SUBCRITICAL EXPONENT OF GENERIC SPIN TORSORS

NIKITA A. KARPENKO

ABSTRACT. The torsion index of an algebraic group G can be defined as the *splitting index* of a generic G-torsor E. In the case of the spin group $G = \mathrm{Spin}(d)$, this is a 2-power 2^t with an exponent t determined in 2005 by Burt Totaro. The critical exponent $\mathrm{i}(t)$ of E is the exponent of the *partial splitting index* $2^{\mathrm{i}(t)}$ (also called *isotropy index*) of E given by the tth vertex of the Dynkin diagram of G. It plays a central role in the theory of all isotropy indexes of E, has been studied a lot, and was determined for many d in the recent years. The subcritical exponent $\mathrm{i}(t-1)$, corresponding to the $(t-1)$st vertex of the Dynkin diagram, was also successfully determined for many d (asymptotically for 100% of them) and always turned out to be equal to $t-1$. Here we find the first d (namely, $d = 33$) breaking this apparent rule. The result is based on several previous joint and solo works of the author as well as on some general additions developed in the present paper.

0. THE INTRODUCTION

Let us fix an arbitrary initial field F_0 and work with its arbitrary extension fields $F \supset F_0$. Fixing an integer $d \geq 3$, consider the split spin group $G := \mathrm{Spin}(d)$ defined over the initial field F_0. The *index* $i(X)$ of an algebraic variety X is the g.c.d. of degrees of its closed points. Recall that a G-torsor E over a field F is split if and only if it has a rational point. The index $i(E)$ is therefore the g.c.d. of degrees of finite field extensions of F splitting E.

Given a parabolic subgroup $P \subset G$, the G-torsor E is P-*isotropic* (c.f. [15]) if it admits reduction of structure to P, or, equivalently, the variety E/P admits a rational point (see [15, Lemma 2.2]). Therefore the P-*index* $i_P(E)$ of E, defined as the index of E/P, equals the g.c.d. of degrees of finite field extensions of F over which E becomes P-isotropic.

For instance, when plugging in a Borel subgroup $B \subset G$ in place of P, B-isotropic means split so that the B-isotropy index $i_B(E)$ of E is the same as the splitting index $i(E)$.

By [12, Theorem 6.4], when F and E vary (with fixed F_0, d, and P), the index $i_P(E)$ is maximal in the case of *generic* E, obtained as the generic fiber of the quotient map $\mathrm{GL}(N) \to \mathrm{GL}(N)/G$ given by an embedding $G \hookrightarrow \mathrm{GL}(N)$ of G into the general linear group $\mathrm{GL}(N)$ for some $N \geq 1$ over F_0. The field of definition for such E is the function field $F = F_0(\mathrm{GL}(N)/G)$.

Date: 10 Oct 2025. Revised: 15 Apr 2026.

Key words and phrases. Quadratic forms over fields; spin groups; orthogonal grassmannians; Chow rings. *Mathematical Subject Classification (2020):* 20G15; 14C25.

This work has been concluded during author's stay at the Max-Planck-Institut für Mathematik in Bonn.

A lot of (partially successful) works have been consecrated to attempts to identify $i_P(E)$ for all P and generic E. This paper provides another contribution to the area.

The index $i_B(E) = i(E)$ for generic E is the torsion index of G (see [8, Theorem A.2] for this result in a most general framework), computed for the spinor group G in [16, Theorem 0.1]. Noteworthily (and a priori not self-evidently), the answer does not depend on F_0.

Before concentrating on generic E, let us make some further remarks on an arbitrary G-torsor E.

Since the torsion index of G is a 2-power, every index $i_P(E)$ is a 2-power too (whether E is generic or not). We write $\mathrm{i}_P(E)$ for the corresponding exponent so that

$$i_P(E) = 2^{\mathrm{i}_P(E)}.$$

A G-torsor E is P-isotropic if and only if it is $P_{\max}$-isotropic for every maximal parabolic subgroup $P_{\max} \subset G$ containing the given parabolic $P \subset G$. Consequently, $i_P(E)$ is the g.c.d. of $i_{P_{\max}}(E)$ over all such $P_{\max}$. So, in order to determine the exponent $i_P(E)$ for every parabolic subgroup P, we just need to know it for all maximal ones.

The index $i_P(E)$ does not change when P is moved inside its conjugacy class. The conjugacy classes of maximal parabolic subgroups are in bijection with the vertices of the Dynkin diagram of G standardly numbered by the integers from 1 to n, where n is the integral part of $d/2$. This way, the problem of computing $i_P(E)$ for every P is reduced to computation of the n exponents $\mathrm{i}_1(E), \dots, \mathrm{i}_n(E)$.

The exponent $\mathrm{i}_1(E)$ can be defined using the standard maximal parabolic subgroup P_1 corresponding to the 1st vertex of the Dynkin diagram. The variety G/P_1 is the projective quadric given by the split d-dimensional quadratic form used to construct the group G itself. The G-torsor E yields a non-degenerate d-dimensional quadratic form q of trivial discriminant and Clifford invariant. The variety E/P_1 of the index

$$i(E/P_1) = i_{P_1}(E) = 2^{\mathrm{i}_1(E)}$$

is the projective quadric $q = 0$. The remaining standard maximal parabolic subgroups $P_2, \dots, P_n$ can be used to define $\mathrm{i}_2(E), \dots, \mathrm{i}_n(E)$. The varieties G/P_i (resp., E/P_i) are split orthogonal grassmannians (resp. orthogonal grassmannians given by q). Note that for even d, the situation is somewhat "messed up" "in the end": G/P_n and G/P_{n-1} are the (isomorphic) components of the (highest) grassmannian of n-planes, whereas the grassmannian of $(n-1)$-planes corresponds to the (non-maximal) parabolic subgroup $P_n \cap P_{n-1}$; however all varieties mentioned have the same index and thus can be interchanged without any influence on the business.

Focusing now on a generic G-torsor E, let us write

$$\mathrm{i}(1), \dots, \mathrm{i}(n)$$

for the corresponding exponents $\mathrm{i}_1(E), \dots, \mathrm{i}_n(E)$. The following properties of this *exponent sequence* have been established in the series of works [2], [6], [13].

Set $t := \mathrm{i}(n)$. Then the exponent sequence is very close to the *simple sequence*

$$1,\ 2,\ \dots,\ t{-}1,\ t,\ t,\ \dots,\ t$$

defined as the sequence of all integers from 1 to t in the natural order followed by the constant sequence. (For $d \le 6$ one has $t = 0$ so that the exponent sequence coincides with the simple one and all terms of the sequences are 0.) Namely, if for some dimension d the exponent sequence deviates from the simple one in some position, then the corresponding value in the exponent sequence is 1 lower than in the simple one. Furthermore, all positions with deviation form an interval which, if nonempty, contains t and starts not earlier than at $t-1$.

In particular, for $d \geq 7$, the exponent sequence is simple if and only if $\mathrm{i}(t) = t$. By this reason, in [10], the exponent $\mathrm{i}(t)$ was given the name of *critical exponent*. And $\mathrm{i}(t-1)$ became (in [7, Remark 3.6]) the *avant-critical*, or the *subcritical exponent* from the title of the present paper.

We say that *the critical exponent is high* (for a given dimension d), if $\mathrm{i}(t) = t$; otherwise $\mathrm{i}(t) = t-1$ and we say that *the critical exponent is low*. Similarly, *"the subcritical exponent is high"* means $\mathrm{i}(t-1) = t-1$ and *"the subcritical exponent is low"* means $\mathrm{i}(t-1) = t-2$.

