Small Non-Associative Division Algebras up to Isotopy

Thomas Schwarz, S.J.[1]

[1] Department of Computer Engineering, Santa Clara University

500 El Camino Real, Santa Clara, CA 95053, USA

tjschwarz@scu.edu

1 Introduction

Assume a distributed database consisting of a large number of objects that can be created, deleted, and modified by manipulations. We want to capture the state of the system in a very small bit-string (a *signature* as in [2]). We now hash (map) the set of all possible manipulations into a finite, non-associative algebra. We can capture the state of an object also in a signature, an element in that algebra, initially 1. Whenever a manipulation changes an object, we multiply the current signature of the object with the signature of the manipulation. Since there are frequent manipuliations that change a large number of objects in a given set (such as increasing the salary of all objects representing faculty), the distributive law becomes useful. The state of the database is given as the sum of the signatures of all objects. Since manipulations do not commute, the finite algebra made up of all possible (non-zero) signatures needs to be non-communative, thus, it also needs to be non-associative. Furthermore, the algebra should be a *division algebra,* i.e. a vector space over a finite field with a multiplication such that the left multiplication of non-zero elements is invertible. A simple way to come up with candidate algebras is to use the isotope of a Galois field $\mathcal{GF}(2^k)$.

The concept of isotopy goes back to A. A. Albert [1]. Our application leads to the mathematical question on the classification of finite algebras up to isotopy. Finite algebras of dimension two are isotopes of Galois fields. Few work seems to have been done in this area, an exception being [3, 4]. In this article, we present a classification for algebras with 8, 16, and 27 elements. To do so, we reduce the number of possibilities using elementary mathematical arguments and then use software for a final, brute force calculation. The vast majority of the work presented here is spent verifying the software, while the actual programs run fast. Due to a combinatorial explosion, obtaining similar results for larger algebras is currently computationally infeasible. The limiting factor is the size of main memory and the much slower performance of hard drives which leads to runtimes of months and years regardless of parallelization. Further mathematical insight is needed here. Because of the bit-based nature of current computing, results in characteristic 2 are especially valuable.

2 Definition and Basic Properties

Definition 1. *A non-associative division algebra $\mathcal{A}$ over a field Φ is a non-associative division algebra such that for every element $a \neq 0$, the left-multiplication $L_a : \mathcal{A} \to \mathcal{A}$, $x \mapsto a \cdot x$ is a bijection.*

Definition 2. *Let f, g, and h be vector space automorphisms of a non-associate* *division algebra $\mathcal{A}$. The (f, g, h) isotope of a (non-associative) algebra $(\mathcal{A}, \cdot)$ is the same algebra $(\mathcal{A}, \star)$ with a new multiplication defined by $x \star y := h^{-1}(f(x) \cdot g(x))$.*

Isotopy is an equivalence relation. Obviously, an isotope of a division algebra is also a division algebra. A finite-dimensional algebra is a division algebra if and only if the equation $x \cdot y = 0$ implies that x or y are zero. Thus, we can equivalently identify finite dimensional division algebras through the right multiplication.

2.1 Existence of Unity

If $\mathcal{A}$ is a division algebra with left multiplication L and $a \in \mathcal{A}$ is not zero, then a is a left one in the isotope with left multiplication $\hat{L}_x = L_a^{-1} \circ L_x$. With a little bit more work, we can find an isotope with a (left and right) one. Assume that $a \in \mathcal{A}$ is a left one. Form the isotope with left multiplication $\hat{L}_x = R_a^{-1} \circ L_x \circ R_a$. Clearly, a is still a left one in this isotope, but it is also a right one because $x \star a$ $= R_a^{-1}(x(aa)) = x$. This important observation is due to Kaplansky, but seems to be unpublished (according to H. Petersson, Hagen).

2.2 Isotopes of Fields

Assume that $(\mathcal{A}, \cdot)$ is a field with one 1. Assume that its (f, g, h)-isotope $(\mathcal{A}, \star)$ has a one e. This implies $h = L_{g(e)} \circ f$ and $g = L_{g(e)/f(e)} \circ f$. In particular, we have the identity $f(a \star b) = h^{-1}\left(\frac{g(e)f(a)f(b)}{f(e)}\right)$. From this, it follows that $(\mathcal{A}, \star)$ is associative. Thus:

