Proceedings of the Royal Society of Edinburgh, **147A**, 831–873, *2017*
DOI:10.1017/S0308210516000366

Invariants of $\mathbf{GL}_n(\mathbb{F}_q)$ in polynomials modulo Frobenius powers

J. Lewis, **V. Reiner** and **D. Stanton**
School of Mathematics, University of Minnesota,
Minneapolis, MN 55455, USA
(jblewis@math.umn.edu; reiner@math.umn.edu;
stanton@math.umn.edu)

(MS received 15 May 2014; accepted 12 February 2016)

Conjectures are given for Hilbert series related to polynomial invariants of finite general linear groups: one for invariants mod Frobenius powers of the irrelevant ideal and one for cofixed spaces of polynomials.

Keywords: finite general linear group; Frobenius power; Dickson invariants; cofixed; divided power invariants; cyclic sieving

2010 *Mathematics subject classification:* Primary 13A50

1. Introduction

This paper proposes two related conjectures in the invariant theory of $\mathrm{GL}_n(\mathbb{F}_q)$, motivated by the following celebrated result of Dickson [8] (see also [5, theorem 8.1.1] and [30, theorem 8.1.5]).

Theorem 1.1 (Dickson [8]). *When $G := \mathrm{GL}_n(\mathbb{F}_q)$ acts via invertible linear substitutions of variables on the polynomial algebra $S = \mathbb{F}_q[x_1, \dots, x_n]$, the G-invariants form a polynomial subalgebra $S^G = \mathbb{F}_q[D_{n,0}, D_{n,1}, \dots, D_{n,n-1}]$.*

Here the *Dickson polynomials* $D_{n,i}$ are the coefficients in the expansion

$$\prod_{\ell(\boldsymbol{x})} (t + \ell(\boldsymbol{x})) = \sum_{i=0}^{n} D_{n,i} t^{q^i},$$

where the product runs over all $\mathbb{F}_q$-linear forms $\ell(\boldsymbol{x})$ in the variables $x_1, \dots, x_n$. In particular, $D_{n,i}$ is homogeneous of degree $q^n - q^i$, so that Dickson's theorem implies the *Hilbert series* formula:

$$\mathrm{Hilb}(S^G, t) := \sum_{d \geqslant 0} \dim_{\mathbb{F}_q}(S^G)_d t^d = \prod_{i=0}^{n-1} \frac{1}{1 - t^{q^n - q^i}}. \tag{1.1}$$

Our main conjecture gives the Hilbert series for the G-invariants in the quotient ring $Q := S/\mathfrak{m}^{[q^m]}$ by an iterated *Frobenius power* $\mathfrak{m}^{[q^m]} := (x_1^{q^m}, \dots, x_n^{q^m})$ of the *irrelevant ideal* $\mathfrak{m} = (x_1, \dots, x_n)$. The ideal $\mathfrak{m}^{[q^m]}$ is G-stable, and hence the action of G on S descends to an action on the quotient Q.

© 2017 The Royal Society of Edinburgh

Conjecture 1.2. *The G-fixed subalgebra Q^G has Hilbert series*

$$\mathrm{Hilb}((S/\mathfrak{m}^{[q^m]})^G, t) = C_{n,m}(t),$$

where

$$C_{n,m}(t) := \sum_{k=0}^{\min(n,m)} t^{(n-k)(q^m-q^k)} \begin{bmatrix} m \\ k \end{bmatrix}_{q,t}. \tag{1.2}$$

The (q,t)-*binomial* appearing in (1.2) is a polynomial in t, introduced and studied in [25], defined by

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q,t} := \frac{\mathrm{Hilb}(S^{P_k}, t)}{\mathrm{Hilb}(S^G, t)} = \prod_{i=0}^{k-1} \frac{1-t^{q^n-q^i}}{1-t^{q^k-q^i}}. \tag{1.3}$$

Here P_k is a *maximal parabolic subgroup* of G stabilizing $\mathbb{F}_q^k \subset \mathbb{F}_q^n$, so G/P_k is the *Grassmannian* of k-planes.

It will be shown in § 3 that conjecture 1.2 implies the following conjecture on the *G-cofixed space* (also known as the *maximal G-invariant quotient* or the *G-coinvariant space*[1]) of S. This is defined to be the quotient $\mathbb{F}_q$-vector space $S_G := S/N$, where N is the $\mathbb{F}_q$-linear span of all polynomials $g(f) - f$ with f in S and g in G.

Conjecture 1.3. *The G-cofixed space of $S = \mathbb{F}_q[x_1, \dots, x_n]$ has Hilbert series*

$$\mathrm{Hilb}(S_G, t) = \sum_{k=0}^{n} t^{n(q^k-1)} \prod_{i=0}^{k-1} \frac{1}{1-t^{q^k-q^i}}.$$

(Here and elsewhere we interpret empty products as 1, as in the $k = 0$ summand above.)

Example 1.4. When $n = 0$, conjectures 1.2 and 1.3 have little to say, since $S = \mathbb{F}_q$ has no variables and $G = \mathrm{GL}_0(\mathbb{F}_q)$ is the trivial group. When $n = 1$, both conjectures are easily verified as follows. The group $G = \mathrm{GL}_1(\mathbb{F}_q) = \mathbb{F}_q^\times$ is cyclic of order $q - 1$. A cyclic generator g for G scales the monomials in $S = \mathbb{F}_q[x]$ via $g(x^k) = (\zeta x)^k = \zeta^k x$, where ζ is a $(q-1)$st root of unity in $\mathbb{F}_q$; g similarly scales the monomial basis elements $\{1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{q^m-1}\}$ of the quotient ring $Q = S/\mathfrak{m}^{[q^m]}$. Hence, $\bar{x}^k$ is G-invariant in Q if and only if $q-1$ divides k, so that Q^G has $\mathbb{F}_q$-basis $\{1, \bar{x}^{q-1}, \bar{x}^{2(q-1)}, \dots, \bar{x}^{q^m-q}, \bar{x}^{q^m-1}\}$. Therefore,

$$\begin{aligned}\mathrm{Hilb}(Q^G, t) &= (1 + t^{q-1} + t^{2(q-1)} + \cdots + t^{q^m-q}) + t^{q^m-1} \\ &= t^0 \begin{bmatrix} m \\ 1 \end{bmatrix}_{q,t} + t^{q^m-1} \begin{bmatrix} m \\ 0 \end{bmatrix}_{q,t} \\ &= C_{1,m}(t).\end{aligned}$$

[1] Warning: the latter terminology is often used for a *different* object, the quotient ring $S/(D_{n,0}, \dots, D_{n,n-1})$, so we avoid it.

For the same reason, the image of x^k survives as an $\mathbb{F}_q$-basis element in the G-cofixed quotient S_G if and only if $q-1$ divides k. Hence, S_G has $\mathbb{F}_q$-basis given by the images of $\{1, x^{q-1}, x^{2(q-1)}, \dots\}$, so that

$$\mathrm{Hilb}(S_G, t) = 1 + t^{q-1} + t^{2(q-1)} + \cdots = \frac{1}{1-t^{q-1}} = 1 + \frac{t^{q-1}}{1-t^{q-1}}.$$

1.1. The parabolic generalization

In fact, we shall work with generalizations of conjectures 1.2 and 1.3 to a *parabolic subgroup* P_α of G specified by a *composition* $\alpha = (\alpha_1, \dots, \alpha_\ell)$ of n, so that $|\alpha| := \alpha_1 + \cdots + \alpha_\ell = n$, and $\alpha_i > 0$ without loss of generality. This P_α is the subgroup of block upper-triangular invertible matrices

$$g = \begin{bmatrix} g_1 & * & \dots & * \\ 0 & g_2 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g_\ell \end{bmatrix}$$

with diagonal blocks $g_1, \dots, g_\ell$ of sizes $\alpha_1 \times \alpha_1, \dots, \alpha_\ell \times \alpha_\ell$. A generalization of Dickson's theorem by Kuhn and Mitchell [21] (related to results of Mui [24], and rediscovered by Hewett [16]) asserts that S^{P_α} is again a polynomial algebra, having Hilbert series given by the following expression, where we denote partial sums of α by $A_i := \alpha_1 + \cdots + \alpha_i$:

$$\mathrm{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i - 1} \frac{1}{1 - t^{q^{A_i} - q^{A_{i-1}+j}}}. \tag{1.4}$$

This leads to a polynomial in t called the (q,t)*-multinomial*, also studied in [25]:

$$\begin{bmatrix} n \\ \alpha \end{bmatrix}_{q,t} := \frac{\mathrm{Hilb}(S^{P_\alpha}, t)}{\mathrm{Hilb}(S^G, t)} = \frac{\prod_{j=0}^{n-1}(1 - t^{q^n - q^j})}{\prod_{i=1}^{\ell}\prod_{j=0}^{\alpha_i - 1}(1 - t^{q^{A_i} - q^{A_{i-1}+j}})}. \tag{1.5}$$

To state the parabolic versions of the conjectures, we consider *weak compositions* $\beta = (\beta_1, \dots, \beta_\ell)$ with $\beta_i \in \mathbb{Z}_{\geqslant 0}$, of a fixed length ℓ, and partially order them *componentwise*, i.e. $\beta \leqslant \alpha$ if $\beta_i \leqslant \alpha_i$ for $i = 1, 2, \dots, \ell$. In this situation, let $B_i := \beta_1 + \beta_2 + \cdots + \beta_i$.

Parabolic conjecture 1.5. For $m \geqslant 0$ and for α a composition of n, the P_α-fixed subalgebra Q^{P_α} of the quotient ring $Q = S/\mathfrak{m}^{[q^m]}$ has Hilbert series

$$\mathrm{Hilb}(Q^{P_\alpha}, t) = C_{\alpha,m}(t),$$

where

$$C_{\alpha,m}(t) := \sum_{\substack{\beta:\ \beta \leqslant \alpha, \\ |\beta| \leqslant m}} t^{e(m,\alpha,\beta)} \begin{bmatrix} m \\ \beta, m - |\beta| \end{bmatrix}_{q,t}, \quad e(m,\alpha,\beta) := \sum_{i=1}^{\ell} (\alpha_i - \beta_i)(q^m - q^{B_i}). \tag{1.6}$$

The $\ell = 1$ case of parabolic conjecture 1.5 is conjecture 1.2. Parabolic conjecture 1.5 also implies the following conjecture, whose $\ell = 1$ case is conjecture 1.3.

Parabolic conjecture 1.6. For a composition α of n, the P_α-cofixed space S_{P_α} of S has Hilbert series

$$\mathrm{Hilb}(S_{P_\alpha}, t) = \sum_{\beta:\ \beta \leqslant \alpha} t^{\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1)} \prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i - 1} \frac{1}{1 - t^{q^{B_i} - q^{B_{i-1}+j}}}. \tag{1.7}$$

1.2. Structure of the paper

The rest of the paper explains the relation between parabolic conjectures 1.5 and 1.6, along with context and evidence for both, including relations to known results.

Section 2 explains why parabolic conjecture 1.5 implies the Hilbert series (1.4) in the limit as $m \to \infty$, with the proof delayed until Appendix A.

Section 3 shows that parabolic conjecture 1.5 implies parabolic conjecture 1.6. It then shows the reverse implication in the case $n = 2$. Appendix B proves both via direct arguments for $n = 2$.

Section 4 checks parabolic conjecture 1.5 for $m = 0, 1$.

Section 5 explains why the P_α-cofixed space S_{P_α} is a finitely generated module of rank 1 over the P_α-fixed algebra S^{P_α}, and why this is consistent with the form of parabolic conjecture 1.6.

Section 6 concerns some of our original combinatorial motivation, comparing two G-representations:

- on the graded quotient $Q = S/\mathfrak{m}^{[q^m]}$;
- permuting the points of $(\mathbb{F}_{q^m})^n$.

These two representations are *not* isomorphic; however, we shall show that they have the same composition factors, i.e. they are *Brauer isomorphic*. After extending scalars from $\mathbb{F}_q G$ to $\mathbb{F}_{q^m} G$-modules, this Brauer isomorphism holds even taking into account a commuting group action $G \times C$, where the cyclic group $C = \mathbb{F}_{q^m}^\times$ is the multiplicative group of $\mathbb{F}_{q^m}$. Consistent with this, parabolic conjecture 1.5 has a strange implication: the two representations have G-fixed spaces and P_α-fixed spaces which are *isomorphic* C-representations. This assertion is equivalent to the fact that evaluating $C_{\alpha,m}(t)$ when t is a $(q^m - 1)$st root of unity exhibits a *cyclic sieving phenomenon* in the sense of [26].

Section 7 collects some further questions and remarks.

2. Conjecture 1.2 implies (1.4)

The following proposition is delicate to verify, but serves two purposes, explained after its statement.

Proposition 2.1. *For any $m \geqslant 0$ and any composition α of n, the power series*

$$\mathrm{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i - 1} \frac{1}{1 - t^{q^{A_i} - q^{A_{i-1}+j}}}$$

is congruent in $\mathbb{Z}[[t]]/(t^{q^m})$ *to the polynomial*

$$C_{\alpha,m}(t) = \sum_{\substack{\beta\colon \beta\leqslant\alpha,\\ |\beta|\leqslant m}} t^{e(m,\alpha,\beta)} \begin{bmatrix} m \\ \beta, m-|\beta| \end{bmatrix}_{q,t}, \quad e(m,\alpha,\beta) = \sum_{i=1}^{\ell} (\alpha_i - \beta_i)(q^m - q^{B_i}).$$

The first purpose of proposition 2.1 is to give evidence for parabolic conjecture 1.5, since it is implied by the conjecture: the ideal $\mathfrak{m}^{[q^m]} = (x_1^{q^m}, \ldots, x_n^{q^m})$ only contains elements of degree q^m and above, so the G-equivariant quotient map $S \twoheadrightarrow Q = S/\mathfrak{m}^{[q^m]}$ restricts to $\mathbb{F}_q$-vector-space isomorphisms

$$\left.\begin{aligned} S_d &\cong Q_d, \\ S_d^{P_\alpha} &\cong Q_d^{P_\alpha}, \end{aligned}\right\} \tag{2.1}$$

for $0 \leqslant d \leqslant q^m - 1$. Consequently, one has

$$\mathrm{Hilb}(S^{P_\alpha}, t) \equiv \mathrm{Hilb}(Q^{P_\alpha}, t) \bmod (t^{q^m}). \tag{2.2}$$

In particular, proposition 2.1 shows why parabolic conjecture 1.5 gives (1.4) in the limit as $m \to \infty$.

The second purpose of proposition 2.1 is to use its precise form in the proof of corollary 3.6 to assert the equivalence of parabolic conjectures 1.5 and 1.6 for $n = 2$.

The proof of proposition 2.1 is rather technical, so it is given in Appendix A.

3. Conjecture 1.2 implies conjecture 1.3

The desired implication follows from an examination of the quotient ring

$$Q := S/\mathfrak{m}^{[q^m]} = \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^{q^m}, \ldots, x_n^{q^m})$$

as a *monomial complete intersection*, and hence a *Gorenstein ring*. Note that Q has monomial basis

$$\{\boldsymbol{x}^a := x_1^{a_1} \cdots x_n^{a_n}\}_{0\leqslant a_i \leqslant q^m - 1} \tag{3.1}$$

and that its homogeneous component Q_{d_0} of top degree,

$$d_0 := n(q^m - 1), \tag{3.2}$$

is one dimensional, spanned over $\mathbb{F}_q$ by the image of the monomial

$$\boldsymbol{x}^{a_0} := (x_1 \cdots x_n)^{q^m - 1}.$$

Furthermore, the $\mathbb{F}_q$-bilinear pairing

$$\left.\begin{aligned} Q_i \otimes Q_j &\to Q_{d_0} = \mathbb{F}_q \cdot \boldsymbol{x}^{a_0} \cong \mathbb{F}_q \\ (f_1, f_2) &\mapsto f_1 \cdot f_2 \end{aligned}\right\} \tag{3.3}$$

is *non-degenerate* (or *perfect*): for monomials $\boldsymbol{x}^a, \boldsymbol{x}^b$ in (3.1) of degrees i, j with $i + j = d_0$, one has

$$(\boldsymbol{x}^a, \boldsymbol{x}^b) = \begin{cases} \boldsymbol{x}^{a_0} & \text{if } a + b = a_0, \\ 0 & \text{otherwise.} \end{cases}$$

PROPOSITION 3.1. *The monomial $\boldsymbol{x}^{a_0} = (x_1 \cdots x_n)^{q^m-1}$ has G-invariant image in the quotient $Q = S/\mathfrak{m}^{[q^m]}$, and hence its span Q_{d_0} carries the trivial G-representation.*

Proof 1. As G acts on S and on Q preserving degree, it induces a one-dimensional G-representation on Q_{d_0}. Thus, Q_{d_0} must carry one of the linear characters of $G = \mathrm{GL}_n(\mathbb{F}_q)$, i.e. $\det^j$ for some j in $\{0, 1, \dots, q-2\}$. We claim that in fact $j = 0$, since the element g in G that scales the variable x_1 by a primitive $(q-1)$st root of unity γ in $\mathbb{F}_q^\times$ and fixes all other variables x_i with $i \geqslant 2$ will have $\det(g) = \gamma$ and has $g(\boldsymbol{x}^{a_0}) = \gamma^{q^m-1}\boldsymbol{x}^{a_0} = \boldsymbol{x}^{a_0}$. □

Proof 2. Note that $G = \mathrm{GL}_n(\mathbb{F}_q)$ is generated by all *permutations* of coordinates, all *scalings* of coordinates, and any *transvection*, such as the element u sending $x_1 \mapsto x_1 + x_2$ and fixing x_i for $i \neq 1$. So it suffices to check that the image of $\boldsymbol{x}^{a_0} = (x_1 \cdots x_n)^{q^m-1}$ in Q is invariant under permutations (obvious), invariant under scalings of a coordinate (easily checked as in (1)), and invariant under the transvection u:

$$\begin{aligned} u(\boldsymbol{x}^{a_0}) &= (x_1 + x_2)^{q^m-1}(x_2 \cdots x_n)^{q^m-1} \\ &= (x_1^{q^m-1} + x_2 h)(x_2 \cdots x_n)^{q^m-1} \\ &\equiv \boldsymbol{x}^{a_0} \bmod \mathfrak{m}^{[q^m]}, \end{aligned}$$

where h is a polynomial whose exact form is unimportant. □

Note that proposition 3.1 is an expected consequence of conjecture 1.2, due to the following observation.