Although, except for $d = 10$, the critical exponent is high for all $d \leq 16$ (c.f. [13, Appendix B]), it turned out that asymptotically, it is low for over 91% of d (see [7, Theorem 2.8]). On the contrary, the subcritical one turned out to be high for asymptotically 100% of d: by [13, Proposition A.4 and Theorem 3.2 with Remark 3.3], the proportion of $d < N$ for which the subcritical exponent is high tends to 1 when $N \to \infty$. And until now the subcritical exponent was high for 100% of all d for which it was determined!

The situation is changed by the present paper, where we find the very first d (namely, $d = 33$) with low subcritical exponent – see Theorem 5.1. We also treat all $d \leq 40$ in this respect and resolve some cases (notably $d = 32$) which were not accessible with the previously existing methods.

Let us point out that there is an algorithm which, in principle, allows one to determine all generic exponents for every d by certain computer calculations. For odd d, the algorithm, rephrased here in Theorem 4.4, has been established earlier in [7, Proposition 3.1] (based on several previous works). For even d the final algorithm is elaborated here for the subcritical exponent in Theorem 4.7 based notably on [9], [11], and [14]. Some important theoretical consequences are deduced from these algorithms. For instance, one sees that the generic exponents do not depend on the initial field F_0 ([11, Corollary 5.5]). This result is even less self-evident than the one on the torsion index mentioned earlier. Its proof is particularly hard for even d.

However, as to the determination of the actual values, when d grows, the computer calculations become extremely heavy very quickly so that the results actually obtained this way so far are reduced to $d \leq 20$. It is unthinkable to get, say, Theorem 5.1 by a direct computer calculation. Finding (sometimes pretty sophisticated) mathematical arguments replacing (or simplifying) computer calculations seems to be of decisive value in this business.

1. The ring C

Let C be the (associative commutative unital) graded ring, generated by homogeneous elements $\{c_i\}_{i\in\mathbb{N}}$ with c_i of degree i, subject for every $i \in \mathbb{N}$ to the degree $2i$ homogeneous relation

$$c_i^2 - 2c_{i-1}c_{i+1} + 2c_{i-2}c_{i+2} - \cdots + (-1)^{i-1}2c_1c_{2i-1} + (-1)^i 2c_{2i} = 0,$$

where $\mathbb{N}$ is the set of natural numbers $\{1, 2, \dots\}$.

Given some $n \in \mathbb{N}$, the *n-truncation of C* is the graded ring C_n, obtained from C by imposing the additional relations $c_i = 0$ for $i > n$. It can be identified with the Chow ring of the highest grassmannian of an alternating non-degenerate $2n$-dimensional bilinear form by mapping c_i to the ith Chern class of the tautological vector bundle. The additive group of C_n is free, a basis is given by the 2^n products $c_I := \prod_{i\in I} c_i$ for $I \subset \{1, \dots, n\}$, (see, e.g., [1, Theorem 1.2]). Since the nth graded component of C maps isomorphically onto the nth graded component of C_n, the additive group of C is also free and a basis is given by the products c_I for $I \subset \mathbb{N}$.

The *augmentation ideal* $\operatorname{Aug} C$ of C is the ideal generated by $\{c_i\}_{i\in\mathbb{N}}$. In other terms, $\operatorname{Aug} C \subset C$ is the ideal, generated by all homogeneous elements of positive degree.

The square of any element in $\operatorname{Aug} C$ is divisible by 2. This makes possible to define the *divided square operation*

$$s\colon \operatorname{Aug} C \to \operatorname{Aug} C, \qquad c \mapsto c^2/2.$$

Another consequence of the above observation is: for any $c \in \operatorname{Aug} C$ and any $a \in \mathbb{N}$, the power c^{2^a} is divisible by 2^{2^a-1}; namely, $c^{2^a} = 2^{2^a-1} s^a(c)$, where $s^a := s \circ \dots \circ s$ is the divided square operation s iterated a times. More generally, writing any given $k \in \mathbb{N}$ as a sum $2^{a_1} + \dots + 2^{a_b}$ of b distinct 2-powers (with $b = b(k) \in \mathbb{N}$ being the sum of the base 2 digits of k), we get that c^k is divisible by $2^{k-b(k)}$. More exactly,

$$c^k = 2^{k-b(k)} s^{(k)}(c), \tag{1.1}$$

where $s^{(k)}(c)$ is the product $s^{a_1}(c) \dots s^{a_b}(c)$.

Let us define *degree* of a set $I \subset \mathbb{N}$ as the sum of its elements whereas the *order* of I is meant to be the number of elements in I. The following computation, made in [7, Lemma 3.4], generalizes [16, Lemma 5.4]:

Lemma 1.2 ([7, Lemma 3.4])**.** *For any $k \in \mathbb{N}$, $s^{(k)}(c_1)$ modulo 2 is the sum of c_I over all degree k sets $I \subset \mathbb{N}$ that can be decomposed in a disjoint union of subsets of order at most 2 and of degree a 2-power.*

Lemma 1.3. *For any $k \in \mathbb{N}$, the highest 2-power divisor of c_1^k is $2^{k-b(k)}$.*

Proof. By Lemma 1.2, $s^{(k)}(c_1)$ from formula (1.1) is not divisible by 2 anymore: the coordinate of $s^{(k)}(c_1)$ modulo 2 at the basis element c_I is nonzero for

$$I = \{2^{a_1}, \dots, 2^{a_{b(k)}}\} = \{2^{a_1}\} \coprod \dots \coprod \{2^{a_{b(k)}}\}. \qquad \square$$

2. The polynomial f_l

For any integer $l \geq 0$, we define a degree 2^l homogeneous polynomial f_l in $l+1$ variables $x, x_1, \dots, x_l$ over the integers $\mathbb{Z}$:

$$f_l := \prod_{I \subset \{1,\dots,l\}} (x - \sum_{i\in I} x_i) \quad \in \mathbb{Z}[x, x_1, \dots, x_l]. \tag{2.1}$$

These polynomials all together satisfy the inductive formula

$$f_{l+1}(x) = f_l(x) \cdot f_l(x - x_{l+1}). \tag{2.2}$$

Using it one proves

Lemma 2.3 ([10, Remark 3.4]). *For any $l \geq 0$, each of the variables $x, x_1, \dots, x_l$ appears in the polynomial f_l modulo 2 with a 2-power exponent only.*[1] *Besides,*

$$f_{l+1}(x) \equiv f_l(x)^2 + f_l(x) \cdot f_l(x_{l+1}) \text{ modulo } 2.$$

Proposition 2.4. *For any $k \in \mathbb{N}$, the coefficient at x^k in the polynomial f_l (viewed this time as a polynomial in x over the ring $\mathbb{Z}[x_1, \dots, x_l]$) is divisible by $2^{b(k)-1}$.*

Proof. Mapping x to $c_1 \in C$ and x_i to $2x_i$ for $i = 1, \dots, l$, we embed the polynomial ring $\mathbb{Z}[x, x_1, \dots, x_l]$ into the polynomial ring $C[x_1, \dots, x_l]$. By Lemma 1.3, it suffices to show that f_l, viewed as an element of the latter ring, is divisible by 2^{2^l-1}. We show this using induction on l, starting with the trivial case of $l = 0$, where $f_l = f_0 = c_1$ and $2^{2^l-1} = 2^0 = 1$.

Note that the divided square operation s, defined on $\operatorname{Aug} C$ in §1, extends to the ideal $(2, \operatorname{Aug} C)[x_1, \dots, x_l]$ in $C[x_1, \dots, x_l]$ generated by 2 and $\operatorname{Aug} C$.

