O. Box 9004
Abha, Saudi Arabia
E-mail: deajim@gmail.com

David Grant
Department of Mathematics
University of Colorado at Boulder
Boulder, Colorado 80309-0395, USA
E-mail: grant@colorado.edu