Title	On the invariants of the cohomology of complements of Coxeter arrangements
Author(s)	Douglass, J. Matthew; Pfeiffer, Götz; Röhrle, Gerhard
Publication Date	2019-05-24
Publication Information	Douglass, J. Matthew, Pfeiffer, Götz, & Röhrle, Gerhard. (2020). On the invariants of the cohomology of complements of Coxeter arrangements. Journal of Algebra, 558, 336-349. doi:https://doi.org/10.1016/j.jalgebra.2019.05.010
Publisher	Elsevier
Link to publisher's version	https://doi.org/10.1016/j.jalgebra.2019.05.010
Item record	http://hdl.handle.net/10379/16537
DOI	http://dx.doi.org/10.1016/j.jalgebra.2019.05.010

ON THE INVARIANTS OF THE COHOMOLOGY OF COMPLEMENTS OF COXETER ARRANGEMENTS

J. MATTHEW DOUGLASS, GÖTZ PFEIFFER, AND GERHARD RÖHRLE

Dedicated to Michel Broué

Abstract. We refine Brieskorn's study of the cohomology of the complement of the reflection arrangement of a finite Coxeter group W. As a result we complete the verification of a conjecture by Felder and Veselov that gives an explicit basis of the space of W-invariants in this cohomology ring.

1. Introduction

Suppose that W is a finite Coxeter group with Coxeter generating set S of size $|S| = l$. Let $V_{\mathbb{R}}$ be an l-dimensional, real vector space that affords the reflection representation of W. Let $V = \mathbb{C} \otimes_{\mathbb{R}} V_{\mathbb{R}}$ be the complexification of $V_{\mathbb{R}}$ and consider W as a subgroup of the group $\mathrm{GL}(V)$ of invertible $\mathbb{C}$-linear transformations of V. Let R denote the set of reflections in W. For each $r \in R$ let V^r denote the hyperplane of fixed points of r in V, and set $\mathcal{A} = \{ V^r \mid r \in R \}$. Then $(V, \mathcal{A})$ is the complexification of a Coxeter arrangement.

The group W acts naturally on the complement $M_W = V \setminus \bigcup_{r\in R} V^r$ of the hyperplanes in $\mathcal{A}$, and hence on the cohomology of M_W as algebra automorphisms. For $p \geq 0$ let $H^p(M_W)$ denote the p^{th} de Rahm cohomology space of M_W with complex coefficients and let $H^*(M_W) = \bigoplus_{p\geq 0} H^p(M_W)$ denote the total cohomology of M_W. Felder and Veselov [5] have conjectured an explicit construction of $H^p(M_W)^W$, the space of W-invariants in $H^p(M_W)$, in terms of so-called special involutions. They have verified their conjecture for all Coxeter groups except those with irreducible components of type E_7, E_8, F_4, H_3, or H_4.

In this note we complete the proof of the conjecture of Felder-Veselov by reducing the problem to a computation in $H^l(M_W)$, implementing this computation in the computer algebra system GAP3 (for any W), and then performing the required calculations (for the remaining exceptional groups); thus verifying that the conjecture is true. In §2 we give more background and state the main result, and in §3 we describe some novel algorithmic aspects of the implementation of the relations for the Orlik-Solomon algebra of W used to complete the calculations on which the main results rely.

2. Background and main results

In order to state the Felder-Veselov conjecture precisely, we need additional notation.

2010 *Mathematics Subject Classification.* Primary 20F55; Secondary 05E10, 52C35.

Key words and phrases. Coxeter groups, Orlik-Solomon algebras, arrangements of hyperplanes, hyperplane complements.

The authors would like to thank their charming wives for their unwavering support during the preparation of this paper.

2.1. **The Felder-Veselov conjecture.** Let $\Phi \subseteq V_{\mathbb{R}}$ be a root system for W as in [7, §1.1] and let $\{ \alpha_s \mid s \in S \}$ be the roots corresponding to elements of S.

Orlik and Solomon [13] give a combinatorial presentation of the cohomology algebra $H^*(M_W)$ that is suitable for machine computation. The *Orlik-Solomon algebra of* W is the $\mathbb{C}$-algebra $A(W)$ with generators $\{ a_r \mid r \in R\}$ and relations

- $a_r a_s = -a_s a_r$ for $r, s \in R$ and
- whenever $\{V^{r_1}, \dots, V^{r_p}\}$ is linearly dependent for $r_1, \dots, r_p \in R$, we have

$$\sum_{i=1}^{p} (-1)^i a_{r_1} \cdots \widehat{a_{r_i}} \cdots a_{r_p} = 0,$$

where the notation $\widehat{a_{r_i}}$ indicates omission of the term a_{r_i}. The algebra $A(W)$ is naturally graded with $A^p(W)$ equal to the span of all $a_{r_1} \cdots a_{r_p}$ such that $\operatorname{codim} V^{r_1} \cap \cdots \cap V^{r_p} = p$. The rule $(w, a_r) \mapsto a_{wrw^{-1}}$, for $w \in W$ and $r \in R$, extends to an action of W on $A(W)$ as degree-preserving, algebra automorphisms. Orlik and Solomon show that the rule $a_s \mapsto d\alpha_s^\vee/\alpha_s^\vee$, where $s \in S$ and $\alpha_s^\vee \in V^*$ denotes the extension of the coroot $\alpha_s^\vee \in V_{\mathbb{R}}^*$, extends to a W-equivariant isomorphism of graded $\mathbb{C}$-algebras $A(W) \cong H^*(M_W)$. See [15] for details. In the following we work with the Orlik-Solomon algebra of W.