PROPOSITION 3.2. *For any composition α of n, the polynomial $C_{\alpha,m}(t)$ is monic of degree $d_0 = n(q^m - 1)$.*

Proof. Letting $\deg_t(\cdot)$ denote degree in t, the product formula (1.5) for the (q,t)-multinomial shows that

$$\begin{aligned} \deg_t \begin{bmatrix} m \\ \beta, m - |\beta| \end{bmatrix}_{q,t} &= \sum_{j=0}^{|\beta|}(q^m - q^j) - \sum_{i=1}^{\ell}\sum_{j=0}^{\beta_i-1}(q^{B_i} - q^{B_{i-1}+j}) \\ &= |\beta|q^m - \sum_{j=0}^{|\beta|} q^j - \sum_{i=1}^{\ell}\beta_i q^{B_i} + \sum_{i=1}^{\ell}\sum_{j=0}^{\beta_i-1} q^{B_{i-1}+j} \\ &= |\beta|q^m - \sum_{i=1}^{\ell}\beta_i q^{B_i}, \end{aligned} \tag{3.4}$$

while the exponent on the monomial $t^{e(m,\alpha,\beta)}$ can be rewritten as

$$e(m,\alpha,\beta) = \sum_{i=1}^{\ell}(\alpha_i - \beta_i)(q^m - q^{B_i}) = nq^m - |\beta|q^m - \sum_{i=1}^{\ell}\alpha_i q^{B_i} + \sum_{i=1}^{\ell}\beta_i q^{B_i}. \tag{3.5}$$

Therefore, the summand of $C_{\alpha,m}(t)$ indexed by β has degree equal to the sum of (3.4) and (3.5), namely

$$nq^m - \sum_{i=1}^{\ell} \alpha_i q^{B_i} \geqslant nq^m - \sum_{i=1}^{\ell} \alpha_i = nq^m - n = n(q^m-1) = d_0.$$

Equality occurs in the above if and only if $B_i = 0$ for all i, so the t-degree is maximized uniquely by the $\beta = 0$ summand, which is the single monomial $t^{n(q^m-1)} = t^{d_0}$. □

Proposition 3.1 shows that the non-degenerate pairing (3.3) is G-*invariant*: for any g in G, one has

$$(g(f_1), g(f_2)) = g(f_1)g(f_2) = g(f_1 f_2) = f_1 f_2 = (f_1, f_2).$$

Thus, one has an isomorphism of G-representations $Q_i \cong Q_j^*$ in complementary degrees $i + j = d_0$. Here the notation U^* denotes the representation *contragredient* or *dual* to the G-representation U on its dual space, in which, for any functional φ in U^*, group element g in G and vector u in U, one has $g(\varphi)(u) = \varphi(g^{-1}(u))$. Cofixed spaces are dual to fixed spaces, as the following well-known proposition shows.

Proposition 3.3. *For any group G and any G-representation U over a field k, one has a k-vector-space isomorphism $(U_G)^* \cong (U^*)^G$, in which U_G is the cofixed space for G acting on U, and $(U^*)^G$ is the subspace of G-fixed functionals in U^*.*

Proof. Recall that $U_G := U/N$, where N is the k-span of $\{g(u) - u\}_{u \in U,\, g \in G}$. Thus, by the universal property of quotients, $(U_G)^*$ is the subspace of functionals φ in U^* vanishing on restriction to N. This is equivalent to $0 = \varphi(g(u) - u) = \varphi(g(u)) - \varphi(u)$ for all u in U and g in G, i.e. to φ lying in $(U^*)^G$. □

Corollary 3.4. *For complementary degrees $i + j = d_0$ in $Q = S/\mathfrak{m}^{[q^m]}$, one has an $\mathbb{F}_q$-vector space duality of fixed and cofixed spaces $(Q_i^{P_\alpha})^* \cong (Q_j)_{P_\alpha}$, and hence the equality of their dimensions. Therefore, one has*

$$\mathrm{Hilb}(Q_{P_\alpha}, t) = t^{d_0}\, \mathrm{Hilb}(Q^{P_\alpha}, t^{-1}), \tag{3.6}$$

$$\mathrm{Hilb}(S_{P_\alpha}, t) \equiv t^{d_0}\, \mathrm{Hilb}(Q^{P_\alpha}, t^{-1}) \mod (t^{q^m}), \tag{3.7}$$

and

$$\mathrm{Hilb}(S_{P_\alpha}, t) = \lim_{m\to\infty} t^{d_0}\, \mathrm{Hilb}(Q^{P_\alpha}, t^{-1}). \tag{3.8}$$

Proof. Equation (3.6) is immediate from the discussion surrounding proposition 3.3. Then (3.6) implies (3.7), since the isomorphism (2.1) shows $(S_{P_\alpha})_d \cong (Q_{P_\alpha})_d$ for $0 \leqslant d \leqslant q^m - 1$. Lastly, (3.7) implies (3.8). □

Corollary 3.5. *Parabolic conjecture 1.5 implies parabolic conjecture 1.6.*

Proof. Assuming parabolic conjecture 1.5 holds, (3.8) implies

$$\mathrm{Hilb}(S_{P_\alpha}, t) = \lim_{m\to\infty} t^{d_0}\, \mathrm{Hilb}(Q^{P_\alpha}, t^{-1}) = \lim_{m\to\infty} t^{d_0} C_{\alpha,m}(t^{-1}).$$

Hence, parabolic conjecture 1.6 follows once one checks the following assertion:

$$t^{d_0} C_{\alpha,m}(t^{-1}) \equiv \sum_{\beta:\ \beta \leqslant \alpha} t^{\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1)} \prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i - 1} \frac{1}{1 - t^{q^{B_i} - q^{B_{i-1}+j}}} \quad \bmod (t^{q^m}). \tag{3.9}$$

To prove (3.9), one first uses the definition (1.6) of $C_{\alpha,m}(t)$ to do a straightforward calculation showing

$$t^{d_0} C_{\alpha,m}(t^{-1}) = \sum_{\substack{\beta:\ \beta \leqslant \alpha, \\ |\beta| \leqslant m}} t^{\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1)} \frac{\prod_{j=0}^{|\beta|-1} (1 - t^{q^m - q^j})}{\prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i - 1} (1 - t^{q^{B_i} - q^{B_{i-1}+j}})}. \tag{3.10}$$

Since $q^{B_i} - 1 \geqslant q^{B_i - 1}$, one has

$$\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1) \geqslant \sum_{i=1}^{\ell} \alpha_i q^{B_i - 1} \geqslant \alpha_\ell q^{B_\ell - 1} \geqslant q^{|\beta| - 1}.$$

This implies that for each $j = 0, 1, \ldots, |\beta| - 1$ one has

$$(q^m - q^j) + \sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1) \geqslant q^m.$$

Therefore, the right-hand side of (3.10) is equivalent $\bmod(t^{q^m})$ to the right-hand side of (3.9). □

Corollary 3.6. *In the bivariate case $n = 2$, the parabolic conjectures 1.5 and 1.6 are equivalent.*

Proof. Corollary 3.5 showed that parabolic conjecture 1.5 implies parabolic conjecture 1.6 for any n. The reverse implication when $n = 2$ arises when two coefficient comparisons valid for general n 'meet in the middle', as we now explain. Again, in this proof, all symbols '$\equiv$' mean congruence $\bmod(t^{q^m})$. On the one hand, one has

$$\mathrm{Hilb}(Q^{P_\alpha}, t) \equiv \mathrm{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i - 1} \frac{1}{1 - t^{q^{A_i} - q^{A_{i-1}+j}}} \equiv C_{\alpha,m}(t),$$

where the left congruence is (2.2), the middle equality is (1.4) and the right congruence is proposition 2.1. Therefore, $\mathrm{Hilb}(Q^{P_\alpha}, t)$ and $C_{\alpha,m}(t)$ have the same coefficients on $1, t, t^2, \ldots, t^{q^m - 1}$. On the other hand, one has

$$\begin{aligned} t^{d_0} \,\mathrm{Hilb}(Q^{P_\alpha}, t^{-1}) &\equiv \mathrm{Hilb}(S_{P_\alpha}, t) \\ &= \sum_{\beta:\ \beta \leqslant \alpha} t^{\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1)} \prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i - 1} \frac{1}{1 - t^{q^{B_i} - q^j}} \\ &\equiv t^{d_0} C_{\alpha,m}(t^{-1}), \end{aligned}$$

where the first congruence is (3.7), the equality is parabolic conjecture 1.6 and the last congruence is corollary 3.9. Therefore, $\mathrm{Hilb}(Q^{P_\alpha}, t)$ and $C_{\alpha,m}(t)$ also have the same coefficients on $t^{d_0}, t^{d_0 - 1}, \ldots, t^{d_0 - (q^m - 1)}$. Since $d_0 = n(q^m - 1)$ when $n = 2$, this means that $\mathrm{Hilb}(Q^{P_\alpha}, t), C_{\alpha,m}(t)$ agree on *all* coefficients. □

EXAMPLE 3.7. We illustrate some of the assertions of corollary 3.4 for $n = m = 2$ and $q = 3$, where

$$S = \mathbb{F}_3[x, y], \qquad Q = S/(x^9, y^9), \qquad d_0 = 2(3^2 - 1) = 16.$$

Our results in Appendix B show that conjectures 1.2 and 1.3 hold for $n = 2$. Therefore, for the group $G = \mathrm{GL}_2(\mathbb{F}_3)(= P_{(2)})$, one can compute that

$$\begin{aligned}\mathrm{Hilb}(S^G, t) &= \frac{1}{(1-t^6)(1-t^8)} = 1 + t^6 + t^8 + O(t^9),\\ \mathrm{Hilb}(Q^G, t) &= C_{2,2}(t) = 1 + t^6 + t^8 + t^{10} + t^{12} + t^{16} \equiv \mathrm{Hilb}(S^G, t) \bmod t^9,\end{aligned}$$

and, similarly,

$$\begin{aligned}\mathrm{Hilb}(S_G, t) &= 1 + \frac{t^4}{1-t^2} + \frac{t^{16}}{(1-t^6)(1-t^8)} = 1 + t^4 + t^6 + t^8 + O(t^9),\\ t^{16}\,\mathrm{Hilb}(Q^G, t^{-1}) &= 1 + t^4 + t^6 + t^8 + t^{10} + t^{16} \equiv \mathrm{Hilb}(S_G, t) \bmod t^9.\end{aligned}$$

Note that $\mathrm{Hilb}(Q^G, t)$ is *not* a reciprocal polynomial in t, i.e. its coefficient sequence is not symmetric. In particular, although the ring Q is Gorenstein, its G-fixed subalgebra Q^G is *not*.

4. The case where *m* is at most 1

When $m = 0$, parabolic conjecture 1.5 says little: $Q = S/\mathfrak{m}^{[q^0]} = S/\mathfrak{m} = \mathbb{F}_q$ has no variables, so $Q^{P_\alpha} = Q = \mathbb{F}_q$ and $\mathrm{Hilb}(Q^{P_\alpha}, t) = 1$. Meanwhile, $C_{\alpha,0}(t) = 1$, since (1.6) has only the $\beta = 0$ summand.

The $m = 1$ case is less trivial.

PROPOSITION 4.1. *Parabolic conjecture 1.5 holds for* $m = 1$.

Proof. Given the composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ of n, the only weak compositions β with $0 \leqslant \beta \leqslant \alpha$ and $|\beta| \leqslant m = 1$ are $\beta = 0$ and $\beta = e_k = (0, \ldots, 0, 1, 0, \ldots, 0)$ for $k = 1, 2, \ldots, \ell$. One therefore finds that

$$\begin{aligned}C_{\alpha,1}(t) &= t^{e(1,\alpha,0)} \begin{bmatrix} 1 \\ 0, 1 \end{bmatrix}_{q,t} + \sum_{k=1}^{\ell} t^{e(1,\alpha,e_k)} \begin{bmatrix} 1 \\ e_k, 0 \end{bmatrix}_{q,t}\\ &= t^{n(q-1)} + \sum_{k=1}^{\ell} t^{A_{k-1}(q-1)}\\ &= \sum_{k=0}^{\ell} t^{A_k(q-1)},\end{aligned}$$

recalling that $A_\ell = n$ and the convention that $A_0 = 0$. Thus, to show $C_{\alpha,1}(t) = \mathrm{Hilb}(Q^{P_\alpha}, t)$, it will suffice to show that Q^{P_α} has $\mathbb{F}_q$-basis given by the images of the monomials

$$\{(x_1 x_2 \cdots x_{A_k})^{q-1}\}_{k=0,1,\ldots,\ell}. \tag{4.1}$$

To argue this, consider any polynomial

$$f(\boldsymbol{x}) = \sum_{\substack{a=(a_1,\dots,a_n),\\ a_i\in\{0,1,\dots,q-1\}}} c_a \boldsymbol{x}^a$$

representing an element of the quotient $Q = S/\mathfrak{m}^{[q]}$. One has that $f(\boldsymbol{x})$ is invariant under the *diagonal matrices* T inside P_α if and only if each entry a_i is either 0 or $q-1$, i.e. if and only if $f(\boldsymbol{x})$ has the form

$$f(\boldsymbol{x}) = \sum_{A\subset\{1,2,\dots,n\}} c_A \boldsymbol{x}_A^{q-1}, \tag{4.2}$$

where $\boldsymbol{x}_A := \prod_{j\in A} x_j$, so that $\boldsymbol{x}_A^{q-1} = \prod_{j\in A} x_j^{q-1}$.

We claim that such an f is furthermore invariant under the *Borel subgroup* B of upper triangular matrices if and only if each monomial $\boldsymbol{x}_A^{q-1}$ in the support of f has A forming an initial segment $A = \{1,2,\dots,k\}$ for some k. To prove this claim, note that B is generated by T together with $\{u_{ij} : 1 \leqslant i < j \leqslant n\}$, where u_{ij} sends $x_j \mapsto x_j + x_i$ and fixes all other variables x_ℓ with $\ell \neq j$. Working mod $\mathfrak{m}^{[q]}$, one checks that

$$u_{i,j}(\boldsymbol{x}_A^{q-1}) = \begin{cases} \boldsymbol{x}_A^{q-1} & \text{if } \{i,j\}\cap A \neq \{j\},\\ \boldsymbol{x}_A^{q-1} + \boldsymbol{x}_{A\setminus\{j\}\cup\{i\}}^{q-1} & \text{if } \{i,j\}\cap A = \{j\}. \end{cases}$$

From this it is easily seen that each monomial $(x_1x_2\cdots x_k)^{q-1}$ has a B-invariant image in Q. On the other hand, if $f(\boldsymbol{x})$ as in (4.2) has $c_A \neq 0$ for some A that is not an initial segment, then there exists $1 \leqslant i < j \leqslant n$ for which $\{i,j\}\cap A = \{j\}$, and one finds that $u_{i,j}(f) \neq f$, since $u_{i,j}(f) - f$ has coefficient c_A on $\boldsymbol{x}_{A\setminus\{j\}\cup\{i\}}^{q-1}$.

Lastly, an element of this more specific form

$$f(\boldsymbol{x}) = \sum_{k=0}^{n} c_k (x_1x_2\cdots x_k)^{q-1}$$

will furthermore be invariant under the subgroup $\mathfrak{S}_{\alpha_1}\times\cdots\times\mathfrak{S}_{\alpha_\ell}$ of block permutation matrices inside P_α if and only if it is supported on the monomials in (4.1). Since P is generated by the Borel subgroup B together with this subgroup $\mathfrak{S}_{\alpha_1}\times\cdots\times\mathfrak{S}_{\alpha_\ell}$, the monomials in (4.1) give an $\mathbb{F}_q$-basis for Q^{P_α}. □

5. The cofixed quotient S_G as an S^G-module

Note that parabolic conjecture 1.6 has the following two consequences for the rational function $\mathrm{Hilb}(S_{P_\alpha},t)/\mathrm{Hilb}(S^{P_\alpha},t)$:

$$\frac{\mathrm{Hilb}(S_{P_\alpha},t)}{\mathrm{Hilb}(S^{P_\alpha},t)} \quad \text{lies in } \mathbb{Z}[t] \tag{5.1}$$

and

$$\lim_{t\to 1} \frac{\mathrm{Hilb}(S_{P_\alpha},t)}{\mathrm{Hilb}(S^{P_\alpha},t)} = 1. \tag{5.2}$$

The subsections below explain why (5.1), (5.2) do indeed hold, essentially due to the following three facts:

(1) the P_α-cofixed quotient S_{P_α} is a finitely generated module over the P_α-invariant ring S^{P_α};

(2) while S_{P_α} is *not* in general a free S^{P_α}-module, it does always have S^{P_α}-rank 1; and

(3) the P_α-invariant ring S^{P_α} is polynomial, as shown in [16, 24].

5.1. The cofixed spaces as a module over fixed subalgebra

Facts (1) and (2) above hold generally for finite group actions, and are analogous to well-known facts about invariant rings. As we have not found them in the literature, we discuss them here.

PROPOSITION 5.1. *Fix a field k, a k-algebra R and an R-module M and let G be any subgroup of $\mathrm{Aut}_R(M)$, the R-module automorphisms of M. Then one has that*

(i) *the k-linear span N of all elements $\{g(m) - m\}_{g \in G, m \in M}$ is an R-submodule of M, and hence*

(ii) *the cofixed space $M_G := M/N$ is a quotient R-module of M.*

Furthermore, if $\{m_i\}_{i \in I}$ generate M as an R-module, and if $\{g_j\}_{j \in J}$ generate G as a group, then

(iii) *the images $\{\bar{m}_i\}_{i \in I}$ generate M_G as an R-module, and*

(iv) *the elements $\{g_j^{\pm 1}(m_i) - m_i\}_{i \in I, j \in J}$ generate N as an R-module.*

Proof. All assertions are completely straightforward, except possibly for (iv), which relies on the calculation

$$g_1 g_2(m) - m = g_1 g_2(m) - g_2(m) + g_2(m) - m,$$

and the hypotheses let one express $g_2(m) = \sum_{i \in I} r_i m_i$ for some r_i in R, so that one can rewrite this as

$$g_1 g_2(m) - m = \sum_{i \in I} r_i (g_1(m_i) - m_i) + (g_2(m) - m).$$

□

COROLLARY 5.2. *Let S be a finitely generated k-algebra and G be a finite subgroup of k-algebra automorphisms of S, e.g. $S = k[x_1, \ldots, x_n]$ and G is a finite subgroup of $\mathrm{GL}_n(k)$ acting by linear substitutions.*

Then the G-cofixed space S_G is a finitely generated module over the G-fixed subalgebra S^G.

