ESSENTIAL DIMENSION, SPINOR GROUPS, AND QUADRATIC FORMS

PATRICK BROSNAN[†], ZINOVY REICHSTEIN[†], AND ANGELO VISTOLI[‡]

ABSTRACT. We prove that the essential dimension of the spinor group $\mathbf{Spin}_n$ grows exponentially with n and use this result to show that quadratic forms with trivial discriminant and Hasse-Witt invariant are more complex, in high dimensions, than previously expected.

1. INTRODUCTION

Let K be a field of characteristic different from 2 containing a square root of -1, $\mathrm{W}(K)$ be the Witt ring of K and $I(K)$ be the ideal of classes of even-dimensional forms in $\mathrm{W}(K)$; cf. [Lam73]. By abuse of notation, we will write $q \in I^a(K)$ if the Witt class on the non-degenerate quadratic form q defined over K lies in $I^a(K)$. It is well known that every $q \in I^a(K)$ can be expressed as a sum of the Witt classes of a-fold Pfister forms defined over K; see, e.g., [Lam73, Proposition II.1.2]. If $\dim(q) = n$, it is natural to ask how many Pfister forms are needed. When $a = 1$ or 2, it is easy to see that n Pfister forms always suffice; see Proposition 4.1. In this paper we will prove the following result, which shows that the situation is quite different when $a = 3$.

Theorem 1.1. *Let k be a field of characteristic different from 2 and $n \geq 2$ be an even integer. Then there is a field extension K/k and an n-dimensional quadratic form $q \in I^3(K)$ with the following property: for any finite field extension L/K of odd degree q_L is not Witt equivalent to the sum of fewer than*

$$\frac{2^{(n+4)/4} - n - 2}{7}$$

3-fold Pfister forms over L.

Our proof of Theorem 1.1 is based on new results on the essential dimension of the spinor groups $\mathbf{Spin}_n$ proven in §3 which are of independent

2000 *Mathematics Subject Classification.* Primary 11E04, 11E72, 15A66.

Key words and phrases. Essential dimension, spinor group, quadratic form, Witt group, Pfister form.

[†]Supported in part by an NSERC discovery grants and by PIMS Collaborative Research Group in Algebraic geometry, cohomology and representation theory.

[‡]Supported in part by the PRIN Project "Geometria sulle varietà algebriche", financed by MIUR.

interest. In particular, Theorem 3.3 gives new lower bounds on the essential dimension of $\mathbf{Spin}_n$ and, in many cases, computes the exact value.

Acknowledgements. We would like to thank the Banff International Research Station in Banff, Alberta (BIRS) for providing the inspiring meeting place where this work was started. We are grateful to A. Merkurjev and B. Totaro for bringing the problem of computing the Pfister numbers $\mathrm{Pf}_k(a, n)$ to our attention and for contributing Proposition 4.2. We also thank N. Fakhruddin for helpful correspondence.

2. Essential dimension

Let k be a field. We will write Fields_k for the category of field extensions K/k. Let $F\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor.

Let L/k be a field extension. We will say that $a \in F(L)$ *descends* to an intermediate field $k \subseteq K \subseteq L$ if a is in the image of the induced map $F(K) \to F(L)$.

The *essential dimension* $\mathrm{ed}(a)$ of $a \in F(L)$ is the minimum of the transcendence degrees $\mathrm{tr\,deg}_k K$ taken over all fields $k \subseteq K \subseteq L$ such that a descends to K.

The essential dimension $\mathrm{ed}(a;p)$ of a at a prime integer p is the minimum of $\mathrm{ed}(a_{L'})$ taken over all finite field extensions L'/L such that the degree $[L' : L]$ is prime to p.

The essential dimension $\mathrm{ed}\, F$ of the functor F (respectively, the essential dimension $\mathrm{ed}(F;p)$ of F at a prime p) is the supremum of $\mathrm{ed}(a)$ (respectively, of $\mathrm{ed}(a;p)$) taken over all $a \in F(L)$ with L in Fields_k.

Of particular interest to us will be the Galois cohomology functors, F_G given by $K \rightsquigarrow \mathrm{H}^1(K, G)$, where G is an algebraic group over k. Here, as usual, $\mathrm{H}^1(K, G)$ denotes the set of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$, in the fppf topology. The essential dimension of this functor is a numerical invariant of G, which, roughly speaking, measures the complexity of G-torsors over fields. We write $\mathrm{ed}\, G$ for $\mathrm{ed}\ F_G$ and $\mathrm{ed}(G;p)$ for $\mathrm{ed}(F_G;p)$. Essential dimension was originally introduced in this context; see [BR97, Rei00, RY00]. The above definition of essential dimension for a general functor F is due to A. Merkurjev; see [BF03].

