The torsion index of the spin groups

Burt Totaro

The torsion index is a positive integer associated by Grothendieck to any connected compact Lie group G [10]. As explained in section 1, knowing the torsion index of a group has direct consequences for the abelian subgroups of G, the integral cohomology of the classifying space, the complex cobordism of the classifying space, the Chow ring of the classifying space [26], and the classification of G-torsors over fields [24]. Demazure [5], Marlin [14], and Tits [25] have given upper bounds for the torsion index. In this paper, we compute the torsion index exactly for all the spin groups $Spin(n)$. In another paper, we will compute the torsion index of the exceptional group E_8. As discussed below, this completes the calculation of the torsion index for all the simply connected simple groups. The topology of the spin groups becomes more and more complicated as the dimension increases, and so it was not at all clear that it would be possible to do the calculation in all dimensions. Indeed, the answer is rather intricate, and the proof in high dimensions requires some deep information from analytic number theory, Bauer and Bennett's theorem on the binary expansion of $\sqrt{2}$ [1].

Theorem 0.1 *Let l be a nonnegative integer. The groups $Spin(2l+1)$ and $Spin(2l+2)$ have the same torsion index, of the form $2^{u(l)}$. For all l, $u(l)$ is either*

$$l - \left\lfloor \log_2 \left(\binom{l+1}{2} + 1 \right) \right\rfloor$$

or that expression plus 1. The second case arises only for certain numbers l (initially: $l = 8, 16, 32, 33, \ldots$) which are equal to or slightly larger than a power of 2. Precisely, the second case arises if and only if $l = 2^e + b$ for some nonnegative integers e, b such that $2b - u(b) \leq e - 3$.

This is an inductive description of $u(l)$, in that to compute $u(l)$ we may need to determine $u(b)$ where b is as above; but that is no problem, since b will be much smaller than l. Roughly, what Theorem 0.1 says is that $u(l)$ is very close to $l - 2\log_2 l$. For the reader's convenience, we list the torsion index of $Spin(n)$ for $n \leq 38$ in the following table, thanks to Theorem 0.1. Equivalently, we list $u(l)$ for $l \leq 18$. In this range, $u(l)$ increases in a somewhat irregular fashion.

l	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$u(l)$	0	0	0	1	1	1	2	3	4	4	5	5	6	7	8	9	10	10	11

I now recall the definition of the torsion index. Let T be a maximal torus in a compact Lie group G, and let N be the complex dimension of the flag manifold G/T. Each character of the torus T determines a complex line bundle on G/T.

Consider the subring of the integral cohomology of G/T generated by the Chern classes in $H^2(G/T, \mathbf{Z})$ of these line bundles. For G simply connected, this subring is simply the subring generated by $H^2(G/T, \mathbf{Z})$. Then the *torsion index* of G is defined as the smallest positive integer $t(G)$ such that $t(G)$ times the class of a point in $H^{2N}(G/T, \mathbf{Z}) \cong \mathbf{Z}$ belongs to this subring.

The prime numbers p dividing the torsion index of G are precisely those such that the integral cohomology of the classifying space BG has p-torsion, or equivalently those such that the integral cohomology of G itself has p-torsion. These "torsion primes" are known for all compact Lie groups, the final answer being given by Borel in 1961 [4]: they are the primes dividing the order of the torsion subgroup of the fundamental group of G, together with 2 if the universal cover of G has a simple factor of type $Spin(n)$ for $n \geq 7$ or G_2, 2 and 3 in the cases F_4, E_6, and E_7, and 2, 3, and 5 in the case E_8.

In particular, the groups $SU(n)$ and the symplectic groups have torsion index 1. Furthermore, the torsion index has been known for all but one of the simply connected exceptional groups, by Tits ([25], Proposition 2): $t(G_2) = 2$, $t(F_4) = 2 \cdot 3$, $t(E_6) = 2 \cdot 3$, and $t(E_7) = 2^2 \cdot 3$. I will show in another paper that the remaining exceptional group E_8 has torsion index $2^6 \cdot 3^2 \cdot 5$. I showed in an earlier paper, [27], that every E_8-torsor over a field splits over a field extension of degree dividing $2^6 \cdot 3^2 \cdot 5$; the calculation of the torsion index shows that this number is optimal, by Grothendieck's theorem (Theorem 1.1). With this paper's computation for the spin groups, the torsion index is now known for all simply connected compact Lie groups. (It is easy to check that $t(G \times H) = t(G)t(H)$.)

Marlin proved in 1974 that the torsion indices of $SO(2l+1)$ and $SO(2l+2)$ both divide 2^l [14]. These are in fact equalities, as follows from a result of Merkurjev ([15], 4.2 and 4.4). Later, Reichstein and Youssin gave an elegant proof ([22], 5.2), discussed in section 1, and we also give a direct topological proof after Lemma 3.1. The spin groups are more difficult. Marlin gave a reasonable upper bound: the torsion indices of $Spin(2l+1)$ and $Spin(2l+2)$ both divide $2^{l-\lfloor \log_2 l \rfloor - 1}$. Marlin's bound first fails to be an equality for the groups $Spin(11)$ and $Spin(12)$, which have torsion index 2^1 rather than 2^2. This was observed by Serre and Tits ([25], Proposition 2), as a consequence of the deep properties of 12-dimensional quadratic forms proved by Pfister: any 12-dimensional quadratic form over a field which lies in the ideal I^3 of the Witt ring can be split (made hyperbolic) by a quadratic extension of the field ([20], pp. 123-124).

We will determine the torsion index of $Spin(n)$ exactly for all n. Equivalently, for any l, by Grothendieck's theorem on the torsion index (Theorem 1.1 below), we determine the smallest power of 2, $t(Spin(2l+2)) = 2^{u(l)}$, such that every $(2l+2)$-dimensional quadratic form over a field which lies in the ideal I^3 of the Witt ring can be split by a field extension of degree an odd multiple of 2^i for some $i \leq u(l)$. (What our calculation says about odd-dimensional quadratic forms is that any $(2l+1)$-dimensional form which is a codimension-1 subform of some form in I^3 can be split by a field extension of degree an odd multiple of 2^i for some $i \leq u(l)$. Here we say that a form of odd dimension $2l+1$ is split if it contains an isotropic subspace of dimension l.) A rather vast problem suggested by this work would be to deduce this statement from more precise information on quadratic forms in I^3 of any given dimension, generalizing Pfister's results on 12-dimensional forms. In particular, can every form of dimension $2l+2$ in I^3 be split by a field extension

of degree 2^i for some $i \leq u(l)$ (that is, without the odd factor)? This is a special case of Question 0.2 in [27] for torsors. Note that, in the more general situation of homogeneous varieties, Question 0.2 has been answered negatively by Florence [6] and Parimala [19].

Another natural problem in this direction was suggested by the referee. For any quadratic form q over a field, let $n(q)$ be the greatest common divisor of the degrees of the finite extensions of k which split q. Then, for any $m \geq 2$ and any even number d, we can ask for the maximum value of $n(q)$, as q ranges over all quadratic forms over all fields such that q has dimension d and belongs to the ideal I^m of the Witt ring. For $m = 2$ and $m = 3$, this number is the torsion index of $SO(d)$ and $Spin(d)$, respectively, and so the answer is given by Theorems 3.2 and 0.1.

I would like to thank Alan Baker and Alexander Vishik for useful discussions. The referee helped a lot with the exposition.

Contents

1 Applications of the torsion index

In this section we explain several applications of the torsion index, for any compact connected Lie group. These results indicate why the torsion index is worth computing.

First, we state Grothendieck's theorem relating the torsion index to the classification of G-torsors over fields ([10], Theorem 2). Let k be any field, and let G_k denote the split reductive group over k which corresponds to the compact Lie group G. By definition, a G_k-torsor is a variety over k with a free G_k-action such that the quotient variety is Spec k; a G_k-torsor is called trivial if it is isomorphic to G_k, or equivalently if it has a k-rational point ([24], section 1). For any G_k-torsor E over a field k, let $n(E)$ be the greatest common divisor of the degrees of all finite field extensions l of k such that E becomes trivial over l.

Theorem 1.1 *(Grothendieck) For any compact connected Lie group G, any field k, and any G_k-torsor E over k, the number $n(E)$ divides the torsion index $t(G)$. Moreover, there is a G_F-torsor E over some extension field F of k such that $n(E)$ is equal to $t(G)$.*

Actually, this is a slight extension of Grothendieck's statement. For example, he assumes that the base field is algebraically closed. But the proof works in this generality. The proof produces an explicit G_F-torsor E with $n(E) = t(G)$: the natural torsor over the function field F of $GL(n)/G_k$, for any embedding of G_k into $GL(n)$ over k. It follows that any versal torsor E has $n(E) = t(G)$; a reference for the notion of versal torsors is Garibaldi-Merkurjev-Serre ([9], section 5). Grothendieck's theorem justifies the definition of the torsion index: the torsion index measures exactly how complicated G-torsors over fields can be.

Next, we state Reichstein and Youssin's theorem which relates the torsion index to the classification of abelian subgroups of a compact Lie group ([22], 4.8).

Theorem 1.2 *Let G be a compact connected Lie group. Then any abelian p-subgroup of G has a subgroup of index dividing the torsion index $t(G)$ which is contained in a maximal torus of G.*

For example, as Reichstein and Youssin observed, this theorem implies easily that Marlin's upper bound 2^l for the torsion index of $SO(2l+1)$ is an equality (and likewise for $SO(2l+2)$) ([22], 5.2). We simply note that $SO(2l+1)$ contains a subgroup isomorphic to $(\mathbf{Z}/2)^{2l}$, the group of diagonal matrices of ± 1's with determinant 1. A maximal torus of $SO(2l+1)$ has rank only l, so any subgroup of $(\mathbf{Z}/2)^{2l}$ contained in a torus must have index a multiple of 2^l. By Theorem 1.2, it follows that the torsion index of $SO(2l+1)$ is a multiple of 2^l, and hence is equal to 2^l.

One could try to use abelian subgroups of the spin groups in the same way to give a lower bound for the torsion index, but it seems difficult. Wood observed that the abelian subgroups of the spin groups are related to linear codes over $\mathbf{F}_2$ and are therefore hard to classify in general [28].

The torsion index also has implications about the Chow ring, or more generally the motivic cohomology, of BG. As above, let k be any field, and let G_k denote the split reductive group over k which corresponds to the compact Lie group G. I defined the Chow ring of the classifying space BG_k [26]. Namely, $CH^i(BG_k)$ is defined as $CH^i(U/G_k)$ for any Zariski open set U in a representation V of G_k such that $V - U$ has codimension greater than i and the quotient variety U/G_k exists; this group is independent of the choice of V and U. Morel and Voevodsky independently defined BG_k as an object in their A^1-homotopy category (they call it $B_{\text{et}}G_k$) ([17], section 4.2), and it is easy to see that their definition leads to the same ring $CH^*(BG_k)$. Let T_k denote a split maximal torus in G_k, and define the Weyl group $W = N(T_k)/T_k$, as usual.

Theorem 1.3 *(1) For all $i \geq 0$, the kernel and cokernel of the homomorphism*

$$CH^i BG_k \to (CH^i BT_k)^W$$

are killed by the torsion index $t(G)$.

(2) For all $i \geq 0$, the kernel and cokernel of

$$H^i(BG, \mathbf{Z}) \to H^i(BT, \mathbf{Z})^W$$

are killed by $t(G)$.

(3) For all $i \geq 0$, the kernel and cokernel of the natural map

$$CH^i BG_{\mathbf{C}} \to H^{2i}(BG, \mathbf{Z})$$

are killed by $t(G)$.

Since $CH^* BT_k$ and $H^*(BT, \mathbf{Z})$ are torsion-free, the statements about the kernels in (1) and (2) imply, in particular, that the torsion subgroups in both $CH^* BG_k$ and $H^*(BG, \mathbf{Z})$ are killed by the torsion index $t(G)$.

Proof. Let B_k be a Borel subgroup containing T_k, and consider the fibration

$$G_k/B_k \to BB_k \to BG_k.$$

To be precise, $CH^i BG_k$ is defined as $CH^i(U/G_k)$ for certain finite-dimensional smooth varieties U with free G_k-action, and the argument that follows can be formulated in terms of the smooth proper morphism $U/B_k \to U/G_k$, whose fibers are isomorphic to G_k/B_k.

The Chow ring of BB_k is isomorphic to that of BT_k, which is the polynomial ring over $\mathbf{Z}$ generated by $CH^1 BT_k$, the group of characters of T_k. We can identify the Chow ring of G_k/B_k with the cohomology ring of the analogous flag manifold over the complex numbers, $G_{\mathbf{C}}/B_{\mathbf{C}} = G/T$. Let N be the dimension of G_k/B_k. By definition of the torsion index $t(G)$, there is an element $a \in CH^N(BB_k)$ which restricts to $t(G)$ times the class of a point in $CH^N(G_k/B_k) \cong \mathbf{Z}$. Equivalently, the pushforward map $f_* : CH^i BB_k \to CH^{i-N} BG_k$ (which is actually defined using the smooth proper morphism $f : U/B_k \to U/G_k$) has

$$f_*(a) = t(G) \in CH^0(BG_k) \cong \mathbf{Z}.$$

Define a homomorphism $\alpha : CH^i BB_k \to CH^i BG_k$ by

$$\alpha(x) = f_*(ax).$$

For any element x in $CH^i BG_k$, we have

$$\begin{aligned} \alpha f^* x &= f_*(a f^* x) \\ &= (f_* a)x \\ &= t(G)x. \end{aligned}$$

Therefore the kernel of f^* is killed by $t(G)$, as we want.

Next, we observe that for any x in $CH^i BG_k$, we have

$$\begin{aligned} f^* \alpha f^* x &= f^*(t(G)x) \\ &= t(G) f^* x. \end{aligned}$$

Thus $f^* \alpha(y) = t(G)y$ for all y in the image of $f^* : CH^i(BG_k) \to CH^i(BB_k) = CH^i(BT_k)$. We know that the representation ring $\mathrm{Rep}(G_k)$ restricts isomorphically

to $\mathrm{Rep}(T_k)^W$. Therefore, by taking Chern characters of representations, we see that $CH^*(BG_k) \otimes \mathbf{Q}$ maps onto $(CH^*(BT_k) \otimes \mathbf{Q})^W$. Therefore, we have

$$f^*\alpha(y) = t(G)y$$

for all $y \in (CH^i(BT_k) \otimes \mathbf{Q})^W$. Since the abelian group $CH^i(BT_k)$ is torsion-free, it follows that

$$f^*\alpha(y) = t(G)y$$

in $CH^i(BT_k)^W$ for all $y \in (CH^i BT_k)^W$. Therefore the cokernel of $f^* : CH^i BG_k \to CH^i(BT_k)^W$ is killed by the torsion index $t(G)$, and (1) is proved.

