

hexagon:2610.00212v1

The Chaise Longue Theorem

Conjecture 1.2 of Degtyarev–Shimada for the Fermat varieties of every degree in every even dimension, and the integral Hodge conjecture for those whose degree is prime, equal to 4, or prime to $(n + 1)!$

Rafael Amichis Luengo

Madrid, Spain · tretoef@gmail.com · 4 October 2026 · version 12

Abstract

Let $X \subset P^{n+1}$ be the complex Fermat variety of degree $m \geq 3$ and even dimension $n = 2k$, and let $L(X) \subseteq H_n(X; Z)$ be the subgroup generated by the classes of its standard k -dimensional linear subspaces. Degtyarev and Shimada conjectured that $H_n(X; Z)/L(X)$ is torsion free [DS, Conjecture 1.2]. **We prove this conjecture for every degree $m \geq 3$ in every even dimension**, modulo two topological results used by [DS]: Pham’s theorem on the homology of the affine Fermat variety, and their intersection numbers. Its algebraic form — the quotient $Z[G]/(\psi_J)$ of the group ring of [DS] is free abelian of rank $m^{2k+1} - Q_k(m)$ — is proved with no topology, and it has been verified for every degree by a complete proof in the proof assistant Lean 4 with the Mathlib library, with no gap and no axiom beyond the three standard ones. The proof reduces the conjecture, prime by prime, to dimension counts in truncated polynomial rings, proved by peeling off one variable at a time. Consequences: the integral Hodge conjecture for X whenever m is prime, or $m = 4$, or m is prime to $(n+1)!$, with the integral Hodge classes of middle degree generated by the standard linear subspaces — in particular for the Fermat quartic of every even dimension; and the primitivity of the sublattices spanned by the linear subspaces that [DS] exhibit on the partial Fermat varieties, which [DS] proved conditionally on the conjecture. This work has not been refereed by a human expert.

1. Introduction and main results

1.0 Summary of results

$m \geq 3$ is the degree, $n = 2k$ the dimension, $N = 2k + 2$, and $Q_k(m) = |\Gamma_{\mathcal{J}}|$ is the number of §1.2. «Lean» means that the statement is proved in Lean 4 with Mathlib, with no gap and no axiom beyond `propext`, `Classical.choice` and `Quot.sound` (§14.8, [LC]).

Result	What it says	Range	What it rests on	Lean
Main Theorem’ (§1.2)	$R/(\psi_J : J \in \mathcal{J})$ is free abelian of rank $m^{2k+1} - Q_k(m)$; the same dimension over every field	every $m \geq 3$, $k \geq 1$	nothing outside this paper: the upper bound is [DS, Claim 4.3], a count of points re-proved in Appendix B, Step 6	yes, every $m \geq 1, k \geq 0$

Result	What it says	Range	What it rests on	Lean
Main Theorem = Conjecture 1.2 of [DS] (§1.2)	$H_{2k}(X; Z)/L(X)$ is torsion free, and $\text{rank } L(X) = Q_k(m) + 1$	every $m \geq 3$, $k \geq 0$	Main Theorem' and [DS, Theorems 1.1(a), 1.4], which Appendix B derives from Pham's theorem [Ph] and [DS, Theorem 2.2]	the algebraic form only
Corollary H (§1.3, §12)	$L(X)$ is primitive in $\text{Hdg}(X)$ with free quotient of rank $ \mathfrak{B} - Q_k(m)$; $\text{Hdg}(X) = L(X)$ iff m is prime, $m = 4$, or $\gcd(m, (n+1)!) = 1$, and then the integral Hodge conjecture holds for X	every $m \geq 3$, $k \geq 1$	the Main Theorem; the classical facts (H1)–(H3); Aoki's theorem (H5) [Aok] (for prime m and $m = 4$, the proofs (H4), (H4') given here)	no
Corollary W (§1.4, §13)	the linear subspaces of [DS] on the partial Fermat varieties span primitive sublattices	every $m \geq 3$, $0 \leq s \leq d$	the Main Theorem; part (i) also the transport argument of [DS, §4.6]	no
Theorem B (§1.5, §5)	the count at the even box $q - 1$, with equality and a free quotient over Z	every odd $q \geq 3$, every field, every k	—	yes, except the graded refinement
Theorem C (§7)	the bipartite counts, $\geq$; equality over $\bar{F}_p$ (Corollaries 7.8, 9.12)	every $q \geq 2$, fields with $C(q-1, t) \neq 0$	—	yes
Theorem O (§1.5, §8)	the count at the odd box r , with equality and a free quotient over Z	every odd $r \geq 3$, every field, every k	—	yes, except the graded refinement
Theorem A (§1.6, §10)	a different count; it does not imply the conjecture; as a count it is due to Kostant (characteristic 0) and to [BRR] (odd characteristic)	$\text{char } F \neq 2$, odd q	— (Appendix A)	no
Corollary 10.8	at the odd box, sum and intersection of the matching ideals coincide	$\text{char } F \neq 2$, odd r	Theorems O and A	no
Fact 11.2	the analogue of the Main Theorem for subfamilies of matchings is false	a computation	—	no

Everything in this table that is not marked «Lean» was read cold by readers other than its writer (§14.6). No human expert has refereed this work. What we found in the literature, and where we searched, is in §1.10.

1.1 The conjecture

We follow [DS]. Let $n = 2k$ with $k \geq 0$, let $m \geq 3$, and let $X \subset P^{n+1}$ be the Fermat variety $z_0^m + \dots + z_{n+1}^m = 0$. All homology is with coefficients in Z .

- $\mathcal{J}$ is the set of partitions of the index set $\{0, 1, \dots, n+1\}$ into unordered pairs, written $J = [[j_0, k_0], \dots, [j_k, k_k]]$ with $j_i < k_i$ and $j_0 < j_1 < \dots < j_k$; in particular $j_0 = 0$. There are $|\mathcal{J}| = (2k+1)!!$ of them.
- For $J \in \mathcal{J}$ and $\beta = (\beta_0, \dots, \beta_k)$ with $\beta_i^m = -1$, the **standard k -space** $L_{J,\beta} \subset X$ is given by $z_{k_i} = \beta_i z_{j_i}$ ($i = 0, \dots, k$).
- For $\emptyset \neq K \subseteq \mathcal{J}$, $L_K(X) \subseteq H_n(X)$ is the subgroup generated by the classes $[L_{J,\beta}]$ with $J \in K$; $L(X) := L_{\mathcal{J}}(X)$.

Conjecture 1.2 of [DS]. *The group $H_n(X)/L(X)$ is torsion free.*

For $k = 1$ the conjecture is a theorem of Degtyarev [De14]; for m prime to 6 it implies that the Picard group of the Fermat surface is generated by its lines. For $k \geq 2$ it has been confirmed by computer for $(n, m) = (4, m)$ with $3 \leq m \leq 12$, and for $(6, 3)$, $(6, 4)$, $(6, 5)$, $(8, 3)$ [DS, §5]. Aljovin, Movasati and Villaflor [AMV] compared the lattice of linear cycles with the lattice of Hodge cycles by computing elementary divisors, for the Fermat surfaces of degree $3 \leq m \leq 14$ and the Fermat fourfolds of degree $3 \leq m \leq 6$ [AMV, Table 1]. The conjecture is restated as open in [De15, Conjecture 4.4]. Before the present work (versions 4 to 12 of this paper) we knew of no proof for any $k \geq 2$ beyond these cells; in particular it had not been decided for any odd degree that is not a prime power when $k \geq 2$ (the odd degrees in the table of [DS, §5] are prime powers). As [DS, §1] point out, for prime m the rational Hodge classes of X are spanned by the classes of the standard spaces, so that the conjecture would upgrade this to the *integral* Hodge classes; §12 carries this out, for prime m and for more degrees.

1.2 The main theorem

Put $N := 2k + 2 = n + 2$, and for $m \geq 3$ let

$$\begin{aligned} Q_k(m) &:= N! \cdot [x^N] I_0(2x)^{(m-1)/2} \quad (m \text{ odd}), \\ Q_k(m) &:= N! \cdot [x^N] \cosh(x) \cdot I_0(2x)^{(m-2)/2} \quad (m \text{ even}), \\ I_0(2x) &= \sum_{b \geq 0} x^{2b} / (b!)^2. \end{aligned}$$

For every m , $Q_k(m)$ is the number $|\Gamma_{\mathcal{J}}|$ of [DS, Definition 1.3] (Lemma 2.2 for odd m , Lemma 9.1 for even m), so that $\text{rank } L(X) = Q_k(m) + 1$ by Theorem 0(c) below. In the algebraic statements of §1.5 and in §2–§7, $Q_k(q)$ is always taken at an odd q .

MAIN THEOREM. *Let $m \geq 3$ and $k \geq 0$. Then $H_{2k}(X; Z)/L(X)$ is torsion free for the Fermat variety X of degree m and dimension $2k$. Equivalently, $L(X)$ is a primitive sublattice of $H_{2k}(X; Z)$, of rank $Q_k(m) + 1$.*

For $k = 0$ the statement is trivial: X is a set of m points and $L(X) = H_0(X)$. From now on $k \geq 1$ whenever topology is involved.

The Main Theorem has an algebraic form, which is proved here with no topology at all (Corollary 7.7 for odd m , Theorem 9.11 for even m). Let $R := Z[t_1, \dots, t_{2k+1}]/(t_1^m - 1, \dots, t_{2k+1}^m - 1)$ be

the integral group ring of $G = (Z/m)^{2k+1}$ and let $\psi_J \in R$ be the generators of [DS], recalled in §2.

MAIN THEOREM' (algebraic form). *Let $m \geq 3$ and $k \geq 1$. Then $R/(\psi_J : J \in \mathcal{J})$ is a free abelian group of rank $m^{2k+1} - Q_k(m)$. Equivalently, $\dim_{F_p} F_p[G]/(\bar{\psi}_J : J \in \mathcal{J}) = m^{2k+1} - Q_k(m)$ for every prime p .*

By [DS, Theorem 1.1(a)] (Theorem 0(a) below) the torsion of $R/(\psi_J : J \in \mathcal{J})$ is that of $H_{2k}(X; Z)/L(X)$, so Main Theorem' implies the Main Theorem; the rank of $L(X)$ is [DS, Theorem 1.4]. These two statements are the only places where topology enters.

The proof has five parts.

- **§2 (the translation).** Using the results of [DS] collected in Theorem 0, torsion-freeness at m is equivalent to a dimension count over F_p for each prime $p|m$ (Proposition 2.1); for $m = q = p^v$ the count is (S) $\dim_{F_p}(D_J : J \in \mathcal{J})C = Q_k(q)$ (Proposition 2.5).
- **§5 (odd prime powers).** Theorem B below proves (S).
- **§6–§7 (odd degrees that are not prime powers).** For odd $m = q \cdot r$ with $q = p^v$, $p \nmid r$, $r > 1$, the count at p splits over the colourings of the coordinates by r -th roots of unity into a sum of products of block dimensions (Proposition 6.9). The blocks are instances of Theorem 5.3 and bipartite ideals, whose count is Theorem C (§7).
- **§8 (the odd box).** Theorem O below: the count of Theorem B at an odd box, on a grid with one zero. It is the root case of Theorem 8.11.
- **§9 (even degrees).** For $m = 2^v$ the ideal of leading forms of the $\bar{\psi}_J$ in characteristic 2 contains the product of $s_1 \cdots s_{2k+1}$ with the ideal of Theorem O for the box $2^v - 1$, an isomorphic copy of it in another ring (Proposition 9.2). For the other even m the colour reduction of §6 applies at every prime; the block of the colour -1 at an odd prime is the ideal of Theorem O for the box p^v , the block of the colour 1 at the prime 2 is the problem for the degree 2^v , and the pair blocks are bipartite ideals, at the prime 2 with an even box (Theorem 9.11).

