ON TOTALLY DECOMPOSABLE ALGEBRAS WITH INVOLUTION IN CHARACTERISTIC TWO

M. G. MAHMOUDI, A.-H. NOKHODKAR

Abstract. A necessary and sufficient condition for a central simple algebra with involution over a field of characteristic two to be decomposable as a tensor product of quaternion algebras with involution, in terms of its Frobenius subalgebras, is given. It is also proved that a bilinear Pfister form, recently introduced by A. Dolphin, can classify totally decomposable central simple algebras of orthogonal type.

Mathematics Subject Classification: 16W10, 16W25, 16K20, 11E39.

1. Introduction

An old result due to A. A. Albert states that every central simple algebra A of degree 4 which carries an involution of the first kind can be decomposed as a tensor product of two quaternion algebras (see [15, §16]). This result is no longer valid if A is of degree 8 by the examples given in [1] over fields of characteristic different from 2 and in [23] over fields of characteristic 2. In [1], it was also shown that if A is of degree 2^n over a field of characteristic different from 2, then A decomposes into a tensor product of quaternion algebras if and only if there exists a finite square-central subset of A (called a *q-generating set*) which satisfies some commuting properties. Over a field of particular cohomological dimension, it is known that central simple algebras which carry an involution of the first kind can be decomposed as a tensor product of quaternion algebras (see [12], and [4] for a characteristic 2 counterpart). In [3], a similar result was proved provided that the base field is of the u-invariant $\leqslant 8$.

A closely related problem is to determine the conditions under which a central simple algebra with involution (A,σ) is *totally decomposable* (i.e., (A,σ) decomposes as a tensor product of σ-invariant quaternion algebras). In [22], it was shown that if A is of degree 4 over a field of characteristic different from 2 and σ is of symplectic type, then A can be decomposed as a tensor product of two σ-invariant quaternion algebras. A proof of this result in characteristic 2 was given in [24], also a characteristic independent proof of this result and a criterion for decomposability in the case where σ is orthogonal can be found in [16]. A similar criterion for the unitary case of degree 4 and of arbitrary characteristic was derived in [13]. A cohomological invariant to detect decomposability for degree 8 algebras with symplectic involution over a field of characteristic different from 2 can be found in [9]. For the case of degree 8 algebras with orthogonal involution (A,σ) over a field of characteristic different from 2, a criterion for decomposability in terms of the Clifford algebra of (A,σ) can be found in [15, (42.11)], see also [25, (3.10)]. For the case where (A,σ) is split and of arbitrary degree 2^n over a field of characteristic different from 2, a decomposability criterion in term of higher degree invariants of a quadratic form q, to which σ is adjoint, can be found in [25].

Another relevant problem is to find invariants which classify central simple algebras with involution (A,σ) up to conjugation. Orthogonal involutions of degree

$\leqslant 4$ can be classified by their Clifford algebras [15, §15], [17, §2]. A degree 4 central simple algebra with symplectic involution (A,σ) can be classified by a 3-fold Pfister form or an Albert form associated to σ, see [14] and [15, §16].

In this work we study the problems of decomposition and classification of central simple algebras with involution in the case of characteristic 2. In (4.5), we show that a central simple algebra with involution over a field of characteristic 2 is totally decomposable if and only if there exists a symmetric and self-centralizing subalgebra $S = \Phi(A,\sigma)$ of A such that (i) $x^2 \in F$ for every $x \in S$ and (ii) $\dim_F S = 2^{r_F(S)}$, where $r_F(S)$ is the minimum rank of S. In the case where (A,σ) is totally decomposable central simple algebra with involution of orthogonal type we show that the aforementioned subalgebra $\Phi(A,\sigma)$, is unique up to isomorphism (see (5.10)). We prove the existence of a natural associative bilinear form $\mathfrak{s}$ on $\Phi(A,\sigma)$, isometric to a recently introduced bilinear Pfister form $\mathfrak{Pf}(A,\sigma)$ in [7], thus providing a more intrinsic definition of $\mathfrak{Pf}(A,\sigma)$ (see (5.5), (5.6)). In [7, (7.5)], it was shown that for every splitting field K of A, the involution σ_K on A_K is adjoint to the bilinear form $\mathfrak{Pf}(A,\sigma)_K$ (see [7, (7.5)], compare [21, (5.1)]), and it was asked (see [7, (7.4)]) if $\mathfrak{Pf}(A,\sigma)$ classify (A,σ) up to conjugation. Using the methods developed in the current work, we give in (6.5) an affirmative answer to this question.

2. Preliminaries

Let V be a finite dimensional vector space over a field F and let $\mathfrak{b} : V \times V \to F$ be a bilinear form. Let $D_F(\mathfrak{b}) = \{\mathfrak{b}(v,v) : v \in V \text{ and } \mathfrak{b}(v,v) \neq 0\}$. If K/F is a field extension, the *extension* of $\mathfrak{b}$ to $V_K = V \otimes_F K$ is denoted by $\mathfrak{b}_K$.

The *orthogonal sum* and the *tensor product* of two bilinear forms $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are denoted by $\mathfrak{b}_1 \perp \mathfrak{b}_2$ and $\mathfrak{b}_1 \otimes \mathfrak{b}_2$ respectively. For α in $F^\times$, the group of invertible elements of F, we use the notation $\langle\alpha\rangle$ for the isometry class of the one-dimensional bilinear space $(V,\mathfrak{b})$ over F defined by $\mathfrak{b}(u,v) = \alpha uv$. The bilinear form $\perp_{i=1}^n \langle\alpha_i\rangle$ is denoted by $\langle\alpha_1,\cdots,\alpha_n\rangle$.

Let F be a field and let $\alpha_1,\cdots,\alpha_n \in F^\times$. The 2^n-dimensional bilinear form $\langle 1,\alpha_1\rangle \otimes \cdots \otimes \langle 1,\alpha_n\rangle$ over F is called a *bilinear n-fold Pfister form* and is denoted by $\langle\langle\alpha_1,\cdots,\alpha_n\rangle\rangle$. If $\mathfrak{b}$ is a bilinear Pfister form then there exists a bilinear form $\mathfrak{b}'$, uniquely determined up to isometry, such that $\mathfrak{b} = \langle 1\rangle \perp \mathfrak{b}'$ (see [2, p. 16]). The form $\mathfrak{b}'$ is called the *pure subform* of $\mathfrak{b}$.

A *quadratic form* over F is a map $q : V \to F$ such that: (1) $q(\alpha v) = \alpha^2 q(v)$ for every $\alpha \in F$ and $v \in V$; (2) the map $\mathfrak{b}_q : V \times V \to F$ defined by $\mathfrak{b}_q(u,v) = q(u+v) - q(u) - q(v)$ for every $u,v \in V$ is a bilinear form. We say that q is *totally singular* if $\mathfrak{b}_q(u,v) = 0$ for every $u,v \in V$. For $\alpha_1,\cdots,\alpha_n \in F$, the isometry class of the n-dimensional totally singular quadratic form (V,q) over F defined by $q(v_1,\ldots,v_n) = \alpha_1 v_1^2 + \cdots + \alpha_n v_n^2$ is denoted by $[\alpha_1] \perp \cdots \perp [\alpha_n]$. The Clifford algebra of a quadratic form (V,q) is denoted by $C(V)$. We refer the reader to [8, Ch. II] for basic definitions and facts regarding Clifford algebras and quadratic and bilinear forms in arbitrary characteristic.

Let R be a ring. An additive map $\delta : R \to R$ is called a *derivation*, if $\delta(ab) = a\delta(b) + \delta(a)b$ for every $a,b \in R$. For $a \in R$, the map $\delta_a : R \to R$ defined by $\delta_a(x) = ax - xa$ is a derivation of R which is called the *inner derivation* induced by a.

All F-algebras considered in this work are supposed to be unital and associative. The reader is referred to [20, Ch. 12] for basic notions concerning central simple algebras. We just recall that the *degree* of a central simple algebra A is defined by $\deg_F A = \sqrt{\dim_F A}$. Also for a subalgebra B of A the centralizer of B in A and the center of B are denoted respectively by $C_A(B)$ and $Z(A)$.

A finite dimensional algebra A over F is called a *Frobenius algebra* if A contains a hyperplane H that contains no nonzero left ideal of A; alternatively A is called a Frobenius F-algebra if there exists a nondegenerate bilinear form $\mathfrak{b} : A \times A \to F$ which is associative, in the sense that $\mathfrak{b}(x, yz) = \mathfrak{b}(xy, z)$ for every $x, y, z \in A$. In this work, we use the following fundamental result about the properties of Frobenius subalgebras of central simple algebras:

Theorem 2.1. [11, (2.2.3)] *Let A be a central simple algebra over a field F and let S be a commutative Frobenius subalgebra of A such that $\dim_F S = \deg_F A$.*

(i) *We have $C_A(S) = S$.*

(ii) *Every derivation of S into A can be extended to an inner derivation of A.*

For further properties of Frobenius algebras see [11] .

The *minimum rank* of a finite dimensional F-algebra A which is denoted by $r_F(A)$ is the minimum number r such that A can be generated as an F-algebra by r elements. Also the *Loewy length* of A which is denoted by $\ell\ell(A)$ is defined as the smallest positive integer l such that $J(A)^l = 0$; in other words $\ell\ell(A)$ is the nilpotency index of the Jacobson radical of A.

Let A be a central simple algebra over a field F. An *involution* on A is an anti-automorphism σ of A such that $\sigma^2 = \mathrm{id}$. The involution σ is called of *the first kind* if $\sigma|_F = \mathrm{id}$. The set of *alternating* and *symmetric* elements of (A, σ) are defined as follows:

$$\mathrm{Alt}(A, \sigma) = \{a - \sigma(a) : a \in A\}, \quad \mathrm{Sym}(A, \sigma) = \{a \in A : \sigma(a) = a\}.$$

An involution σ of the first kind is said to be of *symplectic* type if over a splitting field of A, σ becomes adjoint to an alternating bilinear form. Otherwise, σ is said to be of *orthogonal* type. If $\mathrm{char}\, F = 2$ and σ is of the first kind, then it can be shown that σ is of orthogonal type if and only if $1 \notin \mathrm{Alt}(A, \sigma)$, see [15, (2.6)]. The *discriminant* of an involution σ of orthogonal type is denoted by $\mathrm{disc}\, \sigma$, see [15, (7.1)].

Let F be a field of characteristic 2. A *quaternion algebra* over F is a central simple F-algebra of degree 2. As an F-algebra, every quaternion algebra is generated by two elements u and v subject to the relations

$$u^2 + u \in F, \quad v^2 \in F^\times \quad \text{and} \quad uv + vu = v.$$

Furthermore $\{1, u, v, uv\}$ is a basis of Q over F.

3. Totally singular conic Frobenius algebras

Definition 3.1. In analogy with [10], we call an algebra R over a field F a *totally singular conic algebra* if $x^2 \in F$ for every $x \in R$.

Remark 3.2. Let F be a field of characteristic 2 and let R be a finite dimensional totally singular conic F-algebra. It follows immediately that

(i) R is a local commutative algebra and its unique maximal ideal is $\mathfrak{m} = \{x \in R : x^2 = 0\}$.