Proof. Via (ii) and (iii) of proposition 5.1, it suffices to show that S is a finitely generated S^G-module. This is a well-known argument via [3, corollary 5.2] (see also [5, theorem 1.3.1]; [30, theorem 2.3.1]). One has that S is integral over S^G, as any x in S satisfies the monic polynomial $\prod_{g \in G}(t - g(x))$ in $S^G[t]$, and S is finitely generated as an algebra over S^G because it is finitely generated as a k-algebra. □

Example 5.3. In the case where $M = S = \mathbb{F}_q[x_1, \dots, x_n]$ and $G = \mathrm{GL}_n(\mathbb{F}_q)$, one has that S is even a *free* S^G-module of rank $|G|$ with an explicit S^G-basis of monomials $\{x^\alpha\}_{0 \leqslant \alpha_i \leqslant q^n - q^{i-1} - 1}$ provided by Steinberg [32] in his proof of Dickson's theorem. Consequently, S_G is generated by the images of these monomials, and proposition 5.1(iv) leads to an explicit finite presentation of S_G as a quotient of the free S^G-module S, which is useful for computations.

Corollary 5.4. *When a finite subgroup G of $\mathrm{GL}_n(k)$ acting by linear substitutions on $S = k[x_1, \dots, x_n]$ has a G-fixed subalgebra S^G that is again a polynomial algebra, then* $\mathrm{Hilb}(S_G, t)/\mathrm{Hilb}(S^G, t)$ *lies in* $\mathbb{Z}[t]$.

Proof. When S^G is polynomial, the *Hilbert syzygy theorem* (see, for example, [5, § 2.1]; [30, § 6.3]) implies that S_G will have a finite S^G-free resolution $0 \to F_n \to \cdots \to F_1 \to F_0 \to S_G \to 0$, where $F_i = \bigoplus_{j \geqslant 0} S^G(-j)^{\beta_{i,j}}$ for some non-negative integers $\beta_{i,j}$. Here $R(-j)$ denotes a copy of the graded ring R, regarded as a module over itself, but with grading shift so that the unit 1 is in degree j, so that

$$\mathrm{Hilb}(F_i, t) = \mathrm{Hilb}(S^G, t) \cdot \sum_{j \geqslant 0} \beta_{i,j} t^j.$$

Considering the Euler characteristics in each homogeneous component of the resolution gives

$$\mathrm{Hilb}(S^G, t) \sum_{i,j \geqslant 0} (-1)^i \beta_{i,j} t^j = \mathrm{Hilb}(S_G, t),$$

so that $\mathrm{Hilb}(S_G, t)/\mathrm{Hilb}(S^G, t) = \sum_{i,j \geqslant 0} (-1)^i \beta_{i,j} t^j$ lies in $\mathbb{Z}[t]$. □

5.2. The cofixed space is a rank 1 module

We next explain, via consideration of the rank of S_G as an S^G-module, why one should expect (5.2) to hold.

Definition 5.5. Recall, for a finitely generated M over an integral domain R [12, § 12.1], that $\mathrm{rank}_R(M)$ is the maximum size of an R-linearly independent subset of M.

Alternatively, $\mathrm{rank}_R(M)$ is the largest integer r such that M contains a free R-submodule R^r, and in this situation, the quotient M/R^r will be all R-*torsion*, i.e. for every x in M/R^r there exists some $a \neq 0$ in R with $ax = 0$. One can equivalently define this using the *field of fractions* $K := \mathrm{Frac}(R)$ via

$$\mathrm{rank}_R(M) := \dim_K(K \otimes_R M). \tag{5.3}$$

Indeed, clearing denominators shows that a subset $\{m^{(i)}\} \subset M$ is R-linearly independent if and only if $\{1 \otimes m^{(i)}\} \subset K \otimes_R M$ is K-linearly independent.

In the graded setting, one has the following well-known characterization of rank via Hilbert series.

PROPOSITION 5.6. *For R an integral domain that is also a finitely generated graded k-algebra, and M a finitely generated graded R-module, the two rational functions* $\mathrm{Hilb}(R,t)$ *and* $\mathrm{Hilb}(M,t)$ *satisfy*

$$\mathrm{rank}_R(M) = \lim_{t\to 1} \frac{\mathrm{Hilb}(M,t)}{\mathrm{Hilb}(R,t)}.$$

Proof. Letting $r := \mathrm{rank}_R(M)$, we claim that one can choose an R-linearly independent subset of size r in M consisting of *homogeneous* elements as follows. Given *any* R-linearly independent subset $\{m^{(i)}\}_{i=1,2\cdots,r}$, decompose its elements into their homogeneous components $m^{(i)} = \sum_j m_j^{(i)}$. Then the set of all such components $\{m_j^{(i)}\}$ spans an R-submodule of M containing the R-submodule spanned by $\{m^{(i)}\}_{i=1,2,\ldots,r}$. Thus, the set of all such components must contain an R-linearly independent subset of size r.

Now, consider the free R-submodule $R^r := \bigoplus_{i=1}^r Rm_i$ spanned by a homogeneous R-linearly independent subset $\{m_i\}_{i=1,2,\ldots,r}$, so that the quotient M/R^r will be an R-torsion module. Then

$$\lim_{t\to 1} \frac{\mathrm{Hilb}(M,t)}{\mathrm{Hilb}(R,t)} = \lim_{t\to 1} \frac{\mathrm{Hilb}(R^r,t)}{\mathrm{Hilb}(R,t)} + \lim_{t\to 1} \frac{\mathrm{Hilb}(M/R^r,t)}{\mathrm{Hilb}(R,t)}.$$

Since $\mathrm{Hilb}(R^r,t)/\mathrm{Hilb}(R,t) = \sum_{i=1}^r t^{\deg(m_i)}$, the first limit on the right is r. One can argue that the second limit on the right vanishes as follows. Assume R has Krull dimension d, i.e. $\mathrm{Hilb}(R,t)$ has a pole of order d at $t = 1$. Thus, one must show that $\mathrm{Hilb}(M/R^r,t)$ has its pole of order at most $d-1$. To this end, choose homogeneous generators $y_1,\ldots,y_N$ for the R-torsion module M/R^r, say with $\theta_i y_i = 0$ for non-zero homogeneous θ_i in R. Then one has a graded R-module surjection $\bigoplus_{i=1}^N R/(\theta_i)(-\deg(y_i)) \twoheadrightarrow M/R^r$ sending the basis element of $R/(\theta_i)$ to y_i. This gives a coefficientwise inequality,

$$\mathrm{Hilb}(M/R^r,t) \leqslant \sum_{i=1}^N t^{\deg(y_i)}\,\mathrm{Hilb}(R/(\theta_i),t) = \sum_{i=1}^N (1-t^{\deg(\theta_i)})t^{\deg(y_i)}\,\mathrm{Hilb}(R,t), \tag{5.4}$$

between power series with non-negative coefficients that are also rational functions having poles confined to the unit circle. As each summand on the right-hand side of (5.4) has a pole of order at most $d-1$ at $t = 1$, the same holds for $\mathrm{Hilb}(M/R^r,t)$. □

For a subgroup G of ring automorphisms of the domain S, denote by $K := \mathrm{Frac}(S)^G$ the G-invariant subfield of $L := \mathrm{Frac}(S)$. When G is finite, an easy argument (see [5, proposition 1.1.1]; [30, proposition 1.2.4]) shows that

$$K := \mathrm{Frac}(S^G) = \mathrm{Frac}(S)^G (= L^G),$$

giving the following commuting diagram of inclusions:

$$\begin{tikzcd} S \arrow[r, hook] & L \\ S^G \arrow[u, hook] \arrow[r, hook] & K \arrow[u, hook] \end{tikzcd} \tag{5.5}$$

Consequently, proposition 5.6 and the next result immediately imply (5.2).

Proposition 5.7. *A finite group G of automorphisms of an integral domain S has* $\operatorname{rank}_{S^G} S_G = 1$.

Proof. Using (5.3) to characterize rank, it suffices to show the following chain of three K-vector-space isomorphisms:

$$K \otimes_{S^G} S_G \cong L_G \cong (KG)_G \cong K. \tag{5.6}$$

For the first step in (5.6), start with the short exact sequence that defines S_G

$$0 \to \sum_{\substack{g\in G,\\ s\in S}} S^G(g(s)-s) \to S \to S_G \to 0$$

and apply the exact localization functor $K \otimes_{S^G} (\cdot)$ to give the short exact sequence

$$0 \to \sum_{\substack{g\in G,\\ s\in S}} K \otimes_{S^G} S^G(g(s)-s) \to K \otimes_{S^G} S \to K \otimes_{S^G} S_G \to 0. \tag{5.7}$$

Using the K-vector-space isomorphism $K \otimes_{S^G} S \cong L$ induced by $f \otimes s \mapsto fs$, the sequence (5.7) becomes

$$0 \to \sum_{\substack{g\in G,\\ f\in L}} K(g(f)-f) \to L \to K \otimes_{S^G} S_G \to 0,$$

which shows that $K \otimes_{S^G} S_G \cong L_G$, completing the first step.

The second step in (5.6) comes from considering the Galois extension $K = L^G \hookrightarrow L$ having Galois group G, which appears as the right vertical map in (5.5). The normal basis theorem of Galois theory [23, theorem 13.1] asserts that not only is $L \cong K^{|G|}$ as a K-vector space but L is even isomorphic to the *left-regular representation* KG as KG-module. Hence, $L_G \cong (KG)_G$, completing the second step.

The third step in (5.6) comes from the short exact sequence of KG-modules

$$0 \to I_G \to KG \overset{\varepsilon}{\to} K \to 0. \tag{5.8}$$

Here G acts trivially on K, while the *augmentation ideal* I_G is the kernel of the *augmentation map* ε sending each K-basis element g of KG to 1 in K. Since I_G is K-spanned by $g - h$ for g, h in G, the sequence (5.8) shows that $(KG)_G \cong K$, completing the third step. □

This immediately implies the following corollary, explaining (5.2).

Corollary 5.8. *When a finite subgroup G of* $\mathrm{GL}_n(k)$ *acting by linear substitutions on $S = k[x_1, \ldots, x_n]$ has G-fixed subalgebra S^G that is again a polynomial algebra, we have*

$$\lim_{t\to 1} \frac{\mathrm{Hilb}(S_G, t)}{\mathrm{Hilb}(S^G, t)} = \operatorname{rank}_{S^G} S_G = 1.$$

5.3. On the module structure of the *G*-cofixed space

For the full general linear group $G = \mathrm{GL}_n(\mathbb{F}_q)$, the structure of S_G as an S^G-module exhibited for $n = 1$ in example 1.4 and for $n = 2$ in theorem B.15 suggests a general question.

Recall that $S^G = \mathbb{F}_q[D_{n,0}, D_{n,1}, \ldots, D_{n,n-1}]$, where the Dickson polynomials $D_{n,i}$ are defined in § 1. Consider subalgebras of S^G defined for $i = 1, 2, \ldots, n$ by

$$\mathbb{F}_q[Z_i] := \mathbb{F}_q[D_{n,n-i}, D_{n,n-i+1}, \ldots, D_{n,n-2}, D_{n,n-1}].$$

QUESTION 5.9. Does there exist a subset M of homogeneous elements minimally generating S_G as an S^G-module, with a decomposition $M = \bigsqcup_{i=1}^n M_i$ having the following properties?

- The $\mathbb{F}_q[Z_i]$-submodule generated by M_i within S_G is $\mathbb{F}_q[Z_i]$-free.
- The Dickson polynomials $D_{n,0}, D_{n,1}, \ldots, D_{n,n-i-1}$ not in $\mathbb{F}_q[Z_i]$ all annihilate every element of M_i.
- The last set M_n is a singleton, whose unique element has degree $(n-1)(q^n-1)$.

EXAMPLE 5.10. In the $n = 1$ case, example 1.4 shows that S_G is a free S^G-module of rank 1 with basis element given by the image of 1. This answers question 5.9 affirmatively by setting $M = M_1 := \{1\}$.

EXAMPLE 5.11. In the $n = 2$ case, theorem B.15 will answer question 5.9 affirmatively by setting $M = M_1 \sqcup M_2$, where $M_1 := \{1, XY, X^2Y, \ldots, X^{q-2}Y\}$ and $M_2 := \{X^qY\}$, with $X := x^{q-1}, Y := y^{q-1}$.

Before discussing the $n = 3$ case in further detail, we mention a general recurrence for the power series

$$f_n(t) := \sum_{k=0}^{n} t^{n(q^k-1)} \prod_{i=0}^{k-1} \frac{1}{1 - t^{q^k - q^i}}$$

that was conjectured to equal $\mathrm{Hilb}(S_G, t)$ in conjecture 1.3. An easy calculation shows that

$$f_n(t) = (f_{n-1}(t) - t^{(n-1)(q-1)} f_{n-1}(t^q)) + \frac{t^{(n-1)(q^n-1)}}{\prod_{i=0}^{n-1}(1 - t^{q^n - q^i})}. \tag{5.9}$$

An affirmative answer to question 5.9 would interpret the two summands on the right-hand side of (5.9) as follows:

- the last summand on the right in (5.9) would be the Hilbert series for the S^G-submodule of S_G generated by the singleton set M_n;
- the difference $f_{n-1}(t) - t^{(n-1)(q-1)} f_{n-1}(t^q)$ would be the Hilbert series for the S^G-submodule generated by $M_1 \sqcup \cdots \sqcup M_{n-1}$ or, alternatively, the kernel of multiplication by $D_{n,0}$ on S_G.

Somewhat suggestively, it can be shown directly that the difference

$$f_{n-1}(t) - t^{(n-1)(q-1)} f_{n-1}(t^q)$$

has non-negative coefficients as a power series in t; we omit the details of this proof.

EXAMPLE 5.12. In the $n = 3$ case, the recurrence (5.9) suggests a more precise version of question 5.9 that agrees with computer experiments. Example 5.11 shows that

$$f_2(t) = \frac{1 + t^{2(q-1)}[q-2]_{t^{q-1}}}{1 - t^{q^2-q}} + \frac{t^{q^2-1}}{(1 - t^{q^2-q})(1 - t^{q^2-1})} =: m_{2,1}(t) + m_{2,2}(t),$$

using the notation $[n]_t := 1 + t + \cdots + t^{n-1}$. Then the recurrence (5.9) applied with $n = 3$ gives

$$\begin{aligned} f_3(t) &= (m_{2,1}(t) - t^{2(q-1)} m_{2,1}(t^q)) + (m_{2,2}(t) - t^{2(q-1)} m_{2,2}(t^q)) \\ &\quad + \frac{t^{2(q^3-1)}}{(1 - t^{q^3-q^2})(1 - t^{q^3-q})(1 - t^{q^3-1})} \\ &= \frac{A_1(t)}{1 - t^{q^3-q^2}} + \frac{A_2(t)}{(1 - t^{q^3-q^2})(1 - t^{q^3-q})} + \frac{A_3(t)}{(1 - t^{q^3-q^2})(1 - t^{q^3-q})(1 - t^{q^3-1})}, \end{aligned} \tag{5.10}$$

where one can compute the numerators explicitly:

$$\left.\begin{aligned} A_1(t) &= [q]_{t^{q^2-q}} + t^{2(q-1)}([q-2]_{t^{q-1}}(1 + t^{q^2-q}) - 1) \\ &\qquad + t^{(2q+3)(q-1)}[q-2]_{t^{q^2-q}}[q-3]_{t^{q-1}}, \\ A_2(t) &= t^{q^2-1}[q]_{t^{q^2-1}}[q]_{t^{q^2-q}} - t^{(q-1)(q^2+q+2)}, \\ A_3(t) &= t^{2(q^3-1)}. \end{aligned}\right\} \tag{5.11}$$

Note that $A_1(t)$, $A_2(t)$ are polynomials in t with non-negative coefficients.[2] The following conjecture has been checked by D. Stamate (personal communication, 2014) for $n = 3$ and $q = 2, 3, 4, 5$ using SINGULAR.

CONJECTURE 5.13. *Question 5.9 for $n = 3$ has an affirmative answer for*

$$\sum_{f \in M_i} t^{\deg(f)} = A_i(t)$$

as in (5.11).

We close this section with some remarks on question 5.9, some providing evidence on the affirmative side, and some on the negative side.

REMARK 5.14. If the answer to question 5.9 is affirmative, then this would imply that the Dickson polynomial of lowest degree $D_{n,n-1}$ acts on the S^G-module S_G as a non-zero divisor. One can check that this property does indeed hold for $D_{n,n-1}$

[2] The non-negativity of $A_1(t)$, $A_2(t)$ is manifest from (5.11) for $q \geqslant 3$; for $q = 2$ it also holds, although it is less clear from (5.11).

via the argument of Karagueuzian and Symonds [17, lemma 2.5] used in proposition B.8. The key fact is that Dickson's expression for $D_{n,n-1}$ as a quotient of determinants shows it to be a homogeneous polynomial in $x_1, \ldots, x_n$ of degree $q^n - q^{n-1}$ with $x_n^{q^n - q^{n-1}}$ as its leading monomial in x_n.

Remark 5.15. Recurrence (5.9) with $n = 4$ gives rise, via a calculation similar to (5.10), to the following expression:

$$f_4(t) = \sum_{i=1}^{4} \frac{B_i(t)}{\prod_{j=1}^{i}(1 - t^{q^4 - q^{4-j}})}.$$

However, one finds that for $q = 2$ the numerator $B_1(t)$ is equal to $1 - t^3 + t^4$, which has a negative coefficient. Analogous calculations for higher values of n and small values of q yield similar negative coefficients in the other numerator terms.

Remark 5.16. One might ask why question 5.9 has been formulated only for G, and not for all parabolic subgroups P_α of G. In fact, theorem B.10 does prove such a result for $n = 2$, when there is only one proper parabolic subgroup: the Borel subgroup $B = P_{(1,1)}$ inside $G = \mathrm{GL}_2(\mathbb{F}_q)$.

