Forum of Mathematics, Sigma (2025), **Vol. 13**:e162 1–16
doi:10.1017/fms.2025.10116

RESEARCH ARTICLE

Vanishing of Schubert coefficients via the effective Hilbert nullstellensatz

Igor Pak [1] and Colleen Robichaux [2]

[1]Department of Mathematics, University of California, Los Angeles, Los Angeles, 90095 CA, USA; E-mail: pak@math.ucla.edu.
[2]Department of Mathematics, University of California, Los Angeles, Los Angeles, 90095 CA, USA;
E-mail: robichaux@math.ucla.edu (Corresponding author).

Received: 5 May 2025; **Revised:** 5 August 2025; **Accepted:** 5 August 2025

2020 Mathematics Subject Classification: *Primary* – 05E14; *Secondary* – 14M15, 14N15, 68Q17, 68Q25, 90C27

Abstract
Schubert Vanishing is a problem of deciding whether Schubert coefficients are zero. Until this work it was open whether this problem is in the polynomial hierarchy PH. We prove this problem is in $\mathsf{AM} \cap \mathsf{coAM}$ assuming the *Generalized Riemann Hypothesis* (GRH), that is, relatively low in PH. Our approach uses Purbhoo's criterion [57] to construct explicit polynomial systems for the problem. The result follows from a reduction to *Parametric Hilbert's Nullstellensatz*, recently analyzed in [2]. We extend our results to all classical types.

Contents

1. Introduction

1.1. Foreword

The *Schubert vanishing problem* asks whether Schubert structure constants (*Schubert coefficients*) are zero. This is one of the oldest problems in enumerative geometry, going back to Schubert's original work in the 1870s. Fundamentally, it is about the existence of certain configurations of complex lines, planes, etc., with given dimensions of intersections; see, for example, [31]. Motivated in part by *Hilbert's 15th Problem* aiming to make Schubert's work rigorous (see [30]), the area of Schubert calculus has exploded and developed rich connections with representation theory and algebraic combinatorics (see [3, 34]).

Despite a large body of numerical work, see, for example, [25, 24, 42], the complexity analysis of the problem has been entirely missing, see [11, p. 41]. In this paper we give the first such analysis, placing the Schubert vanishing problem in the complexity class $\mathsf{AM} \cap \mathsf{coAM}$ assuming the GRH (Main Theorem 1.1), that is, relatively low in the polynomial hierarchy PH. Until now, it was not known whether the problem is in PH. This result has a number of combinatorial and complexity implications, notably that Schubert vanishing is unlikely to be NP-hard (Corollary 1.5).

The proof is entirely algebraic and uses concise reductions of the Schubert vanishing problem and its negation to instances of *Hilbert's Nullstellensatz* (HN) over function fields. From this point, the complexity theoretic heavy lifting was done by Koiran [37, 38] and Ait El Manssour et al. [2], who showed that HN is in AM assuming the GRH. The surprising part is that we have two reductions rather than just one, suggesting that there is no *Murphy's law* (universality theorem) for the Schubert vanishing, cf. [46, 63].

Our own motivation comes from the problem of finding a *combinatorial interpretation* for the Schubert coefficients, one of the most celebrated open problems in algebraic combinatorics [61, Problem 11]. In the complexity language, having a combinatorial interpretation implies that *Schubert positivity* (nonvanishing) is in the complexity class NP, see [48, §10]. Our results imply this conclusion, modulo GRH and standard derandomization assumptions (see also §4.4).

Finally, we note that Schubert vanishing is of interest in its own right, independent of geometric considerations, in part because Schubert positivity (nonvanishing) is asymptotically rare (see §4.3). Additionally, positivity of Schubert coefficients is the main assumption in the *generalized Horn inequalities*, see, for example, [4, 7, 8]. In his 2022 ICM paper, Knutson emphasized the importance of the Schubert vanishing problem as follows: *"For applications (including real-world engineering applications) it is more important to know that* [Schubert] *structure constant is positive, than it is to know its actual value"* [34, §1.4].

1.2. Schubert coefficients

We start with a general setup, see, for example, [3] for the background and §2.1 for standard notation. Let G be a complex reductive Lie group. Take $\mathsf{B} \subset \mathsf{G}$ and $\mathsf{B}_- \subset \mathsf{G}$ to be the Borel subgroup and opposite Borel subgroup, respectively. The *torus subgroup* is defined as $\mathsf{T} = \mathsf{B} \cap \mathsf{B}_-$. The *Weyl group* is defined as the normalizer $\mathcal{W} \cong N_{\mathsf{G}}(\mathsf{T})/\mathsf{T}$. The *Bruhat decomposition* states that

$$\mathsf{G} = \bigsqcup_{w \in \mathcal{W}} \mathsf{B}_- \, \dot{w} \, \mathsf{B},$$

where $\dot{w}$ is the preimage of w in the normalizer $N_{\mathsf{G}}(\mathsf{T})$.

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

The *generalized flag variety* is defined as G/B. Recall that G/B has finitely many orbits under the left action of B_-. These are called *Schubert cells* and denoted Ω_w. Schubert cells are indexed by the Weyl group elements $w \in \mathcal{W}$.

The *Schubert varieties* X_w are the Zariski closures of Schubert cells Ω_w. The *Schubert classes* $\{\sigma_w\}_{w\in\mathcal{W}}$ are the Poincaré duals of Schubert varieties. These form a $\mathbb{Z}$-linear basis of the cohomology ring $H^*(\mathsf{G}/\mathsf{B})$. The *Schubert coefficients* $c^w_{u,v}$ are defined as structure constants:

$$\sigma_u \smile \sigma_v \ = \ \sum_{w\in\mathcal{W}} c^w_{u,v}\, \sigma_w\,. \tag{1.1}$$

Thus $c^w_{u,v} = [\sigma_{\mathrm{id}}]\,\sigma_u \smile \sigma_v \smile \sigma_{w_\circ w}$, where $w_\circ$ is the *long word* in $\mathcal{W}$, see §2.3. Generalizing, we take

$$c(u_1, u_2, \ldots, u_k) \ := \ [\sigma_{\mathrm{id}}]\ \sigma_{u_1} \smile \sigma_{u_2} \smile \cdots \smile \sigma_{u_k}, \tag{1.2}$$

where $k \geq 3$. In particular, we have $c^w_{u,v} = c(u, v, w_\circ w)$. By commutativity of $H^*(\mathsf{G}/\mathsf{B})$, Schubert coefficients $c(u_1, \ldots, u_k)$ exhibit S_k-symmetry.

By *Kleiman transversality* [29], the coefficients $c(u_1, \ldots, u_k)$ count the number of points in the intersection of generically translated Schubert varieties:

$$c(u_1, \ldots, u_k) \ = \ \#\big\{\, X_{u_1}\big(F^{(1)}_\bullet\big) \cap \cdots \cap X_{u_k}\big(F^{(k)}_\bullet\big)\,\big\}, \tag{1.3}$$

where $X_{u_i}\big(F^{(i)}_\bullet\big)$ is the Schubert variety X_{u_i} translated by a generic flag $F^{(i)}_\bullet$. In particular, we have $c(u_1, \ldots, u_k) \in \mathbb{N}$. The *Schubert vanishing problem* is a decision problem

$$\textsc{SchubertVanishing} \ := \ \big\{ c(u_1, \ldots, u_k) \stackrel{?}{=} 0 \big\},$$

where $u_1, \ldots, u_k \in \mathcal{W}$. We consider the problem only for classical types $Y \in \{A, B, C, D\}$, and use the notation $\textsc{SchubertVanishing}(Y)$ to denote the Schubert vanishing problem in type Y.[1] These correspond to considering $\mathsf{G} \in \{\mathsf{SL}_n(\mathbb{C}), \mathsf{SO}_{2n+1}(\mathbb{C}), \mathsf{Sp}_{2n}(\mathbb{C}), \mathsf{SO}_{2n}(\mathbb{C})\}$, respectively.

1.3. Main results

Recall the complexity class AM of decision problems whose "yes" answers can be decided in polynomial time by an *Arthur–Merlin protocol* with two messages, see, for example, [6, 20]. Heuristically, one should think of the class AM as a (nonobvious) probabilistic extension of the class NP. The complexity class coAM is the complement of languages in AM, that is, the decision problems whose "no" answers can be decided in polynomial time by an *Arthur–Merlin protocol* with two messages. See §2.4 for connections to other complexity classes.