(ii) For every $u \in R \setminus F$, the subalgebra $F[u]$ is a field if and only if $u^2 \notin F^2 = \{x^2 : x \in F\}$.

Remark 3.3. A local commutative algebra is a Frobenius algebra if and only if it has a unique minimal ideal, see [11, (2.1.3)]. In particular for a finite dimensional totally singular conic algebra, being a Frobenius algebra is a purely ring theoretic property and dose not depend on the base field.

Lemma 3.4. *Let R be a finite dimensional totally singular conic algebra over a field F. If $\dim_F R = 2^{r_F(R)}$, then R is a Frobenius algebra.*

Proof. Set $n = r_F(R)$ and write $R = F[u_1, \cdots, u_n]$ for some $u_1, \cdots, u_n \in R$. The F-algebra homomorphisms $f_i : F[u_i] \to R$ defined by $f_i(u_i) = u_i$, $i = 1, \cdots, n$, induce a surjective F-algebra homomorphism $f : F[u_1] \otimes \cdots \otimes F[u_n] \to R$. By dimension count f is an isomorphism. We know that single generated algebras (i.e., algebras of the form $F[u]$) and the tensor product of Frobenius algebras are Frobenius (see [11, (2.1.4)] and [11, (2.1.2)]), hence R is a Frobenius F-algebra. $\square$

Remark 3.5. The converse of (3.4) is not necessarily true. Here we construct a counter example. Let F be a field of characteristic 2 and for $n \geq 4$, let R_n be the n-dimensional algebra over F with the basis $\{1, u_1, \cdots, u_{n-1}\}$ subject to the relations

$$\begin{aligned} u_i^2 = u_1 u_i = 0, &\quad 1 \leq i \leq n-1, \\ u_i u_j = u_1, &\quad 2 \leq i \neq j \leq n-1. \end{aligned} \tag{1}$$

It is easy to see that the above relations imply that $u_1 u_i = u_i u_1$ for every i. It follows that R_n is a totally singular conic algebra with the unique maximal ideal $\mathfrak{m} = Fu_1 + \cdots + Fu_{n-1}$. In particular for every element $x \in R_n$ one can write $x = a + m$, where $a \in F$ and $m \in \mathfrak{m}$. Set $I := R_n u_1 = Fu_1$. Then I is a minimal ideal of R_n. Let $x, y \in R_n$ and write $x = a + m$ and $y = b + m'$ where $a, b \in F$ and $m, m' \in \mathfrak{m}$. By (1) we have $mm' \in I$. So there exist $c \in F$ such that

$$xy = ay + bx + cu_1 - ab. \tag{2}$$

Let $r = r_F(R_n)$ and write $R_n = F[v_1, \cdots, v_r]$ for some $v_1, \cdots, v_r \in R_n$. Set $S = Fv_1 + \cdots + Fv_r \subseteq R_n$. By (2) every monomial in terms of $v_1, \cdots, v_r$ belongs to the subspace $S + Fu_1 + F$. Since these monomials generate R_n as an F-algebra and $\dim_F R_n = n$, we obtain $r \geq n-2$. On the other hand R_n is generated as an F-algebra by the elements $u_2, \cdots, u_{n-1}$, so $r_F(R_n) = r = n-2$.

Now suppose that n is even. We claim that I is the unique minimal ideal of R_n. Let $J \neq \{0\}$ be an ideal of R_n and let $0 \neq x \in J$. As $J \subseteq \mathfrak{m}$ we have

$$x = \sum_{i=1}^{n-1} a_i u_i, \tag{3}$$

for $a_1, \cdots, a_{n-1} \in F$. Set $b_i = (\sum_{j=2}^{n-1} a_j) - a_i$, $i = 2, \cdots, n-1$. Multiplying (3) by u_i we get $b_i u_1 \in J$, $i = 2, \cdots, n-1$. If $b_i \neq 0$ for some $2 \leq i \leq n-1$ then $u_1 \in J$ and $I \subseteq J$. Otherwise $b_2 = \cdots = b_{n-1} = 0$ which leads to a system of linear equations with respect to $a_2, \cdots, a_{n-1}$. As n is even (and $\operatorname{char} F = 2$) it is easy to see that the only solution of this system is the trivial solution, i.e., $a_2 = \cdots = a_{n-1} = 0$. Since $x \neq 0$ we obtain $a_1 \neq 0$, so again $u_1 \in J$, i.e., $I \subseteq J$. So the claim is proved and by (3.3), R_n is a Frobenius algebra. For every even integer $n \geq 6$ the algebra R_n is a totally singular conic algebra which is Frobenius, but $\dim_F R_n = n \neq 2^{n-2} = 2^{r_F(R_n)}$. Also even if $\dim_F R$ is a power of 2, the converse of (3.4) is not true; take $n = 2^k$, $k \geq 3$ and $R = R_n$.

Remark 3.6. Let R be a finite dimensional totally singular conic algebra over a field F of characteristic 2 and let $L \supseteq F$ be a subfield of R. If R is a field, then $r_L(R) + r_F(L) = r_F(R)$. This fact is an easy consequence of the multiplication formula $[R : F] = [R : L][L : F]$ and the fact that $[K : F] = 2^{r_F(K)}$ for every subfield $K \supseteq F$ of R.

Lemma 3.7. *Let R be a finite dimensional totally singular conic algebra over a field F of characteristic 2 and let $\mathfrak{m}$ be its unique maximal ideal mentioned in* (3.2). *Set $r = r_F(R/\mathfrak{m})$ and $n = r_F(R)$.*

(*i*) *If $K \supseteq F$ is a maximal subfield of R, then the residue field $R/\mathfrak{m}$ and K are isomorphic as F-algebras. In particular K is unique up to F-algebra isomorphism and $[K : F] = \dim_F R/\mathfrak{m} = 2^r$. Also for every $x \in R$ we have $x^2 \in K^2$.*

(*ii*) *There exist a maximal subfield $K \supseteq F$ of R and $u_1, \cdots, u_{n-r} \in \mathfrak{m}$ such that $R = K[u_1, \cdots, u_{n-r}]$.*

(*iii*) *We have $\ell\ell(R) \leq r_F(R) - r_F(R/\mathfrak{m}) + 1$.*

Proof. (*i*) Since $F \subseteq K \subseteq R$, R is a finite dimensional totally singular conic K-algebra as well. Since K is maximal, using (3.2 (*ii*)) we have $x^2 \in K^2$ for every $x \in R$. Consider the map $\varphi : K \to R/\mathfrak{m}$ defined by $\varphi(x) = x + \mathfrak{m}$. Clearly φ is an injective F-algebra homomorphism. We show that φ is surjective. Let $x+\mathfrak{m} \in R/\mathfrak{m}$, where $x \in R$. As $x^2 \in K^2$, there exists $y \in K$ such that $x^2 = y^2 \in K^2$, i.e., $(y + x)^2 = 0$. So we have $y + x \in \mathfrak{m}$ which implies that $\varphi(y) = y + \mathfrak{m} = x + \mathfrak{m}$.

(*ii*) By induction on n, we first prove that there exist a maximal subfield $K \supseteq F$ of R and $u_1, \cdots, u_{n-r} \in R$ such that $R = K[u_1, \cdots, u_{n-r}]$. Choose $v_1, \cdots, v_n \in R$ such that $R = F[v_1, \cdots, v_n]$. If $v_i^2 \in F^2$, for every $i = 1, \cdots, n$, then for every $u \in R$ we obtain $u^2 \in F^2$, so (3.2 (*ii*)) implies that every maximal subfield $K \supseteq F$ of R reduces to F, i.e., $r = 0$ and we are done. Otherwise (by re-indexing if necessary) we may assume that $v_1^2 \notin F^2$. Then $L := F[v_1]$ is a quadratic extension of F and $R = L[v_2, \cdots, v_n]$. By (3.3), R is a Frobenius L-algebra. We have $r_L(R) = n - 1$, also (3.6) implies that $r_L(R/\mathfrak{m}) = r_F(R/\mathfrak{m}) - r_F(L) = r - 1$. So by induction hypothesis there exist a maximal subfield $K \supseteq L$ of R and $u_1, \cdots, u_{n-r} \in R$ such that $R = K[u_1, \cdots, u_{n-r}]$.

Since K is maximal we have $u_i^2 \in K^2$, $i = 1, \cdots, n-r$. Replacing u_i with $u_i+\alpha_i$ for some $\alpha_i \in K$, we may assume that $u_i^2 = 0$, $i = 1, \cdots, n - r$.

(*iii*) By the previous part, there exist a maximal subfield $K \supseteq F$ and $u_1, \cdots, u_{n-r} \in \mathfrak{m}$ such that $R = K[u_1, \cdots, u_{n-r}]$. Consider arbitrary elements $x_1, \cdots, x_{n-r+1} \in \mathfrak{m}$. Since $K \cap \mathfrak{m} = \{0\}$, every x_i can be written as

$$x_i = \sum_{\substack{1\leq l\leq n-r \\ 1\leq i_1<\cdots<i_l\leq n-r}} \alpha_{i_1\cdots i_l} u_{i_1} \cdots u_{i_l}, \qquad \alpha_{i_1\cdots i_l} \in K.$$

So every monomial in the expansion of $x_1 \cdots x_{n-r+1}$ in terms of $u_1, \cdots, u_{n-r}$ has two identical u_i's. As $u_i^2 = 0$ we have $x_1 \cdots x_{n-r+1} = 0$. Thus we obtain $\mathfrak{m}^{n-r+1} = 0$, i.e., $\ell\ell(R) \leq r_F(R) - r_F(R/\mathfrak{m}) + 1$. □

The following result shows that (3.6) is also true for every finite dimensional totally singular conic algebra:

Corollary 3.8. *Let R be a finite dimensional totally singular conic algebra over a field F of characteristic 2. If $L \supseteq F$ is a subfield of R then $r_L(R)+r_F(L) = r_F(R)$.*

Proof. If $L = F$ (in other words $r_F(L) = 0$) the result trivially holds. So suppose that $r_F(L) \geq 1$. We obviously have $r_F(R) \leq r_L(R) + r_F(L)$. So it is enough to show that $r_F(R) \geq r_L(R) + r_F(L)$. We prove this for the case where $r_F(L) = 1$. The general case follows from induction. Let $\mathfrak{m}$ be the unique maximal ideal of R mentioned in (3.2), $r = r_F(R/\mathfrak{m})$ and $n = r_F(R)$. By (3.7 (*ii*)) there exist a maximal subfield $K \supseteq F$ of R and $u_1, \cdots, u_{n-r} \in \mathfrak{m}$ such that $R = K[u_1, \cdots, u_{n-r}]$. Write $L = F[u]$ for some $u \in R$ with $u^2 \in F^\times \setminus F^{\times 2}$. Extend L to a maximal subfield K' of R. By (3.7 (*i*)) we have $K' \simeq K$, so there exists $v_1 \in K$ such that $v_1^2 = u^2 \in F^\times \setminus F^{\times 2}$. Set $m := v_1+u \in R$. Since $m^2 = (v_1+u)^2 = 0$, we have $m \in \mathfrak{m}$. As $r_F(K) = r$ and K is a field, by (3.6) we have $r_{F[v_1]}(K) = r - 1$. So there exist $v_2, \cdots, v_r \in K$ such that $K = F[v_1, \cdots, v_r]$. Then $R = F[v_1, \cdots, v_r, u_1, \cdots, u_{n-r}]$. Set $S = L[v_2, \cdots, v_r, u_1, \cdots, u_{n-r}]$. We claim that $S = R$ which implies that