Statement (2) is proved by exactly the same argument. Finally, we prove (3), saying that the kernel and cokernel of the natural map

$$CH^*BG_{\mathbf{C}} \to H^*(BG, \mathbf{Z})$$

are killed by $t(G)$. This is clear for the kernel, by part (1), using that the natural map from $CH^*BT_{\mathbf{C}}$ to $H^*(BT, \mathbf{Z})$ is an isomorphism. As for the cokernel, let x be any element of $H^*(BG, \mathbf{Z})$. By the proof of (2), we have $\alpha f^*x = t(G)x$ in $H^*(BG, \mathbf{Z})$. But f^*x lies in $H^*(BT, \mathbf{Z})^W = CH^*(BT_{\mathbf{C}})^W$, and so αf^*x is the image of a class in $CH^*BG_{\mathbf{C}}$. Thus $t(G)x$ is the image of a class in $CH^*BG_{\mathbf{C}}$, and (3) is proved. QED

Corollary 1.4 *For any compact connected Lie group G, the image of the natural homomorphism from complex cobordism to ordinary cohomology*

$$MU^iBG \to H^i(BG, \mathbf{Z})$$

contains $t(G)H^i(BG, \mathbf{Z})$.

Proof. This could be proved along the same lines as Theorem 1.3, but it also follows from Theorem 1.3. Namely, I constructed a natural factorization of the cycle map,

$$CH^*BG_{\mathbf{C}} \to MU^*BG \otimes_{MU^*} \mathbf{Z} \to H^*(BG, \mathbf{Z}),$$

in [26]. Since $t(G)$ times any element of $H^*(BG, \mathbf{Z})$ is in the image of $CH^*BG_{\mathbf{C}}$, it follows that $t(G)$ times any element of $H^*(BG, \mathbf{Z})$ is also in the image of MU^*BG. QED

In the case of the spin groups, our calculation of the torsion index does not give any new information about the ordinary cohomology of $BSpin(n)$. Quillen computed the cohomology of $BSpin(n)$ with $\mathbf{Z}/2$ coefficients [21], Kono computed the integral cohomology of $BSpin(n)$ additively and found that the torsion subgroup is killed by 2 [12], and Benson and Wood showed that the cokernel of the homomorphism

$$H^*(BSpin(n), \mathbf{Z}) \to H^*(BT, \mathbf{Z})^W$$

is killed by 2 [2]. In fact, this homomorphism fails to be surjective only when n is at least 6 and is congruent to 3, 4, or 5 modulo 8.

On the other hand, knowing the torsion index of the spin groups does give new information about the complex cobordism of $BSpin(n)$. The Brown-Peterson cohomology at the prime 2 (essentially equivalent to complex cobordism) has been

computed by Kono and Yagita for $BSpin(n)$ with $n \leq 10$ ([13], section 6), and by Kitchloo, Laures, and Wilson for the limiting space $BSpin$ ([11], Theorem 1.11). In general, one knows that Chern classes of complex representations of $Spin(n)$ give elements of the cohomology of $BSpin(n)$ which are in the image of complex cobordism, but Corollary 1.4 produces elements of $MU^*BSpin(n)$ which are in general not polynomials in Chern classes.

2 A first reduction of the problem

Computing the torsion index of a compact Lie group is, by definition, a problem about the integral cohomology ring of the flag manifold G/T. In this section, we show that the problem can be formulated in terms of any homogeneous space G/H such that H is a subgroup of maximal rank with torsion-free cohomology. This is a convenient simplification. More precisely, to compute the p-part of the torsion index of G, for a given prime number p, it suffices to consider any homogeneous space G/H such that H is a subgroup of maximal rank with p-torsion-free cohomology.

Lemma 2.1 *Let G be a compact connected Lie group, p a prime number, and H a closed connected subgroup of maximal rank in G such that p does not divide the torsion index of H. Then the $\mathbf{Z}_{(p)}$-cohomology of G/H is torsion-free and concentrated in even dimensions, and the p-part of the torsion index of G is equal to the index in the top degree of the image of $H^*(BH, \mathbf{Z}_{(p)})$ in the ring $H^*(G/H, \mathbf{Z}_{(p)})$.*

When H is a maximal torus, the lemma is precisely the definition of the torsion index of G.

Proof. Since p does not divide the torsion index of H, the ring $H^*(BH, \mathbf{Z}_{(p)})$ is torsion-free and concentrated in even dimensions, by Theorem 1.3 (2). Let T be a maximal torus of H, and hence of G. We know that $H^*(H/T, \mathbf{Z})$ is torsion-free and concentrated in even dimensions. Therefore the spectral sequence of the fibration $H/T \to BT \to BH$ degenerates in $\mathbf{Z}_{(p)}$-cohomology. So there are homogeneous elements $a_1, \ldots, a_n$ in $H^*(BT, \mathbf{Z}_{(p)})$, say in dimensions $|a_1| \leq \cdots \leq |a_n|$, which restrict to a basis for $H^*(H/T, \mathbf{Z}_{(p)})$ as a free $\mathbf{Z}_{(p)}$-module. It follows that $a_1, \ldots, a_n$ form a basis for $H^*(BT, \mathbf{Z}_{(p)})$ as a free $H^*(BH, \mathbf{Z}_{(p)})$-module. Also, in the fibration $H/T \to G/T \to G/H$, we can restrict the elements $a_1, \ldots, a_n$ to $H^*(G/T, \mathbf{Z}_{(p)})$, where they again restrict to a basis for $H^*(H/T, \mathbf{Z}_{(p)})$ as a free $\mathbf{Z}_{(p)}$-module. So this spectral sequence also degenerates, and $a_1, \ldots, a_n$ form a basis for $H^*(G/T, \mathbf{Z}_{(p)})$ as a free $H^*(G/H, \mathbf{Z}_{(p)})$-module. In particular, the $\mathbf{Z}_{(p)}$-cohomology of G/H is torsion-free and concentrated in even dimensions, since G/T has these properties.

The highest-dimensional element a_n must restrict to a basis element for the $\mathbf{Z}_{(p)}$-cohomology of H/T in the top dimension, and so the top-dimensional $\mathbf{Z}_{(p)}$-cohomology group of G/T must be equal to a_n times the top-dimensional $\mathbf{Z}_{(p)}$-cohomology group of G/H.

We first show that the p-part of the torsion index of G divides the index in the top dimension of the image of $H^*(BH, \mathbf{Z}_{(p)})$ in $H^*(G/H, \mathbf{Z}_{(p)})$. Let x be any element of $H^*(BH, \mathbf{Z}_{(p)})$ which restricts to an element of p-adic order r in the top-dimensional cohomology group of G/H. Then $a_n x$ in $H^*(BT, \mathbf{Z}_{(p)})$ restricts to an element of p-adic order r in the top-dimensional cohomology group of G/T. That is, the p-adic order of the torsion index of G is at most r, as we want.

We now prove the converse. Let r be the p-adic order of the torsion index of G. Then there is an element y of $H^*(BT, \mathbf{Z}_{(p)})$ which restricts to a top-dimensional element of $H^*(G/T, \mathbf{Z}_{(p)})$ of p-adic order r. We can write $y = \sum_{i=1}^{n} a_i x_i$ for some elements x_i of $H^*(BH, \mathbf{Z}_{(p)})$. Here only $a_n x_n$ can have nonzero restriction to the top dimension of $H^*(G/T, \mathbf{Z}_{(p)})$, as the elements x_i with $i < n$ restrict to 0 in $H^*(G/H, \mathbf{Z}_{(p)})$ for dimension reasons. So $a_n x_n$ restricts to a top-dimensional element in the cohomology of G/T which has p-adic order r. Therefore x_n restricts to a top-dimensional element in the cohomology of G/H which has p-adic order r. Thus, the index in the top dimension of the image of $H^*(BH, \mathbf{Z}_{(p)})$ in $H^*(G/H, \mathbf{Z}_{(p)})$ divides the p-part of the torsion index of G. QED

3 The spin groups

In this section, we spell out what Lemma 2.1 says about the torsion index of the spin groups. The same lemma leads to an easy calculation of the torsion index of the groups $SO(n)$. We also present some elementary upper bounds for the torsion index of the spin groups, which suffice to compute it for $Spin(n)$ with $n \leq 12$. These upper bounds are not needed for our general calculation, however.

The torsion index of $Spin(n)$ is defined in terms of the integral cohomology ring of the isotropic flag manifold $Spin(n)/T = SO(n)/T_{SO}$. But the following lemma expresses the torsion index of the spin groups in terms of the cohomology ring of a simpler manifold, the isotropic Grassmannian $SO(2l+1)/U(l) = SO(2l+2)/U(l+1)$. This cohomology ring is ([16], III.6.11):

$$A = H^*(SO(2l+1)/U(l), \mathbf{Z}) \cong \mathbf{Z}[e_1, \ldots, e_l]/(e_i^2 - 2e_{i-1}e_{i+1} + 2e_{i-2}e_{i+2} - \cdots + (-1)^i e_{2i} = 0),$$

where the Chern classes c_j in $H^*BU(l)$ restrict to $2e_j$. Here we understand e_j to mean 0 for $j > l$. The element e_j is in H^{2j}, but for convenience we view A as a graded ring with e_j in degree j.

Lemma 3.1 *For any $l \geq 1$, the groups $Spin(2l+1)$ and $Spin(2l+2)$ have the same torsion index. To compute it, consider all products in the ring A, of the top degree $\binom{l+1}{2}$, of a power of e_1 times a set of distinct elements $2e_i$ with $i \geq 2$. Any such product is equal to some integer multiple of $e_1 \cdots e_l$ in the ring A. The torsion index of $Spin(2l+1)$ and of $Spin(2l+2)$ is the greatest common divisor of the integers so obtained.*

Proof. We consider $Spin(2l+1)$ first. Let $\widetilde{U(l)}$ be the inverse image of $U(l) \subset SO(2l+1)$ in the double cover $Spin(2l+1)$. The derived subgroup of $\widetilde{U(l)}$ is $SU(l)$, and so we have a fibration $BSU(l) \to B\widetilde{U(l)} \to BS^1$. It follows that the cohomology of $B\widetilde{U(l)}$ is torsion-free and concentrated in even degrees, or equivalently that $\widetilde{U(l)}$ has torsion index 1. More precisely, using the fibration, we check easily that the integral cohomology of $H^*(B\widetilde{U(l)}, \mathbf{Z})$ is the polynomial ring generated by $c_1/2$ and $c_2, \ldots, c_l$, where the Chern classes c_i are the standard generators of $H^*(BU(l), \mathbf{Z})$.

By Lemma 2.1, the torsion index of $Spin(2l+1)$ is equal to the index in the top dimension of the image of $H^*(B\widetilde{U(l)}, \mathbf{Z})$ in $H^*(Spin(2l+1)/\widetilde{U(l)}, \mathbf{Z}) = H^*(SO(2l+1)/U(l), \mathbf{Z})$. Equivalently, this is the subring generated by e_1 and $2e_2, \ldots, 2e_l$. It

suffices to consider the product of a power of e_1 with some distinct elements $2e_i$, in view of the relation

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

which follows from the relations defining the ring A. Finally, it follows easily from the relations defining A that $e_1 \cdots e_l$ is a basis element for A in the top dimension. This gives the statement of the lemma for $Spin(2l+1)$.

Likewise, Lemma 2.1 shows that the torsion index of $Spin(2l+2)$ is equal to the index in the top degree of the subring of $H^*(SO(2l+2)/U(l+1), \mathbf{Z})$ generated by e_1 and the elements $2e_i$. This is the same as the corresponding number for $Spin(2l+1)$, by the identification

$$SO(2l+1)/U(l) \cong SO(2l+2)/U(l+1),$$

in which the elements e_i in the cohomology of the two spaces correspond. QED

An analogous argument gives an easy calculation of the torsion index for the groups $SO(n)$. (This was known by other methods, as mentioned in the introduction.)

Theorem 3.2 *The torsion index of $SO(2l+1)$ and $SO(2l+2)$ is 2^l.*

Proof. By Lemma 2.1, the torsion index of $SO(2l+1)$ is equal to the index in the top dimension of the image of $H^*(BU(l), \mathbf{Z})$ in $H^*(SO(2l+1)/U(l), \mathbf{Z})$. This subring is the subring generated by the elements $2e_i$. Also, Lemma 2.1 shows that the torsion index of $SO(2l+2)$ is the same thing, in view of the isomorphism $SO(2l+1)/U(l) = SO(2l+2)/U(l+1)$.

Using the relations in A as in the proof of Lemma 3.1, we find that the torsion index of $SO(2l+1)$ and $SO(2l+2)$ is the greatest common divisor of all products of distinct elements $2e_i$ of degree $\binom{l+1}{2}$ in the ring $A = H^*(SO(2l+1)/U(l), \mathbf{Z})$, as a multiple of $e_1 \cdots e_l$. But there is only one such product, $(2e_1) \cdots (2e_l) = 2^l e_1 \cdots e_l$. So $SO(2l+1)$ and $SO(2l+2)$ have torsion index 2^l. QED

Lemma 3.1 makes it straightforward to check that the group $Spin(n)$ has torsion index 2 for $7 \leq n \leq 12$. (This also follows from Pfister's theorem on 12-dimensional quadratic forms, as mentioned in the introduction.) We know that $Spin(n)$ has torsion index a multiple of 2 for $n \geq 7$ by Borel [4]. So we only have to show that the torsion index divides 2 for $7 \leq n \leq 12$. That is, by the above lemma, we need, for $l = 3, 4, 5$, to find an integral polynomial in e_1 and the elements $2e_i$ which is equal in the ring

$$H^*(SO(2l+1)/U(l), \mathbf{Z}) = \mathbf{Z}[e_1, \ldots, e_l]/(e_i^2 - 2e_{i-1}e_{i+1} + 2e_{i-2}e_{i+2} - \cdots + (-1)^i e_{2i} = 0)$$

to $ce_1 \cdots e_l$ for some integer $c \not\equiv 0 \pmod 4$. We compute that

$$\begin{aligned} e_1^2 &= e_2 \\ e_1^4 &= e_2^2 \\ &= 2e_1e_3 - e_4. \end{aligned}$$

Thus, for $l = 3$, where $e_4 = 0$, we have $e_1^6 = 2e_1e_2e_3$, which shows that the torsion index of $Spin(7)$ and $Spin(8)$ divides 2, hence is equal to 2. For $l = 4$, we compute that

$$e_1^{10} = 12e_1e_2e_3e_4,$$

which does not give the conclusion we want; it only shows that the torsion index of $Spin(9)$ and $Spin(10)$ divides 4. Instead, we can use more of the elements e_1 and $2e_i$. We find that

$$e_1^7(2e_3) = 14e_1e_2e_3e_4.$$

Since 14 is not a multiple of 4, we deduce that the torsion index of $Spin(9)$ and $Spin(10)$ is 2. Finally, for $l = 5$, we can again get the optimal result using only e_1, as follows from the proof of Lemma 3.3 below:

$$e_1^{15} = 286e_1e_2e_3e_4e_5.$$

Since 286 is not a multiple of 4, the torsion index of $Spin(11)$ and $Spin(12)$ is 2.