Theorem 1.1 (Main theorem). $\textsc{SchubertVanishing}(Y)$ *is in* $\mathsf{AM} \cap \mathsf{coAM}$ *assuming the* GRH, *for all* $Y \in \{A, B, C, D\}$.

Here the GRH stands for the *Generalized Riemann Hypothesis*, that all nontrivial zeros of L-functions $L(s, \chi_k)$ have real part $\frac{1}{2}$. In fact, tracing back the references shows that a weaker assumption, the *Extended Riemann Hypothesis* (ERH) suffices. We stick with the GRH as it is better known, and refer to [14, §6] for definitions and relationships between these hypotheses.

To get some idea of the result, recall the *graph isomorphism* problem which is naturally in $\mathsf{NP} \subseteq \mathsf{AM}$. One of the first and most celebrated examples of the interactive proof is the AM protocol for *graph nonisomorphism*, see, for example, [20, §9.1.3]. Heuristically, this means that a prover can convince a verifier that two given graphs are not isomorphic using a probabilistic argument, if the prover has unlimited power, but the verifier can perform only poly-time computations verifying prover's claims.

[1] For nonclassical types E_6, E_7, E_8, F_4 and G_2, there is only a finite number of Schubert coefficients, so the problem is uninteresting from the computational complexity point of view.

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

In particular, this shows that GraphIsomorphism in AM ∩ coAM. Famously, this was used in [13] to conclude that the problem is unlikely to be NP-complete, cf. Corollary 1.5.

There is extensive literature in algebraic combinatorics with necessary and sufficient conditions for the vanishing of Schubert coefficients. We postpone discussion of the prior work, as well as the implications of the main theorem, until later in this section.

1.4. Hilbert's Nullstellensatz

Let $R = \mathbb{C}[x_1, \ldots, x_s]$ for some $s > 0$. *Hilbert's weak Nullstellensatz* states that a polynomial system

$$f_1 \ = \ \ldots \ = \ f_m \ = \ 0 \quad \text{where} \quad f_i \in R \tag{1.4}$$

has no solutions over $\mathbb{C}$ if and only if there exist $(g_1, \ldots, g_m) \in R^m$, such that

$$\sum_{i=1}^{m} f_i \, g_i \ = \ 1.$$

Now let $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_s]$. The decision problem HN (*Hilbert's Nullstellensatz*) asks if the polynomial system (1.4) has a solution over $\mathbb{C}$.[2] Here, the *size* of the polynomial system is the sum of the degrees of the polynomials f_i added to the sum of bit-lengths of the coefficients in the f_i.

The original proof of Hilbert's Nullstellensatz does not imply that HN is decidable. This follows from [45] by Mayr and Meyer, who showed that HN is in EXPSPACE and is also NP-hard. Major improvements by Brownawell [15] and Kollár [39] showed that one can take g_i of single exponential size (*effective Nullstellensatz*), which can be used to show that HN is in PSPACE. In a surprising breakthrough, Koiran showed that HN is in the polynomial hierarchy:

Theorem 1.2 [37, Thm 2]. HN *is in* AM *assuming the* GRH.

For the proof, Koiran needs existence of primes in certain intervals and with modular conditions, thus the GRH assumption. For the proof of Theorem 1.1, we need the following strengthening of Theorem 1.2 to finite algebraic extensions. Let

$$f_1, \ldots, f_m \ \in \ \mathbb{Z}(y_1, \ldots, y_k)\,[x_1, \ldots, x_s].$$

The decision problem HNP (*Parametric Hilbert's Nullstellensatz*) asks if the polynomial system (1.4) has a solution over $\overline{\mathbb{C}(y_1, \ldots, y_k)}$. Most recently, Ait El Manssour, Balaji, Nosan, Shirmohammadi, and Worrell extended Theorem 1.2 to HNP :

Theorem 1.3 [2, theorem 1]. HNP *is in* AM *assuming the* GRH.

In the proof, the authors substantially simplified Koiran's original approach in [37, 38], avoiding the use of semi-algebraic geometry. We refer the reader to a [2] for an extensive background of HNP and other related work.

1.5. Proof outline

We prove Theorem 1.1 by showing that Schubert vanishing can be viewed as an instance of the Parametric Hilbert's Nullstellensatz. We then show that the same holds for Schubert nonvanishing. More precisely, we prove the following:

Lemma 1.4 (Main lemma). *Both* SchubertVanishing(Y) *and* ¬SchubertVanishing(Y) *reduce to* HNP, *for all* $Y \in \{A, B, C, D\}$.

[2]By the Nullstellensatz, this is equivalent to asking if there is a solution over $\overline{\mathbb{Q}}$.

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

Here ¬SchubertVanishing $:= \{c(u_1,\ldots,u_k) >^? 0\}$, where $u_1,\ldots,u_k \in \mathcal{W}$. The lemma, combined with Theorem 1.3 immediately implies Theorem 1.1. For the proof of the Lemma 1.4, we give an explicit construction of two polynomial systems (1.4) with polynomially many parameters, one system for each part of the lemma. For both systems, we start with *Purbhoo's criterion* (Lemma 3.1), and restate it as a lifted formulation, giving reductions to HNP.

Purbhoo's criterion directly connects ¬SchubertVanishing to a particular sum of vector spaces being full-dimensional. We construct generators for this vector space and formulate a pair of polynomial systems to determine if these generators form a basis or not. We note that Purbhoo's criterion is stated in terms of generic group elements. However, such generic elements need not necessarily have succinct (polynomial size) representations. To bypass this issue, we describe explicit constructions of generic elements in terms of formal parameters. The resulting equations have polynomial coefficients in these parameters.

1.6. Prior work

The literature on the vanishing of Schubert coefficients and its various extensions is too extensive to be fully reviewed. Below are some highlights that we believe are most relevant. Although many of these conditions extend to larger k and all types, we restrict our presentation to the case $k = 3$ and type A, which is the best studied.

(1) First, recall a large number of sufficient conditions for the vanishing of Schubert coefficients $c^w_{u,v}$. These conditions are scattered across the literature and include:[3]

- the *number of inversion condition* $\mathrm{inv}(u) + \mathrm{inv}(v) \neq \mathrm{inv}(w)$ [41],
- the *number of descents condition* $\mathrm{des}(w) > \mathrm{des}(u) + \mathrm{des}(v)$ [41],
- *strong Bruhat order condition* $u \not\leq w$, see, for example, [59, §5.1],
- Knutson's *descent cycling condition* $\mathrm{Des}(u) \cap \mathrm{Des}(v) \cap \mathrm{Des}(ww_\circ) \neq \varnothing$ [32],
- Billey–Vakil's *permutation array condition* [11, Thm 5.1] (see also [5, Prop. 9.7]),
- St. Dizier–Yong's condition on certain fillings of Rothe diagrams [59, Thm A], and
- Hardt–Wallach's condition on empty rows in Rothe diagrams [23, Cor. 5.12].

The first three of these follow directly from the Lascoux–Schützenberger definition of Schubert polynomials, see §4.2, while the other conditions are more technical. All of these can be verified in poly-time; this is immediate in all cases except for the strong Bruhat order condition which needs the *Ehresmann criterion* [44, Prop. 2.1.11], and the St. Dizier–Yong condition where this is a part of their main theorem.

For *Grassmannian permutations* (permutations with one descent), Schubert coefficients are the *Littlewood–Richardson* (LR) *coefficients*, see, for example, [43, 44], which are extensively studied in algebraic combinatorics, see, for example, [60, Ch. 7]. In this case, the vanishing problem is in P as a corollary of the Knutson–Tao *saturation theorem* [18, 47].

There are several other classes of permutations, where the Schubert coefficients have a known combinatorial interpretation. In such cases, the combinatorial interpretation can be interpreted as sufficient conditions for nonvanishing. Notable examples include:

- Purbhoo's *root game conditions* [56, 57], and
- Knutson and Zinn-Justin's *tiling conditions* [35, 36].

We refer to [59, §5] and [49, §1.6] for technical details, comparisons, and further background on all these conditions.

(2) Partly motivated by numerical applications, there have also been efforts to give a description of an algebraic system for various Schubert problems. Notably, in [11, Thm 5.4], Billey and Vakil give an algebraic system with exactly $c^w_{u,v}$ solutions for generic values of certain variables. They also describe

[3]Below we assume the reader is familiar with the algebraic combinatorics terminology. To avoid cluttering, we postpone the definitions until §2.3.