$r_L(R) \le n-1 = r_F(R)-1$. It is enough to show that $v_1 \in S$. As $R = K[u_1, \cdots, u_{n-r}]$, one can write

$$m = \sum_{\substack{1\le l\le n-r\\ 1\le i_1<\cdots<i_l\le n-r}} \alpha_{i_1\cdots i_l} u_{i_1}\cdots u_{i_l}, \qquad \alpha_{i_1\cdots i_l} \in K. \tag{4}$$

Every $\alpha_{i_1\cdots i_l} \in K = F[v_1, \cdots, v_r]$ can be written as

$$\alpha_{i_1\cdots i_l} = \beta_{i_1\cdots i_l} + \gamma_{i_1\cdots i_l} v_1,$$

where $\beta_{i_1\cdots i_l}, \gamma_{i_1\cdots i_l} \in F[v_2, \cdots, v_r] \subseteq S$. So by (4) there exist $s, s' \in S$ such that $m = v_1 s + s'$. As $u_1, \cdots, u_{n-r} \in \mathfrak{m}$ and $\mathfrak{m}$ is an ideal, we obtain $s, s' \in \mathfrak{m}$, so $s, s' \in S \cap \mathfrak{m}$. We obtain therefore $u = v_1 + m = v_1(1+s) + s'$, so $(1+s)u = v_1 + (1+s)s'$, i.e., $v_1 = (1+s)(u+s') \in S$. □

Remark 3.9. The statement of (3.7 (ii)) can be strengthened as follows: "For every maximal subfield $K \supseteq F$ of R there exist $u_1, \cdots, u_{n-r} \in \mathfrak{m}$ such that $R = K[u_1, \cdots, u_{n-r}]$." In fact by (3.8) we have $r_K(R) = n-r$. So there exist $u_1, \cdots, u_{n-r} \in R$ such that $R = K[u_1, \cdots, u_{n-r}]$. Since K is maximal we have $u_i^2 \in K^2$ for $i = 1, \cdots, n-r$. Replacing u_i with $u_i + \alpha_i$ for some $\alpha_i \in K$, we may assume that $u_1^2 = \cdots = u_{n-r}^2 = 0$.

Definition 3.10. Let R be a finite dimensional totally singular conic algebra over a field F of characteristic 2 and let $\mathfrak{m}$ be its unique maximal ideal. We say that R is a *ρ-generated* algebra if $r_F(R) = \rho(R)$ where $\rho(R) = \ell\ell(R) + r_F(R/\mathfrak{m}) - 1$.

Proposition 3.11. *Let F be a field of characteristic 2 and let R be a finite dimensional totally singular conic F-algebra. Then R is ρ-generated if and only if $\dim_F R = 2^{r_F(R)}$. In particular every ρ-generated totally singular conic algebra is a Frobenius algebra.*

Proof. By (3.2), R is a local commutative algebra. Let $\mathfrak{m}$ be the unique maximal ideal of R, $r = r_F(R/\mathfrak{m})$ and $n = r_F(R)$.

Suppose that R is a ρ-generated algebra. As $r_F(R) = n$ we have $\dim_F R \le 2^n$. So it is enough to show that $\dim_F R \ge 2^n$. Let $K \supseteq F$ be a maximal subfield of R and write $K = F[u_1, \cdots, u_r]$ for some $u_1, \cdots, u_r \in K$. Since $\ell\ell(R) = n-r+1$ we have $\mathfrak{m}^{n-r} \ne 0$, so there exist $v_1, \cdots, v_{n-r} \in \mathfrak{m}$ such that $v_1 \cdots v_{n-r} \ne 0$. We show that

$$\dim_K K[v_1, \cdots, v_{n-r}] = 2^{n-r}, \tag{5}$$

which concludes that

$$\dim_F R \ge \dim_F K \cdot \dim_K K[v_1, \cdots, v_{n-r}] = 2^n.$$

In order to prove (5), we claim that the set

$$W = \{1\} \cup \{v_{i_1} \cdots v_{i_l} : 1 \le i_1 < \cdots < i_l \le n-r,\ 1 \le l \le n-r\},$$

is linearly independent over K. Suppose that

$$\sum_{\substack{1\le l\le n-r\\ 1\le i_1<\cdots<i_l\le n-r}} \alpha_{i_1\cdots i_l} v_{i_1}\cdots v_{i_l} = \alpha, \qquad \alpha, \alpha_{i_1\cdots i_l} \in K, \tag{6}$$

where at least one of the above terms is nonzero and the number of nonzero terms is minimal. Since the left side of (6) belongs to $\mathfrak{m}$ we have $\alpha = 0$. As $v_j^2 = 0$, $j = 1, \cdots, n-r$, multiplying the equality (6) by v_j implies that either v_j does not appear in the above sum or appears in all terms. It follows that the only nonzero term of the left side of (6) is a multiple of $v_{j_1} \cdots v_{j_l}$ for some $1 \le j_1 < \cdots < j_l \le n-r$ and $1 \le l \le n-r$ which contradicts the assumption $v_1 \cdots v_{n-r} \ne 0$. So the claim is proved and $\dim_K K[v_1, \cdots, v_{n-r}] = 2^{n-r}$.

Conversely suppose that $\dim_F R = 2^n$. As $\dim_F K = 2^r$, we have $\dim_K R = 2^{n-r}$. By (3.9) there exist $u_1, \cdots, u_{n-r} \in \mathfrak{m}$ such that $R = K[u_1, \cdots, u_{n-r}]$. It follows that $u_1 \cdots u_{n-r} \neq 0$, i.e., $\mathfrak{m}^{n-r} \neq 0$. So $\ell\ell(R) \geq n - r + 1$ and thanks to (3.7 (*iii*)), R is a ρ-generated algebra. The last statement of the result follows from (3.4). □

Remark 3.12. For $n = 2^k$, $k \geq 3$, the totally singular conic algebra R_n constructed in (3.5) is a Frobenius algebra which is not ρ-generated, because $\dim_F R_n \neq 2^{r_F(R_n)}$. So the converse of the second statement of (3.11) does not hold.

The next result follows from (3.11) and the standard properties of tensor product.

Corollary 3.13. *Let R and R' be two finite dimensional ρ-generated totally singular conic algebras over a field F of characteristic 2. Then $R \otimes_F R'$ is also a ρ-generated totally singular conic F-algebra.*

Lemma 3.14. *Let (V, q) be a quadratic form over a field F of characteristic 2 and let $f : V \to C(V)$ be an F-linear map such that $f(v) \in Z(C(V))$ for every $v \in V$. Then the map f can be uniquely extended to an F-derivation $\delta : C(V) \to C(V)$.*

Proof. Let $T(V)$ be the tensor algebra of V with the canonical map $^- : T(V) \to C(V)$. Let $g : T(V) \to C(V)$ be the linear map induced by $g(1) = 0$ and

$$g(u_1 \otimes \cdots \otimes u_n) = f(u_1)\overline{u_2} \cdots \overline{u_n} + \overline{u_1} f(u_2)\overline{u_3} \cdots \overline{u_n} + \cdots + \overline{u_1} \cdots \overline{u_{n-1}} f(u_n), \tag{7}$$

for $u_1, \cdots, u_n \in V$. For every $w_1, w_2 \in T(V)$ we have

$$g(w_1 \otimes w_2) = \overline{w_1} g(w_2) + g(w_1)\overline{w_2}. \tag{8}$$

Let I be the ideal of $T(V)$ generated by the elements of the form $v \otimes v - q(v)$ for $v \in V$. We claim that $g(I) = 0$. For every $w \in T(V)$ and $v \in V$ we have

$$\begin{aligned} g(w \otimes (v \otimes v - q(v))) &= \overline{w} g(v \otimes v - q(v)) + g(w)(\overline{v \otimes v - q(v)}) \\ &= \overline{w} g(v \otimes v - q(v)) + 0 = \overline{w}(g(v \otimes v) - g(q(v))) \\ &= \overline{w} g(v \otimes v) = \overline{w}(\overline{v} f(v) + f(v)\overline{v}) = 0, \end{aligned}$$

where in the last equality we used the assumption $f(v) \in Z(C(V))$. Similarly for every $w \in T(V)$ and $v \in V$ we have $g((v \otimes v - q(v)) \otimes w) = 0$. So $g(I) = 0$ and g can be factored through $C(V)$, i.e., g induces a map $\delta : C(V) \to C(V)$. By (8), for every $w_1, w_2 \in C(V)$ we have $\delta(w_1 w_2) = w_1 \delta(w_2) + \delta(w_1) w_2$, so δ is a derivation.

The uniqueness of δ follows from the fact that V generates $C(V)$ as an F-algebra. □

Lemma 3.15. *Let R be a finite dimensional algebra over a field F of characteristic 2 and let $n = r_F(R)$. Then R is a ρ-generated totally singular conic F-algebra if and only if there exists a totally singular quadratic form (V, q) of dimension n over F such that $R \simeq C(V)$. In addition V can be chosen as the vector space generated by every generating subset $\{u_1, \cdots, u_n\}$ of R (as F-algebra) with $q(v) = v^2 \in F$ for every $v \in V$.*

Proof. First suppose that R is a ρ-generated totally singular conic F-algebra. Write $R = F[u_1, \cdots, u_n]$ for some $u_1, \cdots, u_n \in R$. Set $\alpha_i = u_i^2 \in F$, $i = 1, \cdots, n$ and $V = Fu_1 + \cdots + Fu_n \subseteq R$. Define the map $q : V \to F$ via $q(v) = v^2 \in F$. For every $u, v \in V$ we have $q(u + v) - q(u) - q(v) = (u + v)^2 - u^2 - v^2 = 0$. So q is a totally singular quadratic form. Consider the inclusion map $i : V \hookrightarrow R$. The map i is compatible with q and can be extended to an F-algebra homomorphism $\varphi : C(V) \to R$. As $R = F[u_1, \cdots, u_n]$, φ is surjective. Also using (3.11), we have $\dim_F R = 2^n = \dim_F C(V)$, so φ is an isomorphism.

