

José Antonio Cuenca · Alberto Elduque · José María Pérez-Izquierdo

Power associative composition algebras

Received: 1 February 2000

Abstract. Composition algebras of arbitrary dimension over a field and satisfying the identities $x^2x = xx^2$ and $(x^2)^2 = (x^2x)x$ are shown to be precisely the well-known unital composition algebras, with the exception of three two dimensional algebras over the field of two elements.

1. Introduction and main result

A nonassociative (i.e. not necessarily associative) algebra over a field F is said to be a *composition algebra* if it is equipped with a nondegenerate quadratic form (the norm)

$$n : A \longrightarrow F$$

such that

$$n(xy) = n(x)n(y) \tag{1}$$

for any $x, y \in A$. The form being nondegenerate means that if the associated bilinear form is given by

$$n(x, y) = n(x + y) - n(x) - n(y),$$

then $\{x \in A : n(x) = n(x, A) = 0\} = 0$.

The norm is said to be strictly nondegenerate if $A^\perp = \{x \in A : n(x, A) = 0\} = 0$. In case the characteristic of F is not two, $n(x) = \frac{1}{2}n(x, x)$ and both concepts agree.

J. A. Cuenca: Departamento de Algebra, Geometría y Topología, Universidad de Málaga, 29080 Málaga, Spain

A. Elduque: Departamento de Matemáticas y Computación, Universidad de La Rioja, 26004 Logroño, Spain.

Present address: Departamento de Matemáticas, Universidad de Zaragoza, 50009 Zaragoza, Spain. e-mail: elduque@posta.unizar.es

J. M. Pérez-Izquierdo: Departamento de Matemáticas, Universidad de Zaragoza, 50009 Zaragoza, Spain.

Present address: Departamento de Matemáticas y Computación, Universidad de La Rioja, 26004 Logroño, Spain

Mathematics Subject Classification (2000): Primary 17A75; Secondary 17A05

Composition algebras with a unit element constitute a well known class of algebras (see [K 53], [ZSSS 82, Chapter 2] and the references therein). Either their norm is strictly nondegenerate, so that they are the classical Hurwitz algebras of dimension 1, 2, 4 or 8, or the characteristic is 2, $A^\perp = A$ and A is a purely inseparable field extension of exponent one of the ground field F , with $x^2 = n(x)1$ for any $x \in A$.

However, if the existence of a unit element is dropped, infinite dimensional algebras may appear even in characteristic different from 2 (see [U-W 60] for the first examples, [C 92, RP 92, E-P 97] for examples with one-sided unit, and [E-M 93] for commutative examples).

On the other hand, non unital composition algebras satisfying some other conditions have been studied recently. Among these, the associativity of the bilinear form, that is,

$$n(xy, z) = n(x, yz) \quad (2)$$

for any x, y, z , is particularly noteworthy. The composition algebras satisfying (2) are called *symmetric composition algebras* (see [KMRT 98]) and were classified in [E-M 93] over fields of characteristic $\neq 2, 3$ (although the arguments there can be extended to cover the characteristic 2 – see also [KMRT 98, M 94, O-O 81] –) and in [E-P 96, E 97] over arbitrary fields. Identity (2) is equivalent to

$$(xy)x = x(yx) = n(x)y \quad (3)$$

for any x, y . In particular these algebras are flexible ($(xy)x = x(yx)$) and finite dimensional, because for any $x \in A$ with $n(x) \neq 0$ the left and right multiplications by x are bijections (see [K 53]).

Any finite dimensional flexible composition algebra over a field of characteristic $\neq 2$ satisfies (2), as shown in [O 82], and the same happens, if the characteristic is restricted to be $\neq 2, 3$, if only the third power associativity ($x^2x = xx^2$) is required, by [E-P 94], but the infinite dimensional commutative examples in [E-M 93], mentioned above, show that in general (3) does not follow from flexibility. Finally, finite dimensional power associative (that is, the subalgebra generated by any element is associative) composition algebras have been studied in [O 81, P 94, E-P 94]. The most general result known about these algebras is that the finite dimensional composition algebras over fields of characteristic $\neq 2$ satisfying the conditions

$$x^2x = xx^2 \quad \text{and} \quad x^2x^2 = (x^2x)x, \quad (4)$$

(and in particular the finite dimensional power associative composition algebras over these fields) are Hurwitz algebras ([E-P 94, Theorem B]). It must be remarked that the condition (4) implies the power associativity over fields of characteristic zero ([A 48, Lemma 3]).

The purpose of this paper is to prove that the conditions given in (4) for a composition algebra, are sufficient to force them to be unital (and hence Hurwitz algebras if the norm is strictly nondegenerate), with only three exceptions over the field of two elements. No assumption on the dimension and on the field will be

assumed. The proof does not rely on previous works mentioned above on composition algebras with some weak associativity conditions, and simplifies drastically some of those works. Actually, with the exception of the fields of two and three elements the proof is quite straightforward.

Over the real field, if the norm n is substituted by a topological norm, the class of absolute valued algebras is obtained. For these algebras it was already proved by El-Mallah and Micali ([EM-M 80]) that the power associativity (which is equivalent to (4) since the characteristic is zero) implies the existence of a unit element, and this forces the algebra to be one of the Hurwitz division algebras.

In order to state the main result of the paper we need to consider new composition algebras built up from Hurwitz algebras. Given a Hurwitz algebra A of dimension at least 2 with norm n , multiplication denoted by juxtaposition and standard conjugation $x \mapsto \bar{x} = n(x, 1)1 - x$, then new algebras (A, \cdot) with $x \cdot y$ equal either to

$$\text{i) } \bar{x}y, \quad \text{ii) } x\bar{y} \quad \text{or} \quad \text{iii) } \bar{x}\bar{y},$$

are again composition algebras relative to the same quadratic form n . The last one is called the para-Hurwitz algebra associated to A . The algebra in i) (respectively ii)) will be called the *left* (respectively *right*) composition algebra associated to A .