Recall that an action of an algebraic group G on an algebraic variety k-variety X is called "generically free" if X has a dense open subset U such that $\mathrm{Stab}_G(x) = \{1\}$ for every $x \in U(\overline{k})$.

Lemma 2.1. *If an algebraic group G defined over k has a generically free linear k-representation V then* $\mathrm{ed}(G) \leq \dim(V) - \dim(G)$.

Proof. See [Rei00, Theorem 3.4] or [BF03, Lemma 4.11]. ♠

Lemma 2.2. *If G is an algebraic group and H is a closed subgroup of codimension e then*

(a) $\mathrm{ed}(G) \geq \mathrm{ed}(H) - e$*, and*

(b) $\mathrm{ed}(G;p) \geq \mathrm{ed}(H;p) - e$ *for any prime integer p.*

Proof. Part (a) is [BF03, Theorem 6.19]. Both (a) and (b) follow directly from [Bro07, Principle 2.10]. ♠

If G is a finite abstract group, we will write $\mathrm{ed}_k\, G$ (respectively, $\mathrm{ed}_k(G;p)$) for the essential dimension (respectively, for the essential dimension at p) of the constant group scheme G_k over the field k. Let $\mathrm{C}(G)$ denote the center of G.

Theorem 2.3. *Let G be a finite p-group whose commutator $[G,G]$ is central and cyclic. Then $\mathrm{ed}_k(G;p) = \mathrm{ed}_k\, G = \sqrt{|G/\mathrm{C}(G)|} + \mathrm{rank}\ \mathrm{C}(G) - 1$ for any base field k of characteristic $\neq p$ containing a primitive root of unity of degree equal to the exponent of G.*

Note that with the above hypotheses, $|G/\mathrm{C}(G)|$ is a complete square. Theorem 2.3 was originally proved in [BRV07] as a consequence of our study of essential dimension of gerbes banded by $\boldsymbol{\mu}_{p^n}$. Karpenko and Merkurjev [KM07] have subsequently refined our arguments to show that the essential dimension of any finite p-group over any field k containing a primitive p^{th} root of unity is the minimal dimension of a faithful linear k-representation of G. Using [KM07, Remark 4.7] Theorem 2.3 is easily seen to be a special case of their formula. For this reason we omit the proof here.

3. Essential dimension of Spin groups

As usual, we will write $\langle a_1, \dots, a_n \rangle$ for the quadratic form q of rank n given by $q(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i^2$. Let

$$h = \langle 1, -1 \rangle \tag{3.1}$$

denote the 2-dimensional hyperbolic quadratic form over k. For each $n \geq 0$ we define the n-dimensional split form q_n^{split} defined over k as follows:

$$q_n^{\text{split}} = \begin{cases} h^{\oplus n/2}, & \text{if } n \text{ is even,} \\ h^{\oplus (n-1/2)} \oplus \langle 1 \rangle, & \text{if } n \text{ is odd.} \end{cases}$$

Let $\mathbf{Spin}_n \overset{\text{def}}{=} \mathbf{Spin}(q_n^{\text{split}})$ be the split form of the spin group. We will also denote the split forms of the orthogonal and special orthogonal groups by $\mathbf{O}_n \overset{\text{def}}{=} \mathbf{O}(q_n^{\text{split}})$ and $\mathbf{SO}_n \overset{\text{def}}{=} \mathbf{SO}(q_n^{\text{split}})$ respectively.

M. Rost [Ros99] computed the following values of $\mathrm{ed}(\mathbf{Spin}_n)$ for $n \leq 14$:

$$\begin{array}{llll} \mathrm{ed}\,\mathbf{Spin}_3 = 0 & \mathrm{ed}\,\mathbf{Spin}_4 = 0 & \mathrm{ed}\,\mathbf{Spin}_5 = 0 & \mathrm{ed}\,\mathbf{Spin}_6 = 0 \\ \mathrm{ed}\,\mathbf{Spin}_7 = 4 & \mathrm{ed}\,\mathbf{Spin}_8 = 5 & \mathrm{ed}\,\mathbf{Spin}_9 = 5 & \mathrm{ed}\,\mathbf{Spin}_{10} = 4 \\ \mathrm{ed}\,\mathbf{Spin}_{11} = 5 & \mathrm{ed}\,\mathbf{Spin}_{12} = 6 & \mathrm{ed}\,\mathbf{Spin}_{13} = 6 & \mathrm{ed}\,\mathbf{Spin}_{14} = 7, \end{array}$$

for a detailed exposition of these results; see [Gar08]. V. Chernousov and J.–P. Serre [CS06] recently proved the following lower bounds:

$$\mathrm{ed}(\mathbf{Spin}_n; 2) \geq \begin{cases} \lfloor n/2 \rfloor + 1 & \text{if } n \geq 7 \text{ and } n \equiv 1, 0 \text{ or } -1 \pmod 8 \\ \lfloor n/2 \rfloor & \text{for all other } n \geq 11. \end{cases} \tag{3.2}$$

(The first line is due to B. Youssin and the second author in the case that $\operatorname{char} k = 0$ [RY00].)