Sections 5–9 prove lower bounds for the dimensions of the ideals: Theorems 5.3, 7.6 and 8.11. The matching upper bound is the inequality of Proposition 2.1, and it is algebraic too: it is [DS, Claim 4.3] (Theorem 0(b)), a count of points by the Chinese remainder theorem over a field of characteristic 0 (Appendix B, Step 6). So Main Theorem' is proved without topology; topology enters only through Theorem 0(a) and 0(c), which identify the torsion of $R/(\psi_J)$ with that of $H_{2k}(X; Z)/L(X)$ and give the rank of $L(X)$. Theorems 5.9 and 5.9', §4, §10 and §11 are not on the path of the proof, and neither is the equality in Theorem O (Corollary 8.13): the proof uses only its inequality $\geq$. Corollaries 7.8 and 9.12 are consequences of the proof. Main Theorem' has been proved again, for every degree, in the proof assistant Lean 4 (§14.8), and so has Theorem O.

The cubic case $q = 3$ has a shorter proof with an explicit basis given by ballot paths (§4, Theorem 4.1), and so has the box $r = 3$, which is all that the quartics need (§8.8, Theorem 8.15).

1.3 The integral Hodge conjecture

For a smooth complex projective variety Y , the integral Hodge conjecture in degree $2j$ asks whether every class in $H^{2j}(Y; Z) \cap H^{j,j}(Y)$ is the class of an algebraic cycle with integer coefficients. It is false in general [AH], [Kol], and it remains open for many varieties for which the

rational Hodge conjecture is known; for Fermat varieties it is the question studied in [AMV]. Write $\text{Hdg}(X) \subseteq H_n(X; \mathbb{Z})$ for the group of integral Hodge classes of middle degree (§12.1).

COROLLARY H. *Let $m \geq 3$, $k \geq 1$, and let X be the Fermat variety of degree m and dimension $2k$.*

- (i) *If m is prime, or $m = 4$, or every prime factor of m is at least $2k + 3$, then $\text{Hdg}(X) = L(X)$: every integral Hodge class of middle degree is an integral linear combination of classes of standard k -spaces. In particular the integral Hodge conjecture holds for X in every degree.*
- (ii) *For every m , $L(X)$ is a primitive sublattice of $\text{Hdg}(X)$ and $\text{Hdg}(X)/L(X)$ is free of rank $|\mathfrak{B}| - Q_k(m)$, where $\mathfrak{B}$ is the set of Hodge characters of §12.1. It is zero if and only if m is prime, or $m = 4$, or every prime factor of m is at least $2k + 3$.*

For odd m , «every prime factor of m is at least $2k + 3$ » is the same as the condition $\gcd(m, (n + 1)!) = 1$ of [AMV, §1], which we use in the title. (Version 11 wrote $\gcd(m, (n + 2)!) = 1$. It is the same condition: a prime that divides $n + 2 = 2(k + 1)$ and m is at most $k + 1$, so it divides $(n + 1)!$ as well.) For even m the only degree in (i) is $m = 4$: **the integral Hodge conjecture holds for the Fermat quartic of every even dimension, and its integral Hodge classes of middle degree are generated by the standard linear subspaces.** The proof is in §12. It combines the Main Theorem with the classical description of the rational Hodge classes of X by characters [SK], [Shi79], [Ran] ((H3) of §12.1), and with the determination, due to Aoki [Aok, Theorem A], of the degrees in which every Hodge character is of pair type; for prime m and for $m = 4$ we give short proofs of this last fact (§12.1, (H4) and (H4')). The new input is the primitivity of $L(X)$. The classical fact that the rational Hodge classes of pair type are spanned by linear subspaces [Ran, Theorem 4.9] is not used: over $\mathbb{Z}$ it follows from the Main Theorem.

What was known. For $k = 1$ the integral Hodge conjecture is the Lefschetz $(1, 1)$ theorem, and (i) says that the lines generate the Néron–Severi group, which was known when $\gcd(m, 6) = 1$ [SSvL], [De14], and classically for the cubic surface; for odd m these are exactly the degrees of (i) at $k = 1$. For $m = 4$: at $k = 1$ it is the statement that the lines of the Fermat quartic surface generate its Néron–Severi group, of rank 20, which is a result of Mizukami [Miz] (1975; [SSvL, §3 and §6] record it, attribute it to Mizukami and Inose and give another proof; we have not read [Miz]), and which also follows from [De14]; at $k = 2$ it was verified by computer in [AMV], whose abstract states the integral Hodge conjecture for the quartic and quintic Fermat fourfolds; at $k = 2, 3$ the primitivity of $L(X)$ was confirmed by computer in [DS, §5], so that (i) already followed there by the argument of §12.3. For $m = 4$ and $k \geq 4$ it is new, to our knowledge. For $(k, m) = (2, 3)$ the integral Hodge conjecture itself follows from Voisin’s theorem on cubic fourfolds [Voi, Theorem 2.11]; as [AMV, §1] note, the stronger statement $\text{Hdg}(X) = L(X)$ does not follow from it. The cells $(2, 3)$ and $(2, 5)$ were verified by computer in [AMV]. In each prime cell where [DS, §5] confirmed the primitivity of $L(X)$ by computer, namely $(k, m) = (2, 3), (2, 5), (2, 7), (2, 11), (3, 3), (3, 5), (4, 3)$, (i) already followed from that computation and the classical facts by the argument of §12.3; [AMV, §1] make this observation for the cells of their table. The author had also verified the primitivity of $L(X)$ by computer, before the present proof, in the prime cells $(k, m) = (2, 13), (2, 17), (2, 19), (3, 7), (4, 5), (5, 3)$ [Rep]; three of them, $(2, 13)$, $(3, 7)$ and $(5, 3)$, are re-run in §14.1. What is new, for $k \geq 2$, is the uniform statement: the quartics of dimension at least 8, every other cell with m prime, and every cell of (i) with m not prime, for instance $(k, m) = (2, 49), (2, 77), (3, 121), (3, 143)$; to our knowledge no cell of (i) with m not prime and $k \geq 2$ had been decided before. Part (ii) is new for $k \geq 2$, to our knowledge; for $k = 1$ it follows from [De14] and the rank $|\mathfrak{B}| + 1$ of (H3). Recent work on

the *rational* Hodge conjecture for Fermat varieties is complementary to ours: Jumagulov [Jum] gave a computer-assisted proof for the Fermat fourfolds of odd degree at most 199; Miranda, Movasati, Rufino and Villaflor [MMRV] prove it for the Fermat varieties of every dimension and every degree $d < 65$ other than 44, 51, 52, by reducing the lengths of Aoki's exceptional tuples; and Favero and Kelly [FK] prove it for the Fermat fourfold of degree 33, through an explicit formula for Chern characters. These statements are rational; ours concern the lattice $L(X)$ over Z .

1.4 Partial Fermat varieties

Let $0 \leq s \leq d$. Following [DS, §1], a **partial Fermat variety** is a smooth hypersurface $W_s \subset P^{2d+1}$ given by $f_0(z_0, z_1) + f_1(z_2, z_3) + \cdots + f_d(z_{2d}, z_{2d+1}) = 0$, where the f_i are binary forms of degree m , $f_0 = \cdots = f_s = x^m + y^m$, and $f_{s+1}, \dots, f_d$ are generic, pairwise distinct and distinct from $x^m + y^m$. [DS, §1] exhibit $(2s+1)!! \cdot m^{d+1}$ linear d -spaces on it.

COROLLARY W. *Let $m \geq 3$ and $0 \leq s \leq d$.*

- (i) *The classes of the $(2s+1)!! \cdot m^{d+1}$ linear d -spaces of [DS, §1] on W_s generate a primitive sublattice of $H_{2d}(W_s; Z)$.*
- (ii) *On the Fermat variety X of dimension $2d$, let $\mathcal{J}(s, d) \subseteq \mathcal{J}$ be the set of matchings that contain the pairs $\{2i, 2i+1\}$ for $s < i \leq d$. Then $L_{\mathcal{J}(s, d)}(X)$ is primitive in $H_{2d}(X; Z)$, of rank $Q_s(m)(m-1)^{d-s} + 1$.*

[DS, Corollary 1.7] states (i) under the assumption that Conjecture 1.2 holds for the Fermat varieties of dimension $2s$ and degree m , and proves it for $s = 0, 1$; [De15, §4.2–§4.3] reduces (i) and (ii) to the same assumption and proves them in the same cases (in [De15] the index is the dimension $2s$). The Main Theorem removes the assumption. The proof is in §13, where (ii) is proved directly.

1.5 The algebraic statements

Let F be a field and $q \geq 3$ odd. Put $C_F := F[y_1, \dots, y_{2k+1}]/(y_1^{q-1}, \dots, y_{2k+1}^{q-1})$ and define $D(a, b)$ and D_J as in the abstract: D is the polynomial of §2.3, which has integer coefficients.

THEOREM B. *For every field F , every odd $q \geq 3$ and every $k \geq 0$,*

$$\dim_F(D_J : J \in \mathcal{J}) \cdot C_F = Q_k(q).$$

Moreover, with $C_Z := Z[y_1, \dots, y_{2k+1}]/(y_1^{q-1}, \dots, y_{2k+1}^{q-1})$, the group $C_Z/(D_J : J \in \mathcal{J})C_Z$ is free abelian of rank $(q-1)^{2k+1} - Q_k(q)$, and the dimension of each graded piece of $(D_J : J \in \mathcal{J})C_F$ does not depend on F .

Theorem B is the root case of a more general statement about down-sets of partitions (Theorem 5.3 for $\geq$; Theorems 5.9 and 5.9' for $=$ and for the integral statement). Neither the topology nor [DS] enters its proof; they enter only in the translation of §2. With Theorem B and Proposition 2.5, the Main Theorem follows for $m = p^v$ (Corollary 5.4).

The degrees that are not prime powers need a second count, in two sets of variables $x_1, \dots, x_\alpha$ and $z_1, \dots, z_\beta$ with the box (x_i^q, z_l^q) , for $q = p^v$ (p any prime; the box q is even when $p = 2$): the **balanced** bipartite ideal I_a^{bal} , generated by $\prod_{i=1}^a (x_i - z_{\sigma(i)})^{q-1}$ over all $\sigma \in S_a$ ($\alpha = \beta = a$),

and the **phantom** bipartite ideal I_a^{ph} , generated by the same products over all bijections from a of the $a + 1$ variables x_i onto the z_l ($\alpha = a + 1$, $\beta = a$). **Theorem C** (§7) says that their dimensions are at least the numbers of pairs (ξ, η) of tuples in a set of q elements, of lengths (a, a) and $(a + 1, a)$, such that the multiset of η is equal to, respectively contained in, the multiset of ξ . Over $\bar{F}_p$ these are equalities (Corollaries 7.8 and 9.12), and the dimensions do depend on the characteristic.

The even degrees need a third count, at an **odd** box. Let $r \geq 3$ be odd, $D_r(a, b) := \sum_{u=0}^{r-1} (-1)^u a^u b^{r-1-u} = (a^r + b^r)/(a + b)$, and for $J \in \mathcal{J}$ let $D_{r,J}$ be the product of the $D_r(y_a, y_b)$ over the pairs $\{a, b\}$ of J that avoid 0.