Recall also that over any field F and for any dimension 2, 4 or 8 there exists a unique Hurwitz algebra whose form is isotropic. In dimension 2 this is the algebra $F \oplus F$ with componentwise multiplication and norm given by $n(\alpha, \beta) = \alpha\beta$. The Hurwitz algebras of dimension 2 over F are either the split one or the quadratic separable field extensions of F . In particular, over the field of two elements \mathbb{F}_2 there are exactly, up to isomorphism, two two-dimensional Hurwitz algebras: $\mathbb{F}_2 \oplus \mathbb{F}_2$ (split) and \mathbb{F}_4 (the field of four elements, considered as an algebra over \mathbb{F}_2).

Now we can state the main result that will be proved in this paper:

Main Theorem. *Let A be any composition algebra over a field F satisfying (4). Then A is power-associative. Moreover, either A is unital or $F = \mathbb{F}_2$ and A is, up to isomorphism, one of the following:*

- i) *the left or right composition algebra associated to $\mathbb{F}_2 \oplus \mathbb{F}_2$.*
- ii) *the para-Hurwitz algebra associated to \mathbb{F}_4 .*

Notice that if $e_1 = (1, 0)$, $e_2 = (0, 1)$ and $e = e_1 + e_2 = (1, 1)$ in $\mathbb{F}_2 \oplus \mathbb{F}_2$, then $\bar{e}_1 = e_2$, $\bar{e}_2 = e_1$ and the multiplication of these elements in the left composition algebra associated to $\mathbb{F}_2 \oplus \mathbb{F}_2$ gives

$$e_1 \cdot e_1 = e_2 e_1 = 0 = e_2 \cdot e_2 \quad \text{and} \quad e \cdot e = e^2 = e,$$

so that this algebra is clearly power-associative and the same happens with the right counterpart. Besides, $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ with $\omega^2 = \omega + 1$ and thus, in the para-Hurwitz algebra associated to \mathbb{F}_4 , we have

$$1 \cdot 1 = 1, \quad \omega \cdot \omega = (1 + \omega)^2 = 1 + 2\omega + \omega^2 = \omega, \quad \text{and} \quad (1 + \omega) \cdot (1 + \omega) = \omega^2 = 1 + \omega.$$

Hence all the elements are idempotents and this algebra is then trivially power-associative.

The fact that this latter algebra is the only power-associative symmetric composition algebra appears as an exercise in [KMRT 98, Chapter VIII], but this exercise can be done (and should be done) more easily without appealing to the Theorem above.

The paper is organized as follows. The next section will state a crucial identity satisfied by those composition algebras verifying (4), which implies that the dimension of the subalgebra generated by any nonisotropic element is at most two. Then it will be proved that any such composition algebra is unital, provided that the ground field has at least four elements. Thus we will be left with the fields of two and three elements: \mathbb{F}_2 and \mathbb{F}_3 . Over \mathbb{F}_3 the third section will show that no other composition algebras, besides the unital ones, satisfy (4) and, finally, the last section will be devoted to the more difficult case of the field of two elements.

2. The crucial identity and consequences

If A is a composition algebra over a field F with norm n , then the linearization of (1) immediately gives

$$n(xy, xz) = n(x)n(y, z) = n(yx, zx) \quad (5)$$

and

$$n(xy, tz) + n(ty, xz) = n(x, t)n(y, z) \quad (6)$$

for any $x, y, z, t \in A$.

These linearizations are all we need to prove the crucial identity:

Proposition 1. *Let A be a composition algebra with norm n satisfying (4). Then for any $x \in A$:*

$$n(x)x^3 - n(x, x^2)x^2 + n(x)^2x = 0. \quad (7)$$

Notice that, because of (4), it makes sense to write $x^3 (= x^2x = xx^2)$.

Proof. For any $x, y \in A$ and because of (4), (5) and (6):

$$\begin{aligned} & n\left(n(x)x^3 - n(x, x^2)x^2 + n(x)^2x, y\right) \\ &= n(x^3x, yx) - n(x, x^2)n(x^2, y) + n(x^3, yx^2) \\ &= n(x^2x^2, yx) - (n(x^2x, yx^2) + n(x^2x^2, yx)) + n(x^3, yx^2) \\ &= 0 \end{aligned}$$

and

$$\begin{aligned}
& n\left(n(x)x^3 - n(x, x^2)x^2 + n(x)^2x\right) \\
&= n(x)^2n(x^3) + n(x, x^2)^2n(x^2) + n(x)^4n(x) \\
&\quad - n(x)n(x, x^2)n(x^3, x^2) + n(x)^3n(x^3, x) - n(x, x^2)n(x^2)n(x^2, x) \\
&= 2n(x)^5 - n(x)^2n(x, x^2)^2 + n(x)^3n(x^3, x) \\
&= n(x)^2\left(2n(x)^3 - n(x, x^2)^2 + n(x)n(x^3, x)\right) \\
&= n(x)^2\left(2n(x)^3 - \left(n(x, x^2)n(x^2, x) - n(x^3x, x^2)\right)\right) \\
&= n(x)^2\left(2n(x)^3 - \left(n(x, x^2)n(x^2, x) - n(x^2x^2, x^2)\right)\right) \\
&= n(x)^2\left(2n(x)^3 - n(x, x^2)x^2\right) \quad \text{by (6)} \\
&= n(x)^2\left(2n(x)^3 - n(x^3, x^3)\right) = 0.
\end{aligned}$$

Since the quadratic form n is nondegenerate, (7) follows. \square

By applying the linear form $n(x, -)$ to identity (7) we get:

$$n(x)(n(x^3, x) + 2n(x)^2) = n(x, x^2)^2. \quad (8)$$

Now assume that A is a composition algebra with norm n over a ground field F which satisfies (4). If F is finite of characteristic two, then the restriction $n|_{A^\perp} : A^\perp \rightarrow F$ is a one-to-one semilinear map relative to the Frobenius automorphism $F \rightarrow F$, $\alpha \mapsto \alpha^2$. Hence the dimension of A^\perp is at most one and if K is any infinite field containing F , the extension of the norm n to $K \otimes_F A$ verifies that $(K \otimes_F A)^\perp (= K \otimes_F A^\perp)$ has dimension at most one over K , so that n remains nondegenerate.

Hence, if we assume also that F contains at least four elements, the linearizations of the identities in (4) are also valid in A and thus we may extend scalars if F is finite. Therefore, we may assume that the field F is infinite and that the dimension of A is at least 2 (otherwise A is trivially unital).

