Research Paper

On modular invariants of the truncated polynomial rings in low ranks

Le Minh Ha [a], Nguyen Dang Ho Hai [b], Nguyen Van Nghia [c],*

[a] *Faculty of Mathematics-Mechanics-Informatics, University of Science, Vietnam National University, Hanoi, Viet Nam*
[b] *Department of Mathematics, College of Sciences, University of Hue, Viet Nam*
[c] *Faculty of Natural Sciences, Hung Vuong University, Phu Tho, Viet Nam*

A R T I C L E   I N F O

A B S T R A C T

We verify the conjectures due to Lewis, Reiner, and Stanton about the Hilbert series of the invariant ring of the truncated polynomial ring for all parabolic subgroups up to rank 3. This is done by constructing an explicit set of generators for each invariant ring in question. We also propose a conjecture concerning the action of the Steenrod algebra and the Dickson algebra on a certain naturally occurring filtration of the invariant ring under the action of the general linear group.

* Corresponding author.
E-mail addresses: leminhha@hus.edu.vn (L.M. Ha), ndhhai@husc.edu.vn (N.D.H. Hai),
nguyenvannghia@hvu.edu.vn (N.V. Nghia).

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of q elements, where q is a power of a fixed prime number p. Let $I_m(n) = (x_1^{q^m}, \ldots, x_n^{q^m})$ denote the m-th Frobenius power ideal in the polynomial algebra $S(n) = \mathbb{F}_q[x_1, \ldots, x_n]$. Denote by $\mathcal{Q}_m(n)$ the truncated polynomial ring $S(n)/I_m(n)$. The general linear group $G_n = GL_n(\mathbb{F}_q)$ acts on $S(n)$ by linear substitutions of variables. Since $I_m(n)$ is a G_n-invariant ideal, $\mathcal{Q}_m(n)$ inherits a G_n-action from $S(n)$. As we will be working with a fixed number of generators n, we will usually omit n from the notation.

This paper addresses the problem of computing invariants of the truncated ring $\mathcal{Q}_m(n)$ under the action of various parabolic subgroups of G_n. This problem arises in several contexts, including algebraic combinatorics ([11], [12], [9], [4]), algebraic topology ([1], [7], [8]) and number theory [2]. In particular, as shown in [9, Conjecture 1.3], knowing the Hilbert series of $\mathcal{Q}_m(n)^G$ provides the Hilbert series of the cofixed space S_G of the polynomial ring under the action of the general linear group. Surprisingly, while the invariant ring S^G has been completely determined since the beginning of the 20th century, by the fundamental work of Dickson [3], the problem of determining S_G is still an open problem in modular invariant theory.

For a positive integer n, a composition of n of length ℓ is an ordered set $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ of positive integers α_i such that $|\alpha| = \alpha_1 + \ldots + \alpha_\ell = n$. We will also consider weak compositions, which are ordered sets of non-negative integers. The set of weak compositions of a given length is partially ordered by declaring that $\beta \leq \alpha$ iff $\beta_i \leq \alpha_i$ for all i. If α is a composition of n, we denote by $P(\alpha)$ the corresponding parabolic subgroup of G_n. In [9], Lewis, Reiner, and Stanton proposed a marvelous set of conjectures about the Hilbert series of the invariant ring $\mathcal{Q}_m(n)^{P(\alpha)}$ for arbitrary m and any composition α of n, expressed in terms of a new combinatorial object called the (q, t)-binomial coefficient, introduced in [12]:

Conjecture 1.1. *([9, Parabolic Conjecture 1.5]) The Hilbert series of the ring of invariants of $\mathcal{Q}_m(n)$ under the action of the parabolic subgroup $P(\alpha)$ is:*

$$C_{\alpha,m}(t) = \sum_{\beta, \beta \leq \alpha, |\beta| \leq m} t^{e(m,\alpha,\beta)} \begin{bmatrix} m \\ \beta, m - |\beta| \end{bmatrix}_{q,t},$$

where $e(m, \alpha, \beta) = \sum(\alpha_i - \beta_i)(q^m - q^{B_i})$, $B_i = \beta_1 + \ldots + \beta_i$, and for a composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ of d with partial sum $\alpha_1 + \ldots + \alpha_i = A_i$, the (q,t) binomial coefficient $\begin{bmatrix} d \\ \alpha \end{bmatrix}_{q,t}$ is defined as the quotient

$$\begin{bmatrix} d \\ \alpha \end{bmatrix}_{q,t} = \frac{\prod_{j=0}^{d-1}(1 - t^{q^d - q^j})}{\prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i}(1 - t^{q^{A_i} - q^{A_{i-1}+j}})}.$$

In particular, in the most interesting case where $\alpha = (n)$, they conjectured that

Conjecture 1.2. *([9, Conjecture 1.2]) The Hilbert series of the ring of invariants of $\mathcal{Q}_m(n)$ under the action of the general linear group G_n is:*

$$C_{n,m}(t) = \sum_{k=0}^{\min(n,m)} t^{(n-k)(q^m - q^k)} \begin{bmatrix} m \\ k \end{bmatrix}_{q,t}.$$

These conjectures are inspired by properties of the q-Catalan and q-Fuss-Catalan numbers, connecting Hilbert series of certain invariant subspaces with the representation theory of rational Cherednik algebras for Coxeter and complex reflection groups. Some partial results about these two conjectures have been obtained (see Drescher-Shepler [4], Goyal [5], and the original paper [9]). Nevertheless, the role of these combinatorial objects in the series remains quite mysterious.

In our previous work [6], we proved their parabolic conjecture for the minimal parabolic subgroup B by constructing an explicit basis for the $\mathbb{F}_q$-vector space $\mathcal{Q}_m(n)^B$ for all m and n. We also refined their conjectures by proposing an explicit $\mathbb{F}_q$-basis for $\mathcal{Q}_m(n)^{P(\alpha)}$.

Conjecture 1.3. *A basis for the space of $P(\alpha)$-invariants of $\mathcal{Q}_m(n)$ is given by the set $\mathcal{B}_m(\alpha)$ consisting of elements of the form*

$$\delta_{B_1+1;m}^{\alpha_1 - \beta_1} \left(f_1 \delta_{B_2+1;m}^{\alpha_2 - \beta_2} \left(\cdots f_{\ell-1} \delta_{B_\ell+1;m}^{\alpha_\ell - \beta_\ell} (f_\ell) \right) \right)$$

where $\beta \leq \alpha, |\beta| \leq m$, $B_i = \beta_1 + \ldots + \beta_i$ (by convention, $B_0 = 0$) and $f_i \in \Phi^{B_{i-1}} \Delta_{\beta_i}^{m-B_{i-1}} \subseteq \Delta_{B_i}^{m-B_i}$.

Here $\delta_{a;b}$ is the operator constructed in [6] and Δ_s^m is a certain subspace of the Dickson algebra $\mathcal{D}_s$ ([3]) of all GL_s-invariant polynomials:

$$\Delta_s^m \subset \mathcal{D}_s = \mathbb{F}_q[Q_{s,s-1}, \ldots, Q_{s,1}, Q_{s,0}].$$

The Dickson invariants $Q_{s,i}$ are crucial to our investigation and will be reviewed in detail in Section 2. The Frobenius-like operator Φ is a ring map from $\mathcal{D}_s$ to $\mathcal{D}_{s+1}$ which sends $Q_{s,i}$ to $Q_{s+1,i+1}$.

The reader of [6] may notice that in this conjecture, we describe a member of the conjectural generating set $\mathcal{B}_m(\alpha)$ explicitly rather than by induction. In addition, we make use of the core subspace Δ_s^m (see 2.2 below) of the Dickson algebra instead of ∇_s^m in the original conjecture. The two candidates for *core spaces* can be used interchangeably, but Δ_s^m is more convenient for explicit calculation, as we will see later.

In the case $\alpha = (n)$ so that $P(\alpha)$ is the full general linear group, we have

Conjecture 1.4. *The set $\mathcal{B}_m(n)$ consisting of the following family of elements:*

$$\delta_{s+1;m}^{n-s}(f), f \in \Delta_s^m, 0 \le s \le \min(m,n),$$

forms a basis for the $\mathbb{F}_q$-vector space of G_n-invariants of $\mathcal{Q}_m(n)$.

It is a simple counting problem that our proposed bases have the correct Hilbert series as predicted. Hence our conjectures refine the two conjectures proposed by Lewis, Reiner, and Stanton. Furthermore, they also explain where the summands of the Hilbert series occur in the original conjectures: The summands of $C_{n,m}(t)$ are just the Hilbert series of Δ_s^m, $0 \le s \le \min(m,n)$, shifted by an appropriate degree due to the iterated delta operator.

In [6], we have verified the refined parabolic Conjecture 1.3 for the Borel subgroup, that is when $\alpha = 1^n$. The aim of this paper is to verify our conjectures for other parabolic subgroups, including the full general linear group, for $n \le 3$. As an immediate corollary, the parabolic conjecture of Lewis, Reiner and Stanton is true in these cases.

Theorem 1.5. *The refined parabolic Conjectures 1.3 and 1.4 are true for $n \le 3$ and all $m \ge 1$. Hence, the parabolic conjecture of Lewis, Reiner, and Stanton is true in these cases.*

In this paper, we choose to work as explicitly as possible to illuminate the underlying mechanism of our construction and to highlight the additional structure present in our basis. Our computations reveal an interesting property of the invariant rings when considered as modules over the Dickson algebra. We also describe the action of the Steenrod algebra. In future work, we hope to revisit this problem in greater generality.

When $n = 2$, the only parabolic subgroup other than the Borel subgroup is G_2 itself, and the parabolic conjecture has already been verified in the original paper [9]. However, the authors worked with the dual situation involving cofixed spaces and used a specific property of the bivariate case to avoid the truncated ring. As a result, it remains unclear whether the invariant subspace of $\mathcal{Q}_m(n)$, even in rank $n = 2$, can be described explicitly using their method.

In [5, Corollary 4.3], Goyal constructed a family of G_n-invariant polynomials in $\mathcal{Q}_m(n)$ which corresponds to the family $\delta_2^{n-1}(\Delta_1^m)$ in our notation.

To simplify the notation, we will often drop the index n in $\mathcal{Q}_m(n)$, $S(n)$, and G_n when the number of variables is well-understood from the context. If the Frobenius power m is fixed, we write δ_s instead of $\delta_{s;m}$. It is also convenient to write $(e_1, \ldots, e_s) \in \Delta_s^m$ to indicate a Dickson monomial $Q_{s,s-1}^{e_1} \ldots Q_{s,0}^{e_s}$ in Δ_s^m. For any nonnegative integer a, we denote by $[a]_q$ the q-integer $(q^a - 1)/(q-1)$ with the convention that $[0]_q = 1$.

Here is our first result in rank 2.

Proposition 1.6. *The set $\mathcal{B}_m(2)$ consisting of 3 families below forms a basis for the invariant subspace $\mathcal{Q}_m(2)^G$ of the full general linear group.*

(1) $\delta_1(\delta_1(1)) = x_1^{q^m-1} x_2^{q^m-1}$.
(2) $\delta_2(\Delta_1^m)$.
(3) Δ_2^m.

In rank 3, other than the Borel subgroups, there are two proper parabolic subgroups. Their corresponding rings of invariants are described in the next two propositions.

Proposition 1.7. *The set $\mathcal{B}_m(2,1)$ consisting of 6 families below forms a basis for the invariant subspace $\mathcal{Q}_m^{P(2,1)}$ of the parabolic subgroup corresponding to the composition $(2,1)$.*

(1) $Q_{2,1}^{i_1} Q_{2,0}^{i_2} Q_{3,2}^{i}$, $(i_1, i_2) \in \Delta_2^m$, $i < [m-2]_q$.
(2) $Q_{2,1}^{i_1} Q_{2,0}^{i_2} \delta_3(1)$, $(i_1, i_2) \in \Delta_2^m$.
(3) $\delta_2(Q_{1,0}^{i_1} Q_{2,1}^{i})$, $i_1 < [m]_q$, $i < [m-1]_q$.
(4) $\delta_2(Q_{1,0}^{i_1} \delta_2(1))$, $i_1 < [m]_q$.
(5) $\delta_1(\delta_1(Q_{1,0}^i))$, $i < [m]_q$.
(6) $\delta_1(\delta_1(\delta_1(1)))$.

Proposition 1.8. *The set $\mathcal{B}_m(1,2)$ consisting of 6 families below forms a basis for the invariant subspace $\mathcal{Q}_m^{P(1,2)}$ of the parabolic subgroup corresponding to the composition $(1,2)$.*

(1) $Q_{1,0}^{j_1} Q_{3,2}^{i_1} Q_{3,1}^{i_2}$, $j_1 < [m]_q, (i_1, i_2) \in \Delta_2^{m-1}$.
(2) $Q_{1,0}^{j_1} \delta_3(Q_{2,1}^{j_2})$, $j_1 < [m]_q, j_2 < [m-1]_q$.
(3) $Q_{1,0}^{j_1} \delta_2(\delta_2(1))$, $j_1 < [m]_q$.
(4) $\delta_1(Q_{2,1}^{i_1} Q_{2,0}^{i_2})$, $(i_1, i_2) \in \Delta_2^m$.
(5) $\delta_1(\delta_2(Q_{1,0}^{j_1}))$, $j_1 < [m]_q$.
(6) $\delta_1(\delta_1(\delta_1(1)))$.

Our final result, which is also the most technical, is for the full general linear group in rank 3:

Proposition 1.9. *The set $\mathcal{B}_m(3)$ consisting of 4 families below forms a basis for the invariant subspace $\mathcal{Q}_m(3)^G$ of the full general linear group.*

(1) $\delta_1(\delta_1(\delta_1(1))) = x_1^{q^m-1} x_2^{q^m-1} x_3^{q^m-1}$.
(2) $\delta_2(\delta_2(\Delta_1^m))$.
(3) $\delta_3(\Delta_2^m)$.
(4) Δ_3^m.

Since the case of the Borel subgroup, which corresponds to the composition $(1, 1, 1)$ of $n = 3$, was treated in [6], the propositions stated above together imply the main Theorem 1.5.

It is worth noting that when m is small relative to n, all results still hold, provided they are interpreted appropriately. For example, when $n = 3$ and $m = 2$, the set Δ_3^2 is empty, and $\delta_{3;2}(\Delta_2^2)$ consists of just a single element, namely $\delta_{3;2}(1) = 1 \in \mathbb{F}_q$ in degree 0. To avoid excessive attention to these special cases (whose proofs are straightforward), we will generally assume that m is sufficiently large compared to n (in fact, $m \geq n$ is enough!).

In the process of establishing these results, we have also computed the structure of these invariant spaces considered as modules over the Dickson algebra and the mod q Steenrod algebra.