THEOREM O (the odd box). *For every field F , every odd $r \geq 3$ and every $k \geq 0$,*

$$\dim_F(D_{r,J} : J \in \mathcal{J}) \cdot F[y_1, \dots, y_{2k+1}]/(y_1^r, \dots, y_{2k+1}^r) = N! \cdot [x^N] \cosh(x) \cdot I_0(2x)^{(r-1)/2}.$$

Moreover the quotient of $Z[y_1, \dots, y_{2k+1}]/(y_i^r)$ by the ideal generated by the $D_{r,J}$ is a free abelian group.

The right-hand side is the number of N -tuples, in a set of r elements with an involution that has one fixed point, which split into pairs of opposite entries; for $r = m - 1$ it is $Q_k(m)$ for the even number m . Theorem O is the root case of Theorem 8.11, a statement about interlaced pairs of down-sets of partitions. In characteristic p and for $r = p^v$, $D_r(a, b) = (a + b)^{r-1}$. Theorem O was stated as an open problem in version 10 of this paper (there: problem 7 of §13), and proved in version 11.

1.6 A different count: Theorem A

Write $E := (e_1, e_3, \dots, e_{2k+1}) \subseteq F_p[x_0, \dots, x_{2k+1}]$ for the ideal of the odd elementary symmetric polynomials. Over an algebraic closure its zero set is the union of the linear spaces $x_a + x_b = 0$ ($\{a, b\} \in J$), over all $J \in \mathcal{J}$.

THEOREM A. *Let F be a field of characteristic $\neq 2$, let $q \geq 1$ be odd and let $n \geq 0$. Then $\dim_F F[x_1, \dots, x_n]/(e_1, e_3, e_5, \dots; x_1^q, \dots, x_n^q) = n! \cdot [y^n] e^y I_0(2y)^{(q-1)/2}$.*

With $F = F_p$, $q = p^v$ and $n = N$, Theorem A says that $A_k(q) := \dim F_p[x_0, \dots, x_{2k+1}]/(E + (x_i^q))$ equals the number $P_k(q)$ of F_q -points of the union of the matching spaces (Corollary 10.1). **This is not the Main Theorem, and it does not imply it.** Theorem A is a *sum* statement at the *odd* box q on the grid *with* 0; the Main Theorem for $m = q$ is equivalent to an *intersection* statement at the *even* box $q - 1$ on the grid *without* 0 (Proposition 2.6), and §11 shows that the two are independent for families of matchings. The numbers differ as well: $P_2(3) = 141$ against $Q_2(3) = 20$. **As a count, Theorem A is not new:** in characteristic 0 it is a consequence of a classical theorem of Kostant [Kos], and in odd characteristic of a proposition of Bezrukavnikov, Riche and Rider [BRR] on modules with a good filtration, through the dictionary of Remark 10.4. The proof of Appendix A is elementary and independent of both.

1.7 The idea of the proofs

Write the ideal of Theorem B as $V \subseteq C_{2k+1}$ and the point set it should count as $Z \subseteq T^{2k+1}$, $T = F_q^\times$. Peel off the variable y_1 : the ideal splits into $q - 1$ slices $W_0 \subseteq \cdots \subseteq W_{q-2}$, ideals in the remaining variables, and the point set splits into $q - 1$ layers according to how many values of the first coordinate complete a given tail. If every layer is the point set of an ideal contained in the matching slice, induction on the number of variables gives $\dim V \geq |Z|$. To make this work we enlarge the family: to every down-set Λ of partitions under weak dominance we attach an ideal V_Λ , generated by products of divided differences D and Vandermonde determinants Δ , and a point set Z_Λ , the tuples whose «unpaired part» has shape in Λ . Three facts then carry the induction. The number of completions of a tail depends only on the shape μ of the tail (P1). The $q - 1$ possible new shapes form a chain for weak dominance, so the completions in Λ are an initial segment of the chain, and the layers are again down-sets (P2). And each generator of a layer can be lifted to the right slice by one of three explicit constructions, with no room to spare (P3). The full family of matchings enters only once, at the root: the down-set generated by the partition (1) has as ideal exactly the ideal of all the D_J .

For $m = q \cdot r$ with $q = p^v$, $p \nmid r$ and $r > 1$, $t^m - 1 = \prod_{\zeta \in \mu_r} (t - \zeta)^q$ over $\bar{F}_p$, so the group algebra is a product of local rings, one for each colouring c of the coordinates by r -th roots of unity. On the factor of c , the generator ψ_J vanishes unless every pair of J has colours ζ, ζ^{-1} ; the surviving generators are pure tensors along the colour classes, and the ideal is a tensor product of one ideal per class of colour 1 and one per pair of inverse colours. The class of colour 1 is an instance of Theorem 5.3. A pair of inverse colours becomes, after the change of variables $x = \zeta^{-1}t - 1$, $z = (\zeta t)^{-1} - 1$, a bipartite ideal, and the colour of the index 0, which is determined by the others, decides whether it is balanced or phantom. The count of the points factors over the colourings in the same way. For the bipartite ideals, the tail of a point now has two residues, one for each set of variables, and its shape is a pair of partitions: adding a value to the x -side removes a box from the z -residue, adds a box to the x -residue, or starts a new part, and these q options again form a chain, now in the product of two weak dominance orders. The proof of Theorem B then goes through with the box q in place of $q - 1$ and the binomial coefficients $C(q - 1, t) \equiv (-1)^t$ in place of the signs of D .

For even m the same reduction applies at each prime, but two blocks are new. At an odd prime the colour -1 is its own inverse, and after the substitution $u = -t$ its block is the ideal generated by the products of the $(y_a + y_b)^{q-1}$ in the box (y_i^q) . At the prime 2 the block of the colour 1 is the problem for the degree 2^v itself; there we replace each generator by its form of lowest degree in the variables $s = t + 1$, which is $s_1 \cdots s_{2k+1}$ times a product of the polynomials $\sum_w a^w b^{q-2-w}$, and the ideal of the leading forms of an ideal has the same dimension as the ideal. Both are instances of one statement, Theorem O: the count of Theorem B on a grid T with an odd number r of values, one of which, 0, is its own opposite. A tuple may then have one unpaired zero, so the shape of a tuple is a partition together with a mark $\delta \in \{0, 1\}$, and the new coordinate has one more option, the zero, which changes the mark. The r options still form a chain, provided the set of shapes Λ is an **interlaced pair**: a down-set of unmarked shapes and a down-set of marked shapes such that removing a box and switching the mark stays in Λ . The layers of an interlaced pair are interlaced pairs. On the side of the ideals the unmarked shapes carry the generators of §5, with the symmetric polynomial D_r in the place of the divided difference, and a marked shape carries, in the place of its first Vandermonde determinant, the Pfaffian of the antisymmetric polynomials $D_{r-1}(y_i, y_j)$ bordered by a Vandermonde matrix. Of the seven liftings of generators to slices, six are explicit, by expansions of Pfaffians; the seventh needs the membership of the bordered Pfaffian in the ideal generated by the products of a Vandermonde determinant and of polynomials D_r (Lemma 8.7). It follows from one fact: the generating function $\sum_\sigma \zeta^\sigma \omega_{2\sigma+1}(a, b)$ of the antisymmetric polynomials that interpolate between D_{r-1} and the multiples of D_r is $\text{Ev}(a) \cdot \text{Od}(b) - \text{Ev}(b) \cdot \text{Od}(a)$, a matrix of rank two. A rank-two update of

a bordered Pfaffian (Lemma 8.8) then expresses the Pfaffian of D_{r-1} through bordered Pfaffians whose entries are multiples of D_r , and a Laplace expansion finishes the proof.

1.8 A note on the history

For several months the project that produced this paper took the count $A_k(q) = P_k(q)$ of Theorem A to be the algebraic form of Conjecture 1.2. Two earlier notes of the author, on the cases $k = 2$ (*The Sofa Theorem* [Sofa]) and $k = 3$ (*The Hammock Theorem* [Ham]), were written under that identification and stated that they established Conjecture 1.2 in those dimensions. On 23 September 2026, re-deriving the reduction from the original [DS], we found that the identification had never been proved, and that it is false for families of matchings (§11). The conclusions of those notes about Conjecture 1.2 in dimensions 4 and 6 are nevertheless true: for odd m they are the cases $k = 2, 3$ of the Main Theorem, proved here by a different route. Versions 4 and 5 of this paper proved the Main Theorem for odd prime powers and stated the colour reduction for the degrees that are not prime powers as an open problem; the reduction and the bipartite count (§6–§7), added in version 6, complete it. Version 8 added the machine-checked proof of Main Theorem' (§14.8), recorded that the repository [Rep] is public, stated the status of the *Double Ladder* theorem more precisely (Remark 12.2), and added one clause to the proof of Lemma 6.8; no statement and no proof of version 7 changed. Version 9 corrected the attribution of Theorem A: in characteristic 0 it follows from a theorem of Kostant, which the earlier versions did not cite (Remark 10.4). It also recorded that the *Watermark* and *Double Ladder* theorems are now proved for every prime and verified in Lean [WDL] (Remark 12.2). Again no statement and no proof changed. Version 10 corrects the attribution of Theorem A a second time: version 9 said that we knew no version of Kostant's theorem in positive characteristic that gives the count, and there is one, [BRR, Proposition 2.12], which we had not read (Remark 10.4(3)). It also adds the reading of Theorem B in the same language (Proposition 10.5, Corollary 10.6, Remark 10.7) and the equality for the ideals of Appendix A (Corollary A.17), restates problem 6 of §15 and adds problem 7. A supplementary note [Note], deposited with this version, presents the dictionary on its own, with a statistic on walks that gives the Hilbert series of the ring of Theorem A. No statement and no proof of the earlier versions changes. Version 11 proved the conjecture for the even degrees, which version 10 listed as its first open problem, and with it the odd box, which was its seventh: §8 (Theorem O) and §9 (Theorem 9.11) are new. Sections 8 to 14 of version 10 are now sections 10 to 16, with the same internal numbering (Proposition 8.5 of version 10 is Proposition 10.5 here, §12.8 is §14.8, and so on). §7 is now stated for every integer $q \geq 2$, because §9 uses it for $q = 2^v$; its proofs are unchanged. The Main Theorem, Main Theorem' and Corollaries H and W are now stated for every $m \geq 3$; for odd m they are the statements of version 10. New in §10 and §12: Corollary 10.8 and (H4'). The even degrees were found on 2 October 2026 by replacing the generators at $m = 2^v$ by their leading forms, which had been measured to generate an ideal of the right dimension in seven cells, and then proving the count for that ideal. Version 11 was not made public; every statement of it is in the present version, and the two proofs of it that the present version replaces are described where they stood (§8.5, Remark (4); Lemma 9.10). Version 12 (the present one) changes no statement of a theorem, proposition or corollary of version 11, nor Lemma 8.7; the auxiliary results of §8.5 are new (Lemma 8.7', and a Lemma 8.8 and a Corollary 8.9 whose numbers version 11 used for other statements), and the properties of §8.3 are now stated over every commutative ring (version 11: without 2-torsion). Main Theorem' and Theorem O are now proved in Lean 4 for every degree (§14.8). Three proofs are printed in the form that was formalized, which is shorter: Lemma 8.7 by a rank-two update of bordered Pfaffians, in place of the exterior algebra with divided powers of version 11 (§8.5), which also gives the membership for other border sets (Lemma 8.7'); the upper bound of Corollary 8.13 by a pairing of the box ring, so that §8 no longer uses §10; and Lemma 9.10, without the injectivity of the map θ . The signs of §8.3 are

given explicitly, and its properties are attributed to the classical sources. The version also adds the summary of §1.0 and the literature of §1.10; incorporates the notes of the cold reading of the printed text of version 11 (§14.6); corrects the place of Mizukami's theorem (§1.3); and writes the condition of the title in the form $(n + 1)!$ of [AMV], which is the same condition as the $(n + 2)!$ of version 11. Before it was made public, every passage that is new in the writing of version 12 was read cold, with the verdict «holds» (§14.6); its notes are incorporated, and one of its observations extends Remark (2) of §8.5.