Proposition 1. *An isotope of a field that has a one is also a field.*

3 $\mathcal{GF}(3)^3$

We start out with a base $\mathcal{B}$ consisting of a one 1 and two elements x, y of $\mathcal{GF}(3)^3$. Obviously

$$\mathrm{Mat}_{\mathcal{B}}(L_x) = \begin{pmatrix} 0 & a & b \\ 1 & c & d \\ 0 & e & f \end{pmatrix}$$

with scalars a, b, c, d, e, $f \in \mathcal{GF}(3)$. In addition, we know that all linear combinations of the identity matrix and L_x are invertible. Replacing x' by $\alpha \cdot 1 + \beta \cdot x$ in $\mathcal{B}$ changes this matrix to

$$\mathrm{Mat}_{\mathcal{B}}(L_{x'}) = \begin{pmatrix} 0 & \beta^2 a - \alpha^2 - \alpha\beta c & \beta b - \alpha d \\ 1 & 2\alpha + \beta c & d \\ 0 & \beta^2 e & \alpha + \beta f \end{pmatrix}$$

To form a division algebra, all non-trivial linear combinations of the identity matrix and L_x have to be invertible. A computerized brute force calculation reveals that the set of possible left multiplications with the x has 24 equivalence classes. $A \cdot L_x \cdot A^{-1}$ is the left multiplication matrix with respect to the same base in the (A, id, A^{-1})-isotope of the original algebra. Accordingly, we introduce a further equivalence relation on the set of all possible left multiplications of the above form that now only has 5 equivalence classes. That is, we can assume without loss of generality and up to isotopy that L_x is one of the following matrices:

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

The choice of these particular matrices is an artifact of the enumeration of matrices in our program. Similarly,

$$\mathrm{Mat}_{\mathcal{B}}(L_y) = \begin{pmatrix} 0 & a & b \\ 0 & c & d \\ 1 & e & f \end{pmatrix}$$

with (different) scalars a, b, c, d, e, $f \in \mathcal{GF}(3)$. Replacing y by $y' = \alpha \cdot 1 + \beta \cdot y$ in $\mathcal{B}$ changes this matrix to

$$\mathrm{Mat}_{\mathcal{B}}(L_{y'}) = \begin{pmatrix} 0 & \beta a - \alpha e & -\alpha^2 + \beta^2 b - \alpha\beta f \\ 0 & \alpha + \beta c & \beta^2 d \\ 1 & e & 2\alpha + \beta f \end{pmatrix}$$

This gives of course again 24 equivalence classes of matrices. Taking the identity matrix, a matrix from the first list, and a matrix from the second list defines a non-associative algebra. However, it turns out that only 10 of them are division algebras. A final brute force calculation reveals that all these algebras are isotopes.

4 Algebras of size 4, 8, 16

In the case of four elements, we can use elementary case distinctions:

Proposition 2. *GF(4) is the only division algebra with unity 1 over GF(2) such that every sub-algebra generated by* 1 *and an arbitrary element* x *has dimension at most 2.*

Proof: Since L_x is invertible for $x \neq 0$, $x^2 = x$ implies either that $x = 1$ or that $x = 0$. If every sub-algebra generated by 1 and x has dimension at most 2, and $x \neq 0, 1$, then $x^2 = x + 1$. If x and y are linearly independent and not equal to 1, we can apply this equation to $x+y$ and obtain $xy = yx+1$. Finally, if we apply this last equation to three linearly independent elements x, y, and z, neither of which equal 1, we obtain $(x+y+z)^2 = (x+y+z)$, which is a contradiction. Hence, the dimension of such an algebra cannot exceed 3. However, as we will see, it can also not have dimension 3. For assume a basis $(1, x, y)$. Since x already has inverse $1+x$, the product xy cannot equal 1. $xy = x$ implies $y = 1$, a contradiction, and $xy = 1+x$ means $yx = x$, also a contradiction. Hence we remain with $xy = x+y$ or $yx = x+y$. In the first case, $(1+x)(1+x+y) = 0$ and in the second $(1+x+y)(1+x) = 0$, a contradiction. Hence, such an algebra can only have dimension 2, must have a base $(1, x)$ with $x^2 = 1+x$, i.e. must be GF(4).

Proposition 3. *The only division algebras over GF(2) of dimension 3 are isotopes of GF(8).*

Proof: According to Proposition 2, there exists an element x such that $1, x, x^2$ are linearly independent. With respect to this base, the matrix representation of the left multiplications L_1, L_x, and L_{x^2} are given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & * \\ 1 & 0 & * \\ 0 & 1 & * \end{pmatrix}, \begin{pmatrix} 0 & * & * \\ 0 & * & * \\ 1 & * & * \end{pmatrix}.$$

This gives us 2^9 possible algebras. Many are not division algebras and we can apply Proposition 1 to ascertain that those that are are indeed fields. Alternatively, we can find an explicit isotopy relationship to $\mathcal{GF}(8)$. In both cases, a brute force calculation proves the theorem.