Definition 1.10. For each $0 \leq k \leq \min(m, n)$, let $\mathcal{F}_{n,k}$ denote the subspace of $\mathcal{Q}_m(n)^G$ spanned by the subsets $\delta_{s+1}^{n-s}(\Delta_s^m)$ where $0 \leq s \leq k$:

$$\mathcal{F}_{n,k} = \text{Span}\{\delta_{s+1}^{n-s}(f) \colon f \in \Delta_s^m, 0 \leq s \leq k\}.$$

These subspaces form an increasing filtration of $\mathcal{Q}_m(n)^G$, starting with the one-dimensional subspace $\mathcal{F}_{n,0}$, which is spanned by the top-degree class $(x_1 \ldots x_n)^{q^m-1}$. At least in the cases we have computed, this filtration is exhaustive and exhibits remarkable properties. We propose the following:

Conjecture 1.11. *For each $1 \leq k < \min(m, n)$, $\mathcal{F}_{n,k}$ is an $\mathcal{A}$-submodule as well as a $\mathcal{D}_n$-submodule of $\mathcal{Q}_m(n)^G$. Moreover, $\mathcal{F}_{n,k}$ is annihilated by the Dickson invariants $Q_{n,0}, Q_{n,1} \ldots Q_{n,n-k-1}$.*

This conjecture suggests that the filtration $\mathcal{F}_{n,*}$ may admit an alternative description of a topological nature. We are able to verify this conjecture up to rank 3:

Theorem 1.12. *The Conjecture 1.11 is true for $n \leq 3$.*

The layout of this paper is as follows: Section 2 recalls basic results in modular invariant theory and the key constructions from our previous work. In Section 3, we establish a lower bound on the total dimension of the invariant subspaces. The subsequent four sections are devoted to proving Propositions 1.6 through 1.9. The final section discusses the actions of the Dickson algebra and the Steenrod algebra, and presents the proof of Theorem 1.12.

Acknowledgment

2. Recollection

In this section, we recall some background materials about modular invariant theory and the main construction in [6].

2.1. Upper triangular invariants and Dickson invariants

The canonical projection $S \to \mathcal{Q}_m$ is clearly a G-equivariant map. Thus, for each parabolic subgroup of G, there is an induced $\mathbb{F}_q$-algebra homomorphism

$$S^G \subset S^P \to \mathcal{Q}_m^P,$$

which makes the invariant ring $\mathcal{Q}_m^P$ into a module over S^G. The structure of the invariant ring S^G, which is the Dickson algebra [3], is well-known and plays a significant role in our investigation.

For each positive integer k, denote by V_k the product

$$V_k(x_1, \ldots, x_k) = \prod_{\lambda_i \in \mathbb{F}_q} (x_k + \lambda_1 x_1 + \ldots + \lambda_{k-1} x_{k-1}).$$

It is well-known that the invariant ring S^B under the Borel subgroup of upper triangular matrices is a polynomial algebra generated by $V_1^{q-1}, V_2^{q-1}, \ldots, V_n^{q-1}$ (see for example, [10, Theorem 3.4]). Let X be an indeterminate, and recall the fundamental equation

$$V_{n+1}(x_1, \ldots, x_n, X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} Q_{n,i} X^{q^i}.$$

The polynomials $Q_{n,i} = Q_{n,i}(x_1, \ldots, x_n)$ are evidently G-invariant, and are called Dickson invariants because of the following celebrated theorem due to Dickson:

$$\mathcal{D}_n = S^G = \mathbb{F}_q[Q_{n,0}, \ldots, Q_{n,n-1}].$$

The Dickson invariants $Q_{n,i}$ can be described more explicitly as follows. For any n-tuple of non-negative integers $(r_1, \ldots, r_n)$, put

$$[r_1, \ldots, r_n] = \det(x_i^{q^{r_j}})_{1 \leq i,j \leq n}.$$

In particular, let $L_n = L_n(x_1, \ldots, x_n)$ denote $[0, 1 \ldots, n-1]$. We then have

$$Q_{n,i} = [0, \ldots, \hat{i}, \ldots, n]/L_n.$$

In particular, $Q_{n,n} = 1$ and $Q_{n,0} = L_n^{q-1}$. By convention, we set $Q_{n,i} = 0$ if $i < 0$ or $i > n$. The following relations are well-known (see for example, [15, Proposition 1.3]):

Proposition 2.1. *Let n be a positive integer and $0 \le i \le n$. The following relations hold:*

(i) $L_n = V_1 V_2 \cdots V_n$.
(ii) $Q_{n,i} = V_n^{q-1} Q_{n-1,i} + Q_{n-1,i-1}^q$.

Note that L_n is, up to sign, the product of all lines in the $\mathbb{F}_q$-vector space spanned by $x_1, \ldots, x_n$.

2.2. The Δ subspace of the Dickson algebra

Lewis, Reiner and Stanton [9, Subsection 7.4] speculated that a portion of the Dickson algebra studied in [12, Section 5] might form part of an $\mathbb{F}_q$-basis for $\mathcal{Q}_m(n)^G$. Our work confirms this intuition. In fact, this portion, which we call the Delta subspace, plays a central role. We now review its construction and some elementary properties.

Given a positive integer s and a partition $\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_s$ with at most s nonzero parts, we say that a Dickson monomial $Q_{s,s-1}^{e_1} \ldots Q_{s,0}^{e_s}$ in $\mathcal{D}_s$ is of type $(\lambda_1, \ldots, \lambda_s)$ (or q-compatible with $(\lambda_1, \ldots, \lambda_s)$, in the language of [12, Definition 5.4]) if for each $1 \le i \le s$,

$$e_i \in \left[\frac{q^{\lambda_i} - q^{\lambda_{i+1}}}{q-1}, \frac{q^{\lambda_i+1} - q^{\lambda_{i+1}}}{q-1} \right).$$

By convention, $\lambda_{s+1} = 0$. Every Dickson monomial in $\mathcal{D}_s$ is q-compatible with a unique partition $(\lambda_1, \ldots, \lambda_s)$ of length $\le s$.

Now suppose $s \le m$, and we will restrict our attention to partitions whose Ferrers diagrams fit inside a $s \times (m-s)$ rectangle, that is, partitions with at most s nonzero parts and $m - s \ge \lambda_1$. Define $\Delta_{(\lambda_1, \ldots, \lambda_s)}$ as the subset of the Dickson algebra $\mathcal{D}_s$ consisting of Dickson monomials of type $(\lambda_1, \ldots, \lambda_s)$, and let Δ_s^m denote the disjoint union of all subsets over all such partitions fitting inside an $s \times (m-s)$ rectangle. By convention, we put $\Delta_s^m = \emptyset$ if $s > m$, and $\Delta_0^m = \{1\}$.

The Dickson monomials in Δ_s^m for $s \le \min(m, n)$ together with the delta operators recalled below are the building blocks for our basis. For this reason, we will say that Dickson monomials in Δ_s^m *essential* monomials. We will also work with the *edge* monomials, which are the Dickson monomials not in Δ_s^m that have the form $Q_{s,i} f$ where $f \in \Delta_s^m$, for some $0 \le i \le s-1$. Clearly, the edge monomials are those such that $e_j = \frac{q^{\lambda_j+1} - q^{\lambda_j+1}}{q-1}$ for some $1 \le j \le s$ and $e_i \in [\frac{q^{\lambda_i} - q^{\lambda_{i+1}}}{q-1}, \frac{q^{\lambda_i+1} - q^{\lambda_{i+1}}}{q-1})$ for all $i \ne j$.

2.3. The delta operator

The operator $\delta_{a;b}$ introduced in [6] is fundamental to our construction. We now recall its definition and main properties.

Definition 2.2. Let a, b, c be positive integers such that $1 \le a \le c + 1$. If f is a rational function in c variables, then $\delta_{a;b}(f)$ is a function in $(c + 1)$ variables, defined as the quotient

$$
\delta_{a;b}(f) = \frac{
\begin{vmatrix}
x_1 & \cdots & x_a \\
x_1^q & \cdots & x_a^q \\
\vdots & \ddots & \vdots \\
x_1^{q^{a-2}} & \cdots & x_a^{q^{a-2}} \\
x_1^{q^b} f(\widehat{x_1}, x_2, \ldots, x_{c+1}) & \cdots & x_a^{q^b} f(x_1, \ldots, \widehat{x_a}, \ldots, x_{c+1})
\end{vmatrix}
}{
\begin{vmatrix}
x_1 & \cdots & x_a \\
x_1^q & \cdots & x_a^q \\
\vdots & \ddots & \vdots \\
x_1^{q^{a-1}} & \cdots & x_a^{q^{a-1}}
\end{vmatrix}
}.
$$

Thus if $b \ge a - 1$, $\delta_{a;b}$ increases degree by $q^b - q^{a-1}$. By definition, if we separate the first $(a - 1)$ variables and write f in the form $f = \sum g(x_1, \ldots, x_{a-1})h(x_a, \ldots, x_c)$, then

$$
\delta_{a;b}(f) = \sum \delta_{a;b}(g)h(x_{a+1}, \ldots, x_{c+1}).
$$

It was shown in greater generality in [6] that $\delta_s(f)$ is generally not a polynomial. Still, in the cases that we are interested in, it is a genuine polynomial. Moreover, $\delta_s(f)$ is rarely a Dickson polynomial but it is a G_s-invariant modulo I_m. We give a precise statement and provide an elementary proof for δ_3 to make the paper self-contained.

Proposition 2.3. *If f is a G_2-invariant polynomial, then $\delta_3(f)$ is also a polynomial and is G_3-invariant in $\mathcal{Q}_m(3)$.*

Proof. We first show that $\delta_3(f)$ is a polynomial. Recall the denominator $L_3 = V_1 V_2 V_3$ is a product of nonzero linear forms in the variables x_1, x_2, x_3, so it suffices to prove that the numerator of $\delta_3(f)$ becomes zero whenever there exists a nontrivial linear relation among the x_i, which by symmetry, can be assumed to have the following form:

$$
x_3 = a_1 x_1 + a_2 x_2, \quad (a_1, a_2) \in \mathbb{F}_q \times \mathbb{F}_q. \tag{2.1}
$$

We claim that this implies a similar linear relation among the columns of the numerator of $\delta_3(f)$, that is,

$$
x_3^{q^m} f(x_1, x_2) = a_1 x_1^{q^m} f(x_2, x_3) + a_2 x_2^{q^m} f(x_1, x_3). \tag{2.2}
$$

Indeed, this is clear if $a_1 = a_2 = 0$. If the scalars a_1, a_2 are both nonzero, then there is an equality

$$f(x_2, a_1x_1 + a_2x_2) = f(x_1, a_1x_1 + a_2x_2) = f(x_1, x_2),$$

since f is a G_2-invariant. So the right-hand side of (2.2) becomes

$$(a_1x_1^{q^m} + a_2x_2^{q^m})f(x_1, x_2) = (a_1x_1 + a_2x_2)^{q^m}f(x_1, x_2) = x_3^{q^m}f(x_1, x_2).$$

Finally, if one of the a_i is zero, say $a_1 = 0$, Equation (2.2) is reduced to

$$(a_2x_2)^{q^m}f(x_1, x_2) = a_2x_2^{q^m}f(x_1, a_2x_2),$$

which is again true because f is G_2-invariant. We have finished the proof that $\delta_3(f)$ is a polynomial.

The next step is to show that $\delta_3(f)$ is G_3-invariant modulo I_m. By symmetry, it suffices to prove that $\delta_3(f)$ does not change under the operation that sends x_1 to $x_1 + x_2$ and fixes x_2, x_3. The denominator L_3 certainly satisfies this condition. By direct inspection, the difference $\delta_3(f)(x_1 + x_2, x_2, x_3) - \delta_3(f)(x_1, x_2, x_3)$ equals

$$x_2^{q^m} \times \frac{\begin{vmatrix} x_1 & x_2 & x_3 \\ x_1^q & x_2^q & x_3^q \\ f(x_2, x_3) - f(x_1 + x_2, x_3) & f(x_1 + x_2, x_3) - f(x_1, x_3) & 0 \end{vmatrix}}{L_3}.$$

We already know that this is a polynomial. Moreover, x_2 occurs as a simple factor in the denominator L_3, and the determinant in the numerator vanishes when $x_2 = 0$. It follows that this polynomial is divisible by $x_2^{q^m}$, thus trivial in $\mathcal{Q}_m(3)$. $\square$

Example 2.4. The G_1-polynomials are of the form $f(x) = x^{s(q-1)} = Q_{1,0}^s$, $s \geq 0$. Then $\delta_2(x^{s(q-1)})$ is a G_2-invariant polynomial in $\mathcal{Q}_m(2)$. For $s < [m]_q$, this is Goyal's y_s family in [5] where it was defined as

$$y_s = x_1^{q^m - q}x_2^{s(q-1)} + x_1^{q^m - q - (q-1)}x_2^{(s+1)(q-1)} + \ldots + x_1^{s(q-1)}x_2^{q^m - q}.$$

Our construction is also valid for $s \geq [m]_q$. However, it is trivial in $\mathcal{Q}_m(2)$ except when $s = [m]_q + 1$, in which case

$$\delta_2(Q_{1,0}^{[m]_q+1}) = -x_1^{q^m - 1}x_2^{q^m - 1} = -\delta_1^2(1).$$

It is easy to check that y_s is a genuine G_2-invariant (that is, a Dickson polynomial) whenever $s = \frac{q^i - 1}{q - 1}$ for some non-negative integer i.

Example 2.5. For $s \leq [m]_q$, $\delta_2^2(Q_{1,0}^s)$ is a G_3-invariant of degree $2(q^m - q) + s(q - 1)$ in $\mathcal{Q}_m(3)$. This family of elements coincides with Goyal's polynomials $a_{m,3,s}$ in [5, Corollary 4.3] where it was written in a different form:

$$a_{m,3,s} = \sum_{(i_1,i_2,i_3)} x_1^{i_1(q-1)} x_2^{i_2(q-1)} x_3^{i_3(q-1)},$$

where the sum is taken over all triples (i_1, i_2, i_3) of non-negative integers such that $i_s < [m]_q$ and $i_1 + i_2 + i_3 = 2[m]_q - 2 + s$. Again, our definition also works for $s > [m]_q$:

$$\delta_2^2(Q_{1,0}^{[m]_q+2}) = \delta_1^3(1) = x_1^{q^m-1} x_2^{q^m-1} x_3^{q^m-1},$$

and is trivial in all other cases.

Warning 2.6. It is not true in general that if $f = g$ in $\mathcal{Q}_m(n)$ then $\delta_s(f) = \delta_s(g)$ in $\mathcal{Q}_m(n)$, even in the case where all expressions involved are polynomials. This is evident from Example 2.4 above for $f = Q_{1,0}^{[m]_q+1}$ and $g = 0$. Thus when working with iterated delta operators, for example, $\delta_2^2(f) = \delta_2(\delta_2 f)$, we cannot take $\delta_2 f$ modulo I_m before applying δ_2 again.

2.4. The delta operator and the Dickson algebra

For each composition α of n, the invariant ring $\mathcal{Q}_m(n)^{P(\alpha)}$ is a module over the Dickson algebra $\mathcal{D}_n$. The next result describes how the delta operator interacts with the Dickson algebra in low ranks.

Proposition 2.7. *We have the following identities in $\mathcal{Q}_m$.*

(1) $Q_{s,0}\delta_s(f) = 0$ for all $f \in S$.
(2) $Q_{2,1}\delta_2(f) = \delta_2(Q_{1,0}^q f)$ for all $f \in \mathcal{D}_1$.
(3) $Q_{3,i}\delta_3(f) = \delta_3(Q_{2,i-1}^q f)$ for $i = 1$ or 2 and for all $f \in \mathcal{D}_2$.
(4) $Q_{3,2}\delta_2^2(f) = \delta_2^2(Q_{1,0}^{q^2} f)$ for all $f \in \mathcal{D}_1$.
(5) $Q_{3,1}\delta_2^2(f) = 0$ for all $f \in \mathcal{D}_1$.