Conversely suppose that $R \simeq C(V)$ for a totally singular quadratic form (V, q) over F. Let $\{v_1, \cdots, v_n\}$ be a basis of V over F. As (V, q) is totally singular, $C(V)$ is a totally singular conic F-algebra. Also as an F-algebra, $C(V)$ is generated by the set $\{v_1, \cdots, v_n\}$, i.e., $r_F(C(V)) \leq n$. Since $\dim_F C(V) = 2^n$ we obtain $n = r_F(C(V))$. So $\dim_F C(V) = 2^{r_F(C(V))}$ and by (3.11), $C(V)$ (and therefore R) is ρ-generated. $\square$

Corollary 3.16. *Let R and R' be two finite dimensional ρ-generated totally singular conic algebras over a field F of characteristic 2 with respective maximal subfields K and K'. Then there exists an F-algebra isomorphism $R \simeq R'$ if and only if $\dim_F R = \dim_F R'$ and $K \simeq K'$ as F-algebras.*

Proof. First suppose that $\dim_F R = \dim_F R'$ and $K \simeq K'$. By (3.11) we have $\dim_F R = 2^{r_F(R)}$ and $\dim_F R' = 2^{r_F(R')}$. So $\dim_F R = \dim_F R' = 2^n$, where $n = r_F(R) = r_F(R')$. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be respectively the unique maximal ideals of R and R' mentioned in (3.2) and set $r = r_F(R/\mathfrak{m})$. As $K \simeq K'$, by (3.7 (i)) we have $R/\mathfrak{m} \simeq R'/\mathfrak{m}'$ as F-algebras. So $r_F(R'/\mathfrak{m}') = r$. Also by (3.9) there exist $u_1, \cdots, u_{n-r} \in \mathfrak{m}$ and $u'_1, \cdots, u'_{n-r} \in \mathfrak{m}'$ such that $R = K[u_1, \cdots, u_{n-r}]$ and $R' = K'[u'_1, \cdots, u'_{n-r}]$. As $\dim_F R = 2^n$ and $\dim_F K = 2^r$, we have $\dim_K R = 2^{n-r}$. So the set $\{u_1, \cdots, u_{n-r}\}$ is linearly independent over K. Set $V = Ku_1 + \cdots + Ku_{n-r}$ and $V' = K'u'_1 + \cdots + K'u'_{n-r}$. Define the quadratic forms q on V and q' on V' via $q(v) = v^2$ and $q'(v') = v'^2$. Since $u_i \in \mathfrak{m}$ and $u'_i \in \mathfrak{m}'$, $i = 1, \cdots, n-r$, q and q' are zero maps. So $C(V) \simeq C(V')$ as K-algebras. On the other hand by (3.15) we have $R \simeq C(V)$ and $R' \simeq C(V')$ as F-algebras, so $R \simeq R'$ and we are done. The converse is trivial. $\square$

Proposition 3.17. *Let R be a finite dimensional totally singular conic algebra over a field F of characteristic 2 and let $n = r_F(R)$. Consider a subset $\mathcal{B} := \{u_1, \cdots, u_n\} \subseteq R$ which generates R as an F-algebra. Then the following statements are equivalent:*

- (i) *The algebra R is ρ-generated.*
- (ii) *Every map $f : \mathcal{B} \to R$ can be uniquely extended to an F-derivation $\delta : R \to R$.*
- (iii) *Every map $f : \mathcal{B} \to A$ satisfying $f(u_i)^2 = u_i^2 \in F$, $i = 1, \cdots, n$, can be uniquely extended to an F-algebra homomorphism $\varphi : R \to A$.*

Proof. Let $V = Fu_1 + \cdots + Fu_n$ and let $q : V \to F$ be the quadratic form defined by $q(v) = v^2$. By (3.15), R is ρ-generated if and only if $R \simeq C(V)$. So the equivalence $(i) \Leftrightarrow (iii)$ follows from the universal property of Clifford algebras and the implication $(i) \Rightarrow (ii)$ follows from (3.14).
$(ii) \Rightarrow (i)$: Let K be a maximal subfield of R and set $r = r_F(K)$. Let $\mathfrak{m}$ be the unique maximal ideal of R mentioned in (3.2). By (3.9) there exist $v_1, \cdots, v_{n-r} \in \mathfrak{m}$ such that $R = K[v_1, \cdots, v_{n-r}]$. We claim that $v_1 \cdots v_{n-r} \neq 0$. If $v_1 \cdots v_{n-r} = 0$, then there exists a minimal number $l \leq n-r$ and $1 \leq i_1 < i_2 < \cdots < i_l \leq n-r$ such that

$$v_{i_1} \cdots v_{i_l} = 0. \tag{9}$$

Choose $v_{n-r+1}, \cdots, v_n \in R$ such that $K = F[v_{n-r+1}, \cdots, v_n]$, so $\{v_1, \cdots, v_n\}$ generates R as an F-algebra. Let $f : \{v_1, \cdots, v_n\} \to R$ be the map defined by $f(v_{i_1}) = 1$ and $f(v_j) = 0$ for every $j \neq i_1$. By the hypothesis, f can be extended to a derivation δ on R. Note that $l \geq 2$, because all v_i's are nonzero. Applying δ to (9) we obtain $v_{i_2} \cdots v_{i_l} = 0$, which contradicts the minimality of l. So the claim is proved and we have $\mathfrak{m}^{n-r} \neq 0$. It follows that $\ell\ell(R) \geq n-r+1$ and thanks to (3.7 (iii)), R is a ρ-generated algebra. $\square$

4. Decomposability in terms of Frobenius subalgebras

Remarks 4.1. Let (Q, σ) be a quaternion algebra with involution over a field F of characteristic 2.
(i) There exists $u \in \mathrm{Sym}(Q, \sigma) \setminus F$ such that $u^2 \in F^\times$. In fact if σ is of symplectic type and $u \in \mathrm{Sym}(Q, \sigma)$, then u has trivial reduced trace (see [15, pp. 25-26]), so $u^2 \in F$. Replacing u with $u+1$ we may assume that $u^2 \in F^\times$. If σ is of orthogonal type, $\mathrm{Alt}(Q, \sigma)$ is one dimensional and by [15, (2.8 (2))] every nonzero element in $\mathrm{Alt}(Q, \sigma)$ is invertible. So for every $0 \neq u \in \mathrm{Alt}(Q, \sigma)$ we have $u^2 = \mathrm{Nrd}_Q(u) \in F^\times$, where $\mathrm{Nrd}_Q(u)$ is the reduced norm of u in Q.
(ii) If t is the transpose involution, $(Q, \sigma) \simeq (M_2(F), t)$ if and only if σ is of orthogonal type and $\mathrm{disc}\, \sigma$ is trivial, see [15, (7.4)].

The proof of the following result uses the method of that of [16, (3.7)] and [19][1]. The technique was only applied for biquaternion algebras, but the main idea of the general case was present there.

Lemma 4.2. *Let (A, σ) be a central simple algebra with involution over a field F of characteristic 2. Suppose that there exists a totally singular conic subalgebra $S \subseteq \mathrm{Sym}(A, \sigma)$ such that $C_A(S) = S$ and $\dim_F S = 2^r$, where $r = r_F(S)$.*

- (i) *There exists a quaternion F-subalgebra $Q \subseteq A$ such that $\sigma(Q) = Q$.*
- (ii) *If $S = F[u_1, \cdots, u_r]$, where $u_1, \cdots, u_r \in S$, then the quaternion subalgebra Q in part (i) can be chosen so that $F[u_2, \cdots, u_r] \subseteq C_A(Q)$.*
- (iii) *If σ is of orthogonal type, then the quaternion subalgebra Q in part (i) can be chosen so that $S \cap \mathrm{Alt}(Q, \sigma|_Q)$ has an invertible element.*

Proof. (i) By (3.4), S is a Frobenius algebra. Write $S = F[u_1, \cdots, u_r]$, where $u_i \in S$. Replacing u_i with $u_i + 1$ if necessary, which doesn't change $F[u_2, \cdots, u_r]$ and S, we may assume that

$$0 \neq u_i^2 \in F, \ i = 1, \cdots, r. \tag{10}$$

By (3.17), there exists an F-derivation δ of S induced by $\delta(u_1) = u_1$ and $\delta(u_i) = 0$, $i = 2, \cdots, r$. By (2.1 (ii)), δ extends to an inner derivation δ_ξ of A for some $\xi \in A$. As $\delta^2 = \delta$ on S, the element $\xi^2 + \xi$ commutes with S, so $\xi^2 + \xi \in C_A(S) = S$. Let $\eta = \xi^2 \in A$. We have

$$\eta^2 + \eta = \xi^4 + \xi^2 = (\xi^2 + \xi)^2 \in F. \tag{11}$$

Since ξ and ξ^2 induce the same derivation δ on S, we have

$$\eta u_1 + u_1 \eta = \xi u_1 + u_1 \xi = \delta(u_1) = u_1. \tag{12}$$

For $x \in S$ the relations

$$\delta_{\sigma(\xi)}(x) = \sigma(\xi)x - x\sigma(\xi) = \sigma(\xi)\sigma(x) - \sigma(x)\sigma(\xi) = \sigma(x\xi - \xi x) = x\xi - \xi x,$$

imply that the elements ξ and $\sigma(\xi)$ also induce the same derivation δ on S. Thus $\sigma(\xi) = \xi + s$ for some $s \in S$ and

$$\sigma(\eta) = \sigma(\xi)^2 = (\xi + s)^2 = \eta + \delta(s) + s^2, \tag{13}$$

with $\delta(s) \in S$, since S is stable under δ. Also

$$s^2 \in F, \tag{14}$$

since S is totally singular conic algebra. Now consider two cases.
Case 1. If $\delta(s) \in F$, then (13) implies that $\eta + \sigma(\eta) \in F$. By (10), (11) and (12), u_1 and η generate a quaternion algebra Q, which is invariant under σ, because

[1] We are grateful to Professor M.-A. Knus for making [19] available to us.

$\eta + \sigma(\eta) \in F$.
Case 2. If $\delta(s) \in S \setminus F$, we obtain

$$\delta(s) = \delta^2(s) = \delta_{\xi^2}(\delta(s)) = \eta\delta(s) + \delta(s)\eta. \tag{15}$$

Then by (11), (14) and (15), η and $\delta(s)$ generate a quaternion subalgebra Q of A, which is invariant under σ thanks to (13).
(ii) Since $\delta(u_2) = \cdots = \delta(u_r) = 0$, in both cases above $F[u_2, \cdots, u_r]$ commutes with η, thus $F[u_2, \cdots, u_r] \subseteq C_A(Q)$.
(iii) Suppose that σ is of orthogonal type. In case 1 above, as $\eta + \sigma(\eta) \in F$, we obtain $\eta = \sigma(\eta)$. Therefore using (12) we get $\eta u_1 + \sigma(\eta u_1) = \eta u_1 + u_1\eta = u_1$, so $u_1 \in S \cap \mathrm{Alt}(Q, \sigma|_Q)$. Similarly in the case 2, we have $\delta(s) + s^2 \in S \cap \mathrm{Alt}(Q, \sigma|_Q)$ by (13). So in both cases there exists a nonzero element in $S \cap \mathrm{Alt}(Q, \sigma|_Q)$ which is invertible by [15, (2.8 (2))]. □

Corollary 4.3. *Let (A, σ) be a central simple algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2. Suppose that there exists a totally singular conic subalgebra $S \subseteq \mathrm{Sym}(A, \sigma)$ such that $C_A(S) = S$ and $\dim_F S = 2^{r_F(S)}$. Then for $i = 1, \cdots, n$, there exists a σ-invariant quaternion algebra $Q_i \subseteq A$ and an invertible element $v_i \in S \cap \mathrm{Alt}(Q_i, \sigma|_{Q_i})$ such that $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma|_{Q_i})$ and $S = F[v_1, \cdots, v_n]$. In particular $\dim_F S = 2^n$.*

Proof. Set $r = r_F(S)$. Write $S = F[u_1, \cdots, u_r]$ for some $u_1, \cdots, u_r \in S$ and set $S' = F[u_2, \cdots, u_r]$. By (4.2 (i)) there exists a quaternion subalgebra Q_1 of A such that $(A, \sigma) \simeq (Q_1, \sigma|_{Q_1}) \otimes (B, \tau)$, where $B = C_A(Q_1)$ and $\tau = \sigma|_B$. Also by (4.2 (ii)), Q_1 can be chosen such that $S' \subseteq C_A(Q_1) = B$. We have

$$F[u_1] \otimes S' \simeq S = C_A(S) \simeq C_{Q_1}(F[u_1]) \otimes C_B(S') \simeq F[u_1] \otimes C_B(S'),$$

so $\dim_F C_B(S') = \dim_F S'$. As S' is commutative we obtain $C_B(S') = S'$. Since $\dim_F S' = 2^{r_F(S')}$, the induction can be applied to B and we obtain $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma_i)$ where (Q_i, σ_i) is a quaternion algebra over F with involution.