For any $l \geq 1$, let $u(l)$ be the 2-adic order of the torsion index of $Spin(2l+1)$ and $Spin(2l+2)$.

There are some natural upper bounds for the torsion index, which we now present as lemmas. They are not optimal for large l, however, so that we will not use them for our exact calculations of the torsion index. We only mention these results to show that the most obvious methods to bound the torsion index of the spin groups are not optimal. That serves to justify the more difficult methods we will develop later.

Lemma 3.3 *The 2-adic order of the torsion index of $Spin(2l+1)$ and $Spin(2l+2)$ is at most l minus the sum of the 2-adic digits of $\binom{l+1}{2}$.*

Proof. By Lemma 3.1, the 2-adic order of the torsion index of $Spin(2l+1)$ and $Spin(2l+2)$ is the minimum of the 2-adic orders of the integers c such that $ce_1 \cdots e_l$ belongs to the subring of $H^*(SO(2l+1)/U(l), \mathbf{Z})$ generated by e_1 and the elements $2e_i$. This lemma is the bound we get by computing the integer c such that

$$e_1^{\binom{l+1}{2}} = ce_1 \ldots e_l.$$

In other terminology, this number c is the degree of the spinor variety $SO(2l+1)/U(l)$, viewed as a complex projective variety using the ample line bundle corresponding to the generator e_1 of $H^2(SO(2l+1)/U(l), \mathbf{Z})$. This degree follows from Schubert's formula for the degrees of Schubert varieties in Grassmannians together with Giambelli's formula for the top Chern class of the second exterior power of a vector bundle, in [8], Example 14.7.11 and Example 14.5.1:

$$\deg_{e_1}(SO(2l+1)/U(l)) = \frac{\binom{l+1}{2}!\, 1!\, 2! \cdots (l-1)!}{1!\, 3! \cdots (2l-1)!}.$$

Since $\mathrm{ord}_2(n!) = n - \alpha_2(n)$, where $\alpha_2(n)$ is the sum of the 2-adic digits of n, we can compute the 2-adic order of this coefficient. The result is that

$$\mathrm{ord}_2\deg_{e_1}(SO(2l+1)/U(l)) = l - \alpha_2\binom{l+1}{2}.$$

This proves the lemma. QED

Lemma 3.4 *(Marlin [14]) The 2-adic order of the torsion index of $Spin(2l+1)$ and $Spin(2l+2)$ is at most $l - 1 - \lfloor \log_2 l \rfloor$.*

Proof. This proof is as different as could be from the previous one: instead of using only the generator e_1, we will use the generators $2e_i$ as much as possible. So it is somewhat surprising that the two bounds are so close.

We want to compute the index in the top degree of $H^*(SO(2l+1)/U(l), \mathbf{Z})$ of the subring generated by e_1 and the elements $2e_i$. It is trivial that this subring contains $e_1(2e_2)\cdots(2e_l) = 2^{l-1}e_1\cdots e_l$, so that the 2-adic order of the torsion index is at most $l-1$. We can do slightly better by using the relations in $R := H^*(SO(2l+1)/U(l), \mathbf{Z})$ to see that

$$e_i^2 \equiv e_{2i} \pmod{2R}$$

for all i, and hence

$$e_1^{2^i} \equiv e_{2^i} \pmod{2R}$$

for all i. It follows that the product of the elements $2e_j$ for $1 \leq j \leq l$, j not a power of 2, with the elements e_1^j for $1 \leq j \leq l$ such that j is a power of 2, is equal to $2^{l-1-\lfloor \log_2 l \rfloor} e_1 \cdots e_l$ modulo a higher power of 2. QED

By comparing these results with the statement of Theorem 0.1, or with the table after that theorem, we see that neither of these upper bounds for the torsion index is sharp, in general. The true value of $u(l)$, as stated in Theorem 0.1, is very close to $l - 2\log_2 l$. For example, for $l = 5$, Marlin's upper bound for the torsion index of $Spin(11)$ and $Spin(12)$ is 2^2, whereas the true value is 2^1. For $l = 6$, both of the above upper bounds for the torsion index of $Spin(13)$ and $Spin(14)$ are 2^3, whereas the true value is 2^2. Thus these upper bounds are not enough, and we will need different methods to prove Theorem 0.1.

4 A trick, and a strong lower bound for the torsion index

We now introduce a surprising trick into the computation of the torsion index of the spin groups. Namely, we show that this problem is equivalent to a different calculation about the symplectic groups. In these terms, the calculation becomes easier, although still far from trivial. This is all rather strange, since the torsion index of the symplectic groups is 1. At the end of the section, we use this trick to prove a strong lower bound for the torsion index of the spin groups, which turns out to be an equality in most cases.

We use the well-known calculations ([16], III.6.9 and III.6.11):

$$H^*(SO(2l+1)/U(l), \mathbf{Z}) \cong \mathbf{Z}[e_1, \ldots, e_l]/(e_i^2 - 2e_{i-1}e_{i+1} + 2e_{i-2}e_{i+2} - \cdots + (-1)^i e_{2i} = 0)$$
$$H^*(Sp(2l)/U(l), \mathbf{Z}) \cong \mathbf{Z}[f_1, \ldots, f_l]/(f_i^2 - 2f_{i-1}f_{i+1} + 2f_{i-2}f_{i+2} - \cdots + 2(-1)^i f_{2i} = 0)$$

Here e_i and f_i are defined to be 0 for $i > l$. We write $Sp(2l)$ for the simply connected group of type C_l, which topologists usually call $Sp(l)$; the convention here is justified by the inclusions $SU(n) \subset GL(n, \mathbf{C})$, $SO(n) \subset GL(n, \mathbf{C})$, and (with this notation) $Sp(2l) \subset GL(2l, \mathbf{C})$.

We define an injective ring homomorphism from $H^*(Sp(2l)/U(l), \mathbf{Z})$ to $H^*(SO(2l+1)/U(l), \mathbf{Z})$ by sending f_i to $2e_i$ for each i. This is well-defined by inspection of the relations defining these rings.

It is not needed for our proof, but one can give some geometric significance to this ring homomorphism in the following way. This is inspired by Friedlander's

beautiful proof that the spaces $SO(2l+1)/U(l)$ and $Sp(2l)/U(l)$ become homotopy equivalent after localization away from the prime 2 ([7], Theorem 2.5). The point is that there is an isogeny of algebraic groups $SO(2l+1) \to Sp(2l)$ over a field k of characteristic 2 (whereas there is no such isogeny over fields of characteristic not 2). Related to this isogeny of groups, there is a natural map from the Grassmannian X of isotropic l-planes in a quadratic space V of dimension $2l+1$ over k to the Grassmannian Y of isotropic l-planes in the symplectic space $V/V^{\perp}$ of dimension $2l$. This map $X \to Y$ is an inseparable homeomorphism of smooth varieties over k. Like any map between smooth varieties, it determines a homomorphism of Chow rings

$$CH^*Y \to CH^*X$$

[8]. Here the Chow ring of Y is isomorphic to the integral cohomology ring of $Sp(2l)/U(l)$, the Chow ring of X is isomorphic to the integral cohomology ring of $SO(2l+1)/U(l)$, and one can check that the ring homomorphism $CH^*Y \to CH^*X$ is the homomorphism we defined, sending f_i to $2e_i$.

We now return to our purely algebraic point of view, where we simply think of $H^*(Sp(2l)/U(l), \mathbf{Z})$ as a subring of $H^*(SO(2l+1)/U(l), \mathbf{Z})$ via $f_i \mapsto 2e_i$. We have shown that the torsion index of $Spin(2l+1)$ and $Spin(2l+2)$ is the greatest common divisor of the integers c such that

$$e_1^a \prod_{i \in I} 2e_i = ce_1 \cdots e_l$$

in $H^*(SO(2l+1)/U(l), \mathbf{Z})$, where I runs over the subsets of $\{1, \ldots, l\}$ and $a = \binom{l+1}{2} - \deg(I)$, where we define $\deg(I) = \sum_{i \in I} i$. In terms of the elements $f_i = 2e_i$, this equation is equivalent to

$$\begin{aligned} f_1^a \prod_{i \in I} f_i &= 2^a ce_1 \cdots e_l \\ &= 2^{a-l} cf_1 \ldots f_l. \end{aligned}$$

We now observe that the subring $H^*(Sp(2l)/U(l), \mathbf{Z})$ of $H^*(SO(2l+1)/U(l), \mathbf{Z})$ generated by the elements f_i satisfies Poincaré duality. Also, it follows from the relations defining this subring that the elements $\prod_{i \in I} f_i$ with $\deg(I) = j$ form an additive basis for the degree-$2j$ part of the subring. In particular, $f_1 \cdots f_l$ is a basis element for the subring in the top degree, $2\binom{l+1}{2}$. Using Poincaré duality, it follows that for each $0 \le a \le \binom{l+1}{2}$,

$$\mathrm{ord}_2(f_1^a) = \min_{\deg(I) = \binom{l+1}{2} - a} \mathrm{ord}_2 \left(\frac{f_1^a \prod_{i \in I} f_i}{f_1 \cdots f_l} \right).$$

Here, on the left, we define ord_2 of an element x of the ring $H^*(Sp(2l)/U(l), \mathbf{Z})$ to be the largest $i \ge 0$ such that x is divisible by 2^i. Using this formula, we can restate the formula above for the torsion index of $Spin(2l+1)$ and $Spin(2l+2)$ in terms of the ring $H^*(Sp(2l)/U(l), \mathbf{Z})$, as follows.

Lemma 4.1 *The torsion index of $Spin(2l+1)$ and $Spin(2l+2)$ is $2^{u(l)}$, where*

$$u(l) = l + \min_{0 \le a \le \binom{l+1}{2}} (ord_2(f_1^a) - a).$$

Here ord_2 is computed in the ring $R = H^*(Sp(2l)/U(l), \mathbf{Z})$. The minimum here will be negative, but of course $u(l)$ itself is nonnegative.

This translation of the problem leads to an extremely strong lower bound for the torsion index of the spin groups; in fact, this lower bound is an equality in most cases.

We use the relations in $R := H^*(Sp(2l)/U(l), \mathbf{Z})$:

$$f_i^2 - 2f_{i-1}f_{i+1} + 2f_{i-2}f_{i+2} - \cdots + 2(-1)^i f_{2i} = 0.$$

Thus $f_i^2 \in 2R$. Let I be the ideal of elements of positive degree in R, which is generated by $f_1, \ldots, f_l$. From the identity $(x+y)^2 = x^2 + 2xy + y^2$, we see that every element x of the ideal I has $x^2/2 \in I$. In other words, the ideal of elements of positive degree in $H^*(Sp(2l)/U(l), \mathbf{Z}_{(2)})$ has a divided power structure ([3], Definition 3.1). By induction, it follows that f_1, $f_1^2/2$, $f_1^4/2^3$, $f_1^8/2^7$, and so on are in R. That is,

$$\mathrm{ord}_2(f_1^{2^b}) \geq 2^b - 1$$

for all b. Therefore, writing any natural number a as a sum of distinct powers of 2, we have

$$\mathrm{ord}_2(f_1^a) \geq a - \alpha_2(a)$$

for all $a \geq 0$, where $\alpha_2(a)$ denotes the sum of the base-2 digits of a. By our formula for the torsion index in terms of $\mathrm{ord}_2(f_1^a)$, it follows that

$$\begin{aligned} u(l) &\geq l - \max_{0 \leq a \leq \binom{l+1}{2}} \alpha_2(a) \\ &= l - \left\lfloor \log_2 \left(\binom{l+1}{2} + 1 \right) \right\rfloor. \end{aligned}$$

To prove Theorem 0.1, we have to show that this lower bound for the torsion index is an equality for most values of l, and fails to be an equality only by 1 in the other cases. Write $a = \lfloor \log_2(\binom{l+1}{2} + 1) \rfloor$, so that our lower bound for the torsion index is $u(l) \geq l - a$.

5 Reduction to a combinatorial problem

In the last section, we showed how the torsion index of the spin groups could be computed exactly in terms of the symplectic groups, and used this to give a strong lower bound for the torsion index. To prove Theorem 0.1, we need to show that our lower bound is in fact an equality in most cases. In this section, we give a simple combinatorial sufficient condition for our lower bound to be an equality, Corollary 5.5. We apply this at the end of the section to compute the torsion index of $Spin(n)$ for n at most 16. Later, in Lemma 6.3, we will find that this section's sufficient condition for our lower bound to be an equality is also necessary.

In this section, we are looking for a way to prove that $u(l)$, the 2-adic order of the torsion index of $Spin(2l+1)$ and $Spin(2l+2)$, is equal to the lower bound $l - a$ for some values of l. Here $a = \lfloor \log_2(\binom{l+1}{2} + 1) \rfloor$. That is, a is the largest number

such that $2^a - 1 \leq \binom{l+1}{2}$. The previous section shows, in particular, that the element f_1 of $R = H^*(Sp(2l)/U(l), \mathbf{Z})$ satisfies

$$\begin{aligned} \mathrm{ord}_2(f_1^{2^a-1}) &\geq 2^a - 1 - \alpha_2(2^a - 1) \\ &= 2^a - a - 1. \end{aligned}$$

Suppose we can show that $f_1^{2^a-1}$ has 2-adic order equal to $2^a - a - 1$. Then, by the previous section,

$$\begin{aligned} u(l) &= l + \min_{0 \leq i \leq \binom{l+1}{2}} (\mathrm{ord}_2(f_1^i) - i) \\ &\leq l + \mathrm{ord}_2(f_1^{2^a-1}) - (2^a - 1) \\ &= l + (2^a - a - 1) - (2^a - 1) \\ &= l - a. \end{aligned}$$

Thus, to show that $u(l)$ is equal to our lower bound $l - a$, it suffices to show that the single element $f_1^{2^a-1}$ of R has 2-adic order equal to $2^a - a - 1$.