Assuming that the statement holds for f_l with some $l \geq 0$, we prove that it holds for f_{l+1} using inductive formula (2.2) which now reads as

$$f_{l+1}(c_1) = f_l(c_1) \cdot f_l(c_1 - 2x_{l+1}).$$

The quotient $g_l := f_l/2^{2^l-1}$ is a linear combination of

$$s^{(1)}(c_1), s^{(2)}(c_1), \dots, s^{(2^l)}(c_1) = s^l(c_1)$$

with coefficients in $\mathbb{Z}[x_1, \dots, x_l]$, where for each $k \in \mathbb{N}$ the coefficient at $s^{(k)}(c_1)$ is the divided by $2^{b(k)-1}$ coefficient at x^k of the original polynomial

$$f_l(x) \in (\mathbb{Z}[x_1, \dots, x_l])[x]$$

from (2.1). All we need to do is to show that the product

$$g_l(c_1) \cdot g_l(c_1 - 2x_{l+1})$$

is divisible by 2.

The point is that $s^{(k)}(c_1 - 2x_{l+1}) \equiv s^{(k)}(c_1) \mod 2$ for any $k \in \mathbb{N}$ simply because the extended divided square operation

$$s\colon (2, \operatorname{Aug} C)[x_1, \dots, x_l] \to (2, \operatorname{Aug} C)[x_1, \dots, x_l], \qquad c \mapsto c^2/2$$

passes to the quotient $(2, \operatorname{Aug} C)[x_1, \dots, x_l]/2C[x_1, \dots, x_l]$. Therefore

$$g_l(c_1) \cdot g_l(c_1 - 2x_{l+1}) \equiv g_l(c_1)^2 = 2s(g_l(c_1)) \equiv 0. \qquad \square$$

For $l \geq 1$, the degree 2^l homogeneous polynomial f_l decomposes into the product

$$f_l = f_l^{\text{even}} \cdot f_l^{\text{odd}}$$

of two degree 2^{l-1} homogeneous polynomials f_l^{even} and f_l^{odd}, defined as

$$(2.5) \qquad f_l^{\text{even}} := \prod_{\text{even } I \subset \{1,\dots,l\}} (x - \sum_{i \in I} x_i) \quad \text{and} \quad f_l^{\text{odd}} := \prod_{\text{odd } I \subset \{1,\dots,l\}} (x - \sum_{i \in I} x_i),$$

where an even (resp., odd) set $I \subset \{1, \dots, l\}$ is a set of even (resp., odd) order.

These polynomials satisfy the inductive formulas

$$(2.6) \qquad f_{l+1}^{\text{even}}(x) = f_l^{\text{even}}(x) \cdot f_l^{\text{odd}}(x - x_{l+1}) \quad \text{and} \quad f_{l+1}^{\text{odd}}(x) = f_l^{\text{odd}}(x) \cdot f_l^{\text{even}}(x - x_{l+1}).$$

[1] Appearing with exponent 0 is considered as non-appearing and is therefore allowed.

Using them, similarly to [10, Remark 3.4], one proves

Lemma 2.7. *For any $l \geq 1$, each of the variables $x, x_1, \dots, x_l$ appears in the polynomial f_l^{even} (resp., f_l^{odd}) modulo 2 with a 2-power exponent only.*[2] *Besides,*

$$f_{l+1}^{\text{even}}(x) \equiv f_l(x) + f_l^{\text{even}}(x) \cdot f_l^{\text{odd}}(x_{l+1}) \quad \textit{and} \quad f_{l+1}^{\text{odd}}(x) \equiv f_l(x) + f_l^{\text{odd}}(x) \cdot f_l^{\text{even}}(x_{l+1})$$

modulo 2. □

Proposition 2.8. *For any $l \geq 1$, Proposition 2.4 also holds for the polynomial f_l^{even} as well as for the polynomial f_l^{odd} in place of f_l: for any $k \in \mathbb{N}$, the coefficient at x^k in each of these two polynomials is divisible by $2^{b(k)-1}$. Moreover, the sum of the two coefficients is divisible by $2^{b(k)}$.*

Proof. As in the proof of Proposition 2.4, mapping x to $c_1 \in C$ and x_i to $2x_i$ for $i = 1, \dots, l$, we embed the polynomial ring $\mathbb{Z}[x, x_1, \dots, x_l]$ into the polynomial ring $C[x_1, \dots, x_l]$. By Lemma 1.3, to prove the first statement of Proposition 2.8, it suffices to show that f_l^{even} and f_l^{odd}, viewed as elements of the latter ring, are divisible by $2^{2^{l-1}-1}$.

We prove the statement on both polynomials simultaneously by induction on l starting with the trivial case of $l = 1$ and using inductive formulas (2.6) which now read as

$$f_{l+1}^{\text{even}}(c_1) = f_l^{\text{even}}(c_1) \cdot f_l^{\text{odd}}(c_1 - 2x_{l+1}) \text{ and } f_{l+1}^{\text{odd}}(c_1) = f_l^{\text{odd}}(c_1) \cdot f_l^{\text{even}}(c_1 - 2x_{l+1}).$$

The quotients $g_l^{\text{even}} := f_l^{\text{even}}/2^{2^{l-1}-1}$ and $g_l^{\text{odd}} := f_l^{\text{odd}}/2^{2^{l-1}-1}$, viewed modulo 2, are linear combinations of

$$s^{(1)}(c_1),\ s^{(2)}(c_1),\ \dots,\ s^{(2^{l-1})}(c_1) = s^{l-1}(c_1)$$

with coefficients in $\mathbb{Z}[x_1, \dots, x_l]$, where for each $k \in \mathbb{N}$ the coefficient at $s^{(k)}(c_1)$ is the divided by $2^{b(k)-1}$ and then viewed modulo 2 coefficient at x^k of the original

$$f_l^{\text{even}}(x) \quad \text{and} \quad f_l^{\text{odd}}(x) \quad \in (\mathbb{Z}[x_1, \dots, x_l])[x].$$

(Note that unlike $f_l^{\text{even}}(x)$, the polynomial $f_l^{\text{odd}}(x)$ has a nonzero constant term; however the resulting nonzero constant term of the polynomial g_l^{odd} vanishes modulo 2.) All we need to do is to show that the products

$$g_l^{\text{even}}(c_1) \cdot g_l^{\text{odd}}(c_1 - 2x_{l+1}) \quad \text{and} \quad g_l^{\text{odd}}(c_1) \cdot g_l^{\text{even}}(c_1 - 2x_{l+1})$$

are divisible by 2.

Since $s^{(k)}(c_1 - 2x_{l+1}) \equiv s^{(k)}(c_1) \mod 2$ for any k, we have

$$g_l^{\text{even}}(c_1) \cdot g_l^{\text{odd}}(c_1 - 2x_{l+1}) \equiv g_l^{\text{even}}(c_1) \cdot g_l^{\text{odd}}(c_1) = 2g_l(c_1) \equiv 0 \text{ and}$$
$$g_l^{\text{odd}}(c_1) \cdot g_l^{\text{even}}(c_1 - 2x_{l+1}) \equiv g_l^{\text{odd}}(c_1) \cdot g_l^{\text{even}}(c_1) = 2g_l(c_1) \equiv 0,$$

where, as in the proof of Proposition 2.4, g_l stands for $f_l/(2^{2^l-1})$.

The second statement of Proposition 2.8 is equivalent to the congruence

$$g_l^{\text{even}}(c_1) \equiv g_l^{\text{odd}}(c_1) \text{ modulo } 2. \tag{2.9}$$

[2] Appearing with exponent 0 is considered as non-appearing and is therefore allowed.