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

the system of conditions for these variables being generic under the assumption that the set of solutions is 0-dimensional [11, Cor. 5.5]. The authors do not give a complexity analysis for this system; see [49, §8.1] for further details and a complexity discussion.

In [24], Hein and Sottile introduced an algebraic system giving a practical algorithm for computing Schubert coefficients. Their system had additional variables compared to the Billey–Vakil system and allowed polynomial equations to have smaller (polynomial) size. In the first draft [49] of this paper, we used the Hein–Sottile system (in type A), which we modified and extended to other types. We eventually shifted our approach in favor of an algebraic system given by Purbhoo's criterion. This characterization is amenable to a more uniform approach and is a better fit with Hilbert's Nullstellensatz, as this criterion characterizes the vanishing problem in particular. We refer to §4.1 for an overview of our earlier preprints in the evolution of this paper.

(3) Finally, there is very little known about the computational complexity of Schubert vanishing. It follows from existing literature that SchubertVanishing $\in$ PSPACE, but even that bound was never explicitly written. In type A and for $k = 3$, this was observed by Morales as a consequence of the Postnikov–Stanley formula [55, Cor. 17.13], see [48, §10] for details.[4] In combinatorial terminology, this formula shows $c^w_{u,v}$ has a *signed combinatorial interpretation* derived from the (usual) combinatorial interpretation for the Schubert–Kostka numbers (see §4.2) in terms of pipe dreams.

For general $k \geq 4$, the result follows by taking convolutions. For other classical types, one can follow the approach above and combine the pipe dream construction in [58] with the effective Möbius inversion in [51, §2.2]. We omit the details which are straightforward, but require a separate explanation in each type. Another way to see that Schubert vanishing is in PSPACE it to use the recursive, but type-independent *Billey's formula* [9, Eq. (5.5)].

1.7. Implications

From the computational complexity point of view, Main Theorem 1.1 shows that SchubertVanishing is in $\Sigma^{\mathsf{p}}_2 \cap \Pi^{\mathsf{p}}_2$ assuming the GRH, that is, relatively low in the polynomial hierarchy PH. Inclusion in PH was out of reach prior to this paper.

Similarly, it has been conjectured for a while that computing Schubert coefficients is computationally hard, see, for example, an extensive discussion in [11, §5.2] and [49, §1.4]. Notably, Adve, Robichaux, and Yong asked whether SchubertVanishing is NP-hard [1, Question 4.3]. In the opposite direction, the authors conjectured that SchubertPositivity := ¬SchubertVanishing is NP-hard [49, Conj. 1.6]. The following result resolves in the negative both the question and the conjecture under standard assumptions:

Corollary 1.5. SchubertVanishing *is not* NP*-hard, assuming the* GRH *and* PH $\neq \Sigma^p_2$*, that is, the polynomial hierarchy does not collapse to its second level. Similarly,* SchubertPositivity *is not* NP*-hard, under the same assumptions.*

The corollary follows immediately from the Main Theorem 1.1 and a result of Boppana, Håstad and Zachos [13, Thm 2.3]. In particular, the corollary implies that the vanishing of Schubert coefficients is quite different from the *vanishing of Kronecker coefficients* which is known to be coNP-hard [27]. See also [54, §5.2] for further details and references.

In algebraic combinatorics, a major open problem is whether Schubert coefficients have a *combinatorial interpretation* [61, Problem 11]. In the language of computational complexity this is asking whether this counting problem is in #P, the counting analogue of NP. See a detailed discussion in [48, §10]. This would imply that SchubertVanishing is in coNP. In the combinatorial language, this is saying that positivity of Schubert coefficients problem $\{c^w_{u,v} >^? 0\}$ has a *positive rule* [50].

The special cases mentioned above suggest that both Schubert vanishing and Schubert nonvanishing might have a positive rule, that is, that SchubertVanishing $\in$ NP $\cap$ coNP. Until recently this conclusion

[4]In fact, Morales's argument gives a little more, that SchubertVanishing $\in$ C$_=$P. On the other hand, *Tarui's theorem* gives that C$_=$P $\not\subseteq$ PH unless PH collapses, see a discussion in [28].

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

would seem fantastical and out of reach. Now, it was shown by Gutfreund, Shaltiel, and Ta-Shma [21], that if EXP requires exponential time even for AM protocols (we call this assumption GST), then AM ∩ coAM = NP ∩ coNP. In a combinatorial language, this says:

Corollary 1.6. *Both Schubert vanishing and Schubert nonvanishing have a positive rule, assuming* GST *and* GRH.

It is worth comparing this result with other problems where a combinatorial interpretation (#P formula) was recently refuted. These include squared S_n-characters [28], Stanley's inequality for linear extensions [16], and the Stanley–Yan matroid inequality [17]. In all these cases, the vanishing problem is not in PH (unless PH collapses), implying nonexistence of a combinatorial interpretation. Theorem 1.1 shows that a different approach is needed for Schubert coefficients.

2. Definitions and notation

2.1. *Standard notation*

We use $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $[n] = \{1, \ldots, n\}$. Unless stated otherwise, the underlying field is always $\mathbb{C}$. We use $e_1, \ldots, e_n$ to denote the standard basis in $\mathbb{C}^n$, and $\mathbf{0}$ to denote the zero vector. We use bold symbols such as $\boldsymbol{x}$ and $\boldsymbol{\alpha}$ to denote sets and vectors of variables, and bars such as $\overrightarrow{x}$ and $\overrightarrow{\alpha}$ to denote complex vectors.

Recall the following standard notation for almost simple Lie groups, see [26]. We have the *special linear group* $\mathsf{SL}_n(\mathbb{C})$, the *odd special orthogonal group* $\mathsf{SO}_{2n+1}(\mathbb{C})$, the *symplectic group* $\mathsf{Sp}_{2n}(\mathbb{C})$, and the *even special orthogonal group* $\mathsf{SO}_{2n}(\mathbb{C})$. These groups correspond to *root systems* A_n, B_n, C_n, and D_n, and are called *groups of type* A, B, C, and D, respectively.

To distinguish the types, we use subscripts in Schubert coefficients, for example, $c_{\langle A \rangle}(u, v, w)$. We omit the dependence on the type when it is clear from the context. We use bullets to denote flags: $F_\bullet = \{F_0 \subset F_1 \subset \ldots \subset F_n = V\}$ is a *complete flag* in V if $\dim F_i = i$.

2.2. *Computational notation*

For a polynomial $g \in \mathbb{Z}[x_1, \ldots, x_n]$, let $\deg(g)$ denote the degree of g, and let $s(g)$ denote the sum of bit-lengths of coefficients in g. The *size* of the polynomial g is defined as

$$\phi(g) \ := \ \deg(g) \ + \ s(g).$$

For a collection of polynomials $\overrightarrow{f} = (f_1, \ldots, f_m)$ as in (1.4), the *size* is defined as

$$\phi(\overrightarrow{f}) \ := \ \sum_{i=1}^{m} \deg(f_i) \ + \ \sum_{i=1}^{m} s(f_i).$$

For a matrix M with polynomial entries, the *size* $\phi(M)$ is the sum of sizes of these polynomials.

2.3. *Algebraic combinatorics background*

In type A, the Weyl group is $\mathcal{W} \simeq S_n$ and the *length function* is given by the number of inversions $\operatorname{inv}(w) := \#\{(i, j) \ : \ w(i) > i, \ 1 \le i < j \le n\}$. The longest element is $w_\circ = (n, n-1, \ldots, 1)$. A permutation $w \in S_n$ is said to have a *descent* at i, if $w(i) > w(i+1)$. Denote by $\operatorname{Des}(w)$ the *set of descents* of w, and by $\operatorname{des}(\sigma) := |\operatorname{Des}(\sigma)|$ the *number of descents*. The *Rothe diagram* is defined as

$$\mathrm{R}(w) \ := \ \big\{ \big(w(j), i\big) \ : \ i < j, \ w(i) > w(j) \big\} \ \subset \mathbb{N}^2,$$

and note that $|\mathrm{R}(w)| = \operatorname{inv}(w)$.

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

In types B/C, we have $\mathcal{W} \simeq S_n \ltimes \mathbb{Z}_2^n$, and the elements are represented as signed permutations, for example, $(4, -3, 5, -1, 2) \in \mathcal{W}_{C_5}$. In type D, we have $\mathcal{W} \simeq S_n \ltimes \mathbb{Z}_2^{n-1}$, and the elements are represented as signed permutations with an even number of negative signs, as in the example above. See [12] for analogues of inversions and descents in other types, and note that the first four conditions in §1.6 extend verbatim.