The main result of this section, Theorem 3.3 below, shows, in particular, that $\operatorname{ed}(\mathbf{Spin}_n)$ and $\operatorname{ed}(\mathbf{Spin}_n; 2)$ grow exponentially with n.

Theorem 3.3. *(a) Let k be a field of characteristic $\neq 2$ and $n \geq 15$ be an integer.*

$$\operatorname{ed}(\mathbf{Spin}_n; 2) \geq \begin{cases} 2^{(n-1)/2} - \frac{n(n-1)}{2}, \text{ if } n \text{ is odd,} \\ 2^{(n-2)/2} - \frac{n(n-1)}{2}, \text{ if } n \equiv 2 \pmod 4, \\ 2^{(n-2)/2} - \frac{n(n-1)}{2} + 1, \text{ if } n \equiv 0 \pmod 4. \end{cases}$$

(b) Moreover, if $\operatorname{char}(k) = 0$ then

$$\operatorname{ed}(\mathbf{Spin}_n) = \operatorname{ed}(\mathbf{Spin}_n; 2) = 2^{(n-1)/2} - \tfrac{n(n-1)}{2}, \text{ if } n \text{ is odd,}$$
$$\operatorname{ed}(\mathbf{Spin}_n) = \operatorname{ed}(\mathbf{Spin}_n; 2) = 2^{(n-2)/2} - \tfrac{n(n-1)}{2}, \text{ if } n \equiv 2 \pmod 4, \text{ and}$$
$$\operatorname{ed}(\mathbf{Spin}_n; 2) \leq \operatorname{ed}(\mathbf{Spin}_n) \leq 2^{(n-2)/2} - \tfrac{n(n-1)}{2} + n, \text{ if } n \equiv 0 \pmod 4.$$

Note that while the proof of part (a) below goes through for any $n \geq 3$, our lower bounds become negative (and thus vacuous) for $n \leq 14$.

Proof. (a) Since replacing k by a larger field k' can only decrease the value of $\operatorname{ed}(\mathbf{Spin}_n; 2)$, we may assume without loss of generality that $\sqrt{-1} \in k$. The n-dimensional split quadratic form q_n^{split} is then k-isomorphic to

$$q(x_1, \dots, x_n) = -(x_1^2 + \dots + x_n^2). \tag{3.4}$$

over k and hence, we can write $\mathbf{Spin}_n$ as $\mathbf{Spin}(q)$, $\mathbf{O}_n$ as $\mathbf{O}_n(q)$ and $\mathbf{SO}_n$ as $\mathbf{SO}_n(q)$.

Let $\Gamma_n \subseteq \mathbf{SO}_n$ be the subgroup consisting of diagonal matrices. This subgroup is isomorphic to $\boldsymbol{\mu}_2^{n-1}$. Let G_n be the inverse image of Γ_n in $\mathbf{Spin}_n$; this is a constant group scheme over k. By Lemma 2.2(b)

$$\operatorname{ed}(\mathbf{Spin}_n; 2) \geq \operatorname{ed}(G_n; 2) - \frac{n(n-1)}{2}.$$

Thus in order to prove the lower bounds of part (a), it suffices to show that

$$\operatorname{ed}(G_n; 2) = \operatorname{ed}(G_n) = \begin{cases} 2^{(n-1)/2}, \text{ if } n \text{ is odd,} \\ 2^{(n-2)/2}, \text{ if } n \equiv 2 \pmod 4, \\ 2^{(n-2)/2} + 1, \text{ if } n \text{ is divisible by } 4. \end{cases} \tag{3.5}$$

The structure of the finite 2-group G_n is well understood; see, e.g., [Woo89]. Recall that the Clifford algebra A_n of the quadratic form q, as in (3.4) is the algebra given by generators $e_1, \dots, e_n$, and relations $e_i^2 = -1$, $e_i e_j + e_j e_i = 0$ for all $i \neq j$. For any $I = \{i_1, \dots, i_r\} \subseteq \{1, \dots, n\}$ with $i_1 < i_2 < \dots < i_r$ set $e_I \stackrel{\text{def}}{=} e_{i_1} \dots e_{i_r}$. Here $e_\emptyset = 1$. The group G_n consists of the elements of A_n of the form $\pm e_I$, where the cardinality $r = |I|$ of I is even. The element -1 is central, and the commutator $[e_I, e_J]$ is given by $[e_I, e_J] = (-1)^{|I \cap J|}$. It is clear from this description that G_n is a 2-group of order 2^n, the commutator subgroup $[G_n, G_n] = \{\pm 1\}$ is cyclic, and the center $\mathrm{C}(G)$ is as follows:

$$\mathrm{C}(G_n) = \begin{cases} \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}, \text{ if } n \text{ is odd,} \\ \{\pm 1, \pm e_{\{1,\dots,n\}}\} \simeq \mathbb{Z}/4\mathbb{Z}, \text{ if } n \equiv 2 \pmod 4, \\ \{\pm 1, \pm e_{\{1,\dots,n\}}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \text{ if } n \text{ is divisible by 4.} \end{cases}$$

Formula (3.5) now follows from Theorem 2.3.

