Hilbert Series of Quasi-invariant Polynomials of D_n in Characteristic p

Shuxuan (Judy) Li

Under the direction of

Frank Wang
Department of Mathematics
Massachusetts Institute of Technology

Research Science Institute
July 29th, 2025

Abstract

Let $Q_m(W,\mathbb{F})$ denote the space of m-quasi-invariant polynomials of a finite Coxeter group W over a field $\mathbb{F}$. The Hilbert series of both $Q_m(S_n,\mathbb{C})$ and $Q_m(S_n,\mathbb{F}_p)$ have already been extensively studied. Quasi-invariant polynomials of the dihedral group have only been studied by Feigin and Veselov in 2003, who proved the general form of the Hilbert series of $Q_m(D_n,\mathbb{C})$. In this paper, we explore the Hilbert series of $Q_m(D_n,\mathbb{F}_{p^k})$, where k is such that a primitive $2n^{\text{th}}$ root of unity is defined in $\mathbb{F}_{p^k}$. In particular, we prove a sufficient condition for which the Hilbert series of $Q_m(D_n,\mathbb{F}_{p^k})$ is different from that of $Q_m(D_n,\mathbb{C})$. In addition, we prove results about the generators of $Q_m(D_n,\mathbb{F}_{p^k})$, which are relevant to our conjectured form of the Hilbert series of $Q_m(D_4,\mathbb{F}_{p^k})$. In doing so, we come closer to understanding quasi-invariant polynomials with respect to any finite Coxeter group.

Summary

Invariant polynomials of Coxeter groups are polynomials that remain unchanged under certain transformations on its variables known as reflections. Quasi-invariant polynomials are generalizations of invariant polynomials of Coxeter groups, and the study of these polynomials is motivated by their relevance to quantum particle systems and other areas of mathematics such as representation theory. We compare the space of quasi-invariant polynomials over different mathematical structures known as fields by examining their Hilbert series, which encode information about the space.

Contents

1 Introduction

Polynomials that are invariant under the action of some finite Coxeter group, which is a group generated by reflections, are fundamental objects of study in algebra. A quintessential example is the symmetric polynomials, which are invariant under the action of the symmetric group. Notably, in 1955, Chevalley [1] proved the classical result that the algebra of polynomials invariant under a Coxeter group is freely generated by some homogeneous polynomials. In the case of the symmetric group, these generators are the elementary symmetric polynomials.

Quasi-invariant polynomials are a generalization of invariant polynomials with respect to some finite Coxeter group. They were first introduced in 1990 by Chalykh and Veselov [2] in their study of quantum Calogero-Moser systems. These one-dimensional dynamical particle systems were found to be exactly solvable [3] as well as integrable [4]. Quasi-invariant polynomials of the symmetric group describe the harmonic, zero-eigenvalue eigenfunctions of these systems, and are therefore of great interest in mathematical physics.

Furthermore, quasi-invariant polynomials were later found to have fascinating connections with the representation theory of the rational Cherednik algebra. The rational Cherednik algebra is Morita equivalent to its spherical subalgebra, and Berest, Etingof, and Ginzburg [5] showed that there is a unique representation of the spherical subalgebra on the space of quasi-invariant polynomials. In 2021, Braverman, Etingof, and Finkelberg [6] showed that the cyclotomic double affine Hecke algebra (DAHA), a deformation of the rational Cherednik algebra, acts on the space of q-deformed quasi-invariant polynomials. The rational Cherednik algebra has connections to multiple fields of mathematics such as combinatorics and algebraic geometry, and is a central topic in representation theory.

Quasi-invariant polynomials of the symmetric group have been extensively studied over fields of characteristic zero [6, 7] as well as over fields of positive characteristic [8, 9, 10]. In particular, Felder and Veselov in 2001 [7] computed the Hilbert series and lowest degree nonsymmetric elements of $Q_m(S_n, \mathbb{C})$, the space of m-quasi-invariant polynomials of S_n over the field $\mathbb{C}$. In 2020, Ren and Xu [8] proved a sufficient condition on p for the Hilbert series of $Q_m(S_n, \mathbb{F}_p)$ to be different from the Hilbert series of $Q_m(S_n, \mathbb{C})$. They also conjectured a general form for the Hilbert series of $Q_m(S_3, \mathbb{F}_p)$, which was proven by Wang [9] in 2023 for $p > 3$. Recently, the Hilbert series of $Q_m(S_3, \mathbb{F}_2)$ and $Q_m(S_3, \mathbb{F}_3)$ were also computed by Wang and Yee [10].

Quasi-invariant polynomials of the dihedral group have so far only been investigated by Feigin and Veselov [11] in 2003, who computed the Hilbert series of $Q_m(D_n, \mathbb{C})$. This paper builds on their work by studying the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$, where k is such that a $2n^{\text{th}}$ primitive root of unity exists in $\mathbb{F}_{p^k}$. The dihedral groups are the Coxeter groups of rank 2, so through our work, we come closer to understanding quasi-invariant polynomials with respect to any finite Coxeter group.

The paper is structured as follows. In Section 2, we provide the definition of quasi-invariant polynomials and key properties of D_n and $Q_m(D_n, \mathbb{F})$ to formalize the problem we are studying. In

Section 3, we recall results from literature that we use in the paper. In Sections 4-5, we compare the Hilbert series in characteristic p and in characteristic 0. The main result is Theorem 5.1, which provides a sufficient condition for which the Hilbert series in characteristic p is different from characteristic 0. In Sections 6-7, we prove results relevant to our conjectured expression of the Hilbert series of $Q_m(D_4, \mathbb{F}_{p^k})$ in Conjecture 6.1.

2 Preliminaries

In this section, we explain key definitions and fundamental properties relevant to the space of m-quasi-invariant polynomials of the dihedral group over a field $\mathbb{F}$. Let us begin by formally defining m-quasi-invariant polynomials, the main object of our study.

2.1 Main object: m-quasi-invariant polynomials

Quasi-invariant polynomials are defined with respect to a finite Coxeter group W, which is a finite group with presentation $\langle s_1, \ldots, s_k \mid (s_i s_j)^{m_{ij}} = 1\rangle$, where $m_{ii} = 1$ and $m_{ij} = m_{ji} \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ whenever $i \neq j$. We say that W is generated by the reflections $s_1, \ldots, s_k$. Let $\mathbb{F}$ be a field in which a $2m_{ij}^{\text{th}}$ root of unity is defined, which we denote by ω. Let $\mathfrak{h}$ be the $\mathbb{F}$-vector space with basis $\{e_1, \ldots, e_k\}$ and define an inner product $(\cdot, \cdot)$ on $\mathfrak{h}$ given by $(e_i, e_i) = 1$ and $(e_i, e_j) = \frac{-\omega-\omega^{-1}}{2}$ for every $i \neq j$. Then the action of each reflection s_i on $v \in \mathfrak{h}$ is given by $s_i(v) = v - 2(v, e_i)e_i$. We say that $\mathfrak{h}$ is the *reflection representation* of W.

Let $\Sigma \subset W$ denote the set of reflections in W. Choose $\alpha \in \mathfrak{h}^* - \{0\}$ so that the equation $\alpha = 0$ describes the reflection hyperplane Π_α for a reflection in Σ. We call this reflection s_α. For a polynomial $p \in \mathbb{F}[\mathfrak{h}]$ that is invariant under W, the polynomial $p(x) - p(s_\alpha x)$ vanishes on the reflection hyperplane Π_α to infinite order. A natural way to generalize these polynomials is to define polynomials $q \in \mathbb{F}[\mathfrak{h}]$ such that $q(x) - q(s_\alpha x)$ vanishes on Π_α to some order parametrized by a nonnegative integer m. This gives rise to the definition of m-quasi-invariant polynomials.

Definition 2.1 (Chalykh and Veselov [2])**.** A polynomial $q \in \mathbb{F}[\mathfrak{h}]$ is *m-quasi-invariant* with respect to W if for any $s_\alpha \in \Sigma$, the polynomial $q(x) - q(s_\alpha x)$ is divisible by $\alpha(x)^{2m+1}$.

We denote by $Q_m(W, \mathbb{F})$ the space of m-quasi-invariant polynomials with respect to W over $\mathbb{F}$. Previous work on quasi-invariant polynomials in characteristic 0 such as [11] uses an equivalent condition of m-quasi-invariance, given by $\partial_\alpha^{2l-1} q|_{\Pi_\alpha} = 0$ for all $l = 1, 2, \ldots, m$. However, in characteristic p, we have $\partial^N x^k = 0$ for all $N \geq p$. Specifically, this means that ∂^N cannot distinguish m-quasi-invariant polynomials from m'-quasi-invariant polynomials for any $m, m' \geq p$. Therefore, we consider an alternative equivalent condition for m-quasi-invariance.

Definition 2.2 ([12])**.** For $\alpha \in \mathfrak{h}^* - \{0\}$, complete α to a basis $\{\alpha, v_1, \ldots, v_j\}$ of $\mathfrak{h}$. Let us write $q \in \mathbb{F}[\mathfrak{h}]$ in this basis, that is, $q = \sum_k c_k(v_1, \ldots, v_j)\alpha^k$, where $c_k(v_1, \ldots, v_j)$ is a function in $v_1, \ldots, v_j$.