Then, in any finite dimensional subspace B of A , of dimension at least two, such that the restriction of n to B is nondegenerate, $n(x)$ is given by a homogeneous polynomial of degree two, which by nondegeneracy is either irreducible or the product of two different irreducible polynomials. In any case, (8) and unique factorization of polynomials imply the existence of a linear map $\alpha_B : B \rightarrow F$ such that

$$n(x, x^2) = \alpha_B(x)n(x)$$

for any $x \in B$.

But if B_1 and B_2 are two such finite dimensional subspaces of A with $B_1 \subseteq B_2$, since there are no zero divisors in the polynomial functions on B_1 (F is infinite), it is clear that α_{B_1} is the restriction to B_1 of α_{B_2} . As a consequence there is a unique linear map $\alpha : A \rightarrow F$ with

$$n(x, x^2) = \alpha(x)n(x) \quad (9)$$

for any $x \in A$, and by linearization, for any $x, y \in A$:

$$n(x, x \circ y) + n(y, x^2) = \alpha(y)n(x) + \alpha(x)n(x, y), \quad (10)$$

where $x \circ y = xy + yx$.

Now, if e is a unitary idempotent of A ; that is, $e^2 = e$ and $n(e) = 1$, then (9) gives $\alpha(e) = n(e, e) = 2$, and by (10)

$$\begin{aligned} \alpha(y) + 2n(e, y) &= n(e, e \circ y) + n(e, y) \\ &= n(e^2, ey) + n(e^2, ye) + n(e, y) \\ &= n(e, y) + n(e, y) + n(e, y) = 3n(e, y), \end{aligned}$$

where we have used (5). Therefore $\alpha(y) = n(e, y)$ for any $y \in A$, that is, for any $x \in A$

$$n(x, x^2) = n(e, x)n(x). \quad (11)$$

In case n is strictly nondegenerate, this implies that at most there is a unitary idempotent in A .

But for any $x \in A$ with $n(x) \neq 0$, (7) and (9) imply

$$x^3 - \alpha(x)x^2 + n(x)x = 0,$$

so

$$(\alpha(x)x - x^2)x = n(x)x = x(\alpha(x)x - x^2),$$

and the element

$$e = \frac{1}{n(x)}(\alpha(x)x - x^2)$$

verifies $ex = xe = x$, so that $n(e) = 1$, and also $ex^2 = (ex)x = x^2 = x^2e$ by (4). Since the subalgebra generated by x is the span of x and x^2 by Proposition 1, it follows that e is the identity of this subalgebra. In particular it is a unitary idempotent of A .

Hence, if n is strictly nondegenerate, there exists a unique unitary idempotent e in A and $ex = xe = x$ for any $x \in A$ with $n(x) \neq 0$. Since any element in A can be written as a sum of elements with nonzero norm, it follows that e is the identity element of A .

Otherwise the characteristic of F is two and there is a nonzero element $a \in A^\perp$. As above, $e = \frac{1}{n(a)}a^2$ is a unitary idempotent with $ea = ae = a$, so

$$n(e, A) = \frac{1}{n(a)}n(a)n(e, A) = \frac{1}{n(a)}n(ae, aA) = \frac{1}{n(a)}n(a, aA) = 0,$$

because $a \in A^\perp$. Thus $e \in A^\perp$ too and now (11) implies that $n(x, x^2) = 0$ for any $x \in A$ and that all the unitary idempotents of A belong to A^\perp . Again, for any $y \in A$ with $n(y) \neq 0$, $f = \frac{1}{n(y)}y^2$ is a unitary idempotent of A , hence $f \in A^\perp$ and

$$n(y, A) = \frac{1}{n(y)}n(y)n(y, A) = n\left(\frac{1}{n(y)}y^2, Ay\right) = n(f, Ay) = 0,$$

so $y \in A^\perp$ for any $y \in A$ with $n(y) \neq 0$. It follows that $A = A^\perp$. Hence as in [K 53] $n : A \rightarrow F$ is a one-to-one ring homomorphism, so there is a unique $e \in A$ with $n(e) = 1$ and since $n(ex) = n(xe) = n(x)$, it follows that $ex = xe = x$ for any x and A is unital in this case too.

Therefore we have proved the next result:

Proposition 2. *Let A be any composition algebra satisfying (4) over a field F containing at least four elements. Then A is unital.*

This proves our Theorem over any field other than \mathbb{F}_2 and \mathbb{F}_3 . The next sections will deal with these two possibilities.

3. The field of three elements

Throughout this section A will denote a composition algebra satisfying (4) over the field \mathbb{F}_3 of three elements. We want to show that again in this case, if e is a unitary idempotent (the existence of which is proved as in the previous section, replacing $\alpha(x)$ by $\frac{n(x, x^2)}{n(x)}$) then (11) is verified. From this point on the same argument of the previous section applies.

Lemma 1. *Given two unitary idempotents e and f , then $n(e, f) = -1$.*

Proof. If $e = f$ then there is nothing to prove, since $n(e, e) = 2n(e) = 2 = -1$, so assume $e \neq f$ and let $x = e + f$. Then

$$\begin{aligned} n(x, x) &= n(e, e) + n(f, f) - n(e, f) = 1 - n(e, f), \\ n(x, x^2) &= n(e + f, e + f + ef + fe) \\ &= n(x, x) + n(e, ef) + n(e, fe) + n(f, ef) + n(f, fe) \\ &= 1 - n(e, f) + 4n(e, f) = 1, \end{aligned}$$

since $n(e, ef) = n(e^2, ef) = n(e)n(e, f) = n(e, f)$, and so on.

Because of (7), $n(x) \neq 0$, so $n(x, x) \neq 0$. Hence $n(e, f)$ is either -1 or 0 . Assume that $n(e, f) = 0$. Then $n(x) = -1$, which forces x^2 to be linearly independent with x , and by (7) the subalgebra generated by x , $\text{alg}\langle x \rangle$, equals the span of x and x^2 : $\text{span}\langle x, x^2 \rangle$. Besides

$$\begin{vmatrix} n(x, x) & n(x, x^2) \\ n(x^2, x) & n(x^2, x^2) \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} = 1 \neq 0.$$

Hence, $\text{alg}\langle x \rangle$ is a composition algebra and it is unital with identity

$$e_x = \frac{1}{n(x)^2} (n(x, x^2)x - n(x)x^2)$$

because of (7), which is therefore the only unitary idempotent in $\text{alg}\langle x \rangle$.