2.4. Complexity background

As we mentioned in the introduction, the paper can be completely understood without the use of complexity theory, since Main Theorem 1.1 easily follows from the (algebraic) Main Lemma 1.4. Still, for the purposes of motivation, we assume the reader is familiar with basic complexity theory and relationships between standard complexity classes: P, BPP, NP, Σ_m^{p}, Π_m^{p}, PH, PSPACE and $\mathsf{EXPSPACE}$. We refer to [6, 20] for the background.

Let us elaborate on the class AM and its complement coAM, due to their prominence in the paper. One can view complexity problems as *interactive proofs*, with quantifiers describing communications between a prover and verifier. When we have a BPP verifier, that is, when the verifier (Arthur) has powers to flip coins and the prover (Merlin) has unlimited computational powers. Such communication is called the *Arthur–Merlin protocol*. The number of quantifiers becomes the number of messages between the prover and the verifier.

The complexity class AM is a class of decision problems that can be decided in polynomial time by an Arthur–Merlin protocol with two messages, see, for example, [6, §8.2]. Recall the inclusions

$$\mathsf{NP} \ \subseteq \ \exists{\cdot}\mathsf{BPP} \ \subseteq \ \mathsf{AM} \ \subseteq \ \Pi_2^{\mathsf{p}} \ \subseteq \ \mathsf{PH}.$$

Famously, *graph isomorphism* is in coAM, since graph nonisomorphism can be established by a simple interactive protocol (see, e.g., [6, Thm 8.13]). Other problems in $\mathsf{AM} \cap \mathsf{coAM}$ include *code equivalence*, *ring isomorphism*, *permutation group isomorphism* and *tensor isomorphism*; see the references in [52, §1.5.1].

3. Proof of Main Lemma 1.4

3.1. Purbhoo's criterion

Fix $Y \in \{A, B, C, D\}$ and let $\mathsf{G} = \mathsf{G}_Y$ be a semisimple algebraic group of type Y. In each case, G is a matrix group lying in an ambient vector space V. Let N denote the subgroup of unipotent matrices, so we have

$$\mathsf{N} \subset \mathsf{B} \subset \mathsf{G} \subset V.$$

Let $\mathfrak{n}$ denote the Lie algebra of N. We think of $\mathfrak{n}$ as a subspace of V. Finally, for $w \in \mathcal{W}$, let $Z_w := \mathfrak{n} \cap (w\mathsf{B}_{-}w^{-1})$.

It is well-known and follows from [10], that

$$c_{\langle B\rangle}(u_1, \ldots, u_k) \ = \ 2^a \, c_{\langle C\rangle}(u_1, \ldots, u_k), \tag{3.1}$$

where

$$a \ = \ \zeta(w_\circ u_k) \ - \ \zeta(u_1) \ - \ \ldots \ - \ \zeta(u_{k-1})$$

and $\zeta(\pi)$ denotes the number of sign changes in the signed permutation $\pi \in \mathcal{W}$. This shows the vanishing problems in types B and C are equivalent. Thus for simplicity, we consider only types A, B, and D.

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

Table 1. *Positive roots and corresponding matrix entries.*

G	Φ_+	$U(\mathsf{G})$
SL_n	$\{e_i - e_j \,:\, 1 \le i < j \le n\}$	$\{(i,j) \,:\, 1 \le i < j \le n\}$
SO_{2n+1}	$\{e_i \pm e_j \,:\, 1 \le i < j \le n\} \cup \{e_i \,:\, i \in [n]\}$	$\{(i,j) \,:\, 1 \le i < j \le 2n+1-i\}$
SO_{2n}	$\{e_i \pm e_j \,:\, 1 \le i < j \le n\}$	$\{(i,j) \,:\, 1 \le i < j \le 2n-i\}$

Lemma 3.1 (Purbhoo's criterion [57, Cor. 2.6]). *For generic $\rho_1, \ldots, \rho_k \in \mathsf{N} \subset \mathsf{G}$, we have:*

$$c(u_1,\ldots,u_k) > 0 \iff \rho_1 R_{u_1}\rho_1^{-1} + \ldots + \rho_k R_{u_k}\rho_k^{-1} = \rho_1 R_{u_1}\rho_1^{-1} \oplus \ldots \oplus \rho_k R_{u_k}\rho_k^{-1}.$$

Generalizing the number of inversions condition in §1.6(1), the *dimension condition* says that

$$c(u_1,\ldots,u_k) = 0 \quad \text{if} \quad \mathrm{inv}(u_1) + \cdots + \mathrm{inv}(u_k) \neq \dim(\mathfrak{n}). \tag{3.2}$$

Thus it suffices to restrict to the case $\mathrm{inv}(u_1) + \ldots + \mathrm{inv}(u_k) = \dim(\mathfrak{n})$. In that setting,

$$c(u_1,\ldots,u_k) > 0 \iff \rho_1 R_{u_1}\rho_1^{-1} + \ldots + \rho_k R_{u_k}\rho_k^{-1} = \mathfrak{n}.$$

Using Lemma 3.1, it suffices to determine the dimension of the vector space $H := \rho_1 R_{u_1}\rho_1^{-1} + \ldots + \rho_k R_{u_k}\rho_k^{-1}$ for generic ρ_i. In §3.3, we describe how to construct these ρ_i. In §3.2, we describe how to construct bases for these R_{u_i}. In §3.4, we combine these constructions to obtain bases for each summand $\rho_i R_{u_i}\rho_i^{-1}$. From these we obtain vectors π_j which generate H.

In §3.5, we prove Lemma 1.4 in two parts. We construct a system of equations to test whether these π_j are linearly dependent. By Lemma 1.4 and the dimension condition, if π_j are linearly dependent, the corresponding coefficient vanishes. Next we form a square matrix M with columns π_j and test if M is invertible. By Lemma 1.4 and the dimension condition (3.2), if M is nonsingular, the corresponding coefficient is positive.

Our equations are stated in terms of formal parameters to ensure generic choices are made. Thus in each case we test satisfiability of the systems over the appropriate function field.

3.2. Root systems

In each type, the Weyl group $\mathcal{W}$ is generated by reflections r_γ, where γ are roots in a *root system* Φ. The root system Φ is partitioned in terms of its positive and negative roots: $\Phi = \Phi_+ \sqcup \Phi_-$. In Table 1, we recall Φ_+, where e_i denotes the i-th elementary basis vector in $\mathbb{C}^n$.

For ease of notation, define the integer $N(\mathsf{G})$, where

$$N(\mathsf{G}) = \begin{cases} n & \text{if } \mathsf{G} = \mathsf{SL}_n(\mathbb{C}), \\ 2n+1 & \text{if } \mathsf{G} = \mathsf{SO}_{2n+1}(\mathbb{C}), \\ 2n & \text{if } \mathsf{G} = \mathsf{SO}_{2n}(\mathbb{C}). \end{cases}$$

To each $\gamma \in \Phi_+$, we wish to associate a particular $m \times m$ matrix, where $m = N(\mathsf{G})$. Define the subset $U(\mathsf{G}) \subset [m] \times [m]$ as in Table 1. We construct a bijection $\phi : U(\mathsf{G}) \to \Phi_+$ as follows.

(A) For SL_n take $\phi(i,j) := e_i - e_j$.

(B) For SO_{2n+1} take

$$\phi(i,j) := \begin{cases} e_i + e_j & \text{if } j \le n \\ e_i - e_{2n+2-j} & \text{if } n+1 < j \\ e_i & \text{if } j = n+1 \end{cases}$$

(D) For SO_{2n} take

$$\phi(i,j) := \begin{cases} e_i + e_j & \text{if } j \le n \\ e_i - e_{2n+1-j} & \text{if } n < j \end{cases}$$

Thus for every positive root $\gamma \in \Phi_+$ we define E'_γ to be the $m \times m$ matrix with a 1 in position $\phi^{-1}(\gamma)$ and 0 elsewhere. For SL_n let $\mathrm{E}_\gamma := \mathrm{E}'_\gamma$. For SO_{2n+1} and SO_{2n}, let $\mathrm{E}_\gamma := \mathrm{E}'_\gamma - \mathrm{D}_m(\mathrm{E}'_\gamma)^T \mathrm{D}_m$, where D_m is the antidiagonal matrix.