(b) Clearly $\mathrm{ed}(\mathbf{Spin}_n; 2) \le \mathrm{ed}(\mathbf{Spin}_n)$. Hence, we only need to show that for $n \ge 15$

$$\mathrm{ed}(\mathbf{Spin}_n) \le \begin{cases} 2^{(n-1)/2} - \frac{n(n-1)}{2}, \text{ if } n \text{ is odd,} \\ 2^{(n-2)/2} - \frac{n(n-1)}{2}, \text{ if } n \equiv 2 \pmod 4, \\ 2^{(n-2)/2} - \frac{n(n-1)}{2} + n, \text{ if } n \equiv 0 \pmod 4. \end{cases} \tag{3.6}$$

In view of Lemma 2.1 it suffices to show that $\mathbf{Spin}_n$ has a generically free linear representation V of dimension

$$\dim(V) = \begin{cases} 2^{(n-1)/2}, \text{ if } n \text{ is odd,} \\ 2^{(n-2)/2}, \text{ if } n \equiv 2 \pmod 4, \\ 2^{(n-2)/2} + n \text{ if } n \equiv 0 \pmod 4. \end{cases}$$

In the case where n is not divisible by 4 such a representation is given by the following lemma.

Lemma 3.7. (*cf.* [PV94, Theorem 7.11]) *If $n \ge 15$ then, over a field of characteristic 0, the following representations of $\mathbf{Spin}_n$ of characteristic 0 are generically free:*

(i) the spin representation, of dimension $2^{(n-1)/2}$, if n is odd,

(ii) either of the two half-spin representation, of dimension $2^{(n-2)/2}$, if $n \equiv 2 \pmod 4$.

Proof. For $n \ge 27$ this follows directly from [AP71, Theorem 1]. For n between 15 and 25 this is proved in [Po85]. ♠

In the case where $n \ge 16$ is divisible by 4, we define V as the sum of the half-spin representation W of $\mathbf{Spin}_n$ and the natural representation k^n of $\mathbf{SO}_n$, which we will view as a $\mathbf{Spin}_n$-representation via the projection $\mathbf{Spin}_n \to \mathbf{SO}_n$. It remains to check that $V = W \times k^n$ is a generically free representation of $\mathbf{Spin}_n$. Indeed, for $a \in k^n$ in general position, $\mathrm{Stab}(a)$ is conjugate to $\mathbf{Spin}_{n-1}$ (embedded in $\mathbf{Spin}_n$ in the standard way). Thus it suffices to show that the restriction of W to $\mathbf{Spin}_{n-1}$ is generically free. Since W restricted to $\mathbf{Spin}_{n-1}$ is the spin representation of $\mathbf{Spin}_{n-1}$ (see, e.g., [Ada96, Proposition 4.4]), and $n \ge 16$, this follows from Lemma 3.7(i). This completes the proof of Theorem 3.3. ♠

Remark 3.8. The characteristic 0 assumption in part (b) is used only in the proof of Lemma 3.7. It seems likely that Lemma 3.7 (and thus Theorem 3.3(b)) remain true if $\mathrm{char}(k) = p > 2$ but we have not checked this.

If $\mathrm{char}(k) \neq 2$ and $\sqrt{-1} \in k$, we have the weaker (but asymptotically equivalent) upper bound $\mathrm{ed}(\mathbf{Spin}_n) \leq \mathrm{ed}(G_n)$, where $\mathrm{ed}(G_n)$ is given by (3.5). This is a consequence of the fact that every $\mathbf{Spin}_n$-torsor admits reduction of structure to G_n, i.e., the natural map $\mathrm{H}^1(K, G_n) \to \mathrm{H}^1(K, \mathbf{Spin}_n)$ is surjective for every field K/k; cf. [BF03, Lemma 1.9].