For $N \leq \min(k)$, the N^{th} *divided power of the partial derivative* is the map $\partial_\alpha^{(N)} : \mathbb{F}[\mathfrak{h}] \to \mathbb{F}[\mathfrak{h}]$ given by

$$\partial_\alpha^{(N)} q = \sum_k \binom{k}{N} c_k(v_1, \ldots, v_j)\alpha^{k-N}.$$

It follows from this definition that q is m-quasi-invariant if $\partial_\alpha^{(2l-1)} q|_{\Pi_\alpha} = 0$ for $l = 1, 2, \ldots, m$.

Remark. We omit our verification that this condition is equivalent, but note that in characteristic 0, we have $\partial_\alpha^{(N)} = \frac{\partial_\alpha^N}{N!}$, which recovers the condition $\partial_\alpha^{2l-1} q|_{\Pi_\alpha} = 0$. Furthermore, notice that $\partial^{(N)}$ is not killed in characteristic p for all $N \geq p$. For example, $\partial_\alpha^{(p)} \alpha^{p+1} = (p+1)\alpha^p = \alpha^p$.

Before we study the space $Q_m(D_n, \mathbb{F})$, we first consider some key properties of the dihedral group D_n.

2.2 The dihedral group D_n and its irreducible representations

The dihedral group D_n is the group of the $2n$ reflective and rotational symmetries of a regular n-gon. It has presentation $\langle s_1, s_2 \mid s_1^2 = s_2^2 = (s_1 s_2)^n = 1\rangle$. Here, s_1 and s_2 are reflections with the matrix representations $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \beta_2^2 & -\beta_1^2 \\ -\beta_1^2 & -\beta_2^2 \end{smallmatrix}\right)$ respectively, where $\beta_1^j = \frac{\omega^{-j} - \omega^j}{2i}$, $\beta_2^j = \frac{\omega^j + \omega^{-j}}{2}$, and ω is a primitive $2n^{\text{th}}$ root of unity. A rotation in D_n is the composition of two reflections, and we denote by r the rotation $s_1 s_2$.

For odd n, D_n has three irreducible representations: the trivial, the sign, and the standard representation. We denote them by ρ_0, ρ_{-1}, and ρ_1, respectively, and they are given by

$$\begin{array}{ccc} \rho_0 : D_n \to GL_1(\mathbb{F}) & \rho_{-1} : D_n \to GL_1(\mathbb{F}) & \rho_1 : D_n \to GL_2(\mathbb{F}) \\ s_1 \mapsto (1) & s_1 \mapsto (-1) & s_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ s_2 \mapsto (1) & s_2 \mapsto (-1) & s_2 \mapsto \begin{pmatrix} \beta_2^2 & -\beta_1^2 \\ -\beta_1^2 & -\beta_2^2 \end{pmatrix} \end{array}$$

where $\mathbb{F}$ can be any field in which the $2n^{\text{th}}$ roots of unity are defined.

For even n, there are two additional irreducible representations $\rho_{\pm 1}$ and $\rho_{\mp 1}$ of D_n, given by

$$\begin{array}{cc} \rho_{\pm 1} : D_n \to GL_1(\mathbb{F}) & \rho_{\mp 1} : D_n \to GL_1(\mathbb{F}) \\ s_1 \mapsto (1) & s_1 \mapsto (-1) \\ s_2 \mapsto (-1) & s_2 \mapsto (1). \end{array}$$

Due to the conditions on the field $\mathbb{F}$, the field of characteristic p we work in is $\mathbb{F}_{p^k}$, contrary to previous work such as [9] on quasi-invariant polynomials of the symmetric group over $\mathbb{F}_p$. The field $\mathbb{F}_{p^k}$ is the splitting field of $x^{p^k} - x$ over $\mathbb{F}_p$, where k is chosen such that a primitive $2n^{\text{th}}$ root of unity and $\sqrt{-1}$ are defined in $\mathbb{F}_{p^k}$. We assume that p does not divide $2n$, so that the representation theory of D_n over $\mathbb{F}$ is non-modular.

Notice that the standard representation is the reflection representation of D_n, and gives us the action of D_n on the ring of polynomials $\mathbb{F}[x_1, x_2]$. We denote $\beta_1^j x_1 + \beta_2^j x_2$ by α_j, and let s_{α_j} be the reflection about the line $\alpha_j = 0$. Now, we consider some useful properties of the space $Q_m(D_n, \mathbb{F})$.

2.3 The structure of $Q_m(D_n, \mathbb{F})$

Let $\mathbb{F}[x_1, x_2]^{D_n}$ denote the space of polynomials in $\mathbb{F}[x_1, x_2]$ that are invariant with respect to the action of D_n. We describe some fundamental properties of $Q_m(D_n, \mathbb{F})$ in the following proposition.

Proposition 2.3 (Collected in [13][1]). *Consider the spaces $\mathbb{F}[x_1, x_2]^{D_n}$ and $Q_m(D_n, \mathbb{F})$. We have that:*

(1) $\mathbb{F}[x_1, x_2]^{D_n} \subset Q_m(D_n, \mathbb{F})$, $Q_0(D_n, \mathbb{F}) = \mathbb{F}[x_1, x_2]$, and $Q_m(D_n, \mathbb{F}) \subset Q_{m'}(D_n, \mathbb{F})$ if $m > m'$.

(2) $Q_m(D_n, \mathbb{F})$ is a ring.

(3) $Q_m(D_n, \mathbb{F})$ is a finitely generated module over $\mathbb{F}[x_1, x_2]^{D_n}$.

As $Q_m(D_n, \mathbb{F})$ is a space of polynomials, it has a natural grading by degree

$$Q_m(D_n, \mathbb{F}) = \bigoplus_{d \geq 0} Q_{m,d}(D_n, \mathbb{F}),$$

where $Q_{m,d}(D_n, \mathbb{F})$ is the subspace consisting of homogeneous m-quasi-invariant polynomials of degree d. Thus, we may define a Hilbert series to encapsulate the structure of $Q_m(D_n, \mathbb{F})$.

Definition 2.4. Let $V = \bigoplus_{d=0}^{\infty} V_d$ be a graded vector space. The *Hilbert series* of V is the formal power series

$$\mathcal{H}(V) := \sum_{d \geq 0} \dim(V_d) t^d.$$

Example 2.5. Consider $V = \mathbb{F}[x_1, x_2]$. In this instance, each subspace V_d consists of homogeneous polynomials of degree d. Its Hilbert series is given by

$$\mathcal{H}(V) = 1 + 2t + 3t^2 + \cdots = \frac{1}{(1-t)^2}.$$

We denote the Hilbert series of $Q_m(D_n, \mathbb{F})$ by $H_{m,n,\mathbb{F}}(t)$. It is a known result that $\mathbb{F}[x_1, x_2]^{D_n}$ is a free polynomial algebra generated by a degree 2 polynomial and a degree n polynomial [14]. Since $Q_m(D_n, \mathbb{F})$ is a finitely generated module over $\mathbb{F}[x_1, x_2]^{D_n}$, we can write

$$H_{m,n,\mathbb{F}}(t) = \frac{G_{m,n,\mathbb{F}}(t)}{(1-t^2)(1-t^n)},$$

---

[1] In the form of lecture notes summarizing results from [11] and references therein.

where $G_{m,n,\mathbb{F}}(t)$ is a polynomial by Hilbert's syzygy theorem. We say that $G_{m,n,\mathbb{F}}(t)$ is the Hilbert polynomial associated to $H_{m,n,\mathbb{F}}(t)$. Observe that describing $G_{m,n,\mathbb{F}}(t)$ is related to describing the generators and relations of $Q_m(D_n, \mathbb{F})$ as a $\mathbb{F}[x_1, x_2]^{D_n}$-module. This leads us to consider the following two standard representation theory results in the study of quasi-invariants.

Lemma 2.6 ([13]). *The space $Q_m(D_n, \mathbb{F})$ is a representation of D_n.*

Notice that $Q_{m,d}(D_n, \mathbb{F})$ is a subrepresentation of $Q_m(D_n, \mathbb{F})$ and finite-dimensional. As we are working in non-modular representation theory, by Maschke's Theorem $Q_{m,d}(D_n, \mathbb{F})$ decomposes as a direct sum

$$Q_{m,d}(D_n, \mathbb{F}) = \bigoplus_{\tau \in \mathrm{Irrep}(D_n)} Q_{m,d}(D_n, \mathbb{F})_\tau,$$

where $\mathrm{Irrep}(D_n)$ is the set of irreducible representations of D_n and $Q_{m,d}(D_n, \mathbb{F})_\tau$ is the subspace of $Q_{m,d}(D_n, \mathbb{F})$ on which D_n acts by direct sums of copies of τ. Therefore, for $\tau \in \mathrm{Irrep}(D_n)$, we can define

$$Q_m(D_n, \mathbb{F})_\tau = \bigoplus_{d \geq 0} Q_{m,d}(D_n, \mathbb{F})_\tau$$

to be the isotypic components of $Q_{m,d}(D_n, \mathbb{F})$.

Proposition 2.7 ([13]). *The space $Q_m(D_n, \mathbb{F})_\tau$ has the following properties:*

(1) $Q_m(D_n, \mathbb{F})_\tau$ is a module over $\mathbb{F}[x_1, x_2]^{D_n}$.

(2) We have the decomposition

$$Q_m(D_n, \mathbb{F}) = \bigoplus_{\tau \in \mathrm{Irrep}(D_n)} Q_m(D_n, \mathbb{F})_\tau$$

as a $\mathbb{F}[x_1, x_2]^{D_n}$-module.