3.3. Generic unipotent subgroup elements

Let $m := N(\mathsf{G})$. We now describe how to construct an upper unitriangular $m \times m$ matrix $\mathrm{K} = (\kappa_{ij})$ which lies in $\mathsf{N} \subset \mathsf{B} \subset \mathsf{G}$. Define:

$$\kappa_{ij} = \begin{cases} \alpha_{ij} & \text{if } i < j \text{ and } (i,j) \in U(\mathsf{G}), \\ z_{ij} & \text{if } i < j \text{ and } (i,j) \notin U(\mathsf{G}), \\ 1 & \text{if } i = j, \\ 0 & \text{if } i > j. \end{cases}$$

Here we treat α_{ij} as parameters and z_{ij} as variables.

Note we have no additional dependencies placed on κ_{ij} to ensure that $\kappa \in \mathsf{G}$ for $\mathsf{G} = \mathsf{SL}_n(\mathbb{C})$. For $\mathsf{G} = \mathsf{SO}_{2n+1}(\mathbb{C})$ and $\mathsf{G} = \mathsf{SO}_{2n}(\mathbb{C})$, let D_m be the antidiagonal matrix. To ensure $\kappa \in \mathsf{G}$, we need

$$\mathrm{K}^T \cdot \mathrm{D}_m \cdot \mathrm{K} = \mathrm{D}_m \quad \text{and} \quad \det(\mathrm{K}) = 1.$$

Clearly, $\det(\mathrm{K}) = 1$ is already satisfied. Then we need only to impose $\mathrm{K}^T \cdot \mathrm{D}_m \cdot \mathrm{K} = \mathrm{D}_m$.

3.4. Main construction

Let $m = N(\mathsf{G})$. In light of Lemma 3.1, we consider the vector space

$$H = \rho_1 R_{u_1} \rho_1^{-1} + \ldots + \rho_k R_{u_k} \rho_k^{-1}.$$

Let $d := \dim \mathsf{G}/\mathsf{B}$ and note that $\dim \mathfrak{n} = |U(\mathsf{G})| = d \le \binom{m}{2} = O(m^2)$. By the dimension condition, we can assume

$$\operatorname{inv}(u_1) + \ldots + \operatorname{inv}(u_k) = d. \tag{3.3}$$

Further, we can assume that $\operatorname{inv}(u_i) \ge 1$ for all $i \in [k]$, so we have $k \le d$.

Recall that for $w \in \mathcal{W}$, we have $Z_w = \mathfrak{n} \cap (w\mathsf{B}_- w^{-1})$. Equivalently, Z_w is the subspace of $\mathfrak{n}$ generated by basis elements E_γ for $\gamma \in \Phi_+(w)$, where

$$\Phi_+(w) := \{\beta \in \Phi_+ : w^{-1}\beta \notin \Phi_+\}.$$

Thus for $i \in [k]$, we construct bases for the R_{u_i} as follows:

$$S_{u_i} := \{x_{\gamma,i}\, \mathrm{E}_\gamma : \gamma \in \Phi_+(u_i)\}.$$

Since $\operatorname{inv}(u_i) = |\Phi_+(u_i)|$ for $i \in [k]$ and we assumed (3.3), the collection $\cup_{i\in[k]} S_{u_i}$ has $d = O(m^2)$ elements. Let $\boldsymbol{x} := \{x_{\gamma,i}\}$ be the set of those variables appearing in the collection. We have:

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

$$\sum_{i=1}^{k} \operatorname{inv}(u_i) = \sum_{i=1}^{k} \dim(R_{u_i}) = \sum_{i=1}^{k} \left|S_{u_i}\right| = d. \tag{3.4}$$

We now construct generic matrices $\rho_1, \ldots, \rho_k \in \mathsf{N}$ according to §3.3 above, in terms of formal parameters $\alpha_{j\ell}^{(i)}$ and variables $z_{j\ell}^{(i)}$. Define $\boldsymbol{\alpha} := \{\alpha_{j\ell}^{(i)}\}$ and $\boldsymbol{x} := \{z_{j\ell}^{(i)}\}$ to be the sets of parameters and variables, respectively, appearing in some ρ_i, where $i \in [k]$. Then

$$|\boldsymbol{\alpha}| = |\boldsymbol{z}| \le k \cdot m^2 \le d \cdot m^2 = O(m^4).$$

By the construction in §3.3, each matrix ρ_i is an upper triangular $m \times m$ matrix with linear entries. Thus it has size $O(m^2)$, where the *size* is defined in §2.2.

Now for each $i \in [k]$, form the upper unitriangular matrix $\widetilde{\rho_i}$ whose (j, ℓ) entry for $j < \ell$ is the variable $y_{j\ell}^{(i)}$. Define the set of variables $\boldsymbol{y} := \{y_{j\ell}^{(i)} : i \in [k],\ 1 \le j < \ell \le m\}$. For all $i \in [k]$, construct bases for $\rho_i R_{u_i} \widetilde{\rho_i}$ as follows:

$$T_{u_i} := \rho_i S_{u_i} \widetilde{\rho_i} = \{\rho_i \cdot g \cdot \widetilde{\rho_i} : g \in S_{u_i}\}.$$

By (3.4), we have $|T_{u_1}| + \ldots + |T_{u_k}| = d$.

Consider the map τ on $m \times m$ matrices defined by restricting to entries in positions $U(\mathsf{G})$. Recall that for $\mathsf{G} = \mathsf{SL}_n$, we have $\mathfrak{n}$ is the set of strictly upper triangular matrices. For $\mathsf{G} = \mathsf{SO}_{2n+1}$ or $\mathsf{G} = \mathsf{SO}_{2n}$, we have $\mathfrak{n}$ is the set of strictly upper triangular matrices which are skew symmetric with respect to reflection about the main antidiagonal. By the definition of $\mathfrak{n}$, every $m \times m$ matrix in $\mathfrak{n}$ is determined by its entries in positions $U(\mathsf{G})$. Thus, $\dim(T_{u_i}) = \dim\left(\tau(T_{u_i})\right)$ for each $i \in [k]$. Let

$$T := \bigcup_{i \in [k]} \tau(T_{u_i}),$$

and write $T = \{\pi_i : i \in [d]\}$. Since $|U(\mathsf{G})| = d$, we may view each $\pi_i \in T$ as a d-vector.

3.5. *Proof of Main Lemma 1.4*

As mentioned above, by the dimension condition (3.2), we can assume that (3.3) holds, and that $\operatorname{inv}(u_i) \ge 1$ for all $i \in [k]$. Define $\widetilde{\rho_i}$ for all $i \in [k]$, and let $T = \{\pi_i : i \in [d]\}$ as in §3.4 above. We prove the two parts of the lemma separately.

First part of the lemma. For the vanishing result, we analyze the negation of the condition in Lemma 3.1:

$$\rho_1 R_{u_1} \rho_1^{-1} + \ldots + \rho_k R_{u_k} \rho_k^{-1} \subsetneq \mathfrak{n}. \tag{3.5}$$

Note that (3.5) holds if and only if T is linearly dependent for $\widetilde{\rho_i} = \rho_i^{-1}$, with $\rho_i \in \mathsf{N}$ for each $i \in [k]$.

We introduce two new sets of variables: $\boldsymbol{q} = \{q_i : i \in [d]\}$ and $\boldsymbol{s} = \{s_i : i \in [d]\}$. Consider a polynomial system $\mathcal{T}(u_1, \ldots, u_k)$ defined as follows:

$$\begin{cases} \rho_i \cdot \widetilde{\rho_i} = \mathsf{Id}_m \ \text{ for } i \in [k], \\ \rho_i^T \cdot \mathrm{D}_m \cdot \rho_i = \mathrm{D}_m \ \text{ for } i \in [k], \ \text{ if } \mathsf{G} = \mathsf{SO}_m, \\ \displaystyle\sum_{i=1}^{d} q_i \cdot \pi_i = 0, \\ \displaystyle\sum_{i=1}^{d} q_i \cdot s_i = 1. \end{cases}$$

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

Here $\mathcal{T}(u_1,\ldots,u_k)$ uses variables $\boldsymbol{x} \cup \boldsymbol{y} \cup \boldsymbol{x} \cup \boldsymbol{q} \cup \boldsymbol{s}$ and parameters $\boldsymbol{\alpha}$. Note that entries in $\pi_i \in T$ are cubic monomials. Thus the whole system $\mathcal{T}(u_1,\ldots,u_k)$ has size $O(m^5)$. See Table 4 for details regarding the size computations.