Fix an arbitrary linear order on R, say $R = \{ r_1, \dots, r_n \}$. For any subset $T = \{ r_{i_1}, \dots, r_{i_p} \}$ of R with $i_1 < \cdots < i_p$, define

$$a_T := a_{i_1} \cdots a_{i_p} \in A(W).$$

For an involution $t \in W$ there is a direct sum decomposition $V_{\mathbb{R}} \cong V_1 \oplus V_{-1}$, where V_1 and V_{-1} are the 1- and (-1)-eigenspaces of t, respectively. Define $\Phi_1 = \Phi \cap V_1$ and $\Phi_{-1} = \Phi \cap V_{-1}$. Following [5], we say that t is *special*, if for any root $\alpha \in \Phi$ at least one of its projections onto V_1 or V_{-1} is proportional to a root in Φ_1 or Φ_{-1}, respectively. Clearly, this definition does not depend on the choice of root system for W.

Suppose t is a special involution and $p = \dim V_{-1}$. Then Φ_{-1} is a root system in V_{-1}. Choose a base of Φ_{-1} and let $S(t) \subseteq R$ be the reflections in W corresponding to the roots in this base. Then $a_{S(t)} \in A^p(W)$. Let

$$\operatorname{Av}\colon A(W) \to A(W)^W$$

be the averaging map, where $A(W)^W$ is the space of W-invariants of $A(W)$. Felder and Veselov [5] make the following conjecture that we state as a theorem.

Theorem 2.1. *Let W be a finite Coxeter group. Then*

(1) for any special involution t of W, the element $\operatorname{Av}(a_{S(t)}) \in A(W)^W$ is non-zero, and
(2) any element in $A(W)^W$ is a linear combination of elements $\operatorname{Av}(a_{S(t)})$ from (1).

More precisely, if m is the number of conjugacy classes of special involutions in W, then it follows from the theorem (and the observation that, for $w \in W$, up to a sign $\operatorname{Av}(a_{S(wtw^{-1})}) = \operatorname{Av}(a_{S(t)})$) that $\dim A(W)^W \leq m$. For each irreducible finite Coxeter group W, Brieskorn [4, Thm. 7] has computed the Betti numbers of the manifold M_W/W and thus the Poincaré polynomial of $A(W)^W$. It turns out that $\dim A(W)^W = m$ and so the next corollary is an immediate consequence of the theorem.

Corollary 2.2. *Suppose W is a finite Coxeter group and $\{t_1, \dots, t_m\}$ is a set of representatives of the conjugacy classes of special involutions in W. Then $\{\operatorname{Av}(a_{S(t_1)}), \dots, \operatorname{Av}(a_{S(t_m)})\}$ is a basis of $A(W)^W$.*

A proof of Theorem 2.1 is given in the next section. Roughly speaking, the proof of (1) consists of reducing the assertion to the case when t is the longest element in W. This statement is then checked case-by-case, using GAP3 for the exceptional groups. The assertion in (2) follows from an inspection of the reduction used to prove (1).

2.2. **A reduction.** The reduction of Theorem 2.1 (1) to the case of longest words in top degree is based on a decomposition of the representation of W on $A^p(W)$ as a sum of induced representations due to Lehrer and Solomon [11].

Each subset I of S determines

- a standard parabolic subgroup W_I of W generated by I,
- subspaces $V_I = \operatorname{span}\{\, \alpha_s \mid s \in I \,\}$ and $X_I = \bigcap_{s\in I} V^s$ of V such that $V \cong V_I \oplus X_I$, and
- a subspace $A(W)_I = \operatorname{span}\{\, a_{r_1} \cdots a_{r_d} \mid V^{r_1} \cap \cdots \cap V^{r_d} = X_I \,\} \subseteq A^{|I|}(W)$.

Let $N_I = N_W(W_I)$ be the normalizer of W_I in W. It is easy to see that $A(W)_I$ is an N_I-stable subspace of $A(W)$.

It is known that for subsets I and J of S, the following are equivalent:

(1) W_I and W_J are conjugate, and
(2) X_I is a W-translate of X_J.

This motivates the notion of *shapes* of W that index the Lehrer-Solomon decomposition (2.3) of $A(W)$ as follows. For $I, J \subseteq S$, define $I \sim J$ if $J = wIw^{-1}$ for some w in W. This defines an equivalence relation on the power set of S. A *shape* (for W) is a $\sim$-equivalence class. Let Λ denote the set of shapes and for each $\lambda \in \Lambda$, fix once and for all a representative $I_\lambda \in \lambda$ and set $l_\lambda = |I_\lambda|$.

Lehrer and Solomon [11, §2] have shown that the representation of W on $A^p(W)$ decomposes as a direct sum of induced representations:

$$A^p(W) \cong \bigoplus_{\substack{\lambda\in\Lambda \\ l_\lambda = p}} \operatorname{Ind}_{N_{I_\lambda}}^{W} A(W)_{I_\lambda}. \tag{2.3}$$