1.9 Notation

q is odd in §2–§6 and §10–§11. In §2, §6 and §11, p is an odd prime and $q = p^v$. §5 is stated for every odd q over an arbitrary field. §7 is stated for every integer $q \geq 2$ over a field in which the binomial coefficients $C(q - 1, t)$ are non-zero, and is applied with $q = p^v$ for every prime p , 2 included. In §8, r is odd and the box is r . In §9, m is even, r is the odd box and r' is the cofactor that §6 calls r . The word «block» means a column block B_c of a pattern in §5, §7 and §8, and a block of a colouring in §6 and §9; the letter R , with subscripts, denotes several rings (R of §2, R_c of §6, $R_{A,B}$ of §7), each defined where it is used. Symbols introduced inside a section are local to it (§6–§7 have their own local symbols), and Appendix A has its own symbols. Some letters have two or three meanings in different places, each declared where it is used: θ is the map of Lemma 8.12, of Lemma 9.10 and of Corollary 10.6 (the sign of the expansion (F4) is written ϑ); N is $2k + 2$, and in §8.3 a finite ordered set of indices; R is the ring of §2, and in the proof of Proposition 8.10 a product of Vandermonde determinants; σ is a shape in §8.2 and §8.6, an index of the polynomials $\omega_{2\sigma+1}$ in §8.5, and a bijection in §6, §7 and §9.3; ζ is a colour in §6 and §9 and a formal variable in §8.5; η is $e^{\pi i/m}$ in Appendix B, and η_b are the signs of (F2) in §8.3 and §8.6; ρ is a row in §8.2 and §8.6 and the generator ρ_J of [DS] in Remark 2.5'; E is the ideal of §1.6 and §10, an exponent set E_ℓ in §8.5 and §8.6, and a border column in Lemma 8.8; κ is a partition in the proof of Lemma 8.4 and the number $(n - s)/2$ in §8.5; H is the matrix of Corollary 8.9, and H' a group in Lemma 9.10; S is a set of indices, the Pham cycle in Appendix B and a polynomial ring in §11; and r is the odd box in §8 and §9, the cofactor in §6 (written r' in §9), and a row in §5.5.

symbol	meaning	first use
$\mathcal{J}, J, (2k + 1)!!$	perfect matchings of $\{0, \dots, 2k + 1\}$, written with $j_0 = 0$	§1.1
N	$2k + 2$, the number of homogeneous coordinates	§1.2
R, ψ_J, Γ_K	the ring, the generators and the point set of [DS]	§2
T, h	$F_q^\times$ (or any set of $q - 1$ elements with a fixed-point-free involution $u \mapsto -u$); $h = (q - 1)/2$ classes $\{u, -u\}$	§2.2
$Q_k(m)$	$ \Gamma_{\mathcal{J}} : N! \cdot [x^N] I_0(2x)^{(m-1)/2}$ for odd m , $N! \cdot [x^N] \cosh(x) \cdot I_0(2x)^{(m-2)/2}$ for even m	§1.2, §9.1
B, C, C_m	the box rings (y_i^q) and (y_i^{q-1})	§2.3, §5
$D(a, b), D_J, D_P$	divided differences and their products over pairs	§2.3, §5.2
$\Delta(B)$	the Vandermonde determinant of an index set B	§5.2
$\nu(M), \lambda(M)$	the number of negation pairs of a tuple, and the partition of its residue	§3, §5.2
$\text{Par}_m^{(h)}, \preceq, S_t$	partitions allowed at m coordinates; weak dominance; sums of the t largest parts	§5.2

symbol	meaning	first use
V_Λ, Z_Λ	the ideal and the point set of a down-set Λ (§5.2); of a down-set of pairs of partitions (§7.2)	§5.2, §7.2
$W_j(V), F_\Lambda(\mu), \Lambda_i$	slices, completion counts, layers	§5.1, §5.4
$\text{gr}(I)$	the ideal of top-degree forms of an ideal I	§5.9
$c, \mathcal{C}_\zeta, \mu_r$	a colouring of the coordinates, its colour classes, the r -th roots of unity	§6
$I_a^{\text{bal}}, I_a^{\text{ph}}, N_{\text{bal}}, N_{\text{ph}}$	the bipartite ideals and their counts	§6.5, §6.6
$\text{BPar}_q(\alpha, \beta)$	pairs of partitions, with the product of weak dominance orders	§7.2
r, h, T (in §8)	an odd number $r = 2h + 1$; a set T of r elements with an involution with one fixed point 0	§8
$D(a, b), D^-(a, b)$ (in §8)	$D_r(a, b)$, symmetric, and $D_{r-1}(a, b)$, antisymmetric	§8
$N_r(n)$	$n! \cdot [x^n]e^x I_0(2x)^{(r-1)/2}$	§8, §10
$\text{Sh}_m, (\lambda, \delta), \Lambda^0, \Lambda^1$	shapes with a mark $\delta \in \{0, 1\}$; the two components of a set of shapes; interlaced pairs (Definition 8.2)	§8.2
$\text{Pf}(N; c), \text{Pf}_E(N), E_\ell, B_0$	bordered Pfaffians; the border exponents; the marked block of a pattern	§8.3, §8.4
$\omega_s, \text{Ev}, \text{Od}, \mathfrak{U}_\ell(N)$	the antisymmetric polynomials of §8.5; the two columns of its key identity; the ideal of the membership lemma	§8.5
$r', \mathcal{C}_{-1}, I_{c,-1}$	the cofactor of $q = p^v$ in an even m ; the class of the colour -1 and its block	§9
$E, A_k(q), P_k(q)$	odd symmetric ideal; the sum count and the point count of Theorem A	§1.6, §10
$C_r, D_r(a, b), D_{r,J}$	the box ring (x_i^r) in $2s$ variables; the copairing and its products over a matching (Proposition 10.5)	§10
$V, e, \mathcal{Z}, g_t$	$F[x]/(x^q)$ with its form; multiplication by x ; the centralizer of e in $\text{SO}(V)$; the Cayley transform (Remark 10.4)	§10
m	the degree of the Fermat variety (§1, §2, §6, §12, §13); in §5 and Appendix A, the number of variables	—
$\mathfrak{A}, \mathfrak{B}, \alpha $	characters of the primitive cohomology; Hodge characters; the degree of a character	§12

1.10 Literature and priority

Before this version we searched the literature for each result that we call new: the arXiv listings and its index of titles and abstracts; Google Scholar and the open web; the papers that cite [DS], through Semantic Scholar and OpenAlex; the publication lists of the authors of [DS]; MathOverflow; and GitHub, including Mathlib and DeepMind’s formal – conjectures repository, for formalizations. The queries, their dates and their results are recorded in [Rep], **record/literature/**. The sources that decide an attribution were read in the original; the others are cited for the statement they make, and the list of references says which is which. What we found:

- *The even degrees.* To the best of our knowledge, no proof of Conjecture 1.2 for an even degree $m \geq 4$ and $k \geq 1$ had appeared before this paper, beyond the cells confirmed by computer in [DS, §5] (and the case $k = 1$, which is [De14]). The conjecture is listed as open in [De15, Conjecture 4.4].

- *The odd box.* Over Q , Theorem O and Corollary 10.8 can be derived from Kostant's theorem and the first fundamental theorem of invariant theory for the orthogonal group (Remark 10.7(2)); we did not find this derivation written. In positive characteristic we did not find Theorem O, or the statement that the tensors $D_{r,J}$ generate the invariants of the centralizer of a regular unipotent element (Corollary 10.8 and Remark 10.7), in the literature, in particular not in [BRR], [Ric] or [Liu]. To the best of our knowledge, both are new in positive characteristic.
- *Corollary H.* The implication from the primitivity of $L(X)$ to $\text{Hdg}(X) = L(X)$ in the degrees of (i) is the argument of [AMV, §1], with the degrees of Aoki's theorem [Aok]; for $k = 1$ the statement is known ([Miz], [SSvL], [De14]); for $m = 4$ and $k = 2, 3$, and in the prime cells of [DS, §5], it already followed from computations (§1.3). For $k \geq 2$ the uniform statement — every prime m , the quartics of dimension at least 8, every non-prime m of (i), and part (ii) — is, to the best of our knowledge, new.
- *Corollary W.* The implication «Conjecture 1.2 in dimension $2s \implies$ (i)» is [DS, Corollary 1.7]; what is new is that the hypothesis is now a theorem.
- *Theorem A* is due, as a count, to Kostant and to [BRR] (Remark 10.4); our contribution there is the dictionary and an elementary proof.
- *Pfaffians.* The properties (i)–(iii), (F1)–(F4) and (F7) of §8.3 are classical; we cite [Knu] and [Oka]. We did not find the rank-two update of Lemma 8.8 in the sources we read, and we claim nothing for it: it is of the kind of the classical expansions of the Pfaffian of a sum of two alternating matrices, which we have not traced to a source that we have read. Its use to prove the membership lemma (Lemmas 8.7, 8.7') is ours.
- *Orbit harmonics.* The lower bounds by degenerating the ideal of a finite set of points to the ideal of its top-degree forms (Lemma 5.8', Proposition A.5) are the classical method of orbit harmonics (see [GP]).
- *Formalization.* We found no Pfaffian in Mathlib (the version used, tag v4.28.0); we defined Pfaffians and bordered Pfaffians in our project. A separate partial formalization of skew-symmetric matrices and Pfaffians exists outside Mathlib (`Qsdd/Skewsymmetric` on GitHub). We found no formalization of results of the kind of [DS]; to the best of our knowledge, §14.8 is the first machine-checked proof of a case of Conjecture 1.2.
- *Related work on the rational Hodge conjecture:* [Jum], [MMRV], [FK] (§1.3).

2. The translation: Conjecture 1.2 as a dimension count

This section is written from the original [DS] (arXiv:1405.4683v3, the latest version; J. Math. Soc. Japan 68 (2016)), and uses its notation.

- $R := Z[t_1, \dots, t_{n+1}]/(t_1^m - 1, \dots, t_{n+1}^m - 1)$, the group ring of $G \cong (Z/m)^{n+1}$, which acts on X by multiplying the coordinates by m -th roots of unity. The variable $t_0 := (t_1 \cdots t_{n+1})^{-1}$ never enters below.
- $\varphi(u) := u^{m-1} + \cdots + u + 1$.
- For $J \in \mathcal{J}$: $\tau_J := \prod_{i=0}^k (t_{k_i} - 1)$ and $\psi_J := \tau_J \cdot \prod_{i=1}^k \varphi(t_{j_i} t_{k_i})$. Since $j_0 = 0$, the pair containing 0 contributes only the factor $t_{k_0} - 1$.
- $\Gamma_K \subseteq \mu_m^{n+1}$ [DS, Definition 1.3] is the set of $(a_1, \dots, a_{n+1})$ with $a_i \neq 1$ for every i such that, for some $J \in K$, $a_{j_i} a_{k_i} = 1$ for $i = 1, \dots, k$.

We use four results of [DS], collected here.