Proof. We will make use frequently of the relation 2.1 relating upper-triangular invariants V_k and Dickson invariants $Q_{n,i}$.

The first part is clear since $Q_{s,0} = L_s^{q-1}$. Note that the numerator of $\delta_s(f)$ always vanishes in $\mathcal{Q}_m$ by considering the Laplace expansion along the last row.

Proof of (2). Since $f \in \mathcal{D}_1$, let us assume that $f = Q_{1,0}^s$ for some $s \geq 0$. Since

$$Q_{2,1} = V_2^{q-1}(x_1, x_2) + V_1^{q(q-1)}(x_1) = V_2^{q-1}(x_2, x_1) + V_1^{q(q-1)}(x_2),$$

the numerator of the difference $Q_{2,1}\delta_2(f) - \delta_2(Q_{1,0}^q f)$ has the form

$$\begin{vmatrix} x_1 & x_2 \\ x_1^{q^m} V_2(x_2, x_1)^{q-1} x_2^{s(q-1)} & x_2^{q^m} V_2(x_1, x_2)^{q-1} x_1^{s(q-1)} \end{vmatrix}.$$

Observe that $x_1 V_2(x_1, x_2) = x_2 V_2(x_2, x_1) = L_2(x_1, x_2)$, it follows that

$$Q_{2,1}\delta_2(f) - \delta_2(Q_{1,0}^q f) = x_2^{q^m} V_2(x_1, x_2)^{q-2} x_1^{s(q-1)} - x_1^{q^m} V_2(x_2, x_1)^{q-2} x_2^{s(q-1)} = 0$$

in $\mathcal{Q}_m(2)$.

Proof of (3). We will treat the case $i = 1$, as the situation for $i = 2$ is similar. Consider the difference $Q_{3,1}\delta_3(f) - \delta_3(Q_{2,0}^q f)$. Using the identity $Q_{3,1} = V_3^{q-1} Q_{2,1} + Q_{2,0}^q$, the (3,1)-entry in the last row of the determinant in the numerator can be simplified as

$$x_1^{q^m} V_3^{q-1}(x_2, x_3, x_1) Q_{2,1}(x_2, x_3) f(x_2, x_3).$$

There is a similar description for other entries in this row. Since

$$V_3(x_2, x_3, x_1) L_2(x_2, x_3) = L_3(x_2, x_3, x_1) = L_3(x_1, x_2, x_3),$$

the Laplace expansion along the last row of the determinant in the numerator shows that the resulting polynomial belongs to I_m, which is zero in $\mathcal{Q}_m(3)$.

Proof of (4). From Proposition 2.1, we have $Q_{3,2} = V_3^{q-1} + Q_{2,1}^q$. We write $Q_{3,2}$ in two different ways:

$$Q_{3,2} = V_3^{q-1}(x_2, x_3, x_1) + Q_{2,1}^q(x_2, x_3) = V_3^{q-1}(x_1, x_3, x_2) + Q_{2,1}^q(x_1, x_3).$$

It follows that $Q_{3,2}\delta_2(\delta_2 f) - \delta_2(Q_{2,1}^q \delta_2 f)$ equals

$$\frac{1}{L_2(x_1, x_2)} \begin{vmatrix} x_1 & x_2 \\ x_1^{q^m} V_3^{q-1}(x_2, x_3, x_1)(\delta_2 f)(x_2, x_3) & x_2^{q^m} V_3^{q-1}(x_1, x_3, x_2)(\delta_2 f)(x_1, x_3) \end{vmatrix}.$$

Since $x_2 V_3(x_2, x_3, x_1)$ and $x_1 V_3(x_1, x_3, x_2)$ are divisible by $L_2(x_1, x_2)$, the above expression is a polynomial in the ideal generated by $(x_1^{q^m}, x_2^{q^m})$. Thus

$$Q_{3,2}\delta_2(\delta_2 f) = \delta_2(Q_{2,1}^q \delta_2 f) \quad \text{in } \mathcal{Q}_m(3).$$

At this point, as noted in Warning 2.6, we cannot apply immediately part (2), replacing $Q_{2,1}^q \delta_2 f$ with $\delta_2(Q_{1,0}^{q^2} f)$ on the right-hand side. Rather, we make use of the above strategy one more time, writing

$$Q_{2,1}(x_2, x_3) = V_2^{q-1}(x_3, x_2) + V_1^{q^2(q-1)}(x_3),$$

and similarly for $Q_{2,1}(x_1, x_3)$. The difference $\delta_2(Q_{2,1}^q \delta_2 f) - \delta_2^2(Q_{1,0}^{q^2} f)$ can be written as the sum

$$x_3^{q^m} \frac{x_2^{q^m} x_1 f(x_1) V_2^{q^2-q-1}(x_1,x_3) - x_1^{q^m} x_2 f(x_2) V_2^{q^2-q-1}(x_2,x_3)}{L_2(x_1,x_2)} -$$

$$x_2^{q^m} f(x_3) \frac{x_1 x_1^{q^m} V_2^{q^2-q-1}(x_3,x_1) - x_2 x_1^{q^m} V_2^{q^2-q-1}(x_3,x_2)}{L_2(x_1,x_2)}.$$

Now the first summand is a polynomial (since the numerator is divisible by x_1 and vanishes whenever there is a linear relation $x_2 = a_1 x_1$) and is a multiple of $x_3^{q^m}$. Similarly, the second summand belongs to the ideal $(x_2^{q^m})$.

Proof of (5). We first apply the same strategy as part (4), writing

$$Q_{3,1} = V_3^{q-1}(x_1,x_3,x_2) Q_{2,1}(x_1,x_3) + Q_{2,0}^q(x_3,x_2)$$
$$= V_3^{q-1}(x_2,x_3,x_1) Q_{2,1}(x_2,x_3) + Q_{2,0}^q(x_3,x_1),$$

and obtain an equality in $\mathcal{Q}_m(3)$:

$$Q_{3,1}\delta_2(\delta_2 f)) = \delta_2(Q_{2,0}^q \delta_2 f).$$

The right-hand side, by direct inspection, can be written as

$$x_3^{q^m} \frac{x_2^{q^m} x_1^2 f(x_1) L_2^{q^2-q-1}(x_1,x_3) - x_1^{q^m} x_2^2 f(x_2) L_2^{q^2-q-1}(x_2,x_3)}{L_2(x_1,x_2)} +$$

$$x_2^{q^m} f(x_3) x_3 \frac{x_1 x_1^{q^m} L_2^{q^2-q-1}(x_1,x_3) - x_2 x_1^{q^m} L_2^{q^2-q-1}(x_2,x_3)}{L_2(x_1,x_2)}.$$

By the same argument as in part (4), the first summand is divisible by $x_3^{q^m}$ and the second by $x_2^{q^m}$. $\square$

2.5. The Borel subgroup

In [6], we constructed a basis for the invariant ring of $\mathcal{Q}_m(n)$ under the action of the Borel subgroup for arbitrary m and n. In the case $n = 3$, the $\mathbb{F}_q$-basis $\mathcal{B}_m(3)$ for $\mathcal{Q}_m^B$ consists of 4 families:

(1) $x_1^{q^m-1} x_2^{q^m-1} x_3^{j_3(q-1)}$, $j_3 \leq [m]_q$.
(2) $x_1^{q^m-1} x_2^{j_2(q-1)} Q_{2,1}(x_2,x_3)^{j_3}$, $j_2 < [m]_q, j_3 \leq [m-1]_q$.
(3) $x_1^{j_1(q-1)} \delta_2(Q_{2,1}^{j_2})$, $j_1 < [m]_q, j_2 \leq [m-1]_q$.
(4) $x_1^{j_1(q-1)} Q_{2,1}^{j_2} Q_{3,2}^{j_3}$, $j_1 < [m]_q, j_2 < [m-1]_q, j_3 \leq [m-2]_q$.

3. A lower bound on the total dimension of the invariant subspaces

The original Parabolic Conjecture predicted that the Hilbert series of the invariant space $\mathcal{Q}_m(n)^{P(\alpha)}$, where α is a composition of n, is given by the (finite) polynomial

$C_{\alpha,m}(t)$, whose explicit form is stated in Conjecture 1.1. In particular, the value of $C_{\alpha,m}(t)$ when $t = 1$ is expected to equal the total dimension of the finite-dimensional graded $\mathbb{F}_q$-vector space $\mathcal{Q}_m(n)^{P(\alpha)}$.

In this section, we will show that:

Proposition 3.1. *For each $m, n \geq 1$ and any composition α of n, the total dimension of the graded vector space $\mathcal{Q}_m(n)^{P(\alpha)}$ is at least $C_{\alpha,m}(1)$.*

This result is already implicit in [9, Section 6] and holds for arbitrary $n \geq 1$. This relatively simple observation has an important practical consequence: suppose we can construct a generating set for the invariant subspace $\mathcal{Q}_m(n)^{P(\alpha)}$ such that, by dimension counting, the associated Hilbert series $C'_{m,\alpha}(t)$ does not exceed $C_{\alpha,m}(t)$ (i.e. $f(t) \leq g(t)$ if and only if $g(t) - f(t)$ is a polynomial with non-negative coefficients). Then, since the reverse inequality $C'_{\alpha,m}(1) \geq C_{\alpha,m}(1)$ holds evaluated at $t = 1$, we may conclude that these two series must be identical since both are finite degree polynomials with non-negative coefficients. It follows that our generating set is, in fact, a basis for $\mathcal{Q}_m(n)^{P(\alpha)}$.

Proof of Proposition 3.1. Consider the following ungraded quotient of the polynomial algebra:

$$\mathcal{R} = \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^{q^m} - x_1, \ldots, x_n^{q^m} - x_n).$$

The action of $G = GL_n$ on $\mathbb{F}_q[x_1, \ldots, x_n]$ descends to this quotient. There is a natural filtration:

$$\{0\} = F_{-1} \subset F_0 \subset F_1 \subset \cdots \subset F_{n(q^m-1)} = \mathcal{R},$$

where F_i is the image of the set of all polynomials of degree at most i under the canonical projection $\mathbb{F}_q[x_1, \ldots, x_n] \twoheadrightarrow \mathcal{R}$. Let $\mathfrak{gr}_F \mathcal{R}$ denote the associated graded vector space $\bigoplus_{i \geq 0} F_i/F_{i-1}$ and equip $\mathfrak{gr}_F \mathcal{R}$ with a ring structure where the multiplication is induced by the product $F_i F_j \to F_{i+j}$. The canonical $\mathbb{F}_q$-algebra map

$$\mathbb{F}_q[x_1, \ldots, x_n] \to \mathcal{R} \to \mathfrak{gr}_F \mathcal{R}, \quad x_i \mapsto \bar{x}_i \in F_1/F_0,$$

induces an isomorphism of G-equivariant $\mathbb{F}_q$-algebras:

$$\mathcal{Q}_m(n) \cong \mathfrak{gr}_F \mathcal{R}.$$

On the other hand, if we apply the functor taking G-invariants on each short exact sequence of G-modules

$$0 \to F_{i-1} \to F_i \to F_i/F_{i-1} \to 0,$$

and compute the dimension, we obtain an inequality

$$\dim(F_i)^G \leq \dim(F_{i-1})^G + \dim(F_i/F_{i-1})^G$$

and so

$$\dim \mathcal{R}^G \leq \dim(\mathfrak{gr}_F \mathcal{R})^G = \dim \mathcal{Q}_m(n)^G.$$

To compute the $\mathbb{F}_q$-dimension of $\mathcal{R}^G$, we extend the field $\mathbb{F}_q$ to a field $\mathbb{F}$ which contains $\mathbb{F}_{q^m}$. Then the evaluation map

$$f(x_1, \ldots, x_n) \mapsto [(v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n \mapsto f(v_1, \ldots, v_n) \in \mathbb{F}],$$

induces an isomorphism of $\mathbb{F}$-algebras

$$\mathbb{F} \otimes_{\mathbb{F}_q} \mathcal{R} \xrightarrow{\cong} \mathrm{Map}\left(\mathbb{F}_{q^m}^n, \mathbb{F}\right).$$

This isomorphism is also G-equivariant where G acts on the right-hand side via the embedding $G = GL_n(\mathbb{F}_q) \subset GL_n(\mathbb{F}_{q^m})$. It follows that there is an isomorphism

$$(\mathbb{F} \otimes_{\mathbb{F}_q} \mathcal{R})^G \cong \mathrm{Map}\left(\mathbb{F}_{q^m}^n/G, \mathbb{F}\right).$$

The $\mathbb{F}_q$-dimension of $(\mathbb{F} \otimes_{\mathbb{F}_q} \mathcal{R})^G$ is thus equal to the cardinality of the orbit set $\mathbb{F}_{q^m}^n/G$. Finally this cardinality is equal to the sum $\sum_{s=0}^{\min(m,n)} \begin{bmatrix} m \\ s \end{bmatrix}_q$ where $\begin{bmatrix} m \\ s \end{bmatrix}_q$ is the q-binomial coefficient which counts the number of s-dimensional subspaces of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^m}$.

In summary, we have shown that

$$\dim_{\mathbb{F}_q} \mathcal{R}^G = \dim_F(\mathbb{F} \otimes_{\mathbb{F}_q} \mathcal{R}^G) = \sum_{s=0}^{\min(m,n)} \begin{bmatrix} m \\ s \end{bmatrix}_q = C_{m,n}(1) \leq \dim \mathcal{Q}_m(n)^G.$$

The argument above clearly is not affected if one uses a parabolic subgroup P_α instead of G. The proposition is proved. $\square$

We end this section with the following observation about our proposed basis $\mathcal{B}_m(\alpha)$.

Lemma 3.2. *For each composition α of n, the Hilbert series for the $\mathbb{F}_q$-space spanned by $\mathcal{B}_m(\alpha)$ is not greater than $C_{\alpha,m}(t)$.*

Proof. This is almost obvious from the definition of $C_{\alpha,m}(t)$ and the relationship between the subset $\Delta_s^m \subset \mathcal{D}_s$ and the (multinomial) (q,t)-coefficient. Recall that

$$C_{\alpha,m}(t) = \sum_{\beta \leq \alpha, |\beta| \leq m} t^{e(m,\alpha,\beta)} \begin{bmatrix} m \\ \beta, m - |\beta| \end{bmatrix}_{q,t},$$

where $e(m, \alpha, \beta) = \sum (\alpha_i - \beta_i)(q^m - q^{B_i})$. Our conjectural basis explains precisely how the summands in the above expression occur. Indeed, for each composition β, with $\beta \leq \alpha$ and $|\beta| \leq m$, $e(m, \alpha, \beta)$ is exactly the total degree raised by the delta operators in a basis element

$$\delta_{B_1+1;m}^{\alpha_1-\beta_1}\left(f_1\delta_{B_2+1;m}^{\alpha_2-\beta_2}\left(\cdots f_{\ell-1}\delta_{B_\ell+1;m}^{\alpha_\ell-\beta_\ell}(f_\ell)\right)\right),$$

and the (q,t)-multinomial coefficient $\begin{bmatrix} m \\ \beta, m-|\beta| \end{bmatrix}_{q,t}$ corresponds to the number of choices of ℓ-tuple $(f_1, \ldots, f_\ell)$ where $f_i \in \Phi^{B_{i-1}}\Delta_{\beta_i}^{m-B_i-1}$. Note that according to [12, (7.1)], we can write

$$\begin{bmatrix} m \\ \beta, m-|\beta| \end{bmatrix}_{q,t} = \begin{bmatrix} m \\ \beta_1 \end{bmatrix}_{q,t} \varphi^{\beta_1}\begin{bmatrix} m-B_1 \\ \beta_2 \end{bmatrix}_{q,t} \varphi^{\beta_2}\begin{bmatrix} m-B_2 \\ \beta_3 \end{bmatrix}_{q,t}\cdots$$

where φ is the (genuine) Frobenius operator, which reflects how our operator Φ affects the degree. □

The results in this section simplify our tasks considerably. Indeed, in order to show that $\mathcal{B}_m(\alpha)$ is a basis for $\mathcal{Q}_m(n)^{P_\alpha}$, it suffices to verify that it is a generating set.