This congruence is also proved by induction on l. Assuming that it holds for some $l \geq 1$, we prove it for $l+1$ via the formula

$$f_{l+1}^{\text{even}}(c_1) + f_{l+1}^{\text{odd}}(c_1) = (f_l^{\text{even}}(c_1) + f_l^{\text{even}}(c_1 - 2x_{l+1})) \cdot (f_l^{\text{odd}}(c_1) + f_l^{\text{odd}}(c_1 - 2x_{l+1})) - (f_l(c_1) + f_l(c_1 - 2x_{l+1})). \tag{2.10}$$

For the first factor of the product on the right, we have

$$f_l^{\text{even}}(c_1) + f_l^{\text{even}}(c_1 - 2x_{l+1}) = 2^{2^{l-1}-1}(g_l^{\text{even}}(c_1) + g_l^{\text{even}}(c_1 - 2x_{l+1})).$$

The result is divisible by $2^{2^{l-1}}$ by (2.9) because $g_l^{\text{even}}(c_1 - 2x_{l+1}) \equiv g_l^{\text{even}}(c_1)$ modulo 2. Similarly, the second factor of the product on the right in (2.10) is divisible by $2^{2^{l-1}}$ and so the product of the two factors, i.e., the first summand on the right in (2.10) is divisible by 2^{2^l}. As to the sum $f_l(c_1) + f_l(c_1 - 2x_{l+1})$, it is divisible by 2^{2^l-1} and yields $g_l(c_1) + g_l(c_1 - 2x_{l+1}) \equiv 0$ modulo 2 after the division. It follows that $f_{l+1}^{\text{even}}(c_1) + f_{l+1}^{\text{odd}}(c_1)$ is divisible by 2^{2^l} which means that $g_{l+1}^{\text{even}}(c_1) \equiv g_{l+1}^{\text{odd}}(c_1)$ modulo 2 as desired. □

3. The ring E

Let E be the (associative commutative unital) graded ring, generated by homogeneous elements $\{e_i\}_{i\in\mathbb{N}}$ with e_i of degree i, subject for every $i \in \mathbb{N}$ to the degree $2i$ homogeneous relation

$$e_i^2 - 2e_{i-1}e_{i+1} + 2e_{i-2}e_{i+2} - \cdots + (-1)^{i-1}2e_1e_{2i-1} + (-1)^i e_{2i} = 0.$$

We view the ring C of §1 as a subring in E via the embedding $c_i \mapsto 2e_i$, $i \in \mathbb{N}$.

Given $n \in \mathbb{N}$, the *n-truncation of E* is the graded ring E_n, obtained from E by imposing the additional relations $e_i = 0$ for $i > n$. By [3, Proposition 86.16], it can be identified with the Chow ring of the highest grassmannian of a split $(2n+1)$-dimensional quadratic form. The additive group of E_n is free, a basis is given by the products $e_I := \prod_{i\in I} e_i$ for $I \subset \{1, \ldots, n\}$, (see, e.g., [3, Theorem 86.12]). Since the nth graded component of E maps isomorphically onto the nth graded component of E_n, the additive group of E is also free and a basis is given by the products e_I for $I \subset \mathbb{N}$.

It follows from Lemma 1.3 that $2^{b(k)}e_1^k \in C$ for any integer $k \geq 0$. More explicitly,

$$2^{b(k)}e_1^k = s^{(k)}(c_1).$$

Therefore, viewing the polynomial $f_l = f_l(x)$ of (2.1) as a polynomial in the variable x over the ring $\mathbb{Z}[x_1, \ldots, x_l]$ and considering $f_l(e_1) \in E[x_1, \ldots, x_l]$, we get by Proposition 2.4 that $2f_l(e_1) \in C[x_1, \ldots, x_l]$. Moreover, $2f_l(e_1) \in (2, \operatorname{Aug} C)[x_1, \ldots, x_l]$ so that

$$2^{b(k)}f_l(e_1)^k \in (2, \operatorname{Aug} C)[x_1, \ldots, x_l] \subset C[x_1, \ldots, x_l] \subset E[x_1, \ldots, x_l] \quad \text{for any } k \in \mathbb{N}. \tag{3.1}$$

Similarly, applying Proposition 2.8, we get that

$$2^{b(k)}f_l^{\text{even}}(e_1)^k, \;\; 2^{b(k)}f_l^{\text{odd}}(e_1)^k \in (2, \operatorname{Aug} C)[x_1, \ldots, x_l] \quad \text{for any } k \in \mathbb{N}.$$

Moreover, these two elements are congruent modulo $2C[x_1, \ldots, x_l]$ by (2.9) for $k = 1$ and therefore for any k so that

$$2^{b(k)-1}\big(f_l^{\text{even}}(e_1)^k + f_l^{\text{odd}}(e_1)^k\big) \in C[x_1, \ldots, x_l] \quad \text{for any } k \in \mathbb{N}.$$

4. The general algorithm

Let $\tilde{C}_n$ be the Chow ring of the full flag variety of the tautological vector bundle $\mathcal{T}$ on the highest grassmannian of a $2n$-dimensional alternating bilinear form. As a C_n-algebra, $\tilde{C}_n$ is generated by the n roots $\xi_1,\dots,\xi_n$ of $\mathcal{T}$ subject to the relations $\sigma_i = c_i$ for $i \in \{1,\dots,n\}$, where σ_i is the ith elementary symmetric polynomial in $\xi_1,\dots,\xi_n$. Note that the roots $\xi_1,\dots,\xi_n$ generate $\tilde{C}_n$ as a ring whereas the relations are given by vanishing of the elementary symmetric polynomials in the squares $\xi_1^2,\dots,\xi_n^2$.

As a C_n-module, $\tilde{C}_n$ is free; a basis is given by the products

$$\xi_1^{a_1}\dots\xi_n^{a_n} \tag{4.1}$$

with the exponents satisfying $a_i \le n-i$ for $i \in \{1,\dots,n\}$. Note that

$$\xi_i^n - c_1{\cdot}\xi_i^{n-1} + \dots + (-1)^{n-1}c_{n-1}{\cdot}\xi + (-1)^n c_n = 0 \tag{4.2}$$

for any $i \in \{1,\dots,n\}$.

We are going to consider the homomorphism

$$C[x_1,\dots,x_l] \to \tilde{C}_n, \tag{4.3}$$

induced by the truncation homomorphism $C \to C_n$ and mapping the variables $x_1,\dots,x_l$ to the roots $\xi_1,\dots,\xi_l$, respectively.

Using the notation and terminology of §0, for any odd d, we will describe in Theorem 4.4 below the algorithm for the determination of the exponent sequence $\mathrm{i}(1),\dots,\mathrm{i}(n)$. For even d, we will describe in Theorem 4.7 the algorithm for the determination of the subcritical exponent.

The last exponent $t := \mathrm{i}(n)$ is the exponent of the torsion index 2^t of $\mathrm{Spin}(d)$, which has been determined in [16, Theorem 0.1].

It has been shown in [13] (based on [2] and [6]) that $\mathrm{i}(m) = m$ for $m < t-1$, $\mathrm{i}(t-1) \in \{t-2, t-1\}$, and $\mathrm{i}(m) \in \{t-1, t\}$ for $m \ge t$ (cf. §0).

In the case of odd $d = 2n+1$, the algorithm determining $\mathrm{i}(m)$ for $m \ge t-1$, worked out in [7], reads as follows:

Theorem 4.4 ([7, Proposition 3.1])**.** *Assume that $d = 2n+1$.*

For $m = t-1$, one has $\mathrm{i}(m) = t-2$ (i.e., the subcritical exponent is low) if and only if the image in $\tilde{C}_n$ under (4.3) of $2f_{n-m}(e_1) \in C[x_1,\dots,x_{n-m}]$ (see (3.1)) is nontrivial modulo 2.

For $m \ge t$, one has $\mathrm{i}(m) = t-1$ if and only if the image of $2^j f_{n-m}(e_1)^{2^j-1}$ in $\tilde{C}_n/2\tilde{C}_n$ is nontrivial, where $j := m-t+1$.

In particular, $\mathrm{i}(t) = t-1$ (i.e., the critical exponent is low) if and only if the image of $2f_{n-t}(e_1)$ in $\tilde{C}_n/2\tilde{C}_n$ is nontrivial.