Let us consider now the element $y = e - f$ ($\neq 0$), whose norm is $n(e) + n(f) - 2n(e, f) = 2 = -1$. Then,

$$\begin{aligned}x^2 &= e + f + e \circ f = x + e \circ f, \\y^2 &= e + f - e \circ f = x - e \circ f.\end{aligned}$$

Hence, $y^2 \in \text{alg}\langle x \rangle \cap \text{alg}\langle y \rangle$. But then either $\text{alg}\langle x \rangle = \text{alg}\langle y \rangle$, so that e and f belong to $\text{alg}\langle x \rangle$ and by uniqueness $e = e_x = f$, a contradiction, or the subalgebra $\text{alg}\langle x \rangle \cap \text{alg}\langle y \rangle$ is the span of y^2 . In the latter case, since $n(y) = -1$, $n(y^2) = 1$ and either y^2 or $-y^2$ is a unitary idempotent, hence equal to e_x . Also $n(y, y^2) = n(e - f, e + f - ef - fe) = n(e, e) - n(f, f) = 0$ (since $n(e, ef) = n(e^2, ef) = n(e, f) = 0$ and so on), so $\text{alg}\langle y \rangle$ is also a two dimensional Hurwitz algebra and, therefore, its identity element is its unique unitary idempotent. As a consequence, e_x is the identity element of both $\text{alg}\langle x \rangle$ and $\text{alg}\langle y \rangle$. Thus, $e_x(e + f) = e + f$ and $e_x(e - f) = (e - f)$, so $e_x e = e = e^2$ and $e_x f = f = f^2$. But the right multiplication by e and f are one-to-one since they have nonzero norm, so we conclude that $e = e_x = f$, a contradiction. \square

Lemma 2. *Let e be a unitary idempotent of A . Then, for any $x \in A$:*

- i) $n(x, x^2)n(x, e) = -n(x)^2 + n(x)n(e, x^2)$,
- ii) if $n(x) \neq 0$, then $n(e, x^2) = n(x) + n(x, e)^2$,
- iii) $n(x, x^2)n(x, e) = n(x)n(x, e)^2$.

Proof. If $n(x) = 0$ then also $n(x, x^2) = 0$ by (7) and i) and iii) are trivial. Hence assume that $n(x) \neq 0$. Then $e_x = \frac{1}{n(x)^2}(n(x, x^2)x - n(x)x^2)$ is the identity element of the unital subalgebra $\text{alg}\langle x \rangle$. By Lemma 1

$$-1 = n(e_x, e) = \frac{1}{n(x)^2}(n(x, x^2)n(x, e) - n(x)n(x^2, e)),$$

which gives i).

Now substitute x by $x + y$ and by $x - y$ in i) and add the resulting equations to obtain

$$\begin{aligned}n(y, e)(n(x, x \circ y) + n(y, x^2)) + n(x, e)(n(x, y^2) + n(y, x \circ y)) \\= n(x)(n(y^2, e) - n(y)) + n(x, y)(n(x \circ y, e) - n(x, y)) \\+ n(y)(n(x^2, e) - n(x))\end{aligned}$$

which, for $y = e$ gives

$$-(n(x, e \circ x) + n(e, x^2)) = n(x, e)^2 + n(x^2, e).$$

But $n(x, ex) = n(e_x x, ex) = n(e_x, e)n(x) = -n(x)$ by (5) and Lemma 1, and also $n(x, xe) = -n(x)$, so $n(x, e \circ x) = n(x)$. Hence we get

$$-(n(x) + n(e, x^2)) = n(x, e)^2 + n(x^2, e),$$

which gives ii), and iii) follows immediately from i) and ii) if $n(x) \neq 0$. \square

Corollary 1. *Let e be a unitary idempotent of A . Then for any $x \in A$*

$$n(x, x^2) = n(e, x)n(x).$$

Proof. If $n(x) = 0$, then also $n(x, x^2) = 0$ by (7) and this is clear. Also, if $n(e, x) \neq 0$, then the assertion follows from the previous Lemma. So assume that $n(x) \neq 0 = n(e, x)$. Then $n(e, e + x) = -1 \neq 0$, so

$$n(e + x, (e + x)^2) = n(e, e + x)n(e + x). \quad (12)$$

But by our assumptions

$$n(e, e + x)n(e + x) = n(e, e)(n(e) + n(x)) = -(1 + n(x)).$$

Also $n(x, e \circ x) = n(x)$, as in the proof of Lemma 2, and $n(e, ex) = n(e^2, ex) = n(e, x) = 0 = n(e, xe)$. Hence

$$\begin{aligned} n(e + x, (e + x)^2) &= n(e + x, e + x^2 + e \circ x) \\ &= n(e, e) + n(e, x^2) + n(x, x^2) + n(x) \\ &= -1 + n(x) + n(x, x^2) + n(x) \quad (\text{by Lemma 2}) \\ &= -(1 + n(x)) + n(x, x^2). \end{aligned}$$

Hence (12) implies $n(x, x^2) = 0$ and the assertion is also true in this case. \square

As mentioned at the beginning of the section, the Corollary above and the arguments of the previous section give:

Proposition 3. *The only composition algebras over \mathbb{F}_3 satisfying (4) are the Hurwitz algebras.*

4. The field of two elements

We are left with the most tricky case. Throughout this section, A will denote a composition algebra satisfying (4) with norm n over the field \mathbb{F}_2 .