As mentioned in the previous section, the ideal I of elements of positive degree in $R = H^*(Sp(2l)/U(l), \mathbf{Z})$ admits a divided square operation, $s(x) = x^2/2$. Therefore we can rewrite $f_1^{2^a-1}$ as:

$$\begin{aligned} f_1^{2^a-1} &= \prod_{i=0}^{a-1} f_1^{2^i} \\ &= \prod_{i=0}^{a-1} 2^{2^i-1} s^i(f_1) \\ &= 2^{2^a-a-1} \prod_{i=0}^{a-1} s^i(f_1). \end{aligned}$$

Thus, if we can show that $\prod_{i=0}^{a-1} s^i(f_1)$ is nonzero in the ring $R/2$, then $f_1^{2^a-1}$ has 2-adic order equal to $2^a - a - 1$, and therefore our lower bound for the torsion index, $u(l) \leq l - a$, is an equality.

The divided square operation $s(x)$ passes to a divided square operation on the ideal of elements of positive degree in the ring $R/2$. Thus we have made an important advance in the calculation of the torsion index: we have at least a sufficient condition for the equality $u(l) = l - a$ which involves only calculations modulo 2. A priori, the problem requires calculations modulo high powers of 2. We have brought the calculations we need to do from deep under water up to the surface.

From the relations defining $R = H^*(Sp(2l)/U(l), \mathbf{Z})$, we see that $R/2$ is the exterior algebra on generators $f_1, \ldots, f_l$. Also, we read off from these relations that the divided square operation s on the augmentation ideal of the exterior algebra $R/2$ is given by

$$s(f_i) = f_{i-1}f_{i+1} + f_{i-2}f_{i+2} + \cdots + f_1 f_{2i-1} + f_{2i}.$$

To show that $u(l) = l - a$ by the method described above, it suffices to show that the expression $\prod_{i=0}^{a-1} s^i(f_1)$ in $R/2$ is nonzero. This expression looks complicated at first, if one writes it out for small values of a, but it turns out to have a surprisingly neat description. We begin by describing each factor in this product.

Lemma 5.1 *Consider the list of elements of the exterior algebra $R/2$ of the form f_{2^j} with $j \geq 0$ or $f_{2^j-c}f_{2^j+c}$ with $1 \leq c \leq 2^j - 1$. Thus this list consists of:*

$$f_1; f_2; f_4, f_1f_3; f_8, f_1f_7, f_2f_6, f_3f_5; \ldots.$$

Then, for any $b \geq 0$, the iterated divided square $s^b(f_1)$ in $R/2$ is equal to the sum over all subsets S of the given list with total degree 2^b of the product of the elements in S.

Proof. We prove this by induction on b. For $b = 0$, we are just saying that $s^0(f_1) = f_1$, which is true. Suppose that the lemma is true for b; we will prove it for $b + 1$. We compute:

$$s^{b+1}(f_1) = s\left(\sum_{\deg(S)=2^b} \prod_{y\in S} y\right).$$

Here S runs over subsets of the above list of elements of $R/2$ and $\deg(S)$ denotes the sum of the degrees of the elements of S. Using the identity $s(x+y) = s(x)+xy+s(y)$ satisfied by a divided square operation, it follows that

$$s^{b+1}(f_1) = \sum_{\deg(S)=2^b} s\left(\prod_{y\in S} y\right) + \sum_{\substack{\deg(S)=\deg(T)=2^b \\ S<T}} \prod_{y\in S} y \prod_{z\in T} z.$$

Here $S < T$ refers to any fixed ordering on the set of all subsets of the above list.

Furthermore, any divided square operation on an ideal I in a ring R satisfies $s(xy) = 2s(x)s(y)$ for $x, y \in I$. Thus, in the case at hand, we have $s(xy) = 0$ for all x and y in the augmentation ideal of $R/2$. So all terms in the first sum, above, other than $s(f_{2^b})$ are zero. Using the explicit formula for $s(f_i)$ in the ring $R/2$, we have:

$$s^{b+1}(f_1) = f_{2^{b+1}} + f_1f_{2^{b+1}-1} + \cdots + f_{2^b-1}f_{2^b+1} + \sum_{\substack{\deg(S)=\deg(T)=2^b \\ S<T}} \prod_{y\in S} y \prod_{z\in T} z.$$

Here the first terms are part of the formula we want to prove for $s^{b+1}(f_1)$, those corresponding to one-element subsets of the above list of elements of $R/2$. It remains to show that

$$\sum_{\substack{\deg(U)=2^{b+1} \\ U \text{ has } \geq 2 \text{ elements}}} \prod_{y\in U} y = \sum_{\substack{\deg(S)=\deg(T)=2^b \\ S<T}} \prod_{y\in S} y \prod_{z\in T} z.$$

To prove this, first notice that we can restrict the sum on the right to consider only subsets S and T of our list which are disjoint. Indeed, all elements y of positive degree in $R/2$ have $y^2 = 2s(y) = 0$. Next, once we know that S and T are disjoint, their union U is a subset of our list with total degree $\deg(U) = 2^{b+1}$ and with at least two elements. Therefore the above equality follows from a similar equality for each such subset U of our list. Namely, we need to show that for each subset U of our list with total degree $\deg(U) = 2^{b+1}$ and with at least two elements, the

numbers of subsets S of U with total degree 2^b is congruent to 2 modulo 4. Indeed, the number of disjoint pairs S, T with $S < T$, $\deg(S) = \deg(T) = 2^b$, and $S \cup T = U$ is half of the number just mentioned (because of the condition $S < T$), so it will be 1 modulo 2, which is what we need to prove the above identity.

We see that only the degrees of the elements of U matter for this problem, and they are all powers of 2. Thus, we need to show that for any $r \geq 2$ and any nonnegative integers $a_1, \ldots, a_r$ such that $2^{a_1} + \cdots + 2^{a_r} = 2^{b+1}$, the number of subsets S of $\{1, \ldots, r\}$ with $\sum_{i \in I} 2^{a_i} = 2^b$ is congruent to 2 modulo 4. We can assume that $a_1 \leq \cdots \leq a_r$. Also, by subtracting a_1 from $a_1, \ldots, a_r$ and from b, we can assume that $a_1 = 0$. The given class of subsets S is closed under replacing S by $\{1, \ldots, r\} - S$, so it suffices to show that the number of subsets S with $\sum_{i \in I} 2^{a_i} = 2^b$ and $1 \notin S$ is odd. Equivalently, we are given numbers $a_2, \ldots, a_r$ such that $2^{a_2} + \cdots + 2^{a_r} = 2^{b+1} - 1$, and we want to show that the number of subsets S of $\{2, \ldots, r\}$ with $\sum_{i \in S} 2^{a_i} = 2^b$ is odd. This follows from the following lemma, using that $\binom{2^{b+1}-1}{2^b}$ is odd. QED (Lemma 5.1)

Lemma 5.2 *For any nonnegative integers $a_1, \ldots, a_r$, let $N = 2^{a_1} + \cdots + 2^{a_r}$, and let $0 \leq c \leq N$. Then the number of subsets S of $\{1, \ldots, r\}$ with $\sum_{i \in S} 2^{a_i} = c$ is congruent to $\binom{N}{c}$ modulo 2.*

Proof. Use induction on r. We can assume that $a_1 \leq \cdots \leq a_r$. First suppose that $a_1 = 0$. Clearly, the number of subsets S of $\{1, \ldots, r\}$ with $\sum_{i \in S} 2^{a_i} = c$ is equal to the number of subsets S of $\{2, \ldots, r\}$ with $\sum_{i \in S} 2^{a_i} = c$ plus the number of subsets S of $\{2, \ldots, r\}$ with $\sum_{i \in S} 2^{a_i} = c - 1$. By induction on r, the latter sum is congruent modulo 2 to

$$\binom{N-1}{c} + \binom{N-1}{c-1} = \binom{N}{c},$$

as we want. Next, if $a_1 > 0$, we can apply this argument after subtracting a_1 from $a_1, \ldots, a_r$, and we find that the given number of subsets is congruent to $\binom{N/2^{a_1}}{c/2^{a_1}}$ modulo 2. But we check immediately that $\binom{a}{b}$ is always congruent to $\binom{2a}{2b}$ modulo 2, and so this number of subsets is congruent to $\binom{N}{c}$ modulo 2, as we want. QED

This completes the proof of Lemma 5.1, which gives a useful calculation of the iterated divided power $s^b(f_1)$ in the exterior algebra $R/2$, for any nonnegative integer b. What we want, however, is a useful calculation of the product $\prod_{i=0}^{a-1} s^i(f_1)$. The following is a first step.

Lemma 5.3 *Consider the list of elements of the exterior algebra $R/2$ of the form f_{2^j} with $j \geq 0$ or $f_{2^j - c} f_{2^j + c}$ with $1 \leq c \leq 2^j - 1$. Thus this list consists of:*

$$f_1; f_2; f_4, f_1 f_3; f_8, f_1 f_7, f_2 f_6, f_3 f_5; \ldots.$$

Then, for any $b \geq 0$, the product $\prod_{i=0}^{b} s^i(f_1)$ in $R/2$ is equal to the sum over all subsets S of the given list with total degree $2^{b+1} - 1$ of the product of the elements in S.

Proof. This follows from Lemma 5.1 once we show that for each subset S of the given list with total degree $2^{b+1} - 1$, the number of ways of partitioning S into

subsets with total degrees $1, 2, 4, \ldots, 2^b$ is odd. Clearly this question depends only on the degrees of the elements of S, which are all powers of 2. That is, it suffices to show that for any nonnegative integers $a_1, \ldots, a_r$ such that $2^{a_1} + \cdots + 2^{a_r} = 2^{b+1} - 1$, the number of partitions of the set $S = \{1, \ldots, r\}$ into subsets $S = \coprod_{j=0}^{b} S_j$ such that $\sum_{i \in S_j} 2^{a_i} = 2^j$ for $j = 0, \ldots, b$ is odd.

By Lemma 5.2, the number of subsets S_b such that $\sum_{i \in S_b} 2^{a_i} = 2^b$ is congruent modulo 2 to $\binom{2^{b+1}-1}{2^b}$, and thus to 1. The total number of partitions as above is the product of this odd number of subsets S_b with the analogous number of partitions of $S - S_b$ (for any choice of S_b), a set with total degree $2^b - 1$ rather than $2^{b+1} - 1$. By induction on b, the latter number of partitions is odd. Therefore the number of partitions we consider is also odd. QED

Surprisingly, we can now give an even more elementary description of the product $\prod_{i=0}^{b} s^i(f_1)$ in the exterior algebra $R/2$. Namely, we can give a purely combinatorial description of whether the coefficient of a given monomial $\prod_{i \in I} f_i$, for $I \subset \{1, \ldots, l\}$, is 0 or 1. In order to state this, we define the *degree* $\deg(I)$ of a subset I of $\{1, \ldots, l\}$ to be the sum of the elements of I. This terminology will be used for the rest of the paper.

Lemma 5.4 *Given any $b \geq 0$ and any subset I of $\{1, \ldots, l\}$ with degree $deg(I) = \sum_{i \in I} i$ equal to $2^{b+1} - 1$, the coefficient of the monomial $\prod_{i \in I} f_i$ in the element $\prod_{i=0}^{b} s^i(f_1)$ of the exterior algebra $R/2 = \mathbf{F}_2\langle f_1, \ldots, f_l \rangle$ is 1 if and only if the set I can be written as a disjoint union of subsets of order at most 2 and of degree a power of 2.*

Proof. By Lemma 5.3, the product $\prod_{i=0}^{b} s^i(f_1)$ in $R/2$ is the sum of all monomials in the elements f_{2^j} and $f_{2^j - c} f_{2^j + c}$ which have total degree $2^{b+1} - 1$. Any such monomial which involves the same generator f_i twice is 0 and so can be omitted. So the coefficient of a given monomial $\prod_{i \in I} f_i$ in this expression is the number (modulo 2) of ways of writing I as a disjoint union of subsets which have order at most 2 and have degree a power of 2.

To prove the lemma, we will show that for any subset I of $\{1, \ldots, l\}$, the number of ways of decomposing I as a disjoint union of subsets as above is always 0 or 1 (not just modulo 2). That is, if I can be decomposed into such subsets, then the decomposition is unique. We prove this by induction on the order of I. Consider the largest element x of I. If x is a power of 2, 2^j, then the subset of I containing x must be (2^j), because the larger element of any 2-element subset $(2^j - c, 2^j + c)$ cannot be a power of 2. If x is not a power of 2, then there is a unique way of writing it as $2^j + c$ with $0 < c < 2^j$, and the subset of I containing x must be $(2^j - c, 2^j + c)$. In either case, we remove the subset of I which contains x, and we find by induction that there is a unique way of decomposing the rest of I into subsets of the given type. QED

We showed earlier in this section that if we let $a = \lfloor \log_2(\binom{l+1}{2} + 1) \rfloor$, and if the element $\prod_{i=0}^{a-1} s^i(f_1)$ of the exterior algebra $R/2$ is not zero, then we know the torsion index: $u(l) = l - a$. Using Lemma 5.4, we have the following combinatorial way to determine the torsion index, the climax of this section. (Later, in Lemma 6.3, we will show that the following sufficient condition for proving $u(l) = l - a$ is also necessary.)