Remark 4.5. As already mentioned in the beginning of this section, the ring $\tilde{C}_n$ is generated by the elements $\xi_1,\dots,\xi_n$ subject to the relations given by vanishing of all elementary symmetric polynomials in $\xi_1^2,\dots,\xi_n^2$. To make the statement of Theorem 4.4 more straightforward, we notice that the image of $2^{n-m}f_{n-m}(e_1)$ in $\tilde{C}_n$ equals

$$\prod(\pm\xi_1 \pm \dots \pm \xi_{n-m} + \xi_{n-m+1} + \dots + \xi_n).$$

As we know, this product is divisible by 2^{n-m-1} in $\tilde{C}_n$. We also know that each of its powers is always divisible by a certain higher 2-power. In each case listed in Theorem 4.4, the algorithm asks about divisibility of a certain power of this element by the 2-power directly following the one from the previous sentence.

Recall that $\tilde{C}_n/2\tilde{C}_n$ is the modulo 2 Chow ring $\mathrm{Ch}(X)$ of the complete flag variety X of the tautological vector bundle on the highest grassmannian of a $2n$-dimensional alternating bilinear form b. For every $m \in \{1, \dots, n\}$, the variety X projects to the mth grassmannian X_m of b. The pull-back pr^* with respect to this projection $pr\colon\ X \to X_m$ yields a ring homomorphism $\mathrm{Ch}(X_m) \to \mathrm{Ch}(X)$.

Lemma 4.6. *The image in $\tilde{C}_n/2\tilde{C}_n$ of the element $2f_{n-m}(e_1)$, appearing in Theorem 4.4, lies in the image of pr^*. The image in $\tilde{C}_n/2\tilde{C}_n$ of the element $f^{\mathrm{even}}_{n-m}(e_1) + f^{\mathrm{odd}}_{n-m}(e_1)$, appearing in Theorem 4.7 below, also lies in the image of pr^*. Multiplication by $c_1 \dots c_{n-m}$ is injective on the image of pr^*.*

Proof. The image of the pull-back homomorphism $\mathrm{CH}(X_m) \to \mathrm{CH}(X)$ of the integral Chow rings is the subring in $\mathrm{CH}(X)$ generated by the elementary symmetric polynomials in $\xi_{n-m+1}, \dots, \xi_n$. The symmetric polynomials in $\xi_1^2, \dots, \xi_{n-m}^2$ are also in the image. Therefore the product of Remark 4.5 is in the image of $\mathrm{CH}(X_m)$. By [2, Proof of Lemma 2.2], the additive homomorphism $\mathrm{CH}(X_m) \to \mathrm{CH}(X)$ is a split injection. This proves the first statement of Lemma 4.6. The second statement is proved similarly.

To prove the third statement, let us notice that multiplication by an appropriate multiple μ of $c_1 \dots c_{n-m}$ followed by the push-forward pr_* provides a splitting for pr^*. The described composition provides indeed a splitting by the projection formula [3, Proposition 56.9] once $pr_*(\mu) = 1$. To achieve this equality, one chooses μ the way that its pull-back to the generic fiber of pr yields the class of a rational point, c.f. [2, Proof of Lemma 2.2]. Note that the generic fiber of pr is a flag variety over the highest grassmannian X' of an alternating non-degenerate $2(n-m)$-dimensional bilinear form; therefore the class of a rational point on the generic fiber is divisible by the class $c_1 \dots c_{n-m}$ of a rational point on X'. □

In the case of even $d = 2n$, a similar to Theorem 4.4 algorithm, determining $\mathrm{i}(m)$ for $m \geq t-1$, can be worked out from [11, Theorem 5.3] with a help of the duality result [14, Theorem 1.2]. Since this current paper is centered around the subcritical exponent, we formulate it for $m = t-1$ only:

Theorem 4.7. *Assume that $d = 2n$. For $m = t-1$, one has $\mathrm{i}(m) = t-2$ (i.e., the subcritical exponent is low) if and only if the image of $f^{\mathrm{even}}_{n-m}(e_1) + f^{\mathrm{odd}}_{n-m}(e_1)$ in $\tilde{C}_n$ multiplied by $\xi := \xi_{n-m+1} \dots \xi_n \in \tilde{C}_n$ is nontrivial modulo $2\tilde{C}_n$.*

Proof. For $m = t-1$, let Y_m be the mth grassmannian of the split d-dimensional quadratic form q_0, and let Y be the full flag variety of q_0. In terms of the group $G = \mathrm{Spin}(d)$, Y is the quotient G/B by the standard Borel subgroup $B \subset G$, whereas Y_m is the quotient G/P_m by the mth standard maximal parabolic subgroup $P_m \subset G$.

Let $\tilde{E}_n$ be the E_n-algebra generated by elements $\xi_1, \dots, \xi_n$ subject to the relations $\sigma_i = c_i$ for $i \in \{1, \dots, n\}$, where, as before, $c_i = 2e_i$ and σ_i is the ith elementary symmetric polynomial in $\xi_1,\dots,\xi_n$. By [3, Proposition 86.16], the integral Chow ring $\mathrm{CH}(Y_n)$ is identified with the ring E_{n-1} which is the quotient $E_n/(e_n)$ of the ring E_n by the ideal $(e_n)=e_nE_n$. Since Y is the full flag variety of the tautological vector bundle on Y_n, the integral Chow ring $\mathrm{CH}(Y)$ is identified with the quotient $\tilde{E}_n/(e_n)$ of the ring $\tilde{E}_n$ by the ideal $(e_n)=e_n\tilde{E}_n$. The pull-back with respect to the projection $Y\to Y_m$ identifies $\mathrm{CH}(Y_m)$ with a subring in $\mathrm{CH}(Y)$.

Let D be the subring in $\mathrm{CH}(Y_m)$, generated by the Chern classes of the tautological vector bundle on Y_m. As a subring in $\mathrm{CH}(Y)$, D is generated by the elementary symmetric polynomials in $\xi_{n-m+1},\dots,\xi_n$. The additive group of D is free of finite rank, see e.g. [4, Theorem 2.1]. By [4, Theorem 6.1], the ring D can be viewed as the Chow ring of the mth grassmannian of a *generic* d-dimensional quadratic form (without any restriction on its discriminant or Clifford invariant).

By arguments as in the proof of Lemma 4.6, the image φ of $f^{\mathrm{even}}_{n-m}(e_1)$ in $\tilde{E}_n/(e_n)=\mathrm{CH}(Y)$, as well as the image of $f^{\mathrm{odd}}_{n-m}(e_1)$, belong to $\mathrm{CH}(Y_m)\subset\mathrm{CH}(Y)$. If $n\le 8$, then $\dim Y_m$ is smaller than the degree $2^{n-m-1}=2^{n-t}$ of these homogeneous elements of the Chow ring. It follows that the two images (as well as their sum) vanish. In particular, the condition of Theorem 4.7 dealing with the sum $f^{\mathrm{even}}_{n-m}(e_1)+f^{\mathrm{odd}}_{n-m}(e_1)$ is *not* satisfied. At the same time, the subcritical exponent is known to be high and therefore Theorem 4.7 holds for $n\le 8$.

So, we can assume (and we do from now on in this proof) that $n\ge 9$. This implies that $n-m\ge 6$ (the difference increases with n and is 6 for $n=9$). Therefore, by [11, Theorem 5.3], the (additive) degree homomorphism

$$\deg\colon\ \mathrm{CH}(Y_m)\to\mathbb{Z}, \tag{4.8}$$

given by the push-forward of the structure map of the variety Y_m, maps the subring $D[\varphi]\subset\mathrm{CH}(Y_m)$ onto the ideal $2^{\mathrm{i}(m)}\mathbb{Z}\subset\mathbb{Z}$. This is a "first approximation" of the algorithm for the determination of $\mathrm{i}(m)$ which we are going to work out to eventually get Theorem 4.7.