THEOREM 0 [DS]. *Let $n = 2k \geq 2$, $m \geq 3$, $\emptyset \neq K \subseteq \mathcal{J}$, and $A_K := R/(\psi_J : J \in K)$.*

- (a) [DS, Theorem 1.1(a)] $\text{Tors}(H_n(X)/L_K(X)) \cong \text{Tors}(A_K)$.
- (b) [DS, Claim 4.3] *If K_p is an algebraically closed field of characteristic $p = 0$ or $p \nmid m$, then $\dim_{K_p}(A_K \otimes K_p) = m^{n+1} - |\Gamma_K|$.*
- (c) [DS, Theorem 1.4] $\text{rank } L_K(X) = |\Gamma_K| + 1$.
- (d) [DS, Corollary 1.5] *The order of the torsion of $H_n(X)/L_K(X)$ is divisible only by primes dividing m .*

Part (b) is algebraic: it is a count of points by the Chinese remainder theorem (Appendix B, Step 6). Parts (c) and (d) follow from (a), (b) and the proof of (a) in a few lines. For the reader who wants to check the only topological input, Appendix B gives a self-contained proof of Theorem 0 modulo two results that we do not re-prove: Pham's description of the homology of the affine Fermat variety [Ph], and the intersection numbers of the standard spaces with the Pham cycle [DS, Theorem 2.2].

2.1 Torsion as one dimension

Proposition 2.1. *Let $\emptyset \neq K \subseteq \mathcal{J}$. For every prime p , $\dim_{F_p}(A_K \otimes F_p) \geq m^{n+1} - |\Gamma_K|$, and $H_n(X)/L_K(X)$ is torsion free if and only if equality holds for every prime p dividing m . More precisely, for each prime p , equality holds iff A_K has no p -torsion, iff $H_n(X)/L_K(X)$ has no p -torsion.*

Proof. R is a free Z -module of rank m^{n+1} (basis t^ν , $\nu \in (Z/m)^{n+1}$), so A_K is a finitely generated abelian group; write $A_K \cong Z^\rho \oplus \bigoplus_\ell T_\ell$ with T_ℓ a finite ℓ -group. Tensoring with F_p gives $\dim_{F_p}(A_K \otimes F_p) = \rho + c_p$, where c_p is the number of cyclic factors of T_p (since $Z/\ell^a \otimes F_p$ is F_p for $\ell = p$ and 0 otherwise). By Theorem 0(b) with $p = 0$, $\rho = \dim_C(A_K \otimes C) = m^{n+1} - |\Gamma_K|$. So the inequality holds, and equality at p means $T_p = 0$. (This part of the proof uses only Theorem 0(b), which is algebraic.) By Theorem 0(a), $H_n(X)/L_K(X)$ is torsion free iff A_K is; by Theorem 0(d), only primes dividing m can occur. ■

From now on, until the end of §5, p is an odd prime, $v \geq 1$ and $m = q = p^v$ (odd m that are not prime powers are treated in §6–§7). Then only the prime p matters, and $A_K \otimes F_p = F_p[G]/(\bar{\psi}_J : J \in K)$, where $F_p[G] := F_p[t_1, \dots, t_{2k+1}]/(t_i^q - 1)$ and $\bar{\psi}_J$ is the image of ψ_J .

2.2 The count

Let T be a finite set of $q - 1$ elements with a fixed-point-free involution $u \mapsto -u$ (for instance $T = F_q^\times$). It has $h := (q - 1)/2$ orbits $\{u, -u\}$, which we call **classes**.

Lemma 2.2. *For odd q , $|\Gamma_{\mathcal{J}}| = Q_k(q)$. More precisely, $|\Gamma_{\mathcal{J}}|$ is the number of N -tuples in $\mu_q \setminus \{1\}$ whose multiset is closed under inversion, and this is also the number of N -tuples in T whose multiset is closed under the involution.*

Proof. Let $a = (a_1, \dots, a_{2k+1}) \in \Gamma_J$ and put $a_0 := (a_1 \cdots a_{2k+1})^{-1}$. The pairs $\{j_i, k_i\}$, $i \geq 1$, cover $\{1, \dots, 2k+1\} \setminus \{k_0\}$ and their products are 1, so $\prod_{i \geq 1} a_i = a_{k_0}$ and $a_0 = a_{k_0}^{-1} \neq 1$. Hence $a \in \Gamma_{\mathcal{J}}$ iff the multiset $\{a_0, \dots, a_{2k+1}\} \subseteq \mu_q \setminus \{1\}$ splits into inverse pairs. Conversely, if an N -tuple in $\mu_q \setminus \{1\}$ is closed under inversion, its product is 1, so it is determined by its last

$2k + 1$ entries. Since q is odd, inversion has no fixed point on $\mu_q \setminus \{1\}$, which splits into h pairs $\{c, c^{-1}\}$. By the exponential formula (the generating function of a product of labelled structures is the product of the generating functions), each pair contributes the factor $\sum_b x^{2b}/(b!)^2 = I_0(2x)$ (choose b coordinates equal to c and b equal to c^{-1}). This gives $Q_k(q)$, and the same computation applies to T . ■

Lemma 2.2 and its proof hold for every odd m in place of q ; §6, §12 and §13 use it in that form. Likewise Lemma 2.3 below holds in any ring $F[t]/((t-1)^q)$ with $F \supseteq F_p$ a field and $q = p^v$, and Lemma 2.4(i) over any such field F ; this is how §6.4 uses them.

External check. At $k = 1$, $Q_1(q) = 3(q-1)(q-2)$, so $\text{rank } L(X) = 3(m-1)(m-2) + 1$. For $m = 3$ this is 7, the Picard number of the cubic surface, which is generated by its 27 lines. It agrees with the constant-term description of $\text{rank } L(X)$ in [DS, Remark 4.4].¹

2.3 A coordinate in which the relations become linear

Lemma 2.3 (identities in characteristic p). *In $F_p[t]/(t^q - 1)$ put $y := t - t^{-1}$. Then:*

- (i) $F_p[t]/(t^q - 1) = F_p[y]/(y^q)$, and $t \mapsto t^{-1}$ becomes $y \mapsto -y$;
- (ii) in $F_p[t_j, t_k]/(t_j^q - 1, t_k^q - 1)$, $t_j t_k - 1 = (\text{unit}) \cdot (y_j + y_k)$;
- (iii) $\varphi(u) = (u - 1)^{q-1}$ in $F_p[u]$.

Proof. (i) $t^q - 1 = (t - 1)^q$ in characteristic p , because $q = p^v$; so $t - 1$ is nilpotent, and the ring is local with maximal ideal $(t - 1)$. The elements t and $t + 1 = 2 + (t - 1)$ are units, the second because $2 \in F_p^\times$. Hence $y = t^{-1}(t - 1)(t + 1)$ is a unit times $t - 1$, so $y^j \neq 0$ for $j \leq q - 1$ and $y^q = (\text{unit}) \cdot (t - 1)^q = 0$. The q elements $1, y, \dots, y^{q-1}$ lie in successive powers of the maximal ideal and not in the next, so they are linearly independent; the ring has dimension q , so it is $F_p[y]/(y^q)$. Inversion sends $t - t^{-1}$ to $t^{-1} - t = -y$. (ii) $y_j + y_k = t_j + t_k - t_j^{-1} - t_k^{-1} = (t_j + t_k)(t_j t_k)^{-1}(t_j t_k - 1)$, and $t_j + t_k = 2 + (t_j - 1) + (t_k - 1)$ is a unit. (iii) $(u - 1)\varphi(u) = u^q - 1 = (u - 1)^q$, and $F_p[u]$ is a domain. ■

Write $B := F_p[y_1, \dots, y_{2k+1}]/(y_1^q, \dots, y_{2k+1}^q)$; by (i), $F_p[G] \cong B$. Put

$$D(a, b) := \sum_{u=0}^{q-2} (-1)^u a^u b^{q-2-u} = (b^{q-1} - a^{q-1})/(a + b).$$

The second expression holds in $Z[a, b]$ because $q - 2$ is odd. D is antisymmetric, $D(b, a) = -D(a, b)$, and at $q = 3$ it is $D(a, b) = b - a$.

Lemma 2.4 (identities in characteristic p). (i) $(a + b)^{q-1} \cdot b = -ab \cdot D(a, b)$ in $F_p[a, b]/(b^q)$. (ii) For every $J \in \mathcal{J}$, $\bar{\psi}_J = (\text{unit}) \cdot Y \cdot D_J$ in B , where $Y := y_1 y_2 \cdots y_{2k+1}$ and $D_J := \prod_{i=1}^k D(y_{j_i}, y_{k_i})$ is the product over the k pairs of J that do not contain 0.

Proof. (i) The sum $(a + b) \cdot \sum_{s=0}^{q-1} (-1)^s a^s b^{q-1-s}$ telescopes to $(-1)^{q-1} a^q + b^q = a^q + b^q$, which is $(a + b)^q$ in characteristic p . So $(a + b)^{q-1} = \sum_{s=0}^{q-1} (-1)^s a^s b^{q-1-s}$ in the domain $F_p[a, b]$. Multiply by b and drop b^q : $\sum_{s=1}^{q-1} (-1)^s a^s b^{q-s} = -ab \cdot \sum_{u=0}^{q-2} (-1)^u a^u b^{q-2-u}$. (ii) By Lemma 2.3, up to a unit, $\bar{\psi}_J = \prod_{i=0}^k y_{k_i} \cdot \prod_{i=1}^k (y_{j_i} + y_{k_i})^{q-1}$. By (i), $y_{k_i}(y_{j_i} + y_{k_i})^{q-1} = -y_{j_i} y_{k_i} D(y_{j_i}, y_{k_i})$ for each $i \geq 1$. The indices $\{k_0\} \cup \bigcup_{i \geq 1} \{j_i, k_i\}$ are exactly $\{1, \dots, 2k + 1\}$, so the monomial factors multiply to Y . ■

¹The polynomials displayed in [DS, Remark 4.4] are, for odd m , the corresponding values of $|\Gamma_{\mathcal{J}}|$, in accordance with the constant-term description $\text{rank } L(X) = 1 + |\Gamma_{\mathcal{J}}|$ given there; this is how we quote them in §3.

2.4 The sum form (S)

Let $C := F_p[y_1, \dots, y_{2k+1}]/(y_1^{q-1}, \dots, y_{2k+1}^{q-1})$, of dimension $(q-1)^{2k+1}$.

Proposition 2.5 (the translation). *Let $q = p^v$, $k \geq 1$ and $\emptyset \neq K \subseteq \mathcal{J}$. Then $\dim_{F_p} F_p[G]/(\bar{\psi}_J : J \in K) = q^{2k+1} - \dim_{F_p}(D_J : J \in K)C$, and*

- $\dim_{F_p}(D_J : J \in K)C \leq |\Gamma_K|$ *always;*
- $H_{2k}(X)/L_K(X)$ *is torsion free iff $\dim_{F_p}(D_J : J \in K)C = |\Gamma_K|$.*

In particular ($K = \mathcal{J}$), the Main Theorem at (k, q) is equivalent to

$$(S) \dim_{F_p}(D_J : J \in \mathcal{J}) \cdot C = Q_k(q).$$

Proof. Multiplication by Y on B kills exactly the monomials having some exponent $\geq q-1$, so its kernel is $(y_1^{q-1}, \dots, y_{2k+1}^{q-1})B$, and it induces an injective linear map $C \rightarrow B$, $f \mapsto Yf$. By Lemma 2.4(ii), the ideal $(\bar{\psi}_J : J \in K)B = (YD_J : J \in K)B$ is the image of the ideal $(D_J : J \in K)C$ under this map, so the two have the same dimension. The two claims follow from Proposition 2.1 and Lemma 2.2. $\blacksquare$

Remarks 2.5'. (1) The generators D_J all have degree $k(q-2)$. (2) **What the topology is needed for.** The inequality $\dim(D_J)C \leq Q_k(q)$ can also be proved with no topology: it is part of Theorem 5.9, and it also follows from Propositions 2.6 and 11.1. The inequality is also the case $p|m$ of Proposition 2.1, whose proof uses only Theorem 0(b), a Chinese-remainder count. [DS] is needed only for two things: that equality in (S) is *equivalent* to torsion-freeness, and the rank of $L(X)$. (3) [DS, §5] formulate a computational criterion of the same kind in the ring $\bar{R} := Z[t_1, \dots, t_{n+1}]/(\varphi(t_1), \dots, \varphi(t_{n+1}))$, through their Lemma 4.5 ($\psi_J = \pm \lambda \rho_J$, $\lambda = \Pi(t_i - 1)$). We do not use it.