However, computer calculations in Sage suggest that a naive formulation of such a question has a negative answer in general. Specifically, for $n = 3$ and $q = 4$ with $B = P_{(1,1,1)}$ inside $G = \mathrm{GL}_3(\mathbb{F}_4)$, one encounters the following difficulty. One wants a minimal generating set M for S_B as an S^B-module of a particular form. Note that here $S^B = \mathbb{F}_4[f_3, f_{12}, f_{48}]$, where $f_3 := x^3$, $f_{12} := \prod_{c \in \mathbb{F}_4}(y + cx)^3 = y^{12} + x^3y^9 + x^6y^6 + x^9y^3$ and $f_{48} := D_{3,2}(x, y, z)$. One can also show, using the idea in [17, § 2.1] and proposition B.8, that f_{48} acts as a non-zero divisor on S_B. Thus, one might expect a decomposition of the minimal generators as

$$M = M_1 \sqcup M_2 \sqcup M_3 \sqcup M_4, \tag{5.12}$$

in which

- $\mathbb{F}_4[f_3, f_{12}, f_{48}]$ acts freely on M_4,
- $\mathbb{F}_4[f_{12}, f_{48}]$ acts freely on M_3, but f_3 annihilates it,
- $\mathbb{F}_4[f_3, f_{48}]$ acts freely on M_2, but f_{12} annihilates it, and
- $\mathbb{F}_4[f_{48}]$ acts freely on M_1, but both f_3, f_{12} annihilate it.

We argue that this is impossible as follows. Let

$$(S_B)_{\leqslant d} := \bigoplus_{i=0}^{d} (S_B)_d$$

and, similarly,

$$(S_B)_{<d} := \bigoplus_{i=0}^{d-1} (S_B)_d.$$

Given a subset $A \subset S_B$, let $S^B A$ denote the S^B-submodule of S_B that it generates. Then computations show $\mathrm{Hilb}(S^B(S_B)_{\leqslant 42}, t) - \mathrm{Hilb}(S^B(S_B)_{<42}, t)$ agrees up to degree 90 with

$$t^{42} \cdot \mathrm{Hilb}(\mathbb{F}_4[f_3, f_{48}], t) + t^{42} \cdot \mathrm{Hilb}(\mathbb{F}_4[f_{12}, f_{48}], t).$$

One can check that, in any decomposition (5.12), the sets M_2, M_3 must each contain exactly one element of degree 42. But computations show that for every element f in $(S_B)_{42}$ the difference

$$\mathrm{Hilb}(S^B((S_B)_{<42} \cup \{f\}), t) - \mathrm{Hilb}(S^B(S_B)_{<42}, t)$$

is equal neither to $t^{42}\,\mathrm{Hilb}(\mathbb{F}_4[f_3, f_{48}], t)$ nor to $t^{42}\,\mathrm{Hilb}(\mathbb{F}_4[f_{12}, f_{48}], t)$. Thus, there are no suitable choices for these elements of M_2, M_3.

Remark 5.17. Question 5.9 is reminiscent of the *Landweber–Stong conjecture* [22] in modular invariant theory, proven for the case when $q = p$ is prime by Bourguiba and Zarati [6].

Conjecture 5.18 (Landweber and Stong). *For a subgroup H of $\mathrm{GL}_n(\mathbb{F}_q)$ acting on $S = \mathbb{F}_q[\boldsymbol{x}]$, the depth of the H-invariant ring S^H is the maximum i for which the elements $D_{n,n-i}, D_{n,n-i+1}, \ldots, D_{n,n-2}, D_{n,n-1}$ form a regular sequence on S^H.*

6. Comparing two representations

This section reveals the original motivation for our conjectures, analogous to questions on real and complex reflection groups W, their *parking spaces*, *W-Catalan numbers* and *Fuss–Catalan* generalizations. We refer the reader to [2, 27] for the full story on this analogy (see also § 7.5). Roughly speaking, we start by examining two strikingly similar G-representations, which we shall call the *graded* and *ungraded G-parking spaces.* Parabolic conjecture 1.5 turns out to yield a comparison of their P_α-fixed subspaces.

6.1. The graded and ungraded $\mathrm{GL}_n(\mathbb{F}_q)$-parking spaces

Definition 6.1. For a field $k \supset \mathbb{F}_q$, the *graded parking space* for $G = \mathrm{GL}_n(\mathbb{F}_q)$ over k is

$$Q_k := k \otimes_{\mathbb{F}_q} Q = k[x_1, \ldots, x_n]/(x_1^{q^m}, \ldots, x_n^{q^m}) = S_k/\mathfrak{m}^{[q^m]},$$

where $S_k := k[x_1, \ldots, x_n]$ and $\mathfrak{m} := (x_1, \ldots, x_n)$. The group $G = \mathrm{GL}_n(\mathbb{F}_q) \subset \mathrm{GL}_n(k)$ acts on S_k via linear substitutions, and also on Q_k, just as before. Thus, Q_k is a graded kG-module.

Definition 6.2. For a field $k \supset \mathbb{F}_q$, the *ungraded parking space*

$$k[\mathbb{F}_{q^m}^n] := \mathrm{span}_k\{e_v \colon v \in \mathbb{F}_{q^m}^n\}$$

for G over k is the G-permutation representation on the points of $\mathbb{F}_{q^m}^n$ via the embedding $G = \mathrm{GL}_n(\mathbb{F}_q) \subset \mathrm{GL}_n(\mathbb{F}_{q^m})$, considered as a kG-module. In other words, the element g in $G = \mathrm{GL}_n(\mathbb{F}_q)$ represented by a matrix (g_{ij}) will send the k-basis element e_v indexed by $v = (v_1, \ldots, v_n)$ in $\mathbb{F}_{q^m}^n$ to $g(e_v) = e_{g(v)}$, where $g(v)_i = \sum_{j=1}^n g_{ij} v_j$.

Example 6.3. When $q = 3$, $n = 2$, $m = 1$, the ungraded parking space has the following nine k-basis elements:

$$\begin{Bmatrix} e_{(-1,+1)}, & e_{(0,+1)}, & e_{(+1,+1)}, \\ e_{(-1,0)}, & e_{(0,0)}, & e_{(+1,0)}, \\ e_{(-1,-1)}, & e_{(0,-1)}, & e_{(+1,-1)} \end{Bmatrix}.$$

For example, $-I_{2\times 2}$ in $G = \mathrm{GL}_2(\mathbb{F}_3)$ fixes $e_{(0,0)}$ and swaps the remaining basis elements as follows:

$$\begin{aligned} e_{(-1,0)} &\leftrightarrow e_{(+1,0)}, \\ e_{(-1,+1)} &\leftrightarrow e_{(+1,-1)}, \\ e_{(0,+1)} &\leftrightarrow e_{(0,-1)}, \\ e_{(+1,+1)} &\leftrightarrow e_{(-1,-1)}. \end{aligned}$$

Note that both kG-modules Q_k and $k[\mathbb{F}_{q^m}^n]$ have dimension $(q^m)^n$. Before investigating their further similarities, we first note that they are *not in general isomorphic* for $n \geqslant 2$.

Example 6.4. As in example 6.3, take $q = 3$, $n = 2$, $m = 1$. One can argue that

$$Q_k = k[x_1, x_2]/(x_1^3, x_2^3) \ncong k[\mathbb{F}_3^2]$$

as follows. The action of $G = \mathrm{GL}_2(\mathbb{F}_3)$ commutes with the action of its centre $C = \{\pm I_{2\times 2}\} \cong \mathbb{Z}/2\mathbb{Z}$. Thus, a kG-module isomorphism $Q_k \cong k[\mathbb{F}_3^2]$ would necessarily lead to a $k[G \times C]$-module isomorphism, and hence also kG-module isomorphisms between the C-isotypic subspaces Q_k^- and $k[\mathbb{F}_3^2]^-$, where for $U = Q_k$ or $k[\mathbb{F}_3^2]$ we define

$$U^- := \{u \in U \text{ such that } -I_{2\times 2} \colon u \mapsto -u\}.$$

It therefore suffices to check that these two isotypic subspaces are *not* kG-module isomorphic:

$$\begin{aligned} Q_k^- &= \{f \in Q_k \colon f(-x_1, -x_2) = -f(x_1, x_2)\} \\ &= (Q_k)_1 \oplus (Q_k)_3 \\ &= \mathrm{span}_k\{x_1, x_2\} \oplus \mathrm{span}_k\{x_1^2 x_2, x_1 x_2^2\}, \\ k[\mathbb{F}_3^2]^- &= \{w \in k[\mathbb{F}_3^2] \colon -I_{2\times 2} \colon w \mapsto -w\} \\ &= \mathrm{span}_k\{w_1 := e_{(+1,0)} - e_{(-1,0)},\ w_2 := e_{(0,+1)} - e_{(0,-1)}, \\ &\qquad\qquad w_3 := e_{(+1,+1)} - e_{(-1,-1)},\ w_4 := e_{(-1,+1)} - e_{(+1,-1)}\}. \end{aligned}$$

To argue that $Q_k^- \ncong k[\mathbb{F}_3^2]^-$ as kG-modules, check that

$$u = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

the transvection in G, acts on both the two-dimensional summands $(Q_k)_1$ and $(Q_k)_3$ of Q_k^- via 2×2 Jordan blocks, but it acts on the four-dimensional space $k[\mathbb{F}_3^2]^-$ by fixing w_1 and cyclically permuting $w_2 \mapsto w_3 \mapsto w_4 \mapsto w_2$. This three-cycle action is conjugate to a 3×3 Jordan block when k has characteristic 3.

Although Q_k and $k[\mathbb{F}_{q^m}^n]$ are not *isomorphic* as kG-modules, they do turn out to be *Brauer isomorphic*. This Brauer isomorphism was essentially observed by Kuhn [20] (see remark 6.12).

Definition 6.5. Recall [29, ch. 18] that two finite-dimensional representations U_1, U_2 of a finite group G over a field k are said to be *Brauer isomorphic* as kG-modules, written $U_1 \approx U_2$, if each simple kG-module has the same composition multiplicity in U_1 as in U_2. Equivalently, each *p-regular element* g in G has the same *Brauer character values* $\chi_{U_1}(g) = \chi_{U_2}(g)$.

In fact, when the field extension k of $\mathbb{F}_q$ actually contains $\mathbb{F}_{q^m}$, it is useful to consider an extra cyclic group,

$$C := \mathbb{F}_{q^m}^{\times} \cong \mathbb{Z}/(q^m - 1)\mathbb{Z},$$

acting on both Q_k and $k[\mathbb{F}_{q^m}^n]$ in a way that commutes with the G-actions.

Definition 6.6 (C-action on the graded parking space). When $k \supset \mathbb{F}_{q^m}$, an element γ in $C = \mathbb{F}_{q^m}^{\times}$ acts on $S_k = k[x_1, \dots, x_n]$ by the scalar variable substitution

$$x_i \mapsto \gamma x_i \quad \text{for } i = 1, 2, \dots, n.$$

This C-action preserves $\mathfrak{m}^{[q^m]} = (x_1^{q^m}, \dots, x_n^{q^m})$, so that it descends to a C-action on Q_k. Also this C-action commutes with the action of G, so that Q_k becomes a $k[G \times C]$-module.

Note that the C-action on Q_k depends in a trivial way on the *grading* structure of Q_k: an element γ of $C = \mathbb{F}_{q^m}^{\times}$ scales all elements of a fixed degree d in Q_k by the same scalar γ^d.

Definition 6.7 (C-action on the ungraded parking space). When $k \supset \mathbb{F}_{q^m}$, an element γ in $C = \mathbb{F}_{q^m}^{\times}$ permutes the elements of $\mathbb{F}_{q^m}^n$ via diagonal scalings:

$$v = (v_1, \dots, v_n) \overset{\gamma}{\mapsto} (\gamma v_1, \dots, \gamma v_n).$$

Again this commutes with the permutation action of G on $\mathbb{F}_{q^m}^n$, giving $k[\mathbb{F}_{q^m}^n]$ the structure of a permutation $k[G \times C]$-module.

To understand why the $k[G \times C]$-modules Q_k and $k[\mathbb{F}_{q^m}^n]$ are Brauer isomorphic, we introduce a third object: an ungraded ring R_k that turns out to be a thinly disguised version of $k[\mathbb{F}_{q^m}^n]$.

Definition 6.8. Define an ungraded quotient ring R_k of $S_k = k[x_1, \dots, x_n]$ by

$$R_k := S_k/\mathfrak{n}, \quad \text{where } \mathfrak{n} := (x_1^{q^m} - x_1, \dots, x_n^{q^m} - x_n).$$

As $\mathfrak{n}$ is stable under the $G \times C$-action on S_k, the quotient R_k inherits the structure of a $k[G \times C]$-module.

Proposition 6.9. *When $k \supset \mathbb{F}_{q^m}$, one has a $k[G \times C]$-module isomorphism $R_k \cong k^{\mathbb{F}_{q^m}^n}$, where $k^{\mathbb{F}_{q^m}^n}$ is the ring of all k-valued functions on the finite set $\mathbb{F}_{q^m}^n$ with pointwise addition and multiplication. In particular, R_k is $k[G \times C]$-module isomorphic to the contragredient of $k[\mathbb{F}_{q^m}^n]$, and hence to $k[\mathbb{F}_{q^m}^n]$ itself.*

Proof. The map $S_k \to k^{\mathbb{F}_{q^m}^n}$ that evaluates a polynomial $f(x_1, \ldots, x_n)$ at the points of $\mathbb{F}_{q^m}^n$ is well known to be a surjective ring homomorphism with kernel $\mathfrak{n}$ when $k \supset \mathbb{F}_{q^m}$. This proves most of the assertions. For the last assertion, note that permutation representations are self-contragredient. □

It will turn out that S_k is closely related to R_k via a filtration

$$F_0 \subset F_1 \subset F_2 \subset \cdots \subset R_k, \tag{6.1}$$

where F_i is the image within R_k of polynomials in S_k of degree at most i. Note that $F_i F_j \subset F_{i+j}$, allowing one to define the *associated graded ring*

$$\mathfrak{gr}_F R_k := F_0 \oplus F_1/F_0 \oplus F_2/F_1 \oplus F_3/F_2 \oplus \cdots$$

with multiplication $F_i/F_{i-1} \times F_j/F_{j-1} \to F_{i+j}/F_{i+j-1}$ induced from $F_i \times F_j \to F_{i+j}$.

Proposition 6.10. *When $k \supset \mathbb{F}_{q^m}$, one has a $G \times C$-equivariant isomorphism of graded rings $Q_k \cong \mathfrak{gr}_F R_k$.*

Proof. Consider the k-algebra map φ defined by

$$\left.\begin{aligned} S_k &\xrightarrow{\varphi} \mathfrak{gr}_F R_k \\ x_i &\mapsto \bar{x}_i \in F_1/F_0. \end{aligned}\right\} \tag{6.2}$$

We claim φ surjects: R_k is generated as a k-algebra by the images of $x_1, \ldots, x_n$, so the multiplication map

$$\underbrace{F_1 \times \cdots \times F_1}_{i \text{ factors}} \to F_i$$

is surjective, and hence likewise for the induced multiplication map $F_1/F_0 \times \cdots \times F_1/F_0 \to F_i/F_{i-1}$.

The relation $x_i^{q^m} = x_i$ that holds in R_k shows that $\bar{x}_i^{q^m} = \bar{x}_i = 0$ inside the q^m-graded component F_{q^m}/F_{q^m-1} of $\mathfrak{gr}_F R_k$. Hence, the surjection $S_k \overset{\varphi}{\twoheadrightarrow} \mathfrak{gr}_F R_k$ has $\mathfrak{m}^{[q^m]}$ in its kernel, and descends to a surjection $Q_k \overset{\varphi}{\twoheadrightarrow} \mathfrak{gr}_F R_k$. But all of Q_k, R_k, $\mathfrak{gr}_F R_k$ have dimension $(q^m)^n$, so φ is an isomorphism. Furthermore, it is easily seen to be $G \times C$-equivariant. □

Corollary 6.11. *When $k \supset \mathbb{F}_q$, one has a Brauer isomorphism of kG-modules $Q_k \approx k[\mathbb{F}_{q^m}^n]$. Furthermore, when $k \supset \mathbb{F}_{q^m}$, this is a Brauer isomorphism of $k[G \times C]$-modules.*

Proof. One may assume without loss of generality that $k \supset \mathbb{F}_{q^m}$, as one has Brauer isomorphisms between two kG-modules if and only if the Brauer isomorphism holds after extending scalars to any field containing k.

Then one has a string of $k[G \times C]$-module Brauer isomorphisms and isomorphisms

$$k[\mathbb{F}_{q^m}^n] \cong R_k \approx \mathfrak{gr}_F R_k \cong Q_k$$

derived, respectively, from proposition 6.9, from the filtration defining $\mathfrak{gr}_F R_k$ and from proposition 6.10. □

Remark 6.12. The Brauer isomorphism of kG-modules asserted in corollary 6.11, ignoring the C-action, is essentially a result of Kuhn, as we now explain.

Note that a choice of $\mathbb{F}_q$-vector space basis for $\mathbb{F}_{q^m}$ identifies $\mathbb{F}_{q^m}$ with the length-m row vectors $\mathbb{F}_q^m$, and hence also identifies $\mathbb{F}_{q^m}^n$ with the $n \times m$ matrices $\mathbb{F}_q^{n\times m}$. Hence, the kG-module $k[\mathbb{F}_{q^m}^n]$ is isomorphic to the permutation action of $G = \mathrm{GL}_n(\mathbb{F}_q)$ left-multiplying matrices in $\mathbb{F}_q^{n\times m}$.

Kuhn proved [20, theorem 1.8] via similar filtration methods to ours that, for $k = \mathbb{F}_p$ with p a prime, the quotient ring $Q_k := k[x_1, \dots, x_n]/(x_1^{p^m}, \dots, x_n^{p^m})$ has the same composition factors as the permutation representation $k[\mathbb{F}_p^{n\times m}]$ on the space of $n \times m$ matrices. In fact, he proves this holds not only as kG-modules for $G = \mathrm{GL}_n(\mathbb{F}_p)$, but even as modules over the larger semigroup ring $k[\mathrm{Mat}_n(\mathbb{F}_p)]$ of $n \times n$ matrices, which still acts by linear substitutions on Q_k and acts by matrix left-multiplication on $k[\mathbb{F}_p^{n\times m}]$.