Now, the proper containment in (3.5) holds if and only if $\mathcal{T}(u_1,\ldots,u_k)$ is satisfiable over $\mathbb{C}(\boldsymbol{\alpha})$. We note the following statements are equivalent since the parameters α are algebraically independent:

1. $\mathcal{T}(u_1,\ldots,u_k)$ has a solution over $\mathbb{C}(\boldsymbol{\alpha})$,
2. $X \times_{\mathrm{Spec}(\mathbb{C}[\alpha])} \mathrm{Spec}\,(\overline{\mathbb{C}(\boldsymbol{\alpha})}) \neq \emptyset$,
3. $X \times_{\mathrm{Spec}(\mathbb{C}[\alpha])} \mathrm{Spec}(\,\mathbb{C}(\boldsymbol{\alpha})) \neq \emptyset$,
4. the general fiber of $X \to \mathrm{Spec}(\mathbb{C}[\boldsymbol{\alpha}])$ is nonempty, and
5. $\mathcal{T}(u_1,\ldots,u_k)$ has a solution over $\mathbb{C}$ for a generic choice of evaluations $\overrightarrow{\alpha}$ of $\boldsymbol{\alpha}$.

The equivalence of (i) and (ii), (ii) and (iii), and (iv) and (v) are straightforward. The equivalence of (iii) and (iv) follows from [62, Lemma 37.24.1] and [62, Lemma 37.24.2]).

Therefore, by Lemma 3.1 and (3.1), the problem SchubertVanishing(Y) reduces to HNP for every type $Y \in \{A,B,C,D\}$. □

Second part of the lemma. To prove the nonvanishing result, we analyze the condition in Lemma 3.1:

$$\rho_1 R_{u_1}\rho_1^{-1} \ + \ \ldots \ + \rho_k R_{u_k}\rho_k^{-1} \ = \ \mathfrak{n}. \tag{3.6}$$

Let M be the $d\times d$ matrix formed by the vectors in T. Then (3.6) holds if and only if M is invertible for $\widetilde{\rho_i} = \rho_i^{-1}$ with $\rho_i \in \mathsf{N}$ for each $i \in [k]$.

Let $\widetilde{M} = (t_{ij})$ be a $d\times d$ matrix of variables. Define the set of variables $\boldsymbol{t} = \{t_{ij} : i,j \in [d]\}$. Let $\mathcal{S}(u_1,\ldots,u_k)$ be the system defined as follows:

$$\begin{cases} \rho_i \cdot \widetilde{\rho_i} \ = \ \mathsf{Id}_m \ \text{ for } i \in [k], \\ \rho_i^T \cdot \mathrm{D}_m \cdot \rho_i \ = \ \mathrm{D}_m \ \text{ for } i \in [k], \ \text{if } \mathsf{G} = \mathsf{SO}_N, \\ M \cdot \widetilde{M} \ = \ \mathsf{Id}_d\,. \end{cases}$$

Here the system $\mathcal{S}(u_1,\ldots,u_k)$ uses variables $\boldsymbol{x} \cup \boldsymbol{y} \cup \boldsymbol{x} \cup \boldsymbol{t}$ and parameters $\boldsymbol{\alpha}$. Note that entries in M are cubic monomials. Thus the whole system $\mathcal{S}(u_1,\ldots,u_k)$ has size $O(m^6)$. See Table 4 for details regarding the size computations.

Now, the equality in (3.6) holds if and only if the system $\mathcal{S}(u_1,\ldots,u_k)$ is satisfiable over $\mathbb{C}(\boldsymbol{\alpha})$. As in the previous part, since the parameters in $\boldsymbol{\alpha}$ are algebraically independent, the system $\mathcal{S}(u_1,\ldots,u_k)$ has a solution over $\mathbb{C}(\boldsymbol{\alpha})$ if and only if $\mathcal{S}(u_1,\ldots,u_k)$ has a solution over $\mathbb{C}$ for a generic choice of evaluations $\overrightarrow{\alpha}$ of $\boldsymbol{\alpha}$. Therefore, just as in the first part, by Lemma 3.1 and (3.1), the problem ¬SchubertVanishing(Y) reduces to HNP, for every type $Y \in \{A,B,C,D\}$. □

4. Final remarks

4.1. Evolution of this paper

This paper grew out of a series of unpublished preprints and research announcements of the authors (aimed at somewhat different audiences), where we successively strengthened the results while we simultaneously streamlined and simplified the proofs. Below is a brief description of these preprints. This paper is the definitive version that we do not plan to modify.

The original preprint [49], v1, proved only the coAM inclusion in the Main Theorem 1.1 and only for types A,B,C. The proof was technical, employed the Hein–Sottile algebraic system, and did not cover type D. The presentation was aimed at complexity theorists and included results in the Blum–Shub–Smale (nonstandard) models of computing that were established using Purbhoo's criterion: SchubertPositivity is in $\mathsf{NP}_{\mathbb{C}} \cap \mathsf{P}_{\mathbb{R}}$. The latter results are included in the STOC'25 extended abstract based on [49], but are omitted in the current version of the paper.

In v2 of the same preprint [49], we added an extensive description of the prior combinatorial work on the subject. We also added a new Appendix C (joint with David Speyer) with a different algebraic system based on the *Cayley transform*. This proved the coAM inclusion for all types, in particular for type D.

In a companion paper [50] aimed at algebraic combinatorialists, we gave an extensive epistemological and theological discussion on the delicate subject of proving combinatorial results under standard assumptions from other areas. This paper is a short announcement with no new proofs.

Finally, the most recent preprint [52] gives a proof of Main Theorem 1.1 based on a technical new tool (Determinant Lemma 2.2). Here we are using Purbhoo's criterion to prove that Schubert vanishing is in AM for all types. We also use this Determinant Lemma to resolve the type D case that was omitted in [49]. These tools proved crucial in our forthcoming paper [53], where we extend parts of Main Theorem 1.1 to enriched cohomology theories.

In this paper we are able to obtain a simple proof of both parts of Main Theorem 1.1, avoiding technicalities of the earlier preprints. Let us emphasize that this paper is the first version where we are able to take the intersection of k Schubert varieties, for all $k \geq 3$. While for many applications it is useful to have larger k, until now we were unable to give an algebraic system simple enough to prove the reduction to HNP for nonconstant k.

4.2. Schubert polynomials

A combinatorial approach to Schubert coefficients is given by *Schubert polynomials* $\mathfrak{S}_w \in \mathbb{N}[x_1, x_2, \ldots]$ indexed by permutations $w \in S_n$. They were introduced by Lascoux and Schützenberger [41], building on the earlier works by Demazure (1974) and Bernstein–Gelfand–Gelfand (1973). In type A, the translation is given by *Borel's ring isomorphism*:

$$\Phi \, : \, H^*(\mathsf{G}/\mathsf{B}) \longrightarrow \mathbb{Z}[x_1, \ldots, x_n]/\langle e_i(x_1, \ldots, x_n) \, : \, i \in [n] \rangle \, ,$$

where e_i are elementary symmetric polynomials. Schubert polynomials are polynomial representatives of Schubert classes: $\mathfrak{S}_w := \Phi(\sigma_w)$. Then *Schubert coefficients* can be defined as multiplication constants:

$$\mathfrak{S}_u \cdot \mathfrak{S}_v = \sum_{w \in S_\infty} c^w_{u,v} \, \mathfrak{S}_w \, .$$

In this notation, the *Schubert–Kostka numbers* mentioned in §1.6 are the coefficients $[\boldsymbol{x}^\alpha]\mathfrak{S}_u$. We refer to [43, 44] for introductory surveys, [33, 34] for overviews of recent results, and to [48, §10] for computational complexity aspects. Let us mention that Schubert polynomials play a central role in algebraic combinatorics, but do not appear in the proof of Main Theorem 1.1.

4.3. Vanishing is exponentially likely

It is easy to see that asymptotically, Schubert coefficients are almost always zero. Indeed, for $k = 3$ in type A, we have $\mathbb{P}[c^w_{u,v} > 0] < c^{-n}$ for some $c > 1$, where the probability is over uniform permutations $u, v, w \in S_n$. Recall the sufficient conditions for vanishing given in §1.6, and take their complements. The result follows from the number of inversions necessary condition $\operatorname{inv}(u) + \operatorname{inv}(v) = \operatorname{inv}(w)$ and the asymptotic normality of the inv statistics on S_n, see, for example, [19, §X.6].