It follows from this proposition that to study the generators and relations of $Q_m(D_n, \mathbb{F})$, it suffices to study the generators and relations of $Q_m(D_n, \mathbb{F})_\tau$ as a $\mathbb{F}[x_1, x_2]^{D_n}$-module. We use this method in Sections 6 and 7 to work towards proving the conjectured expression for the Hilbert series of $Q_m(D_4, \mathbb{F}_{p^k})$.

3 Existing results

In this section, we consider existing work on $Q_m(D_n, \mathbb{C})$ which we extend to fields of characteristic p, as well as approaches used to compare and compute Hilbert series of $Q_m(S_n, \mathbb{F})$ in different characteristics.

First, we introduce key results about $Q_m(D_n, \mathbb{C})$ due to Feigin and Veselov [11].

Theorem 3.1 (Feigin and Veselov [11]). *The Hilbert series for* $Q_m(D_n, \mathbb{C})$ *is*

$$H_m(t) = \frac{1 + 2t^{mn+1} + \cdots + 2t^{mn+n-1} + t^{(2m+1)n}}{(1-t^2)(1-t^n)}.$$

In our paper, we use two intermediate results that Feigin and Veselov used in the proof of this theorem. First, they showed that all polynomials in $Q_m(D_n, \mathbb{C})$ with degree at most mn are in fact invariant. They then constructed certain polynomials with degrees $mn+1, \ldots, mn+n-1$, and $(2m+1)n$, and used the following condition in polar coordinates for quasi-invariance in D_n to show that they are generators.

Lemma 3.2 (Feigin and Veselov [11]). *Consider any polynomial* $q \in \mathbb{C}[x_1, x_2]$. *Let* $z = x_1 + ix_2$, $\bar{z} = x_1 - ix_2$, *and we write* $z = re^{i\phi}$. *Then we have* $\partial_{\alpha_j}^{2l-1} q|_{\Pi_{\alpha_j}} = 0$ *if and only if* $\partial_{\alpha_j}^{2l-1} q|_{\phi = \frac{\pi j}{n}} = 0$.

Intuitively, the space $Q_m(D_n, \mathbb{F}_{p^k})$ is different from $Q_m(D_n, \mathbb{C})$ for certain values of p as some terms in the partial derivatives are killed in characteristic p. Therefore, we are motivated to compare the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$ with the Hilbert series of $Q_m(D_n, \mathbb{C})$. To do so, we adapt the approaches used to study quasi-invariant polynomials of the symmetric group in characteristic p. In 2020, Ren and Xu [8] found that the Hilbert series of $Q_m(S_n, \mathbb{F}_p)$ is at least as great as the Hilbert series of $Q_m(S_n, \mathbb{C})$, and is strictly greater for finitely many values of p. This enabled them to prove the following result.

Theorem 3.3 (Ren and Xu [8]). *Let* $m \geq 0$ *and* $n \geq 3$ *be integers. Let* p *be a prime such that there exist integers* $a \geq 0$ *and* $k \geq 0$ *with*

$$\frac{mn(n-2) + \binom{n}{2}}{n(n-2)k + \binom{n}{2} - 1} \leq p^a \leq \frac{mn}{nk+1}.$$

Then the Hilbert series of $Q_m(S_n, \mathbb{F}_p)$ *is different from the Hilbert series of* $Q_m(S_n, \mathbb{C})$.

Ren and Xu conjectured that the above condition is also necessary. In 2023, by studying the generators and relations of $Q_m(S_n, \mathbb{F}_p)_\tau$, Wang [9] gave the general form of the Hilbert series of $Q_m(S_3, \mathbb{F}_p)$ for $p > 3$ as follows.

Theorem 3.4 (Wang [9]). *The Hilbert series of* $Q_m(S_3, \mathbb{F}_p)$ *for* $p > 3$ *is*

$$H_m(t) = \frac{1 + 2t^d + 2t^{6m+3-d} + t^{6m+3}}{(1-t)(1-t^2)(1-t^3)}.$$

We follow Ren and Xu's approach [8] to prove the equivalent of Theorem 3.3 for the dihedral group in Sections 4 and 5. We then use Wang's method [9] of studying the generators and relations of $Q_m(W, \mathbb{F})_\tau$ to compute the Hilbert series of $Q_m(D_4, \mathbb{F}_{p^k})$ in Section 7.

4 Comparing the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$ and $Q_m(D_n, \mathbb{C})$

In this section, we prove two results that help us to compare the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$ and $Q_m(D_n, \mathbb{C})$. First, we note that the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$ is at least as large as the Hilbert series of $Q_m(D_n, \mathbb{C})$.

Proposition 4.1. *For any fixed m, d, n, we have* $\dim Q_{m,d}(D_n, \mathbb{F}_{p^k}) \geq \dim Q_{m,d}(D_n, \mathbb{C})$.

Proof. For convenience, we use the complex coordinates $z = x_1 + ix_2$, $\overline{z} = x_1 - ix_2$. Let us consider the polynomial $F = a_0 z^d + a_1 z^{d-1}\overline{z} + \cdots + a_d \overline{z}^d$. In [11], Feigin and Veselov used Lemma 3.2 to show that F is in $Q_{m,d}(D_n, \mathbb{F})$ if and only if the system of linear equations

$$\sum_{j=0}^{d-(2s-1)} \binom{d-j}{2s-1} a_j = 0 \tag{1}$$

holds, where $1 \leq s \leq m$. Some coefficients in (1) evaluate to 0 in $\mathbb{F}_{p^k}$ for certain values of p, so the solution space of the equation over $\mathbb{F}_{p^k}$ is at least as large as the solution space over $\mathbb{C}$. ■

However, for each m and n, there are only finitely many primes for which the strict inequality holds.

Proposition 4.2. *For any fixed m and n, there are only finitely many primes p for which the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$ is greater than that of $Q_m(D_n, \mathbb{C})$.*

To prove this proposition, we use the following set-up. Let us denote the ring $\mathbb{Z}[\omega, i]$ as R. Let $P = R[x_1, x_2]$ and $Q = \bigoplus_{0 \leq l \leq n-1} P/(\alpha_l)^{2m+1}P$. Let h be the linear map from P to Q defined as

$$h(F) = \bigoplus_{0 \leq l \leq n-1} (1 - s_{\alpha_l})F.$$

Notice that $\ker(h)$, the kernel of h, coincides with $Q_m(D_n, \mathbb{F})$. Let $M = \operatorname{coker}(h)$ be the cokernel of h in Q. As P, Q and M are R-modules, we take tensor products over R. We show that the dimension of $Q_m(D_n, \mathbb{F}_{p^k})$ is greater than that of $Q_m(D_n, \mathbb{C})$ only when M has p-torsion. The following lemma then implies that there are only finitely many p such that M has p-torsion.

Lemma 4.3. *For a Noetherian integral domain A, a finitely generated A-algebra B, and a finitely generated B-module M, there exists a nonzero element r of A such that the localization M_r is a free A_r-module.*

Proof of Proposition 4.2. Let $h \otimes_R 1$ be the map from $P \otimes_R \mathbb{Q}[\omega, i]$ to $Q \otimes_R \mathbb{Q}[\omega, i]$, and we have that

$$\begin{aligned}\dim_{\mathbb{Q}[\omega,i]}(\ker(h \otimes_R 1)) = &\dim_{\mathbb{Q}[\omega,i]}(P \otimes_R \mathbb{Q}[\omega, i]) - \dim_{\mathbb{Q}[\omega,i]}(Q \otimes_R \mathbb{Q}[\omega, i]) \\ &+ \dim_{\mathbb{Q}[\omega,i]}(\operatorname{coker}(h \otimes_R 1)).\end{aligned}$$

To show that $\operatorname{coker}(h \otimes_R 1) \cong M \otimes_R \mathbb{Q}[\omega, i]$, consider the exact sequence $P \xrightarrow{h} Q \xrightarrow{\pi} M \to 0$, where π is the canonical surjection from Q to $Q/\operatorname{Im}(h)$. As $\mathbb{Q}[\omega, i]$ is a R-module, we obtain another exact sequence

$$P \otimes_R \mathbb{Q}[\omega, i] \xrightarrow{h \otimes_R 1} Q \otimes_R \mathbb{Q}[\omega, i] \xrightarrow{\pi \otimes_R 1} M \otimes_R \mathbb{Q}[\omega, i] \to 0,$$

so $\operatorname{Im}(h \otimes_R 1) = \ker(\pi \otimes_R 1)$. As $\pi \otimes_R 1$ is surjective, we have $Q \otimes_R \mathbb{Q}[\omega, i]/\ker(\pi \otimes_R 1) \cong M \otimes_R \mathbb{Q}[\omega, i]$ by the first isomorphism theorem. Thus, $\operatorname{coker}(h \otimes_R 1) = \mathbb{Q}[\omega, i]/\operatorname{Im}(h \otimes_R 1) \cong M \otimes_R \mathbb{Q}[\omega, i]$. By the same logic, we consider a map $h \otimes_R 1'$ from $P \otimes_R \mathbb{F}_{p^k}$ to $Q \otimes_R \mathbb{F}_{p^k}$ with $\operatorname{coker}(h \otimes 1') \cong M \otimes_R \mathbb{F}_{p^k}$.