2.5 An equivalent intersection form

Proposition 2.6. *Let $I'_J := (y_{j_i} + y_{k_i} : i = 1, \dots, k)$ and $b_k(r) := \dim F_p[y_1, \dots, y_{2k+1}]/\bigcap_{J \in \mathcal{J}}(I'_J + (y_1^r, \dots, y_{2k+1}^r))$. Then $\dim(D_J : J \in \mathcal{J})C = b_k(q-1)$, so (S) is equivalent to $b_k(q-1) = Q_k(q)$. Eliminating $x_0 := -(y_1 + \dots + y_{2k+1})$, $b_k(r) = \dim F_p[x_0, \dots, x_{2k+1}]/\bigcap_{J \in \mathcal{J}}(I_J + (x_0^r, \dots, x_{2k+1}^r))$ with $I_J := (x_a + x_b : \{a, b\} \in J)$.*

Proof. On B put $\langle f, g \rangle :=$ the coefficient of $\prod_i y_i^{q-1}$ in fg . Then $\langle y^\alpha, y^\beta \rangle = 1$ if $\alpha + \beta = (q-1, \dots, q-1)$ and 0 otherwise, a permutation matrix, so the pairing is non-degenerate. For an ideal $I \subseteq B$, $\langle f, gh \rangle = \langle fg, h \rangle$ shows that $f \in \text{ann}_B(I)$ iff $f \perp I$; hence $\dim \text{ann}_B(I) = \dim B - \dim I$, and $\text{ann}_B(\sum_J I_J) = \bigcap_J \text{ann}_B(I_J)$. So $\dim(\bar{\psi}_J : J)B = \dim B / \bigcap_J \text{ann}_B(\bar{\psi}_J)$, which equals $\dim(D_J : J)C$ by the proof of Proposition 2.5. For a fixed J , the linear forms $w := y_{k_0}$, $u_i := y_{j_i} + y_{k_i}$, $v_i := y_{k_i}$ ($i \geq 1$) form a basis of $F_p y_1 \oplus \dots \oplus F_p y_{2k+1}$. Since $\ell^q = \sum c_i y_i^q$ for every linear form $\ell = \sum c_i y_i$ over F_p (Frobenius, and $c^q = c$ on F_p), the ideal (y_i^q) is also generated by w^q, u_i^q, v_i^q . In these coordinates $\bar{\psi}_J = (\text{unit}) \cdot w \cdot \prod_{i \geq 1} v_i u_i^{q-1}$, a monomial times a unit, whose annihilator in the box ring is the monomial ideal $(w^{q-1}) + (v_i^{q-1}, u_i : i \geq 1)$. Modulo u_i one has $y_{j_i} \equiv -v_i$, so this ideal is $I'_J + (y_1^{q-1}, \dots, y_{2k+1}^{q-1})$. Finally $y_i^q \in (y_i^{q-1})$, so $B / \bigcap_J (\dots) = F_p[y]/\bigcap_J(I'_J + (y_i^{q-1}))$. For the last sentence, put $\sigma := x_0 + \dots + x_{2k+1}$ and substitute $y_i = x_i$ ($i \geq 1$), $x_0 = -\sum y_i$. Two facts are used. (1) Every I_J contains σ (it is the sum of the generators $x_a + x_b$); by the correspondence between the ideals of S containing σ and the ideals of $S/(\sigma) \cong F_p[y]$, the intersection of the ideals $I_J + (x_i^r)$ maps onto the intersection of their images. (2) Modulo I_J , $x_0 \equiv -x_{k_0}$, so $x_0^r \in I_J + (x_1^r, \dots, x_{2k+1}^r)$, and the image of $I_J + (x_0^r, \dots, x_{2k+1}^r)$ is $I'_J + (y_1^r, \dots, y_{2k+1}^r)$. $\blacksquare$

By Matlis duality this form is **equivalent** to (S), not weaker: it is a restatement, not a reduction. It is used in §11.

2.6 A worked example: the cubic surface, $(k, q) = (1, 3)$

Here $n = 2$, $N = 4$, and $\mathcal{J}$ has three matchings, $[[0, 1], [2, 3]]$, $[[0, 2], [1, 3]]$, $[[0, 3], [1, 2]]$. The pairs avoiding 0 are $(2, 3)$, $(1, 3)$, $(1, 2)$, and at $q = 3$, $D(a, b) = b - a$, so the generators are $y_3 - y_2$, $y_3 - y_1$, $y_2 - y_1$ in $C = F_3[y_1, y_2, y_3]/(y_1^2, y_2^2, y_3^2)$, of dimension 8. The ideal they generate has dimension 2 in degree 1 (two of the three are independent), 3 in degree 2 ($y_1(y_2 - y_1) = y_1y_2$, $y_1(y_3 - y_1) = y_1y_3$, and $y_2(y_3 - y_1) = y_2y_3 - y_1y_2$), and 1 in degree 3: in total 6. On the other side, $T = F_3^\times = \{1, 2\}$, and Γ' (§3) consists of the tuples in T^3 with one negation pair, i.e. the $2^3 - 2 = 6$ non-constant tuples. So (S) holds, $\text{rank } L(X) = 7$, and $\dim F_3[G]/(\psi_J) = 3^3 - 6 = 21$.

3. The count

By Lemma 2.2, $Q_k(q) = N! \cdot [x^N]I_0(2x)^h$ with $N = 2k + 2$ counts the N -tuples in T whose multiset is closed under the involution. In small cases:

- $Q_0(q) = q - 1$;
- $Q_1(q) = 3(q - 1)(q - 2)$ (the coefficient of x^4 in $I_0(2x)^h$ is $h/4 + h(h - 1)/2$, times 4!);
- $Q_k(3) = C(2k + 2, k + 1)$ (here $h = 1$, and $[x^{2k+2}]I_0(2x) = 1/((k + 1)!)^2$);
- $Q_2(q) = 15q^3 - 90q^2 + 175q - 100$ and $Q_3(q) = 105q^4 - 1050q^3 + 3955q^2 - 6335q + 3325$, the polynomials of [DS, Remark 4.4].

$q \setminus k$	1	2	3	4	5
3	6	20	70	252	924
5	36	400	4 900	63 504	853 776
7	90	1 860	44 730	1 172 556	32 496 156
9	168	5 120	190 120	7 939 008	357 713 664
11	270	10 900	551 950	32 232 060	2 070 891 900
13	396	19 920	1 281 420	96 807 312	8 175 770 064
25	1 656	182 400	26 926 200	4 890 642 624	1 038 711 332 736
27	1 950	234 260	37 849 630	7 550 855 676	1 767 675 505 596

(By the Main Theorem, for $m = q$, $\text{rank } L(X) = Q_k(q) + 1$ and $L(X)$ is primitive in every cell of the table.)

The zero-free point set. For the proof we use a set of points of the same cardinality. For a tuple M in T let $\nu(M)$ be the largest number of pairwise disjoint pairs of indices $\{a, b\}$ with $y_b = -y_a$, and put

$$\Gamma' := \{y \in T^{2k+1} : \nu(y) = k\}.$$

Lemma 3.1. $|\Gamma'| = Q_k(q)$.

Proof. In each class $\{u, -u\}$, a tuple M has a entries equal to u and $\bar{a}$ equal to $-u$; the class contributes $\min(a, \bar{a})$ disjoint negation pairs, and $\nu(M)$ is the sum of these contributions, since negation pairs never leave a class. If $\nu(y) = k$ for $y \in T^{2k+1}$, then exactly one entry

is left unpaired, with a value w . Appending $-w$ gives an N -tuple closed under the involution. Conversely, if an N -tuple is closed under the involution, deleting its last entry z leaves a $(2k+1)$ -tuple with $\nu = k$ whose unpaired value is $-z$, so the last entry is determined by the others. This is a bijection onto the closed N -tuples, which number $Q_k(q)$ by Lemma 2.2. ■

4. Warm-up: the cubic case $q = 3$

For $q = 3$ the proof of §5 applies, but there is a shorter proof that also produces an explicit basis. It works over every field; we write it over F_3 . Put $n' := 2k + 1$. Then $C = F_3[y_1, \dots, y_{n'}]/(y_i^2)$ has the basis $y_U := \prod_{i \in U} y_i$, $U \subseteq [n'] := \{1, \dots, n'\}$, and $D(a, b) = b - a$, so $D_J = \prod_{(a,b)} (y_b - y_a)$ over the k pairs $(a < b)$ of J not containing 0. Order the monomials lexicographically with $y_1 > y_2 > \dots > y_{n'}$.

For $U \subseteq [n']$, read $i = 1, \dots, n'$ as a path: an up-step if $i \in U$, a down-step if $i \notin U$. Let $h(i) := |U \cap [i]| - |[i] \setminus U|$, and let $\mathcal{U} := \{U : h(i) \geq -1 \text{ for all } i\}$ (paths that never go below -1).

Theorem 4.1. *For every $k \geq 0$, $\dim_{F_3}(D_J : J \in \mathcal{J})C = C(2k+2, k+1) = Q_k(3)$. The lexicographic leading monomials of the ideal are exactly the y_U , $U \in \mathcal{U}$, and its graded ranks are $C(n', u) - C(n', u+2)$ in degree $u = k, \dots, n'$. Hence Conjecture 1.2 of [DS] holds for the cubic Fermat variety of every even dimension.*

Proof. (i) *Leading monomials of certificate elements.* For $T \subseteq [n']$ and $J \in \mathcal{J}$ with $\{0, c\} \in J$, the element $y_T \cdot D_J$ is $y_c^{[c \in T]} \cdot \prod_{(a,b)} f_{a,b}$, where $f_{a,b} = y_b - y_a$ if $\{a, b\} \cap T = \emptyset$ («untouched»), $f_{a,b} = y_a y_b$ if $a \in T \not\equiv b$, $f_{a,b} = -y_a y_b$ if $b \in T \not\equiv a$, and $f_{a,b} = 0$ if $\{a, b\} \subseteq T$. The factors involve disjoint sets of variables, so a non-zero $y_T D_J$ is a sum of $2^{\#\text{untouched}}$ distinct squarefree monomials with coefficients ± 1 . The lexicographically largest one chooses $-y_a$ in every untouched pair: two of these monomials first differ at the smaller element of a pair where the choices differ, and that element is an a . So $\text{LM}(y_T D_J) = y_U$ with coefficient ± 1 , where $U = \{a : (a, b) \text{ untouched}\} \cup \bigcup_{\text{touched}} \{a, b\} \cup (\{c\} \cap T)$.