Notice that for $I \subseteq S$, W_I is a Coxeter group with Coxeter generating set I, and that V_I is the complexification of the reflection representation of W_I. Thus, we may consider the Orlik-Solomon algebra $A(W_I)$ of W_I. Clearly the action of W_I on $A(W_I)$ extends to an action of N_I, and so in particular to a representation of N_I on the top component $A^{|I|}(W_I)$. It follows easily from a standard property of Orlik-Solomon algebras (see [15, §3.1, Cor. 6.28]) that there is an N_I-equivariant isomorphism $A(W)_I \cong A^{|I|}(W_I)$. Therefore, summing over p, the decomposition (2.3) and Frobenius reciprocity yield

$$A(W)^W = A^l(W)^W + \sum_{\lambda\in\Lambda\setminus\{S\}} (A(W)_{I_\lambda})^{N_{I_\lambda}} \cong A^l(W)^W \oplus \bigoplus_{\lambda\in\Lambda\setminus\{S\}} A^{l_\lambda}(W_{I_\lambda})^{N_{I_\lambda}}. \tag{2.4}$$

The decomposition (2.4) reduces the computation of $A(W)^W$ to that of $A^l(W)^W$ and $A^{|I|}(W_I)^{N_I}$, for I a proper subset of S. We show below that the non-zero summands are indexed by the set of conjugacy classes of special involutions, that each non-zero summand is one-dimensional, and that this decomposition is just the decomposition of $A(W)^W$ into one-dimensional subspaces given by the basis in Corollary 2.2.

2.3. **Top degree invariants.** Consider first the summand $A^l(W)^W$ in (2.4). Following Richardson [12], we say that a subset $I \subseteq S$ satisfies the (-1)-condition if W_I contains an element that acts as -1 on V_I. Let w_I denote the longest element in W_I with respect to the length function determined by S. Obviously I satisfies the (-1)-condition if and only if each irreducible factor of W_I does. In addition, it is straightforward to check that, for W_I irreducible, I satisfies the (-1)-condition if and only if w_I is equal to $-\mathrm{id}_{V_I}$ (see [12, §1]). It follows that in general, I satisfies the (-1)-condition if and only if w_I is equal to $-\mathrm{id}_{V_I}$.

Taking $I = S$, it is clear that if S satisfies the (-1)-condition, then w_S is a special involution in W. Conversely, Felder and Veselov [5] have observed that if W is irreducible and S does not satisfy the (-1)-condition, then w_S is a not a special involution. It is immediate from the definition that an involution $t \in W$ is special if and only if the components of t in each irreducible factor of W are special. It follows that in general, S satisfies the (-1)-condition if and only if w_S is a special involution in W.

As noted above, Brieskorn has computed the Poincaré polynomials of the graded vector spaces $A(W)^W$ for all irreducible W. It follows from this computation that $\dim A^l(W)^W = 1$ or 0 according as to whether or not S satisfies the (-1)-condition. It follows that in general, S satisfies the (-1)-condition if and only if $A^l(W)^W \neq 0$, and if so, then $A^l(W)^W$ is one-dimensional.

To summarize, the following are equivalent for any finite Coxeter group:

- $A^l(W)^W \neq 0$.
- The longest element in W acts as minus the identity in the reflection representation.
- The longest element in W is a special involution.

Notice that for $I \subseteq S$, we have $S(w_I) = I$ and hence $a_I = a_{S(w_I)}$. We can now state our main theorem.

Theorem 2.5. *Suppose W is a finite Coxeter group with Coxeter generating set S of size $|S| = l$. The following are equivalent:*

(1) $A^l(W)^W \neq 0$.
(2) The longest element in W is a special involution.
(3) $\mathrm{Av}(a_S) \neq 0$.

If these conditions hold, then $A^l(W)^W$ is one-dimensional with generator $\mathrm{Av}(a_S)$.

Proof. The equivalence of (1) and (2) is explained above, and it is clear that if $\mathrm{Av}(a_S) \neq 0$, then $A^l(W)^W \neq 0$. Thus, it remains to show that if w_S is a special involution, then $\mathrm{Av}(a_S) \neq 0$. It follows from the preceding discussion that without loss of generality we may assume that W is irreducible. Then w_S is a special involution if and only if W is of type A_1, B_n, D_{2n}, F_4, E_7, E_8, H_3, H_4, or $I_2(2n)$. Felder and Veselov [5] have established the statement for all types other than E_7, E_8, F_4, H_3, and H_4. We have checked these remaining instances by machine computations. The most challenging cases are when W is of type E_7 and E_8, requiring sophisticated programming techniques and intricate reductions to deal with the relations in $A(W)$. Details regarding the implementation of these computations are given in the next section. □

The summands in (2.4) not equal $A^l(W)^W$ are described in the next lemma.

Lemma 2.6. *Let $I \subseteq S$ with $|I| = p$ and consider $A^p(W_I)^{N_I}$.*

(1) Suppose I does not satisfy the (-1)-condition. Then $A^p(W_I)^{N_I} = 0$.

(2) *Suppose I satisfies the* (-1)*-condition and* w_I *is a not special involution in* W*. Then* $A^p(W_I)^{N_I} = 0$.
(3) *Suppose I satisfies the* (-1)*-condition and* w_I *is a special involution in* W*. Then* $A^p(W_I)^{N_I}$ *is one-dimensional and* $\operatorname{Av}(a_I) \neq 0$.

Proof. By Theorem 2.5 we may assume that I is a proper subset of S.

If I does not satisfy the (-1)-condition, then $A^p(W_I)^{W_I} = 0$, by Theorem 2.5, and $A^p(W_I)^{N_I} \subseteq A^p(W_I)^{W_I}$, so $A^p(W_I)^{N_I} = 0$.

In order to handle the cases when I does satisfy the (-1)-condition, we need to recall some facts about the structure of the normalizer N_I due to Howlett and Pfeiffer-Röhrle. First, Howlett [8] has shown that W_I has a canonical complement in N_I, denoted here by C_I. Second, Pfeiffer and Röhrle [16] have shown, under the assumption that I satisfies the (-1)-condition, w_I is a special involution in W if and only if C_I centralizes W_I.