4. Proof of Proposition 1.6

As remarked in the previous section, it suffices to show that $\mathcal{B}_m(2)$ is a generating set for $\mathcal{Q}_m(2)^G$. The proof of Proposition 1.6 is done in two steps. Firstly, we use the relative transfer from the known invariant ring $\mathcal{Q}^B$ of the Borel subgroup B to show that a bigger set $\mathcal{B}'$, consisting of 3 families:

(1) $\delta_1^2(1) = x_1^{q^m-1}x_2^{q^m-1}$,
(2) $\delta_2(Q_{1,0}^s) = y_s$, $0 \leq s < [m]_q$,
(3) $\mathcal{D}_2$,

is a generating set for $\mathcal{Q}_m(2)^G$. Then we show that to generate the invariant ring, it is possible to replace the Dickson algebra $\mathcal{D}_2$ in the third family by the smaller subspace Δ_2^m.

Lemma 4.1. *The set $\mathcal{B}'$ consisting of 3 families above spans $\mathcal{Q}_m(2)^G$.*

Proof. In [6], we described an $\mathbb{F}_q$-basis $\mathcal{B}_m(1,1)$ for the ring of invariants under the Borel subgroup consisting of the following 2 families:

(i) $x_1^{q^m-1}x_2^{i(q-1)}$, $i \leq [m]_q$,

(ii) $Q_{1,0}^{i_1}Q_{2,1}^{i_2}$, $i_1 < [m]_q$, $i_2 \leq [m-1]_q$.

It is a standard fact about the relative transfer $\mathrm{Tr}\colon \mathcal{Q}_m(2)^B \to \mathcal{Q}_m(2)^G$ that it is onto since the index of B in G is relatively prime to p (see [14, Section 2.2]), so a generating set for $\mathcal{Q}_m(2)^G$ can be obtained from the image of Tr.

In what follows, we adopt Goyal's notation y_s for $\delta_2(Q_{1,0}^s)$ for the sake of brevity. By direct inspection, we have the following identity in $\mathcal{Q}_m(2)$ for any $0 \leq s < [m]_q$:

$$x_1^{q^m-1}x_2^{s(q-1)} = y_0 x_1^{(s+1)(q-1)} - y_{s+1}.$$

Since y_s is already a G_2-invariant, this formula allows us to compute the transfer of the first family:

$$\mathrm{Tr}(x_1^{q^m-1}x_2^{s(q-1)}) = y_0\,\mathrm{Tr}(x_1^{(s+1)(q-1)}) - y_{s+1}.$$

Note that $\mathrm{Tr}(x_1^{(s+1)(q-1)})$ is a Dickson polynomial divisible by $Q_{2,0}$ because $x_1^{(s+1)(q-1)}$ is a genuine B-invariant which vanishes when setting $x_1 = 0$. By the first two parts of Proposition 2.7, the product of y_0 with $Q_{2,0}$ is trivial in $\mathcal{Q}_m(2)$. Thus

$$\mathrm{Tr}(x_1^{q^m-1}x_2^{s(q-1)}) = -y_{s+1}.$$

For the second family, we argue similarly, noting that

$$\mathrm{Tr}(Q_{1,0}^{i_1}Q_{2,1}^{i_2}) = \mathrm{Tr}(Q_{1,0}^{i_1})Q_{2,1}^{i_2} \in \mathcal{D}_2.$$

The lemma follows. □

The next step is to show that one only needs part of the Dickson algebra. The following observation about the Dickson monomials $Q_{2,1}^{\frac{q^{m-1}-q^i}{q-1}} Q_{2,0}^{\frac{q^i-1}{q-1}}$ at the "edge" of Δ_2^m is crucial.

Proposition 4.2. *For each $0 \leq i \leq m-1$, we have the following decomposition in S:*

$$Q_{2,1}^{\frac{q^{m-1}-q^i}{q-1}} Q_{2,0}^{\frac{q^i-1}{q-1}} = \delta_2(Q_{1,0}^{\frac{q^i-1}{q-1}}) + \text{essential monomials divisible by } Q_{2,0}^{\frac{q^{i+1}-1}{q-1}}.$$

Proof. It is easy to see, by determinant manipulation, that $\delta_2(Q_{1,0}^{\frac{q^i-1}{q-1}}) = y_{\frac{q^i-1}{q-1}}$ is a genuine Dickson polynomial. When $i = 0$, the Dickson monomial y_0 must contain $Q_{2,1}^{\frac{q^{m-1}-1}{q-1}}$ as a nontrivial summand since both are reduced to $x_1^{q^m-q}$ when setting $x_2 = 0$. Furthermore, $y_0 - Q_{2,1}^{\frac{q^{m-1}-1}{q-1}}$ is divisible by $Q_{2,0}$. Note that in degree $q^m - q$, $Q_{2,1}^{\frac{q^{m-1}-1}{q-1}}$ is the only non-essential Dickson monomial. We have proved that

$$y_0 = Q_{2,1}^{\frac{q^{m-1}-1}{q-1}} + \text{essential monomials divisible by } Q_{2,0}.$$

For the general case, we make use of the identity $y_{m,\frac{q^i-1}{q-1}} = Q_{2,0}^{\frac{q^i-1}{q-1}} y_{m-i,0}^{q^i}$ where $y_{m,s}$ stands for $\delta_{2;m}(Q_{1,0}^s)$. It follows that

$$y_{\frac{q^i-1}{q-1}} = Q_{2,1}^{\frac{q^{m-1}-q^i}{q-1}} Q_{2,0}^{\frac{q^i-1}{q-1}} + (fQ_{2,0})^{q^i} Q_{2,0}^{\frac{q^i-1}{q-1}},$$

for some Dickson polynomial f. A Dickson monomial appearing in the second term of the sum above has the form $Q_{2,1}^{i_1} Q_{2,0}^{i_2}$ where $i_2 \geq \frac{q^{i+1}-1}{q-1}$. Comparing the degree, we have $i_1 \leq \frac{q^{m-1}-q^{i+1}}{q-1}$, hence $Q_{2,1}^{i_1} Q_{2,0}^{i_2}$ is essential. $\quad\square$

Remark 4.3. It is easy to check that if $i > [m-1]_q$, then $Q_{2,0}^i = L_2^{i(q-1)\geq q^{m-1}} = 0$ in $\mathcal{Q}_m(2)$. Also, by induction on m, we have another interesting formula:

$$Q_{2,1}^{\frac{2(q^{m-1}-1)}{q-1}} = y_{\frac{q^m-q}{q-1}} = x_1^{q^m-q} x_2^{q^m-q} \quad \text{in } \mathcal{Q}_m(2).$$

We are now ready to finish the proof of Proposition 1.6.

Consider a Dickson monomial $Q_{2,1}^{i_1} Q_{2,0}^{i_2}$ and suppose, by way of contradiction, that it is not in the span of $\mathcal{B}_m(2)$. Further, assume that it is the smallest monomial in grevlex order with this property. Since $Q_{2,0}^k = 0$ if $k > [m-1]_q$, we must have $i_2 \leq \frac{q^{m-1}-1}{q-1} = [m-1]_q$. Let $i \leq m-1$ be the unique integer such that $[i]_q \leq i_2 < [i+1]_q$. Then $i_1 \geq \frac{q^{m-1}-q^i}{q-1}$. It follows from Proposition 4.2 that

$$Q_{2,1}^{i_1} Q_{2,0}^{i_2} - Q_{2,1}^{i_1 - \frac{q^{m-1}-q^i}{q-1}} Q_{2,0}^{i_2 - \frac{q^i-1}{q-1}} y_{\frac{q^i-1}{q-1}}$$

is a sum of Dickson monomials in strictly smaller grevlex order than (i_1, i_2), and at least one of them is again not in the span of $\mathcal{B}_m(2)$. We have a contradiction.

5. Proof of Proposition 1.7

It is straightforward to check that all elements in the six families listed in Proposition 1.7 are $P(2,1)$-invariants. By results in Section 3, it suffices to show that $\mathcal{B}_m(2,1)$ is a generating set for $\mathcal{Q}_m(3)^{P(2,1)}$.

Suppose f is a nonzero polynomial in $\mathcal{Q}_m(3)^{P(2,1)}$, and we write f as a polynomial in x_3:

$$f = x_3^{a(q-1)} f_a + x_3^{(a-1)(q-1)} f_{a-1} + \dots .$$

We will prove by downward induction on the highest x_3-degree $a(q-1)$.

Observe that the coefficients f_i belong to the space of invariants $\mathcal{Q}_m(2)^G$ in the variables x_1 and x_2. If f_a is a scalar multiple of $x_1^{q^{m-1}} x_2^{q^{m-1}}$, then since $x_3^{a(q-1)} x_1^{q^{m-1}} x_2^{q^{m-1}}$

is already $P(2,1)$-invariant (which is a member of the 5th and 6th family in $\mathcal{B}_m(2,1)$), we can subtract it from f to obtain a new one with strictly smaller x_3-degree.

Now let us assume that f_a, and hence all f_i, for degree reasons, are generated by $\delta_2(\Delta_1^m)$ and Δ_2^m. In particular, its x_1-degree (and hence x_2-degree as well, by symmetry) is strictly less than $q^m - 1$. We claim that a must be a multiple of q. Indeed, since f is a B-invariant, from the list of generators given in 2.5, we see that f must be a linear combination of polynomials of the form $x_1^{j_1(q-1)}\delta_2(Q_{2,1}^{j_2})$ or $x_1^{j_1(q-1)}Q_{2,1}^{j_2}Q_{3,2}^{j_3}$. In both cases, the highest x_3-degrees are divisible by q.

If f_a contains $\delta_2(Q_{1,0}^{i_1})$ for some $i_1 < [m]_q$, then we can subtract from f an appropriate polynomial from the third or fourth family in the list 1.7. So we can assume that $f_a \in \Delta_2^m$. In this case, it follows that $x_3^{a(q-1)}f_a$ is a nontrivial summand of a B-invariant polynomial of the form $x_1^{j_1(q-1)}Q_{2,1}^{j_2}Q_{3,2}^{j_3}$. In particular, a must be divisible by q^2.

Finally, when $a(q-1) = iq^2(q-1)$ for some $i < [m-2]_q$ or $a(q-1) = q^m - q^2$, by subtracting from f an appropriate linear combination of the first two families of $\mathcal{B}_m(2,1)$, we will obtain a $P(2,1)$-invariant polynomial of strictly smaller x_3-degree. The result follows by induction on the highest x_3-degree. $\quad\square$

Remark 5.1. We can also prove that $\mathcal{B}_m(2,1)$ is linearly independent as follows. Consider these elements of $\mathcal{B}_m(2,1)$ as polynomials in x_3. The table below records the coefficient of the highest x_3-degree.

$\mathcal{B}_m(2,1)$	Highest x_3-degree	Coefficient
(1) $Q_{2,1}^{i_1}Q_{2,0}^{i_2}Q_{3,2}^{i}$	$i(q^3-q^2) < q^m-q^2$	$Q_{2,1}^{i_1}Q_{2,0}^{i_2}, (i_1,i_2) \in \Delta_2^m$
(2) $Q_{2,1}^{i_1}Q_{2,0}^{i_2}\delta_3(1)$	q^m-q^2	$Q_{2,1}^{i_1}Q_{2,0}^{i_2}, (i_1,i_2) \in \Delta_2^m$
(3) $\delta_2(Q_{1,0}^{i_1}Q_{2,1}^{i})$	$i(q^2-q) < q^m-q$	$\delta_2(Q_{1,0}^{i_1}), i_1 < [m]_q$
(4) $\delta_2(Q_{1,0}^{i_1}\delta_2(1))$	q^m-q	$\delta_2(Q_{1,0}^{i_1}), i_1 < [m]_q$
(5) $\delta_1(\delta_1(Q_{1,0}^i))$	$i(q-1) < q^m-1$	$x_1^{q^m-1}x_2^{q^m-1}$
(6) $\delta_1(\delta_1(\delta_1(1)))$	q^m-1	$x_1^{q^m-1}x_2^{q^m-1}$

From the table, it is easy to see that the polynomials in $\mathcal{B}_m(2,1)$ are linearly independent.

6. Proof of Proposition 1.8

It suffices to show that $\mathcal{B}_m(1,2)$ is a generating set, and the proof is by downward induction on the lowest x_1-degree. Write

$$f = x_1^{i(q-1)}g_i(x_2,x_3) + x_1^{(i+1)(q-1)}g_{i+1}(x_2,x_3) + \ldots$$

Note that all coefficient polynomials g_j are G_2-invariant in x_2 and x_3. If $i(q-1) = q^m-1$, then $x_1^{q^m-1}g(x_2,x_3)$ is a linear combination of polynomials from the last three families of $\mathcal{B}_m(1,2)$. We can then subtract from f this polynomial and can now assume that $i(q-1) \le q^m-q$.

Since f is a B-invariant, it is a linear combination of polynomials of the form $x_1^{j_1(q-1)}\delta_2(Q_{2,1}^{j_2})$ or $Q_{1,0}^{j_1}Q_{2,1}^{j_2}Q_{3,2}^{j_3}$. Their lowest x_1-degree summands are $x_1^{j_1(q-1)}x_2^{q^m-q}x_3^{j_2q(q-1)}$ and $x_1^{j_1(q-1)}x_2^{j_2q(q-1)}Q_{2,1}^{qj_3}(x_2,x_3)$ respectively. In both cases, the exponents of x_2 and x_3 in these summands are divisible by $q(q-1)$. So the same is true for $g_i(x_2, x_3)$. Since $g_i \in \mathcal{Q}_m(x_2,x_3)^G$, it must be a q-th power of a polynomial in $\mathcal{Q}_{m-1}(2)$ in the variables x_2, x_3.

On the other hand, the lowest x_1-degree summand of the first three families of $\mathcal{B}_m(1,2)$ are

(1) $x_1^{j_1(q-1)}\big(Q_{2,1}^{i_1}(x_2,x_3)Q_{2,0}^{i_2}(x_2,x_3)\big)^q$, $(i_1, i_2) \in \Delta_2^{m-1}$;
(2) $x_1^{j_1(q-1)}\big(\delta_{2;m-1}(Q_{1,0}^{j_2})\big)^q$, $j_2 < [m-1]_q$;
(3) $x_1^{j_1(q-1)}\big(x_2^{q^{m-1}-1}x_3^{q^{m-1}-1}\big)^q$.