Remark 3.9. A. S. Merkurjev (unpublished) recently strengthened our lower bound on $\mathrm{ed}(\mathbf{Spin}_n; 2)$, in the case where $n \equiv 0 \pmod 4$ as follows:

$$\mathrm{ed}(\mathbf{Spin}_n; 2) \geq 2^{(n-2)/2} - \frac{n(n-1)}{2} + 2^m\,,$$

where 2^m is the highest power of 2 dividing n. If $n \geq 16$ is a power of 2 and $\mathrm{char}(k) = 0$ this, in combination with the upper bound of Theorem 3.3(b), yields

$$\mathrm{ed}(\mathbf{Spin}_n; 2) = \mathrm{ed}(\mathbf{Spin}_n) = 2^{(n-2)/2} - \frac{n(n-1)}{2} + n\,.$$

In particular, $\mathrm{ed}(\mathbf{Spin}_{16}) = 24$. The first value of n for which $\mathrm{ed}(\mathbf{Spin}_n)$ is not known is $n = 20$, where $326 \leq \mathrm{ed}(\mathbf{Spin}_{20}) \leq 342$.

Remark 3.10. The same argument can be applied to the half-spin groups yielding

$$\mathrm{ed}(\mathbf{HSpin}_n; 2) = \mathrm{ed}(\mathbf{HSpin}_n) = 2^{(n-2)/2} - \frac{n(n-1)}{2}$$

for any integer $n \geq 20$ divisible by 4 over any field of characteristic 0. Here, as in Theorem 3.3, the lower bound

$$\mathrm{ed}(\mathbf{HSpin}_n; 2) \geq 2^{(n-2)/2} - \frac{n(n-1)}{2}$$

is valid for over any base field k of characteristic $\neq 2$. The assumptions that $\mathrm{char}(k) = 0$ and $n \geq 20$ ensure that the half-spin representation of $\mathbf{HSpin}_n$ is generically free; see [PV94, Theorem 7.11].

Remark 3.11. Theorem 3.3 implies that for large n, $\mathbf{Spin}_n$ is an example of a split, semisimple, connected linear algebraic group whose essential dimension exceeds its dimension. Previously no examples of this kind were known, even for $k = \mathbb{C}$.

Note that no complex connected semisimple adjoint group G can have this property. Indeed, let $\mathfrak{g}$ be the adjoint representation of G on its Lie algebra. If G is an adjoint group then $V = \mathfrak{g} \times \mathfrak{g}$ is generically free; see, e.g., [Rich88, Lemma 3.3(b)]. Thus $\mathrm{ed}\, G \leq \dim(G)$ by Lemma 2.1.

Remark 3.12. Since $\mathrm{ed}\,\mathbf{SO}_n = n - 1$ for every $n \geq 3$ (cf. [Rei00, Theorem 10.4]), it follows that, for large n, $\mathbf{Spin}_n$ is also an example of a split, semisimple, connected linear algebraic group G with a central subgroup Z such that $\mathrm{ed}\, G > \mathrm{ed}\, G/Z$. To the best of our knowledge, this example is new as well.

4. Pfister numbers

Let K be a field of characteristic not equal to 2 and $a \geq 1$ be an integer. We will continue to denote the Witt ring of K by $W(K)$ and its fundamental ideal by $I(K)$. If non-singular quadratic forms q and q' over K are Witt equivalent, we will write $q \sim q'$.

As we mentioned in the introduction, the a-fold Pfister forms generate $I^a(K)$ as an abelian group. In other words, every $q \in I^a(K)$ is Witt equivalent to $\sum_{i=1}^{r} \pm p_i$, where each p_i is an a-fold Pfister form over K. We now define the *a-Pfister number* of q to be the smallest possible number r of Pfister forms appearing in any such sum. The *(a,n)-Pfister number* $\mathrm{Pf}_k(a,n)$ is the supremum of the a-Pfister number of q, taken over all field extensions K/k and all n-dimensional forms $q \in I^a(K)$.

Proposition 4.1. *Let k be a field of characteristic $\neq 2$ and let n be a positive even integer. Then* (a) $\mathrm{Pf}_k(1,n) \leq n$ *and* (b) $\mathrm{Pf}_k(2,n) \leq n-2$.

Proof. (a) Immediate from the identity

$$\langle a_1, a_2\rangle \sim \langle 1, a_1\rangle - \langle 1, -a_2\rangle = \ll -a_1 \gg - \ll a_2 \gg$$

in the Witt ring.

(b) Let $q = \langle a_1, \dots, a_n\rangle$ be an n-dimensional quadratic form over K. Recall that $q \in I^2(K)$ iff n is even and $d_{\pm}(q) = 1$, modulo $(K^*)^2$ [Lam73, Corollary II.2.2]. Here $d_{\pm}(q)$ is the signed discriminant given by $(-1)^{n(n-1)/2} d(q)$ where $d(q) = \prod_{i=1}^{n} a_n$ is the discriminant of q; cf. [Lam73, p. 38].