Now suppose I satisfies the (-1)-condition and w_I is a not special involution in W. Then $A^p(W_I)^{N_I} \subseteq A^p(W_I)^{W_I}$, $A^p(W_I)^{W_I}$ is one-dimensional with generator $\operatorname{Av}_I(a_I)$, where $\operatorname{Av}_I : A(W_I) \to A(W_I)^{W_I}$ denotes the averaging map for W_I, and C_I does not centralize W_I. We may assume that W is irreducible. Then it follows from the classification of irreducible finite Coxeter groups that W_I has at most one component not of type A, and because I satisfies the (-1)-condition, each component of type A also satisfies the (-1)-condition and so is of type A_1. Moreover, the component not of type A must be of type B_k $(k \geq 2)$, D_{2k} $(k \geq 2)$, E_7, or H_3. Considering these possibilities case-by-case using the description of C_I in [8], it can be checked that in all cases when C_I does not centralize W_I, the group C_I contains an element c that acts on W_I as a graph automorphism that transposes two nodes of the Coxeter graph of W_I and leaves the other nodes fixed.

Thus the relations of $A(W)$ yield $c(a_I) = -a_I$ and so

$$c\big(\operatorname{Av}_I(a_I)\big) = \operatorname{Av}_I(c(a_I)) = -\operatorname{Av}_I(a_I),$$

showing that $\operatorname{Av}_I(a_I)$ is not invariant under N_I. Consequently, $A^p(W_I)^{N_I} \neq A^p(W_I)^{W_I}$, whence $A^p(W_I)^{N_I} = 0$ as $\dim A^p(W_I)^{W_I} = 1$.

Finally, suppose I does satisfy the (-1)-condition and w_I is a special involution in W. Then $A^p(W_I)^{N_I} \subseteq A^p(W_I)^{W_I}$, $A^p(W_I)^{W_I}$ is one-dimensional with generator $\operatorname{Av}_I(a_I)$, and C_I centralizes W_I. Hence, for all $c \in C_I$, $c\big(\operatorname{Av}_I(a_I)\big) = \operatorname{Av}_I(a_I)$ and so $A^p(W_I)^{N_I} = A^p(W_I)^{W_I} \neq 0$. To complete the proof, let $Y \subseteq W$ be a complete set of left N_I-coset representatives in W. Then

$$\operatorname{Av}(a_I) = |Y|^{-1} \sum_{y \in Y} y\big(\operatorname{Av}_I(a_I)\big) \in \sum_{y \in Y} y\big(A(W)_I\big).$$

But now the sum $\sum_{y \in Y} y\big(A(W)_I\big)$ in (2.4) is direct and $y\big(\operatorname{Av}_I(a_I)\big) \in y\big(A(W)_I\big)$ for $y \in Y$, so $\operatorname{Av}(a_I) \neq 0$. □

2.4. **Proof of Theorem 2.1.** Richardson [12] has shown that $t \in W$ is an involution if and only if there is a subset $I \subseteq S$ that satisfies the (-1)-condition such that w_I is conjugate to t. Therefore, if t is a special involution, there is a subset $I \subseteq S$ that satisfies the (-1)-condition such that t is conjugate to w_I. But then w_I is a special involution and $\operatorname{Av}(a_{S(t)}) = \pm \operatorname{Av}(a_I)$, so it follows from Theorem 2.5 and Lemma 2.6 that $\operatorname{Av}(a_{S(t)}) \neq 0$.

Finally, it follows from the decomposition (2.4), Theorem 2.5, and Lemma 2.6, that $A(W)^W$ is spanned by the elements $\operatorname{Av}(a_I)$ where I runs over the subsets of S that satisfy the (-1)-condition and for which w_I is a special involution. More precisely, if Λ_{-1}

denotes the set of shapes consisting of subsets that satisfy the (-1)-property and Λ_1 denotes the set of shapes consisting of subsets I such that C_I centralizes W_I, then $\Lambda_{-1} \cap \Lambda_1$ indexes the set of conjugacy classes of special involutions and $\{ \operatorname{Av}(a_{I_\lambda}) \mid \lambda \in \Lambda_{-1} \cap \Lambda_1 \}$ is a basis of $A(W)^W$.

3. Computational and algorithmic aspects

We have implemented the relations for the Orlik-Solomom algebra $A(W)$ with the use of the computer algebra system GAP3 [17] and the CHEVIE package [6]. The papers [1], [2], and [3] contain some of the details of this implementation. In this section, we describe some refinements of our earlier techniques that allow us to complete the computations used in the proof of Theorem 2.5.

3.1. **The broken circuit bases of $A(W)$.** The broken circuit bases of $A(W)$ is a computationally efficient basis to use for machine calculations for individual Coxeter groups that is compatible with the decomposition of $A(W)$ arising from (2.3). For later reference we briefly recall the construction of this basis.

Recall the fixed linear order on $R = \{ r_1, \dots, r_n \}$. Recall that a subset $T \subseteq R$ is *independent* if $\operatorname{codim}(\bigcap_{r\in T} V_{\mathbb{R}}^r) = |T|$ and *dependent* otherwise. A *circuit* is a subset of R that is minimally linearly dependent. That is, it is linearly dependent, but any proper subset is linearly independent. A *broken circuit* is a subset of R that is obtained from a circuit by deleting the maximal element with respect to the fixed linear order on R. Thus, broken circuits are subsets of the form $\{r_{i_1}, \dots, r_{i_p}\}$ where there is a $j > i_p$ so that $\{r_{i_1}, \dots, r_{i_p}, r_j\}$ is a circuit. A subset of R is *χ-independent* if it does not contain a broken circuit.