Alternatively, Knutson's *descent cycling* necessary condition states that we must have $\operatorname{Des}(u) \cap \operatorname{Des}(v) \cap \operatorname{Des}(w w_\circ) = \varnothing$. Since distant descents are given by mutually independent fair coin flips, this condition also gives an exponential decay for the probability $\mathbb{P}[c^w_{u,v} > 0]$, even if we condition on the number of inversions equality. Finally, the strong Bruhat order necessary condition $u \leqslant w$ was studied asymptotically in [22]. Although only polynomial upper bounds are known, exponential decay is likely again.

https://doi.org/10.1017/fms.2025.10116 Published online by Cambridge University Press

4.4. Combinatorial interpretations

When it comes to finding combinatorial interpretations for Schubert coefficients, there are two ways to think of our results. On the one hand, as we mentioned in §1.7, these are the first positive results obtained in full generality, suggesting that both Schubert vanishing and Schubert positivity have a positive rule, under standard assumptions. On the other hand, the AM protocols of this paper are far removed from the type of positive rule that people are interested in, see quotes in [52, Appendix B] and an extensive discussion in [50].

We should emphasize that the complexity of *counting* solutions of algebraic systems (1.4) remains a major open problem, so our approach cannot be extended to the problem of computing Schubert coefficients. Furthermore, in contrast with the Billey–Vakil and Hein–Sottile algebraic systems (see §1.6), Purbhoo's criterion applies only to the vanishing of Schubert coefficients.

4.5. Unconditional approaches

It is an interesting question whether the GRH assumption in Theorem 1.1 can be weakened or completely removed. In fact, Koiran's proof of Theorem 1.2 uses only an effective version of the *Chebotarev density theorem* given in [40]. The latter assumes the GRH or a slightly weaker assumption ERH mentioned in the introduction. Despite recent advances in the area, it seems unlikely that the GRH assumption can be removed from Theorem 1.3 which we crucially employ.

A. Size Charts

We recall the values of $N(\mathsf{G})$ and $U(\mathsf{G})$, as defined in §3.2, for each G.

Now we describe the size computations for the systems $\mathcal{T}(u_1,\dots,u_k)$ and $\mathcal{S}(u_1,\dots,u_k)$ in Main Lemma 1.4 for each group G. In these systems, we assumed $k \le |U(\mathsf{G})|$, so $k = O(n^2)$ in each case. Additionally, note that $m = O(n)$.

Table 2. *Indices and Number of Positive Roots.*

G	$N(\mathsf{G})$	$\lvert U(\mathsf{G})\rvert$
SL_n	n	$\binom{n}{2}$
SO_{2n+1}	$2n+1$	n^2
SO_{2n}	$2n$	$n(n-1)$

Table 3. *Parameter and Variable Size Analysis for $\mathcal{T}(u_1,\dots,u_k)$ and $\mathcal{S}(u_1,\dots,u_k)$.*

	$\boldsymbol{\alpha}$	$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{z}$	$\boldsymbol{q}$	$\boldsymbol{s}$	$\boldsymbol{t}$
$\mathsf{G} = \mathsf{SL}_n$	$k\cdot\binom{n}{2}$	$\binom{n}{2}$	$k\cdot\binom{n}{2}$	0	$\binom{n}{2}$	$\binom{n}{2}$	$\binom{n}{2}^2$
$\mathsf{G} = \mathsf{SO}_{2n+1}$	$k\cdot n^2$	$\binom{2n+1}{2}$	$k\cdot\binom{2n+1}{2}$	$k\cdot(n^2+n)$	$\binom{2n+1}{2}$	$\binom{2n+1}{2}$	$\binom{2n+1}{2}^2$
$\mathsf{G} = \mathsf{SO}_{2n}$	$k\cdot(n^2-n)$	$\binom{2n}{2}$	$k\cdot\binom{2n}{2}$	$k\cdot n^2$	$\binom{2n}{2}$	$\binom{2n}{2}$	$\binom{2n}{2}^2$

Table 4. *Equation Size Analysis for $\mathcal{T}(u_1,\dots,u_k)$ and $\mathcal{S}(u_1,\dots,u_k)$.*

Equations	Sizes
$\rho_i\cdot\widetilde{\rho_i} = \mathsf{Id}_m$ for $i\in[k]$	$k\Big(2\binom{m}{2}+\big(\binom{m-1}{2}m+m(m+1)\big)\Big) = O(km^3)$
$\rho_i^T\cdot \mathrm{D}_m\cdot\rho_i = \mathrm{D}_m$ for $i\in[k]$	$k\Big(2\binom{m-1}{2}+m\binom{m-1}{2}\Big) = O(km^3)$
$\sum_{i=1}^d q_i\cdot\pi_i = 0$	$4+d^2 = O(d^2)$
$\sum_{i=1}^d q_i\cdot s_i = 1$	$3+d = O(d)$
$M\cdot\widetilde{M} = \mathsf{Id}_d$	$4d^2+(d^2-d)d+d(d+1) = O(d^3)$

First we give the sizes of the variables and parameters used in the systems. In Table 3, the size measures the cardinality of the set.

Then we describe the sizes of the equations in the systems. In Table 4, the size is defined as in §2.2. Below $m = N(\mathsf{G})$ and $d = U(\mathsf{G})$.

Note that for $\mathsf{G} = \mathsf{SL}_n$, the equations in the second line in Table 4 are not used.

Acknowledgments. We are grateful to Kevin Purbhoo for sharing his insights which partially motivated this paper. We thank Sara Billey, Nickolas Hein, Minyoung Jeon, Allen Knutson, Leonardo Mihalcea, Greta Panova, Oliver Pechenik, Maurice Rojas, Mahsa Shirmohammadi, Alex Smith, Frank Sottile, Avi Wigderson, James Worrell, Weihong Xu, Alex Yong, and Paul Zinn-Justin for interesting discussions and helpful comments. We are especially grateful to David Speyer for suggesting we use the Cayley transform in types C/D, and for his insights leading to Appendix C in [49].

This paper was partially written when the first author was a member at the Institute of Advanced Study in Princeton, NJ. We are grateful for the hospitality.

Competing interest. The authors have no competing interests to declare.

Financial support. The first author was partially supported by the NSF grant CCF-2302173. The second author was partially supported by the NSF MSPRF grant DMS-2302279.

References

[1] A. Adve, C. Robichaux and A. Yong, 'Vanishing of Littlewood–Richardson polynomials', *Comput. Complexity* **28** (2019), 241–257.
[2] R. Ait El Manssour, N. Balaji, K. Nosan, M. Shirmohammadi and J. Worrell, 'A parametric version of the Hilbert Nullstellensatz', in *Proc. 8th SOSA* (2025), 444–451.
[3] D. Anderson and W. Fulton, *Equivariant Cohomology in Algebraic Geometry* (Cambridge Univ. Press, Cambridge, UK, 2024), 446 pp.
[4] D. Anderson, E. Richmond and A. Yong, 'Eigenvalues of Hermitian matrices and equivariant cohomology of Grassmannians', *Compos. Math.* **149** (2013), 1569–1582.
[5] F. Ardila and S. Billey, 'Flag arrangements and triangulations of products of simplices', *Adv. Math.* **214** (2007), 495–524.
[6] S. Arora and B. Barak, Computational Complexity. *A Modern Approach* (Cambridge Univ. Press, Cambridge, UK, 2009), 579 pp.
[7] A. Berenstein and R. Sjamaar, 'Coadjoint orbits, moment polytopes, and the Hilbert–Mumford criterion', *J. Amer. Math. Soc.* **13** (2000), 433–466.
[8] N. Berline, M. Vergne and M. Walter, 'The Horn inequalities from a geometric point of view', *Enseign. Math.* **63** (2017), 403–470.
[9] S. Billey, 'Kostant polynomials and the cohomology ring for G/B', *Duke Math. J.* **96** (1999), 205–224.
[10] S. Billey and M. Haiman, 'Schubert polynomials for the classical groups', *J. Amer. Math. Soc.* **8** (1995), 443–482.
[11] S. Billey and R. Vakil, 'Intersections of Schubert varieties and other permutation array schemes', in *Algorithms in Algebraic Geometry* (Springer, New York, 2008), 21–54.
[12] A. Björner and F. Brenti, *Combinatorics of Coxeter Groups* (Springer, New York, 2005), 363 pp.
[13] R. B. Boppana, J. Hastad and S. Zachos, 'Does... have short interactive proofs?', *Inform. Process. Lett.* **25** (1987), 127–132.
[14] P. Borwein, S. Choi, B. Rooney and A. Weirathmueller (eds.), *The Riemann Hypothesis* (Springer, New York, 2008), 533 pp.
[15] W. D. Brownawell, 'Bounds for the degrees in the Nullstellensatz', *Ann. Math.* **126** (1987), 577–591.
[16] S. H. Chan and I. Pak, 'Equality cases of the Alexandrov–Fenchel inequality are not in the polynomial hierarchy', *Forum Math. Pi* **12** (2024), Paper No. e21, 38 pp.
[17] S. H. Chan and I. Pak, 'Equality cases of the Stanley–Yan log-concave matroid inequality', preprint (2024), 36 pp.; arXiv:2407.19608.
[18] J. A. De Loera and T. B. McAllister, 'On the computation of Clebsch–Gordan coefficients and the dilation effect', *Experiment. Math.* **15** (2006), 7–19.
[19] W. Feller, *An Introduction to Probability Theory and Its Applications*, *Vol. I*, 3rd edn (Wiley, New York, 1968), 509 pp.
[20] O. Goldreich, *Computational Complexity. A Conceptual Perspective* (Cambridge Univ. Press, Cambridge, UK, 2008), 606 pp.
[21] D. Gutfreund, R. Shaltiel and A. Ta-Shma, 'Uniform hardness versus randomness tradeoffs for Arthur–Merlin games', *Comput. Complexity* **12** (2003), 85–130.
[22] A. Hammett and B. Pittel, 'How often are two permutations comparable?', *Trans. Amer. Math. Soc.* **360** (2008), 4541–4568.
[23] A. Hardt and D. Wallach, 'When do Schubert polynomial products stabilize?', preprint (2024), 32 pp.; arXiv:2412.06976.
[24] N. Hein and F. Sottile, 'A lifted square formulation for certifiable Schubert calculus', *J. Symbolic Comput.* **79** (2017), 594–608.
[25] B. Huber, F. Sottile and B. Sturmfels, 'Numerical Schubert calculus', *J. Symbolic Comput.* **26** (1998), 767–788.