Let us first have a look at the subalgebra generated by an element x with $n(x) \neq 0$. By (7),

$$x^3 + n(x, x^2)x^2 + x = 0. \quad (13)$$

Now, if $n(x, x^2) = 1$, then $e_x = x^3 = x + x^2$ verifies $n(e_x) = 1$ and

$$\begin{aligned} e_x x &= (x + x^2)x = x^2 + x^3 = x, \quad \text{by (13)} \\ e_x x^2 &= (x + x^2)x^2 = x^3 + x^3 x = (x + x^2) + x = x^2, \end{aligned}$$

so $e_x = x + x^2$ is the identity element of $\text{alg}(x) = \text{span}\langle x, x^2 \rangle$ and $\text{alg}\langle x \rangle$ is isomorphic to \mathbb{F}_4 . Otherwise $n(x, x^2) = 0$, so $x^3 = x$ by (13), then either $x^2 = x$ and $\text{alg}\langle x \rangle = \text{span}\langle x \rangle$, or $x^2 \neq x$, $\text{alg}\langle x \rangle = \text{span}\langle x^2, x + x^2 \rangle$ and $x^2 x^2 = x^3 x = x^2, x^2(x + x^2) = x + x^2 = (x + x^2)x^2$ and $(x + x^2)^2 = x^2 + x^2 x^2 = x^2 + x^2 = 0$.

In this last case, $\text{alg}\langle x \rangle$ is isomorphic to the algebra of “dual numbers” $\mathbb{F}_2 1 + \mathbb{F}_2 \epsilon$, with $\epsilon^2 = 0$ and $n(1) = 1, n(\epsilon) = n(1, \epsilon) = 0$.

In any case, $\text{alg}\langle x \rangle$ is a unital algebra, whose identity element will be denoted by e_x . Besides, for any $y \in A, n(x, xy) = n(xe_x, xy) = n(e_x, y) = n(x, yx)$, so that for any $x, y \in A$ with $n(x) = 1$

$$n(x, x \circ y) = 0. \tag{14}$$

Assume first that $A^\perp \neq 0$. Then, since the restriction $n|_{A^\perp} : A^\perp \rightarrow F$ is one-to-one and linear (because $n(\alpha x) = \alpha^2 x = \alpha x$ for any $\alpha (= 0 \text{ or } 1)$ in \mathbb{F}_2), it follows that $A^\perp = \mathbb{F}_2 e$ for some e with $n(e) = 1$. From (13), $e^3 = e$, so for any $x \in A, n(e^2, x) = n(e)n(e^2, x) = n(e^3, ex) = n(e, ex) = 0$ and $e^2 \in A^\perp = \mathbb{F}_2 e$. Therefore, $e^2 = e$. Now, for any $x \in A$ with $n(x) = 0, n(e+x) = n(e) + n(x) = 1$, so there exists a unitary idempotent f (the identity element of the algebra generated by $e+x$) such that $f(e+x) = (e+x)f = e+x$ and

$$\begin{aligned} n(x, ex) &= n(e+x, ex) = n(f(e+x), ex) \\ &= n(e(e+x), fx) + n(f, e)n(e+x, x) \quad \text{by (6)} \\ &= n(e+ex, fx) = n(ex, fx) = n(e, f)n(x) = 0. \end{aligned}$$

Also, if $n(x) = 1$, then $n(e+x) = 0$, so $n(x, ex) = n(e+x, e(e+x)) = 0$. Hence, $n(x, ex) = 0$ for any $x \in A$. As a consequence, for any $x, y \in A, n(x, ey) = n(y, ex)$, so

$$n(y, ex) = n(e)n(y, ex) = n(ey, e(ex)) = n(y, e(e(ex))),$$

so that $(L_e^3 - L_e)(x) \in A^\perp = \mathbb{F}_2 e$ for any $x \in A$ and then $0 = (L_e - 1)(L_e^3 - L_e) = L_e(L_e - 1)^3$, where L_e denotes the left multiplication by e in A . But L_e is one-to-one, because $n(e) = 1$ and n is nondegenerate, so we conclude that $(L_e - 1)^3 = 0$, so that L_e is a bijection.

In exactly the same way we conclude that the right multiplication R_e by e is a bijection, and as in [K 53] that the the new algebra obtained over A with the new multiplication given by

$$x \cdot y = \left(R_e^{-1} x \right) \left(L_e^{-1} y \right)$$

is a unital composition algebra over \mathbb{F}_2 with the same norm, whose identity element is e . Since we are assuming that $A^\perp \neq 0$ and \mathbb{F}_2 is perfect, we conclude that the dimension of A is one in this case.

Therefore, from now on we will assume that the norm n on A is strictly nondegenerate. Hence the dimension of A is either 2, 4, 8 or infinite.

The two dimensional case is settled in the next result:

Proposition 4. *Let A be a two dimensional composition algebra over \mathbb{F}_2 with strictly nondegenerate norm and satisfying (4). Then, up to isomorphism, A is either:*

- i) a Hurwitz algebra, hence it is either $\mathbb{F}_2 \oplus \mathbb{F}_2$ or \mathbb{F}_4 ,
- ii) the left or right composition algebra associated to $\mathbb{F}_2 \oplus \mathbb{F}_2$, or
- iii) the para-Hurwitz algebra associated to \mathbb{F}_4 .

Proof. Assume first that there is a nonzero element $0 \neq x \in A$ such that x and x^2 are linearly independent. Then $A = \mathbb{F}_2x + \mathbb{F}_2x^2$, $n(x, x^2) = 1$ by the nondegeneracy of $n(\cdot, \cdot)$ so, by (7), $n(x) = 1$ and $A = \text{alg}\langle x \rangle \cong \mathbb{F}_4$, as above.

Otherwise, for any $x \in A$, x^2 equals either 0 or x , so for any $0 \neq e \in A$ with $n(e) = 1$, we have $e^2 = e$. Choose one such e and take $a \in A$ such that $A = \mathbb{F}_2e + \mathbb{F}_2a$, so that $n(e, a) = 1$.

In case $n(a) = 1$, then $n(e + a) = 1$ too and therefore $a^2 = a$ and $(e + a)^2 = e + a$. Moreover, if $ea = e = e^2$ then $e(e + a) = 0$ and this is a contradiction since the left multiplication by e is a bijection. The same happens if $ea = a = a^2$. Hence $ea = ae = e + a$ and A is thus isomorphic to the para-Hurwitz algebra associated to \mathbb{F}_4 .