(ii) *Every $U \in \mathcal{U}$ is reached.* Match the steps greedily: each down-step $i \notin U$ is matched with the nearest earlier unmatched up-step. A down-step stays unmatched exactly when the path reaches a new minimum below 0 at it, so the number of unmatched down-steps is $\max(0, -\min_i h(i)) \leq 1$.

- If there is one unmatched down-step, call it c . The number of unmatched up-steps is then $|U| - (n' - |U| - 1)$, which is even.
- If there is none, $2|U| - n'$ up-steps are unmatched. This number is odd and ≥ -1 , hence ≥ 1 ; let c be the largest unmatched up-step. An even number remain.

Pair the remaining unmatched up-steps consecutively into «full pairs». The matched pairs $(a < b)$, the full pairs and $\{0, c\}$ form a matching $J \in \mathcal{J}$. Let T consist of the smaller element of each full pair, together with c if $c \in U$. Then every matched pair is untouched and every full pair is touched exactly once, so by (i) $\text{LM}(y_T D_J) = \pm y_U$. Conversely, if y_U is a leading monomial as in (i), then every element of $[n'] \setminus U$ other than possibly c is the larger element b of an untouched pair whose smaller element a lies in U . This injection shows that at most one down-step is unmatched, so $U \in \mathcal{U}$.

(iii) *Counting.* Paths of length n' with u up-steps number $C(n', u)$. By reflecting the part after the first visit to -2 (André's reflection), those that visit -2 are in bijection with the paths with $n' - u - 2$ up-steps, of which there are $C(n', u+2)$. For $u \leq k-1$ the endpoint $2u - n' \leq -3$ forces a visit to -2 . So $\#\{U \in \mathcal{U} : |U| = u\} = C(n', u) - C(n', u+2)$ for $u \geq k$ and 0 otherwise. The sum telescopes to $C(n', k) + C(n', k+1) = C(2k+2, k+1)$.

(iv) *Conclusion.* Elements of a subspace with pairwise distinct leading monomials are linearly independent, in any characteristic: the leading monomial of a non-trivial combination is the largest leading monomial that occurs with a non-zero coefficient. Hence $\dim(D_J)C \geq |\mathcal{U}| = C(2k+2, k+1) = Q_k(3)$. Equality holds by Theorem 5.9 (or by Proposition 2.5), and it forces the set of leading monomials of the ideal to be exactly $\{y_U : U \in \mathcal{U}\}$, which gives the graded ranks. ■

Remarks 4.2. (1) The graded ranks $C(n', k+j) - C(n', k+j+2)$ are the ballot numbers $C(2k+2, k+1-j)(2j+1)/(k+2+j)$ (OEIS A039599). For $k = 1, \dots, 6$ they are 2, 3, $1 \cdot 5$, 9, 5, $1 \cdot 14$, 28, 20, 7, $1 \cdot 42$, 90, 75, 35, 9, $1 \cdot 132$, 297, 275, 154, 54, 11, $1 \cdot 429$, 1001, 1001, 637, 273, 77, 13, 1. (2) The proof uses the full family: step (ii) needs matchings that are arbitrary. For a subfamily the same argument only bounds the union of the leading-monomial sets, and at $q = 3$, $k = 2$ there are subfamilies for which the analogue of (S) fails (§11). (3) *An alternative route, not needed here.* In the N -variable form of Proposition 2.6, the span of the generators at $q = 3$ is spanned by the Specht polynomials of the two-row shape $(k+1, k)$ of S_{2k+1} , and the degree- $(N-r)$ part of the ideal can be identified with the Specht module $S^{(N-r, r)}$, whose dimension does not depend on the field [Jam]. We checked this identification at $N = 4, 6, 8$ (dimensions 6, 20, 70), but we have not written it out as a proof, and Theorem 4.1 does not depend on it.

5. The proof of Theorem B

Throughout this section, F is an arbitrary field, $q \geq 3$ is odd, $h = (q-1)/2$, and T is a set of $q-1$ elements with a fixed-point-free involution $u \mapsto -u$ (so T has h classes $\{u, -u\}$). For $m \geq 0$ put

$$C_m := F[y_1, \dots, y_m]/(y_1^{q-1}, \dots, y_m^{q-1}), \text{ so } C_F = C_{2k+1}.$$

The field and the set T never interact: F carries the ideals, T carries the point sets, and the two are compared only through dimensions and cardinalities. Every identity used is an identity of polynomials with integer coefficients. The field reappears in §5.9, where we evaluate the generators on a copy of T inside F .

The idea in one paragraph. Peeling off y_1 splits an ideal V into $q-1$ nested slices, and a point set Z into $q-1$ nested layers (Lemma 5.1). If each layer is the point set of an ideal contained in the corresponding slice, induction on m gives $\dim V \geq |Z|$. To make this possible we index both sides by down-sets of partitions: V_Λ is generated by products of divided differences and Vandermonde determinants, and Z_Λ is the set of tuples whose unpaired part has shape in Λ . The number of values of y_1 that complete a tail depends only on the shape μ of the tail (P1, §5.4). The $q-1$ shapes obtained from μ form a chain for weak dominance (§5.5), so the layers are again down-sets (P2, §5.6). And each generator of a layer lifts to the right slice by one of three explicit constructions (P3, §5.7).

5.1 Peeling one variable

Write $C_m = C_{m-1}[y_1]/(y_1^{q-1})$, where C_{m-1} is the ring in $y_2, \dots, y_m$. For an ideal $V \subseteq C_m$ and $0 \leq j \leq q-2$ put

$$V_{\leq j} := \{f \in V : \deg_{y_1} f \leq j\},$$

$$W_j(V) := \{[y_1^j]f : f \in V_{\leq j}\} \subseteq C_{m-1}.$$

Lemma 5.1 (peeling; linear algebra and counting). (i) $W_j(V)$ is an ideal of C_{m-1} . (ii) $W_j(V) \subseteq W_{j+1}(V)$ for $0 \leq j < q-2$. (iii) $\dim V = \sum_{j=0}^{q-2} \dim W_j(V)$. (iv) For $Z \subseteq T^m$, let $F(M') := \{y \in T : (y, M') \in Z\}$ for $M' \in T^{m-1}$ and $Z_{>i} := \{M' : |F(M')| > i\}$. Then $|Z| = \sum_{i=0}^{q-2} |Z_{>i}|$.

Proof. (i) For $g \in C_{m-1}$ and $f \in V_{\leq j}$, $gf \in V_{\leq j}$ and $[y_1^j](gf) = g \cdot [y_1^j]f$. (ii) If $f \in V_{\leq j}$, then $y_1 f \in V_{\leq j+1}$ and $[y_1^{j+1}](y_1 f) = [y_1^j]f$; this uses $y_1^{j+1} \neq 0$, i.e. $j+1 \leq q-2$. (iii) The map $V_{\leq j} \rightarrow W_j(V)$, $f \mapsto [y_1^j]f$, is onto with kernel $V_{\leq j-1}$, and $V = V_{\leq q-2}$. (iv) $|Z| = \sum_{M'} |F(M')|$. Since $|F(M')| \leq q-1$, each M' lies in $Z_{>i}$ for exactly the $|F(M')|$ values $i = 0, \dots, |F(M')| - 1$, so $\sum_i |Z_{>i}| = \sum_{M'} |F(M')|$. ■

5.2 Partitions, residues and weak dominance

- **Residue.** Regard $M \in T^m$ as a multiset of values. In each class $\{u, -u\}$ let $a, \bar{a}$ be the multiplicities of u and $-u$ in M . The class contributes $\min(a, \bar{a})$ negation pairs, and $\nu(M) = \sum_{\text{classes}} \min(a, \bar{a})$, since a negation pair lies inside one class and the classes are disjoint. The **residue** keeps, in each class with $a \neq \bar{a}$, $|a - \bar{a}|$ copies of the majority value.
- $\lambda(M)$ is the partition formed by the multiplicities of the residue. Distinct residual values lie in distinct classes, so $\ell(\lambda(M)) \leq h$, and $|\lambda(M)| = \sum |a - \bar{a}| = m - 2\nu(M) \equiv m \pmod{2}$.
- $\text{Par}_m^{(h)} := \{\lambda : |\lambda| \leq m, |\lambda| \equiv m \pmod{2}, \ell(\lambda) \leq h\}$. The cap $\ell(\lambda) \leq h$ matters: for example $(1^m) \notin \text{Par}_m^{(h)}$ when $m > h$. We write Par_m when h is fixed.
- **Weak dominance.** For a partition λ let $S_t(\lambda)$ be the sum of its t largest parts, padded with zeros. Put $\lambda \preceq \mu$ iff $S_t(\lambda) \leq S_t(\mu)$ for all $t \geq 1$. The order is defined also between partitions of different sizes; it is a partial order, not a total one ((2) and (1, 1, 1) are incomparable).
- For a $\preceq$ -down-set $\Lambda \subseteq \text{Par}_m$, $Z_\Lambda := \{M \in T^m : \lambda(M) \in \Lambda\}$.
- **Tight patterns.** For $\lambda \in \text{Par}_m$ and an index set I with $|I| = m$, a tight pattern of λ on I consists of $p = (m - |\lambda|)/2$ pairwise disjoint pairs P of elements of I , together with pairwise disjoint blocks $B_1, \dots, B_{\lambda_1}$ with $|B_c| = \lambda'_c$ (the column lengths of λ), which partition the rest of I . Its **product** is $D_P \cdot \prod_c \Delta(B_c)$, where $D_P := \prod_{(a,b) \in P} D(y_a, y_b)$ and, for $B = \{b_1 < \dots < b_r\}$, $\Delta(B) := \det(y_{b_c}^{e-1})_{e,c=1..r} = \prod_{c < c'} (y_{b_{c'}} - y_{b_c})$ (the Vandermonde determinant, with $\Delta(\emptyset) = \Delta(\{b\}) = 1$).
- The blocks are indexed by the *columns* of λ . In the proof of Theorem 5.9 a row of λ carries one value and a column carries pairwise distinct values.
- $V_\Lambda \subseteq C_m$ is the ideal generated by the products of all tight patterns on $[m]$ of all $\lambda \in \Lambda$. For $m = 0$ the empty product is 1.

Lemma 5.2 (the root; the only place where the full family enters). In Par_{2k+1} , $\Lambda = \{(1)\}$ is a down-set, $V_{(1)} = (D_J : J \in \mathcal{J})C_{2k+1}$, and $Z_{(1)} = \Gamma'$, so $|Z_{(1)}| = Q_k(q)$.