We also see that M is graded, with $M = \bigoplus_d M_d$, where M_d consists of homogeneous polynomials of degree d. For each d, the module M_d is finitely generated over R. As R is a Dedekind domain, we have a decomposition $M_d \cong T \oplus I_1 \oplus \cdots \oplus I_r$, where T is the torsion submodule of M_d and $I_1, \ldots, I_r$ are fractional ideals of R. This decomposition gives us

$$M_d \otimes_R \mathbb{Q}[\omega, i] \cong T_d \otimes_R \mathbb{Q}[\omega, i] \oplus \bigoplus_{j=1}^{r} I_j \otimes_R \mathbb{Q}[\omega, i],$$

$$M_d \otimes_R \mathbb{F}_{p^k} \cong T_d \otimes_R \mathbb{F}_{p^k} \oplus \bigoplus_{j=1}^{r} I_j \otimes_R \mathbb{F}_{p^k}.$$

We first show that $M_d \otimes_R \mathbb{Q}[\omega, i] \cong \mathbb{Q}[\omega, i]^r$. As $\mathbb{Q}[\omega, i]$ is the field of fractions of R, we have $I_j \otimes_R \mathbb{Q}[\omega, i] \cong \mathbb{Q}[\omega, i]$. Now, consider some nonzero $m \in T_d$, which has q-torsion. We see that $m \otimes_R 1 = m \otimes_R \frac{q}{q} = mq \otimes_R \frac{1}{q} = 0$. Thus, $T_d \otimes_R \mathbb{Q}[\omega, i] = 0$.

Now, we look at $M_d \otimes_R \mathbb{F}_{p^k}$. We can find some $a \in R$ such that $aI_j \subseteq R$ and aI_j contains at least one non-multiple of p. From the exact sequence $I_j \xrightarrow{\cdot a} R \to R/aI_j \to 0$, we obtain another exact sequence

$$I_j \otimes_R \mathbb{F}_{p^k} \xrightarrow{a \otimes_R 1} \mathbb{F}_{p^k} \to (R/aI_j) \otimes_R \mathbb{F}_{p^k} \to 0.$$

Note that $(R/aI_j) \otimes_R \mathbb{F}_{p^k} \cong R \otimes_R (\mathbb{F}_{p^k}/aI_j)$ and $\mathbb{F}_{p^k}/aI_j = 0$. Thus, the map $a \otimes_R 1$ is surjective. From verification, the map is also injective. Therefore, we have $I_j \otimes_R \mathbb{F}_{p^k} \cong \mathbb{F}_{p^k}$, which gives us $M_d \otimes_R \mathbb{F}_{p^k} \cong \mathbb{F}_{p^k}^r \oplus T_d \otimes_R \mathbb{F}_{p^k}$.

We have a decomposition $M \cong T \oplus S$, where $T = \bigoplus_d T_d$ is the torsion submodule of M. The module $T \otimes_R \mathbb{F}_{p^k}$ is nonzero if and only if T has p-torsion. We now apply Lemma 4.3 to $A = \mathbb{Z}[\omega, i]$, $B = \mathbb{Z}[\omega, i][x_1, x_2]^{D_n}$, and $M = \operatorname{coker}(h)$. It follows that there is some $r \in A \backslash \{0\}$ such that M_r is free over $\mathbb{Z}[\omega, i][1/r]$. Thus, if M has p-torsion, then $p \mid r$. There are only finitely many such primes p. ■

5 Condition for Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$ to be greater than the Hilbert series of $Q_m(D_n, \mathbb{C})$

In this section, we find a sufficient condition on p for which the Hilbert series in characteristic p is greater for fixed m and n.

Theorem 5.1. *Let $m \geq 0$ and $n \geq 3$ be integers. Let p be a prime that does not divide $2n$ such that there exist integers $a \geq 0$ and $r \geq 0$ with*

$$\frac{mn+n}{nr+n-1} \leq p^a \leq \frac{mn}{nr+1}.$$

Then the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$ is different from the Hilbert series of $Q_m(D_n, \mathbb{C})$.

We show that if p satisfies the inequality, then we can construct a polynomial in $Q_m(D_n, \mathbb{F}_{p^k})$ that has a lower degree than every generator of $Q_m(D_n, \mathbb{C})$.

Proof. As seen in the proof of Theorem 3.1, all polynomials in $Q_m(D_n, \mathbb{C})$ with degree at most mn are invariant, and $Q_m(D_n, \mathbb{C})$ as a module over its subring of D_n-invariant polynomials has a generator of degree $mn+1$. We denote this generator by P_m. We consider the following non-invariant polynomial

$$F = P_r^{p^a} \prod_{0 \leq j \leq n-1} \left(\beta_1^j x_1 + \beta_2^j x_2\right)^{2b},$$

where $b = \max\left(\frac{2m+1-p^a(2r+1)}{2}, 0\right)$. Notice that

$$\begin{aligned} \deg F &= p^a(nr+1) + 2bn \\ &= p^a(nr+1) + n(2m+1-p^a(2r+1)) \\ &= n(2m+1) + p^a(1-n-nr) \\ &\leq n(2m+1) - (n+mn) = mn < \deg P_m. \end{aligned}$$

Now, we show that F is in $Q_m(D_n, \mathbb{F}_{p^k})$. From computation (see Appendix A), for any reflection s_{α_l} we have

$$s_{\alpha_l} \prod_{0 \leq j \leq n-1} \left(\beta_1^j x_1 + \beta_2^j x_2\right) = - \prod_{0 \leq j \leq n-1} \left(\beta_1^j x_1 + \beta_2^j x_2\right). \tag{2}$$

Thus,

$$s_{\alpha_l} \prod_{0 \leq j \leq n-1} \left(\beta_1^j x_1 + \beta_2^j x_2\right)^{2b} = \prod_{0 \leq j \leq n-1} \left(\beta_1^j x_1 + \beta_2^j x_2\right)^{2b}.$$

As $(u+v)^{p^a} = u^{p^a} + v^{p^a}$ in $\mathbb{F}_{p^k}$, this gives us

$$\begin{aligned}(1-s_{\alpha_l})\left(P_r^{p^a}\prod_{0\le j\le n-1}\left(\beta_1^j x_1+\beta_2^j x_2\right)^{2b}\right) &= (1-s_{\alpha_l})\left(P_r^{p^a}\right)\prod_{0\le j\le n-1}\left(\beta_1^j x_1+\beta_2^j x_2\right)^{2b}\\ &= (1-s_{\alpha_l})\left(P_r\right)^{p^a}\prod_{0\le j\le n-1}\left(\beta_1^j x_1+\beta_2^j x_2\right)^{2b}.\end{aligned}$$

Since α_l^{2r+1} divides $(1-s_{\alpha_l})\,P_r$, we have that $\alpha_l^{(2r+1)p^a+2b} = \alpha_l^{2m+1}$ divides $(1-s_{\alpha_l})\,F$. Thus, F is in $Q_m(D_n,\mathbb{F}_{p^k})$. As F has a lower degree than P_m, the module $Q_m(D_n,\mathbb{F}_{p^k})$ has a generator of a lower degree than the generators of $Q_m(D_n,\mathbb{C})$ and thus has a different Hilbert series. ■

We conjecture that the condition in Theorem 5.1 is also necessary for the Hilbert series of $Q_m(D_n,\mathbb{F}_{p^k})$ to be greater than the Hilbert series of $Q_m(D_n,\mathbb{C})$.

Conjecture 5.2. *Let $m \ge 0$ and $n \ge 3$ be integers. Suppose that p is a prime that does not divide $2n$ such that the Hilbert series of $Q_m(D_n,\mathbb{F}_{p^k})$ is different from the Hilbert series of $Q_m(D_n,\mathbb{C})$. Then there exist integers $a \ge 0$ and $r \ge 0$ with*

$$\frac{mn+n}{nr+n-1} \le p^a \le \frac{mn}{nr+1}.$$

This is supported by our calculations for small values of n. Table 1 summarizes our verification for $n=4$, $m \le 15$ and $3 \le p \le 50$, which was performed on Sagemath.

6 Generators of $Q_m(D_n,\mathbb{F})_\tau$ for one-dimensional representations τ

From our computer calculations for $n=4$, we also conjecture that the Hilbert series of $Q_m(D_4,\mathbb{F}_{p^k})$ takes the form as follows.

Conjecture 6.1. *The Hilbert series of $Q_m(D_4,\mathbb{F}_{p^k})$ is*

$$H_{m,4,\mathbb{F}_{p^k}}(t) = \frac{1+2t^d+2t^{2(2m+1)}+2t^{4(2m+1)-d}+t^{4(2m+1)}}{(1-t^2)(1-t^4)},$$

where d is the degree of the smallest non-D_4-invariant generator of $Q_m(D_4,\mathbb{F}_{p^k})$.

Recall the definition of $Q_m(D_n,\mathbb{F})_\tau$, where τ is an irreducible representation of D_n. In this section, we find the generators of $Q_m(D_n,\mathbb{F})_\tau$ for all 1-dimensional representations τ. In the case of D_4, these generators account for the terms 1, $2t^{2(2m+1)}$, and $t^{4(2m+1)}$ in the numerator $G_{m,4,\mathbb{F}_{p^k}}(t)$.

First, we show that the $\mathbb{F}[x_1,x_2]^{D_n}$-modules $Q_m(D_n,\mathbb{F})_{\rho_0}$ and $Q_m(D_n,\mathbb{F})_{\rho_{-1}}$ have generators of degree 0 and $n(2m+1)$ respectively.