To explain how to write q in terms of $n-2$ Pfister forms, we will temporarily assume that $\sqrt{-1} \in K$. In this case, without loss of generality, $a_1 \dots a_n = 1$. Since $\langle a, a\rangle$ is hyperbolic for every $a \in K^*$, we see that $q = \langle a_1, \dots, a_n\rangle$ is Witt equivalent to

$$\ll a_2, a_1 \gg \oplus \ll a_3, a_1 a_2 \gg \oplus \dots \oplus \ll a_{n-1}, a_1 \dots a_{n-2} \gg .$$

By inserting appropriate powers of -1, we can modify this formula so that it remains valid even if we do not assume that $\sqrt{-1} \in K$, as follows:

$$q = \langle a_1, \dots, a_n\rangle \sim \sum_{i=2}^{n} (-1)^i \ll (-1)^{i+1} a_i, (-1)^{i(i-1)/2+1} a_1 \dots a_{i-1} \gg \quad \spadesuit$$

We do not have an explicit upper bound on $\mathrm{Pf}_k(3,n)$; however, we do know that $\mathrm{Pf}_k(3,n)$ is finite for any k and any n. To explain this, let us recall that $I^3(K)$ is the set of all classes $q \in \mathrm{W}(K)$ such that q has even dimension, trivial signed discriminant and trivial Hasse-Witt invariant [KMRT98]. The following result was suggested to us by Merkurjev and Totaro.

Proposition 4.2. *Let k be a field of characteristic different from* 2. *Then* $\mathrm{Pf}_k(3,n)$ *is finite.*

Sketch of proof. Let E be a versal torsor for $\mathbf{Spin}_n$ over a field extension L/k; cf. [GMS03, Section I.V]. Let q_L be the quadratic form over L corresponding to E under the map $\mathrm{H}^1(L, \mathbf{Spin}_n) \to \mathrm{H}^1(L, \mathbf{O}_n)$. The 3-Pfister number of q_L is then an upper bound for the 3-Pfister number of any n-dimensional form in I^3 over any field extension K/k. ♠

Remark 4.3. For $a > 3$ the finiteness of $\mathrm{Pf}_k(a, n)$ is an open problem.

5. Proof of Theorem 1.1

The goal of this section is to prove Theorem 1.1 stated in the introduction, which says, in particular, that

$$\mathrm{Pf}_k(3, n) \geq \frac{2^{(n+4)/4} - n - 2}{7}$$

for any field k of characteristic different from 2 and any positive even integer n. Clearly, replacing k by a larger field k' strengthens the assertion of Theorem 1.1. Thus, we may assume without loss of generality that $\sqrt{-1} \in k$. This assumption will be in force for the remainder of this section.

For each extension K of k, denote by $\mathrm{T}_n(K)$ the image of $\mathrm{H}^1(K, \mathbf{Spin}_n)$ in $\mathrm{H}^1(K, \mathbf{SO}_n)$. We will view T_n as a functor $\mathrm{Fields}_k \to \mathrm{Sets}$. Note that $\mathrm{T}_n(K)$ is the set of isomorphism classes of n-dimensional quadratic forms $q \in I^3(K)$.

Lemma 5.1. *We have the following inequalities:*

(a) $\operatorname{ed} \mathbf{Spin}_n - 1 \leq \operatorname{ed} \mathrm{T}_n \leq \operatorname{ed} \mathbf{Spin}_n$,

(b) $\operatorname{ed}(\mathbf{Spin}_n; 2) - 1 \leq \operatorname{ed}(\mathrm{T}_n; 2) \leq \operatorname{ed}(\mathbf{Spin}_n; 2)$.

Proof. In the language of [BF03, Definition 1.12], we have a fibration of functors

$$\mathrm{H}^1(*, \boldsymbol{\mu}_2) \rightsquigarrow \mathrm{H}^1(*, \mathbf{Spin}_n) \longrightarrow \mathrm{T}_n(*).$$

The first inequality in part (a) follows from [BF03, Proposition 1.13] and the second from Proposition [BF03, Lemma 1.9]. The same argument proves part (b). ♠

Let K/k be a field extension. Let $h_K = \langle 1, -1 \rangle$ be the 2-dimensional hyperbolic form over K. (Note in §3 we wrote h in place of h_k; see (3.1).) For each n-dimensional quadratic form $q \in I^3(K)$, let $\mathrm{ed}_n(q)$ denote the essential dimension of the class of q in $\mathrm{T}_n(K)$.

Lemma 5.2. *Let q be an n-dimensional quadratic form in $I^3(K)$. Then*

$$\mathrm{ed}_{n+2s}(h_K^{\oplus s} \oplus q) \geq \mathrm{ed}_n(q) - \frac{s(s + 2n - 1)}{2}$$

for any integer $s \geq 0$.