Recall that the Chow ring $\mathrm{CH}(Y_m)$ is graded by codimension. To distinguish the degree of a homogeneous element in this graded ring from degree (4.8), let us refer as *codimension degree* to the first one.

By Lemma 4.9 below, the codimension degree of φ^2 exceeds $\dim Y_m$. Consequently, $D[\varphi]=D+\varphi D$. Since $\deg(D)=2^m\mathbb{Z}=2^{t-1}\mathbb{Z}$, the subcritical exponent $\mathrm{i}(t-1)$ is determined by $\deg(\varphi D)$: it is low if and only if $\deg(\varphi D)\ni 2^{t-2}$.

The ring $\mathrm{CH}(Y)$ possesses an involution τ changing the sign of ξ_1 and leaving invariant $\xi_2,\dots,\xi_n$. Note that the involution is determined by its action on $\xi_1,\dots,\xi_n$; in particular, $\tau(e_1)=e_1-\xi_1$. This involution leaves the subring $\mathrm{CH}(Y_m)\subset\mathrm{CH}(Y)$ globally invariant; moreover, the resulting involution on $\mathrm{CH}(Y_m)$ is given by an involution on Y_m. It follows that the degree homomorphism (4.8) satisfies $\deg\circ\tau=\deg$.

The involution τ acts as identity on D and changes the sign of the element

$$\varepsilon:=\xi_1\dots\xi_{n-m}\in\mathrm{CH}(Y_m)$$

which is the image of the Euler class (defined as in [5]) under the homomorphism of [2, Lemma 2.2]. It follows that $D\cap\varepsilon D=0$ and $\deg(\varepsilon D)=0$. By [13, Proposition 5.6], the element 2φ belongs to the direct sum $D\oplus\varepsilon D\subset\mathrm{CH}(Y_m)$, and $\tau(\varphi)$ is given by the image of $f^{\mathrm{odd}}_{n-m}(e_1)$. The D-component $\varphi+\tau(\varphi)$ of $2\varphi \in D\oplus\varepsilon D$ is therefore related to the sum $f^{\mathrm{even}}_{n-m}(e_1)+f^{\mathrm{odd}}_{n-m}(e_1)$ considered in Theorem 4.7.

Let q_0' be a $(d+1)$-dimensional non-degenerate quadratic form containing q_0 as a subform. The mth grassmannian Y_m' of q_0' contains Y_m as a closed subvariety. As explained in [14, §2], the push-forward homomorphism $\mathrm{CH}(Y_m)\to\mathrm{CH}(Y_m')$ maps D to the subring $D'\subset\mathrm{CH}(Y_m')$ generated by the Chern classes of the tautological vector bundle on Y_m'. By [14, Proposition 2.2], the induced homomorphism $D/2D\to D'/2D'$ is injective. Furthermore, the pull-back homomorphism $\mathrm{CH}(Y_m')\to\mathrm{CH}(Y')$ with respect to the projection $Y'\to Y_m'$ of the full flag variety Y' of q_0' yields a split injection $D'\to\tilde{C}_n$. As a consequence, the induced homomorphism $D'/2D'\to\tilde{C}_n/2\tilde{C}_n$ is also injective.

The image of the element $\varphi+\tau(\varphi)\in D$ in $\tilde{C}_n$ coincides with the image of the sum $f^{\mathrm{even}}_{n-m}(e_1)+f^{\mathrm{odd}}_{n-m}(e_1)$ multiplied by ξ.

After all these preliminaries, we are now finally in position to directly proceed with the proof of Theorem 4.7. Assume that the image of $f^{\mathrm{even}}_{n-m}(e_1)+f^{\mathrm{odd}}_{n-m}(e_1)$ in $\tilde{C}_n/2\tilde{C}_n$ multiplied by ξ vanishes, where $m=t-1$. Then $\varphi+\tau(\varphi)\in 2D$ implying that

$$\deg(\varphi D)=\deg\left(\frac{\varphi+\tau(\varphi)}{2}D\right)\subset\deg(D)\not\ni 2^{t-2}$$

and yielding highness of the subcritical exponent.

To finish, let us now assume that the image of $f^{\mathrm{even}}_{n-m}(e_1)+f^{\mathrm{odd}}_{n-m}(e_1)$ in $\tilde{C}_n/2\tilde{C}_n$ multiplied by ξ does not vanish. Then the element $\varphi+\tau(\varphi)$ of D does not vanish modulo $2D$ and it follows by the duality theorem [14, Theorem 1.2] (which is Theorem 1.3 in the preprint version of [14]) that $\deg(\varphi D)\ni 2^{t-2}$ meaning lowness of the subcritical exponent. □

Here is the dimension estimation applied in the above proof:

Lemma 4.9. *Let t be Totaro's number for an even dimension $d=2n+2$. (We write d in this form, not in the form $d=2n$, in order to comply with the convention of* [13, Appendix A]*.) Then*

$$\dim Y_{t-1}<2^{n-t+2},$$

where Y_{t-1} is the subcritical grassmannian of a d-dimensional quadratic form.

Proof. By [13, Proposition A.1], one has $\dim Y_t<3\cdot 2^{n-t}$, where Y_t is the critical grassmannian of a d-dimensional quadratic form. Therefore it suffices to check that

$$\dim Y_{t-1}-\dim Y_t\le 2^{n-t}.$$

We have

$$\dim Y_{t-1}-\dim Y_t=3t-3-2n\le n$$

because $t\le n$. On the other hand,

$$2^{n-t+2}\ge\dim Y_{n+1}=n(n+1)/2$$

by definition of t and so

$$2^{n-t}\ge n(n+1)/8.$$

Since $n(n+1)/8\ge n$ for $n\ge 7$, we are done for such n. For $n\le 7$, as already mentioned in the proof of Theorem 4.7, even the stronger inequality $\dim Y_{t-1}\le 2^{n-t+1}$ holds than the one of Lemma 4.9 as one checks directly. □

Remark 4.10. As already mentioned in the beginning of this section, the ring $\tilde{C}_n$ is generated by the elements $\xi_1, \dots, \xi_n$ subject to the relations given by vanishing of all elementary symmetric polynomials in $\xi_1^2, \dots, \xi_n^2$. Let us also recall that $c_n = \xi_1 \dots \xi_n$ in $\tilde{C}_n$. To make the statement of Theorem 4.7 more straightforward, we notice that the images of $2^{n-m-1} f^{\text{even}}_{n-m}(e_1)$ and $2^{n-m-1} f^{\text{odd}}_{n-m}(e_1)$ in $\tilde{C}_n$ equal respectively

$$\prod_{\text{even}} (\pm\xi_1 \pm \dots \pm \xi_{n-m} + \xi_{n-m+1} + \dots + \xi_n) \qquad \text{and}$$

$$\prod_{\text{odd}} (\pm\xi_1 \pm \dots \pm \xi_{n-m} + \xi_{n-m+1} + \dots + \xi_n),$$

where the first product is taken over the sums with even number of minuses whereas the second product is taken over the sums with odd number of minuses.

Remark 4.11. Since the algorithm in the case of even d is more complicated (and requires much more work to be obtained) than in the case of odd d, it is useful to take into account a tight relationship between the exponent sequence for $d = 2n + 1$ and the exponent sequence for $d = 2n + 2$ (rather than for $d = 2n$). First of all, Totaro's number t is the same for both $d \in \{2n+1,\ 2n+2\}$. And then, by [13, Lemma 2.3], the deviation interval for the odd d is contained in the deviation interval for the even d. (In particular, if the (sub)critical exponent is low for the odd d, then it is also low for the even d.) Moreover, still by [13, Lemma 2.3], the end positions of the two deviation intervals differ at most by 1.