Finally, in case $n(a) = 0$ we are left with two subcases: either $a^2 = a$ or $a^2 = 0$. In the first subcase ($a^2 = a$) $n(ea, e) = n(ea, e^2) = n(a, e) = 1 = n(ae, e)$, and $n(ea, a) = n(ea, a^2) = n(a)n(e, a) = 0 = n(ae, a)$, which force $ea = ae = a$, so A is, up to isomorphism, the split Hurwitz algebra $\mathbb{F}_2 \oplus \mathbb{F}_2$.

In the second subcase ($a^2 = 0$), it must be that $(e + a)^2 = 0$, otherwise interchange a and $e + a$ in the paragraph above to get that A is isomorphic to $\mathbb{F}_2 \oplus \mathbb{F}_2$, which contradicts $a^2 = 0$. Hence $a^2 = 0 = (e + a)^2$, so $e \circ a = e$. But $n(ea, e) = 1$, as above, and $n(ea) = 0$, which gives either:

- $ea = a$, $ae = e + a$ and we are in case ii), or
 - $ea = e + a$, $ae = a$ (opposite to the previous one), and we are in case ii) again.
-

The dimension four case is settled in a completely different way:

Proposition 5. *Let A be a four dimensional composition algebra over \mathbb{F}_2 with strictly nondegenerate norm and satisfying (4). Then A is a Hurwitz algebra.*

Proof. Take any idempotent $0 \neq e = e^2$ with $n(e) = 1$ (for instance the identity element e_x of any $\text{alg}\langle x \rangle$ with $n(x) = 1$). Then the new multiplication given by

$$x \cdot y = (R_e^{-1}x)(L_e^{-1}y),$$

(where L_e and R_e denote the left and right multiplications by e) makes A a four dimensional Hurwitz algebra with unit e , that is, a four dimensional central simple associative algebra, which is necessarily isomorphic to the algebra $\text{Mat}_2(\mathbb{F}_2)$ of 2×2 matrices over \mathbb{F}_2 with the determinant function as norm, since there are no central simple division algebras over finite fields by the well-known Wedderburn's Theorem.

But in $\text{Mat}_2(\mathbb{F}_2)$, the set of invertible elements is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$

that is, the invertible elements are the nonzero elements of the orthogonal subspaces

$$S_1 = \text{span} \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \quad \text{and} \quad S_2 = \text{span} \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle.$$

Thus S_1 and S_2 are the only two dimensional subspaces without nonzero isotropic elements. Therefore, with $S = S_i$ such that $e \in S_i$, $A = S \oplus S^\perp$ (where S^\perp denotes the orthogonal subspace to S) for a two dimensional subspace S with $e \in S$, such that the restrictions of the norm n to S and to S^\perp do not represent 0 and any element $x \notin S \cup S^\perp$ verifies $n(x) = 0$. Moreover, S and S^\perp are the only two dimensional subspaces without nonzero isotropic elements.

Therefore, for any $x \in A$ with $n(x) = 1$, either $xS = S$ and $xS^\perp = S^\perp$, or $xS = S^\perp$ and $xS^\perp = S$; and the same with Sx and $S^\perp x$.

Since $e = e^2 \in S$, it follows easily from this that S is a subalgebra ($SS \subseteq S$) and that $SS^\perp + S^\perp S \subseteq S^\perp$ and $S^\perp S^\perp \subseteq S$.

For any $0 \neq y \in S^\perp$, $n(e + y) = 0$, so $n(e + y, (e + y)^2) = 0$ by (7). Now (14) and the above give

$$0 = n(e + y, (e + y)^2) = n(e, e \circ y) + n(y, e \circ y) + n(y, y^2) + n(e, y^2) = n(e, y^2),$$

so $y^2 = e$ since $n(x_1, x_2) = 1$ for any $0 \neq x_1 \neq x_2 \neq 0$ in S . As a consequence e is the only nonzero idempotent in S (otherwise the same argument would give $y^2 = f \neq e$) and hence for any nonzero $x \neq e$ in S , $S = \text{alg}\langle x \rangle$ and $e = e_x$. Besides $ey = y^2 y = y = ye$ by (13) for any $y \in S^\perp$, so that e is the identity element in A and A is a Hurwitz algebra, as required. \square

In order to finish the proof of the Theorem, it must be proved that if A is a composition algebra with strictly nondegenerate norm of dimension > 4 (hence 8 or ∞) over \mathbb{F}_2 and satisfies (4), then A is a Hurwitz algebra. Let us start with an easy Lemma:

Lemma 3. *Let V be a vector space over \mathbb{F}_2 of dimension > 2 equipped with a strictly nondegenerate quadratic form n , then:*

- a) *For any $x \in V$ with $n(x) = 1$, there exists an $y \in V$ with $n(y) = 1 = n(x, y)$.*
- b) $V = \text{span} \langle x \in V : n(x) = 0 \rangle$.
- c) *For any $x \in V$ with $n(x) = 0$, there exists $x', x'' \in V$ with $n(x') = 1 = n(x'')$ and $x = x' + x''$.*

Proof. a) By nondegeneracy there is a $z \in V$ with $n(x, z) = 1$. If $n(z) = 1$ we are finished. Otherwise $n(z) = 0$, $V = \text{span} \langle x, z \rangle \oplus \text{span} \langle x, z \rangle^\perp$ and we can take an element $z' \in \text{span} \langle x, z \rangle^\perp$ with $n(z') = 1$ so that the element $y = z + z'$ verifies $n(y) = 1 = n(x, y)$.

b) For any $v \in V$ with $n(v) = 1$, take $v' \in V$ with $n(v') = 1 = n(v, v')$ as in a) and take $v'' \in \text{span} \langle v, v' \rangle^\perp$ with $n(v'') = 1$. Then $n(v' + v'') = 0 = n(v + v' + v'')$ and $v = (v' + v'') + (v + v' + v'') \in \text{span} \langle x \in V : n(x) = 0 \rangle$.

c) If $n(x) = 0$, take $x' \in \text{span} \langle x \rangle^\perp$ with $n(x') = 1$. Then $n(x + x') = 1$ and $x = x' + (x + x')$. \square

Let us assume from now on that A is a composition algebra with strictly non-degenerate norm n of dimension > 4 over \mathbb{F}_2 satisfying (4).