Corollary 5.5 *Let* $a = \lfloor \log_2(\binom{l+1}{2} + 1) \rfloor$. *Suppose that there is an subset* I *of* $\{1, \ldots, l\}$ *which has degree* $deg(I) = \sum_{i \in I} i$ *equal to* $2^a - 1$ *and which can be decomposed as a disjoint union of subsets of order at most 2 and of degree a power of 2. Then the torsion index* $2^{u(l)}$ *of* $Spin(2l+1)$ *and* $Spin(2l+2)$ *is given by*

$$u(l) = l - a.$$

For example, we can use Corollary 5.5 to prove that $u(l) = l - a$ for $l \leq 7$. To do this, we exhibit a subset I of degree $2^a - 1$ in $\{1, \ldots, l\}$ which is a disjoint union of subsets of order at most 2 and of degree a power of 2, as follows.

l	$\binom{l+1}{2}$	$2^a - 1$	I
1	1	1	(1)
2	3	3	(1)(2)
3	6	3	(1)(2)
4	10	7	(1)(2)(4)
5	15	15	(3, 5)(1)(2)(4)
6	21	15	(3, 5)(1)(2)(4)
7	28	15	(3, 5)(1)(2)(4)

Thus, we know that $u(l) = l - a$ for $l \leq 7$; equivalently, we have computed the torsion index of $Spin(n)$ for $n \leq 16$. This calculation proves Theorem 0.1 for $l \leq 7$. Thus, in all our later analyses of $u(l)$, we can assume that $l \geq 8$ whenever that is convenient.

The above argument fails for $l = 8$ (there is no subset I of $\{1, \ldots, 8\}$ with the properties required). Indeed, for $l = 8$, we will show later, as the first case of Lemma 7.2, that $u(l)$ is $l - a + 1 = 4$ rather than $l - a = 3$.

6 Proof that $u(l) = l - a$ for most values of l

In this section, we prove that our lower bound for the torsion index of the spin groups is an equality in most cases. After this section, it will only remain to compute the torsion index of $Spin(2l+1)$ and $Spin(2l+2)$ when l is equal to or slightly greater than a power of 2 or $\sqrt{2}$ times a power of 2. At the end of the section, we show that even for these difficult values of l, the 2-adic order of the torsion index is either equal to our lower bound or is one more than that (in agreement with Theorem 0.1). We also give a combinatorial way to decide which of the two possibilities occurs (Lemma 6.3). The rest of the paper will be devoted to solving this combinatorial problem.

We begin by proving that $u(l) = l - a$ for some values of l where this can be done easily. First, we prove this for a certain number l which is not much bigger than any given power of 2.

Lemma 6.1 *Let* $l = 2^c + 2^{c-3}$, *for any* $c \geq 3$. *Let* $a = \lfloor \log_2(\binom{l+1}{2} + 1) \rfloor$, *which in this case is* $2c - 1$. *Then there is a subset* I *of* $\{1, \ldots, l\}$ *of degree* $2^a - 1$ *which can be decomposed into subsets of order at most 2 and of degree a power of 2. It follows that* $u(l) = l - a$.

Proof. The following subset I does it.

$$(2^c - 2^{c-3}, 2^c + 2^{c-3}) \cdots (2^c - 1, 2^c + 1)\ (2^{c-2} + 1, 2^c - 2^{c-2} - 1) \cdots (2^{c-1} - 1, 2^{c-1} + 1)\ (1)(2)(4) \cdots (2^{c-1})(2^c).$$

Then Corollary 5.5 implies that $u(l) = l - a$. QED

Next, we prove that $u(l) = l - a$ for a number l which is not much bigger than $2^{c+\frac{1}{2}}$, for any given value of c.

Lemma 6.2 *Let $l = 2^{c+1} - 2^{c-1} - 1$, for any $c \geq 2$. Let $a = \lfloor \log_2(\binom{l+1}{2} + 1) \rfloor$, which in this case is $2c$. Then there is a subset I of $\{1, \ldots, l\}$ of degree $2^a - 1$ which can be decomposed into subsets of order at most 2 and of degree a power of 2. It follows that $u(l) = l - a$.*

Proof. The following subset I does it.

$$(2^{c-1} + 1, 2^{c+1} - 2^{c-1} - 1) \cdots (2^c - 1, 2^c + 1)\ (1)(2)(4) \cdots (2^{c-1})(2^c).$$

QED

Let us sum up what we can deduce from Lemmas 6.1 and 6.2. First, notice that the function a of l defined by $\lfloor \log_2(\binom{l+1}{2} + 1) \rfloor$ is mostly constant, and only increases by 1 when l is a power of 2, $l = 2^c$, or when l is a certain number l_0 around $2^{c+\frac{1}{2}}$. Explicitly, throughout the paper, let l_0 denote the smallest integer l such that $\binom{l+1}{2} \geq 2^{2c} - 1$. It is straightforward to check that $|2^{c+\frac{1}{2}} - l_0| < 1$ for all c. Now Lemma 6.1 says that for $l = 2^c + 2^{c-3}$, which lies between 2^c and $l_0 \doteq 2^{c+\frac{1}{2}}$ so that $a = 2c-1$, there is a subset I of $\{1, \ldots, l\}$ of degree $2^a - 1$ which can be decomposed into subsets of order at most 2 and of degree a power of 2. This immediately implies the same statement for all $2^c + 2^{c-3} \leq l < l_0$. In particular, we know the torsion index, $u(l) = l - a$, for all l in that interval. Likewise, Lemma 6.2 implies that for all $2^{c+1} - 2^{c-1} - 1 \leq l < 2^{c+1}$, there is a subset I, of degree $2^a - 1$ (where $a = 2c$), decomposed as above. So again we have $u(l) = l - a$ for all l in that interval.

At this point, we have determined the torsion index for most of the spin groups. The intervals above are not optimal, and we will need to improve them. Before doing that, however, we can deduce some rough information about $u(l)$ for all l from the results so far.

First, from Lemmas 6.1 and 6.2 (or the discussion above), it is clear that for all l, if we define a as usual, then there is a subset I of $\{1, \ldots, l\}$ which has degree $2^{a-1} - 1$ (rather than $2^a - 1$) and which is decomposed as above. By Corollary 5.5, it follows that, in the ring $R = H^*(Sp(2l)/U(l), \mathbf{Z})$, $f_1^{2^{a-1}-1}$ has the smallest 2-adic order it could have, $2^{a-1} - (a-1) - 1$. By our formula for the torsion index in terms of R, Lemma 4.1, it follows that $u(l)$ is at most $l - a + 1$, hence is either $l - a$ or $l - a + 1$. Thus we have determined $u(l)$ to within 1 for all l. Of course, this agrees with the statement of Theorem 0.1.

The rest of the paper will nail down the ambiguity in $u(l)$ for the remaining values of l. At least we can see that this is a purely combinatorial problem, as follows. We only have to decide whether $u(l)$ is $l - a$ or $l - a + 1$ when l is in the interval $[2^c, 2^c + 2^{c-3}]$ or in the interval $[l_0, 2^{c+1} - 2^{c-1} - 1]$ ($l_0 \doteq 2^{c+\frac{1}{2}}$, as defined above); otherwise we have already shown that $u(l) = l - a$ by producing a suitable subset I. Now we observe that for l in one of these rather short intervals, $\binom{l+1}{2}$ is not much bigger than $2^a - 1$; in particular, it is less than $2^{a+1} - 2^{a-1} - 1$. It follows that the only number $\leq \binom{l+1}{2}$ which has a nonzero binary digits is $2^a - 1$, since the next larger such number is $2^{a+1} - 2^{a-1} - 1$ ($= 1011 \cdots 11$). By our formula for the torsion index in terms of the ring R, Lemma 4.1, it follows that $u(l)$ is equal to

$l-a$ if and only if $f_1^{2^a-1}$ has the smallest 2-adic order it could have, 2^a-a-1; no other power of f_1 is relevant. Combining this with Lemma 5.4 gives the following statement, which strengthens Corollary 5.5 to an "if and only if" statement.

Lemma 6.3 *For any $l \geq 1$, let $a = \lfloor \log_2(\binom{l+1}{2}+1) \rfloor$. Write $2^{u(l)}$ for the torsion index of Spin$(2l+1)$ and Spin$(2l+2)$. Then $u(l)$ is either $l-a$ or $l-a+1$. It is equal to $l-a$ if and only if there is a subset I of $\{1,\ldots,l\}$ of degree 2^a-1 which can be decomposed as a disjoint union of subsets of order at most 2 and of degree a power of 2.*

7 Determination of $u(l)$ for l near a power of 2

As explained in the previous section, we know that $u(l)$ is equal to $l-a$ except possibly when there is an integer c such that l lies in one of two intervals, $[2^c, 2^c + 2^{c-3}]$ or $[l_0, 2^{c+1} - 2^{c-1} - 1]$, where l_0 is roughly $2^{c+\frac{1}{2}}$. In this section, we determine $u(l)$ completely for l in the first interval, $[2^c, 2^c + 2^{c-3}]$.

For all l in this interval, the number $a = \lfloor \log_2(\binom{l+1}{2}+1) \rfloor$ is $2c-1$. Therefore, by Lemma 6.3, we must have $u(l) = l-a+1$ for an initial part of this interval (possibly empty), and then $u(l) = l-a$ for the remaining part of this interval (again possibly empty), where the change comes for the first value of l such that there is a subset I of $\{1,\ldots,l\}$ of degree $2^a - 1 = 2^{2c-1} - 1$ which can be decomposed into subsets of order at most 2 and of degree a power of 2. We begin by finding a number B (much smaller than 2^{c-3}) such that $l = 2^c + B$ satisfies $u(l) = l - a$. This improved version of Lemma 6.1 will in fact be optimal.

Lemma 7.1 *Given any $c \geq 2$, let B be the smallest nonnegative integer such that $2B - u(B) > c-3$. Let $l = 2^c + B$. Then there is a subset I of $\{1,\ldots,l\}$ of degree $2^a - 1 = 2^{2c-1} - 1$ which can be decomposed into subsets of order at most 2 and of degree a power of 2. It follows that $u(l) = l - a$.*

We already know $u(l)$ to within 1 for all l by the previous section; in particular, $u(l)$ is always close to $l - 2\log_2 l$. So the condition on B says roughly that $B + 2\log_2(B) > c-3$, and hence B is roughly $c - 3 - 2\log_2 c$.

Proof. Let f be the largest number such that there is a subset J of $\{1,\ldots,B\}$ of degree $2^f - 1$ which can be decomposed into subsets of order at most 2 and degree a power of 2. By Lemma 6.3, we have $u(B) = B - f$. Thus our assumption on B can be restated in terms of f: we have $B + f > c-3$, or equivalently $B + f \geq c-2$.

Using that $l = 2^c + B$, we compute that

$$\binom{l+1}{2} - (2^{2c-1} - 1) = B \cdot 2^c + 2^{c-1} + \binom{B+1}{2} + 1.$$

We can rewrite this as:

$$\binom{l+1}{2} - (2^{2c-1}-1) = (B+f-(c-2))2^c + (2^c - 2^f) + \cdots + (2^c - 2^{c-2}) + \left[\binom{B+1}{2} - (2^f - 1)\right].$$

For most values of c, we will have $B + f = c - 2$. In that case, we can take the subset I defined as:

$$(2^c - B, 2^c + B) \cdots (2^c - 1, 2^c + 1)(2^c)\ (B+1, 2^c - (B+1)) \cdots (2^{c-1} - 1, 2^{c-1} + 1)(2^{c-1})\ J,$$

where we include the pair $(2^r, 2^c - 2^r)$ for $\lfloor \log_2 B \rfloor + 1 \leq r \leq f - 1$, while we replace $(2^r, 2^c - 2^r)$ by (2^r) alone for $f \leq r \leq c - 2$. The previous paragraph's formula makes it easy to see that I has degree $2^{2c-1} - 1$, as we want, when $B + f = c - 2$. The only other possibility is for $B + f$ to be $c - 1$. In this case, we have to remove one of the terms $(j, 2^c - j)$ from the above definition of I, and then again I has degree $2^{2c-1} - 1$. QED

This lemma implies that $u(l) = l - a$ for all l in the interval $[2^c + B, l_0 - 1]$, where $l_0 \doteq 2^{c+\frac{1}{2}}$. We now complete the determination of the torsion index for l near 2^c by showing that $u(l) = l - a + 1$ for l in the interval $[2^c, 2^c + B - 1]$. This confirms Theorem 0.1 for this range of l's.

Lemma 7.2 *For any $c \geq 2$, define B as in Lemma 7.1. Then $u(l) = l - a + 1$ for all l in the interval $[2^c, 2^c + B - 1]$.*

Proof. Write $l = 2^c + b$, where $0 \leq b < B$. Let f be the largest number such that there is a subset of $\{1, \ldots, b\}$ of degree $2^f - 1$ which can be decomposed as in Lemma 6.3. Our assumption that $b < B$ means that $b + f \leq c - 3$. We want to show that there is no subset of the much larger interval $\{1, \ldots, l\}$ of degree $2^{2c-1} - 1$ which can be decomposed as in Lemma 6.3.

We know by Lemma 6.3 and the preceding discussion that f is either $\lfloor \log_2(\binom{b+1}{2} + 1) \rfloor$ or one less than that. Let us first assume that f is equal to $\lfloor \log_2(\binom{b+1}{2} + 1) \rfloor$, as is true for most values of b.

Suppose that there is a subset I of $\{1, \ldots, l\}$ of degree $2^{2c-1} - 1$ which can be decomposed as in Lemma 6.3; we will derive a contradiction. By the proof of Lemma 5.3, any collection of powers of 2 with sum $2^{2c-1} - 1$ can be partitioned into subsets whose sums are 1, 2, 4, ..., and 2^{2c-2}. Therefore, we can partition I into disjoint subsets $I_0, \ldots, I_{2c-2}$ such that I_j has degree 2^j and each set I_j is a union of some of the subsets of order at most 2 and of degree a power of 2 into which we decomposed I.

Let j be a number in the range $f + 1 \leq j \leq c - 2$. Since $j \geq f + 1 = \lfloor \log_2(\binom{b+1}{2} + 1) \rfloor + 1$, we have $j > \log_2(\binom{b+1}{2} + 1)$, and so $2^j > \binom{b+1}{2} + 1$; in particular, $2^j > \binom{b+1}{2}$. Since the sum of the elements of the subset I_j of $\{1, \ldots, l\}$ is 2^j, it follows that I_j contains at least one element greater than b. Choose one, and call it x_j. Clearly x_j is at most 2^j.