Proof. Set $m \stackrel{\text{def}}{=} \mathrm{ed}_{n+2s}(h_K^{\oplus s} \oplus q)$. By definition, $h_K^{\oplus s} \oplus q$ descends to an intermediate subfield $k \subset F \subset K$ such that $\operatorname{tr\,deg}_k(F) = m$. In other words, there is an $(n + 2s)$-dimensional quadratic form $\widetilde{q} \in I^3(F)$ such that $\widetilde{q}_K$ is K-isomorphic to $h_K^{\oplus s} \oplus q$. Let X be the Grassmannian of s-dimensional subspaces of F^{n+2s} which are totally isotropic with respect to $\widetilde{q}$. The dimension of X over F is $s(s + 2n - 1)/2$.

The variety X has a rational point over K; hence there exists an intermediate extension $F \subseteq E \subseteq K$ such that $\operatorname{tr\,deg}_F E \leq s(s+2n-1)/2$, with the property that $\widetilde{q}_E$ has a totally isotropic subspace of dimension s. Then $\widetilde{q}_E$ splits as $h_E^s \oplus q'$, where $q' \in I^3(E)$. By Witt's Cancellation Theorem, q'_K is K-isomorphic to q; hence

$$\operatorname{ed}_n(q) \leq \operatorname{tr\,deg}_k\, E = \operatorname{tr\,deg}_k\, F + \operatorname{tr\,deg}_F\, E = m + s(s+2n-1)/2\,,$$

as claimed. ♠

We now proceed with the proof of Theorem 1.1. For $n \leq 10$ the statement of the theorem is vacuous, because $2^{(n+4)/4} - n - 2 \leq 0$. Thus we will assume from now on that $n \geq 12$.

Lemma 5.1 implies, in particular, that $\operatorname{ed}(\mathrm{T}_n; 2)$ is finite. Hence, there exist a field K/k and an n-dimensional form $q \in I^3(K)$ such that $\operatorname{ed}_n(q) = \operatorname{ed}(\mathrm{T}_n; 2)$. We will show that this form has the properties asserted by Theorem 1.1. In fact, it suffices to prove that if q is Witt equivalent to

$$\sum_{i=1}^{r} \ll a_i, b_i, c_i \gg.$$

over K then $r \geq \dfrac{2^{(n+4)/4} - n - 2}{7}$. Indeed, by our choice of q, $\operatorname{ed}_n(q_L) = \operatorname{ed}(\mathrm{T}_n; 2)$ for any finite odd degree extension L/K. Thus if we can prove the above inequality for q, it will also be valid for q_L.

Let us write a 3-fold Pfister form $\ll a, b, c \gg$ as $\langle 1 \rangle \oplus \ll a, b, c \gg_0$, where

$$\ll a, b, c \gg_0 \overset{\text{def}}{=} \langle a_i, b_i, c_i, a_i b_i, a_i c_i, b_i c_i, a_i b_i c_i \rangle.$$

Set

$$\phi \overset{\text{def}}{=} \begin{cases} \sum_{1=1}^{r} \ll a_i, b_i, c_i \gg_0, \text{ if } r \text{ is even, and} \\ \langle 1 \rangle \oplus \sum_{1=1}^{r} \ll a_i, b_i, c_i \gg_0, \text{ if } r \text{ is odd.} \end{cases}$$

Then q is Witt equivalent to ϕ over K; in particular, $\phi \in I^3(K)$. The dimension of ϕ is $7r$ or $7r+1$, depending on the parity of r.

We claim that $n < 7r$. Indeed, assume the contrary. Then $\dim(q) \leq \dim(\phi)$, so that q is isomorphic to a form of type $h_K^s \oplus \phi$ over K. Thus

$$\frac{3n}{7} \geq 3r \geq \operatorname{ed}_n(q) = \operatorname{ed}(\mathrm{T}_n; 2) \overset{\text{by Lemma 5.1}}{\geq} \operatorname{ed}(\mathbf{Spin}_n; 2) - 1\,.$$

The resulting inequality fails for every even $n \geq 12$ because for such n

$$\operatorname{ed}(\mathbf{Spin}_n; 2) \geq n/2;$$

see (3.2).

So, we may assume that $7r > n$, i.e., ϕ is isomorphic to $h_K^{\oplus s} \oplus q$ over K, for some $s \geq 1$. By comparing dimensions we get the equality $7r = n + 2s$ when r is even, and $7r + 1 = n + 2s$ when r is odd. The essential dimension of the form ϕ, as an element of $\mathrm{T}_{7r}(K)$ or $\mathrm{T}_{7r+1}(K)$ is at most $3r$, while Lemma 5.2 tells us that this essential dimension is at least $\operatorname{ed}_n(q) - s(s+2n-1)/2$.