Recall that the *opposite* algebra A^{op} of an algebra A (with multiplication $\cdot$) is the same vectorspace, but a new multiplication defined by $x \cdot_{\mathrm{op}} y = y \cdot x$.

Theorem 1. *There are three isotopy classes among the division algebras of dimension* 4 *over* $\mathcal{GF}(2)$*. One class contains* $\mathcal{GF}(2^4)$*, and any of the other two classes contains the opposite algebras of the remaining class. contains the opposite algebras of the other.*

Proof: We classify these division algebras using the matrix representation of the left multiplications with respect to a chosen basis. For convenience of presentation, we encode a column vector ${}^t(b_1, b_2, b_3, b_4)$ with coefficients in $\{0, 1\}$ as the hexadecimal digit $b_1 * 8 + b_2 * 4 + b_3 * 2 + b_4 * 1 \in \{0, 1, \ldots, 9, a, \ldots f\}$. Because of Proposition 2, any four-dimensional division algebra over $\mathcal{GF}(2)$ contains an element x such that $1, x, x^2$ are linearly independent. Assume that $x^3 := x \cdot x^2$ is in the linear span $< 1, x, x^2 >$ of $1, x, x^2$. We expand $1, x, x^2$ to a basis of the algebra and have with respect to this base

$$L(x) = \begin{pmatrix} 0 & 0 & * & * \\ 1 & 0 & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 0 & * \end{pmatrix}$$

and either $L(x)$ or $L(x+1)$ is not invertible. Therefore, $1, x, x^2, x^3$ is a base. With respect to this base, the matrix for $L(x)$, $L(x^2)$, and $L(x^3)$ respectively must have the form

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}, \begin{pmatrix} 0 & * & * & * \\ 0 & * & * & * \\ 1 & * & * & * \\ 0 & * & * & * \end{pmatrix}, \begin{pmatrix} 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 1 & * & * & * \end{pmatrix}.$$

The small number of possibilities (2^{28}) allows us to use computer software to determine the isotopy classes. To keep the runtime under control, we first generate a list of all invertibe 4 by 4 matrices. We use this list to decide for each possible assignments of the free variables (the stars in the preceeding equation) whether the resulting algebra is a division algebra. This gives us 178 division algebras. We then determine isotopy classes by identifying in a first pass whether for $\mathbf{X} \in \mathbf{GL}(4)$ and algebras A and A' we have

$$\mathbf{X}\{L(a)|a \in A\}\mathbf{X}^{-1} = \{\mathbf{X}L(a)\mathbf{X}^{-1}|a \in A\} = \{L'(a')|a' \in A'\}$$

This leaves us with 6 equivalence classes under this relation with finer equivalency classes. Our second, much more compute-intensive pass then uses a brute force enumeration of all pairs of invertible matrices $\mathbf{X}$ and $\mathbf{Y}$ whether

$$\mathbf{X}\{L(a)|a \in A\}\mathbf{Y} = \{L'(a')|a' \in A'\}$$

This leaves exactly three equivalence classes. One has representative $\mathcal{GF}(16)$, the other ones are given by $L(1)$, $L(x)$, $L(x^2)$, and $L(x^3)$ equal to (8421, 4219, 21f5, 1a87) and (8421, 4219, 2945, 15f3). It turns out that the latter two algebras are opposite algebras of each other.

I have not succeeded in proving or disproving that the only division algebras of dimension 3 over a field $\mathcal{GF}(p)$, p a prime, are isotopes of fields and leave it as a conjecture.

References

[1] A. A. Albert, *Nonassociative Algebras.* I, Annals of Mathematics, **43** (1942), p. 685-707.

[2] W. Litwin and T. Schwarz. *Algebraic Signatures for Scalable Distributed Data Structures.* Proceedings of the 20th International Conference on Data Engineering (ICDE), Boston, 2004.

[3] R. H. Oehmke and R. Sandler. *The collineation group of division ring planes. I. Jordan algebras.* Journal f. Reine und Angewandte Mathematik, **216** (1964), p. 67-87.

[4] H. P. Petersson. *Isotopism of Jordan Algebras.* Proceedings of the American Mathematical Society. **20**(2), (1969), p. 477 - 482.