By (4.2 (iii)) for every i there exists an invertible element $v_i \in S \cap \mathrm{Alt}(Q_i, \sigma|_{Q_i})$. We claim that $S = F[v_1, \cdots, v_n]$. Set $S'' = F[v_1, \cdots, v_n] \subseteq S$. Then $\dim_F S'' = 2^n = 2^{r_F(S'')}$, so by (3.4) and (2.1 (i)), S'' is a Frobenius algebra and $C_A(S'') = S''$. As $S'' \subseteq S$ and $C_A(S) = S$, we have $S'' = S$. □

Remark 4.4. The converse of (4.3) is trivially true. In fact let $(A, \sigma) = \bigotimes_{i=1}^n (Q_i, \sigma_i)$ be a totally decomposable algebra with involution over a field F of characteristic 2. By (4.1) there exists $v_i \in \mathrm{Sym}(Q_i, \sigma_i)$ such that $v_i^2 \in F^\times$. Set $S = F[v_1, \cdots, v_n] \subseteq \mathrm{Sym}(A, \sigma)$. Then S is a totally singular conic F-algebra and $\dim_F S = 2^n = 2^{r_F(S)}$. By (3.4) and (2.1 (i)), we have $C_A(S) = S$.

Theorem 4.5. *Let (A, σ) be a central simple algebra of degree 2^n with involution over a field F of characteristic 2. Then the following statements are equivalent:*

- (i) *(A, σ) is totally decomposable.*
- (ii) *There exists a ρ-generated totally singular conic F-algebra $S \subseteq \mathrm{Sym}(A, \sigma)$ such that $C_A(S) = S$.*

Furthermore if σ is of orthogonal type then for every F-algebra S satisfying (ii), we have necessarily $S \subseteq \mathrm{Alt}(A, \sigma) + F$. More precisely there exist $v_1, \cdots, v_n \in \mathrm{Alt}(A, \sigma) \cap A^*$ such that $S = F[v_1, \cdots, v_n]$ and $v_{i_1} \cdots v_{i_l} \in \mathrm{Alt}(A, \sigma)$ for every $1 \leq i_1 < \cdots < i_l \leq n$ and $1 \leq l \leq n$. Thus, if σ is of orthogonal type the statement (ii) can be replaced by the following:

- (iii) *There exists a ρ-generated totally singular conic F-algebra $S \subseteq \mathrm{Alt}(A, \sigma) + F$ such that $C_A(S) = S$.*

Finally if S is any subalgebra of A satisfying the condition (ii) or (iii) then $r_F(S) = n$ and $\dim_F S = \deg_F A = 2^n$.

Proof. The equivalence $(i) \Leftrightarrow (ii)$ follows from (3.11), (4.3) and (4.4).

If σ is of orthogonal type, then by (4.3) for every i there exists an invertible element $v_i \in S \cap \mathrm{Alt}(Q_i, \sigma_i)$ such that $S = F[v_1, \cdots, v_n]$. Choose an element $w_i \in Q_i$ such that $v_i = w_i - \sigma(w_i)$, $i = 1, \cdots, n$. Then $v_{i_1} \cdots v_{i_l} = w_{i_1} v_{i_2} \cdots v_{i_l} - \sigma(w_{i_1} v_{i_2} \cdots v_{i_l}) \in \mathrm{Alt}(A, \sigma)$ for every $1 \leq i_1 < \cdots < i_l \leq n$ and $1 \leq l \leq n$.

The last statement of the result follows from (4.3). □

5. A new description of the Pfister invariant

Definition 5.1. Let (A, σ) be a totally decomposable algebra with involution of orthogonal type over a field F of characteristic 2. By (4.5 (ii)) there exists a ρ-generated totally singular conic algebra $S \subseteq \mathrm{Sym}(A, \sigma)$ such that $C_A(S) = S$. By (4.5 (iii)) we have necessarily $S \subseteq \mathrm{Alt}(A, \sigma) + F$ and there exist $v_1, \cdots, v_n \in \mathrm{Alt}(A, \sigma) \cap A^*$ such that $S = F[v_1, \cdots, v_n]$ and $v_{i_1} \cdots v_{i_l} \in \mathrm{Alt}(A, \sigma)$ for $1 \leq i_1 < \cdots < i_l \leq n$ and $1 \leq l \leq n$. We call the set $\{v_1, \cdots, v_n\}$, a *set of alternating generators* of S.

Definition 5.2. Let (A, σ) be a totally decomposable algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2 and let $S \subseteq \mathrm{Sym}(A, \sigma)$ be a ρ-generated totally singular conic algebra such that $C_A(S) = S$. Define a map $\mathfrak{s} : S \times S \to F$ as follows: for every $v, w \in S$, as $vw \in S \subseteq \mathrm{Alt}(A, \sigma) + F$, there exists a unique $\alpha \in F$ such that $vw + \alpha \in \mathrm{Alt}(A, \sigma)$. Set $\mathfrak{s}(v, w) = \alpha$. It is easy to see that $\mathfrak{s}$ is a symmetric bilinear form on S. Note that for every $v \in S$, as $v^2 \in F$ and $F \cap \mathrm{Alt}(A, \sigma) = \{0\}$, we obtain

$$\mathfrak{s}(v, v) = v^2 \in F. \tag{16}$$

Furthermore for every $u, v, w \in S$ and $\alpha \in F$, we have $u(vw) + \alpha \in \mathrm{Alt}(A, \sigma)$ if and only if $(uv)w + \alpha \in \mathrm{Alt}(A, \sigma)$, so $\mathfrak{s}(u, vw) = \mathfrak{s}(uv, w)$, i.e., $\mathfrak{s}$ is an *associative* bilinear form. We also have the orthogonal decomposition $S = F \perp S_0$ with respect to $\mathfrak{s}$, where $S_0 = S \cap \mathrm{Alt}(A, \sigma)$.

Remark 5.3. Let (A, σ) be a totally decomposable algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2 and let $S \subseteq \mathrm{Sym}(A, \sigma)$ be a ρ-generated totally singular conic algebra such that $C_A(S) = S$. If $\{v_1, \cdots, v_n\}$ is a set of alternating generators of S with $v_i^2 = \alpha_i \in F^\times$ and $\mathfrak{s}$ is the bilinear form defined in (5.2), then $\mathfrak{s} \simeq \langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$; in particular $\mathfrak{s}$ is nondegenerate.

Definition 5.4. Let $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma_i)$ be a totally decomposable algebra with involution of orthogonal type over a field F of characteristic 2 and let $\alpha_i \in F^\times$, $i = 1, \cdots, n$, be a representative of the class $\operatorname{disc} \sigma_i \in F^\times / F^{\times 2}$. In [7] it is shown that the bilinear n-fold Pfister form $\mathfrak{Pf}(A, \sigma) := \langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$ is independent of the decomposition of (A, σ). As in [7] we call this form the *Pfister invariant* of (A, σ).

The following result gives another description of $\mathfrak{Pf}(A, \sigma)$:

Lemma 5.5. *Let (A, σ) be a totally decomposable algebra with involution of orthogonal type over a field F of characteristic 2 and let $S \subseteq \mathrm{Sym}(A, \sigma)$ be a ρ-generated totally singular conic algebra such that $C_A(S) = S$. Then the bilinear form $\mathfrak{s}$ on S defined in (5.2) is isometric to $\mathfrak{Pf}(A, \sigma)$.*

Proof. By (4.3) there exists a σ-invariant quaternion algebra $Q_i \subseteq A$, $i = 1, \cdots, n$ with $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma|_{Q_i})$ and an invertible element $v_i \in \mathrm{Alt}(Q_i, \sigma|_{Q_i})$ such that $S = F[v_1, \cdots, v_n]$ and $v_i^2 = \alpha_i \in F^\times$, $i = 1, \cdots, n$. Then $\{v_1, \cdots, v_n\}$ is set of alternating generators of S and $\mathfrak{s} \simeq \langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$. We also have $\operatorname{disc} \sigma_i = \operatorname{Nrd}_{Q_i}(v_i) F^{\times 2} = \alpha_i F^{\times 2} \in F^\times / F^{\times 2}$, so $\mathfrak{Pf}(A, \sigma) \simeq \langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle \simeq \mathfrak{s}$. □

Let $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_n \in F^\times$. The bilinear Pfister forms $\langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$ and $\langle\langle \beta_1, \cdots, \beta_n \rangle\rangle$ are said to be *simply P-equivalent* if either $n = 1$ and $\alpha_1 F^{\times 2} = \beta_1 F^{\times 2}$ or $n \geq 2$ and there exist $1 \leq i < j \leq n$ such that $\langle\langle \alpha_i, \alpha_j \rangle\rangle \simeq \langle\langle \beta_i, \beta_j \rangle\rangle$ and $\alpha_k = \beta_k$ for $k \neq i, j$. We say that two bilinear Pfister forms $\mathfrak{b}$ and $\mathfrak{c}$ are *chain P-equivalent*, if there exist bilinear Pfister forms $\mathfrak{b}_0, \cdots, \mathfrak{b}_m$ such that $\mathfrak{b} = \mathfrak{b}_0$, $\mathfrak{c} = \mathfrak{b}_m$ and for every $i = 0, \cdots, m-1$, $\mathfrak{b}_i$ and $\mathfrak{b}_{i+1}$ are simply P-equivalent.