Remark 6.13. (The authors thank N. Kuhn for pointing out the following consequence of conjecture 1.2.) Since the filtration $F = \{F_i\}$ on the ring $R := R_k$ defined in (6.1) is G-stable, it induces a filtration $F^G = \{(F_i)^G\}$ on the G-fixed subring R^G. One has well-defined injective maps $(F_i)^G/(F_{i-1})^G \hookrightarrow F_i/F_{i-1}$, whose images lie in the subspace $(F_i/F_{i-1})^G$. Compiling these injections gives an injective ring homomorphism

$$\mathfrak{gr}_{F^G}(R^G) \hookrightarrow (\mathfrak{gr}_F R)^G. \tag{6.3}$$

Proposition 6.14. *The specialization of conjecture 1.2 to $t = 1$ is equivalent to the injection (6.3) being an isomorphism.*

Thus, conjecture 1.2 implies that the operations of taking G-fixed points and forming the associated graded ring commute when applied to the ungraded parking space R.

Proof of proposition 6.14. Proposition 6.10 shows that $Q \cong \mathfrak{gr}R$, and hence $Q^G \cong (\mathfrak{gr}R)^G$. Thus, the specialization of conjecture 1.2 to $t = 1$ is equivalent to the assertion that

$$\sum_{k=0}^{\min(m,n)} \begin{bmatrix} m \\ k \end{bmatrix}_q = \dim_{\mathbb{F}_q} Q^G = \dim_{\mathbb{F}_q} (\mathfrak{gr}R)^G.$$

On the other hand, theorem 6.16 shows that the sum on the left equals $\dim_{\mathbb{F}_q} R^G$, and hence also equals $\dim_{\mathbb{F}_q} \mathfrak{gr}_{F^G}(R^G)$. Thus, conjecture 1.2 at $t = 1$ asserts that the source and target of the injection (6.3) have the same dimension. □

6.2. P_α-fixed spaces, orbits and parabolic conjecture 1.5

We next compare the P_α-fixed spaces in Q_k and in $k[\mathbb{F}_{q^m}^n]$. Since $k[\mathbb{F}_{q^m}^n]$ is a permutation representation, one can identify its fixed space as

$$k[\mathbb{F}_{q^m}^n]^{P_\alpha} \cong k[P_\alpha \backslash \mathbb{F}_{q^m}^n],$$

where $P_\alpha \backslash \mathbb{F}_{q^m}^n$ is the set of P_α-orbits on $\mathbb{F}_{q^m}^n$. This orbit set $P_\alpha \backslash \mathbb{F}_{q^m}^n$ turns out to be closely related to the mysterious summation in the definition (1.6) of $C_{\alpha,m}(t)$.

Definition 6.15. Let $\beta = (\beta_1, \ldots, \beta_\ell)$ be a weak composition having $|\beta| \leqslant m$, and define its partial sums $B_i = \beta_1 + \beta_2 + \cdots + \beta_i$ as usual. A *$(\beta, m - |\beta|)$-flag* in $\mathbb{F}_{q^m}$ is a tower

$$0 = V_{B_0} \subset V_{B_1} \subset V_{B_2} \subset \cdots \subset V_{B_\ell} \subset \mathbb{F}_{q^m} \tag{6.4}$$

of $\mathbb{F}_q$-subspaces inside $\mathbb{F}_{q^m}$ with $\dim_{\mathbb{F}_q} V_{B_i} = B_i$ for each i.

Let Y_β be the set of $(\beta, m - |\beta|)$-flags in $\mathbb{F}_{q^m}$, whose cardinality is known to be a *q-multinomial coefficient*:

$$|Y_\beta| = \begin{bmatrix} m \\ \beta, m - |\beta| \end{bmatrix}_q := \begin{bmatrix} m \\ \beta, m - |\beta| \end{bmatrix}_{q,t=1} = \frac{\prod_{j=0}^{n-1} (q^n - q^j)}{\prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i - 1} (q^{B_i} - q^{B_{i-1}+j})}.$$

Given a composition α of n, define the set

$$X_\alpha := \bigsqcup_{\substack{\beta:\ \beta \leqslant \alpha, \\ |\beta| \leqslant m}} Y_\beta,$$

which has cardinality given by

$$|X_\alpha| = \sum_{\substack{\beta:\ \beta \leqslant \alpha, \\ |\beta| \leqslant m}} |Y_\beta| = [C_{\alpha,m}(t)]_{t=1}.$$

Theorem 6.16. *The set X_α naturally indexes $P_\alpha \backslash \mathbb{F}_{q^m}^n$. Therefore,*

$$\dim_k k[\mathbb{F}_{q^m}^n]^{P_\alpha} = |P_\alpha \backslash \mathbb{F}_{q^m}^n| = [C_{\alpha,m}(t)]_{t=1}.$$

Proof. Fix $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ and denote its partial sums by $A_i = \alpha_1 + \alpha_2 + \cdots + \alpha_i$ as usual. To any vector $v = (v_1, \ldots, v_n)$ in $\mathbb{F}_{q^m}^n$ one can associate a flag $(V_i)_{i=1}^{\ell}$ in $\mathbb{F}_{q^m}$ defined by $V_i := \mathrm{span}_{\mathbb{F}_q}\{v_1, v_2, \ldots, v_{A_i}\}$. This gives rise to a weak composition $\beta = (\beta_1, \ldots, \beta_\ell)$ with

$$\beta_i = \dim_{\mathbb{F}_q} V_i - \dim_{\mathbb{F}_q} V_{i-1} = \dim_{\mathbb{F}_q} V_i / V_{i-1} \leqslant \alpha_i,$$

where the inequality arises because V_i/V_{i-1} is spanned by the α_i vectors

$$\{v_{A_{i-1}+1}, v_{A_{i-1}+2}, \ldots, v_{A_i}\}.$$

Also one has

$$|\beta| = \dim_{\mathbb{F}_q} \mathrm{span}_{\mathbb{F}_q}\{v_1, v_2, \ldots, v_n\} \leqslant \dim_{\mathbb{F}_q} \mathbb{F}_{q^m} = m.$$

Thus, the flag $(V_i)_{i=1}^{\ell}$ associated to v lies in $Y_\beta \subset X_\alpha$, and this flag is a complete invariant of the P_α-orbit of v: one has $P_\alpha v = P_\alpha v'$ if and only if $V_i = V_i'$ for $i = 1, 2, \ldots, \ell$. This gives a bijection $P_\alpha \backslash \mathbb{F}_{q^m}^n \to X_\alpha$. □

Remark 6.17. When $\alpha = (n)$ so that $P_\alpha = G = \mathrm{GL}_n(\mathbb{F}_q)$, the analysis of the G-orbits $G \backslash \mathbb{F}_{q^m}^n$ just given in theorem 6.16 is closely related to Kuhn's analysis in [20, § 5, corollary 5.3] (see also remark 6.12).

Something even more striking is true regarding the action of the cyclic group $C = \mathbb{F}_{q^m}^\times$ on the set of flags X_α inside $\mathbb{F}_{q^m}$. Fix a multiplicative generator γ for $C = \langle\gamma\rangle = \mathbb{F}_{q^m}^\times$, so γ has multiplicative order $q^m - 1$. Also fix a primitive $(q^m - 1)$st root of unity ζ in $\mathbb{C}^\times$. For an element γ^d in C, denote its fixed subset by

$$(X_\alpha)^{\gamma^d} := \{x \in X_\alpha \colon \gamma^d(x) = x\}.$$

Proposition 6.18. *For any composition α and integer d, one has*

$$|(X_\alpha)^{\gamma^d}| = [C_{\alpha,m}(t)]_{t=\zeta^d}.$$

In other words, the triple $(X_\alpha, C_{\alpha,m}(t), C)$ exhibits a cyclic sieving phenomenon in the sense of [26].

Proof. It follows from [26, theorem 9.4] that for a weak composition β with $|\beta| \leqslant m$ and integer d one has

$$|(Y_\beta)^{\gamma^d}| = \begin{bmatrix} m \\ \beta, m - |\beta| \end{bmatrix}_{q,t=\zeta^d}.$$

So, by (1.6), it suffices to show $(Y_\beta)^{\gamma^d} \neq \emptyset$ implies that $[t^{e(m,\alpha,\beta)}]_{t=\zeta^d} = 1$.

One checks this as follows. Let r be the multiplicative order of γ^d within $C = \mathbb{F}_{q^m}^\times$, and of ζ^d within $\mathbb{C}^\times$. One knows that $\mathbb{F}_q(\gamma^d) = \mathbb{F}_{q^\ell}$ for some divisor ℓ of m with the property that r divides $q^\ell - 1$. Then any $(\beta, m - |\beta|)$-flag of $\mathbb{F}_q$-subspaces in $\mathbb{F}_{q^m}$ stabilized by γ^d must actually be a flag of $\mathbb{F}_q(\gamma^d)$-subspaces, and hence a flag of $\mathbb{F}_{q^\ell}$-subspaces. Therefore, ℓ must divide each partial sum B_i for $i = 1, 2, \dots, \ell$. As ℓ also divides m, this means that ℓ divides each $m - B_i$, so that $q^\ell - 1$ divides each $q^{m-B_i} - 1$, and hence $q^\ell - 1$ divides each $q^m - q^{B_i} = q^{B_i}(q^{m-B_i} - 1)$. This means that r will also divide each $q^m - q^{B_i}$, so that r divides $e(m, \alpha, \beta)$, and $[t^{e(m,\alpha,\beta)}]_{t=\zeta^d} = 1$ as desired. □

One can reinterpret proposition 6.18 in the following fashion.

Proposition 6.18′. *Parabolic conjecture 1.5 implies that for any field $k \supset \mathbb{F}_{q^m}$, one has a kC-module isomorphism of the P_α-fixed spaces*

$$Q_k^{P_\alpha} \cong k[\mathbb{F}_{q^m}^n]^{P_\alpha}. \tag{6.5}$$

Proof. Note that $|C| = q^m - 1$ is relatively prime to the characteristic of $k \supset \mathbb{F}_q$, and hence kC is semisimple. Thus, it suffices to check that $Q_k^{P_\alpha}$ and $k[\mathbb{F}_{q^m}^n]^{P_\alpha}$ have the same kC-module Brauer characters. Recall [29, § 18.1] that to compute these Brauer characters, one starts by fixing an embedding of cyclic groups

$$C = \mathbb{F}_{q^m}^\times = \langle\gamma\rangle \to \mathbb{C}^\times$$
$$\gamma^d \mapsto \zeta^d, \quad \text{where } \zeta := \exp\left\{\frac{2\pi \mathrm{i}}{q^m - 1}\right\}.$$

Then, whenever an element γ^d in C acts in some r-dimensional $\mathbb{F}_{q^m}C$-module U with multiset of eigenvalues $(\gamma^{i_1}, \dots, \gamma^{i_r})$, its Brauer character value on U is defined to be

$$\chi_U(\gamma^d) := \zeta^{i_1} + \cdots + \zeta^{i_r}.$$

To compute Brauer character values on $Q_k^{P_\alpha}$, recall from definition 6.6 that the element γ^d in C acting on this graded vector space will scale the eth homogeneous component by $(\gamma^d)^e$. Hence,

$$\chi_{Q_k^{P_\alpha}}(\gamma^d) = [\mathrm{Hilb}(Q_k^{P_\alpha}, t)]_{t=\zeta^d}. \tag{6.6}$$

To compute the Brauer character values on $k[\mathbb{F}_{q^m}^n]^{P_\alpha}$, note that, since $k[\mathbb{F}_{q^m}^n]$ is a permutation representation of $P_\alpha \times C$, its P_α-fixed space $k[\mathbb{F}_{q^m}^n]^{P_\alpha}$ is isomorphic to the permutation representation of C on the set of P_α-orbits on $P_\alpha \backslash \mathbb{F}_{q^m}^n$. Equivalently, by theorem 6.16, this is the permutation representation of C on X_α. For a *permutation* representation of a finite group, it is easily seen that its Brauer character value for a (p-regular) element is its usual ordinary complex character value, i.e. its number of fixed points. Hence, the Brauer character value for γ^d when acting on $k[\mathbb{F}_{q^m}^n]^{P_\alpha}$ is $|(X_\alpha)^{\gamma^d}|$. Comparing this value with (6.6), and assuming parabolic conjecture 1.5, one finds that proposition 6.18 exactly asserts that the two kC-modules in (6.5) have the same Brauer characters. □

7. Further questions and remarks

7.1. The two limits where t, q go to 1

In [25, (1.3)], it was noted that two different kinds of limits applied to the (q,t)-binomials yield the same answer after swapping q and t, namely

$$\lim_{t\to 1} \begin{bmatrix} n \\ k \end{bmatrix}_{q,t} = \begin{bmatrix} n \\ k \end{bmatrix}_q \quad \text{and} \quad \lim_{q\to 1} \begin{bmatrix} n \\ k \end{bmatrix}_{q,t^{1/(q-1)}} = \begin{bmatrix} n \\ k \end{bmatrix}_t .$$

One can similarly apply these two kinds of limits to $C_{n,m}(t)$, giving two somewhat different answers:

$$\lim_{t\to 1} C_{n,m}(t) = \sum_{k=0}^{\min(n,m)} \begin{bmatrix} m \\ k \end{bmatrix}_q , \tag{7.1}$$

$$\lim_{q\to 1} C_{n,m}(t^{1/(q-1)}) = \sum_{k=0}^{\min(n,m)} t^{(n-k)(m-k)} \begin{bmatrix} m \\ k \end{bmatrix}_t . \tag{7.2}$$

The limit (7.1) can be interpreted, via theorem 6.16 for $\alpha = (n)$, as counting $\mathrm{GL}_n(\mathbb{F}_q)$-orbits on $\mathbb{F}_{q^m}^n$. When $m \geqslant n$, it gives the *Galois number* G_n counting all $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$ and studied, for example, by Goldman and Rota [13]. We have no insightful explanation or interpretation for the limit (7.2).

In addition, it is perhaps worth noting two further specializations of (7.2): setting $m = n$ or $m = n-1$ and then taking the limit as $n \to \infty$, one obtains the left-hand sides of the two *Rogers–Ramanujan identities*:

$$\sum_{k=0}^{\infty} \frac{t^{k^2}}{(t;t)_k} = \frac{1}{(t;t^5)_\infty (t^4;t^5)_\infty} \quad \text{and} \quad \sum_{k=0}^{\infty} \frac{t^{k^2+k}}{(t;t)_k} = \frac{1}{(t^2;t^5)_\infty (t^3;t^5)_\infty},$$

where $(x;t)_k := (1-x)(1-tx)\cdots(1-t^{k-1}x)$ and $(x;t)_\infty = \lim_{k\to\infty}(x;t)_k$. We have no explanation for this.

7.2. *G*-fixed divided powers versus *G*-cofixed polynomials

We reformulate conjecture 1.3 slightly.

Setting $V := \mathbb{F}_q^n$, one can regard the symmetric algebra $S = \mathbb{F}_q[x_1, \ldots, x_n] = \mathrm{Sym}(V^*)$ as a *Hopf algebra*, which is graded of *finite type*, meaning that each graded piece S_d is finite-dimensional. Then the *(restricted) dual* Hopf algebra $D(V)$ has as its dth graded piece $D(V)_d = S_d^*$, the $\mathbb{F}_q$-dual vector space to S_d, and naturally carries the structure of a *divided power algebra* on V (see, for example, [1, §§ I.3, I.4]). Consequently, proposition 3.3 implies that the G-fixed space $D(V)_d^G$ is $\mathbb{F}_q$-dual to the G-cofixed space $(S_d)_G$, so that

$$\mathrm{Hilb}(D(V)^G, t) = \mathrm{Hilb}(S_G, t).$$

This means one can regard conjecture 1.3 as being about $\mathrm{Hilb}(D(V)^G, t)$ instead. Since $D(V)^G$ is a subalgebra of the divided power algebra $D(V)$, this suggests the following.

QUESTION 7.1. For $V = \mathbb{F}_q^n$ and $G = \mathrm{GL}_n(\mathbb{F}_q)$, is conjecture 1.3 suggesting a predictable or well-behaved ring structure for the G-fixed subalgebra $D(V)^G$ of the divided power algebra $D(V)$?

The invariant theory literature for finite subgroups of $GL(V)$ acting on divided powers $D(V)$ is much less extensive than the literature for actions on polynomial rings $S = \mathrm{Sym}(V)$, although one finds a few results in [28]. M. Crabb (personal communication, 2013) informs us that, in work with J. Hubbuck and D. Salisbury, some results on the structure of $D(V)^G$ were known to them for $G = \mathrm{GL}_2(\mathbb{F}_p)$ acting on $V = \mathbb{F}_p^2$ with $p = 2, 3$.

7.3. Homotopy theory

Kuhn [20], mentioned in § 6, is part of a large literature relating modular representations of $\mathrm{GL}_n(\mathbb{F}_q)$ and its action on $S = \mathbb{F}_q[x_1, \ldots, x_n]$ to questions about stable splittings in homotopy theory. In this work, an important role is played by a commuting action on S of the mod p Steenrod algebra; some references are [30, ch. 10, 11], [7], the two surveys [33] and [34, § 7] and the papers of Doty and Walker [9–11]. We have not seen how to use these results in attacking parabolic conjectures 1.5 and 1.6.

7.4. Approaches to conjecture 1.2

In approaching conjecture 1.2 we would like an explicit $\mathbb{F}_q$-basis for Q^G, where $Q = S/\mathfrak{m}^{[q^m]}$, in degrees suggested by the (q,t)-binomial summands in (1.2) for $C_{n,m}(t)$. For example, when $m \geqslant n$ one can at least make a reasonable guess about *part* of such a basis that models the $k = n$ summand in (1.2), as follows. It was shown in [25, (5.6)] that

$$\begin{bmatrix} m \\ n \end{bmatrix}_{q,t} = \sum_{(\lambda,a)} t^{\sum_{i=0}^{n-1} a_i(q^n - q^{n-i})},$$

where (λ, a) ranges over all pairs in which $\lambda = (\lambda_1, \ldots, \lambda_n)$ satisfies $m - n \geqslant \lambda_1 \geqslant \cdots \geqslant \lambda_n \geqslant 0$, and $a = (a_0, \ldots, a_{n-1})$ is a tuple of non-negative integers *q-compatible* with λ in the sense that $a_i \in [\delta_i, \delta_i + q^{\lambda_i})$, where $\delta_i := q^{\lambda_{i+1}} + q^{\lambda_{i+1}+1} + \cdots + q^{\lambda_i - 1}$. Thus, one might guess that the images of the monomials

$$\prod_{i=0}^{n-1} D_{n,n-i}^{a_i}$$

as one ranges over the same pairs of (λ, a) form part of an $\mathbb{F}_q$-basis for Q^G, and their $\mathbb{F}_q$-linear independence has been checked computationally for a few small values of n, m and q.