It is convenient to identify $R = \{r_1, \dots, r_n\}$ with the set $\{1, \dots, n\}$ and to identify ordered subsets of R with words in the alphabet $\{1, \dots, n\}$. If $T = i_1 \cdots i_p$ is such a word, then adjectives applied to $\{r_{i_1}, \dots, r_{i_p}\}$ are also applied to T. For example, $T = i_1 \cdots i_p$ is *independent* if the subset $\{r_{i_1}, \dots, r_{i_p}\}$ of R is independent.

Write a_i instead of a_{r_i} for the corresponding algebra generator of $A(W)$. Given a word $T = i_1 \cdots i_p$ of positive integers less than or equal n, define an element, a_T, in $A^p(W)$ by $a_T = a_{i_1} \cdots a_{i_p}$ (in analogy with the definiton of a_T for a *subset* T of R in Section 2). Let $\mathcal{B}$ denote the set of all χ-independent words $i_1 \cdots i_p$ such that $i_1 < \cdots < i_p$. It is shown in [15, §3.1] that $\{ a_T \mid T \in \mathcal{B} \}$ is a basis of $A(W)$, called there a *broken circuit* basis. A broken circuit basis is a common basis for the subspaces $A(W)^p$ and $A(W)_I$ of $A(W)$ and is compatible with the isomorphisms $A(W)_I \cong A^{|I|}(W_I)$ for $I \subseteq S$.

When working in GAP3 it is more convenient to let groups act on the right. Thus, in this section we consider the right action of W on $A(W)$ that satisfies $a_T.w = a_{T.w}$, where if $T = i_1 \cdots i_p$, then $T.w = j_1 \cdots j_p$, where $w^{-1} r_{i_1} w = r_{j_1}, \dots, w^{-1} r_{i_p} w = r_{j_p}$. Let $|T.w| = j_1' \cdots j_p'$ be a rearrangement of $T.w$ in increasing order and let $\epsilon(T, w)$ be the sign of a permutation that is needed to sort the word $T.w$ in increasing order. Then $a_T.w = a_{T.w} = \epsilon(T, w) a_{|T.w|}$.

For $a \in A(W)$, let us denote by $\overline{a}$ the coordinate vector of a with respect to the broken circuit basis $\{a_T \mid T \in \mathcal{B}\}$ of $A(W)$, i.e., an explicit list of coefficients $\beta_T \in \mathbb{C}$ such that $a = \sum_T \beta_T a_T$. In the application, most coefficients β_T are zero and the list can be stored as a sparse list consisting of the non-zero coefficients only.

The proof of Theorem 2.5 boils down to computing

$$\omega = a_S. \sum_{w\in W} w = \sum_{w \in W} a_S.w.$$

The task of checking whether $\omega \neq 0$ reduces to

(1) computing the image $a_S.w$ of a_S under each group element $w \in W$,
(2) expressing each image $a_S.w$ as $\overline{a_S.w}$ in terms of the broken circuit basis,
(3) computing $\overline{\omega} = \sum_{w \in W} \overline{a_S.w}$.

While this looks straightforward (and in the case of small groups W it is straightforward), it can be challenging for higher rank Coxeter groups of exceptional type, i.e., for E_7 and E_8. The difficulties arise from

- the order of W and hence the number of images $a_S.w$ that need to be determined,
- the need to explicitly express an element a_T for arbitrary subsets T of R as a linear combination $\overline{a_T}$ of the broken circuit basis,
- the need to efficiently represent the $|W|$ elements of the broken circuit basis of $A(W)$.

We address all these points in turn in the following subsections.

3.2. **Decomposing W.** In all cases, it turns out that the element ω has tiny support in the broken circuit basis of $A(W)$ relative to the size of W. In contrast, this need not be the case for intermediate results, and the time it takes to compute $\overline{\omega}$ depends subtly on the order in which various steps are taken. We chose to separate the calculation as follows.

The standard parabolic subgroup W_J has a distinguished set D of left coset representatives, consisting of the unique elements of minimal length in their coset. As each element $w \in W$ has a decomposition $w = x \cdot w'$ for uniquely determined elements $x \in D$, $w' \in W_J$, in the group algebra of W we can write

$$\sum_{w \in W} w = \Big(\sum_{x \in D} x\Big) \cdot \Big(\sum_{w' \in W_J} w'\Big).$$

In fact, there are parabolic subgroups

$$\{1\} = W_0 < W_1 < \cdots < W_l = W,$$

such that W_{j-1} is a maximal standard parabolic subgroup of W_j, and $W_j = D_j W_{j-1}$ for the distinguished set D_j of left coset representatives of W_{j-1} in W_j, for $j = 1, \ldots, l$. Thus each element $w \in W$ can be written as

$$w = x_l \cdots x_2 \cdot x_1,$$

for uniquely determined elements $x_j \in D_j$, $j = 1, \ldots, l$. Hence, in the group algebra of W,

$$\sum_{w \in W} w = \Big(\sum_{x_l \in D_l} x_l\Big) \cdots \Big(\sum_{x_2 \in D_2} x_2\Big) \cdot \Big(\sum_{x_1 \in D_1} x_1\Big),$$

and we can compute

$$\omega = \Big(\Big(\cdots \Big(a_S. \sum_{x_l \in D_l} x_l\Big) \cdots\Big) \cdot \sum_{x_2 \in D_2} x_2\Big) \cdot \sum_{x_1 \in D_1} x_1.$$

In this way, instead of $\prod |D_j| = |W|$, only $\sum |D_j|$ images of algebra elements under group elements need to be computed and converted into the basis.