Proposition 6. *For any $x, y, z \in A$, $n(x \circ y, z) = n(x, y \circ z)$.*

Proof. If $n(x) = 1$ and e_x denotes the identity element of $\text{alg}(x)$, then for any $y \in A$, $n(x, xy) = n(xe_x, xy) = n(e_x, y) = n(e_x x, yx) = n(x, yx)$, so that $n(x, x \circ y) = 0$. Now, given $x, z \in A$ with $n(x) = n(z) = n(x, z) = 1$ we have for any $y \in A$

$$0 = n(x + z, (x + z) \circ y) = n(x, z \circ y) + n(z, x \circ y),$$

so

$$n(x \circ y, z) = n(x, y \circ z). \quad (15)$$

Let us fix $x \in A$ with $n(x) = 1$. By the previous Lemma there is an $x' \in A$ with $n(x') = 1 = n(x, x')$. Then (15) is valid for any $z \in \text{span}\langle x, x' \rangle$, and if $v \in \text{span}\langle x, x' \rangle^\perp$ with $n(v) = 0$, $n(x' + v) = 1 = n(x, x' + v)$ so (15) is valid with $z = x' + v$ and hence with $z = v$. From Lemma 3.b) it follows that (15) is valid for any $x, y, z \in A$ with $n(x) = 1$ and, finally, by Lemma 3.c), it is valid for any $x, y, z \in A$. \square

Corollary 2. *Let V be a subspace of A such that $n(x, x^2) = 0$ for any $x \in V$, then $V \circ V \subseteq V^\perp$.*

Proof. For any $x, y \in V$, $0 = n(x + y, (x + y)^2) = n(x, y^2) + n(x^2, y)$ by Proposition 6. Hence $n(x^2, y) = n(x, y^2)$ for any $x, y \in V$. Now for any $x, y, z \in V$,

$$\begin{aligned} n(x + z, y^2) &= n((x + z)^2, y) = n(x^2, y) + n(z^2, y) + n(x \circ z, y) \\ &= n(x, y^2) + n(z, y^2) + n(x \circ z, y) = n(x + z, y^2) + n(x \circ z, y), \end{aligned}$$

so $x \circ z \in V^\perp$, as required. \square

Proposition 7. *There are elements $x \in A$ with $n(x, x^2) = 1$.*

Proof. Otherwise, by the Corollary above, $A \circ A = 0$, so that A is commutative. Moreover, by (7) $n(x)(x^3 + x) = 0$ for any $x \in A$. Take $0 \neq e = e^2 \in A$ with $n(e) = 1$ and (Lemma 3.a)) an $f \in A$ with $n(f) = 1 = n(e, f)$. Then

$$\begin{aligned} e + f &= (e + f)^3 = (e^2 + f^2)(e + f) \\ &= e + ef + f^2e + f^3 = e + f + e(f + f^2). \end{aligned}$$

Hence $f^2 = f$. Now, for any $v \in \text{span}\langle e, f \rangle^\perp$ with $n(v) = 0$, $y = f + v$ also verifies $n(e, y) = 1 = n(y)$, so $y^2 = y$ too and, therefore, $v^2 = v$. From Lemma 3.b) and the commutativity it follows that $x^2 = x$ for any $x \in A$. But for $x, y, z \in A$,

$$\begin{aligned} n(x)n(y, z) &= n(xy, xz) = n(xy, zx) \\ &= n(zy, x^2) + n(x, z)n(y, x) \\ &= n(x, yz) + n(x, y)n(x, z). \end{aligned}$$

With y, z such that $n(y, z) = 1$ and x orthogonal to y, z and yz and with $n(x) = 1$, we get a contradiction. \square

Therefore, we may fix an element $a \in A$ with $n(a, a^2) = 1$. Because of (4) $n(a) = 1$ and $\text{alg}\langle a \rangle$ is isomorphic to \mathbb{F}_4 . Let e be the identity element of $\text{alg}\langle a \rangle$. The proof of the Theorem will be finished if we show that $ex = xe = x$ for any $x \in A$.

Proposition 8. *For any $x \in \text{alg}\langle a \rangle^\perp$, $n(x, x^2) = 0$.*

Proof. In case $n(x) = 0$, this follows from (7). Otherwise $n(x) = 1$ and for any $0 \neq b \in \text{alg}\langle a \rangle$, $n(b + x) = n(b) + n(x) = 1 + 1 = 0$, so using Proposition 6 we get

$$0 = n(b + x, (b + x)^2) = n(b, b^2) + n(b, x^2) + n(x, x^2).$$

Taking in turn $b = e, a, a^2$ and adding up the results, it follows that

$$\begin{aligned} 0 &= n(x, x^2) + n(e + a + a^2, x^2) + n(a, a^2) + n(a^2, (a^2)^2) \\ &= n(x, x^2) + n(0, x^2) + 1 + 1 = n(x, x^2). \quad \square \end{aligned}$$

And finally:

Proposition 9. *A is a Hurwitz algebra.*

Proof. Let $V = \text{alg}\langle a \rangle^\perp$, by the Corollary above $V \circ V \subseteq \text{alg}\langle a \rangle$.

For any $x \in V$ with $n(x) = 1$, as in the proof of the previous Proposition

$$n(e, x^2) = 0 \quad \text{and} \quad n(a, x^2) = n(a, a^2) = 1,$$

so

$$x^2 = e + u_x$$

for some $u_x \in V$. But $1 = n(x^2) = n(e) + n(u_x)$, so $n(u_x) = 0$. Also $n(x, u_x) = n(x, x^2) = 0$. Besides, since the multiplication by e is an orthogonal transformation, $ex \in V$, so $ex + x = u_x x \in V$ and also $xu_x \in V$. Thus, $x \circ u_x \in V \cap (V \circ V) \subseteq V \cap \text{alg}\langle a \rangle = 0$, and therefore $e \circ x = 0$. By Lemma 3.c) $e \circ z = 0$ for any $z \in V$, so $ev = ve$ for any $v \in A$. Moreover, since $n(x, x^2) = 0$, $e_x = x^2$ is the identity of $\text{alg}\langle x \rangle$ and

$$e + u_x = x^2 = (x^2)^2 = (e + u_x)^2 = e + e \circ u_x + u_x^2 = e + u_x^2.$$

Hence $u_x = u_x^2$.