However, one knows that at least *some* of the basis elements accounting for other summands in (1.2) are *not* sums of products of Dickson polynomials $D_{n,i}$, as the natural map $S^G \to Q^G$ is *not* surjective for $n \geqslant 2$. One seems to need recursive constructions that produce invariants in n variables from invariants in $n-1$ variables with predictable effects on the degrees. Currently, we lack such constructions.

Non-surjectivity of $S^G \to Q^G$ appears in another initially promising approach. As $\mathfrak{m}^{[q^m]} = (x_1^{q^m}, \ldots, x_n^{q^m})$ is generated by a regular sequence on S, one has an S-free *Koszul resolution* [23, § XVI.10] for $Q = S/\mathfrak{m}^{[q^m]}$:

$$0 \to S \otimes_{\mathbb{F}} \wedge^n V \to \cdots \to S \otimes_{\mathbb{F}} \wedge^2 V \to S \otimes_{\mathbb{F}} \wedge^1 V \to S \to Q \to 0.$$

Taking G-fixed spaces gives a *complex*, which is generally not exact when $\mathbb{F}_q G$ is not semisimple, but at least contains Q^G at its right end:

$$0 \to (S \otimes_{\mathbb{F}} \wedge^n V)^G \to \cdots \to (S \otimes_{\mathbb{F}} \wedge^2 V)^G \to (S \otimes_{\mathbb{F}} \wedge^1 V)^G \to S^G \to Q^G \to 0. \quad (7.3)$$

A result of Hartmann and Shepler [15, § 6.2] very precisely describes each term $(S \otimes_{\mathbb{F}} \wedge^i V)^G$ in (7.3) as a free S^G-module with explicit S^G-basis elements that are homogeneous with predictable degrees; this is an analogue of a classic result on invariant differential forms for complex reflection groups due to Solomon [31]. Thus, each term $(S \otimes_{\mathbb{F}} \wedge^i V)^G$ has a simple explicit Hilbert series. However, non-exactness means that (7.3) is not a resolution of Q^G, so it does not let us directly compute its Hilbert series.

7.5. Rational Cherednik algebras for $\mathbf{GL}_{\boldsymbol{n}}(\mathbb{F}_{\boldsymbol{q}})$

Section 6 alluded to the considerations that led to conjecture 1.2, coming from the theory of real reflection groups W. When W acts irreducibly on $\mathbb{R}^n$ and on the polynomial algebra $\mathbb{C}[\boldsymbol{x}] = \mathbb{C}[x_1, \ldots, x_n]$, one can define its graded W*-parking space* $\mathbb{C}[\boldsymbol{x}]/(\theta_1, \ldots, \theta_n)$, as a quotient by a certain homogeneous system of parameters $\theta_1, \ldots, \theta_n$ of degree $h+1$ inside $\mathbb{C}[\boldsymbol{x}]$, where h is the *Coxeter number* of W (see [2]).

Replacing W by $G := \mathrm{GL}_n(\mathbb{F}_q)$, we think of $h := q^n - 1$ as the *Coxeter number*, with $x_i^{q^n}$ playing the role of θ_i, and $Q = S/\mathfrak{m}^{q^n}$ playing the role of the graded G-parking space.

In the real reflection group theory, the W-parking space carries the structure of an irreducible finite-dimensional representation $L_c(\mathrm{triv})$ for the *rational Cherednik algebra* $H_c(W)$ with parameter value $c = (h+1)/h$. Here the θ_i span the common kernel of the *Dunkl operators* in $H_c(W)$ when acting on $\mathbb{C}[\boldsymbol{x}] = M_c(\mathrm{triv})$. In addition, the W-fixed space $L_c(\mathrm{triv})^W$ is a graded subspace whose Hilbert series is the W*-Catalan polynomial.*

This explains why we examined the Hilbert series of Q^G in our context. In fact, rational Cherednik algebras $H_c(G)$ for $G = \mathrm{GL}_n(\mathbb{F}_q)$ and their finite-dimensional representations $L_c(\mathrm{triv})$ have been studied by Balagović and Chen [4]. However, their results show that the common kernel of the Dunkl operators in $H_c(G)$ acting on $S = \mathbb{F}_q[\boldsymbol{x}]$ is *not* spanned by $x_1^{q^n}, \ldots, x_n^{q^n}$. In fact, for almost all choices of n and the prime power $q = p^r$, they show [4, theorem 4.10] that it is spanned by $x_1^p, \ldots, x_n^p$, independent of the exponent r.

Can one modify this rational Cherednik theory for G to better fit our setting, and gain insight into Q^G?

Appendix A. Proof of proposition 2.1

We recall here the statement to be proven.

Proposition 2.1. *For any $m \geqslant 0$ and any composition α of n, the power series*

$$\mathrm{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i - 1} \frac{1}{1 - t^{q^{A_i} - q^{A_{i-1}+j}}}$$

is congruent in $\mathbb{Z}[[t]]/(t^{q^m})$ to the polynomial

$$C_{\alpha,m}(t) = \sum_{\substack{\beta:\, \beta \leqslant \alpha, \\ |\beta| \leqslant m}} t^{e(m,\alpha,\beta)} \begin{bmatrix} m \\ \beta, m - |\beta| \end{bmatrix}_{q,t}, \quad e(m, \alpha, \beta) = \sum_{i=1}^{\ell} (\alpha_i - \beta_i)(q^m - q^{B_i}).$$

Fix $m \geqslant 0$. Throughout the proof, '$\equiv$' denotes equivalence in $\mathbb{Z}[[t]]/(t^{q^m})$.

Proof. Given the composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, denote its ith partial sum by $A_i = \alpha_1 + \alpha_2 + \cdots + \alpha_i$ as before. Adopting the convention that $A_0 := 0, A_{\ell+1} := +\infty$, define L to be the largest index in $0 \leqslant L \leqslant \ell$ for which $A_L \leqslant m$, so that $A_{L+1} > m$. Part of the relevance of the index L comes from the truncation to the first L factors in the product formula

$$\mathrm{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}})^{-1} \equiv \prod_{i=1}^{L} \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}})^{-1}, \quad \text{(A 1)}$$

where the last equivalence is justified as follows. As q is a prime power, one has $q \geqslant 2$. Thus, for integers a, b, c, one has

$$a > b, c \quad \Longrightarrow \quad q^a - q^b - q^c \geqslant q^a - 2q^{a-1} = (q-2)q^{a-1} \geqslant 0. \quad \text{(A 2)}$$

In particular, $q^{A_i} - q^{A_{i-1}+j} \geqslant q^{A_i - 1} \geqslant q^m$ for all $i \geqslant L+1$. Thus, all of the factors in (A 1) with $i > L$ are equivalent to 1 modulo (t^{q^m}).

We shall make frequent use of (A 2); for example, it helps to prove the following lemma, which shows that most summands of $C_{\alpha,m}(t)$ in (1.6) vanish in $\mathbb{Z}[[t]]/(t^{q^m})$.

Lemma A.1. *Given m and α, with A_i and L defined as above, the weak compositions $\beta = (\beta_1, \ldots, \beta_\ell)$ with $0 \leqslant \beta \leqslant \alpha$ and $|\beta| \leqslant m$ for which $e(m, \alpha, \beta) < q^m$ are exactly those of the following two forms: either*

$$\beta = \hat{\alpha} := \begin{cases} \alpha & \text{if } L = \ell, \\ (\alpha_1, \ldots, \alpha_L, m - A_L, 0, \ldots, 0) & \text{otherwise,} \end{cases}$$

or, for $k = 1, 2, \ldots, L$,

$$\begin{aligned} \beta &= \hat{\alpha}^{(k)} \\ &:= \begin{cases} (\alpha_1, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_\ell) & \text{if } L = \ell, \\ (\alpha_1, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_L, m - A_L + 1, 0, \ldots, 0) & \text{otherwise.} \end{cases} \end{aligned}$$

In the former case, $e(m, \alpha, \beta) = 0$, and in the latter, $e(m, \alpha, \beta) = q^m - q^{A_k - 1}$.

Proof of lemma A.1. Assume $\beta = (\beta_1, \ldots, \beta_\ell)$ has $0 \leqslant \beta \leqslant \alpha$ with $|\beta| \leqslant m$, and that $e(m, \alpha, \beta) < q^m$. As before, let $B_i = \beta_1 + \beta_2 + \cdots + \beta_i$ for $i = 0, 1, \ldots, \ell + 1$, with conventions $B_0 := 0$ and $B_{\ell+1} := m$. By (A 2), the condition $e(m, \alpha, \beta) < q^m$ implies that at most one summand in $e(m, \alpha, \beta)$ may be non-zero, and if the ith summand $(\alpha_i - \beta_i)(q^m - q^{B_i})$ is non-zero, then $\alpha_i - \beta_i = 1$. Choose j minimal so that $0 \leqslant j \leqslant \ell + 1$ and $B_j = m$. We consider two cases, depending on whether or not $e(m, \alpha, \beta) = 0$.

Case 1 ($e(m, \alpha, \beta) = 0$). In this case all summands in $e(m, \alpha, \beta)$ are zero, so $\beta_i = \alpha_i$ for all $i < j$. If $j = \ell + 1$, then it follows immediately that $\beta = \alpha = \hat{\alpha}$. Otherwise, $j \leqslant \ell$. Since $B_j = m$ but $A_i = B_i < m$ for $i < j$, we have $j = L$. Therefore, $\beta = (\alpha_1, \ldots, \alpha_L, m - A_L, 0, \ldots, 0) = \hat{\alpha}$ in this case.

Case 2 ($e(m, \alpha, \beta) > 0$). In this case there is an index k such that $k < j$ and $\alpha_i - \beta_i = 1$, and for all other $i < j$ we have $\beta_i = \alpha_i$. If $j = \ell + 1$, then it follows immediately that $\beta = (\alpha_1, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_\ell) = \hat{\alpha}^{(k)}$. Otherwise, $j \leqslant \ell$. Since $B_j = m$ but $A_i \leqslant B_i + 1 \leqslant m$ for $i < j$, we have $j = L$. Therefore, $\beta = (\alpha_1, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_L, m - A_L + 1, 0, \ldots, 0) = \hat{\alpha}^{(k)}$ in this case. □

Returning to the proof of proposition 2.1, note that lemma A.1 implies

$$C_{\alpha,m}(t) \equiv \begin{bmatrix} m \\ \hat{\alpha} \end{bmatrix}_{q,t} + \sum_{k=1}^{L} t^{q^m - q^{A_k - 1}} \begin{bmatrix} m \\ \hat{\alpha}^{(k)} \end{bmatrix}_{q,t}. \tag{A 3}$$

We next process the summands on the right. By definition, one has that

$$t^{q^m - q^{A_k - 1}} \begin{bmatrix} m \\ \hat{\alpha}^{(k)} \end{bmatrix}_{q,t} = t^{q^m - q^{A_k - 1}} \prod_{j=0}^{A_L - 1} (1 - t^{q^m - q^j}) \Big/ \prod_{i=1}^{L} \prod_{j=0}^{\hat{\alpha}_i^{(k)} - 1} (1 - t^{q^{\hat{A}_i^{(k)}} - q^{\hat{A}_{i-1}^{(k)} + j}}),$$

where here $\hat{A}_i^{(k)} := \hat{\alpha}_1^{(k)} + \cdots + \hat{\alpha}_i^{(k)}$ as usual. We shall attempt to simplify the fraction on the right-hand side, working $\mathrm{mod}(t^{q^m})$. Note that in its numerator, only $t^{q^m - q^{A_k - 1}}$ survives, as (A 2) implies $(q^m - q^{A_k - 1}) + (q^m - q^j) \geqslant q^m$. Meanwhile, in its denominator, only the factors indexed by $i = 1, 2, \ldots, k$ survive multiplication by $t^{q^m - q^{A_k - 1}}$ when working mod(t^{q^m}): since $\hat{A}_i^{(k)} \geqslant A_k$ for $i \geqslant k+1$, (A 2) implies

$$(q^m - q^{A_k - 1}) + (q^{\hat{A}_i^{(k)}} - q^{\hat{A}_{i-1}^{(k)}+j}) \geqslant q^m.$$

Thus, one has

$$\begin{aligned} t^{q^m - q^{A_k - 1}} \begin{bmatrix} m \\ \hat{\alpha}^{(k)} \end{bmatrix}_{q,t} &\equiv t^{q^m - q^{A_k - 1}} \prod_{i=1}^{k} \prod_{j=0}^{\hat{\alpha}_i^{(k)} - 1} (1 - t^{q^{\hat{A}_i^{(k)}} - q^{\hat{A}_{i-1}^{(k)}+j}})^{-1} \\ &= \biggl(\prod_{i=1}^{k-1} \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}})^{-1} \biggr) \\ &\qquad \times t^{q^m - q^{A_k - 1}} \prod_{j=0}^{\alpha_k - 2} (1 - t^{q^{A_k - 1} - q^{A_{k-1}+j}})^{-1}. \end{aligned}$$

Using (A 2), the last, unparenthesized factor is equivalent mod(t^{q^m}) to

$$t^{q^m - q^{A_k - 1}} + \sum_{j=0}^{\alpha_k - 2} t^{q^m - q^{A_{k-1}+j}} = \sum_{j=0}^{\alpha_k - 1} t^{q^m - q^{A_{k-1}+j}}.$$

Consequently, one has

$$t^{q^m - q^{A_k - 1}} \begin{bmatrix} m \\ \hat{\alpha}^{(k)} \end{bmatrix}_{q,t} \equiv \biggl(\sum_{j=0}^{\alpha_k - 1} t^{q^m - q^{A_{k-1}+j}} \biggr) \bigg/ \prod_{i=1}^{k-1} \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}}). \quad \text{(A 4)}$$

Similarly, one finds that

$$\begin{bmatrix} m \\ \hat{\alpha} \end{bmatrix}_{q,t} = \prod_{j=0}^{A_L - 1} (1 - t^{q^m - q^j}) \bigg/ \prod_{i=1}^{L} \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}}). \quad \text{(A 5)}$$

The numerator on the right-hand side of (A 5) can be rewritten mod(t^{q^m}) using (A 2) as

$$\prod_{j=0}^{A_L - 1} (1 - t^{q^m - q^j}) \equiv 1 - \sum_{j=0}^{A_L - 1} t^{q^m - q^j} = 1 - \sum_{k=1}^{L} \sum_{j=0}^{\alpha_k - 1} t^{q^m - q^{A_{k-1}+j}}.$$

Comparing this with (A 1) shows that

$$\begin{aligned} \begin{bmatrix} m \\ \hat{\alpha} \end{bmatrix}_{q,t} &= \operatorname{Hilb}(S^{P_\alpha}, t) - \sum_{k=1}^{L} \biggl(\sum_{j=0}^{\alpha_k - 1} t^{q^m - q^{A_{k-1}+j}} \biggr) \bigg/ \prod_{i=1}^{L} \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}}) \\ &\equiv \operatorname{Hilb}(S^{P_\alpha}, t) - \sum_{k=1}^{L} \biggl(\sum_{j=0}^{\alpha_k - 1} t^{q^m - q^{A_{k-1}+j}} \biggr) \bigg/ \prod_{i=1}^{k-1} \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}}). \end{aligned} \quad \text{(A 6)}$$

The last equivalence $\bmod(t^{q^m})$ arises since if $i \geqslant k$, then $A_i \geqslant A_k$, so

$$(q^m - q^{A_{k-1}+j}) + (q^{A_i} - q^{A_{i-1}+j}) \geqslant q^m$$

by (A 2). Finally, combining (A 3), (A 4) and (A 6) shows that

$$C_{\alpha,m}(t) \equiv \mathrm{Hilb}(S^{P_\alpha}, t),$$

as desired. □

Appendix B. Proofs in the bivariate case

Our goal here is to prove parabolic conjectures 1.5 and 1.6 for $n = 2$. Their equivalence for $n = 2$ was shown in corollary 3.6, so we only prove parabolic conjecture 1.6.

The group $G = \mathrm{GL}_2(\mathbb{F}_q)$ has only two parabolic subgroups P_α, namely the whole group $G = P_{(2)}$ itself and the Borel subgroup $B = P_{(1,1)}$. We establish parabolic conjecture 1.6 for these subgroups in theorems B.15 and B.10, respectively.

We consider the chain of subgroups

$$1 \subset T \subset B \subset G \tag{B 1}$$

where

$$T = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a, d \in \mathbb{F}_q^\times \right\},$$
$$B = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, d \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\},$$
$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \in \mathbb{F}_q^\times \right\}.$$

We first recall the known descriptions of the invariant subrings for each of these subgroups, and then prove some preliminary facts about their cofixed quotients. Using this, we complete our analysis first for the quotient S_B, and then for the quotient S_G.