Thus, for each $f + 1 \leq j \leq c - 2$, the original set I contains a number x_j with $b + 1 \leq x_j \leq 2^j$. Also, the numbers x_j are different for different j's, since x_j is in I_j. The pair $(x_j, 2^c - x_j)$ cannot be one of the subsets into which I is partitioned, since it would have to be contained in I_j, whereas the sum of all elements of I_j is only 2^j, which is at most 2^{c-2} and in particular is less than 2^c. It follows that the number $2^c - x_j$ is not in the set I at all; apart from $(x_j, 2^c - x_j)$, the next way it could appear in I would be in a pair $(2^c - x_j, 2^c + x_j)$, but we arranged that $x_j \geq b + 1$ and so $2^c + x_j$ is greater than $2^c + b = l$, which is not allowed.

Since we have found some numbers in $\{1, \ldots, l\}$ which are not in I, we get a

lower bound for $\binom{l+1}{2} - \deg(I)$:

$$\begin{aligned}\binom{l+1}{2} - \deg(I) &\geq (2^c - x_{f+1}) + \cdots + (2^c - x_{c-2}) \\ &\geq (2^c - 2^{f+1}) + \cdots + (2^c - 2^{c-2}) \\ &= (c-f-3)2^c + 2^{c-1} + 2^{f+1} \\ &> (c-f-3)2^c + 2^{c-1} + \binom{b+1}{2} + 1.\end{aligned}$$

On the other hand, we are assuming that $\deg(I) = 2^{2c-1} - 1$, and therefore we compute that

$$\binom{l+1}{2} - \deg(I) = b \cdot 2^c + 2^{c-1} + \binom{b+1}{2} + 1.$$

Comparing these two results, we find that $b > c - f - 3$, that is, $b + f > c - 3$. This contradicts the fact that $b + f \leq c - 3$. Thus we have shown that there is no set I as above.

This proves the lemma when f is $\lfloor \log_2(\binom{b+1}{2}+1) \rfloor$, as is true for most values of b. It remains to prove the lemma for those values of b such that $f = \lfloor \log_2(\binom{b+1}{2}+1) \rfloor - 1$. In this case, we know from Lemmas 6.1 and 6.2, and the discussion afterward, that b is only a little greater than 2^x or $2^{x+\frac{1}{2}}$ for some integer x. Therefore $\binom{b+1}{2}$ is just a little greater than 2^{f+1}. Precisely, the fact we will need in what follows is that $\binom{b+1}{2} < 2^{f+2} - 2^f - 1$, as mentioned before Lemma 6.3 (there using the notation a for $f + 1 = \lfloor \log_2(\binom{b+1}{2} + 1) \rfloor$).

The proof of the lemma goes along the same lines as in the previous case. Suppose that there is a subset I of $\{1, \ldots, l\}$ of degree $2^{2c-1} - 1$ which can be decomposed into subsets as in Lemma 6.3; we will derive a contradiction. We can partition I into subsets $I_0, \ldots, I_{2c-2}$ as above.

In this case, we can only say that 2^{f+2}, not 2^{f+1}, is greater than $\binom{b+1}{2} + 1$. So the above argument only produces elements x_j for $f + 2 \leq j \leq c - 2$; that is, for each such j, we can find an element x_j of I_j such that $b + 1 \leq x_j \leq 2^j$. In this case, however, we can also say that at least one of the sets S_j with $0 \leq j \leq f$ contains an element greater than b. If not, then $S_0 \cup \cdots \cup S_f$ would be a subset of $\{1, \ldots, b\}$ of degree $2^{f+1} - 1$ which can be decomposed as in Lemma 6.3, which would contradict the definition of f. Thus, let x_f denote an element of $S_0 \cup \cdots \cup S_f$ which is greater than b. Clearly $x_f \leq 2^f$. Finally, $S_0 \cup \cdots \cup S_f \cup S_{f+1}$ must contain at least one other element greater than b, besides x_f. Indeed, the sum of the elements of $S_0 \cup \cdots \cup S_{f+1} - \{x_f\}$ is $2^{f+2} - x_f - 1$, hence is at least $2^{f+2} - 2^f - 1$, hence is greater than $\binom{b+1}{2}$, by the inequality discussed above. Thus, let x_{f+1} be an element of $S_0 \cup \cdots \cup S_{f+1}$ other than x_f which is greater than b. Clearly $x_{f+1} \leq 2^{f+1}$.

By the same argument as in the previous case of the lemma, the subset I of $\{1, \ldots, l\}$ does not contain $2^c - x_j$ for $f \leq j \leq c - 2$. Therefore

$$\begin{aligned}\binom{l+1}{2} - \deg(I) &\geq (2^c - x_f) + \cdots + (2^c - x_{c-2}) \\ &\geq (2^c - 2^f) + \cdots + (2^c - 2^{c-2}) \\ &= (c-f-2)2^c + 2^{c-1} + 2^f.\end{aligned}$$

On the other hand, we have $\deg(I) = 2^{2c-1} - 1$, and so

$$\binom{l+1}{2} - \deg(I) = b \cdot 2^c + 2^{c-1} + \binom{b+1}{2} + 1.$$

Combining this with the previous inequality, we conclude that

$$(c - b - f - 2)2^c \leq \binom{b+1}{2} + 1 - 2^f.$$

Here $\binom{b+1}{2}$ is just a little greater than 2^{f+1}; in particular, the right side of this inequality is less than 2^c, since f is much less than c. So

$$c - b - f - 2 \leq 0,$$

which contradicts the fact that $b + f \leq c - 3$. Thus in fact there is no subset I as above. QED

8 Analysis of $u(l)$ for l near $2^{c+\frac{1}{2}}$: reduction to an arithmetic inequality

To complete the proof of Theorem 0.1, it suffices to show for each integer c at least 2 that our lower bound for $u(l)$ is an equality for a single value l_0 of l, roughly $2^{c+\frac{1}{2}}$. Indeed, this will imply that our lower bound is an equality for all l from l_0 to $2^{c+1} - 1$, which is the last range where we have not yet computed $u(l)$. To show that our lower bound for $u(l)$ is an equality when $l = l_0$, we will check the combinatorial condition of Lemma 6.3, but that turns out to be hard. In this section, we only show that the combinatorial condition is satisfied if a certain arithmetic inequality holds (Lemma 8.2). At the end of the section, we check the arithmetic inequality for $c \leq 20$, which confirms Theorem 0.1 for $l < 2^{21+\frac{1}{2}}$, that is, for the spin groups $Spin(n)$ with $n < 2^{22+\frac{1}{2}}$. The last section will prove the arithmetic inequality in general.

The proof in the case $c = 6$ is very special, because in this case, the number $2^{2c} - 1 = 4095$ can be written as $\binom{l+1}{2}$, with $l = 90$, as Ramanujan observed (in a slightly different form). By contrast, Nagell showed that this never happens for c at least 7 [18]. (It is equivalent to solve the diophantine equation $x^2 + 7 = 2^n$, with $n = 2c + 3$.)

The number $l = l_0$ we need to consider is the least integer l such that $\binom{l+1}{2} \geq 2^{2c} - 1$. As we have mentioned, it follows that l is within 1 of $2^{c+\frac{1}{2}}$. We know that $u(l) \geq l - a$, where a denotes $\lfloor \log_2(\binom{l+1}{2} + 1) \rfloor$, which in this case is $2c$. We want to show that $u(l) = l - a$. It is clear from Lemma 6.3 that proving this for $l = l_0$ will imply it for all l from l_0 to $2^{c+1} - 1$, since that is the range of integers which correspond to the given value of a.

Let $l = l_0$. To prove that $u(l) = l - a$, by Lemma 6.3, we need to find a subset I of $\{1, \ldots, l\}$ of degree $\deg(I) = \sum_{i \in I} i$ equal to $2^a - 1 = 2^{2c} - 1$ which can be decomposed into subsets of order at most 2 and of degree a power of 2. This is more difficult than any of the constructions of such subsets we have made until now, because there is no simple formula for $\binom{l+1}{2} - (2^{2c} - 1)$. Indeed, this difference is closely related to the binary expansion of $\sqrt{2}$, since l is within 1 of $2^{c+\frac{1}{2}}$.

To look for such a subset I, let us begin by partitioning the whole set $\{1,\dots,l\}$ into subsets of order at most 2 and of degree a power of 2. There is a unique way to do this, for any l, as one easily checks "from l downward." Namely, this partition has the form:

$$(2^{c_0+1}-x_0,x_0)\cdots(2^{c_0}-1,2^{c_0}+1)(2^{c_0})\ (2^{c_1+1}-x_1,x_1)\cdots(2^{c_1}-1,2^{c_1}+1)(2^{c_1})\ \cdots,$$

where $x_0=l$, $c_0=c$, and

$$\begin{aligned} x_{j+1} &= 2^{c_j+1}-x_j-1\\ c_{j+1} &= \lfloor \log_2 x_{j+1}\rfloor. \end{aligned}$$

The process stops when we reach $x_t=0$; then we adopt the convention that $c_t=-1$. One checks easily that the binary expansion of x_{j+1} is obtained from the binary expansion of x_j by replacing every 0 by 1 and every 1 by 0 (and then removing the zeros in front).

Example. This procedure works very easily to prove Theorem 0.1 in the case $c=6$ mentioned earlier in this section, where $l=90$. (That is, we are proving that the exponent of 2 in the torsion index of $Spin(181)$ is $l-a=90-12=78$, as Theorem 0.1 says.) In this very special case, the sum of the numbers from 1 to l, $\binom{l+1}{2}=4095$, is equal to $2^{2c}-1=2^{12}-1$. So the above procedure shows that the whole set $I:=\{1,\dots,l\}$ has degree $\deg(I)$ equal to $2^{2c}-1$ and can be decomposed into subsets of order at most 2 and of degree a power of 2, as we want. Concretely, we obtain the following decomposition of $I=\{1,\dots,90\}$:

$$(38,90)\dots(63,65)(64)(27,37)\dots(31,33)(32)(6,26)\dots(15,17)(16)(3,5)(4)(2)(1).$$

We return to the above procedure for an arbitrary value of c. Our plan will be to start with the above decomposition of the whole set $\{1,\dots,l\}$ and to reduce the overall degree from $\binom{l+1}{2}$ to $2^{2c}-1$ by operations of the following three types:

(1) remove a two-element set of the form $S=(x,2^b-x)$;

(2) replace a two-element set of the form $T=(2^a,2^b-2^a)$ by the one-element set (2^a);

(3) remove a one-element set of the form $U=(2^a)$.

Here S, T, and U are assumed to occur in the decomposition of the whole set $\{1,\dots,l\}$ which was constructed above.

It is clear that $c_0>c_1>\cdots>c_t=-1$. It may be helpful to point out that the numbers c_j can be read off from the binary expansion of l; a number $d\ge 0$ is equal to some c_j if and only if the coefficient of 2^d differs from that of 2^{d+1}. For our purpose, we need to pay special attention to those values of j such that c_j-c_{j+1} is at least 2. This means that the above partition of $\{1,\dots,l\}$ contains at least one pair of the form $(2^x,2^{c_j+1}-2^x)$: namely, this occurs for all $c_{j+1}+1\le x\le c_j-1$. Let $(a_1,b_1),\dots,(a_r,b_r)$ be the list of all pairs of integers such that the subset $(2^{a_k},2^{b_k}-2^{a_k})$ occurs in the above partition of $\{1,\dots,l\}$. Here $b_k-a_k\ge 2$ for all k. We order these pairs in such a way that $a_1>a_2>\cdots>a_r$. In terms of the binary expansion of l, the number r of these pairs (a_k,b_k) is the number of digits of l which are equal to the preceding digit.

Example. Let us compute the numbers (a_k,b_k) for $c=14$. In this case, we compute that $l=23170$, which is 101101010000010 in binary. Therefore the

numbers c_j, corresponding to the binary digits of l that differ from the preceding digit, are $c = 14$, $c-1 = 13$, $c-2 = 12$, $c-4 = 10$, $c-5 = 9$, $c-6 = 8$, $c-7 = 7$, $c-8 = 6$, $c-13 = 1$, $c-14 = 0$, and $c-15 = -1$. So the pairs (a_k, b_k), corresponding to the binary digits of l that are equal to the preceding digit, are $(11, 13), (5, 7), (4, 7), (3, 7), (2, 7)$.

Here is a first result, showing that we can construct a subset of $\{1, \ldots, l\}$ with the desired properties if the "gap" $\binom{l+1}{2} - (2^{2c} - 1)$ is fairly large. (It seems that this happens for about 3/4 of all c's.)

Lemma 8.1 *Suppose that*

$$\binom{l+1}{2} - (2^{2c} - 1) \geq \sum_k (2^{b_k} - 2^{a_k}).$$

Then there is a subset I of $\{1, \ldots, l\}$ of degree $2^{2c} - 1$ which can be partitioned into subsets of order at most 2 and of degree a power of 2. Therefore, $u(l) = l - a$.

Proof. Consider the partition of the whole set $\{1, \ldots, l\}$ constructed above. Let us replace all the pairs of the form $(2^{a_k}, 2^{b_k} - 2^{a_k})$ in this partition by (2^{a_k}). The inequality assumed in this lemma means that the resulting subset I of $\{1, \ldots, l\}$ still has degree at least $2^{2c} - 1$. Also, I comes with a partition into subsets of order at most 2 and of degree a power of 2. Finally, by the construction of I, this partition of I includes the singleton (2^j) for all $0 \leq j \leq c$.

Let us then remove pairs $(j, 2^k - j)$ (note that we always have $k \leq c + 1$ here) from the given partition of I as long as possible while keeping the degree of the resulting set J at least $2^{2c} - 1$. When we stop, the degree of J must be at most $(2^{2c} - 1) + (2^{c+1} - 1)$ (otherwise we could remove more). Therefore, by removing some of the singletons (2^j) for $0 \leq j \leq c$ from J, we can find a subset K of J which has degree equal to $2^{2c} - 1$, and which has a partition of the kind we want. This implies that $u(l) = l - a$ by Lemma 6.3. QED

Since the hypothesis of Lemma 8.1 does not hold for all values of c, we will need an additional approach. Let s be the smallest nonnegative integer such that

$$\binom{l+1}{2} - (2^{2c} - 1) \geq \sum_{k>s} (2^{b_k} - 2^{a_k}).$$

Clearly such an s exists, since the inequality holds at least when $s = r$ (where the pairs (a_k, b_k) are indexed by $1 \leq k \leq r$). The condition that $s = 0$ is exactly the hypothesis of Lemma 8.1. If $s > 0$, then let i denote the unique number such that $b_s = c_i + 1$. The following lemma will be our tool for proving Theorem 0.1 for all values of c, whether $s = 0$ or not.