Let us also mention that the only pair $\{2n + 1,\ 2n + 2\}$ for which the two deviation intervals are *not* the same, known so far, is the pair $\{9,\ 10\}$ (check it out with the table of [13, Appendix B]!).

5. The main result

Theorem 5.1. *The subcritical exponent is low for* $d \in \{33,\ 34\}$*. For all remaining* $d \le 40$ *(for which it is defined), the subcritical exponent is high.*

Proof. Since $t \le 1$ for $d \le 12$, the subcritical exponent is defined for $d \ge 13$ only.

For $d = 2n + 1$ and $d = 2n + 2$ (with $n \ge 6$)), the subcritical exponent $\mathrm{i}(t - 1)$ is high if the dimension

$$(t - 1)(t - 2)/2 + (t - 1)(d - 2(t - 1))$$

of the $(t - 1)$st orthogonal grassmannian of a d-dimensional quadratic form is less than $2^{n-(t-1)}$, because the elements which determine the subcritical exponent in Theorems 4.4 and 4.7 have degree at least $2^{n-(t-1)}$ and come by Lemma 4.6 from the Chow ring of the grassmannian. This dimension condition is satisfied for all

$$d \in \{13,\ \dots,\ 40\} \setminus \{17,\ 18,\ 31,\ 32,\ 33,\ 34\}.$$

For $d \in \{17,\ 18\}$ the subcritical exponent has been showed to be high in [6, §5 and §6] by an argument specific to the low dimension.

It is shown below that the subcritical exponent is high for $d \in \{31,\ 32\}$. In fact, by Remark 4.11, the case $d = 31$ is a consequence of the case $d = 32$; the proof for $d = 31$ is included because it is simpler than the proof for $d = 32$.

It is also shown below that the subcritical exponent is low for $d = 33$; therefore, by Remark 4.11, it is low for $d = 34$ as well. □

The case of $d = 31$. The dimension $d = 31$ is of the form $d = 2n + 1$ with $n = 15$. By [16], the corresponding Totaro's number t is 9 so that $n - (t - 1) = 7$. By Theorem 4.4, to show that the subcritical exponent i(8) is high, it suffices to show that

$$2f_7(e_1) \text{ vanishes in } \tilde{C}_{15}/2\tilde{C}_{15}. \tag{5.2}$$

For this, by Lemma 4.6, it suffices to verify the vanishing of $2cf_7(e_1)$, where $c := c_1 \dots c_7$.

Recall that $2f_7(e_1)$ is a linear combination of $s^{(k)}(c_1)$, $k \in \mathbb{N}$, with coefficients in $\mathbb{Z}[x_1, \dots, x_7]$, where the coefficient at $s^{(k)}(c_1)$ is the divided by $2^{b(k)-1}$ coefficient at x^k of the polynomial $f_7(x) \in (\mathbb{Z}[x_1, \dots, x_7])[x]$. By Lemma 1.2, since c_i^2 is 0 modulo 2, the product $cs^{(k)}(c_1)$ vanishes in $\tilde{C}_{15}/2\tilde{C}_{15}$ for $k \neq 8$. Moreover, the image of $cs^{(8)}(c_1)$ is cc_8.

Let $a \in (\mathbb{Z}/2\mathbb{Z})[x_1, \dots, x_7]$ be the coefficient modulo 2 of $f_7(x)$ at x^8. This is a homogeneous polynomial of degree $2^7 - 8 = 120$. By Lemma 2.3, the variables $x_1, \dots, x_7$ appear in a with 2-power exponents only. Since $16 \cdot 7 < 120$, every monomial contains at least one variable x_i with an exponent ≥ 32 and therefore vanishes in $\tilde{C}_{15}/2\tilde{C}_{15}$ because

$$\xi_i^{30} = (\xi_i^{15})^2 = (c_1\xi_i^{14} - c_2\xi_i^{13} + \dots - c_{14}\xi_i + c_{15})^2 \equiv 0 \text{ modulo } 2$$

by (4.2). We conclude that the image of $cs^{(8)}(c_1) \cdot a$ in $\tilde{C}_{15}/2\tilde{C}_{15}$ vanishes. This implies (5.2) and therefore shows that the subcritical exponent in dimension $d = 31$ is high. □

The case of $d = 32$. The dimension $d = 32$ is of the form $d = 2n$ with $n = 16$. By [16], the corresponding Totaro's number t is 9 so that $n - (t - 1) = 8$. By Theorem 4.7, to show that the subcritical exponent i(8) is high, it suffices to show that the image of $f_8^{\text{even}}(e_1) + f_8^{\text{odd}}(e_1)$ in $\tilde{C}_{16}/2\tilde{C}_{16}$ multiplied by $\xi := \xi_9 \dots \xi_{16}$ vanishes. For this, by Lemma 4.6, it suffices to prove vanishing of

$$\text{the image of } f(e_1) \cdot c \text{ in } \tilde{C}_{16}/2\tilde{C}_{16} \text{ multiplied by } \xi, \tag{5.3}$$

where $c := c_1 \dots c_8$ and $f = f(x) := f_8^{\text{even}}(x) + f_8^{\text{odd}}(x)$.

The element $f(e_1)$ is a linear combination of $s^{(k)}(c_1)$, $k \geq 0$, with coefficients in $\mathbb{Z}[x_1, \dots, x_8]$, where the coefficient a_k at $s^{(k)}(c_1)$ is the divided by $2^{b(k)}$ coefficient at x^k of the polynomial $f(x) \in (\mathbb{Z}[x_1, \dots, x_8])[x]$. (Here for $k = 0$ we have $s^{(k)}(c_1) := 1$ and $b(k) = 0$.) By Lemma 1.2, the product $cs^{(k)}(c_1)$ vanishes in $\tilde{C}_{16}/2\tilde{C}_{16}$ for all $k \in \mathbb{N}\backslash\{0,\ 16\}$. So, to conclude, we need information on $a_{16}, a_0 \in (\mathbb{Z}/2\mathbb{Z})[x_1, \dots, x_8]$, where a_{16} is the modulo 2 one half of the coefficient at x^{16} for the polynomial $f(x)$, and a_0 is the modulo 2 constant term of $f(x)$.

Note that, since the image of $cs^{(16)}(c_1)$ is cc_{16} by Lemma 1.2, any divisible by $x_1 \dots x_8$ monomial in a_{16} will not contribute to the value of (5.3) because $(\xi_1 \dots \xi_8) \cdot \xi \cdot c_{16} = c_{16}^2 = 0$ in $\tilde{C}_{16}$. Therefore we do not need to care about such monomials. Besides, a monomial containing a variable in a power ≥ 32 will not contribute because

$$\xi_i^{32} = (\xi_i^{16})^2 = (c_1\xi_i^{15} - c_2\xi_i^{14} + \dots + c_{15}\xi_i - c_{16})^2 \equiv 0 \text{ modulo } 2 \tag{5.4}$$

by (4.2).