B.1. The invariant rings

Acting on $S = \mathbb{F}_q[x, y]$, the tower of subgroups (B 1) induces a tower of invariant subalgebras $S \supset S^T \supset S^B \supset S^G$, with the following explicit descriptions. Abbreviate $X := x^{q-1}, Y := y^{q-1}$, and recall from § 1 that for $n = 2$ the two Dickson polynomials $D_{2,0}, D_{2,1}$ are defined by

$$\prod_{(c_1,c_2)\in\mathbb{F}_q^2} (t + c_1 x + c_2 y) = t^{q^2} + D_{2,1}t^q + D_{2,0}t. \tag{B 2}$$

Proposition B.1. *For* $S = \mathbb{F}_q[x, y]$ *one has*

(i) $S^T = \mathbb{F}_q[X, Y]$,

(ii) $S^B = \mathbb{F}_q[X, D_{2,1}]$ *and*

(iii) $S^G = \mathbb{F}_q[D_{2,0}, D_{2,1}]$, *with explicit formulae*

$$\begin{aligned} D_{2,1} &= Y^q + XY^{q-1} + \cdots + X^{q-1}Y + X^q, \\ D_{2,0} &= XY^q + X^2Y^{q-1} + \cdots + X^qY = XD_{2,1} - X^{q+1}. \end{aligned}$$

Proof. Assertion (i) is straightforward. Assertion (ii) follows from the work of Mui [24] or Hewett [16]. Assertion (iii) is Dickson's theorem [8] for $n = 2$. The last two equalities follow from Dickson's expressions

$$\left.\begin{aligned} D_{2,1} &= \begin{vmatrix} x & y \\ x^{q^2} & y^{q^2} \end{vmatrix} \Bigg/ \begin{vmatrix} x & y \\ x^q & y^q \end{vmatrix} \\ &= \frac{xy^{q^2} - x^{q^2}y}{xy^q - x^qy} = Y^q + XY^{q-1} + \cdots + X^{q-1}Y + X^q, \\ D_{2,0} &= \begin{vmatrix} x^q & y^q \\ x^{q^2} & y^{q^2} \end{vmatrix} \Bigg/ \begin{vmatrix} x & y \\ x^q & y^q \end{vmatrix} \\ &= \frac{x^qy^{q^2} - x^{q^2}y^q}{xy^q - x^qy} = XY^q + X^2Y^{q-1} + \cdots + X^qY, \end{aligned}\right\} \qquad \text{(B 3)}$$

for the $D_{n,i}$ as quotients of determinants. □

B.2. The cofixed spaces

The tower of subgroups in (B 1) induces quotient maps $S \twoheadrightarrow S_T \twoheadrightarrow S_B \twoheadrightarrow S_G$. The quotient map $S \twoheadrightarrow S_T$ is easily understood.

Proposition B.2. *A monomial x^iy^j in S survives in the T-cofixed space S_T if and only if $q-1$ divides both i and j, i.e. if and only if $x^iy^j = X^{i'}Y^{j'}$ for some i', j'. Furthermore, these monomials $\{X^iY^j\}_{i,j\geqslant 0}$ form an $\mathbb{F}_q$-basis for S_T.*

Proof. Proposition 5.1(iv) implies that S_T is the quotient of S by the $\mathbb{F}_q$-subspace spanned by all elements $t(x^iy^j) - x^iy^j$. A typical element t in T sends $x \mapsto c_1x$ and $y \mapsto c_2y$ for some c_1, c_2 in $\mathbb{F}_q^\times$. Therefore,

$$t(x^iy^j) - x^iy^j = (c_1^ic_2^j - 1)x^iy^j.$$

If both i and j are divisible by $q-1$, then this will always be zero, and otherwise, there exist choices of c_1, c_2 for which it is a non-zero multiple of x^iy^j. □

In understanding the quotients S_P, S_G, it helps to define two $\mathbb{F}_q$-linear functionals on S that descend to one or both of S_P, S_G. They will be used in the proof of corollary B.6 to detect certain non-zero products.

Definition B.3. Define two $\mathbb{F}_q$-linear functionals $S \xrightarrow{\mu,\nu} \mathbb{F}_q$ by setting $\mu(x^iy^j) = \nu(x^iy^j) = 0$ unless $q-1$ divides both i, j, and setting

$$\mu(X^iY^j) = \begin{cases} 1 & \text{if } i, j \geqslant 1, \\ 0 & \text{if } i = 0 \text{ or } j = 0 \end{cases}$$

and

$$\nu(X^iY^j) = \begin{cases} 1 & \text{if } i = 0, \\ 0 & \text{if } i \geqslant 1. \end{cases}$$

In other words, μ applied to $f(x,y)$ sums the coefficients in f on monomials of the form X^iY^j that are not pure powers X^i or Y^j, while ν sums the coefficients on the pure Y-powers Y^j. It should be clear from their definitions and proposition B.2 that both μ and ν descend to well-defined $\mathbb{F}_q$-linear functionals on S_T.

Proposition B.4. *One has the following:*

(i) *the functional* $S \xrightarrow{\nu} \mathbb{F}$ *descends to a well-defined functional on* S_B*;*

(ii) *the functional* $S \xrightarrow{\mu} \mathbb{F}$ *descends to a well-defined functional on both* S_B *and* S_G*.*

Proof. The Borel subgroup B is generated by the torus T together with a transvection

$$\left.\begin{aligned} x &\overset{u}{\mapsto} x \\ y &\overset{u}{\mapsto} x + y, \end{aligned}\right\} \tag{B 4}$$

while the full general linear group G is generated by B together with a transposition σ that swaps x, y. Hence, by proposition 5.1(iv), it suffices to check that for every monomial x^iy^j, both μ and ν vanish on

$$u(x^iy^j) - x^iy^j = \sum_{k=0}^{j-1} \binom{j}{k} x^{i+j-k} y^k \tag{B 5}$$

and that μ vanishes on

$$\sigma(x^iy^j) - x^iy^j = x^jy^i - x^iy^j. \tag{B 6}$$

The fact that μ vanishes on (B 6) is clear from the symmetry between X and Y in its definition.

To see that ν vanishes on (B 5), observe that ν vanishes on every monomial $x^{i+j-k}y^k$ appearing in the sum, as $k < j$ means it is never a pure power of y (or Y).

To see that μ vanishes on (B 5), we do a calculation. Applying μ to the right-hand side gives

$$\sum_{k=0}^{j-1} \binom{j}{k} \mu(x^{i+j-k}y^k) = \sum_{\substack{k=1,2,\ldots,j-1, \\ q-1 \mid k}} \binom{j}{k}, \tag{B 7}$$

which equals the sum (in $\mathbb{F}_q$) of the coefficients on the monomials of the form $x^{\ell(q-1)}$ within the polynomial

$$f(x) := \sum_{k=1}^{j-1} \binom{j}{k} x^k = (x+1)^j - (x^j + 1).$$

One can then advantageously rewrite (B 7) by taking advantage of a root of unity fact:

$$\sum_{\beta \in \mathbb{F}_q^\times} \beta^k = \begin{cases} q-1=-1 & \text{if } k=\ell(q-1) \text{ for some } \ell \in \mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases}$$

Noting also that $f(0)=0$, this lets one rewrite the right-hand side of (B 7) as

$$\begin{aligned} -\sum_{\beta \in \mathbb{F}_q^\times} f(\beta) = -\sum_{\beta \in \mathbb{F}_q} f(\beta) &= -\sum_{\beta \in \mathbb{F}_q} (\beta+1)^j + \sum_{\beta \in \mathbb{F}_q} \beta^j + \sum_{\beta \in \mathbb{F}_q} 1 \\ &= -\sum_{\beta \in \mathbb{F}_q} \beta^j + \sum_{\beta \in \mathbb{F}_q} \beta^j + q \\ &= 0. \end{aligned}$$

□

The following technical lemma on vanishing and equalities lies at the heart of our analysis of S_B, S_G.

Lemma B.5. *Beyond the vanishing in S_T of monomials except for $\{X^iY^j\}_{i,j \geqslant 0}$, in the further quotient S_B one also has*

(i) $X^i = 0$ *for all* $i \geqslant 1$,

(ii) $X^iY^j = X^{i'}Y^{j'}$ *for all* $i, i' \geqslant 1$ *and* $1 \leqslant j, j' \leqslant q$ *if* $i+j = i'+j'$.

In the even further quotient S_G, one additionally has

(iii) $Y^j = 0$ *for all* $j \geqslant 1$, *and*

(iv) $X^iY^j = X^{i'}Y^{j'}$ *for all* $i, i', j, j' \geqslant 1$ *with* $i+j = i'+j' \leqslant 2q$.

Proof. For (i), since B contains the transvection u from (B 4), one has in S_B for any $k > 0$ that

$$0 \equiv u(x^{k-1}y) - x^{k-1}y = x^{k-1}(x+y) - x^{k-1}y = x^k.$$

Hence, $X^i = x^{i(q-1)}$ vanishes in S_B for all $i > 0$.

For (ii), we claim that it suffices to show that whenever $i, j \geqslant 1$ and $2 \leqslant j \leqslant q$, one can express X^iY^j as a sum of $X^{i'}Y^{j'}$ having $i+j = i'+j'$ and $j' < j$: then all such monomials X^iY^j will be scalar multiples of each other, but they all take the same value 1 when one applies the functional μ from definition B.3 and proposition B.4, so they must all be equal.

To this end, let $d := (i+j)(q-1) = \deg(X^iY^j)$. Using the transvection u from (B 4), and taking advantage of the vanishing of x^iy^j in S_B unless $q-1$ divides i, j, one has

$$\begin{aligned}
0 &\equiv u(x^{d-(jq-1)}y^{jq-1}) - x^{d-(jq-1)}y^{jq-1}\\
&= x^{d-(jq-1)}(x+y)^{jq-1} - x^{d-(jq-1)}y^{jq-1}\\
&= \left(\sum_{k=0}^{jq-1}\binom{jq-1}{k}x^{d-k}y^k\right) - x^{d-(jq-1)}y^{jq-1}\\
&\equiv \binom{jq-1}{j(q-1)}x^{i(q-1)}y^{j(q-1)} + \sum_{m=0}^{j-1}\binom{jq-1}{m(q-1)}x^{(i+j-m)(q-1)}y^{m(q-1)}\\
&= \binom{jq-1}{j(q-1)}X^iY^j + \sum_{m=0}^{j-1}\binom{jq-1}{m(q-1)}X^{i+j-m}Y^m.
\end{aligned}$$

Thus, it remains only to show that $\binom{jq-1}{j(q-1)} \neq 0$ in $\mathbb{F}_q$ when $1 \leqslant j \leqslant q$. Letting $q = p^s$ for some prime p and exponent $s \geqslant 1$, we have

$$\binom{jq-1}{j(q-1)} = \frac{(jq-1)(jq-2)\cdots(jq-j+1)}{1\cdot 2\cdots(j-1)}. \tag{B 8}$$

For any integers a, b such that $1 \leqslant a \leqslant p^s - 1$ and $b \geqslant 1$, the largest power of p dividing $b\cdot p^s - a$ is equal to the largest power of p dividing a. Since $j \leqslant q$, it follows that the largest power of p dividing the numerator of the right-hand side of (B 8) is equal to the largest power of p dividing the denominator, so $\binom{jq-1}{j(q-1)} \neq 0$ in $\mathbb{F}_q$.

For (iii), note that, since (i) implies X^i vanishes in S_B, the same vanishing holds in the further quotient S_G. But then Y^i also vanishes in S_G by applying the transposition σ in G swapping x and y.

For (iv), note that (ii) shows that, fixing $d := i + j$, all monomials X^iY^j with $i, j \geqslant 1$ and $j \leqslant q$ are equal in S_B, and hence also equal in the further quotient S_G. Applying the transposition σ as before, one concludes that these monomials are also all equal to the monomials X^iY^j with $i, j \geqslant 1$ and $i \leqslant q$. But when $d = i + j \leqslant 2q$ these two sets of monomials exhaust all of the possibilities for X^iY^j with $i, j \geqslant 1$. □

The following corollary will turn out to be a crucial part of the structure of S_G as an S^G-module in the bivariate case, used in the proof of theorem B.15.

Corollary B.6. *In the G-fixed quotient space S_G, the images of the monomials*

$$\{1, XY, X^2Y, \ldots, X^{q-2}Y\} \tag{B 9}$$

are all annihilated by $D_{2,0}$, but none of them is annihilated by any power of $D_{2,1}$.

Proof. Proposition B.1 shows that $D_{2,0}$ is a sum of q monomials of the form X^iY^j with $i, j \geqslant 1$. The same is true for the product $D_{2,0} \cdot M$, where M is any of the monomials in (B 9). Since these monomials M have degree at most $(q-1)^2$, the product $D_{2,0}\cdot M$ has degree at most $q^2-1+(q-1)^2 = 2q(q-1)$, and hence all q of the monomials in the product are equal to the same monomial M' by lemma B.5(iv). Therefore, $D_{2,0}M \equiv qM' = 0$ in S_G, as desired.

Proposition B.1 shows that $D_{2,1} = Y^q + XY^{q-1} + \cdots + X^{q-1}Y + X^q$, a sum of $q+1$ monomials. Hence, for $j \geqslant 0$, the power $D_{2,1}^j$ is a sum of $(q+1)^j$ monomials, of the form

$$D_{2,1}^j = Y^{qj} + \Biggl(\sum_{i,j \geqslant 1} c_{i,j} X^i Y^j \Biggr) + X^{qj}$$

with $\sum_{i,j\geqslant 1} c_{i,j} = (q+1)^j - 2$. Thus, the $\mathbb{F}_q$-linear functional μ from definition B.3 and proposition B.4 has

$$\mu(D_{2,1}^j \cdot 1) = \mu(D_{2,1}^j) = (q+1)^j - 2 = 1^j - 2 = -1 \neq 0,$$

while for any of the rest of the monomials $M = X^iY$ with $i \geqslant 1$ in (B 9), it has

$$\mu(D_{2,1} \cdot M) = (q+1)^j = 1^j = 1 \neq 0.$$

Thus, no power $D_{2,1}^j$ annihilates any of the monomials in (B 9) within S_G. □

B.3. Analysing the fixed quotient S_B for the Borel subgroup $B = P_{(1,1)}$

One can regard the polynomial algebra S with its B-action as a module for the group algebra $S^B[B]$ having coefficients in the B-invariant subalgebra $S^B = \mathbb{F}_q[D_{2,1}, X]$. We begin by describing the $S^B[B]$-module structure on S, and thereby deduce the S^B-module structure on the B-cofixed space S_B. For this purpose, we borrow an idea from Karagueuzian and Symonds [17, § 2.1].

Definition B.7. Let $\hat{S}$ be the $\mathbb{F}_q$-subspace of S spanned by the monomials

$$\{x^i y^j : 0 \leqslant j \leqslant q^2 - q\}.$$

It is easily seen that $\hat{S}$ is stable under the action of B, and also under multiplication by x and so, by its B-invariant power, $X = x^{q-1}$, so that $\hat{S}$ becomes an $\mathbb{F}_q[X][B]$-module. Thus, the tensor product

$$\mathbb{F}_q[D_{2,1}] \otimes_{\mathbb{F}_q} \hat{S}$$

is naturally a module for the ring

$$\mathbb{F}_q[D_{2,1}] \otimes_{\mathbb{F}_q} \mathbb{F}_q[X][B] \cong \mathbb{F}_q[D_{2,1}, X][B] = S^B[B]$$

via the tensor product action

$$(a \otimes c)(b \otimes d) = ab \otimes cd$$

for any elements

$$a, b \in \mathbb{F}_q[D_{2,1}], \quad c \in \mathbb{F}_q[X][B] \quad \text{and} \quad d \in \hat{S}.$$

Proposition B.8 (Karagueuzian and Symonds [17, lemma 2.5]). *The multiplication map*

$$\begin{aligned} \mathbb{F}_q[D_{2,1}] \otimes_{\mathbb{F}_q} \hat{S} &\to S \\ f_1 \otimes f_2 &\mapsto f_1 f_2 \end{aligned}$$

induces an $S^B[B]$*-module isomorphism. Hence, as a module over* $S^B = \mathbb{F}_q[D_{2,1}, X]$*, one has an isomorphism*

$$\mathbb{F}_q[D_{2,1}] \otimes_{\mathbb{F}_q} \hat{S}_B \cong S_B.$$

Proof. The multiplication map is easily seen to be a morphism of $S^B[B]$-modules, so it remains only to check that it is an $\mathbb{F}_q$-vector-space isomorphism. This follows by iterating a direct sum decomposition

$$D_{2,1}S_d \oplus \hat{S}_{d+q^2-q} = S_{d+q^2-q} \tag{B 10}$$

justified for $d \geqslant 0$ as follows. The leftmost summand $D_{2,1}S_d$ in (B 10) has as $\mathbb{F}_q$-basis the set $\{D_{2,1}x^iy^j\}_{i+j=d}$. Since (B 3) shows that $D_{2,1} = y^{q^2-q} + x^{q-1}y^{q^2-2q+1} + \cdots + x^{q^2-q}$, the leading monomials in y-degree for $D_{2,1}S_d$ are

$$\{x^iy^{j'} : i + j' = d + q^2 - q \text{ and } j' \geqslant q^2 - q\}.$$

Meanwhile the summand $\hat{S}_{d+q^2-q}$ has as $\mathbb{F}_q$-basis the complementary set of monomials

$$\{x^iy^j : i + j = d + q^2 - q \text{ and } j < q^2 - q\}$$

within the set of all monomials $\{x^iy^j : i + j = d + q^2 - q\}$ that form an $\mathbb{F}_q$-basis for S_{d+q^2-q}. □

In analysing S_B, it therefore suffices to analyse $\hat{S}_B$.

Proposition B.9. *Within the quotient space* $\hat{S}_B$*, one has the following.*

(i) $X^iY^j \equiv X^{i+j-1}Y$ *for all* $i \geqslant 1$ *and* $1 \leqslant j \leqslant q-1$.

(ii) *There is an* $\mathbb{F}_q$*-basis*

$$\{Y, XY, X^2Y, X^3Y, \dots\} \cup \{1, Y^2, Y^3, \dots, Y^{q-1}\}. \tag{B 11}$$

(iii) *There is an* $\mathbb{F}_q[X]$*-module direct sum decomposition* $\hat{S}_P = M_1 \oplus M_2$*, where*

- $M_1 = \mathbb{F}_q[X] \cdot Y$ *is a free* $\mathbb{F}_q[X]$*-module on the basis* $\{Y\}$*, and*
- M_2 *is the* $\mathbb{F}_q[X]$*-submodule spanned by*

$$\{1, Y^2 - XY, Y^3 - X^2Y, \dots, Y^{q-1} - X^{q-2}Y\}, \tag{B 12}$$

having $\mathbb{F}_q[X]$*-module structure isomorphic to a direct sum of copies of the quotient module* $\mathbb{F}_q[X]/(X)$ *with the elements of (B 12) as basis.*

Proof.
(i) This follows from lemma B.5(ii).