Proposition 6.2. *As a $\mathbb{F}[x_1,x_2]^{D_n}$-module, we have*

$m\backslash p$	3	5	7	11	13	17	19	23	29	31	37	41	43	47
0														
1	(1,0)													
2		(1,0)	(1,0)											
3	(2,0)		(1,0)	(1,0)										
4	(2,0)		(1,0)	(1,0)	(1,0)									
5	(2,0)			(1,0)	(1,0)	(1,0)	(1,0)							
6				(1,0)	(1,0)	(1,0)	(1,0)	(1,0)						
7	(3,0)	(2,0)		(1,0)	(1,0)	(1,0)	(1,0)	(1,0)						
8	(3,0)	(2,0)			(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)				
9	(3,0)	(2,0)	(1,1)			(1,0)	(1,0)	(1,0)	(1,0)	(1,0)				
10	(3,0)	(2,0)	(1,1)			(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)			
11	(3,0)	(2,0)	(1,1)			(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	
12	(3,0)	(2,0)					(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)
13	(3,0)	(2,0)	(2,0)				(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)
14	(3,0)	(2,0)	(2,0)	(1,1)				(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)
15	(3,0)	(2,0)	(2,0)	(1,1)				(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)

Table 1: Values of (a, r) for given (m, p)

(1) $Q_m(D_n, \mathbb{F})_{\rho_0}$ *is freely generated by 1.*

(2) $Q_m(D_n, \mathbb{F})_{\rho_{-1}}$ *is freely generated by* $\prod_{0\leq j\leq n-1} \alpha_j^{2m+1}$.

Proof. To prove (1), note that the condition that D_n acts by ρ_0 on $f \in \mathbb{F}[x_1, x_2]$ is equivalent to the condition that f is D_n-invariant. Thus, $Q_m(D_n, \mathbb{F})_{\rho_0} \subset \mathbb{F}[x_1, x_2]^{D_n}$. Conversely, for any $f \in \mathbb{F}[x_1, x_2]^{D_n}$, we have $(1 - s_{\alpha_j})f = f - f = 0$ is divisible by α_j^{2m+1} for all j. Thus, $Q_m(D_n, \mathbb{F})_{\rho_0}$ is precisely $\mathbb{F}[x_1, x_2]^{D_n}$.

To prove (2), we see that if $f \in Q_m(D_n, \mathbb{F})_{\rho_{-1}}$, then $s_{\alpha_j} f = -f$ for all j, so $(1 - s_{\alpha_j})f = 2f$ is divisible by α_j^{2m+1}. Thus, f is divisible by $\prod_{0\leq j\leq n-1} \alpha_j^{2m+1}$, and we write $f = f' \prod_{0\leq j\leq n-1} \alpha_j^{2m+1}$, where $f' \in \mathbb{F}[x_1, x_2]$. From Equation 2 in the proof of Theorem 5.1, we have

$$s_{\alpha_l} \prod_{0\leq j\leq n-1} \alpha_j^{2m+1} = - \prod_{0\leq j\leq n-1} \alpha_j^{2m+1}$$

for all reflections s_{α_l}. Hence, as

$$s_{\alpha_l} f = (s_{\alpha_l} f') \left(s_{\alpha_l} \prod_{0\leq j\leq n-1} \alpha_j^{2m+1} \right) = -f,$$

we have $s_{\alpha_l} f' = f'$. Therefore, f' is D_n-invariant, so f is in the $\mathbb{F}[x_1, x_2]^{D_n}$-module generated by $\prod_{0\leq j\leq n-1} \alpha_j^{2m+1}$.

Conversely, for any $f' \in \mathbb{F}[x_1, x_2]^{D_n}$, consider $f = f' \prod_{0 \le j \le n-1} \alpha_j^{2m+1}$. For all s_{α_l}, we have

$$(1 - s_{\alpha_l}) \left(f' \prod_{0 \le j \le n-1} \alpha_j^{2m+1} \right) = 2f' \prod_{0 \le j \le n-1} \alpha_j^{2m+1},$$

which is divisible by α_l^{2m+1}. Thus, the $\mathbb{F}[x_1, x_2]^{D_n}$-module generated by $\prod_{0 \le j \le n-1} \alpha_j^{2m+1}$ is contained in $Q_m(D_n, \mathbb{F})_{\rho_{-1}}$. Hence, $Q_m(D_n, \mathbb{F})_{\rho_{-1}}$ is exactly this module. Freeness follows from the fact that $\mathbb{F}[x_1, x_2]$ is an integral domain. ■

For even n, we also have the one-dimensional representations $\rho_{\pm 1}$ and $\rho_{\mp 1}$. We show that $Q_m(D_n, \mathbb{F})_{\rho_{\pm 1}}$ and $Q_m(D_n, \mathbb{F})_{\rho_{\mp 1}}$ both have generators of degree $\frac{n(2m+1)}{2}$.

Proposition 6.3. *As a $\mathbb{F}[x_1, x_2]^{D_n}$-module, we have*

(1) $Q_m(D_n, \mathbb{F})_{\rho_{\pm 1}}$ is freely generated by $\prod_{\text{odd } j} \alpha_j^{2m+1}$.

(2) $Q_m(D_n, \mathbb{F})_{\rho_{\mp 1}}$ is freely generated by $\prod_{\text{even } j} \alpha_j^{2m+1}$.

We provide the proof of statement (1), as the proof of (2) follows the same logic.

Proof. If $f \in Q_m(D_n, \mathbb{F})_{\rho_{\pm 1}}$, then $s_{\alpha_{2l}} f = f$, so $(1 - s_{\alpha_{2l}}) f = 0$. We also have $s_{\alpha_{2l+1}} f = -f$, so $\left(1 - s_{\alpha_{2l+1}}\right) f = 2f$ is divisible by α_{2l+1}^{2m+1}. Thus, $f = f' \prod_{\text{odd } j} \alpha_j^{2m+1}$ for some $f' \in \mathbb{F}[x_1, x_2]$. From computation (see Appendix B), we have

$$s_{\alpha_{2l+1}} \prod_{\text{odd } j} \alpha_j^{2m+1} = - \prod_{\text{odd } j} \alpha_j^{2m+1}.$$

Thus,

$$s_{\alpha_{2l+1}} f = (s_{\alpha_{2l+1}} f') \left(s_{\alpha_{2l+1}} \prod_{\text{odd } j} \alpha_j^{2m+1} \right) = -f,$$

giving us $s_{\alpha_{2l+1}} f' = f'$. Hence, $f' \in \mathbb{F}[x_1, x_2]^{D_n}$, so f is the $\mathbb{F}[x_1, x_2]^{D_n}$-module generated by $\prod_{\text{odd } j} \alpha_j^{2m+1}$.

Conversely, for any $f' \in \mathbb{F}[x_1, x_2]^{D_n}$, consider $f = f' \prod_{\text{odd } j} \alpha_j^{2m+1}$. For all $s_{\alpha_{2l+1}}$, we have

$$(1 - s_{\alpha_{2l+1}}) \left(f' \prod_{\text{odd } j} \alpha_j^{2m+1} \right) = 2f' \prod_{\text{odd } j} \alpha_j^{2m+1},$$

which is divisible by $\prod_{\text{odd } j} \alpha_j^{2m+1}$. For all $s_{\alpha_{2l}}$, from computation we also have

$$s_{\alpha_{2l}} \prod_{\text{odd } j} \alpha_j^{2m+1} = \prod_{\text{odd } j} \alpha_j^{2m+1},$$

which gives us $(1-s_{\alpha_{2l}})f = 0$. Thus, the $\mathbb{F}[x_1, x_2]^{D_n}$-module generated by $\prod_{\text{odd } j} \alpha_j^{2m+1}$ is contained in $Q_m(D_n, \mathbb{F})_{\rho_{\pm 1}}$. Hence, $Q_m(D_n, \mathbb{F})_{\rho_{\pm 1}}$ is exactly this module. ■

In the case of D_4, Propositions 6.2 and 6.3 tell us that the generators of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_0}$, $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_{-1}}$, $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_{\pm 1}}$, and $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_{\mp 1}}$ respectively account for the terms 1, $t^{4(2m+1)}$, $t^{2(2m+1)}$ and $t^{2(2m+1)}$ to $G_{m,4,\mathbb{F}_{p^k}}(t)$. Thus, to prove Conjecture 6.1, it remains for us to show that the generators of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ account for the terms $2t^d$ and $2t^{4(2m+1)-d}$..

7 The generators of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$

In this section, we study the generators of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$. To begin, let V be a copy of the standard representation ρ_1. Then V contains a one-dimensional -1 eigenspace of s_{α_l}, which we denote by $V^-_{s_{\alpha_l}}$. In D_4, we have the reflections s_1, s_2, s_3, s_4 about x_2, $x_1 - x_2$, x_1, and $x_1 + x_2$, respectively. We have the following result on polynomials in $V^-_{s_1}$.

Lemma 7.1. *Let $V \subset Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ be a copy of the standard representation, and let $f \in V^-_{s_1}$. Then we have $f + rf + r^2 f + r^3 f = 0$ and $f + r^2 f = 0$, where $r = s_1 s_2 \in D_4$, and $f = x_2^{2m+1} f'$ for some polynomial f' that is invariant under s_1 and satisfies Equation* (3).