Substituting $-x_1$ for x_1 and then $x - x_1$ for x, one transforms the polynomial $f_8^{\text{even}}(x)$ to $f_8^{\text{odd}}(x)$. Therefore the monomials in a_{16} without x_1 are exactly the same as the monomials in the modulo 2 coefficient a'_{16} at x^{16} in $f_8^{\mathrm{even}}(x)$. Substituting 0 for x_8, one transforms $f_8^{\mathrm{even}}(x)$ to $f_7(x)$. By Lemma 5.5 below, the modulo 2 coefficient at x^{16} for $f_7(x)$ contains the monomial $(x_1\dots x_7)^{16}$. Therefore, a'_{16} also contains the monomial $(x_1\dots x_7)^{16}$. By symmetry in $x_1,\dots,x_8$ of f_8^{even}, we conclude that a'_{16} contains the monomial $(x_2\dots x_8)^{16}$ and so, a_{16} also contains this monomial. By symmetry, we conclude that a_{16} contains all the 8 monomials of the sum

$$\sum_{i=1}^{8}(x_1\dots x_8/x_i)^{16}.$$

Moreover, these are the only "important" monomials of a_{16}: any other is divisible by $x_1\dots x_8$ or contains a variable in a power ≥ 32 and therefore does not contribute to the value of (5.3). So, taking (4.2) with $n=16$ into account along with the relations $c_i^2=0$, we see that the contribution of a_{16} to (5.3) equals

$$c_1\dots c_8c_{16}\xi\sum_{i=1}^{8}(\xi_1\dots\xi_8/\xi_i)^{16}=c_1\dots c_{16}\sum_\sigma \xi_{\sigma(1)}\xi_{\sigma(2)}^2\dots\xi_{\sigma(7)}^7\xi,$$

where σ runs over all the 8! embeddings $\{1\dots,7\}\hookrightarrow\{1,\dots,8\}$.

As to a_0, note that it coincides with the modulo 2 constant term of $f_8^{\mathrm{odd}}(x)$. In particular, the variables appear in a_0 with 2-power exponents only. Any monomial other than $(x_1\dots x_8)^{16}$ therefore contains at least one variable in a power at least 32 and does not contribute to (5.3). The monomial $(x_1\dots x_8)^{16}$ is present: it appears in $(xx_2\dots x_8)^{16}$ after the substitution of x by $x-x_1$ and, as we already know, $(xx_2\dots x_8)^{16}$ appears in $f_8^{\mathrm{even}}(x)$ whereas $f_8^{\mathrm{odd}}(x)\equiv f_8^{\mathrm{even}}(x-x_1)\pmod 2$. It follows that the contribution to (5.3) of a_0 coincides with the contribution of a_{16} and so, both contributions cancel each other. □

The case of $d=33$. The dimension $d=33$ is of the form $d=2n+1$ with $n=16$. By [16], the corresponding Totaro's number t is 10 so that $n-(t-1)=7$. By Theorem 4.4, to show that the subcritical exponent i(9) is low, it suffices to show that $2f_7(e_1)$ does not vanish in $\tilde C_{16}/2\tilde C_{16}$. To get this, we prove a stronger statement: $2cf_7(e_1)$ does not vanish, where $c:=c_1c_2\dots c_8$.

Recall that $2f_7(e_1)$ is a linear combination of $s^{(k)}(c_1)$, $k\in\mathbb{N}$, with coefficients in $\mathbb{Z}[x_1,\dots,x_7]$, where the coefficient at $s^{(k)}(c_1)$ is the divided by $2^{b(k)-1}$ coefficient at x^k of the polynomial $f_7(x)\in(\mathbb{Z}[x_1,\dots,x_7])[x]$. By Lemma 1.2, the product $cs^{(k)}(c_1)$ vanishes in $\tilde C_{16}/2\tilde C_{16}$ for $k\neq 16$. Moreover, the image of $cs^{(16)}(c_1)$ is cc_{16}.

Let $a\in(\mathbb{Z}/2\mathbb{Z})[x_1,\dots,x_7]$ be the coefficient modulo 2 of $f_7(x)$ at x^{16}. This is a homogeneous polynomial of degree $2^7-16=112=16\cdot 7$. By Lemma 2.3, the variables $x_1,\dots,x_7$ appear in a with 2-power exponents only. By Lemma 5.5 below, the monomial $(x_1\dots x_7)^{16}$ is present. Any other monomial contains at least one variable x_i with an exponent ≥ 32 and therefore vanishes in $\tilde C_{16}/2\tilde C_{16}$ by (5.4). Using the relation

$$\xi_i^{16}=c_1\xi_i^{15}-c_2\xi_i^{14}+\dots+c_{15}\xi_i-c_{16},$$

we conclude that the image of $cs^{(16)}(c_1)\cdot a$ in $\tilde C_{16}/2\tilde C_{16}$ equals

$$c_1c_2\dots c_{15}c_{16}\cdot\sum_\sigma\xi_{\sigma(1)}\xi_{\sigma(2)}^2\dots\xi_{\sigma(7)}^7,$$

where σ runs over the 7! permutations of the set $\{1,\dots,7\}$. The result is nonzero because the summands of the sum are basis elements from (4.1). □

Here is the computation used in the above proof:

Lemma 5.5. *The polynomial f_7, viewed modulo 2 and as a polynomial in $x, x_1, \dots, x_7$, contains the monomial $\mu := (xx_1 \dots x_7)^{16}$.*

Proof. The congruence of Lemma 2.3 with $l = 6$ tells us that $f_7(x)$ modulo 2 contains μ if (and only if) $f_6(x)f_6(x_7)$ modulo 2 contains μ. The latter condition holds if (and only if) the square a^2 of the modulo 2 coefficient $a \in (\mathbb{Z}/2\mathbb{Z})[x_1, \dots, x_6]$ at x^{16} in $f_6(x)$ contains $(x_1 \dots x_6)^{16}$, or, equivalently, a contains $(x_1 \dots x_6)^8$. A direct computer verification shows that the very last condition is satisfied. □

Acknowledgements. I thanks an anonymous referee for extraordinarily careful reading and valuable suggestions.

References

[1] Buch, A. S., Kresch, A., and Tamvakis, H. Quantum Pieri rules for isotropic Grassmannians. *Invent. Math. 178*, 2 (2009), 345–405.

[2] Devyatov, R. A., Karpenko, N. A., and Merkurjev, A. S. Maximal indexes of flag varieties for spin groups. *Forum Math. Sigma 9* (2021), Paper No. e34, 12.

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

[4] Karpenko, N. A. On generic quadratic forms. *Pacific J. Math. 297*, 2 (2018), 367–380.

[5] Karpenko, N. A. On classifying spaces of spin groups. *Results Math. 77*, 4 (2022), Paper No. 144, 8 pages.

[6] Karpenko, N. A. On generic flag varieties for odd spin groups. *Publ. Mat. 67*, 2 (2023), 743–756.

[7] Karpenko, N. A. On Spin(2023)-torsors. *New York J. Math. 30* (2024), 550–560.

[8] Karpenko, N. A. Finite extensions partially splitting PGO-torsors. *Math. Res. Lett. 32*, 2 (2025), 427–455. With an appendix by Alexander S. Merkurjev.

[9] Karpenko, N. A. On characteristic classes modulo torsion for spin groups. *J. Algebra Appl. 24*, 10 (2025), 2550236 (15 pages).

[10] Karpenko, N. A. On isotropy fields of Spin(18)-torsors. *St. Petersburg Math. J. 36*, 1 (2025), 115–120.

[11] Karpenko, N. A. On special Clifford groups and their characteristic classes. *Ric. Mat. 74*, 1 (2025), 449–470.

[12] Karpenko, N. A., and Merkurjev, A. S. Canonical p-dimension of algebraic groups. *Adv. Math. 205*, 2 (2006), 410–433.

[13] Karpenko, N. A., and Merkurjev, A. S. Indexes of generic Grassmannians for spin groups. *Proc. Lond. Math. Soc. (3) 125*, 4 (2022), 825–840.

[14] Karpenko, N. A., and Merkurjev, A. S. Poincaré duality for tautological Chern subrings of orthogonal grassmannians. *Math. Scand. 128*, 2 (2022), 221–228.

[15] Ofek, D. Reduction of structure to parabolic subgroups. *Doc. Math. 27* (2022), 1421–1446 (electronic).

[16] Totaro, B. The torsion index of the spin groups. *Duke Math. J. 129*, 2 (2005), 249–290.

Mathematical & Statistical Sciences, University of Alberta, Edmonton, CANADA
Email address: karpenko@ualberta.ca
URL: www.ualberta.ca/~karpenko