Lemma 8.2 *Given $c \geq 2$, let $l = l_0 \doteq 2^{c+\frac{1}{2}}$. Define s, i as above. Suppose that either $s = 0$ or $s > 0$, $c_i < 2c_{i+1} - 2$, and $c_{i+1} \geq 6$. Then there is a subset I of $\{1, \ldots, l\}$ of degree $2^{2c} - 1$ which can be partitioned into subsets of order at most 2 and of degree a power of 2. Therefore, $u(l) = l - a$.*

Proof. For $s = 0$, this is Lemma 8.1. So we can assume that $s > 0$, $c_i < 2c_{i+1} - 2$, and $c_{i+1} \geq 6$. By definition of s, we know that

$$\binom{l+1}{2} - (2^{2c} - 1) \geq \sum_{k>s} (2^{b_k} - 2^{a_k}).$$

We begin with the decomposition, constructed early in this section, of the whole set $\{1,\dots,l\}$ into subsets of order at most 2 and of degree a power of 2. Then replace the pairs $(2^{a_k}, 2^{b_k}-2^{a_k})$ with $k>s$ by (2^{a_k}). This gives a partition of a subset I of $\{1,\dots,l\}$ into the same type of subsets. The above inequality shows that I has degree at least $2^{2c}-1$. Moreover, because $a_1>\cdots>a_r$, the given partition of I includes the singleton (2^i) for all $0\le i<a_s$.

Because s is the smallest number which satisfies the above inequality, we know that the degree of I is not much larger than $2^{2c}-1$; precisely, we have

$$|I|-(2^{2c}-1)<2^{b_s}-2^{a_s}.$$

Let us remove two-element subsets $(j,2^k-j)$ from the partition of I as long as possible while keeping the degree of the resulting set J at least $2^{2c}-1$. Here all the pairs $(j,2^k-j)$ that we remove from I will automatically have $k\le c_{i+1}+1$. Indeed, the possible values of k are all of the form c_j+1, where $c_0>c_1>\cdots>c_t=-1$, and if we removed a pair $(j,2^k-j)$ from I with $k\ge c_i+1=b_s$, then the degree of the resulting set would be less than $2^{2c}-1$, by the above inequality.

Suppose that our partition of the set J still contains some pair $(j,2^k-j)$ with $k\le c_{i+1}+1$. Then the definition of J implies that the degree of J is very close to $2^{2c}-1$, in the sense that

$$|J|-(2^{2c}-1)\le 2^{c_{i+1}+1}-1.$$

The definition of the pairs (a_j,b_j), plus our convention that $b_s=c_i+1$, implies that

$$c_{i+1}+1\le a_s\le c_i-1.$$

Therefore,

$$|J|-(2^{2c}-1)\le 2^{a_s}-1.$$

Our partition of J still contains all the singletons (2^j) for $0\le j<a_s$, as the partition of I did. So this inequality shows that we can reduce the degree of J to $2^{2c}-1$ by removing some of these singletons (2^j) from our partition of J. Thus the lemma is proved in this case (where our partition of J still contains some pair $(j,2^k-j)$ with $k\le c_{i+1}+1$).

Thus, we can assume that our partition of J contains no pair $(j,2^k-j)$ with $k\le c_{i+1}+1$. We will derive a contradiction in this case, using the hypotheses of the lemma.

By the construction of our original partition of $\{1,\dots,l\}$, since our partition of J contains no pair $(j,2^k-j)$ with $k\le c_{i+1}+1$, it follows that the subset J of $\{1,\dots,l\}$ contains no positive integers at most x_{i+1} other than powers of 2. We will now show that we must have removed many numbers at most x_{i+1} in passing from I to J. We first have to observe that the subset I of $\{1,\dots,l\}$ still contains most of the numbers at most x_{i+1}. Namely, by the construction of I, we removed at most c_{i+1} of the numbers at most x_{i+1} from the set $\{1,\dots,l\}$ to form I (as well as, possibly, removing some larger numbers). Thus the degree of the set $I\cap\{1,\dots,x_{i+1}\}$ satisfies

$$|I\cap\{1,\dots,x_{i+1}\}|\ge\binom{x_{i+1}+1}{2}-c_{i+1}x_{i+1}.$$

On the other hand, since J contains no positive integers at most x_{i+1} other than powers of 2, we have (remembering that $c_{i+1} = \lfloor \log_2 x_{i+1} \rfloor$):

$$|J \cap \{1, \ldots, x_{i+1}\}| \leq 2^{c_{i+1}+1} - 1.$$

By comparing these two inequalities, we deduce that the subset J of I satisfies:

$$|I| - |J| \geq \binom{x_{i+1}+1}{2} - c_{i+1}x_{i+1} - 2^{c_{i+1}+1} + 1.$$

On the other hand, the subset I has degree not much larger than $2^{2c} - 1$, in the sense that

$$|I| - (2^{2c} - 1) < 2^{b_s} - 2^{a_s},$$

while we have also arranged that

$$|J| - (2^{2c} - 1) \geq 0.$$

Therefore $|I| - |J|$ is less than $2^{b_s} - 2^{a_s}$. Combining this with the previous paragraph gives the inequality:

$$\binom{x_{i+1}+1}{2} - c_{i+1}x_{i+1} - 2^{c_{i+1}+1} + 1 < 2^{b_s} - 2^{a_s}.$$

On the other hand, we can prove the opposite inequality, giving the desired contradiction. We are assuming that $c_i < 2c_{i+1} - 2$ and $c_{i+1} \geq 6$. Since c_i is an integer, it follows that $b_s = c_i + 1 \leq 2c_{i+1} - 2$. We have $a_s \geq c_{i+1} + 1$, and so

$$2^{b_s} - 2^{a_s} \leq 2^{2c_{i+1}-2} - 2^{c_{i+1}+1}.$$

Also, $x_{i+1} \geq 2^{c_{i+1}}$ and $x_{i+1} < 2^{c_{i+1}+1}$. So the left side of the previous paragraph's inequality is at least

$$\begin{aligned} &\geq \binom{2^{c_{i+1}}+1}{2} - c_{i+1}2^{c_{i+1}+1} - 2^{c_{i+1}+1} + 1 \\ &= 2^{2c_{i+1}-1} + 2^{c_{i+1}-1} - (c_{i+1}+1)2^{c_{i+1}+1} + 1. \end{aligned}$$

Thus, to prove the opposite of the previous paragraph's inequality, it suffices to show that

$$2^{2c_{i+1}-2} - 2^{c_{i+1}+1} \leq 2^{2c_{i+1}-1} + 2^{c_{i+1}-1} - (c_{i+1}+1)2^{c_{i+1}+1} + 1,$$

that is, that

$$c_{i+1}2^{c_{i+1}+1} \leq 2^{2c_{i+1}-2} + 2^{c_{i+1}-1} + 1.$$

This clearly holds if $c_{i+1} \leq 2^{c_{i+1}-3}$. But that follows from our assumption that $c_{i+1} \geq 6$. QED

We are only considering values of c at least 2. Let us now consider the cases $2 \leq c \leq 20$. We list $l = l_0 \doteq 2^{c+\frac{1}{2}}$ in the following table. We see that the binary

expansion of l is close to that of $\sqrt{2}$, as it should be.

c	l	$\binom{l+1}{2} - (2^{2c}-1)$	$\sum_k (2^{b_k} - 2^{a_k})$	l in binary
2	5	0	0	101
3	11	3	3	1011
4	23	21	13	10111
5	45	12	12	101101
6	90	0	24	1011010
7	181	88	48	10110101
8	362	168	96	101101010
9	724	307	195	1011010100
10	1448	501	397	10110101000
11	2896	553	809	101101010000
12	5793	5106	1618	1011010100001
13	11585	3042	3298	10110101000001
14	23170	580	6596	101101010000010
15	46341	25488	13192	1011010100000101
16	92682	55608	26384	10110101000001010
17	185364	129747	52771	101101010000010100
18	370728	333621	105549	1011010100000101000
19	741455	222297	211161	10110101000001001111
20	1482910	147730	422322	101101010000010011110

Here the expression $\sum_k (2^{b_k} - 2^{a_k})$ is easy to compute, from its definition: the sum has one term for each binary digit of l which is equal to the preceding digit of l.

In all the cases $2 \le c \le 5$, $7 \le c \le 10$, $c = 12$, and $15 \le c \le 19$, we see that the gap $\binom{l+1}{2} - (2^{2c}-1)$ is "large", in the sense that it is at least $\sum_k (2^{b_k} - 2^{a_k})$. That means that the number s we defined is 0, and so the condition in Lemma 8.2 holds. Thus $u(l) = l - a$ in all the cases mentioned.

The case $c = 6$ is exceptional. In this case, we have $l = 90$, and $\binom{l+1}{2} = 4095$ is actually equal to $2^{2c} - 1$. The first Example above shows that $u(l) = l - a$, thus proving Theorem 0.1 in this case. It happens that the condition in Lemma 8.2 fails in the case $c = 6$: we have $s > 0$, $c_i = c - 2 = 4$, $c_{i+1} = c - 4 = 2$, and so the inequality $c_i < 2c_{i+1} - 2$ fails; but that does not matter for our purpose.

Finally, for $c = 11$, 13, 14, or 20, we have $s > 0$; in each case, we compute that $s = 1$, $c_i = c - 2$ and $c_{i+1} = c - 4$. For example, let $c = 14$, which is the case that comes closest to failing. Here $\binom{l+1}{2} - (2^{2c}-1) = 580$, while the sum $\sum_k (2^{b_k} - 2^{a_k})$ is

$$(2^{13} - 2^{11}) + (2^7 - 2^5) + (2^7 - 2^4) + (2^7 - 2^3) + (2^7 - 2^2),$$

as we read off from the binary expansion of l (cf. the second Example above). We have $s > 0$ because this sum is 6596, which is greater than 580. But the sum of the last four terms is only 452, which is at most 580, and so we have $s = 1$. We read from the omitted term $(2^{13} - 2^{11})$ that $c_i = 12 = c - 2$ and $c_{i+1} = 10 = c - 4$, as claimed.

It follows that, in the cases $c = 11$, 13, 14, or 20, we have $c_i < 2c_{i+1} - 2$ and $c_{i+1} \ge 6$; that is, the condition in Lemma 8.2 holds. We have now shown that $u(l) = l - a$ for all $2 \le c \le 20$, where $l = l_0 \doteq 2^{c+\frac{1}{2}}$. Thus Theorem 0.1 is proved for all $l < 2^{21+\frac{1}{2}}$.

9 Proof of the arithmetic inequality

By the discussion at the beginning of section 8, Theorem 0.1 will be proved if we can show that for all $c \geq 21$, if we let $l = l_0 \doteq 2^{c+\frac{1}{2}}$, then the condition in Lemma 8.2 holds. As will become apparent, this condition holds if the first c or so digits of the binary expansion of $\sqrt{2}$ do not contain excessively long sequences of zeros or ones. We will prove this for $c \geq 326$ using Bauer and Bennett's general theorem bounding the length of sequences of zeros or ones in the binary expansion of $\sqrt{2}$ [1]. For $21 \leq c \leq 325$, their general theorem is not strong enough for our purpose, but we can prove what we want by inspecting the first 330 binary digits of $\sqrt{2}$.

Notice that Bauer and Bennett's theorem is asymptotically much weaker than the truth. Namely, Ridout's p-adic version of the Thue-Siegel-Roth theorem [23] implies that the inequality

$$\left|\sqrt{2} - \frac{y}{2^n}\right| \leq (2^n)^{-1-\epsilon}$$

has only finitely many solutions in positive integers, for any $\epsilon > 0$. Equivalently, the maximum length of any sequence of zeros or ones in the first n digits of the binary expansion of $\sqrt{2}$ is $o(n)$, as one would expect. The problem is that, like the original Thue-Siegel-Roth theorem, Ridout's theorem is not effective. We need Bauer and Bennett's explicit result that the only solutions of the inequality

$$\left|\sqrt{2} - \frac{y}{2^n}\right| \leq (2^n)^{-1.48}$$

with $n > 3$ are those with $n = 7$ or $n = 8$ ([1], Corollary 1.6). Roughly, this says that the maximum length of any sequence of zeros or ones in the first n digits of $\sqrt{2}$ is at most $(0.48/1.48)n$, thus at most $(0.32)n$, apart from a surprising sequence of 5 zeros early in the binary expansion of $\sqrt{2}$ (listed a few pages ahead).

For each $c \geq 21$, let $l = l_0 \doteq 2^{c+\frac{1}{2}}$. We want to show that the condition in Lemma 8.2 holds. That is, we assume that $s > 0$, and we want to show that $c_i < 2c_{i+1} - 2$ and $c_{i+1} \geq 6$. We will first do this in the case $c \geq 326$. Since we assume that $s > 0$, we know that

$$b_s - 2 = c_i - 1 \leq a_s \leq c_{i+1} + 1,$$

and so $c_{i+1} \leq c_i - 2$.

By definition of s, since $s > 0$, we know that

$$\binom{l+1}{2} - (2^{2c} - 1) < \sum_{k \geq s} (2^{b_k} - 2^{a_k}).$$

Here we have $b_s \geq b_{s+1} \geq \cdots$, by definition of this sequence. Also, $a_s > a_{s+1} > \cdots > a_r \geq 0$, and so the number of terms in the above sum is at most $a_s + 1$, hence at most c_i. We deduce the following crude bound:

$$\binom{l+1}{2} - (2^{2c} - 1) < c_i 2^{c_i+1}.$$

The Bauer-Bennett theorem implies that $l + \frac{1}{2}$ cannot be too close to $2^{c+\frac{1}{2}}$; combining this with the previous inequality will imply that c_i must be at least

about $c/2$ for c large. First, the above inequality implies the following sequence of inequalities:

$$\begin{aligned} 4l(l+1) &< 2^{2c+3} + c_i 2^{c_i+4} - 8 \\ (2l+1)^2 &< 2^{2c+3} + c_i 2^{c_i+4} - 7 \\ &< 2^{2c+3} + c_i 2^{c_i+4} \\ \left(\frac{2l+1}{2^{c+1}}\right)^2 &< 2 + c_i 2^{c_i+2-2c} \\ \frac{2l+1}{2^{c+1}} &< \sqrt{2} + c_i 2^{c_i+0.5-2c}. \end{aligned}$$

In the last step we use that if $x^2 \leq y + e$ with x, y, e positive, then $x \leq \sqrt{y} + e/(2\sqrt{y})$. Also, it is clear that $(2l+1)/2^{c+1}$ is at least $\sqrt{2}$, just using that the "gap" $\binom{l+1}{2} - (2^{2c} - 1)$ is at least 2: it is clearly not 1, and it is not 0 for $c \geq 7$ by Nagell [18]. So the above inequality gives an upper bound for $|\sqrt{2} - (2l+1)/2^{c+1}|$. Here $c+1$ is greater than 8 since we are assuming $c \geq 326$. So we can apply Bauer and Bennett's theorem to deduce that

$$c_i 2^{c_i+0.5-2c} > 2^{-1.48(c+1)},$$

and hence

$$c_i 2^{c_i+0.5} > 2^{0.52c-1.48}.$$

This inequality implies that c_i is at least about $c/2$ for c large. Precisely, we can use our assumption that $c \geq 326$ to deduce that

$$(0.98)c_i > (0.48)c + 0.52 + 0.005,$$

which is the inequality we will need later.