[26] J. E. Humphreys, *Linear Algebraic Groups, Graduate Texts in Mathematics*, vol. 21 (Springer, New York–Heidelberg, 1975).
[27] C. Ikenmeyer, K. D. Mulmuley and M. Walter, 'On vanishing of Kronecker coefficients', *Comput. Complexity* **26** (2017), 949–992.
[28] C. Ikenmeyer, I. Pak and G. Panova, 'Positivity of the symmetric group characters is as hard as the polynomial time hierarchy', *Int. Math. Res. Not.* (2024), 8442–8458.
[29] S. L. Kleiman, 'The transversality of a general translate', *Compos. Math.* **28** (1974), 287–297.
[30] S. L. Kleiman, 'Problem 15: Rigorous foundation of Schubert's enumerative calculus', in *Mathematical Developments Arising from Hilbert Problems* (Amer. Math. Soc., Providence, RI, 1976), 445–482.
[31] S. L. Kleiman and D. Laksov, 'Schubert calculus', *Amer. Math. Monthly* **79** (1972), 1061–1082.
[32] A. Knutson, 'Descent-cycling in Schubert calculus', *Experiment. Math.* **10** (2001), 345–353.
[33] A. Knutson, 'Schubert calculus and puzzles', in *Schubert Calculus* (MSJ, Tokyo, Japan, 2016), 185–209.
[34] A. Knutson, 'Schubert calculus and quiver varieties', in *Proc. ICM*, *vol. VI* (EMS Press, 2023), 4582–4605.
[35] A. Knutson and P. Zinn-Justin, 'Schubert puzzles and integrability I: invariant trilinear forms', preprint (2017), 51 pp.; arXiv:1706.10019.
[36] A. Knutson and P. Zinn-Justin, 'Schubert puzzles and integrability III: separated descents', preprint (2023), 42 pp.; arXiv:2306.13855.
[37] P. Koiran, 'Hilbert's Nullstellensatz is in the polynomial hierarchy', *J. Complexity* **12** (1996), 273–286.
[38] P. Koiran, 'A weak version of the Blum, Shub and Smale model', *J. Comput. System Sci.* **54**(1, part 2) (1997), 177–189.
[39] J. Kollár, 'Sharp effective Nullstellensatz', *J. Amer. Math. Soc.* **1** (1988), 963–975.
[40] J. C. Lagarias and A. M. Odlyzko, 'Effective versions of the Chebotarev density theorem', in *Algebraic Number Fields: L -functions and Galois Properties* (Academic Press, New York, 1977), 409–464.
[41] A. Lascoux and M.-P. Schützenberger, 'Polynômes de Schubert', *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982), 447–450.
[42] A. Leykin, A. Martín del Campo, F. Sottile, R. Vakil and J. Verschelde, 'Numerical Schubert calculus via the Littlewood–Richardson homotopy algorithm', *Math. Comp.* **90** (2021), 1407–1433.
[43] I. G. Macdonald, *Notes on Schubert Polynomials* (Publ. LaCIM, UQAM, Montreal, 1991), 116 pp.
[44] L. Manivel, *Symmetric Functions, Schubert Polynomials and Degeneracy Loci* (SMF/AMS, Providence, RI, 2001), 167 pp.
[45] E. W. Mayr and A. R. Meyer, 'The complexity of the word problems for commutative semigroups and polynomial ideals', *Adv. Math.* **46** (1982), 305–329.
[46] N. E. Mnëv, 'The universality theorems on the classification problem of configuration varieties and convex polytopes varieties', in *Lecture Notes in Math*. vol. 1346 (Springer, Berlin, 1988), 527–543.
[47] K. D. Mulmuley, H. Narayanan and M. Sohoni, 'Geometric complexity theory III. On deciding nonvanishing of a Littlewood–Richardson coefficient', *J. Algebraic Combin.* **36** (2012), 103–110.
[48] I. Pak, 'What is a combinatorial interpretation?', in *Open Problems in Algebraic Combinatorics* (Amer. Math. Soc., Providence, RI, 2024), 191–260.
[49] I. Pak and C. Robichaux, 'Vanishing of Schubert coefficients', preprint (2024), arXiv:2412.02064; v1, 24 pp.; v2 (with D. E. Speyer, App. C), 30 pp.; extended abstract in *Proc. 57th STOC* (2025), 1118–1129.
[50] I. Pak and C. Robichaux, 'Positivity of Schubert coefficients', preprint (2024), 7 pp.; arXiv:2412.18984.
[51] I. Pak and C. Robichaux, 'Signed combinatorial interpretations in algebraic combinatorics', *Algebr. Combin.* **8** (2025), 495–519.
[52] I. Pak and C. Robichaux, 'Vanishing of Schubert coefficients is in assuming the. . . ', preprint (2025), 18 pp.; arXiv:2504.03004.
[53] I. Pak, C. Robichaux and W. Xu, 'On vanishing of Gromov–Witten invariants', preprint (2025), 11 pp.; arXiv:2508.15715.
[54] G. Panova, 'Computational complexity in algebraic combinatorics', in *Current Developments in Mathematics* (Int. Press, Boston, MA, 2024), 241–280.
[55] A. Postnikov and R. P. Stanley, 'Chains in the Bruhat order', *J. Algebraic Combin.* **29** (2009), 133–174.
[56] K. Purbhoo, *Vanishing and Non-vanishing Criteria for Branching Schubert Calculus*, Ph.D. thesis (UC Berkeley, 2004), 96 pp.
[57] K. Purbhoo, 'Vanishing and nonvanishing criteria in Schubert calculus', *Int. Math. Res. Not.* (2006), Art. 24590, 38 pp.
[58] E. Smirnov and A. Tutubalina, 'Pipe dreams for Schubert polynomials of the classical groups', *European J. Combin*. **107** (2023), Paper No. 103613, 46 pp.
[59] A. St. Dizier and A. Yong, 'Generalized permutahedra and Schubert calculus', *Arnold Math. J.* **8** (2022), 517–533.
[60] R. P. Stanley, *Enumerative Combinatorics, Vol. 2* (Cambridge Univ. Press, 1999), 581 pp.
[61] R. P. Stanley, 'Positivity problems and conjectures in algebraic combinatorics', in *Mathematics: Frontiers and Perspectives* (Amer. Math. Soc., Providence, RI, 2000), 295–319.
[62] The Stacks Project Authors, *The Stacks Project*, available at https://stacks.math.columbia.edu (2025).
[63] R. Vakil, 'Murphy's law in algebraic geometry: badly-behaved deformation spaces', *Invent. Math.* **164** (2006), 569–590.