Hence $x_1^{i(q-1)}g_i(x_2,x_3)$ is the lowest x_1-degree part of a polynomial in the span of $\mathcal{B}_m(1,2)$. By subtracting from f an appropriate linear combination of polynomials in $\mathcal{B}_m(1,2)$, we obtain another $P(1,2)$-invariant polynomial whose lowest x_1-degree is strictly greater than that of f. By induction, the required result follows. $\square$

Remark 6.1. We can also prove directly that $\mathcal{B}_m(1,2)$ is linearly independent. In fact, the generators can be distinguished by looking at the lowest x_1-degrees and the corresponding coefficients as given in the table below.

$\mathcal{B}_m(1,2)$	Lowest x_1-degree	Coefficient
(1) $Q_{1,0}^{j_1}Q_{3,2}^{i_1}Q_{3,1}^{i_2}$	$j_1(q-1) < q^m - 1$	$Q_{2,1}^{qi_1}(x_2,x_3)Q_{2,0}^{qi_2}(x_2,x_3)$, $(i_1, i_2) \in \Delta_2^{m-1}$
(2) $Q_{1,0}^{j_1}\delta_3(Q_{2,1}^{j_2})$	$j_1(q-1) < q^m - 1$	$y_{m-1,j_2}^q(x_2,x_3)$, $j_2 < [m-1]_q$
(3) $Q_{1,0}^{j_1}\delta_2(\delta_2(1))$	$j_1(q-1) < q^m - 1$	$x_2^{q^m-q}x_3^{q^m-q}$
(4) $\delta_1(Q_{2,1}^{i_1}Q_{2,0}^{i_2})$	$q^m - 1$	$Q_{2,1}^{i_1}(x_2,x_3)Q_{2,0}^{i_2}(x_2,x_3)$, $(i_1, i_2) \in \Delta_2^m$
(5) $\delta_1(\delta_2(Q_{1,0}^{j_1}))$	$q^m - 1$	$y_{j_1}(x_2,x_3)$, $j_1 < [m]_q$
(6) $\delta_1(\delta_1(\delta_1(1)))$	$q^m - 1$	$x_2^{q^m-1}x_3^{q^{m-1}}$

7. Proof of Proposition 1.9

We need to prove that $\mathcal{B}_m(3)$ is a generating set for $\mathcal{Q}_m(3)^G$. Our strategy is the same as in the rank 2 case, but the details are much more involved. The proof is divided into three steps. Using the transfer, we first construct a slightly bigger generating set $\mathcal{B}'$ of the required form without restricting the Dickson polynomials:

$$\mathcal{B}' = \delta_1^3(\Delta_0^m)\coprod\delta_2^2(\Delta_1^m)\coprod\delta_3(\mathcal{D}_2)\coprod\mathcal{D}_3.$$

Once this is done, we then show that $\delta_3(\mathcal{D}_2)$ is actually contained in the span of

$$\delta_1^3(\Delta_0^m)\coprod\delta_2^2(\Delta_1^m)\coprod\delta_3(\Delta_2^m),$$

and as a result, $\mathcal{D}_2$ can be replaced by the much smaller subset Δ_2^m. Finally, we prove that when restricted to $\mathcal{Q}_m(3)$, the rank 3 Dickson algebra belongs to the subspace spanned by $\mathcal{B}_m(3)$. This is proved by first showing that all the edge monomials of Δ_3^m are in this span. Thus the subspace spanned by $\mathcal{B}_m(3)$ is a $\mathcal{D}_3$-submodule of $\mathcal{Q}_m(3)^G$. Since it contains Δ_3^m, it will contain the entirety of $\mathcal{D}_3$.

Lemma 7.1. *The set $\mathcal{B}'$ consisting of 4 families below is a generating set for $\mathcal{Q}_m(3)^G$.*

(1) $x_1^{q^m-1} x_2^{q^m-1} x_3^{q^m-1}$.
(2) $\delta_2^2(\Delta_1^m) = \{a_{m,3,s}, \ 0 \le s < [m]_q\}$.
(3) $\delta_3(\mathcal{D}_2)$.
(4) $\mathcal{D}_3$.

Proof. A generating set for $\mathcal{Q}_m(3)^G$ can be obtained by taking the image of the relative transfer

$$\mathrm{Tr}_{P(2,1)}^G \colon \mathcal{Q}_m^{P(1,2)} \longrightarrow \mathcal{Q}_m^G$$

from the parabolic subgroup $P(1,2)$ to G, applied to the basis of $\mathcal{Q}_m^{P(1,2)}$ given in Proposition 1.8.

First, observe that $Q_{1,0}^{j_1} Q_{3,2}^{i_1} Q_{3,1}^{i_2}$ is a genuine $P(1,2)$-invariant, and hence its transfer is a genuine G-invariant, i.e., a Dickson polynomial.

Next, consider the second family. Since $\delta_3(Q_{2,1}^{j_2})$ is already a G-invariant in $\mathcal{Q}_m(3)$, we have

$$\mathrm{Tr}_{P(2,1)}^G(Q_{1,0}^{j_1} \delta_3(Q_{2,1}^{j_2})) = (\mathrm{Tr}_{P(2,1)}^G Q_{1,0}^{j_1}) \delta_3(Q_{2,1}^{j_2}).$$

On the other hand, the transfer $\mathrm{Tr}_{P(2,1)}^G(Q_{1,0}^{j_1})$ is a genuine Dickson polynomial divisible by $Q_{3,0}$ unless $j_1 = 0$. Therefore, if j_1 is positive, the whole expression vanishes in $\mathcal{Q}_m(3)$:

$$\mathrm{Tr}_{P(2,1)}^G(Q_{1,0}^{j_1} \delta_3(Q_{2,1}^{j_2})) = 0 \quad \text{in } \mathcal{Q}_m.$$

A similar argument applies to the third family. Since $\delta_2^2(1)$ is already a G-invariant and is annihilated by $Q_{3,0}$, its transfer also vanishes. Hence from the second and third families in $\mathcal{B}_m(1,2)$, only elements $\delta_3(Q_{2,1}^{j_2})$ (for $j_2 < [m-1]_q$) and $\delta_2^2(1)$ contribute nontrivially.

Now we turn to the fourth family. Recall that

$$\delta_1(Q_{2,1}^{i_1} Q_{2,0}^{i_2}) = x_1^{q^m-1} Q_{2,1}^{i_1}(x_2, x_3) Q_{2,0}^{i_2}(x_2, x_3).$$

We claim that

$$\mathrm{Tr}_{P(1,2)}^G(\delta_1(Q_{2,1}^{i_1} Q_{2,0}^{i_2})) = \delta_3(Q_{2,1}^{i_1} Q_{2,0}^{i_2+1}).$$

Indeed, by Proposition 2.3, the right-hand side is G-invariant. Moreover, we use the identity:

$$V_3(x_2, x_1, x_3) = V_2(V_2(x_2, x_1), V_2(x_2, x_3)) = V_2(x_2, x_3)^q - V_2^{q-1}(x_2, x_1)V_2(x_2, x_3),$$

from which it follows that

$$L_2^q(x_2, x_3) = x_2^q V_2(x_2, x_3)^q = x_2^q V_3(x_2, x_1, x_3) + Q_{2,0}(x_1, x_2)L_2(x_2, x_3).$$

Applying the Laplace expansion along the last row of the numerator, we obtain:

$$\delta_3(Q_{2,1}^{i_1} Q_{2,0}^{i_2+1}) = Q_{2,0}\delta_3(Q_{2,1}^{i_1} Q_{2,0}^{i_2}) - \delta_2(Q_{1,0}Q_{2,1}^{i_1} Q_{2,0}^{i_2}).$$

Now consider $x_1^{q^m-1} Q_{2,1}^{i_1}(x_2, x_3)Q_{2,0}^{i_2}(x_2, x_3)$ as a B_3-invariant and take the transfer from B_3 to $P(2,1)$. From Section 4, we have

$$\mathrm{Tr}_{B_2}^{G_2}(x_1^{q^m-1} x_2^{a(q-1)}) = -y_{a+1}(x_1, x_2) = -\delta_2(Q_{1,0}^{a+1}).$$

Write

$$Q_{2,1}^{i_1}(x_2, x_3)Q_{2,0}^{i_2}(x_2, x_3) = \sum_{(a,b)} \lambda(a,b)x_2^{a(q-1)}x_3^{b(q-1)}, \quad \lambda(a,b) \in \mathbb{F}_q,$$

then

$$\begin{aligned}
\mathrm{Tr}_{B_3}^{P(2,1)}\left(x_1^{q^m-1} Q_{2,1}^{i_1}(x_2, x_3)Q_{2,0}^{i_2}(x_2, x_3)\right) &= -\sum_{(a,b)} \lambda(a,b)\delta_2(Q_{1,0}^{a+1})x_3^{b(q-1)} \\
&= -\delta_2\Big(\sum_{(a,b)} \lambda(a,b)x_1^{(a+1)(q-1)}x_2^{b(q-1)}\Big) \\
&= -\delta_2(Q_{1,0}Q_{2,1}^{i_1} Q_{2,0}^{i_2}) \\
&= \delta_3(Q_{2,1}^{i_1} Q_{2,0}^{i_2+1}) - Q_{2,0}\delta_3(Q_{2,1}^{i_1} Q_{2,0}^{i_2}).
\end{aligned}$$

Finally, we observe that

$$\mathrm{Tr}_{P(2,1)}^G\left(Q_{2,0}\delta_3(Q_{2,1}^{i_1} Q_{2,0}^{i_2})\right) = \mathrm{Tr}_{P(2,1)}^G(Q_{2,0})\delta_3(Q_{2,1}^{i_1} Q_{2,0}^{i_2}) = 0,$$

which proves the claim for the fourth family.

Now we consider the fifth family (note that the 6th family already consists of G-invariants). A similar argument shows that if $j < [m]_q$, then

$$\mathrm{Tr}_{P(1,2)}^G(x_1^{q^m-1}\delta_2(Q_{1,0}^j)(x_2, x_3)) = -\delta_2^2(Q_{1,0}^{j+1}).$$

Indeed, recall

$$\mathrm{Tr}_{B_3}^{P(2,1)}(x_1^{q^m-1}y_j(x_2,x_3)) = -\sum_{a=j}^{(q^m-q)/(q-1)} y_{a+1}(x_1,x_2)x_3^{q^m-q+j(a-1)-a(q-1)}.$$

This sum is exactly $-a_{m,3,j+1} = -\delta_2^2(Q_{1,0}^{j+1})$, which is a G_3-invariant. The result follows by the transitivity of the transfer. The proof is complete. $\square$

The next step is to show that in the third family, one does not need to use all $\mathcal{D}_2$. The following technical lemma will be used repeatedly.

Lemma 7.2. *Let s, t, i be non-negative integers. Then the following equality holds in $\mathcal{Q}_m(3)$:*

$$\delta_2\left(V_1^{s(q-1)}V_2^{t(q-1)}\delta_2(Q_{1,0}^i)\right)$$

$$= \begin{cases} 0 & \text{if } t \geq 1 \text{ and } s > 1; \\ x_1^{q^m-1}x_2^{q^m-1}x_3^{(qt+i-1)(q-1)} & \text{if } t \geq 1 \text{ and } s = 1; \\ (t+1)x_1^{q^m-1}x_2^{q^m-1}x_3^{(qt+i-2)(q-1)} & \text{if } t \geq 1 \text{ and } s = 0; \\ \delta_2^2(Q_{1,0}^{i+s}) & \text{if } t = 0, s \leq 1; \\ \delta_2^2(Q_{1,0}^{i+s}) - x_1^{q^m-1}x_2^{q^m-1}x_3^{(s+i-2)(q-1)} & \text{if } t = 0, s \geq 2. \end{cases}$$

Proof. Recall that $\delta_2(f)$ is a polynomial if f is a polynomial (possibly with more than one variable), which is G_1-invariant. Hence, the expression under consideration is a polynomial. If $t \geq 1$, unravelling the definition, we see that $\delta_2(V_1^{s(q-1)}V_2^{t(q-1)}\delta_2(Q_{1,0}^i))$ equals

$$\frac{1}{L_2(x_1,x_2)}\left[x_2^{q^m}x_1^{s(q-1)}V_2^{t(q-1)-1}(x_1,x_3)\begin{vmatrix} x_1 & x_3 \\ x_1^{q^m}x_3^{i(q-1)} & x_3^{q^m}x_1^{i(q-1)} \end{vmatrix} - \right.$$

$$\left. x_1^{q^m}x_2^{s(q-1)}V_2^{t(q-1)-1}(x_2,x_3)\begin{vmatrix} x_2 & x_3 \\ x_2^{q^m}x_3^{i(q-1)} & x_3^{q^m}x_2^{i(q-1)} \end{vmatrix}\right]$$

$$= x_3^{q^m}\frac{x_2^{q^m}x_1^{(s+i)(q-1)+1}V_2^{t(q-1)-1}(x_1,x_3) - x_1^{q^m}x_2^{(s+i)(q-1)+1}V_2^{t(q-1)-1}(x_2,x_3)}{L_2(x_1,x_2)} -$$

$$x_1^{q^m}x_2^{q^m}x_3^{i(q-1)+1}\frac{x_1^{s(q-1)}V_2^{t(q-1)-1}(x_1,x_3) - x_2^{s(q-1)}V_2^{t(q-1)-1}(x_2,x_3)}{L_2(x_1,x_2)}.$$

The first summand is trivial in $\mathcal{Q}_m(3)$ because the quotient involved is a polynomial. Indeed, in this quotient, the numerator is divisible by x_1 and vanishes whenever there is a linear relation $x_2 = a_1 x_1$.

By a similar argument, the second summand is also trivial if $s > 1$, and equals $x_1^{q^m-1}x_2^{q^m-1}x_3^{(qt+i-1)(q-1)}$ if $s = 1$. If $s = 0$, it equals

$$(t(q-1)-1)x_1^{q^m-1}x_2^{q^m-1}x_3^{(qt+i-2)(q-1)}.$$

Now suppose $t = 0$, we get

$$\frac{1}{L_2(x_1, x_2)} \Big[x_1^{q^m} x_2^{s(q-1)} \frac{\begin{vmatrix} x_2 & x_3 \\ x_2^{q^m} x_3^{i(q-1)} & x_3^{q^m} x_2^{i(q-1)} \end{vmatrix}}{V_2(x_2, x_3)}$$

$$- x_2^{q^m} x_1^{s(q-1)} \frac{\begin{vmatrix} x_1 & x_3 \\ x_1^{q^m} x_3^{i(q-1)} & x_3^{q^m} x_1^{i(q-1)} \end{vmatrix}}{V_2(x_1, x_3)} \Big]$$

$$= \frac{1}{L_2(x_1, x_2)} \Big[x_1^{q^m} x_2 \frac{\begin{vmatrix} x_2 & x_3 \\ x_2^{q^m} x_3^{(s+i)(q-1)} & x_3^{q^m} x_2^{(s+i)(q-1)} \end{vmatrix}}{L_2(x_2, x_3)}$$

$$- x_2^{q^m} x_1 \frac{\begin{vmatrix} x_1 & x_3 \\ x_1^{q^m} x_3^{(s+i)(q-1)} & x_3^{q^m} x_1^{(s+i)(q-1)} \end{vmatrix}}{L_2(x_1, x_3)} \Big] +$$

$$\frac{x_1^{q^m} x_2^{q^m} x_3^{i(q-1)}}{L_2(x_1, x_2)} \left[\frac{x_2^{s(q-1)} - x_3^{s(q-1)}}{x_2^{q-1} - x_3^{q-1}} - \frac{x_1^{s(q-1)} - x_3^{s(q-1)}}{x_1^{q-1} - x_3^{q-1}} \right].$$

The first summand is $\delta_2^2(Q_{1,0}^{s+i})$. The second summand is trivial when $s \leq 1$ and equals $-x_1^{q^m-1} x_2^{q^m-1} x_3^{(s-2+i)(q-1)}$ if $s \geq 2$. $\quad\square$

Corollary 7.3. *If $g \in \mathcal{D}_2$ and $i \geq 0$, then $\delta_3(g\delta_2(Q_{1,0}^i))$ is a linear combination of polynomials from the following families:*

- $\delta_2^2(Q_{1,0}^s)$, $0 \leq s < [m]_q$.
- $x_1^{q^m-1} x_2^{q^m-1} x_3^{s(q-1)}$, $0 \leq s \leq [m]_q$.