To prove that $c_i < 2c_{i+1} - 2$, we will need to use Bauer and Bennett's theorem again. In section 8, we defined $x_0 = l \doteq 2^{c+\frac{1}{2}}$, $c_0 = c$, and

$$\begin{aligned} x_{i+1} &= 2^{c_i+1} - x_i - 1 \\ c_{i+1} &= \lfloor \log_2 x_{i+1} \rfloor. \end{aligned}$$

Therefore we have:

$$\begin{aligned} x_0 &= 2^{c_0+1} - x_1 - 1 \\ &= 2^{c_0+1} - 2^{c_1+1} + x_2 \\ &= \cdots \\ &= 2^{c_0+1} - 2^{c_1+1} + \cdots + (-1)^i 2^{c_i+1} + (-1)^{i+1} x_{i+1} + \begin{cases} -1 & \text{if } i \text{ is even} \\ 0 & \text{if } i \text{ is odd} \end{cases}. \end{aligned}$$

Here $|2^{c+\frac{1}{2}} - x_0| < 1$. Therefore, dividing the above equation by 2^c yields the existence of an integer y such that:

$$\left|\sqrt{2} - \frac{y}{2^{c-c_i-1}}\right| < \frac{x_{i+1}+2}{2^c}.$$

We can also use the above equation for x_0 to prove that the numbers c_j are very close to the numbers d_j which form the "signed binary expansion" of $\sqrt{2}$:

$$\begin{aligned}2^{c+\frac{1}{2}} &= 2^{d_0+1} - 2^{d_1+1} + 2^{d_2+1} - \cdots \\ &= 2^{c+1} - 2^{(c-1)+1} + 2^{(c-2)+1} - 2^{(c-4)+1} + 2^{(c-5)+1} - 2^{(c-6)+1} + 2^{(c-7)+1} - 2^{(c-8)+1} \\ &\quad + 2^{(c-13)+1} - \cdots .\end{aligned}$$

To be precise, the above equation for x_0 plus the fact that $|2^{c+\frac{1}{2}} - x_0| < 1$ imply the following statement, as one checks directly.

Lemma 9.1 *Let j be an even number such that d_{j+1} is nonnegative. Then $c_k = d_k$ for $0 \le k \le j$.*

Let us first prove that $c_i < 2c_{i+1} - 2$ on the assumption that $c_i \ge c - 9$. Since $c \ge 326$, Lemma 9.1 shows that the numbers c_j coincide with the numbers d_j in this range, as listed above. That is, the numbers c_j begin: $c, c-1, c-2, c-4, c-5, c-6, c-7, c-8, c-13$. We know that $c_{i+1} \le c_i - 2$ by our assumption that $s > 0$, as mentioned at the beginning of this section. So either c_i is $c-2$ and c_{i+1} is $c-4$, or c_i is $c-8$ and c_{i+1} is $c-13$. In both cases, we have $c_i < 2c_{i+1} - 2$ as claimed, using that $c \ge 326$. This proves the desired inequality when $c_i \ge c - 9$.

On the other hand, when $c_i < c-9$, we can apply Bauer and Bennett's theorem to the above inequality for $|\sqrt{2} - y/2^{c-c_i-1}|$. It follows that

$$\log_2(x_{i+1} + 2) - c \ge -(1.48)(c - c_i - 1).$$

Since $c_{i+1} = \lfloor \log_2 x_{i+1} \rfloor$, we have $x_{i+1} + 2 \le 2^{c_{i+1}+1} + 1$ and so

$$\log_2(x_{i+1} + 2) \le c_{i+1} + 1 + \frac{1}{2^{c_{i+1}+1} \log 2}.$$

Therefore

$$c_{i+1} + \frac{1}{2^{c_{i+1}+1} \log 2} \ge (1.48)c_i - (0.48)c + 0.48.$$

We showed earlier that $(0.98)c_i > (0.48)c + 0.52 + 0.005$. Inserting this into the above inequality shows that

$$c_{i+1} + \frac{1}{2^{c_{i+1}+1} \log 2} > (0.5)c_i + 1 + 0.005.$$

Since $c \ge 326$, our inequality between c_i and c implies that $c_i \ge 161$ (as c_i is an integer), and then this last inequality implies that $c_{i+1} \ge 81$. In particular, c_{i+1} is at least 6, which is part of the condition in Lemma 8.2.

Moreover, this lower bound for c_{i+1} implies that the fraction in the above inequality is much smaller than 0.005, and so we deduce the simpler inequality:

$$c_{i+1} > (0.5)c_i + 1.$$

Equivalently, we have shown that $c_i < 2c_{i+1} - 2$. This completes the proof that the condition in Lemma 8.2 holds for all $c \ge 326$.

We now turn to the proof for $c \le 325$. We need to inspect the first 330 binary digits of $\sqrt{2}$ after the decimal point, listed here.

1.01101 01000 00100 11110 01100 11001 11111 10011 10111 10011 00100 10000 10001 01100
10111 11011 00010 01101 10011 01110 10101 00101 01011 11101 00111 11000 11101 01101
11101 10000 01011 10101 00010 01001 11011 10101 00001 00110 01110 11010 00101 11101
01100 10000 10110 00001 10011 00111 00110 01000 10101 01001 01011 11110 01000 00110
00001 00001 11010 10111 00010 10001 01100 00111 01010 00101 ...

We see that all strings of consecutive zeros or ones in this range have length at most 7. In particular, all strings of zeros or ones which start at the jth digit after the decimal point with $j \leq 329$ have length at most 7. Equivalently, for all integers y and all $0 \leq j \leq 328$,

$$\left|\sqrt{2} - \frac{y}{2^j}\right| \geq \frac{1}{2^{j+8}}.$$

We now prove the theorem for $27 \leq c \leq 325$, replacing our two uses of the Bauer-Bennett theorem by the above calculation. For each c, if $s = 0$ then the condition of Lemma 8.2 holds, and so we assume that $s > 0$. First, as in the argument for $c \geq 326$, we have

$$\left|\sqrt{2} - \frac{2l+1}{2^{c+1}}\right| < c_i 2^{c_i + 0.5 - 2c},$$

and so the above estimate gives that

$$c_i 2^{c_i + 0.5 - 2c} \geq 2^{-(c+1)-8}.$$

Equivalently, $c_i \geq c - 9.5 - \log_2 c_i$. Here $c_i \leq c \leq 325$, and so $\log_2 c_i < 8.5$. It follows that $c_i > c - 18$, and hence $c_i \geq c - 17$ since these are integers.

We can read off from the beginning of the binary expansion of $\sqrt{2}$ that the signed binary expansion of $\sqrt{2}$ begins as follows:

$$\begin{aligned} 2^{c+\frac{1}{2}} &= 2^{d_0+1} - 2^{d_1+1} + 2^{d_2+1} - \cdots \\ &= 2^{c+1} - 2^{(c-1)+1} + 2^{(c-2)+1} - 2^{(c-4)+1} + 2^{(c-5)+1} - 2^{(c-6)+1} + 2^{(c-7)+1} - 2^{(c-8)+1} \\ &\quad + 2^{(c-13)+1} - 2^{(c-14)+1} + 2^{(c-16)+1} - 2^{(c-20)+1} + 2^{(c-22)+1} - 2^{(c-24)+1} + \cdots . \end{aligned}$$

Since we are assuming that $c \geq 27$, the last number d_j shown here, $d_{13} = c - 24$, is nonnegative. By Lemma 9.1, all the earlier numbers d_j coincide with the corresponding numbers c_j. That is, the numbers c_j begin: $c, c-1, c-2, c-4, c-5, c-6, c-7, c-8, c-13, c-14, c-16, c-20, c-22$.

We have $c_i \geq c - 17$, so c_i is one of the numbers $c, c-1, \ldots, c-16$, and we know the corresponding number c_{i+1}. From this, we can read off that $c_i < 2c_{i+1} - 2$, using that $c \geq 27$. Also, we see that $c_{i+1} \geq c - 20 \geq 7 \geq 6$. Thus the condition of Lemma 8.2 is proved for all $c \geq 27$.

Similar arguments prove the condition of Lemma 8.2 for $21 \leq c \leq 27$. We observe that all strings of zeros or ones in the binary expansion of $\sqrt{2}$ starting at place j after the decimal point with $j \leq 29$ have length at most 5. This gives a lower bound for c_i, by the same argument as above:

$$c_i \geq c - 7.5 - \log_2 c_i.$$

Here $c_i \le c \le 27$, and so $\log_2 c_i < 5$. It follows that $c_i \ge c - 12.5$, and hence $c_i \ge c - 12$ since these are integers.

Since $c \ge 21$, the number $d_{11} = c - 20$ in the signed binary expansion of $\sqrt{2}$ is nonnegative. By Lemma 9.1, the numbers d_j before this one are equal to the corresponding c_j's. That is, the numbers c_j begin: $c, c-1, c-2, c-4, c-5, c-6, c-7, c-8, c-13, c-14, c-16$. Since $c_i \ge c-12$, c_i is one of these numbers $c, \dots, c-8$, and we know what the corresponding number c_{i+1} is. From this, we can read off that $c_i < 2c_{i+1} - 2$, using that $c \ge 21$. Also, we see that $c_{i+1} \ge c - 13 \ge 8 \ge 6$.

Thus the condition of Lemma 8.2 holds for all $c \ge 21$. As discussed at the beginning of Section 8, this completes the proof of Theorem 0.1. QED

References

[1] M. Bauer and M. Bennett. Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation. *Ramanujan J.* **6** (2002), 209–270.

[2] D. Benson and J. Wood. Integral invariants and cohomology of $BSpin(n)$. *Topology* **34** (1995), 13–28.

[3] P. Berthelot and A. Ogus. *Notes on crystalline cohomology.* Princeton (1978).

[4] A. Borel. Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes. *Tohoku Math. J.* **13** (1961), 216–240.

[5] M. Demazure. Invariants symétriques entiers des groupes de Weyl et torsion. *Invent. Math.* **21** (1973), 287–301.

[6] M. Florence. Zéro-cycles de degré un sur les espaces homogènes. *Int. Math. Res. Notices* **54** (2004), 2897–2914.

[7] E. Friedlander. Maps between localized homogeneous spaces. *Topology* **16** (1977), 205–216.

[8] W. Fulton. *Intersection theory.* Berlin: Springer (1984).

[9] R. S. Garibaldi, A. Merkurjev, and J.-P. Serre. *Cohomological invariants in Galois cohomology.* Providence: AMS (2003).

[10] A. Grothendieck. Torsion homologique et sections rationnelles. Exposé 5 in *Anneaux de Chow et applications. Séminaire C. Chevalley 1958.* Paris (1958).

[11] N. Kitchloo, G. Laures, and W. S. Wilson. The Morava K-theory of spaces related to BO. *Adv. Math.,* to appear.

[12] A. Kono. On the integral cohomology of $BSpin(n)$. *J. Math. Kyoto Univ.* **26** (1986), 333–337.

[13] A. Kono and N. Yagita. Brown-Peterson and ordinary cohomology theories of classifying spaces for compact Lie groups. *Trans. AMS* **339** (1993), 781–798.

[14] R. Marlin. Anneaux de Chow des groupes algébriques $SU(n)$, $Sp(n)$, $SO(n)$, $Spin(n)$, G_2, F_4; torsion. *C. R. Acad. Sci. Paris* **279** (1974), 119–122.

[15] A. Merkurjev. Maximal indexes of Tits algebras. *Doc. Math.* **1** (1996), 229–243.

[16] M. Mimura and H. Toda. *Topology of Lie groups.* Providence: AMS (1991).

[17] F. Morel and V. Voevodsky. A^1-homotopy theory of schemes. *Publ. Math. IHES* **90** (1999), 45–143.

[18] T. Nagell. The diophantine equation $x^2 + 7 = 2^n$. *Nordisk Mat. Tidskr.* **30** (1948), 62–64; *Ark. Math.* **4** (1961), 185–187.

[19] R. Parimala. Homogeneous varieties – zero cycles of degree one versus rational points. Preprint (2004).

[20] A. Pfister. Quadratische Formen in beliebigen Körpern. *Invent. Math.* **1** (1966), 116–132.

[21] D. Quillen. The mod 2 cohomology rings of extra-special 2-groups and the spinor groups. *Math. Ann.* **194** (1971), 197–212.

[22] Z. Reichstein and B. Youssin. Splitting fields of G-varieties. *Pac. J. Math.* **200** (2001), 207–249.

[23] D. Ridout. The p-adic generalization of the Thue-Siegel-Roth theorem. *Mathematika* **5** (1958), 40–48.

[24] J.-P. Serre. Cohomologie galoisienne: progrés et problèmes. *Séminaire Bourbaki 1993/94,* exposé 783, Astérisque **227** (1995), 229–257; also in *Oeuvres,* v. 4, 443–471.

[25] J. Tits. Sur les degrés des extensions de corps déployant les groupes algébriques simples. *C. R. Acad. Sci. Paris* **315** (1992), 1131–1138.

[26] B. Totaro. The Chow ring of a classifying space. *Algebraic K-theory*, ed. W. Raskind and C. Weibel. Proc. Symp. Pure Math. **67** (1999), 249–281.

[27] B. Totaro. Splitting fields for E_8-torsors. *Duke Math. J.* **121** (2004), 425-455.

[28] J. A. Wood. Spinor groups and algebraic coding theory. *J. Combin. Theory* A **51** (1989), 277–313.

DPMMS, Wilberforce Road, Cambridge CB3 0WB, England
b.totaro@dpmms.cam.ac.uk