From this, Lemma 5.1 and Theorem 3.3(a) we obtain the following chain of inequalities

$$\begin{aligned} 3r &\geq \mathrm{ed}_n(q) - \frac{s(s+2n-1)}{2} = \mathrm{ed}(\mathrm{T}_n; 2) - \frac{s(s+2n-1)}{2} \\ &\geq \mathrm{ed}(\mathbf{Spin}_n; 2) - 1 - \frac{s(s+2n-1)}{2} \\ &\geq 2^{(n-2)/2} - \frac{n(n-1)}{2} - 1 - \frac{s(s+2n-1)}{2}. \end{aligned} \tag{5.3}$$

Now suppose r is even. Substituting $s = (7r-n)/2$ into inequality (5.3), we obtain

$$\frac{49r^2 + (14n+10)r - 2^{(n+4)/2} - n^2 + 2n - 8}{8} \geq 0.$$

We interpret the left hand side as a quadratic polynomial in r. The constant term of this polynomial is negative for all $n \geq 8$; hence this polynomial has one positive real root and one negative real root. Denote the positive root by r_+. The above inequality is then equivalent to $r \geq r_+$. By the quadratic formula

$$r_+ = \frac{\sqrt{49 \cdot 2^{(n+4)/2} + 168n - 367} - (7n+5)}{49} \geq \frac{2^{(n+4)/4} - n - 2}{7}.$$

This completes the proof of Theorem 1.1 when r is even. If r is odd then substituting $s = (7r+1-n)/2$ into (5.3), we obtain an analogous quadratic inequality whose positive root is

$$r_+ = \frac{\sqrt{49 \cdot 2^{(n+4)/2} + 168n - 199} - (7n+12)}{49} \geq \frac{2^{(n+4)/4} - n - 2}{7},$$

and Theorem 1.1 follows. ♠

References

[Ada96] J. F. Adams, *Lectures on exceptional Lie groups*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1996.

[AP71] E. M. Andreev, V. L. Popov, *The stationary subgroups of points in general position in a representation space of a semisimple Lie group* (in Russian), Funkcional. Anal. i Priložen. **5** (1971), no. 4, 1–8.
English Translation in Functional Anal. Appl. **5** (1971), 265–271.

[BF03] Grégory Berhuy and Giordano Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330 (electronic).

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179.

[Bro07] Patrick Brosnan, *The essential dimension of a g-dimensional complex abelian variety is 2g*, Transform. Groups **12** (2007), no. 3, 437–441.

[BRV07] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli, *Essential dimension and algebraic stacks*, 2007, `arXiv:math/0701903v1 [math.AG]`.

[CS06] Vladimir Chernousov and Jean-Pierre Serre, *Lower bounds for essential dimensions via orthogonal representations*, J. Algebra **305** (2006), no. 2, 1055–1070.

[Gar08] Skip Garibaldi, *Cohomological invariants: exceptional groups and spin groups*, to appear in Memoirs of the AMS, preprint available at `arXiv:math.AG/0411424`.

[GMS03] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003.

[KM07] Nikita A. Karpenko and Alexander S. Merkurjev, *Essential dimension of finite groups*, to appear in Inventiones Math., **172**, no. 3, June, 2008. Preprint available at `http://www.mathematik.uni-bielefeld.de/lag/man/263.html`, 2007.

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998.

[Lam73] T. Y. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, Inc., Reading, Mass., 1973, Mathematics Lecture Note Series.

[Po85] A. M. Popov, *Finite stationary subgroups in general position of simple linear Lie groups* (Russian), Trudy Moskov. Mat. Obshch. **48** (1985), 7–59. English translation in *Transactions of the Moscow Mathematical Society*, A translation of Trudy Moskov. Mat. Obshch. 48 (1985). Trans. Moscow Math. Soc. 1986. American Mathematical Society, Providence, RI, 1986, 3–63.

[PV94] V. L. Popov, E. B. Vinberg, Invariant theory, in Algebraic geometry. IV. A translation of Algebraic geometry. **4** (Russian), Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989. Encyclopaedia of Mathematical Sciences, **55**, Springer-Verlag, Berlin, 1994.

[Rei00] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304.

[Rich88] R. W. Richardson, *Conjugacy classes of n-tuples in Lie algebras and algebraic groups*, Duke Math. J. **57** (1988), no. 1, 1–35.

[Ros99] Markus Rost, *On the Galois cohomology of* **Spin**(14), `http://www.mathematik.uni-bielefeld.de/~rost/spin-14.html`, 1999.

[RY00] Zinovy Reichstein and Boris Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056, With an appendix by János Kollár and Endre Szabó.

[Woo89] Jay A. Wood, *Spinor groups and algebraic coding theory*, J. Combin. Theory Ser. A **51** (1989), no. 2, 277–313.

(Brosnan, Reichstein) Department of Mathematics, The University of British Columbia, 1984 Mathematics Road, Vancouver, B.C., Canada V6T 1Z2

(Vistoli) Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy
E-mail address, Brosnan: `brosnan@math.ubc.ca`
E-mail address, Reichstein: `reichst@math.ubc.ca`
E-mail address, Vistoli: `angelo.vistoli@sns.it`