Proof. We first observe that by direct inspection, $\delta_3(g\delta_2(Q_{1,0}^i))$ can be written as a quotient of determinants:

$$\delta_3(g\delta_2(Q_{1,0}^i)) = \frac{\begin{vmatrix} x_1^{i(q-1)+1} & x_2^{i(q-1)+1} & x_3^{i(q-1)+1} \\ x_1^{q^m} & x_2^{q^m} & x_3^{q^m} \\ x_1^{q^m} g(x_2, x_3) & x_2^{q^m} g(x_1, x_3) & x_3^{q^m} g(x_1, x_2) \end{vmatrix}}{L_3(x_1, x_2, x_3)}.$$

Since

$$L_3(x_1, x_2, x_3) = V_3(x_1, x_2, x_3) L_2(x_1, x_2)$$
$$= [V_2(x_2, x_3)^{q-1} - V_2(x_2, x_1)^{q-1}] V_2(x_2, x_3) L_2(x_1, x_2)$$
$$= [V_2(x_1, x_3)^{q-1} - V_2(x_1, x_2)^{q-1}] V_2(x_1, x_3) L_2(x_1, x_2),$$

the quotient above can be rewritten in the form:

$$\varphi(h) := \frac{1}{L_2(x_1, x_2)} \left[x_1^{q^m} x_2 h(x_1, x_2, x_3) \frac{\begin{vmatrix} x_2^{i(q-1)+1} & x_3^{i(q-1)+1} \\ x_2^{q^m} & x_3^{q^m} \end{vmatrix}}{L_2(x_2, x_3)} \right.$$

$$\left. - x_2^{q^m} x_1 h(x_2, x_1, x_3) \frac{\begin{vmatrix} x_1^{i(q-1)+1} & x_3^{i(q-1)+1} \\ x_1^{q^m} & x_3^{q^m} \end{vmatrix}}{L_2(x_1, x_3)} \right]$$

$$= \frac{1}{L_2(x_1, x_2)} (x_1^{q^m} x_2 h(x_1, x_2, x_3) \delta_2(Q_{1,0}^i)(x_2, x_3) - x_2^{q^m} x_1 h(x_2, x_1, x_3) \delta_2(Q_{1,0}^i)(x_1, x_3)),$$

where

$$h(x_1, x_2, x_3) = \frac{g(x_2, x_3) - g(x_2, x_1)}{V_2(x_2, x_3)^{q-1} - V_2(x_2, x_1)^{q-1}}.$$

Since $g \in \mathcal{D}_2$, it can be written in terms of upper triangular invariants

$$g = \sum_{s,t} V_1^{s(q-1)} V_2^{t(q-1)},$$

where the sum is taken over certain subset $A \subset \mathbb{N}^2$. Then

$$h(x_1, x_2, x_3) = \sum_{(s,t) \in A, t \geq 1} x_2^{s(q-1)} \left(\sum_{j=0}^{t-1} V_2(x_2, x_3)^{(t-1-j)(q-1)} V_2(x_2, x_1)^{j(q-1)} \right).$$

Observe that if $j > 0$, then both $x_1^{q^m} x_2 V_2(x_2, x_1)^{j(q-1)}/L_2$ and $x_2^{q^m} x_1 V_2(x_1, x_2)^{j(q-1)}/L_2$ are zero in $\mathcal{Q}_m$, so the terms in h corresponding to those j do not contribute to $\varphi(h)$. It follows that $\varphi(h)$ is reduced to the sum

$$\sum_{(s,t) \in A, t \geq 1} \varphi(x_2^{s(q-1)} V_2(x_2, x_3)^{(t-1)(q-1)}).$$

On the other hand, we have an equality which is essentially by definition:

$$\varphi(x_2^{s(q-1)} V_2(x_2, x_3)^{(t-1)(q-1)}) = \delta_2(V_1^{s(q-1)} V_2^{(t-1)(q-1)} \delta_2(Q_{1,0}^i)).$$

We can now use the computation in Lemma 7.2 of the right-hand side to finish the proof. $\square$

We are now ready to replace $\mathcal{D}_2$ by Δ_2^m in the generating set $\mathcal{B}'$ of $\mathcal{Q}_m(3)^G$.

Lemma 7.4. *The subspace of $\mathcal{Q}_m(3)^G$ spanned by the following three families of elements*

(1) $\delta_1^3(\Delta_0^m)$,
(2) $\delta_2^2(\Delta_1^m)$,
(3) $\delta_3(\Delta_2^m)$,

contains $\delta_3(\mathcal{D}_2)$.

Proof. Suppose f is a Dickson monomial in $\mathcal{D}_2$ but is not essential. Then it can be written in the form

$$Q_{2,1}^{\frac{q^{m-1}-q^i}{q-1}} Q_{2,0}^{\frac{q^i-1}{q-1}} Q_{2,1}^a Q_{2,0}^b,$$

for some $0 \le i \le m-1$, $0 \le a, b$. Recall from 4.2 that

$$Q_{2,1}^{\frac{q^{m-1}-q^i}{q-1}} Q_{2,0}^{\frac{q^i-1}{q-1}} = \delta_2(Q_{1,0}^{\frac{q^i-1}{q-1}}) + \text{essential monomials divisible by } Q_{2,0}^{\frac{q^{i+1}-1}{q-1}}.$$

Repeating this process if necessary, we can write f as a sum of essential monomials and Dickson polynomials of the form

$$\delta_2(Q_{1,0}^{\frac{q^j-1}{q-1}}) Q_{2,1}^{a_j} Q_{2,0}^{b_j}, \quad j \ge i.$$

Thus it suffices to consider $\delta_3(f)$ for $f = g\delta_2(Q_{1,0}^{\frac{q^i-1}{q-1}})$, where $g \in \mathcal{D}_2$ and $0 \le i \le m-1$.

We know from Corollary 7.3 that $\delta_3(g\delta_2(Q_{1,0}^{\frac{q^i-1}{q-1}}))$ is a linear combination of polynomials in the following families:

- $\delta_2^2(\Delta_1^m)$,
- $x_1^{q^m-1} x_2^{q^m-1} x_3^{s(q-1)}, \ 0 \le s \le [m]_q$.

Since $\delta_2(Q_{1,0}^{\frac{q^i-1}{q-1}})$ is a genuine Dickson polynomial, $\delta_3(g\delta_2(Q_{1,0}^{\frac{q^i-1}{q-1}}))$ is a G_3-invariant in $\mathcal{Q}_m(3)$. We conclude that $\delta_3(g\delta_2(Q_{1,0}^{\frac{q^i-1}{q-1}}))$ must belong to the space

$$\text{Span}\{\delta_2^2(\Delta_1^m), \delta_1^3(1)\},$$

because any monomial of the form $x_1^{q^m-1} x_2^{q^m-1} x_3^{i(q-1)}$, $0 \le i < [m]_q$, is not G_3-invariant in $\mathcal{Q}_m(3)$. $\quad\square$

The third, and final step is to replace the full Dickson algebra $\mathcal{D}_3$ by Δ_3^m. We first need some preliminary calculations. In the following, δ_3 will again stand for $\delta_{3;m}$.

Lemma 7.5. *The following equalities hold in S:*

(1) $\delta_3(Q_{2,0}^{\frac{q^i-1}{q-1}}) = \left(\delta_{3;m-i}(1)\right)^{q^i} Q_{3,0}^{\frac{q^i-1}{q-1}}$ *for all $i \ge 0$. In particular,*

$$\delta_3(Q_{2,0}^{\frac{q^{m-2}-1}{q-1}}) = Q_{3,0}^{\frac{q^{m-2}-1}{q-1}} \quad \text{and} \quad \delta_3(Q_{2,0}^{\frac{q^{m-3}-1}{q-1}}) = Q_{3,2}^{q^{m-3}} Q_{3,0}^{\frac{q^{m-3}-1}{q-1}}.$$

(2) $Q_{3,0}^k = 0$ in $\mathcal{Q}_m$ for all $k > \frac{q^{m-2}-1}{q-1}$.

(3) $\delta_3(Q_{2,1}^{q^{m-3}} Q_{2,0}^{\frac{q^{m-3}-1}{q-1}}) = Q_{3,1}^{q^{m-3}} Q_{3,0}^{\frac{q^{m-3}-1}{q-1}}$.

(4) In general, for $\lambda_2 \geq \lambda_3 \geq 0$, then

$$\delta_3\big(Q_{2,1}^{\frac{q^{\lambda_2}-q^{\lambda_3}}{q-1}} Q_{2,0}^{\frac{q^{\lambda_3}-1}{q-1}}\big) = \Big(\delta_{3;m-\lambda_3}\big(Q_{2,1}^{\frac{q^{\lambda_2-\lambda_3}-1}{q-1}}\big)\Big)^{q^{\lambda_3}} Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}}.$$

Proof. The proofs of these statements are quite similar and essentially make use of the Laplace expansion. We will prove the last statement only. Apply the Laplace expansion along the last row of the determinant in the numerator of $\delta_3\big(Q_{2,1}^{\frac{q^{\lambda_2}-q^{\lambda_3}}{q-1}} Q_{2,0}^{\frac{q^{\lambda_3}-1}{q-1}}\big)$, we obtain

$$x_1^{q^m} Q_{2,1}^{\frac{q^{\lambda_2}-q^{\lambda_3}}{q-1}}(x_2,x_3) L_2^{q^{\lambda_3}}(x_2,x_3)$$

$$- x_2^{q^m} Q_{2,1}^{\frac{q^{\lambda_2}-q^{\lambda_3}}{q-1}}(x_1,x_3) L_2^{q^{\lambda_3}}(x_1,x_3)$$

$$+ x_3^{q^m} Q_{2,1}^{\frac{q^{\lambda_2}-q^{\lambda_3}}{q-1}}(x_1,x_2) L_2^{q^{\lambda_3}}(x_1,x_3).$$

After writing this expression as a q^{λ_3} power, the result follows easily. □

Our second technical result is similar to Proposition 4.2 in the case of 3 variables.

Proposition 7.6. Let $m \geq 2$ be an integer.

(i) The following equality holds in S:

$$\frac{[0,1,m-1]}{[0,1,2]} \delta_{3;m}(Q_{2,1}) - \frac{[0,2,m-1]}{[0,1,2]} \delta_{3;m}(1) = Q_{3,1}^{\frac{q^{m-2}-1}{q-1}} + \text{other terms},$$

where the other terms are in the ideal $(Q_{3,0})$ of $\mathcal{D}_3$ generated by $Q_{3,0}$.

(ii) For $0 \leq \ell \leq m-2$, the following equality holds in S:

$$\frac{[0,1,\ell+1]}{[0,1,2]} \delta_{3;m}(Q_{2,1}) - \frac{[0,2,\ell+1]}{[0,1,2]} \delta_{3;m}(1) = Q_{3,2}^{\frac{q^{m-2}-q^\ell}{q-1}} Q_{3,1}^{\frac{q^\ell-1}{q-1}} + \text{other terms},$$

where the other terms are in the ideal $(Q_{3,1}^{\frac{q^{\ell+1}-1}{q-1}}, Q_{3,0})$ of $\mathcal{D}_3$.

Proof. The key observation is that if two Dickson polynomials coincide after setting one of the variables, say x_3, to zero, then their difference must be a multiple of $Q_{3,0}$.

Note that in Dickson's notation, we can write

$$\delta_{3;m}(Q_{2,1}) = \frac{[0,2,m]}{[0,1,2]}, \quad \delta_{3;m}(1) = \frac{[0,1,m]}{[0,1,2]},$$

so that all the terms in the above equations are genuine Dickson polynomials.

Proof of (i): When $x_3 = 0$, the equation under consideration becomes

$$\frac{[1, m-1]}{[1,2]} \cdot \frac{[2, m]}{[1,2]} - \frac{[2, m-1]}{[1,2]} \cdot \frac{[1, m]}{[1,2]} = Q_{2,0}^{\frac{q^{m-1}-q}{q-1}}.$$

It is now a simple computation that the two sides are the same.

Proof of (ii): Again, we consider the reduction of the left-hand side when setting $x_3 = 0$. The result, after simplification, is

$$\delta_{2;m-\ell-1}(1)^{q^{\ell+1}} Q_{2,0}^{\frac{q^{\ell+1}-q}{q-1}}.$$

Now setting $x_2 = 0$, $\delta_{2;m-\ell-1}(1)$ is reduced to $Q_{1,0}^{\frac{q^{m-\ell-1}-q}{q-1}}$, which implies that

$$\delta_{2;m-\ell-1}(1) = Q_{2,1}^{\frac{q^{m-\ell-2}-1}{q-1}} + \text{other terms divisible by } Q_{2,0}.$$

It follows that

$$\delta_{2;m-\ell-1}(1)^{q^{\ell+1}} Q_{2,0}^{\frac{q^{\ell+1}-q}{q-1}} = Q_{2,1}^{\frac{q^{m-1}-q^{\ell+1}}{q-1}} Q_{2,0}^{\frac{q^{\ell+1}-q}{q-1}} + \text{other terms divisible by } Q_{2,0}^{\frac{q^{\ell+2}-q}{q-1}}.$$

Thus, we can conclude that the left-hand side equals

$$Q_{3,2}^{\frac{q^{m-2}-q^{\ell}}{q-1}} Q_{3,1}^{\frac{q^{\ell}-1}{q-1}} + \text{other terms,}$$

where the other terms consist of Dickson monomials which are divisible by $Q_{3,1}^{\frac{q^{\ell+1}-1}{q-1}}$ or by $Q_{3,0}$. $\square$

The following corollary will be useful for induction.

Corollary 7.7. *Suppose $0 \le \ell \le m-2$ and $m-3 \ge \lambda_2 \ge \lambda_3 \ge 0$. The following equalities hold in S:*
(1)

$$\delta_{3;m-\ell-1}(1)^{q^{\ell}} \delta_{3;m}(Q_{2,1}^{q^{\ell}} Q_{2,0}^{\frac{q^{\ell}-1}{q-1}}) - \delta_{3;m-\ell-1}(Q_{2,1})^{q^{\ell}} \delta_{3;m}(Q_{2,0}^{\frac{q^{\ell}-1}{q-1}})$$

$$= Q_{3,1}^{\frac{q^{m-2}-q^{\ell}}{q-1}} Q_{3,0}^{\frac{q^{\ell}-1}{q-1}} + \text{other terms,}$$

where the other terms are in the ideal $(Q_{3,0}^{\frac{q^{\ell+1}-1}{q-1}})$.