Proposition 5.6. *Let (A, σ) be a totally decomposable algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2 and let $S \subseteq \operatorname{Sym}(A, \sigma)$ be a ρ-generated totally singular conic algebra such that $C_A(S) = S$. Let $\mathfrak{s}$ be the bilinear form on S defined in* (5.2). *If $\mathfrak{s} \simeq \langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$ for some $\alpha_1, \cdots, \alpha_n \in F^\times$, then there exists a set of alternating generators $\{u_1, \cdots, u_n\}$ of S such that $u_i^2 = \alpha_i$, $i = 1, \cdots, n$.*

Proof. First suppose that $n = 1$ and let $\{v_1\}$ is a set of alternating generators of S with $v_1^2 = \beta \in F^\times$. Since A is a quaternion algebra, we have $\operatorname{disc} \sigma = \operatorname{Nrd}_A(v_1) = \beta F^{\times 2} \in F^\times / F^{\times 2}$ and the result follows from [15, (7.4)].

Now suppose that $n = 2$. Set $S_0 = S \cap \operatorname{Alt}(A, \sigma) = F^\perp$, $\mathfrak{s}_0 = \mathfrak{s}|_{S_0 \times S_0}$ and $\mathfrak{b} = \langle\langle \alpha_1, \alpha_2 \rangle\rangle$. As $\mathfrak{s} \simeq \mathfrak{b}$, by [2, p. 16] the pure subforms of these forms are also isometric. So $\mathfrak{s}_0 \simeq \langle \alpha_1, \alpha_2, \alpha_1\alpha_2 \rangle$. Let V be the underlying vector space of $\mathfrak{b}_0 := \langle \alpha_1, \alpha_2, \alpha_1\alpha_2 \rangle$ with a respective orthogonal basis $\{v_1, v_2, v_3\}$. Let $f : (V, \mathfrak{b}_0) \simeq (S_0, \mathfrak{s}_0)$ be an isometry and set $u_i = f(v_i) \in S_0$, $i = 1, 2$. We have $u_i^2 = f(v_i)^2 = v_i^2 = \alpha_i$, $i = 1, 2$. We also have $\mathfrak{s}(1, u_1u_2) = \mathfrak{s}(u_1, u_2) = \mathfrak{b}(v_1, v_2) = 0$, so $u_1u_2 \in F^\perp = S_0 \subseteq \operatorname{Alt}(A, \sigma)$. Thus $\{u_1, u_2\}$ is the desired set of alternating generators of S.

Finally suppose that $n \geq 3$. Let $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma_i)$ be a decomposition of (A, σ) and let $v_i \in \operatorname{Alt}(Q_i, \sigma_i)$ with $v_i^2 = \beta_i \in F^\times$, $i = 1, \cdots, n$. Then $\{v_1, \cdots, v_n\}$ is set of alternating generators of S and by (5.3) we have $\mathfrak{s} \simeq \langle\langle \beta_1, \cdots, \beta_n \rangle\rangle$, so

$$\langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle \simeq \langle\langle \beta_1, \cdots, \beta_n \rangle\rangle.$$

By [2, (A. 1)] there exist bilinear n-fold Pfister forms $\mathfrak{b}_0, \cdots, \mathfrak{b}_m$ such that $\mathfrak{b}_0 = \langle\langle \beta_1, \cdots, \beta_n \rangle\rangle$, $\mathfrak{b}_m = \langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$ and for every $i = 0, \cdots, m-1$, $\mathfrak{b}_i$ is simply P-equivalent to $\mathfrak{b}_{i+1}$. In order to prove the result, using induction on m, it is enough to consider the case where $\langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$ and $\langle\langle \beta_1, \cdots, \beta_n \rangle\rangle$ are simply P-equivalent. By re-indexing if necessary we may assume that $\langle\langle \alpha_1, \alpha_2 \rangle\rangle \simeq \langle\langle \beta_1, \beta_2 \rangle\rangle$ and $\alpha_i = \beta_i$ for $i \geq 3$. Set $(B, \tau) = (Q_1, \sigma_1) \otimes (Q_2, \sigma_2)$ and $S' = F[v_1, v_2]$. Then $S' \subseteq \operatorname{Sym}(B, \tau)$ is a ρ-generated totally singular conic algebra and $C_B(S') = S'$. As proved in the case $n = 2$, there exists a set of alternating generators $\{u_1, u_2\}$ of S' such that $u_i^2 = \alpha_i$, $i = 1, 2$. We have $S = S' \otimes F[v_3, \cdots, v_n] \simeq F[u_1, u_2] \otimes F[v_3, \cdots, v_n]$. So $\{u_1, u_2, v_3, \cdots, v_n\}$ is the desired set of alternating generators of S. □

Proposition 5.7. *Let (A, σ) be a totally decomposable algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2 and let $S \subseteq \operatorname{Sym}(A, \sigma)$ be a ρ-generated totally singular conic algebra such that $C_A(S) = S$. Then the following statements are equivalent: (i) $(A, \sigma) \simeq (M_{2^n}(F), t)$. (ii) $\mathfrak{Pf}(A, \sigma) \simeq \langle\langle 1, \cdots, 1 \rangle\rangle$. (iii) $u^2 \in F^2$ for every $u \in S$. (iv) Every maximal subfield of S containing F reduces to F.*

Proof. The implication $(i) \Rightarrow (ii)$ follows from the fact that the transpose involution in characteristic 2 has trivial discriminant, see [15, p. 82].

$(ii) \Rightarrow (i)$: Let $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma_i)$ be a decomposition of (A, σ) to quaternion algebras with involution over F. Since $\operatorname{char} F = 2$ a sum of squares in F is again a square, so $D_F(\mathfrak{Pf}(A,\sigma)) = D_F(\langle\langle 1,\cdots,1\rangle\rangle) = F^2$. It follows that for every i, $\operatorname{disc}\sigma_i$ is trivial. So by (4.1) we have $(Q_i,\sigma_i) \simeq (M_2(F),t)$ which implies that $(A,\sigma) \simeq (M_{2^n}(F),t)$. The equivalence $(ii) \Leftrightarrow (iii)$ follows from (5.3), (5.5) and (5.6) and $(iii) \Leftrightarrow (iv)$ follows from (3.2). □

The proof of the following result is left to the reader.

Lemma 5.8. *Let (A,σ) be a totally decomposable algebra with involution of orthogonal type over a field F of characteristic 2 and let $S \subseteq \operatorname{Sym}(A,\sigma)$ be a ρ-generated totally singular conic F-algebra such that $C_A(S) = S$. If K/F is a field extension, then $S_K \subseteq \operatorname{Sym}(A_K,\sigma_K)$ is a ρ-generated totally singular conic K-algebra and $C_{A_K}(S_K) = S_K$.*

Lemma 5.9. *Let (A,σ) be a totally decomposable algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2 and let $S \subseteq \operatorname{Sym}(A,\sigma)$ be a ρ-generated totally singular conic algebra such that $C_A(S) = S$. If $K \supseteq F$ is a maximal subfield of S, then $(A_K,\sigma_K) \simeq (M_{2^n}(K),t)$. In particular K is a splitting field of A.*

Proof. By (5.8), $S_K \subseteq \operatorname{Sym}(A_K,\sigma_K)$ is a ρ-generated totally singular conic algebra and $C_{A_K}(S_K) = S_K$. As K is a maximal subfield of S, by (3.2) we have $u^2 \in K^2$ for every $u \in S$. This, together with $K^2 \subseteq S^2 \subseteq F$ implies that $x^2 \in K^2$ for every $x \in S_K$. So by (5.7) we have $(A_K,\sigma_K) \simeq (M_{2^n}(K),t)$. □

Let (A,σ) be a totally decomposable algebra with involution of orthogonal type over a field F of characteristic 2. By [7, (7.2)], (5.5) and (5.6) all ρ-generated totally singular conic subalgebras S of (A,σ) with $S \subseteq \operatorname{Sym}(A,\sigma)$ and $C_A(S) = S$ are isomorphic as F-algebras. Here, we give a proof of this fact which is independent from [7]:

Lemma 5.10. *Let (A,σ) be a totally decomposable algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2 and let S and S' be two ρ-generated totally singular conic subalgebras of (A,σ) such that $S, S' \subseteq \operatorname{Sym}(A,\sigma)$, $C_A(S) = S$ and $C_A(S') = S'$.*

(*i*) *If $K \supseteq F$ and $K' \supseteq F$ are respectively maximal subfields of S and S', then $K \simeq K'$ as F-algebras.*
(*ii*) *We have $S \simeq S'$ as F-algebras.*

Proof. By (5.9) we have $(A_K,\sigma_K) \simeq (M_{2^n}(K),t)$. Also according to (5.8), S'_K is a ρ-generated totally singular conic subalgebra of (A_K,σ_K) with $S'_K \subseteq \operatorname{Sym}(A_K,\sigma_K)$ and $C_{A_K}(S'_K) = S'_K$. So we have $u^2 \in K^2$ for every $u \in S'_K$ by (5.7). In particular if $K' = F[v'_1,\cdots,v'_r]$, where $r = r_F(K')$ and $v'_1,\cdots,v'_r \in K' \subseteq S' \subseteq S'_K$, then ${v'_i}^2 \in K^2$, $i = 1,\cdots,r$. So for every i there exists $v_i \in K$ such that $v_i^2 = {v'_i}^2 \in K^2$. By (3.17) the linear map $f : K' \to K$ induced by $f(v'_i) = v_i$ is an F-algebra homomorphism. As K' is a field, f is a monomorphism. Similarly there exists an F-algebra monomorphism $K \hookrightarrow K'$. So $\dim_F K = \dim_F K'$ and $K \simeq K'$ as F-algebras. This proves (i). The statement (ii) follows from (i) and (3.16). □

Notation 5.11. Let (A,σ) be a totally decomposable algebra with involution of orthogonal type over a field F of characteristic 2. In view of (5.10 (ii)) there exists, up to isomorphism, a unique ρ-generated totally singular conic algebra $S \subseteq \operatorname{Sym}(A,\sigma)$ such that $C_A(S) = S$. We denote this algebra by $\Phi(A,\sigma)$. Note that if $\mathfrak{s}$ is the bilinear form on $\Phi(A,\sigma)$ defined in (5.2), then $\mathfrak{s} \simeq \mathfrak{Pf}(A,\sigma)$ by (5.5).

Remark 5.12. Let (Q,σ) be a quaternion algebra with involution over a field F of characteristic 2. Then $\Phi(Q,\sigma) = F + \operatorname{Alt}(Q,\sigma)$. In fact by (4.5) we have $\Phi(Q,\sigma) \subseteq F + \operatorname{Alt}(Q,\sigma)$ and $\dim \Phi(Q,\sigma) = 2$. As $\operatorname{Alt}(Q,\sigma)$ is one dimensional, we obtain $\Phi(Q,\sigma) = F + \operatorname{Alt}(Q,\sigma)$.