In practice, we use the chain of parabolics induced by the labelling of generators $S = \{s_1, \ldots, s_l\}$ in CHEVIE, with $W_j = \langle s_1, \ldots, s_j \rangle$, $j = 1, \ldots, l$. In the case of E_8 with Coxeter diagram

```
        2
        |
1 - 3 - 4 - 5 - 6 - 7 - 8 ,
```

this reduces the number of image calculations from a formidable $|W| = 696,729,600$ to a mere $\sum |D_j| = 356$. However, the algebra elements now are linear combinations of words, rather than just words.

Set $q_j = a_S . \sum_{x_l \in D_l} x_l \cdots \sum_{x_j \in D_j} x_j$, for $j = 1, \dots, l$. Then $\omega = q_1$. Now $\overline{\omega}$ is computed in l steps, for j from l down to 1, as follows. Assuming that $\overline{q_{j+1}}$ is known, one obtains

$$\overline{q_j} = \overline{\overline{q_{j+1}}. \sum_{x \in D_j} x} = \sum_{x \in D_j} \overline{\overline{q_{j+1}}.x}.$$

Here, if $\overline{q_{j+1}} = \sum_T \beta_T a_T$, then

$$\overline{\overline{q_{j+1}}.x} = \sum_T \beta_T \overline{a_T.x} = \sum_T \beta_T \, \epsilon(T, x) \, \overline{a_{|T.x|}}.$$

Initially, this requires us to compute $\overline{a_S}$. For this, it turns out to be convenient to choose an order on R that makes a_S a basis element, or at least close to one.

3.3. **Rewrite Rules.** In order to express arbitrary elements of $A(W)$ in terms of the broken circuit basis, we need to be able to express an element a_T, for an arbitrary word $T = i_1 \cdots i_p$ with $i_1 < \cdots < i_p$, in terms of the broken circuit basis, i.e., to compute the coefficients of $\overline{a_T}$. First we note that the broken circuit basis has the following useful *Schreier property*: if $T = i_1 \cdots i_p$ is in $\mathcal{B}$, then T' is in $\mathcal{B}$ for any *prefix* $T' = i_1 \dots i_k$ of T ($k \leq p$). Thus, if T is a strictly increasing word and T' is a proper prefix of T such that $a_{T'}$ is not a basis element, then neither is a_T. Using the relations in $A(W)$, we compute $\overline{a_T}$ as follows.

(1) Find the minimal k such that $i_1 \cdots i_k$ contains a broken circuit. If no such k exists, then a_T is a basis element of $A(W)$ (by definition).
(2) Otherwise, find the maximal index u such that $i_1 \cdots i_k \, u$ is a circuit (such u exists, is larger than i_k, and can easily be identified by computing the rank of the corresponding matrix of root vectors).
(3) If u occurs in T, then $a_T = 0$. Otherwise, using the relations in $A(W)$,

$$i_1 i_2 \cdots i_k = \sum_j (-1)^{k-j} (i_1 \cdots \hat{i}_j \cdots i_k) u$$

and we can compute $\overline{a_T}$ recursively as

$$\overline{a_T} = \sum_j (-1)^{k-j} \overline{(i_1 \cdots \hat{i}_j \cdots i_k) u (i_{k+1} \cdots i_p)}.$$

This process must terminate since (in the lexicographic order of words in $\{1, \dots, n\}$) all of the replacement terms on the right hand side are strictly bigger than the original word T.

3.4. **Constructing and Managing a Basis.** The above procedure for expressing an element of $A(W)$ in the broken circuit basis depends on an efficient procedure for distinguishing words of $\mathcal{B}$ from other words. The definition of a broken circuit basis is not particularly well suited for this purpose: testing whether a subword of a word T is in $\mathcal{B}$ in isolation is not straightforward, and the cost of testing all subwords of T is exponential. This task can be carried out more efficiently in the presence of some pre-computed data. If, for example, a complete list of words in $\mathcal{B}$ is known, then deciding whether an arbitrary increasing word T is in $\mathcal{B}$ or not is a simple lookup operation. However, as $|\mathcal{B}| = |W|$, such a list is expensive to compute and to store for larger groups.

Here, taking advantage of the Schreier property, we use a rooted, directed acyclic graph Γ on a small number of nodes to represent the words in $\mathcal{B}$. The root node, labelled 0, corresponds to the empty word. All other nodes are labelled by the positive integers indexing the generators $a_1, \ldots, a_n$ of $A(W)$. In this graph, directed paths starting at the root node represent words in $\mathcal{B}$. To decide whether a given word lies in $\mathcal{B}$, one simply traces the word (reading from left to right), beginning at the root node, through the graph. If at some point no edge leads to a node labelled by the next letter, the corresponding prefix (and hence the word) is not in $\mathcal{B}$ (whereas all prefixes so far were in $\mathcal{B}$).

The graph Γ for W of type A_3 with the reflections linearly ordered by $s_{12} < s_{23} < s_{34} < s_{13} < s_{24} < s_{14}$ is given in Figure 3. For example the words 2, 2 4, and 2 4 6 are in $\mathcal{B}$ and the word 2 4 5 is not.