(2) *More generally,*

$$\delta_{3;\lambda_2-\lambda_3+1}(1)^{q^{\lambda_3}}\delta_{3;m}(Q_{2,1}^{q^{\lambda_3}}Q_{2,0}^{\frac{q^{\lambda_3}-1}{q-1}}) - \delta_{3;\lambda_2-\lambda_3+1}(Q_{2,1})^{q^{\lambda_3}}\delta_{3;m}(Q_{2,0}^{\frac{q^{\lambda_3}-1}{q-1}}) =$$

$$Q_{3,2}^{\frac{q^{m-2}-q^{\lambda_2}}{q-1}}Q_{3,1}^{\frac{q^{\lambda_2}-q^{\lambda_3}}{q-1}}Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}} + \text{ other terms,}$$

where the other terms are in the ideal $(Q_{3,0}^{\frac{q^{\lambda_3+1}-1}{q-1}}, Q_{3,1}^{\frac{q^{\lambda_2+1}-q^{\lambda_3}}{q-1}}Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}})$.

Proof. This is just combining Lemma 7.5 and Proposition 7.6.

For the first part, note that

$$\delta_{3;m}(Q_{2,1}^{q^\ell}Q_{2,0}^{\frac{q^\ell-1}{q-1}}) = \delta_{3;m}(Q_{2,1}^{\frac{q^{\ell+1}-q^\ell}{q-1}}Q_{2,0}^{\frac{q^\ell-1}{q-1}}) = \delta_{3;m-\ell}(Q_{2,1})^{q^\ell}Q_{3,0}^{\frac{q^\ell-1}{q-1}},$$

and similarly

$$\delta_{3;m}(Q_{2,0}^{\frac{q^\ell-1}{q-1}}) = \delta_{3;m-\ell}(1)^{q^\ell}Q_{3,0}^{\frac{q^\ell-1}{q-1}}.$$

The left-hand side of the required formula becomes

$$\left(\delta_{3;m-\ell-1}(1)\delta_{3;m-\ell}(Q_{2,1}) - \delta_{3;m-\ell-1}(Q_{2,1})\delta_{3;m-\ell}(1)\right)^{q^\ell}Q_{3,0}^{\frac{q^\ell-1}{q-1}}.$$

We can then apply 7.6 part (i) to finish the proof.

The second part is proved similarly. □

Corollary 7.8. *The Dickson monomials at the edge of* Δ_3^m *listed below are also in the span of* $\mathcal{B}_m(3)$:

(1) $Q_{3,0}^{\frac{q^{m-2}-1}{q-1}}$,

(2) $Q_{3,1}^{\frac{q^{m-2}-q^{\lambda_3}}{q-1}}Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}}$, *where* $m-3 \geq \lambda_3$,

(3) $Q_{3,2}^{\frac{q^{m-2}-q^{\lambda_2}}{q-1}}Q_{3,1}^{\frac{q^{\lambda_2}-q^{\lambda_3}}{q-1}}Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}}$, *where* $m-3 \geq \lambda_2 \geq \lambda_3$.

Proof. We have already seen from part (1) of Lemma 7.5 that the monomial $Q_{3,0}^{\frac{q^{m-2}-1}{q-1}}$ belongs to $\delta_3(\Delta_2^m)$. For the remaining 2 families, we will show that they belong to the span of $\mathcal{B}_m(3)$ by downward induction on λ_3.

When $\lambda_3 = m-3$, it follows that $\lambda_2 = \lambda_3 = m-3$. The edge monomials

$$Q_{3,1}^{q^{m-3}}Q_{3,0}^{\frac{q^{m-3}-1}{q-1}} \quad \text{and} \quad Q_{3,2}^{q^{m-3}}Q_{3,0}^{\frac{q^{m-3}-1}{q-1}}$$

belong to the span of $\mathcal{B}_m(3)$ by parts (1) and (3) of Lemma 7.5. In addition, by Proposition 2.7, any Dickson monomial divisible by these monomials is also in the image of δ_3, and thus belongs to the span of $\mathcal{B}_m(3)$.

Now suppose, as induction hypothesis, that all edge monomials with $Q_{3,0}$-exponent $\frac{q^{\lambda_3+1}-1}{q-1}$ as well as their multiples are already in the span of $\mathcal{B}_m(3)$. We consider the edge monomials corresponding to λ_3:

(1) $Q_{3,1}^{\frac{q^{m-2}-q^{\lambda_3}}{q-1}} Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}}$,

(2) $Q_{3,2}^{\frac{q^{m-2}-q^{\lambda_2}}{q-1}} Q_{3,1}^{\frac{q^{\lambda_2}-q^{\lambda_3}}{q-1}} Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}}$.

Part (i) of Corollary 7.7 shows that $Q_{3,1}^{\frac{q^{m-2}-q^{\lambda_3}}{q-1}} Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}}$ lies in the image of $\delta_3(\Delta_2^m)$ modulo terms with strictly higher λ_3. By the induction hypothesis, these higher terms are already in the span of $\mathcal{B}_m(3)$.

For the second monomial, observe that if there exists a monomial with the same $Q_{3,0}$-exponent $\frac{q^{\lambda_3}-1}{q-1}$ but a higher exponent of $Q_{3,1}$, such that it becomes non-essential, then this monomial must be a multiple of

$$Q_{3,1}^{\frac{q^{m-2}-q^{\lambda_3}}{q-1}} Q_{3,0}^{\frac{q^{\lambda_3}-1}{q-1}},$$

which by the previous step, is already in the span of $\mathcal{B}_m(3)$. Alternatively, if the $Q_{3,0}$-exponent is strictly greater than $\frac{q^{\lambda_3}-1}{q-1}$, the induction hypothesis can be applied directly. $\square$

Now we are ready to finish the proof of the claim that $\mathcal{B}_m(3)$ is a generating set for $\mathcal{Q}_m(3)^G$. Corollary 7.8 shows that the subspace of $\mathcal{Q}_m(3)^G$ spanned by $\mathcal{B}_m(3)$ is closed under the action of the Dickson algebra $\mathcal{D}_3$. Indeed, we have already computed the action of $\mathcal{D}_3$ on $\delta_{s+1}^{3-s}(\Delta_s^m)$ for $0 \le s \le 2$ in 2.7, and the product of $Q_{3,i}$ with a monomial in Δ_3^m is clearly an edge monomial, which is in the span of $\mathcal{B}_m(3)$ by Corollary 7.8. The proof is finished.

8. A filtration of submodules over the Steenrod algebra

In this final section, we investigate the filtration $\mathcal{F}_{n,k}$ of $\mathcal{Q}_m(n)^G$ as defined in the Introduction 1.10. Recall that for each positive integer n, $0 \le k \le \min(m,n)$, $\mathcal{F}_{n,k}$ is the $\mathbb{F}_q$-subspace of $\mathcal{Q}_m(n)^G$:

$$\mathcal{F}_{n,k} = \mathrm{Span}\{\delta_{s+1}^{n-s}(f)\colon f \in \Delta_s^m, 0 \le s \le \min(m,k)\}.$$

The aim of this final section is to demonstrate Theorem 1.12. For $n \le 3$, we have shown that this increasing filtration of subspaces is exhaustive. We begin with the following observation which allows more flexibility in working with $\mathcal{F}_{n,k}$:

Lemma 8.1. *Let $n \leq 3$. For each $0 \leq k \leq \min(m, n)$, we have*

$$\mathcal{F}_{n,k} = \mathrm{Span}\{\delta_{s+1}^{n-s}(f) \colon f \in \mathcal{D}_s, 0 \leq s \leq \min(m, k)\}.$$

The point is that this filtration does not depend on the subspace Δ_s^m.

Proof. For $n = 2$ this is essentially pointed out in Example 2.4 and the proof of Proposition 1.6. For $n = 3$, this is a combination of Example 2.5 and the proof of Proposition 1.9. □

Corollary 8.2. *For $n \leq 3$, $\mathcal{F}_{n,*}$ is a filtration of $\mathcal{D}_n$-submodules of the invariant ring $\mathcal{Q}_m(n)^G$. Moreover, for $0 \leq k < \min(m, n)$, $\mathcal{F}_{n,k}$ is annihilated by $Q_{n,0}, \ldots, Q_{n,n-k-1}$.*

Proof. This is immediate from the above Lemma and Proposition 2.7. □

The calculations in the previous sections demonstrate that our basis $\mathcal{B}_m(3)$ for $\mathcal{Q}_m(3)^G$ is natural in the sense that the resulting filtration is a filtration by $\mathcal{D}_3$-submodules. Moreover, the action of the Dickson algebra follows a pattern similar to the one discussed in [9], where the structure of the cofixed space S_G is described as an S^G-module. A similar pattern also emerges in the case $n = 2$.

We now turn our attention to the Steenrod algebra. For background on the mod q Steenrod algebra $\mathcal{A}$ and its role in modular invariant theory, we refer to Larry Smith's article [13], which provides a purely algebraic treatment of the Steenrod algebra over a general finite field.

Recall that for each $i \geq 0$, the ith Steenrod reduced power operation $\mathcal{P}^i$ is an $\mathbb{F}_q$-linear map satisfying the following conditions:

(1) The unstable condition: $\mathcal{P}^i(f) = f^q$ if $i = \deg(f)$ and $\mathcal{P}^i(f) = 0$ if $i > \deg(f)$.
(2) The Cartan formulae: $\mathcal{P}^i(fg) = \sum_{a+b=i} \mathcal{P}^a(f)\mathcal{P}^b(g)$.

Moreover, $\mathcal{P}^0$ acts as the identity. Over the polynomial ring $S = \mathbb{F}_q[x_1, \ldots, x_n]$, in which each x_i is given degree 1, the action of the Steenrod algebra is completely determined by the unstable condition and the Cartan formulae. More concretely, we have

$$\mathcal{P}^i(v^j) = \binom{j}{i} v^{j+i(q-1)},$$

for any linear polynomial v. Here the binomial coefficient is taken modulo p. Thus, if j is a q-power, then $\mathcal{P}^i(v^j) \neq 0$ iff $i = 0$ (in which case $\mathcal{P}^0$ is the identity operator) or $i = j$ (in which case $\mathcal{P}^i(v^i) = v^{qi}$ is the Frobenius operator). It is convenient to make the convention that $\mathcal{P}^k = 0$ if $k < 0$.

The Steenrod algebra action and the group G action on S commute. Moreover, it is evident that the Frobenius ideal I_m is stable under the action of the Steenrod operations.

Consequently, the quotient $\mathcal{Q}_m = S/I_m$ inherits the structure of an $\mathcal{A}$-module. It follows that each Steenrod reduced power $\mathcal{P}^i$ induces a well-defined endomorphism of $\mathcal{Q}_m^G$. In other words, the subspace of invariants $\mathcal{Q}_m^G$ is closed under the action of the Steenrod algebra, and therefore forms an $\mathcal{A}$-module.

The proof of Theorem 1.12 uses several lemmas. We begin with a general formula describing how the Steenrod operations interact with the delta operator.

Lemma 8.3. *If f is a polynomial which is G_1-invariant in the first variable, then for any $k \geq 0$, the following holds in S:*

$$\mathcal{P}^k(\delta_2 f) + Q_{2,1}\mathcal{P}^{k-q}(\delta_2 f) + Q_{2,0}\mathcal{P}^{k-q-1}(\delta_2 f) =$$
$$\delta_2(Q_{1,0}\mathcal{P}^{k-1}f) + \delta_2(\mathcal{P}^k f) + \delta_{2;m+1}(Q_{1,0}\mathcal{P}^{k-1-q^m}f) + \delta_{2;m+1}(\mathcal{P}^{k-q^m}f).$$

Proof. The condition imposed on f assures that $\delta_2(f)$ as well as the other terms in this lemma are polynomial. The equation above is then obtained by applying the Cartan formula for the product $L_2\delta_2(f)$ and then dividing both sides by L_2. Note that $\mathcal{P}^q L_2 = Q_{2,1}L_2$, $\mathcal{P}^{q+1}L_2 = Q_{2,0}L_2$ and $\mathcal{P}^k L_2 = 0$ for all other $k \geq 1$. $\square$

Corollary 8.4. *$\mathcal{F}_{2,1}$ is a submodule of $\mathcal{Q}_m(2)^G$ over the Steenrod algebra.*

Proof. We must show that for each $0 \leq s < [m]_q$, $\mathcal{P}^k(\delta_2 Q_{1,0}^s) \in \mathcal{F}_{2,1}$ for all $k > 0$. If $k \geq q^m$, the degree of $\mathcal{P}^k(\delta_2 Q_{1,0}^s)$ is at least

$$q^m(q-1) + q^m - q + s(q-1) \geq 2(q^m - 1).$$

So we can assume that $k < q^m$. In this case, when we apply the formula of Lemma 8.3 for $f = Q_{1,0}^a$, the last two summands on the right-hand side vanish. Thus we have an equality in S:

$$\mathcal{P}^k(\delta_2 Q_{1,0}^s) + Q_{2,1}\mathcal{P}^{k-q}(\delta_2 Q_{1,0}^s) + Q_{2,0}\mathcal{P}^{k-q-1}(\delta_2 Q_{1,0}^s)$$
$$= \delta_2(Q_{1,0}\mathcal{P}^{k-1}Q_{1,0}^s) + \delta_2(\mathcal{P}^k Q_{1,0}^s). \tag{8.1}$$

Both summands on the right-hand side are evidently of the form $\delta_2(Q_{1,0}^s)$. Now we can proceed by induction on k using the above formula and the calculation in Proposition 2.7 when working in $\mathcal{Q}_m(2)$. $\square$

Note that $\mathcal{F}_{2,0}$ is spanned by the top class $x_1^{q^m-1}x_2^{q^m-1}$, and $\mathcal{F}_{2,2} = \mathcal{Q}_m(2)^G$. Both are evidently $\mathcal{A}$-submodules of $\mathcal{Q}_m(2)^G$.

Proposition 8.5. *$\mathcal{F}_{3,1}$ is a submodule of $\mathcal{Q}_m(3)^G$ over the Steenrod algebra.*

Proof. We need to show that for each $k \geq 1$ and $0 \leq a < [m]_q$, $\mathcal{P}^k(\delta_2^2 Q_{1,0}^s)$ is in the span of $\delta_1^3(1)$ and $\delta_2^2(\Delta_1^m)$. Note that $\delta_1^3(1)$ spans the one-dimensional space of $\mathcal{Q}_m(3)^G$ in the top degree $3(q^m - 1)$.

First of all, if $k \geq q^m$, then the degree of $\mathcal{P}^k(\delta_2^2 Q_{1,0}^s)$, which is $q^m(q-1) + 2(q^m - q) + s(q-1)$ is at least $3(q^m - 1)$ unless $q = 2$ and $k = 2^m$, $s = 0$. In this range, $\mathcal{Q}_m(3)$ is either spanned by $\delta_3^3(1)$ or zero.