Corollary 5.13. *Let (A,σ) and (B,τ) be two totally decomposable algebras with involution of orthogonal type over a field F of characteristic 2. Then we have $\Phi(A\otimes B,\sigma\otimes\tau)\simeq\Phi(A,\sigma)\otimes\Phi(B,\tau)$.*

Proof. (i) Set $S=\Phi(A,\sigma)\otimes\Phi(B,\tau)$. Then $S\subseteq \mathrm{Sym}(A\otimes B,\sigma\otimes\tau)$ is a totally singular conic F-algebra and $C_{A\otimes B}(S)=S$. Also by (3.13), S is a ρ-generated algebra. So by (5.10 (ii)), we have $\Phi(A\otimes B,\sigma\otimes\tau)\simeq S$. The part (ii) follows from (5.8) and (5.10 (ii)). □

6. Some characterizing properties of the Pfister invariant

Lemma 6.1. (Compare [5, (2.4)]) *Let K/F be a finite extension of fields of characteristic 2 and let (Q,σ) be a quaternion algebra with involution of orthogonal type over K. If $u^2\in F$ for every $u\in\Phi(Q,\sigma)$, then there exists a quaternion F-subalgebra $Q_0\subseteq Q$ such that $\sigma(Q_0)=Q_0$, i.e., $(Q,\sigma)\simeq_K(Q_0,\sigma|_{Q_0})\otimes(K,\mathrm{id})$.*

Proof. The idea of the proof is similar to the proof of (4.2). Set $S=\Phi(Q,\sigma)$. By (5.12) we have $S=K+\mathrm{Alt}(Q,\sigma)=K[u]$, where $0\neq u\in\mathrm{Alt}(Q,\sigma)$. Let δ be the K-derivation of S induced by $\delta(u)=u$. By (2.1 (ii)), δ extends to an inner derivation δ_ξ of Q for some $\xi\in Q$. Let $\eta=\xi^2\in Q$. As $\xi^2+\xi\in C_Q(S)=S$, we obtain $(\xi^2+\xi)^2\in F$ and $(\xi+\xi^2)u=u(\xi+\xi^2)$, thus

$$\eta^2+\eta=\xi^4+\xi^2=(\xi^2+\xi)^2\in F,\quad \eta u+u\eta=\xi u+u\xi=\delta(u)=u.$$

So the F-algebra generated by u and η is a quaternion algebra. As $\mathrm{Alt}(Q,\sigma)=Ku$, we have $\eta+\sigma(\eta)=\alpha u$ for some $\alpha\in K$. If $\alpha\in F$, then the quaternion F-algebra Q_0 generated by u and η is invariant under σ. Otherwise $\alpha\neq 0$ and the quaternion F-algebra Q_0 generated by αu and η is invariant under σ. □

Corollary 6.2. *Let K/F be a finite extension of fields of characteristic 2. Let (A,σ) be a totally decomposable algebra with involution of orthogonal type over K. If $u^2\in F$ for every $u\in\Phi(A,\sigma)$, then there exists a central simple F-algebra $B\subseteq A$ such that $(A,\sigma)\simeq_K(B,\sigma|_B)\otimes(K,\mathrm{id})$.*

Proof. Let $(A,\sigma)\simeq_K\bigotimes_{i=1}^n(Q_i,\sigma_i)$ be a decomposition of (A,σ) into quaternion K-algebras with involution and choose an invertible element $u_i\in\mathrm{Alt}(Q_i,\sigma_i)$, $i=1,\cdots,n$. Then we have $\Phi(A,\sigma)\simeq K[u_1,\cdots,u_n]$, so $u_i^2\in F^\times$ for $i=1,\cdots,n$. It follows from (5.13) that $u^2\in F$ for every $u\in\Phi(Q_i,\sigma_i)$. So by (6.1), $(A,\sigma)\simeq_K\bigotimes_{i=1}^n(Q_i',\sigma|_{Q_i'})\otimes(K,\mathrm{id})$, where Q_i' is a quaternion F-subalgebra of Q_i. □

Lemma 6.3. *Let (A,σ) be a totally decomposable algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2. Consider an element $u\in\Phi(A,\sigma)$ with $u^2\in F^\times\setminus F^{\times2}$. Set $B=C_A(u)$ and $K=F[u]$.*

- (i) *The pair $(B,\sigma|_B)$ is a totally decomposable algebra with involution of orthogonal type over K and $\Phi(B,\sigma|_B)\simeq\Phi(A,\sigma)$ as K-algebras.*
- (ii) *There exists a quaternion algebra $Q\subseteq A$ containing u such that $\sigma(Q)=Q$.*

Proof. (i) Since $\sigma(u)=u$, $\sigma|_B$ is of the first kind. We also have $1\notin\mathrm{Alt}(A,\sigma)$ which implies that $1\notin\mathrm{Alt}(B,\sigma|_B)$, so $\sigma|_B$ is of orthogonal type. Set $S=\Phi(A,\sigma)$. By (3.8) we have $r_K(S)=r_F(S)-1=n-1$. So $\dim_K S=2^{r_K(S)}$ and using (3.11), S is a Frobenius ρ-generated K-algebra. As $\dim_K S=\deg_K B$, by (2.1 (i)) we have $C_B(S)=S$. By (4.5) and (5.10 (ii)) $(B,\sigma|_B)$ is totally decomposable and $\Phi(B,\sigma|_B)\simeq S$.

(ii) As $u^2\in F$ for every $u\in\Phi(B,\sigma|_B)\simeq S$, by (6.2) there exists a central simple F-algebra $B_0\subseteq B$ such that $(B,\sigma|_B)\simeq_K(B_0,\sigma|_{B_0})\otimes(K,\mathrm{id})$. Then $Q=C_A(B_0)\subseteq A$ is a quaternion algebra containing u which is invariant under σ. □

Lemma 6.4. *Let (A, σ) be a totally decomposable algebra with involution of orthogonal type over a field F of characteristic 2. Let $\{u_1, \cdots, u_n\}$ be a set of alternating generators of $\Phi(A, \sigma)$ and set $\alpha_i = u_i^2 \in F^\times$, $i = 1, \cdots, n$. Suppose that $\alpha_n \notin F^2$ and set $B = C_A(u_n)$ and $K = F[u_n]$. Then $(B, \sigma|_B)$ is a totally decomposable algebra with involution of orthogonal type over K and $\{u_1, \cdots, u_{n-1}\}$ is a set of alternating generators of $\Phi(B, \sigma|_B)$. In particular $\mathfrak{Pf}(B, \sigma|_B) \simeq \langle\langle \alpha_1, \cdots, \alpha_{n-1} \rangle\rangle_K$.*

Proof. By (6.3 (i)), $(B, \sigma|_B)$ is a totally decomposable algebra with involution of orthogonal type over K and we have an isomorphism of K-algebras $\Phi(B, \sigma|_B) \simeq \Phi(A, \sigma)$. Let $1 \leq l \leq n-1$ and $1 \leq i_1 < \cdots < i_l \leq n-1$. We claim that $u_{i_1} \cdots u_{i_l} \in \mathrm{Alt}(B, \sigma|_B)$. By (4.5 (iii)) we have $\Phi(B, \sigma|_B) \subseteq \mathrm{Alt}(B, \sigma|_B) + K$, so there exists $\lambda \in K$ such that $w := u_{i_1} \cdots u_{i_l} + \lambda \in \mathrm{Alt}(B, \sigma|_B)$. Write $\lambda = \alpha + \beta u_n$ for some $\alpha, \beta \in F$. Then

$$w = u_{i_1} \cdots u_{i_l} + \alpha + \beta u_n \in \mathrm{Alt}(B, \sigma|_B) \subseteq \mathrm{Alt}(A, \sigma).$$

As σ is of orthogonal type, we have $\alpha = 0$. As $u_n \in K = Z(B)$ we have $u_n w \in \mathrm{Alt}(B, \sigma|_B)$. On the other hand $u_n w = u_n u_{i_1} \cdots u_{i_l} + \alpha_n \beta \in \mathrm{Alt}(B, \sigma|_B) \subseteq \mathrm{Alt}(A, \sigma)$. Again, as σ is of orthogonal type, we have $\beta = 0$. So $u_{i_1} \cdots u_{i_l} \in \mathrm{Alt}(B, \sigma|_B)$ and the claim is proved, i.e., $\{u_1, \cdots, u_{n-1}\}$ is a set of alternating generators of $\Phi(B, \sigma|_B)$. □

In [7] it was shown that if $(A, \sigma) \simeq (A', \sigma')$ then $A \simeq A'$ and $\mathfrak{Pf}(A, \sigma) \simeq \mathfrak{Pf}(A', \sigma')$. It was also asked whether the converse is also true (see [7, (7.4)]). The following result shows that this question has an affirmative answer, i.e., totally decomposable algebras with involution of orthogonal type can be classified, up to conjugation, by their Pfister invariant.

Theorem 6.5. *Let (A, σ) and (A', σ') be two totally decomposable algebras with involution of orthogonal type over a field F of characteristic 2. If $A \simeq A'$ and $\mathfrak{Pf}(A, \sigma) \simeq \mathfrak{Pf}(A', \sigma')$, then $(A, \sigma) \simeq (A', \sigma')$.*

Proof. Let $\{u_1, \cdots, u_n\}$ be a set of alternating generators of $\Phi(A, \sigma)$ with $u_i^2 = \alpha_i \in F^\times$, so that $\mathfrak{Pf}(A, \sigma) \simeq \langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$. By (5.5) and (5.6) there exists a set of alternating generators $\{u'_1, \cdots, u'_n\}$ of $\Phi(A', \sigma')$ such that ${u'_i}^2 = \alpha_i$, $i = 1, \cdots, n$.

We use induction on n. If $n = 1$, we have $\operatorname{disc} \sigma = \operatorname{disc} \sigma' = \mathrm{Nrd}_A(u_1) F^{\times 2} = \alpha_1 F^{\times 2}$, so the result follows from [15, (7.4)]. So suppose that $n > 1$. If $\alpha_i \in F^{\times 2}$ for every $i = 1, \cdots, n$, then using (5.7) we obtain $(A, \sigma) \simeq (A', \sigma') \simeq (M_{2^n}(F), t)$ and we are done. So (by re-indexing if necessary) we may assume that $\alpha_n \in F^\times \setminus F^{\times 2}$. Set $B = C_A(u_n)$, $K = F[u_n]$, $B' = C_{A'}(u'_n)$ and $K' = F[u'_n]$. As $K \simeq K' = F(\sqrt{\alpha_n})$, we may consider B' as a central simple algebra over K. By (6.3 (i)) and (6.4), $(B, \sigma|_B)$ and $(B', \sigma'|_{B'})$ are totally decomposable algebras with involution of orthogonal type over K and $\mathfrak{Pf}(B, \sigma|_B) \simeq \mathfrak{Pf}(B', \sigma'|_{B'}) \simeq \langle\langle \alpha_1, \cdots, \alpha_{n-1} \rangle\rangle_K$. Since $A \simeq_F A'$, we obtain $B \simeq_K B'$, so by induction hypothesis there exists an isomorphism of K-algebras with involution

$$f : (B, \sigma|_B) \simeq_K (B', \sigma'|_{B'}).$$

By (6.3 (i)) we have a K-algebra isomorphism $\Phi(B, \sigma|_B) \simeq \Phi(A, \sigma)$. So we get $u^2 \in F$ for every $u \in \Phi(B, \sigma|_B)$. By (6.2) there exists a central simple F-subalgebra $B_0 \subseteq B$ such that $(B, \sigma|_B) \simeq_K (B_0, \sigma|_{B_0}) \otimes (K, \mathrm{id})$. Set $B'_0 = f(B_0) \subseteq B'$, hence $(B_0, \sigma|_{B_0}) \simeq_F (B'_0, \sigma'|_{B'_0})$. Then B'_0 is a σ'-invariant central simple subalgebra of B' and $(B', \sigma'|_{B'}) \simeq_K (B'_0, \sigma'|_{B'_0}) \otimes (K, \mathrm{id})$. Set $Q := C_A(B_0) \supseteq C_A(B) = C_A(C_A(u_n))$, hence $u_n \in Q$. Similarly set $Q' := C_{A'}(B'_0) = C_{A'}(f(B_0)) \supseteq C_{A'}(f(B)) = C_{A'}(B') = C_{A'}(C_{A'}(u'_n))$, hence $u'_n \in Q'$. As $\deg_F Q = \deg_F Q' = 2$, Q and Q' are quaternion algebras over F. We also have $(A, \sigma) \simeq_F (Q, \sigma|_Q) \otimes$