We construct such a graph as follows. First of all, it is useful to represent the subsets of $\{1, \ldots, n\}$ with at most $l + 1$ elements as nodes in a rooted, ranked tree Υ, with nodes labeled by $\{0, 1, \ldots, n\}$. Here, the root node, labeled 0, corresponds to the empty set and has rank 0. Each other node represents the subset consisting of the labels of the nodes along the unique path back to the root node (excluding the root node). Figure 1 shows this tree for the case when $l = 3$ and $n = 6$. For example, the last circled node labelled by 5 with rank 3 represents the subset $\{3, 4, 5\}$, obtained from the path 0-3-4-5. The formal definition of Υ is easily extracted from this example.

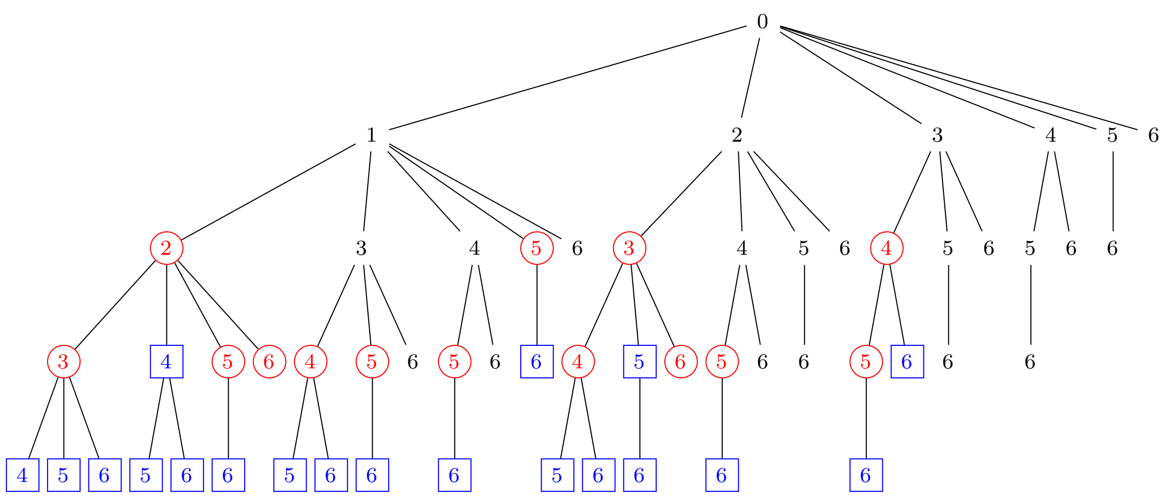

FIGURE 1. Υ: Subsets of $\{1, 2, 3, 4, 5, 6\}$

In the case at hand, the nodes in Υ can be decorated to encode information about the sets of reflections in R that they ultimately represent. In Figure 1, square nodes indicate dependent sets and circled nodes indicate independent sets that contain a broken circuit. The remaining nodes, by definition, correspond to the broken circuit basis, and form a subtree, $\Upsilon_{\mathcal{B}}$, shown in Figure 2.

The tree $\Upsilon_{\mathcal{B}}$ can alternately be constructed recursively by successively adding the nodes with labels $1, 2, \ldots, n$ to the tree consisting of the root node 0 only. Let us call the *tree at stage* m the tree consisting of nodes with labels $0, 1, \ldots, m$. The tree at stage m is constructed from the tree at stage $m - 1$ by checking, for *each node* in the stage $m - 1$ tree, whether it can be extended by a node with label m, and if so, then by adding a node with label m.

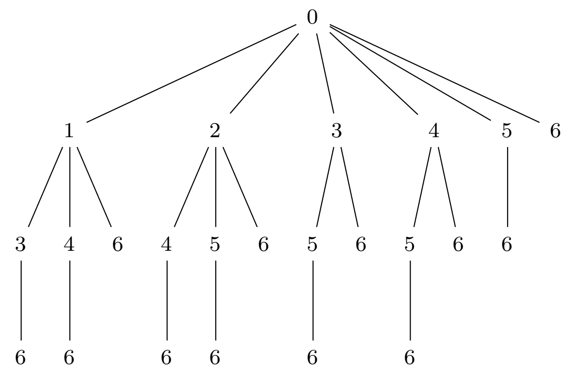

FIGURE 2. $\Upsilon_{\mathcal{B}}$: Words in $\mathcal{B}$

To decide whether the node with word $i_1 \cdots i_k$ in the tree at stage $m-1$ can be extended by a node labelled m, we use the following observation: Suppose $i_1 \cdots i_k$ is a word in $\mathcal{B}$ with $i_k < m$. Then the word $i_1 \cdots i_k\, m$ *contains* (we don't claim it *is*) a broken circuit if and only if there is an index $u > m$ such that the word $i_1 \cdots i_k\, m\, u$ is dependent. Indeed, since $i_1 \cdots i_k$ does not contain a broken circuit, if $i_1 \cdots i_k\, m$ contains a broken circuit, then this broken circuit must contain m.

In the example in Figure 2, many subtrees appear repeatedly in the tree $\Upsilon_{\mathcal{B}}$ and carry redundant information. This suggests storing the information in the form of a smaller directed acyclic graph with the property that each rooted path in this smaller graph corresponds to a node in the original tree with the same rooted path.