(ii) We first argue that the monomials in (B 11) span $\hat{S}_B$. By definition B.7, one has that $\hat{S}$ is $\mathbb{F}_q$-spanned by $\{x^iy^j : i \geqslant 0 \text{ and } 0 \leqslant j < q^2 - q\}$. Since monomials other than those of the form X^iY^j vanish in S_T and thus in its further quotient S_B, one concludes that $\hat{S}_B$ is $\mathbb{F}_q$-spanned by

$$\{X^iY^j : i \geqslant 0 \text{ and } 0 \leqslant j < q\}.$$

Table 1.

degree	monomial	μ value	ν value
0	1	0	1
1	Y	0	1
2	XY	1	0
	Y^2	0	1
3	X^2Y	1	0
	Y^3	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$q-1$	$X^{q-2}Y$	1	0
	Y^{q-1}	0	1
q	$X^{q-1}Y$	1	0
$q+1$	$X^{q-2}Y$	1	0
$q+2$	$X^{q-3}Y$	1	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Lemma B.5(i) says that X^i vanishes in S_B for $i \geqslant 1$, so one may discard these monomials and still have a spanning set. Also, assertion (i) of this proposition shows that one may further discard monomials of the form X^iY^j with $i \geqslant 1$ and $j > 1$. Thus, $\hat{S}_B$ is $\mathbb{F}_q$-spanned by

$$\{X^iY\}_{i\geqslant 0} \cup \{Y^j\}_{0\leqslant j\leqslant q-1},$$

which is the same set as in (B 11).

To see that these monomials are $\mathbb{F}_q$-linearly independent in $\hat{S}_B$ or S_B, table 1 shows that they are separated in each degree by the $\mathbb{F}_q$-linear functionals μ and ν on S_B from definition B.3 and proposition B.4.

(iii) First, note that, since $\{Y, XY, X^2Y, X^3Y, \dots\}$ is a subset of an $\mathbb{F}_q$-basis for $\hat{S}_B$, the submodule $M_1 = \mathbb{F}_q[X] \cdot Y$ indeed forms a free $\mathbb{F}_q[X]$-module on the basis $\{Y\}$ inside of $\hat{S}_B$. Since

$$\{1\} \cup \{Y^j\}_{2\leqslant j\leqslant q-1}$$

extends $\{Y, XY, X^2Y, X^3Y, \dots\}$ to an $\mathbb{F}_q$-basis for $\hat{S}_B$, so does the set (B 12):

$$\{1\} \cup \{Y^j - X^{j-1}Y\}_{2\leqslant j\leqslant q-1}.$$

In particular, none of these elements vanish in $\hat{S}_B$, and $\hat{S}_B = M_1 + M_2$, where M_2 is the $\mathbb{F}_q[X]$-span of (B 12). On the other hand, each element of (B 12) is annihilated on multiplication by X: this holds for the monomial 1 since X vanishes in S_B by lemma B.5(i), and it holds for $Y^j - X^{j-1}Y$ with $2 \leqslant j \leqslant q-1$ since $XY^j \equiv X^jY$ in S_B by lemma B.5(ii). Thus, M_2 has (B 12) as an $\mathbb{F}_q$-basis, and its $\mathbb{F}_q[X]$-module structure is that of a free $\mathbb{F}_q[X]/(X)$-module on this same basis. This also shows that one has a *direct* sum $\hat{S}_B = M_1 \oplus M_2$. □

The following is immediate from propositions B.8 and B.9.

THEOREM B.10. *One has a direct sum decomposition* $S_B = M_1' \oplus M_2'$ *as modules for* $S^B = \mathbb{F}_q[D_{2,1}, X]$, *where*

- M_1' *is a free* $\mathbb{F}_q[D_{2,1}, X]$*-module on* $\{Y\}$, *and*
- M_2' *is a direct sum of copies of the quotient* S^B*-module* $\mathbb{F}_q[D_{2,1}, X]/(X)$ *with basis listed in (B 12).*

In particular, one has

$$\mathrm{Hilb}(S_B, t) = \frac{t^{q-1}}{(1-t^{q-1})(1-t^{q^2-q})} + \frac{1 + t^{2(q-1)} + t^{3(q-1)} + \cdots + t^{(q-1)^2}}{1 - t^{q^2-q}},$$

which equals the prediction from parabolic conjecture 1.6 for $\alpha = (1,1)$, *namely*

$$\mathrm{Hilb}(S_B, t) = 1 + \frac{t^{q-1}}{1-t^{q-1}} + \frac{t^{2(q-1)}}{1-t^{q-1}} + \frac{t^{q^2+q-2}}{(1-t^{q-1})(1-t^{q^2-q})},$$

with the four summands corresponding to $\beta = (0,0)$, $(0,1)$, $(1,0)$ *and* $(1,1)$, *respectively.*

B.4. Analysing the fixed quotient S_G for the full group $G = \mathrm{GL}_2(\mathbb{F}_q) = P_{(2)}$

One can again regard the polynomial algebra S with its G-action as a module for the group algebra $S^G[G]$ with coefficients in the G-invariant subalgebra $S^G = \mathbb{F}_q[D_{2,0}, D_{2,1}]$. Our strategy here in understanding S_G as an S^G-module differs from the previous section, as we do not have a G-stable subspace in S acted on freely by $D_{2,1}$ to play the role of the B-stable subspace $\hat{S} \subset S$. Instead we shall work with quotients by $D_{2,1}$.

PROPOSITION B.11. *One has an* S^G*-module isomorphism*

$$(S/(D_{2,1}))_G \cong S_G/D_{2,1}S_G.$$

Proof. Both are isomorphic to $S/(D_{2,1}S + \mathrm{span}_{\mathbb{F}_q}\{g(f) - f\}_{g\in G, f\in S})$. □

We wish to first analyse $(S/(D_{2,1}))_G$ as an S^G-module. For this it helps that we already understand $(S/(D_{2,1}))_B$ as an S^B-module, due to the following result.

PROPOSITION B.12. *The composite map* $\hat{S} \hookrightarrow S \twoheadrightarrow S/(D_{2,1})$ *is an isomorphism of* $\mathbb{F}_q[X][B]$*-modules, which then induces an isomorphism of* $\mathbb{F}_q[X]$*-modules* $\hat{S}_B \cong (S/(D_{2,1}))_B$.

Proof. The first assertion comes from proposition B.8, and the second assertion follows from the first. □

PROPOSITION B.13. *The set*

$$\{1, XY, X^2Y, \ldots, X^{q-2}Y\} \cup \{X^qY\} \tag{B 13}$$

generates $S_G/D_{2,1}S_G$ *as a module over* $\mathbb{F}_q[D_{2,0}]$, *and hence generates* S_G *as module over* $\mathbb{F}_q[D_{2,0}, D_{2,1}] = S^G$.

Proof. The second assertion follows from the first via the following well-known general lemma.

LEMMA B.14. *Let R be an $\mathbb{N}$-graded ring. Let $I \subset R_+ := \bigoplus_{d>0} R_d$ be a homogeneous ideal of positive degree elements. Let M be a $\mathbb{Z}$-graded R-module with non-zero degrees bounded below.*

Then a subset generates M as an R-module if and only if its images generate M/IM as R/I-module.

Proof of lemma B.14. The 'only if' direction is clear. For the 'if' direction, one assumes that $\{m_i\}$ in M have $\{m_i + IM\}$ generating M/IM as R/I-module, and shows that every homogeneous element m in M lies in $\sum_i Rm_i$ via a straightforward induction on the degree of m. □

Returning to the proof of the first assertion in the proposition, we use proposition B.11 to work with $(S/(D_{2,1}))_G$ rather than $S_G/D_{2,1}S_G$. As noted in proposition B.1, $D_{2,0} = XD_{2,1} - X^{q+1}$, and hence

$$D_{2,0} \equiv -X^{q+1} \bmod (D_{2,1}).$$

Thus, via the quotient map $(S/(D_{2,1}))_B \twoheadrightarrow (S/(D_{2,1}))_G$, one obtains an $\mathbb{F}_q[D_{2,0}]$-spanning set for $(S/(D_{2,1}))_G$ from any $\mathbb{F}_q[X^{q+1}]$-spanning set of $(S/(D_{2,1}))_B$, or equivalently via proposition B.12, from any $\mathbb{F}_q[X^{q+1}]$-spanning set of $\hat{S}_B$. Since $\hat{S}_B$ has as $\mathbb{F}_q$-basis the monomials $\{X^iY\}_{i\geqslant 0} \cup \{1, Y^2, Y^3, \ldots, Y^{q-1}\}$ from (B 11), it has as an $\mathbb{F}_q[X^{q+1}]$-spanning set

$$\{X^iY\}_{0\leqslant i\leqslant q} \cup \{1, Y^2, Y^3, \ldots, Y^{q-1}\}.$$

Thus, this set is an $\mathbb{F}_q[D_{2,0}]$-spanning set for $(S/(D_{2,1}))_G$. However, lemma B.5(iii) says that the pure powers $\{Y^j\}_{j\geqslant 1}$ all vanish in S_G, so one obtains this smaller $\mathbb{F}_q[D_{2,0}]$-spanning set for $(S/(D_{2,1}))_G$:

$$\{1, XY, X^2Y, \ldots, X^{q-2}Y, X^{q-1}Y, X^qY\}.$$

We claim that the second-to-last element $X^{q-1}Y$ on this list is also redundant, as it vanishes in $(S/(D_{2,1}))_G$. To see this claim, note that in $(S/(D_{2,1}))_G$ one has

$$0 \equiv D_{2,1} = Y^q + (XY^{q-1} + X^2Y^{q-2} + \cdots + X^{q-2}Y^2 + X^{q-1}Y) + X^q.$$

Here the two pure powers X^q, Y^q vanish in S_G and also in $(S/(D_{2,1}))_G$ due to (i) and (iii) of lemma B.5. Similarly, the $q-1$ monomials inside the parentheses, X^iY^{q-i} for $i = 1, 2, \ldots, q-1$, are all equal to $X^{q-1}Y$ due to lemma B.5(i). This implies $0 \equiv (q-1)X^{q-1}Y = -X^{q-1}Y$ as claimed. □

THEOREM B.15. *One has an S^G-module direct sum decomposition $S_G = N_1 \oplus N_2$, in which*

- *$N_1 = S^G \cdot X^qY$ is a free S^G-module on the basis $\{X^qY\}$, and*
- *N_2 is the S^G-submodule spanned by the elements of (B 9), whose S^G-module structure is a direct sum of $q-1$ copies of $S^G/(D_{2,0})$ with the elements of (B 9) as basis.*

In particular, in the bivariate case $n=2$*, question 5.9 has an affirmative answer, and one has*

$$\begin{aligned}\mathrm{Hilb}(S_G,t) &= \frac{t^{q^2-1}}{(1-t^{q^2-1})(1-t^{q^2-q})} + \frac{1+t^{2(q-1)}+t^{3(q-1)}+\cdots+t^{(q-1)^2}}{1-t^{q^2-q}} \\ &= 1+\frac{t^{2(q-1)}}{1-t^{q-1}} + \frac{t^{2(q^2-1)}}{(1-t^{q^2-1})(1-t^{q^2-q})},\end{aligned}$$

so that conjecture 1.3 holds.

Proof. Define N_1, N_2 to be the S^G submodules of S_G spanned by $\{X^qY\}$ and of the elements of (B 9), respectively. Then proposition B.13 implies $S^G = N_1 + N_2$. Note that corollary B.6 already shows that the submodule N_2 has the claimed structure. In particular, $D_{2,0}\cdot N_2 = 0$, i.e. $N_2 \subset \mathrm{Ann}_{S_G} D_{2,0}$.

We claim that this forces $N_2 = S^G\cdot X^qY \cong S^G$, i.e. no element f in S^G can annihilate X^qY. Otherwise, there would be an element $D_{2,0}f$ in S^G annihilating both N_1 and N_2, and hence annihilating all of S_G, contradicting the assertion from proposition 5.7 that S_G is a rank 1 S^G-module.

Once one knows $N_2 = S^G\cdot X^qY \cong S^G$, one can also conclude that the sum $S_G = N_1 + N_2$ is direct, since

$$N_1 \cap N_2 \subset \mathrm{Ann}_{S_G}(D_{2,0}) \cap N_2 = 0.$$

□

REMARK B.16. Our proof for parabolic conjectures 1.5 and 1.6 with $n=2$ is hands-on and technical. One might hope to use more of the results of Karagueuzian and Symonds [17–19]. They give a good deal of information about the action of $G=\mathrm{GL}_n(\mathbb{F}_q)$ on $S=\mathbb{F}_q[x_1,\ldots,x_n]$, by analysing in some detail the structure of S as an $\mathbb{F}_qU$-module, where U is the p-Sylow subgroup of G consisting of all unipotent upper-triangular matrices. We have not seen how to apply this toward resolving our conjectures in general.

Acknowledgements

This work was partly supported by National Science Foundation Grant nos DMS-1148634 and DMS-1001933. The authors thank A. Broer, M. Crabb, N. Kuhn, A. Shepler, L. Smith, and P. Webb for valuable suggestions and references, as well as D. Stamate for computations discussed in example 5.12 regarding question 5.9.

Note added in proof

The $m=2$ special case of conjecture 1.2 was recently verified by Goyal in [14].

References

1 K. Akin, D. A. Buchsbaum and J. Weyman. Schur functors and Schur complexes. *Adv. Math.* **44** (1982), 207–278.

2 D. Armstrong, V. Reiner and B. Rhoades. Parking spaces. *Adv. Math.* **269** (2015), 647–706.

3 M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra* (Addison-Wesley, 1969).

4 M. Balagović and H. Chen. Representations of rational Cherednik algebras in positive characteristic. *J. Pure Appl. Alg.* **217** (2013), 716–740.

5 D. J. Benson. *Polynomial invariants of finite groups.* London Mathematical Society Lecture Note Series, vol. 190 (Cambridge University Press, 1993).

6 D. Bourguiba and S. Zarati. Depth and the Steenrod algebra: with an appendix by J. Lannes. *Invent. Math.* **128** (1997), 589–602.

7 D. P. Carlisle and N. J. Kuhn. Subalgebras of the Steenrod algebra and the action of matrices on truncated polynomial algebras. *J. Alg.* **121** (1989), 370–387.

8 L. E. Dickson. A fundamental system of invariants of the general modular linear group with a solution of the form problem. *Trans. Am. Math. Soc.* **12** (1911), 75–98.

9 S. Doty and G. Walker. The composition factors of $F_p[x_1, x_2, x_3]$ as a $GL(3, p)$-module. *J. Alg.* **147** (1992), 411–441.

10 S. Doty and G. Walker. Modular symmetric functions and irreducible modular representations of general linear groups. *J. Pure Appl. Alg.* **82** (1992), 1–26.

11 S. Doty and G. Walker. Truncated symmetric powers and modular representations of GL_n. *Math. Proc. Camb. Phil. Soc.* **119** (1996), 231–242.

12 D. S. Dummit and R. M. Foote. *Abstract algebra*, 3rd edn (Hoboken, NJ: Wiley, 2004).

13 J. Goldman and G.-C. Rota. The number of subspaces of a vector space. In *Recent progress in combinatorics*, pp. 75–83 (New York: Academic, 1969).

14 P. Goyal. Invariant theory of finite general linear groups modulo Frobenius powers. Preprint, 2017. (Available at https://arxiv.org/abs/1701.06329v1.)

15 J. Hartmann and A. V. Shepler. Reflection groups and differential forms. *Math. Res. Lett.* **14** (2007), 955–971.

16 T. J. Hewett. Modular invariant theory of parabolic subgroups of $\mathrm{GL}_n(F_q)$ and the associated Steenrod modules. *Duke Math. J.* **82** (1996), 91–102. (Correction *Duke Math. J.* **97** (1999), 217.)

17 D. Karagueuzian and P. Symonds. The module structure of a group action on a polynomial ring. *J. Alg.* **218** (1999), 672–692.

18 D. Karagueuzian and P. Symonds. The module structure of a group action on a polynomial ring: examples, generalizations, and applications. In *Invariant theory in all characteristics*, CRM Proceedings and Lecture Notes, vol. 35, pp. 139–158 (Providence, RI: American Mathematical Society, 2004).

19 D. Karagueuzian and P. Symonds. The module structure of a group action on a polynomial ring: a finiteness theorem. *J. Am. Math. Soc.* **20** (2007), 931–967.

20 N. J. Kuhn. The Morava K-theories of some classifying spaces. *Trans. Am. Math. Soc.* **304** (1987), 193–205.

21 N. Kuhn and S. Mitchell. The multiplicity of the Steinberg representation of $\mathrm{GL}_n F_q$ in the symmetric algebra. *Proc. Am. Math. Soc.* **96** (1986), 1–6.

22 P. S. Landweber and R. E. Stong. *The depth of rings of invariants over finite fields.* Springer Lecture Notes in Mathematics, vol. 1240, pp. 259–274 (New York: Springer, 1987).

23 S. Lang. *Algebra*, 3rd rev. edn. Graduate Texts in Mathematics, vol. 211 (New York: Springer, 2002).

24 H. Mui. Modular invariant theory and cohomology algebras of symmetric groups. *J. Fac. Sci. Univ. Tokyo (1)* A **22** (1975), 319–369.

25 V. Reiner and D. Stanton. (q, t)-analogues and $\mathrm{GL}_n(\mathbb{F}_q)$. *J. Algebraic Combin.* **31** (2010), 411–454.

26 V. Reiner, D. Stanton and D. White. The cyclic sieving phenomenon. *J. Combin. Theory* A **108** (2004), 17–50.

27 B. Rhoades. Parking structures: Fuss analogs. *J. Alg. Combin.* **40** (2014), 417–473.

28 J. Segal. Notes on invariant rings of divided powers. In *Invariant theory in all characteristics.* CRM Proceedings and Lecture Notes, vol. 35, pp. 229–239 (Providence, RI: American Mathematical Society, 2004).

29 J.-P. Serre. *Linear representations of finite groups.* Graduate Texts in Mathematics, vol. 42 (New York: Springer, 1977).

30 L. Smith. *Polynomial invariants of finite groups.* Research Notes in Mathematics, vol. 6 (Wellesley, MA: A. K. Peters, 1995).

31 L. Solomon. Invariants of finite reflection groups. *Nagoya Math. J.* **22** (1963), 57–64.

32 R. Steinberg. On Dickson's theorem on invariants. *J. Fac. Sci. Univ. Tokyo (1)* A **34** (1987), 699–707.

33 R. M. W. Wood. Modular representations of $GL(n, \mathbb{F}_p)$ and homotopy theory. In *Algebraic topology: Göttingen 1984*, Lecture Notes in Mathematics, vol. 1172, pp. 188–203 (Berlin: Springer, 1985).

34 R. M. W. Wood. Problems in the Steenrod algebra. *Bull. Lond. Math. Soc.* **30** (1998), 449–517.