If $q = 2$, $k = 2^m$, $s = 0$, then $\mathcal{P}^{2^m}(\delta_2^2(1))$ is in degree $3(2^m - 1) - 1$. We claim that there is no G-invariant polynomial in this degree. Indeed, the only non-zero symmetric polynomial in this degree is

$$x_1^{2^m - 1} x_2^{2^m - 1} x_3^{2^m - 2} + x_1^{2^m - 1} x_2^{2^m - 2} x_3^{2^m - 1} + x_1^{2^m - 2} x_2^{2^m - 1} x_3^{2^m - 2}.$$

By direct inspection, this polynomial is not invariant under the action of the operation mapping $x_1 \mapsto x_1 + x_2$ and fixes x_2, x_3.

Now let us consider the case $k < q^m$. By Lemma 8.3, we have the following equality in S:

$$\mathcal{P}^k(\delta_2 f) + Q_{2,1}\mathcal{P}^{k-q}(\delta_2 f) + Q_{2,0}\mathcal{P}^{k-q-1}(\delta_2 f) = \delta_2(Q_{1,0}\mathcal{P}^{k-1}f) + \delta_2(\mathcal{P}^k f) \qquad (8.2)$$

for all polynomial f which is GL_1-invariant in the first variable. Applying this for $f = Q_{1,0}^s$, it follows by induction on k that for $0 \leq k < q^m$, $\mathcal{P}^k(\delta_2 Q_{1,0}^s)$ is a linear combination of polynomials of the form

$$Q_{2,1}^a Q_{2,0}^b \delta_2(Q_{1,0}^c).$$

Now applying (8.2) again but for $f = \delta_2(Q_{1,0}^s)$, we get

$$\mathcal{P}^k(\delta_2^2(Q_{1,0}^s)) + Q_{2,1}\mathcal{P}^{k-q}(\delta_2^2(Q_{1,0}^s)) + Q_{2,0}\mathcal{P}^{k-q-1}(\delta_2^2(Q_{1,0}^s))$$
$$= \delta_2(Q_{1,0}\mathcal{P}^{k-1}\delta_2(Q_{1,0}^s)) + \delta_2(\mathcal{P}^k\delta_2(Q_{1,0}^s)). \qquad (8.3)$$

The right-hand side is then a sum of polynomials of the following forms

- $\delta_2(Q_{1,0}Q_{2,1}^a Q_{2,0}^b \delta_2(Q_{1,0}^c))$, or
- $\delta_2(Q_{2,1}^a Q_{2,0}^b \delta_2(Q_{1,0}^c))$.

Up to this point, we have been working in S. Now we consider the situation in $\mathcal{Q}_m(3)$. From Lemma 7.2, we see that this sum belongs to the subspace of $\mathcal{Q}_m(3)$ spanned by polynomials of the forms

- $\delta_2^2(Q_{1,0}^a)$, or
- $x_1^{q^m - 1} x_2^{q^m - 1} x_3^{a(q-1)}$.

Both sides of Equation (8.3) now are $P(2,1)$-invariant. Take the transfer from $P(2,1)$ to G. We have $\mathcal{P}^i(\delta_2^2(Q_{1,0}^s))$ is G-invariant in $\mathcal{Q}_m(3)$ and

$$\text{Tr}_{P(2,1)}^G(Q_{2,1}) = \text{Tr}_{P(2,1)}^G(Q_{2,0}) = \text{Tr}_{P(2,1)}^G(x_1^{q^{m-1}}x_2^{q^{m-1}}x_3^{a(q-1))}) = 0.$$

The first two terms vanish in S for degree reasons: there are no genuine G-invariants in degrees $q^2 - q$ and $q^2 - 1$. The third vanishes in $\mathcal{Q}_m(3)$ because if $x_1^{q^{m-1}}x_2^{q^{m-1}}x_3^{a(q-1)}$ is a nontrivial summand of a G-invariant polynomial in $\mathcal{Q}_m(3)$, then it is a $P(1,2)$-invariant as well, but from Remark 6.1, this can only happen at the top degree.

It follows that $\mathcal{P}^k(\delta_2^2(Q_{1,0}^s))$ must be a scalar multiple of some $\delta_2^2(Q_{1,0}^a)$, and thus belongs to $\mathcal{F}_{3,1}$. $\quad\square$

We now consider the interaction between the Steenrod powers and the operator δ_3.

Lemma 8.6. *If f is a polynomial which is G_2-invariant in the first two variables, then for any $k \geq 0$, the following holds in S:*

$$\mathcal{P}^k(\delta_3 f) + Q_{3,2}\mathcal{P}^{k-q^2}(\delta_3 f) + Q_{3,1}\mathcal{P}^{k-q^2-q}(\delta_3 f) + Q_{3,0}\mathcal{P}^{k-q^2-q-1}(\delta_3 f) =$$

$$\delta_3\left(\mathcal{P}^k(f) + Q_{2,1}\mathcal{P}^{k-q}(f) + Q_{2,0}\mathcal{P}^{k-q-1}(f)\right)$$

$$+ \delta_{3;m+1}\left(\mathcal{P}^{k-q^m}(f) + Q_{2,1}\mathcal{P}^{k-q^m-q}(f) + Q_{2,0}\mathcal{P}^{k-q^m-q-1}(f)\right).$$

Proof. The above equality is again an application of the Cartan formula to $\mathcal{P}^k(L_3\delta_3 f)$, using the formulae for the action of the Steenrod powers on L_2 given in the proof of Lemma 8.3, and similar formulae for these actions on L_3: $\mathcal{P}^{q^2}L_3 = Q_{3,2}L_3$, $\mathcal{P}^{q^2+q}L_3 = Q_{3,1}L_3$, $\mathcal{P}^{q^2+q+1}L_3 = Q_{3,0}L_3$ and $\mathcal{P}^kL_3 = 0$ for all other $k \geq 1$. $\quad\square$

The next lemma discusses how to deal with the last term in the above formula.

Lemma 8.7. *If $h \in \mathcal{D}_2$, then the following holds in $\mathcal{Q}_m$,*

$$\delta_{3;m+1}(h) = \begin{cases} 0 & \text{if } q > 3 \text{ or } q = 3 \text{ and } \deg(h) > 0; \\ \delta_{3;m}(Q_{2,1}^{q^{m-1}}) & \text{if } q = 3 \text{ and } h = 1; \\ \in \text{Span}\{\delta_{2;m}^2(\Delta_1^m), \delta_{1;m}^3(1)\} & \text{if } q = 2. \end{cases}$$

Proof. Recall from the fundamental equation that $X^{q^3} - Q_{3,2}X^{q^2} + Q_{3,1}X^q - Q_{3,0}X = 0$ if X is in the span of x_1, x_2, x_3. It follows that

$$x_i^{q^{m+1}} - Q_{3,2}^{q^{m-2}}x_i^{q^m} + Q_{3,1}^{q^{m-2}}x_i^{q^{m-1}} - Q_{3,0}^{q^{m-2}}x_i^{q^{m-2}} = 0, \quad 1 \leq i \leq 3,$$

and we obtain the following identity in S relating δ_3 for various m:

$$\delta_{3;m+1}(h) - Q_{3,2}^{q^{m-2}}\delta_{3;m}(h) + Q_{3,1}^{q^{m-2}}\delta_{3;m-1}(h) - Q_{3,0}^{q^{m-2}}\delta_{3;m-2}(h) = 0.$$

Note that the degree of $\delta_{3;m+1}(h)$ equals $q^{m+1} - q^2 + \deg(h)$. If $q > 3$, this is strictly greater than $3(q^m - 1)$, and we can conclude immediately that $\delta_{3;m+1}(h) = 0$ in $\mathcal{Q}_m(3)$.

Consider now the case $q = 3$. Observe that, by direct computation, $Q_{3,0} = Q_{3,1} = 0$, $Q_{3,2} = (x_1 x_2 x_3)^{3^2 - 3^1}$ in $\mathcal{Q}_2(3)$. Hence $Q_{3,1}^{q^{m-2}} = Q_{3,0}^{q^{m-2}} = 0$ in $\mathcal{Q}_m(3)$ and the above equation becomes

$$\delta_{3;m+1}(h) = Q_{3,2}^{q^{m-2}}\delta_{3;m}(h) = (x_1 x_2 x_3)^{3^m - 3^{m-1}}\delta_{3;m}(h) \quad \text{in } \mathcal{Q}_m(3). \tag{8.4}$$

On the other hand, for degree reasons, we must have $\deg(h) \leq 3(3^m - 1) - (3^{m+1} - 3^2) = 6$. In this range, there are (up to a scalar) only two Dickson polynomials, namely $h = 1$ or $h = Q_{2,1}$. If $h = 1$, then from Proposition 2.7, we have immediately

$$\delta_{3;m+1}(1) = Q_{3,2}^{3^{m-2}}\delta_{3;m}(1) = \delta_{3;m}(Q_{2,1}^{3^{m-1}}).$$

If $h = Q_{2,1}$, we prove by induction on $m \geq 2$ that

$$\delta_{3;m+1}(Q_{2,1}) = 0 \quad \text{in } \mathcal{Q}_m(3).$$

Indeed, the base case can be checked directly since $\delta_{3;3}(Q_{2,1}) = Q_{3,1}$ in S, and the induction step follows immediately from Equation (8.4).

The next and final case is $q = 2$. Using the identity

$$x_1^{2^{m+1}} = x_1^{2^m}(x_1^{2^m} + x_2^{2^m} + x_3^{2^m}) - x_1^{2^m}(x_2^{2^m} + x_3^{2^m}),$$

and similarly for $x_2^{2^{m+1}}$ and $x_3^{2^{m+1}}$, we see that $\delta_{3;m+1}(h)$ equals in $\mathcal{Q}_m(3)$ to

$$\frac{1}{L_3}\begin{vmatrix} x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \\ x_1^{2^m} h(x_2,x_3)(x_2^{2^m}+x_3^{2^m}) & x_2^{2^m} h(x_1,x_3)(x_1^{2^m}+x_3^{2^m}) & x_3^{2^m} h(x_1,x_2)(x_1^{2^m}+x_2^{2^m}) \end{vmatrix}.$$

It is straightforward to verify the following equality in S:

$$x_1^{2^m} + x_2^{2^m} = Q_{2,1}\delta_{2;m}(1) - \delta_{2;m}(Q_{1,0}^2).$$

We then obtain an equality in $\mathcal{Q}_m(3)$:

$$\delta_{3;m+1}(h) = \delta_{3;m}(Q_{2,1}h\delta_{2;m}(1)) - \delta_{3;m}(h\delta_{2;m}(Q_{1,0}^2)).$$

The conclusion follows from Corollary 7.3. □

Remark 8.8. With a little more work, using 7.2, it can be shown that when $q = 2$, then for $h \in \mathcal{D}_2$, we have the following explicit formula for $\delta_{3;m+1}(h)$ in $\mathcal{Q}_m(3)$:

$$\delta_{3;m+1}(h) = \begin{cases} 0 & \text{if } h \text{ is a multiple of } Q_{2,0}; \\ \delta_{2;m}^2(Q_{1,0}^{2s}) & \text{if } h = Q_{2,1}^s,\ s \geq 0. \end{cases}$$

We leave the details for the interested reader.

Now we can finish the proof of Theorem 1.12. It remains to show that $\mathcal{F}_{3,2}$ is an $\mathcal{A}$-submodule of $\mathcal{Q}_m(3)^G$. From Lemma 8.7, we see that if $f \in \mathcal{D}_2$, then

$$\mathcal{P}^k(\delta_3 f) + Q_{3,2}\mathcal{P}^{k-q^2}(\delta_3 f) + Q_{3,1}\mathcal{P}^{k-q^2-q}(\delta_3 f) + Q_{3,0}\mathcal{P}^{k-q^2-q-1}(\delta_3 f) \in \mathcal{F}_{3,2}.$$

We can proceed by induction. If $\mathcal{P}^i(\delta_3 f) \in \mathcal{F}_{3,2}$ for all $i < k$, then $Q_{3,j}\mathcal{P}^i(\delta_3 f)$ also belongs to $\mathcal{F}_{3,2}$ by Proposition 2.7. It follows that $\mathcal{P}^k(\delta_3 f)$ also belongs to $\mathcal{F}_{3,2}$ and the proof is complete.

Data availability

No data was used for the research described in the article.

References

[1] J. Michael Boardman, Modular representations on the homology of powers of real projective space, in: Algebraic Topology, Oaxtepec, 1991, in: Contemp. Math., vol. 146, Amer. Math. Soc., Providence, RI, 1993, pp. 49–70. MR 1224907.
[2] Taiwang Deng, Torsions in cohomology of $\mathrm{SL}_2(\mathbb{Z})$ and congruence of modular forms, J. Number Theory 246 (2023) 87–156. MR 4531581.
[3] Leonard Eugene Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem, Trans. Am. Math. Soc. 12 (1) (1911) 75–98. MR 1500882.
[4] C. Drescher, A.V. Shepler, Invariants of polynomials mod Frobenius powers, J. Algebra 556 (2020) 908–935. MR 4088444.
[5] Pallav Goyal, Invariant theory of finite general linear groups modulo Frobenius powers, Commun. Algebra 46 (10) (2018) 4511–4529. MR 3847131.
[6] Le Minh Ha, Nguyen Dang Ho Hai, Nguyen Van Nghia, A proof of the Lewis-Reiner-Stanton conjecture for the Borel subgroup, Trans. Am. Math. Soc. (2024).
[7] T.J. Hewett, Modular invariant theory of parabolic subgroups of $\mathrm{GL}_n(\mathbf{F}_q)$ and the associated Steenrod modules, Duke Math. J. 82 (1) (1996) 91–102. MR 1387223.
[8] N.J. Kuhn, The Morava K-theories of some classifying spaces, Trans. Am. Math. Soc. 304 (1) (1987) 193–205. MR 906812.
[9] J. Lewis, V. Reiner, D. Stanton, Invariants of $\mathrm{GL}_n(\mathbb{F}_q)$ in polynomials modulo Frobenius powers, Proc. R. Soc. Edinb., Sect. A 147 (4) (2017) 831–873. MR 3681566.
[10] Huynh Mui, Modular invariant theory and cohomology algebras of symmetric groups, J. Fac. Sci., Univ. Tokyo, Sect. 1A, Math. 22 (3) (1975) 319–369. MR 422451.
[11] V. Reiner, D. Stanton, D. White, The cyclic sieving phenomenon, J. Comb. Theory, Ser. A 108 (1) (2004) 17–50. MR 2087303.
[12] Victor Reiner, Dennis Stanton, (q,t)-analogues and $\mathrm{GL}_n(\mathbb{F}_q)$, J. Algebraic Comb. 31 (3) (2010) 411–454.
[13] Larry Smith, An algebraic introduction to the Steenrod algebra, in: Proceedings of the School and Conference in Algebraic Topology, in: Geom. Topol. Monogr., vol. 11, 2007, pp. 327–348. MR 2402812.
[14] M.D. Neusel, L. Smith, Invariant Theory of Finite Groups, Mathematical Surveys and Monographs, vol. 94, Amer. Math. Soc., Providence, RI, 2002. MR 1869812.
[15] C.W. Wilkerson Jr., A primer on the Dickson invariants, Contemp. Math. 19 (1983) 421–434. MR 0711066.