Conversely, let f' be an s_1-invariant polynomial which satisfies Equation (3) *such that $f = x_2^{2m+1} f'$ satisfies $f + rf + r^2 f + r^3 f = 0$ and $f + r^2 f = 0$. Then $x_2^{2m+1} f'$ belongs to the -1 eigenspace of s_1 in some copy of ρ_1 inside $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$.*

Remark. This lemma is almost exactly analogous to Lemma 3.2 in [9], where Wang studied polynomials in a -1 eigenspace of $Q_m(S_3, \mathbb{F}_p)_{\text{std}}$, where std is the standard representation of S_3. However, just imposing the analogous conditions on f', which are $f = x_2^{2m+1} f'$ satisfies $f + rf + r^2 f + r^3 f = 0$ and $f + r^2 f = 0$, in the converse direction as Lemma 3.2 in [9] is not enough. For example, letting $f' = x_1^2 x_2^2$ satisfies these two conditions, but $x_1^2 x_2^5$ is not 1-quasi-invariant. We found an additional necessary condition, namely, f' must satisfy Equation (3).

Proof. Since $f \in V^-_{s_1}$, we have $(1 - s_1)f = 2f$ is divisible by x_2^{2m+1}, so $f = x_2^{2m+1} f'$ for some polynomial f'. Both f and x_2^{2m+1} are anti-invariant under s_1, so f' must be s_1-invariant. As f is an element of ρ_1, we have $f + rf + r^2 f + r^3 f = 0$ and $f + r^2 f = 0$. Note that $r = s_1 s_2 = s_4 s_1$, $r^2 = s_3 s_1$, and $r^3 = s_2 s_1$, and $s_1 f = -x_2^{2m+1} f'$. Thus, we have

$$x_2^{2m+1} f' + s_4(-x_2^{2m+1} f') + s_3(-x_2^{2m+1} f') + s_2(-x_2^{2m+1} f') = 0,$$

which gives us

$$x_2^{2m+1} f' + x_1^{2m+1} s_4 f' - x_2^{2m+1} s_3 f' - x_1^{2m+1} s_2 f' = 0.$$

From $f + r^2 f = 0$, we also have

$$x_2^{2m+1} f' + s_3(-x_2^{2m+1} f') = x_2^{2m+1} f' - x_2^{2m+1} s_3 f' = 0,$$

so $f' = s_3 f'$ and $s_2 f' = s_4 f'$. This implies that f' is even in x_1 and x_2, so we write

$$f' = \sum_a c_a x_1^{2a} x_2^{d-2a},$$

where d is even. As f is m-quasi-invariant, we have $(1 - s_2)f$ is divisible by $(x_1 - x_2)^{2m+1}$, that is,

$$\left. \frac{\partial^{(k)}}{\partial x_1^i \partial x_2^{k-i}} (1 - s_2) f \right|_{x_1 = x_2} = 0 \tag{3}$$

for all $k \leq 2m$. From computation (see Appendix C), this gives us a system of $m+1$ linear equations in the coefficients of f in the form

$$\sum_a c_a \left(\binom{2a + 2m + 1}{i} \binom{d - 2a}{k - i} - \binom{d - 2a}{i} \binom{2a + 2m + 1}{k - i} \right) = 0,$$

where i ranges from 0 to m.

For the converse direction, we first show that f is m-quasi-invariant. We see that $f' = s_3 f'$, so $(1 - s_3)f = 0$. We also have $(1 - s_1)f = 2x_2^{2m+1} f'$. As f' satisfies Equation (3), we have $(1 - s_2)f$ is divisible by $(x_1 - x_2)^{2m+1}$. From computation, we see that

$$\left. \frac{\partial^{(k)}}{\partial x_1^i \partial x_2^{k-i}} (1 - s_4) f \right|_{x_1 = -x_2} = (-1)^{k-i} \left. \frac{\partial^{(k)}}{\partial x_1^i \partial x_2^{k-i}} (1 - s_2) f \right|_{x_1 = x_2},$$

so $(1 - s_4)f$ is divisible by $(x_1 + x_2)^{2m+1}$.

Observe that the span of the D_4 orbit of f is the space spanned by $x_2^{2m+1} f'$ and $x_1^{2m+1} s_2 f'$, so it is 2-dimensional. The only 2-dimensional irreducible representation of D_4 is ρ_1, so $x_2^{2m+1} f'$ belongs to some copy of ρ_1 in $Q_m(D_4, \mathbb{F})_{\rho_1}$. We have $s_1(x_2^{2m+1} f') = -x_2^{2m+1} f'$, so $x_2^{2m+1} f'$ belongs to the -1 eigenspace of s_1. ■

We note that $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ is a graded $\mathbb{F}_{p^k}[x_1, x_2]^{D_4}$-module, so we can assume its generators are homogeneous. From now, instead of considering the generating elements of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$, we consider its *generating representations*. A generating representation is a copy of ρ_1 inside $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ that is involved in a generators and relations presentation of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ as a $\mathbb{F}_{p^k}[x_1, x_2]^{D_4}$-module with a minimal number of generators. We are now ready to consider a useful corollary of Lemma 7.1.

Corollary 7.2. *Let V be a generating representation of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ and let $f \in V^-_{s_{\alpha_l}}$. We write $f = \alpha_l^{2m+1} f'$. Then f' is not divisible by any nonconstant D_4-invariant polynomial.*

Proof. As f lies in $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$, it satisfies $f + rf + r^2 f + r^3 f = 0$ and $f + r^2 f = 0$, and f' satisfies Equation (3) by Lemma 7.1. We assume for contradiction that f' is divisible by some nonconstant D_4-invariant polynomial g. Then $f/g + r(f/g) + r^2(f/g) + r^3(f/g) = 0$, and $f/g + r^2(f/g) = 0$. One can verify that f/g also satisfies Equation (3), so f/g is contained in $Q_m(D_4, \mathbb{F}_{p^k})$ by Lemma 7.1. However, f is in the $\mathbb{F}_{p^k}[x_1, x_2]^{D_4}$-module generated by f/g. As f is generated by an element of a lower degree, it is not in the generating representation, giving us a contradiction. ■

A generating representation V of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ consists of homogeneous polynomials of degree d, so we say that V has degree d. Recall that to prove Conjecture 6.1, it suffices to show that the remaining terms in $G_{m,4,\mathbb{F}_{p^k}}(t)$ are exactly $2t^d$ and $2t^{4(2m+1)-d}$. Here, we show that the sum of the degrees of two generating representations of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ is indeed bounded below by $8m + 4$.

Lemma 7.3. *Let V, W be distinct generating representations of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$. Let $v \in V^-_{s_1}$, $w \in W^-_{s_1}$. Then $vs_2w - ws_2v$ is a nonzero element of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_{-1}}$, and* $\deg V + \deg W \geq 8m+4$.

To prove this lemma, we work in the algebraic closure $\overline{\mathbb{F}_p}$ instead of $\mathbb{F}_{p^k}$. This is so that we can use Hilbert's Nullstellensatz. We note that the space $Q_m(D_4, \overline{\mathbb{F}_p})$ is $Q_m(D_4, \mathbb{F}_{p^k}) \otimes \overline{\mathbb{F}_p}$. Recall from Proposition 4.1 that $Q_{m,d}(D_4, \mathbb{F}_{p^k})$ consists of polynomials whose coefficients satisfy the system of linear equations (1). The dimension of the solution space of the system of equations remains unchanged under tensor product with $\overline{\mathbb{F}_p}$, so the Hilbert series of $Q_m(D_4, \overline{\mathbb{F}_p})$ is the same as that of $Q_m(D_4, \mathbb{F}_{p^k})$. This implies that $Q_m(D_4, \overline{\mathbb{F}_p})$ has the same generators and relations as $Q_m(D_4, \mathbb{F}_{p^k})$, so our previous results in this section and Section 6 also hold in $Q_m(D_4, \overline{\mathbb{F}_p})$.

Proof. The polynomial $vs_3w - ws_3v$ lies in $Q_m(D_4, \overline{\mathbb{F}_p})$ since $Q_m(D_n, \overline{\mathbb{F}_p})$ is a ring. It also spans a quotient of a copy of $\wedge^2\rho_1$ inside $V \otimes W$. We see that

$$\begin{aligned}
\wedge^2\rho_1(s_1)(x_1 \wedge x_2) &= \rho_1(s_1)(x_1 \otimes x_2 - x_2 \otimes x_1) = x_1 \otimes (-x_2) - (-x_2) \otimes x_1 \\
&= -(x_1 \otimes x_2 - x_2 \otimes x_1), \\
\wedge^2\rho_2(s_2)(x_1 \wedge x_2) &= \rho_1(s_2)(x_1 \otimes x_2 - x_2 \otimes x_1) = x_2 \otimes x_1 - x_1 \otimes x_2 = -(x_1 \otimes x_2 - x_2 \otimes x_1),
\end{aligned}$$

so $\wedge^2\rho_1$ is the representation ρ_{-1}. It remains for us to show that $vs_2w - ws_2v$ is nonzero. By Lemma 7.1, we can write $v = x_2^{2m+1}v'$ and $w = x_2^{2m+1}w'$, where v' and w' are invariant under s_1 and s_3, and $s_2v' = s_4v'$, $s_2w' = s_4w'$. We see that

$$vs_2w - ws_2v = x_2^{2m+1}v'x_1^{2m+1}s_2w' - x_2^{2m+1}w'x_1^{2m+1}s_2v' = x_1^{2m+1}x_2^{2m+1}(v's_2w' - w's_2v').$$

Assume for the sake of contradiction that $vs_2w - ws_2v = 0$. Then $v's_2w' = w's_2v'$, so $v's_2w'$ is

s_2-invariant. We now show that this either implies $v' = w'$ up to a scalar, which contradicts V and W being distinct, or $v's_2w'$ is s_2-anti-invariant, which contradicts v' and w' being nonzero.