Such a graph Γ is constructed from $\Upsilon_{\mathcal{B}}$ by starting with the leftmost maximal path in $\Upsilon_{\mathcal{B}}$, then adjoining the other maximal paths (say from left to right), then adjoining any missing paths of length $l-1$, then adjoining any missing paths of length $l-2$, and so on. Continuing the example of W of type A_3, the graph Γ has 9 nodes (as opposed to 24 in the orignal tree) and is given in Figure 3.

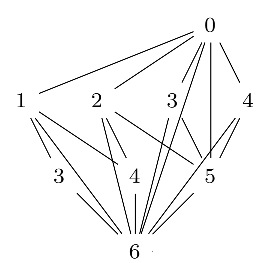

FIGURE 3. The graph Γ for W of type A_3

Finally, the rooted paths in Γ can be enumerated by a recursive depth first traversal. Thus, the graph Γ can be alternately be constructed in the same fashion as $\Upsilon_{\mathcal{B}}$, by successively adding the nodes with label $1, 2, \ldots, n$, and carefully tracking of the prefixes represented by nodes with the same label.

Naturally, the graph Γ depends on the chosen total order on R. In the case of E_8, with the order of roots and reflections as produced by CHEVIE, the graph Γ has $1,207,608$ nodes and $15,552,964$ edges, representing the $|W| = 696,729,600$ basis elements.

Acknowledgments: The research of this work was supported by the Simons Foundation (Grant #245399 to J.M. Douglass) and by the DFG (Grant #RO 1072/16-1 to G. Röhrle). J.M. Douglass would like to acknowledge that some of this material is based upon work supported by (while serving at) the National Science Foundation. Part of the research for this paper was carried out during a stay at the Mathematical Research Institute Oberwolfach supported by the "Research in Pairs" program.

References

[1] M. Bishop, J.M. Douglass, G. Pfeiffer, and G. Röhrle. Computations for Coxeter arrangements and Solomon's descent algebra: Groups of rank three and four. *Journal of Symbolic Comput.*, 50:139–158, 2013.

[2] M. Bishop, J.M. Douglass, G. Pfeiffer, and G. Röhrle. Computations for Coxeter arrangements and Solomon's descent algebra II: Groups of rank five and six. *J. Algebra*, 377:320–332, 2013.

[3] M. Bishop, J.M. Douglass, G. Pfeiffer, and G. Röhrle. Computations for Coxeter arrangements and Solomon's descent algebra III: Groups of rank seven and eight. *J. Algebra*, 423:1213–1232, 2015.

[4] E. Brieskorn. Sur les groupes de tresses [d'après V. I. Arnold]. In *Séminaire Bourbaki, 24ème année (1971/1972), Exp. No. 401*, pages 21–44. Lecture Notes in Math., Vol. 317. Springer, Berlin, 1973.

[5] G. Felder and A. P. Veselov. Coxeter group actions on the complement of hyperplanes and special involutions. *J. Eur. Math. Soc. (JEMS)*, 7(1):101–116, 2005.

[6] M. Geck, G. Hiß, F. Lübeck, G. Malle, and G. Pfeiffer. CHEVIE — A system for computing and processing generic character tables. *Appl. Algebra Engrg. Comm. Comput.*, 7:175–210, 1996.

[7] M. Geck and G. Pfeiffer. *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, volume 21 of *London Mathematical Society Monographs. New Series.* The Clarendon Press,' Oxford University Press, New York, 2000.

[8] R. B. Howlett. Normalizers of parabolic subgroups of reflection groups. *J. London Math. Soc. (2)*, 21(1):62–80, 1980.

[9] R.B. Howlett and G.I. Lehrer. Duality in the normalizer of a parabolic subgroup of a finite Coxeter group. *Bull. London Math. Soc.*, 14(2):133–136, 1982.

[10] G.I. Lehrer. On the Poincaré series associated with Coxeter group actions on complements of hyperplanes. *J. London Math. Soc. (2)*, 36(2):275–294, 1987.

[11] G.I. Lehrer and L. Solomon. On the action of the symmetric group on the cohomology of the complement of its reflecting hyperplanes. *J. Algebra*, 104(2):410–424, 1986.

[12] R. W. Richardson, Conjugacy classes of involutions in Coxeter groups. *Bull. Austral. Math. Soc.* 26(1)1–15, 1982.

[13] P. Orlik and L. Solomon. Combinatorics and topology of complements of hyperplanes. *Invent. Math.*, 56(2):167–189, 1980.

[14] P. Orlik and L. Solomon. Coxeter arrangements. In *Singularities*, volume 40 of *Proc. Symp. Pure Math.*, pages 269–292. Amer. Math. Soc., 1983.

[15] P. Orlik and H. Terao. *Arrangements of Hyperplanes.* Springer-Verlag, 1992.

[16] G. Pfeiffer and G. Röhrle, Special involutions and bulky parabolic subgroups in finite Coxeter groups, *J. Aust. Math. Soc.*, 79(1):141–147, 2005.

[17] M. Schönert et al. *GAP – Groups, Algorithms, and Programming – version 3 release 4*. Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 1997.

[18] L. Solomon. A decomposition of the group algebra of a finite Coxeter group. *J. Algebra*, 9:220–239, 1968.

Division of Mathematical Sciences, National Science Foundation, 2415 Eisenhower Ave, Alexandria, VA 22314, USA
E-mail address: mdouglas@nsf.gov

School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway, University Road, Galway, Ireland
E-mail address: goetz.pfeiffer@nuigalway.ie

Fakultät für Mathematik, Ruhr-Universität Bochum, D-44780 Bochum, Germany
E-mail address: gerhard.roehrle@rub.de