By Lemma 3.a) there is an element $y \in V$ with $n(y) = 1 = n(x, y)$, so that

$$x^2 = e + u_x, \quad y^2 = e + u_y \quad \text{and} \quad (x + y)^2 = e + u_{x+y}.$$

But $(x + y)^2 = x^2 + y^2 + x \circ y = u_x + u_y + x \circ y$ and $x \circ y \in \text{alg}\langle a \rangle$ by the last Corollary. Thus, $x \circ y = e$. Also, for any $v \in V \cap \text{span}\langle x, y \rangle^\perp$ with $n(v) = 0$, $n(y + v) = 1 = n(x, y + v)$, so $x \circ (y + v) = e$ and $x \circ v = 0$. Because of Lemma 3.b) we conclude that $x \circ u = n(x, u)e$ for any $x \in V$ with $n(x) = 1$ and

for any $u \in V$. A new application of Lemma 3 (this time its part c)) gives for any $u, v \in V$:

$$u \circ v = n(u, v)e.$$

This also implies that

$$n(u \circ v) = n(n(u, v)e) = n(u, v)^2 = n(u, v) \quad (16)$$

for any $u, v \in V$ since we are dealing with the field of two elements. Also notice that

$$\begin{aligned} n(u \circ v) &= n(uv, vu) + n(uv) + n(vu) \\ &= n(uv, vu) + 2n(u)n(v) = n(uv, vu). \end{aligned} \quad (17)$$

Finally, for any $x \in V$ with $n(x) = 1$ and for any $z \in V$,

$$\begin{aligned} 0 &= n(z + u_x, (z + u_x)^2) = n(z + u_x, z^2 + u_x^2) \quad (\text{by Propositions 6 and 8}) \\ &= n(z, u_x) + n(z^2, u_x) = n(z, u_x) + n(z^2, u_x^2) \quad (\text{since } u_x = u_x^2) \\ &= n(z, u_x) + n(zu_x, u_x z) + n(z, u_x)^2 \quad (\text{by (6)}) \\ &= n(zu_x, u_x z) = n(z \circ u_x) = n(z, u_x) \quad (\text{by (17) and (16)}). \end{aligned}$$

Therefore $n(z, u_x) = 0$ for any $z \in V$ and, since n is strictly nondegenerate, it follows that $u_x = 0$, so $x^2 = e$ and $ex = x^2x = x = xe$ for any $x \in V$ with $n(x) = 1$. By Lemma 3.c) it then follows that $ez = ze = z$ for any $z \in V$ and hence also for any $z \in A$, as desired. \square

Acknowledgements. The first author acknowledges support by the Spanish DGES (Pb 97-1497) and by the ‘‘Plan Andaluz de Investigaci3n y Desarrollo Tecnol3gico’’ (FQM 0125); the second author by DGICYT (Pb 94-1311-C03-03) and DGES (Pb 97-1291-C03-03); while the last author by DGICYT (Pb 94-1311-C03-03), DGES (Pb 97-1291-C03-02) and by a grant from the ‘‘Programa de Formaci3n del Personal Investigador en el Extranjero’’ (M.E.C.).

References

- [A 48] Albert, A.A.: Power-Associative Rings. Trans. Amer. Math. Soc. **64**, 552–593 (1948)
- [C 92] Cuenca, J.A.: One-sided infinite-dimensional normed real algebras. Publ. Mat. **36**, 485–488 (1992)
- [E 97] Elduque, A.: Symmetric composition algebras. J. Algebra **196**, 283–300 (1997)
- [EM-M 80] El-Mallah, M.L. and Micali, A.: Sur les algèbres normées sans diviseurs topologiques de zéro. Bol. Soc. Mat. Mex. **25**, 23–28 (1980)
- [E-M 93] Elduque, A. and Myung, H.C.: On flexible composition algebras. Commun. Algebra **21**, 2481–2505 (1993)
- [E-P 94] Elduque, A. and Pérez, J.M.: Third power associative composition algebras. manuscripta math. **84**, 73–87 (1994)
- [E-P 96] Elduque, A. and Pérez, J.M.: Composition algebras with associative bilinear form. Commun. Algebra **24**, 1091–1116 (1996)

- [E-P 97] Elduque, A. and Pérez, J.M.: Infinite dimensional quadratic forms admitting composition. *Proc. Amer. Math. Soc.* **125**, 2207–2216 (1997)
- [K 53] Kaplansky, I.: Infinite-dimensional quadratic forms admitting composition. *Proc. Amer. Math. Soc.* **4**, 956–960 (1953)
- [KMRT 98] Knus, M.A., Merkurjev, A.S, Rost, M. and Tignol, J.P.: *The Book of Involutions*. American Math. Soc. Colloquium Publ., vol. **44**, Providence, 1998
- [M 94] Myung, H.C.: *Non-Unital Composition Algebras*. Research Institute of Mathematics, Global Analysis Research Center, Lecture Notes Series no. **22**, Seoul 1994
- [O 81] Okubo, S.: Dimension and classification of general composition algebras. *Hadronic J.* **4**, 216–273 (1981)
- [O 82] Okubo, S.: Classification of flexible composition algebras, I and II. *Hadronic J.* **5**, 1564–1626 (1982)
- [O-O 81] Okubo, S. and Osborn, J.M.: Algebras with nondegenerate associative symmetric bilinear form permitting composition, I and II. *Commun. Algebra* **9**, 1233–1261 and 2015–2073 (1981)
- [P 94] Pérez, J.M.: *Power-associative composition algebras*. *Non Associative Algebra and its Applications* (S. González, ed.), Kluwer Academic Publishers, 1994
- [RP 92] Rodríguez Palacios, A.: One-sided division absolute valued algebras. *Publ. Mat.* **36**, 925–954 (1992)
- [U-W 60] Urbanik, K. and Wright, F.B.: Absolute-valued algebras. *Proc. Amer. Math. Soc.* **11**, 861–866 (1960)
- [ZSSS 82] Zhevlakov, K.A., Slin'ko, A.M., Shestakov, I.P. and Shirshov, A.I.: *Rings that are Nearly Associative*. Academic Press, New York 1982