We decompose v' into its irreducible factors, and let f be any such factor. We show that f must also be a factor of w'. Let r, s be elements of $\overline{\mathbb{F}_p}$ such that $f(r, s) = 0$. Then $v'(r, s) = 0$, and $s_1f(r, -s) = s_3f(-r, s) = 0$. By Lemma 7.1, v' must be even in x_1 and x_2, so $v'(r, -s) = v'(-r, s) = 0$. As f is irreducible, by Hilbert's Nullstellensatz, v' must be divisible by s_1f and s_3f. We also see that $v's_2w'$ is s_2-invariant, so it is divisible by s_2f. If s_2w' is divisible by s_2f, then w' is divisible by f and we are done. Thus, v' must be divisible by s_2f. As $s_2f(s, r) = 0$, we have $v'(s, r) = 0$. This also gives us $v'(-s, -r) = 0$, so v' is divisible by s_4f. It follows similarly that v' must be divisible by rf, r^2f, and r^3f.

Therefore, v' is divisible by the least common multiple of all of the s_lf and r^lf, which we denote by g. The action of D_4 fixes g as a factor of v', so D_4 must act on g by scalars. It cannot act on g trivially, as then g would be a D_4-invariant polynomial that divides v', which contradicts Corollary 7.2. Therefore, D_4 must act on g by either ρ_{-1}, $\rho_{\pm 1}$, or $\rho_{\mp 1}$, and sends g to $-g$. Observe that v' can only have one such factor on which D_4 acts on by any of these representations, as otherwise the product of two such factors is a D_4-invariant polynomial factor of v'. Hence, every irreducible factor of v' is also a factor of w', except for possibly a factor in one of the representations ρ_{-1}, $\rho_{\pm 1}$, or $\rho_{\mp 1}$. It then follows from applying all the above argument to w' that there is a bijection between all irreducible factors of v' and w', except for possibly a factor in each of ρ_{-1}, $\rho_{\pm 1}$, or $\rho_{\mp 1}$. Note that $\rho_{-1} \otimes \rho_{\pm 1} = \rho_{\mp 1}$, $\rho_{-1} \otimes \rho_{\mp 1} = \rho_{\pm 1}$, and $\rho_{\mp 1} \otimes \rho_{\pm 1} = \rho_{-1}$, so we can assume that v' and w' each have an additional factor in at most one of ρ_{-1}, $\rho_{\pm 1}$, and $\rho_{\mp 1}$.

We therefore have three cases to consider: either v' and w' both do not have a factor in any of the representations, or they both have an additional factor in the same representation, or only one has an additional factor in a representation. In the first case, there is a bijection between all irreducible factors of v' and w', so they are equal up to a scalar. In the second case, suppose the two additional factors lie in the representation ρ'. Then by Proposition 2.3, these factors lie in $Q_0(D_4, \overline{\mathbb{F}_p})_{\rho'}$. By Propositions 6.2 and 6.3, each factor is a multiple of the generator of $Q_0(D_4, \overline{\mathbb{F}_p})_{\rho'}$ by a D_4-invariant polynomial. It follows from Corollary 7.2 that this D_4-invariant must be a constant. Thus, v' and w' are equal up to a scalar. Both cases give us the desired contradiction, so $vs_2w - ws_2v$ must be nonzero.

In the third case, we show that $v's_2w'$ must be s_2-anti-invariant. We have two subcases: either v' and w' have additional factors in two distinct representations, or exactly one of them does not have an additional factor in any of the representations. For the former, as v' and w' are both s_1-invariant, the two representations must be ρ_{-1} and $\rho_{\mp 1}$. Suppose that v' has the factor P in ρ_{-1}, and w' has the factor Q in $\rho_{\mp 1}$. Then we write $v' = PF$ and $w' = QF$, where F is some polynomial. We have $v's_2w' = PF(s_2Q)(s_2F)$ and $w's_2v' = QF(s_2P)(s_2F)$. Notice that $s_2Q = Q$ and $s_2P = -P$, so $w's_2v' = -v's_2w'$. For the latter subcase, as v' and w' are both s_1-invariant, one of them must have an additional factor in $\rho_{\pm 1}$. Suppose that w' has an additional factor Q in $\rho_{\pm 1}$. Then we write $w' = Qv'$, and $v's_2w' = v'(s_2Q)(s_2v')$, and $w's_2v' = Qv'(s_2v')$. We have $s_2Q = -Q$, so $w's_2v' = -v's_2w'$. We have the desired contradiction, so $vs_2w - ws_2v$ must also be nonzero in this case. ■

Lemma 7.4. *Suppose that there exist generating representations V and W of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ such that* $\deg V + \deg W = 8m + 4$. *Then $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ is a free module over $\mathbb{F}_{p^k}[x_1, x_2]^{D_4}$ generated by V and W.*

Proof. We assume for contradiction that there exists another generating representation U of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$. Then by Lemma 7.3, we have $\deg U \geq \deg W$. Let $v \in V_{s_1}^-$, $w \in W_{s_1}^-$, $u \in U_{s_1}^-$. By Lemma 7.3, we have

$$vs_2w - ws_2v = c \prod_{1 \leq j \leq 4} \alpha_j^{2m+1}$$

as $vs_2w - ws_2v$ has degree $8m + 4$ and lies in $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_{-1}}$. We also have

$$vs_2u - us_2v = f \prod_{1 \leq j \leq 4} \alpha_j^{2m+1},$$

where f is some D_4-invariant polynomial. Notice that the representation generated by $cu - fw$ is also a generating representation of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$. However, we also have

$$\begin{aligned} vs_2(cu - fw) - (cu - fw)s_2v &= c(vs_2u - us_2v) - f(vs_2w - ws_2v) \\ &= (cf - fc) \prod_{1 \leq j \leq 4} \alpha_j^{2m+1} \\ &= 0, \end{aligned}$$

which contradicts Lemma 7.3. Therefore, the only generating representations of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ are V and W.

Now, we show that $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$ is a free module. If it were not free, then there would be nonzero D_4-invariant polynomials f, g such that $fv = gw$. However, we would have

$$fg(vs_2w - ws_2v) = fvs_2(gw) - gws_2(fv) = fvs_2(fv) - fvs_2(fv) = 0,$$

which is impossible as f, g, and $vs_2w - ws_2v$ are all nonzero. ■

8 Conclusion

In this paper, we extend the study of quasi-invariant polynomials of D_n to fields of characteristic p. In particular, we find a sufficient condition on p such that the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$ and

$Q_m(D_n, \mathbb{C})$ are different. We conjecture that this is also a necessary condition in Conjecture 5.2. To gain insight into the general form of the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$, we study the generators of $Q_m(D_n, \mathbb{F}_{p^k})_\tau$. We specifically examine the case $n = 4$ and prove results relevant to our conjectured form for the Hilbert series of $Q_m(D_4, \mathbb{F}_{p^k})$ in Conjecture 6.1.

While our work draws from previous approaches used to study quasi-invariant polynomials of the symmetric group in characteristic p, we hereby note several important differences. As the reflection representation of D_n is only defined over fields in which a primitive $2n^{\text{th}}$ root of unity is defined, we work in $\mathbb{F}_{p^k}$ instead of $\mathbb{F}_p$. We also impose an additional condition in Lemma 7.1.

For future work, we plan to prove the conjectured expression for the Hilbert series of $Q_m(D_4, \mathbb{F}_{p^k})$, building on our results in Sections 6 and 7. Specifically, following Lemma 7.4, we hope to then prove that there are exactly two generating representations of $Q_m(D_4, \mathbb{F}_{p^k})_{\rho_1}$. We would also like to investigate the Hilbert series of $Q_m(D_n, \mathbb{F}_{p^k})$. Our current strategies in Section 7 are insufficient for the general case. In doing so, we get closer to proving Conjecture 5.2.

9 Acknowledgements

I would like to extend my deepest gratitude to my mentor, Frank Wang, for his invaluable guidance and help throughout the project. I kindly thank Professor Pavel Etingof for suggesting the topic of this project. I would also like to thank Dr. Tanya Khovanova for her feedback on earlier renditions of this paper, and Professor Roman Bezrukavnikov and Dr. Jonathan Bloom for their insightful suggestions. Thank you to my tutor at the Research Science Institute, AnaMaria Perez, for her detailed advice on communicating and presenting my research, as well as her endless encouragement. Thank you also to Merrick Cai, Yale Fan, Victor Kolev and Austin Luo for their feedback on the penultimate draft of this paper. Last but certainly not least, I am thankful to the Massachusetts Institute of Technology (MIT), the Center for Excellence in Education (CEE), the Research Science Institute (RSI), and my sponsors, for making this once-in-a-lifetime research opportunity possible.

References

[1] C. Chevalley. Invariants of finite groups generated by reflections. *American Journal of Mathematics*, 77(4):778–782, 1955.

[2] O. Chalykh and A. Veselov. Commutative rings of partial differential operators and Lie algebras. *Communications in Mathematical Physics*, 126(3):597–611, 1990.