$(B_0, \sigma|_{B_0})$ and $(A', \sigma') \simeq_F (Q', \sigma'|_{Q'}) \otimes (B'_0, \sigma'|_{B'_0})$. Since $B_0 \simeq_F B'_0$ and $A \simeq_F A'$, we obtain

$$Q' \simeq_F C_{A'}(B'_0) \simeq_F C_A(B_0) \simeq_F Q.$$

Also as $u_n \in \mathrm{Alt}(A, \sigma) \cap Q$, by [18, (3.5)] we have $u_n \in \mathrm{Alt}(Q, \sigma|_Q)$. It follows that $\operatorname{disc} \sigma|_Q = \mathrm{Nrd}_Q(u_n) F^{\times 2} = \alpha_n F^{\times 2}$ and similarly $\operatorname{disc} \sigma'|_{Q'} = \alpha_n F^{\times 2}$, hence $(Q, \sigma|_Q) \simeq_F (Q', \sigma'|_{Q'})$ by [15, (7.4)]. Using this isomorphism we obtain

$$(A, \sigma) \simeq_F (Q, \sigma|_Q) \otimes (B_0, \sigma|_{B_0}) \simeq_F (Q', \sigma'|_{Q'}) \otimes (B'_0, \sigma'|_{B'_0}) \simeq (A', \sigma'). \qquad \square$$

A bilinear space $(V, \mathfrak{b})$ over a field F is called *metabolic* if there exists a subspace W of V such that $\dim W = \frac{1}{2} \dim V$ and $\mathfrak{b}|_{W \times W} = 0$. An F-algebra with involution (A, σ) is called *metabolic* if there exists an idempotent $e \in A$ such that $\sigma(e)e = 0$ and $\dim_F eA = \frac{1}{2} \dim_F A$. A bilinear form is metabolic if and only if its adjoint involution is metabolic, see [6, (4.8)].

As an application we complement a characterization of totally decomposable algebras with metabolic involution given in [7].

Theorem 6.6. ([7, (7.5)]) *Let (A, σ) be a totally decomposable algebra of degree 2^n with involution of orthogonal type over a field F of characteristic 2. Then the following statements are equivalent:*

- (i) *(A, σ) is metabolic.*
- (ii) *$\mathfrak{Pf}(A, \sigma)$ is metabolic.*
- (iii) *$\Phi(A, \sigma)$ is not a field.*
- (iv) *There exists a central simple algebra with involution of orthogonal type (B, τ) over F such that $(A, \sigma) \simeq (M_2(F), t) \otimes (B, \tau)$.*

Proof. The equivalence of (i) and (ii) was shown in [7, (7.5)].

$(ii) \Rightarrow (iii)$: If $\mathfrak{Pf}(A, \sigma)$ is metabolic, then as $\mathfrak{Pf}(A, \sigma) \simeq \mathfrak{s}$, by the relation (16) given in (5.2) there exists a nonzero $x \in \Phi(A, \sigma)$ such that $x^2 = 0$ and we obtain (iii).

$(iii) \Rightarrow (iv)$: We use induction on n. If $n = 1$, the result follows from (5.7) and (5.12). So suppose that $n > 1$. Let $\mathfrak{m}$ be the unique maximal ideal of $\Phi(A, \sigma)$ and let $K \supseteq F$ be a maximal subfield of $\Phi(A, \sigma)$. If $K = F$ the result again follows from (5.7); so suppose that $K \neq F$. Write $K = F[u_1, \cdots, u_r]$, where $r = r_F(K)$ and $u_1, \cdots, u_r \in K$. Since $\Phi(A, \sigma)$ is not a field we have $\mathfrak{m} \neq \{0\}$. So using (3.9) one can find $u_{r+1}, \cdots, u_n \in \mathfrak{m}$ such that $\Phi(A, \sigma) = K[u_{r+1}, \cdots, u_n]$. It follows that $\Phi(A, \sigma) = F[u_1, \cdots, u_n]$ with $u_1 \in K \setminus F$ and $u_n \in \mathfrak{m}$. By (4.2 (ii)) there exists a σ-invariant quaternion subalgebra Q of A such that $F[u_2, \cdots, u_n] \subseteq C_A(Q)$. Set $B = C_A(Q)$. We have $\dim_F F[u_2, \cdots, u_n] = \deg_F B = 2^{n-1}$, so by (3.11), $F[u_2, \cdots, u_n]$ is a ρ-generated F-algebra. Also it is easy to see that $C_B(F[u_2, \cdots, u_n]) = F[u_2, \cdots, u_n]$. As $F[u_2, \cdots, u_n] \subseteq \mathrm{Sym}(B, \sigma|_B)$, by (4.5), $(B, \sigma|_B)$ is a totally decomposable algebra with involution of orthogonal type over F. By (5.10 (ii)) we have $\Phi(B, \sigma|_B) \simeq F[u_2, \cdots, u_n]$. As $u_n \in F[u_2, \cdots, u_n] \cap \mathfrak{m}$, $\Phi(B, \sigma|_B)$ is not a field. So the result follows from induction hypothesis.

$(iv) \Rightarrow (i)$: Let

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(F).$$

Then e is a metabolic idempotent for $(M_2(F), t)$. So $(M_2(F), t)$ is metabolic which implies that $(A, \sigma) \simeq (M_2(F), t) \otimes (B, \tau)$ is also metabolic. $\square$

References

[1] S. A. Amitsur, L. H. Rowen, J.-P. Tignol, Division algebras of degree 4 and 8 with involution. *Israel J. Math.* **33** (1979), no. 2, 133–148.

[2] J. Arason, R. Baeza, Relations in I^n and I^nW_q in characteristic 2. *J. Algebra* **314** (2007), no. 2, 895–911.

[3] D. Barry, Decomposable and indecomposable algebras of degree 8 and exponent 2 (with an appendix by A. S. Merkurjev). *Math. Z.* **276** (2014), no. 3-4, 1113–1132.

[4] D. Barry, A. Chapman, Square-Central and Artin-Schreier Elements in Division Algebras. arXiv:1501.03831 [math.RA].

[5] H. Dherte, Quadratic descent of involutions in degree 2 and 4. *Proc. Am. Math. Soc.* **123** (1995), no.7, 1963–1969 .

[6] A. Dolphin, Metabolic involutions. *J. Algebra* **336** (2011), 286–300.

[7] A. Dolphin, Orthogonal Pfister involutions in characteristic two. *J. Pure Appl. Algebra* **218** (2014), no. 10, 1900–1915.

[8] R. Elman, N. Karpenko, A. Merkurjev, *The algebraic and geometric theory of quadratic forms.* American Mathematical Society Colloquium Publications, 56. American Mathematical Society, Providence, RI, 2008.

[9] S. Garibaldi, R. Parimala, J.-P. Tignol, Discriminant of symplectic involutions. *Pure Appl. Math. Q.* **5** (2009), no. 1, 349–374.

[10] S. Garibaldi, H. P. Petersson, Wild Pfister forms over Henselian fields, K-theory, and conic division algebras. *J. Algebra* **327** (2011), 386–465.

[11] N. Jacobson, *Finite-dimensional division algebras over fields.* Springer-Verlag, Berlin, 1996.

[12] B. Kahn, Quelques remarques sur le u-invariant. *Sémin. Théor. Nombres Bordx. Sér. II* **2** (1990), no. 1, 155–161; Erratum **3** (1991), no. 1, 247.

[13] N. Karpenko, A. Quéguiner, A criterion of decomposability for degree 4 algebras with unitary involution. *J. Pure Appl. Algebra* **147** (2000), no. 3, 303–309.

[14] M.-A. Knus, T.Y. Lam, D.B. Shapiro, J.-P. Tignol, Discriminants of involutions on biquaternion algebras. Jacob, Bill (ed.) et al., K-theory and algebraic geometry: connections with quadratic forms and division algebras. Providence, RI: American Mathematical Society. *Proc. Symp. Pure Math.* **58**, Part 2, (1995), 279–303.

[15] M.-A. Knus, A. S. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions.* American Mathematical Society Colloquium Publications, 44. American Mathematical Society, Providence, RI, 1998.

[16] M.-A. Knus, R. Parimala, R. Sridharan, Involutions on rank 16 central simple algebras. *J. Indian Math. Soc. (N.S.)* **57** (1991), no. 1–4, 143–151.

[17] D.W. Lewis, J.-P. Tignol, Classification theorems for central simple algebras with involution (with an appendix by R. Parimala). *Manuscr. Math.* **100** (1999), no. 3, 259–276.

[18] M. G. Mahmoudi, A.-H. Nokhodkar, On split products of quaternion algebras with involution in characteristic two. *J. Pure Appl. Algebra* **218** (2014), no. 4, 731–734.

[19] R. Parimala, Correction to the proof of Proposition 3.7 of the paper Involutions on rank 16 central simple algebras [16], January 2014.

[20] R. S. Pierce, *Associative algebras.* Graduate Texts in Mathematics, 88. Springer-Verlag, New York-Heidelberg-Berlin, 1982.

[21] A. Quéguiner-Mathieu, J.-P. Tignol, Algebras with involution that become hyperbolic over the function field of a conic. *Israel. J. Math.* **180** (2010), 317–344.

[22] L. H. Rowen, Central simple algebras. *Israel J. Math.* **29** (1978), 285–301.

[23] L. H. Rowen, Division algebras of exponent 2 and characteristic 2. *J. Algebra* **90** (1984), 71–83.

[24] W. Streb, Zentrale einfache PI-Algebren der Charakteristik 2 vom Exponenten 2. *J. Algebra* **83** (1983), 20–25.

[25] J.-P. Tignol, Cohomological invariants of central simple algebras with involution. Colliot-Thélène, Jean-Louis (ed.) et al., Quadratic forms, linear algebraic groups, and cohomology. New York, NY: Springer, Developments in Mathematics **18** (2010), 137-171.

M. G. Mahmoudi, mmahmoudi@sharif.ir, A.-H. Nokhodkar, anokhodkar@yahoo.com
Department of Mathematical Sciences, Sharif University of Technology, P. O. Box 11155-9415, Tehran, Iran.