[3] F. Calogero. Solution of the one-dimensional N body problems with quadratic and/or inversely quadratic pair potentials. *Journal of Mathematical Physics*, 12:419–436, 1971.

[4] J. Moser. Three integrable Hamiltonian systems connected with isospectral deformations. *Advances in Mathematics*, 16(2):197–220, 1975.

[5] Y. Berest, P. Etingof, and V. Ginzburg. Cherednik algebras and differential operators on quasi-invariants. *Duke Mathematical Journal*, 118(2):279–337, 2003.

[6] A. Braverman, P. Etingof, and M. Finkelberg. Cyclotomic Double Affine Hecke Algebras. *Annales Scientifiques de l'École Normale Supérieure*, 53(5):1249–1312, 2020. With an appendix by Hiraku Nakajima and Daisuke Yamakawa.

[7] G. Felder and A. P. Veselov. Action of Coxeter Groups on m-Harmonic Polynomials and Knizhnik-Zamolodchikov Equations. *Moscow Mathematical Journal*, 3(4):1269–1291, 2003.

[8] M. Ren and X. Xu. Quasi-Invariants in Characteristic p and Twisted Quasi-Invariants. *Symmetry, Integrability and Geometry: Methods and Applications*, 21:107, 2020.

[9] F. Wang. Toward explicit Hilbert series of quasi-invariant polynomials in characteristic p and q-deformed quasi-invariants. *New York Journal of Mathematics*, 29:613–634, 2023.

[10] F. Wang and E. Yee. Hilbert Series of S_3-Quasi-Invariant Polynomials in Characteristics 2, 3. *Symmetry, Integrability and Geometry: Methods and Applications*, 21:057, 2025.

[11] M. Feigin and A. P. Veselov. Quasiinvariants of Coxeter groups and m-harmonic polynomials. *International Mathematics Research Notices*, 2003(10):521–545, 2003.

[12] A. Braverman, T. Chmutova, P. Etingof, and X. Yang. Introduction to Algebraic D-Modules. `https://math.mit.edu/~etingof/dmodules.pdf`, 2016. Lecture notes, available online.

[13] P. Etingof and E. Strickland. Lectures on quasi-invariants of Coxeter groups and the Cherednik algebra. *L'Enseignement Mathématique*, 49(2):035–065, 2003.

[14] J. E. Humphreys. *Reflection Groups and Coxeter Groups*, volume 29 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1990.

A Computations for Theorem 5.1

$$\begin{aligned} s_{\alpha_l} \prod_{0\le j\le n-1} \left(\beta_1^j x_1 + \beta_2^j x_2\right) &= \prod_{0\le j\le n-1} \left[\beta_1^j \left(\beta_2^{2l} x_1 - \beta_1^{2l} x_2\right) + \beta_2^j \left(\beta_1^{2l} x_1 - \beta_2^{2l} x_2\right)\right] \\ &= \prod_{0\le j\le n-1} \left[\left(\beta_1^j \beta_2^{2l} - \beta_2^j \beta_1^{2l}\right) x_1 - \left(\beta_1^j \beta_1^{2l} + \beta_2^j \beta_2^{2l}\right) x_2\right] \\ &= (-1)^n \prod_{0\le j\le n-1} \left(\beta_1^{2l-j} x_1 + \beta_2^{2l-j} x_2\right). \end{aligned}$$

Noting that $\beta_1^{\lambda+n} = -\beta_1^{\lambda}$ and $\beta_2^{\lambda+n} = -\beta_2^{\lambda}$, we rewrite the indices:

$$\begin{aligned} s_{\alpha_l} \prod_{0\le j\le n-1} \left(\beta_1^j x_1 + \beta_2^j x_2\right) &= (-1)^{2n} \prod_{0\le j\le n-1} \left(\beta_1^{2l-j+n} x_1 + \beta_2^{2l-j+n} x_2\right) \\ &= \prod_{2l+1\le j'\le 2l+n} \left(\beta_1^{j'} x_1 + \beta_2^{j'} x_2\right). \end{aligned}$$

If $2l+1 \le n-1$, then we have

$$\begin{aligned} \prod_{2l+1\le j'\le 2l+n} \left(\beta_1^{j'} x_1 + \beta_2^{j'} x_2\right) &= \prod_{2l+1\le j'\le n-1} \left(\beta_1^{j'} x_1 + \beta_2^{j'} x_2\right) \cdot \prod_{n\le j'\le 2l+n} \left(\beta_1^{j'} x_1 + \beta_2^{j'} x_2\right) \\ &= \prod_{2l+1\le j'\le n-1} \left(\beta_1^{j'} x_1 + \beta_2^{j'} x_2\right) \cdot (-1)^{2l+1} \prod_{0\le j'\le 2l} \left(\beta_1^{j'} x_1 + \beta_2^{j'} x_2\right) \\ &= - \prod_{0\le j'\le n-1} \left(\beta_1^{j'} x_1 + \beta_2^{j'} x_2\right). \end{aligned}$$

If $2l+1 \ge n$, we work with $2n - j'$ instead and obtain the same expression.

B Computations for Proposition 6.3

We consider $s_{\alpha_r} \prod_{\text{odd } j} \alpha_j$. Due to the page limit, we show the computation for r such that $2r+1 \le n-1$. Let $J_1 = \{2r+1, \dots, n-1\}$ and $J_2 = \{n+1, \dots, 2r+n-1\}$. Then

$$\begin{aligned} s_{\alpha_r} \prod_{j=1,3,\dots,n-1} \alpha_j &= \prod_{j'\in J_1\cup J_2} \alpha_{j'} \\ &= \prod_{j'\in J_1} \alpha_{j'} \cdot \prod_{j'\in J_2} \alpha_{j'} \\ &= \prod_{j'\in J_1} \alpha_{j'} \cdot (-1)^{r+2} \prod_{j'=1,3\dots,n-1} \alpha_{j'} \\ &= (-1)^r \prod_{j=1,3,\dots,n-1} \alpha_j. \end{aligned}$$

C Computations for Lemma 7.1 and Corollary 7.2

Substituting our expression for f' into Equation (3), we get

$$\frac{\partial^{(k)}}{\partial x_1^i \partial x_2^{k-i}} \sum_a c_a \left(x_1^{2a+2m+1}x_2^{d-2a} - x_1^{d-2a}x_2^{2a+2m+1}\right)\Bigg|_{x_1=x_2} = 0.$$

This gives us

$$\begin{aligned}
&\sum_a c_a \left(\binom{2a+2m+1}{i}\binom{d-2a}{k-i} x_1^{2a+2m+1-i} x_1^{d-2a-(k-i)} - \binom{d-2a}{i}\binom{2a+2m+1}{k-i} x_1^{d-2a-i} x_1^{2a+2m+1-(k-i)}\right)\\
=&\sum_a c_a \left(\binom{2a+2m+1}{i}\binom{d-2a}{k-i} - \binom{d-2a}{i}\binom{2a+2m+1}{k-i}\right) x_1^{d+2m+1-k}\\
=&0.
\end{aligned}$$

We now consider $(1-s_4)f$.

$$\begin{aligned}
&\frac{\partial^{(k)}}{\partial x_1^i \partial x_2^{k-i}} (1-s_4)f\Bigg|_{x_1=-x_2}\\
=&\frac{\partial^{(k)}}{\partial x_1^i \partial x_2^{k-i}} \sum_a c_a \left(x_1^{2a+2m+1}x_2^{d-2a} + x_1^{d-2a}x_2^{2a+2m+1}\right)\Bigg|_{x_1=-x_2}\\
=&\sum_a c_a \left(\binom{2a+2m+1}{i}\binom{d-2a}{k-i}(-1)^{d-2a-(k-i)} + \binom{d-2a}{i}\binom{2a+2m+1}{k-i}(-1)^{2a+2m+1-(k-i)}\right) x_1^{d+2m+1-k}\\
=&\sum_a c_a \left(\binom{2a+2m+1}{i}\binom{d-2a}{k-i} - \binom{d-2a}{i}\binom{2a+2m+1}{k-i}\right) x_1^{d+2m+1-k}(-1)^{k-i}\\
=&(-1)^{k-i}\ \frac{\partial^{(k)}}{\partial x_1^i \partial x_2^{k-i}} (1-s_2)f\Bigg|_{x_1=x_2}\\
=&0.
\end{aligned}$$

Let P denote $(1-s_2)f$. Then $(1-s_2)(f/g) = P/g$, and we see that

$$\frac{\partial^{(k)}(P/g)}{\partial x_1^i \partial x_2^{k-i}} = \sum_{a=0}^{i}\sum_{b=0}^{k-i} \binom{i}{a}\binom{k-i}{b}(-1)^{a+b}\cdot \frac{\partial^{(a+b)}P}{\partial x_1^a \partial x_2^b}\cdot \frac{\partial^{(k-a-b)}(1/g)}{\partial x_1^{i-a}\partial x_2^{k-b}}.$$

As $\frac{\partial^{(k)}P}{\partial x_1^i \partial x_2^{k-i}}\Big|_{x_1=x_2} = 0$ for all $k \le 2m$, we have $\frac{\partial^{(a+b)}P}{\partial x_1^a \partial x_2^b}\Big|_{x_1=x_2} = 0$ for every a and b. Thus, $\frac{\partial^{(k)}}{\partial x_1^i \partial x_2^{k-i}}(1-s_2)(f/g)\Big|_{x_1=x_2} = 0$ for all $k \le 2m$.