Proof. If $\lambda \preceq (1)$ then $S_t(\lambda) \leq 1$ for all t , so $|\lambda| \leq 1$; since $|\lambda|$ is odd, $\lambda = (1)$. A tight pattern of (1) on $[2k+1]$ consists of k disjoint pairs and one singleton block (with $\Delta = 1$), so its product is D_P for a set P of k disjoint pairs covering $[2k+1] \setminus \{c\}$. Adding the pair $\{0, c\}$ gives a matching $J \in \mathcal{J}$, and every J arises in this way; since D is antisymmetric, $D_P = \pm D_J$. So $V_{(1)}$ contains D_J for every matching J : this is where the whole family $\mathcal{J}$ is used, and a subfamily would give a smaller ideal. Finally $\lambda(M) = (1)$ iff $\nu(M) = k$, so $Z_{(1)} = \Gamma'$, and $|\Gamma'| = Q_k(q)$ by Lemma 3.1. ■

5.3 The theorem

Theorem 5.3. *For every field F , every odd $q \geq 3$, every $m \geq 0$ and every $\preceq$ -down-set $\Lambda \subseteq \text{Par}_m^{(h)}$, $\dim_F V_\Lambda \geq |Z_\Lambda|$.*

Corollary 5.4. *Theorem B holds, and so does (S) for every $k \geq 0$ and every $q = p^v$, p an odd prime. Hence the Main Theorem for $m = p^v$, p an odd prime.*

Proof of the Corollary. By Lemma 5.2 and Theorem 5.3 with $m = 2k + 1$ and $\Lambda = \{(1)\}$, $\dim_F(D_J : J \in \mathcal{J})C_F \geq |\Gamma'| = Q_k(q)$. The equality clause and the integral statement of Theorem B are Theorems 5.9 and 5.9' below (with Lemma 5.2, which holds verbatim over Z); for (S) the reverse inequality is also Proposition 2.5. Proposition 2.5 then turns (S) into the Main Theorem. $\blacksquare$

The proof of Theorem 5.3 is by induction on m , with q fixed, and occupies §5.4–§5.8. We fix $m \geq 1$, a down-set $\Lambda \subseteq \text{Par}_m$, and peel y_1 (Lemma 5.1).

5.4 (P1) The fibres depend only on the residue partition

Take $Z = Z_\Lambda$ in Lemma 5.1(iv). Fix $M' \in T^{m-1}$ (indices $2, \dots, m$) with $\lambda(M') = \mu$, residual values $u_1, \dots, u_\ell$ in distinct classes, and multiplicities $\mu_1 \geq \dots \geq \mu_\ell$. Adding a value y for the index 1 gives:

- $y = -u_j$: the class of u_j gains a negation pair, and $\lambda(y, M') = \mu - e_j$ (one box removed from row j , re-sorted);
- $y = u_j$: $\lambda(y, M') = \mu + e_j$;
- y in one of the $h - \ell$ classes absent from the residue (where M' has equal multiplicities, possibly $0 = 0$): $\lambda(y, M') = \mu \sqcup 1$ (a new part equal to 1). There are $2(h - \ell) = q - 1 - 2\ell$ such y .

These are $\ell + \ell + (q - 1 - 2\ell) = q - 1 = |T|$ values. Hence $|F(M')| = F_\Lambda(\mu)$, where

$$F_\Lambda(\mu) := \#\{j : \mu - e_j \in \Lambda\} + \#\{j : \mu + e_j \in \Lambda\} + (q - 1 - 2\ell) \cdot [\mu \sqcup 1 \in \Lambda],$$

which depends only on μ . So $Z_{>i} = Z_{\Lambda_i}$ with $\Lambda_i := \{\mu \in \text{Par}_{m-1} : F_\Lambda(\mu) > i\}$. All the options lie in Par_m : their size is $|\mu| \pm 1 \leq m$, with the parity of m , and $\mu \sqcup 1$ only occurs when $\ell < h$.

5.5 (Chain) The options form a chain

Let $\bar{r}_j$ be the last row of μ of length μ_j , and $\underline{r}_j$ the first. Removing a box from row j lowers the last row of that length, and adding a box to row j raises the first one, so for all $t \geq 1$:

$$\begin{aligned} S_t(\mu - e_j) &= S_t(\mu) - [t \geq \bar{r}_j], & S_t(\mu + e_j) &= S_t(\mu) + [t \geq \underline{r}_j], \\ S_t(\mu \sqcup 1) &= S_t(\mu) + [t > \ell]. \end{aligned}$$

List the $L := q - 1$ options by position $p = 1, \dots, L$:

$$\mu - e_1 \preceq \mu - e_2 \preceq \dots \preceq \mu - e_\ell \preceq \mu \sqcup 1 = \dots = \mu \sqcup 1 \preceq \mu + e_\ell \preceq \dots \preceq \mu + e_1$$

with $\mu - e_p$ at position $p \leq \ell$, the $q - 1 - 2\ell$ copies of $\mu \sqcup 1$ at positions $\ell < p \leq L - \ell$, and $\mu + e_j$ at position $L + 1 - j$.

Lemma 5.5 (inequality of partitions). *The options at positions $1, \dots, L$ are weakly increasing for $\preceq$. Consequently the options lying in Λ form an initial segment, and $F_\Lambda(\mu)$ is the length of that segment.*

Proof. $\bar{r}_j$ is non-decreasing in j (rows are sorted), so $\mu - e_j \preceq \mu - e_{j+1}$. Next, $\mu - e_\ell \preceq \mu \preceq \mu \sqcup 1$. Then $\mu \sqcup 1 \preceq \mu + e_\ell$, because $\bar{r}_\ell \leq \ell < t$ whenever $[t > \ell] = 1$. Finally $\bar{r}_j$ is non-decreasing in j , so $\mu + e_{j+1} \preceq \mu + e_j$. Since Λ is a down-set, $\text{opt}_p \in \Lambda$ implies $\text{opt}_{p'} \in \Lambda$ for all $p' \leq p$. ■

In particular the removals in Λ are $\mu - e_1, \dots, \mu - e_r$ for some $r \leq \ell$. Since rows of equal length give equal partitions, the options at the positions of equal rows coincide, so $r = 0$ or r is the last row of its length. The additions in Λ are $\mu + e_j$ for $j_0 \leq j \leq \ell$, with j_0 (if it exists) the first row of its length. Put $\iota := [\mu \sqcup 1 \in \Lambda]$ (so $\iota = 0$ when $\ell = h$). If some addition lies in Λ , then $r = \ell$, and $\iota = 1$ whenever $\ell < h$; if $\iota = 1$ then $r = \ell$. Therefore

$$F_\Lambda(\mu) = r + (q - 1 - 2\ell) \cdot \iota + (\ell - j_0 + 1) \cdot [j_0 \text{ exists}]. \quad (5.1)$$

5.6 (P2) The layers are down-sets

Proposition 5.6 (inequality of partitions). *If $\mu, \tilde{\mu} \in \text{Par}_{m-1}$ and $\mu \preceq \tilde{\mu}$, then $\text{opt}_p(\mu) \preceq \text{opt}_p(\tilde{\mu})$ for every position p . Hence $F_\Lambda(\mu) \geq F_\Lambda(\tilde{\mu})$, and every Λ_i is a $\preceq$ -down-set of Par_{m-1} .*

The second sentence follows from the first: if $\text{opt}_p(\tilde{\mu}) \in \Lambda$ then $\text{opt}_p(\mu) \in \Lambda$, so $F_\Lambda(\tilde{\mu}) \leq F_\Lambda(\mu)$, and $\tilde{\mu} \in \Lambda_i$ implies $\mu \in \Lambda_i$. We prove the first sentence. Write $\ell = \ell(\mu)$, $\tilde{\ell} = \ell(\tilde{\mu})$, and mark with a tilde the quantities of $\tilde{\mu}$. Recall that $|\mu| \equiv |\tilde{\mu}| \pmod{2}$, since both lie in Par_{m-1} . Two facts are used throughout.

- (T) If $t \geq 1$ is **tight**, i.e. $S_t(\mu) = S_t(\tilde{\mu})$, then $\mu_t \geq \tilde{\mu}_t$ (from $S_{t-1}(\mu) \leq S_{t-1}(\tilde{\mu})$) and $\mu_{t+1} \leq \tilde{\mu}_{t+1}$ (from $S_{t+1}(\mu) \leq S_{t+1}(\tilde{\mu})$).
- (G) Each comparison below has the form $S_t(\mu) + \delta \leq S_t(\tilde{\mu}) + \tilde{\delta}$ with $\delta, \tilde{\delta} \in \{-1, 0, 1\}$. If $\delta - \tilde{\delta} \leq 1$, it can only fail at a tight t with $\delta = \tilde{\delta} + 1$. The one place where $\delta - \tilde{\delta} = 2$ is possible is treated explicitly, in (d1).

The positions fall into seven cases. A removal of one partition is never compared with an addition of the other, because $\ell + \tilde{\ell} \leq 2h = q - 1$ leaves the middle positions of μ in between.

case	positions	option of μ	option of $\tilde{\mu}$	only possible failure	why it cannot occur
(a)	$p \leq \min(\ell, \tilde{\ell})$	$\mu - e_p$	$\tilde{\mu} - e_p$	tight t , $\tilde{\bar{r}}_p \leq t < \bar{r}_p$	forces $S_{p-1}(\tilde{\mu}) < S_{p-1}(\mu)$
(b)	$j \leq \min(\ell, \tilde{\ell})$	$\mu + e_j$	$\tilde{\mu} + e_j$	tight t , $\bar{r}_j \leq t < \tilde{\bar{r}}_j$	forces $S_j(\tilde{\mu}) < S_j(\mu)$
(c)	middle	$\mu \sqcup 1$	$\tilde{\mu} \sqcup 1$	$\ell < t \leq \tilde{\ell}$	the rows $\ell + 1, \dots, t$ of $\tilde{\mu}$, (5.2)
(d1)	$\ell < p \leq \tilde{\ell}$	$\mu \sqcup 1$	$\tilde{\mu} - e_p$	$\delta - \tilde{\delta} = 2$	(5.2) and parity
(d2)	$\ell < j \leq \tilde{\ell}$	$\mu \sqcup 1$	$\tilde{\mu} + e_j$	none	(5.2)
(e1)	$\tilde{\ell} < p \leq \ell$	$\mu - e_p$	$\tilde{\mu} \sqcup 1$	none	chain $\mu - e_p \preceq \mu \preceq \tilde{\mu} \preceq \tilde{\mu} \sqcup 1$
(e2)	$\tilde{\ell} < j \leq \ell$	$\mu + e_j$	$\tilde{\mu} \sqcup 1$	tight $t \leq \tilde{\ell}$	forces $S_j(\tilde{\mu}) < S_j(\mu)$

(a) *Removal against removal*, $p \leq \min(\ell, \tilde{\ell})$. We need $S_t(\mu) - [t \geq \bar{r}_p] \leq S_t(\tilde{\mu}) - [t \geq \tilde{\bar{r}}_p]$. The only danger is a tight t with $\tilde{\bar{r}}_p \leq t < \bar{r}_p$. Then $t \geq p$, and rows $p, \dots, t + 1$ of μ all have length μ_p ; in particular $\mu_t = \mu_{t+1} = \mu_p$. Since $t + 1 > \tilde{\bar{r}}_p$, $\tilde{\mu}_{t+1} < \tilde{\mu}_p$. By (T), $\tilde{\mu}_{t+1} \geq \mu_{t+1} = \mu_t \geq \tilde{\mu}_t \geq \tilde{\mu}_{t+1}$,

so $\tilde{\mu}_t = \tilde{\mu}_{t+1} = \mu_p$ and $\tilde{\mu}_p > \mu_p$. Hence $S_t(\tilde{\mu}) - S_{p-1}(\tilde{\mu}) = \sum_{s=p}^t \tilde{\mu}_s \geq \tilde{\mu}_p + (t-p)\mu_p > (t-p+1)\mu_p = S_t(\mu) - S_{p-1}(\mu)$. Since t is tight, $S_{p-1}(\tilde{\mu}) < S_{p-1}(\mu)$, contradicting $\mu \preccurlyeq \tilde{\mu}$.

(b) *Addition against addition*, $j \leq \min(\ell, \tilde{\ell})$ (position $L+1-j$). We need $S_t(\mu) + [t \geq r_j] \leq S_t(\tilde{\mu}) + [t \geq \tilde{r}_j]$. The only danger is a tight t with $r_j \leq t < \tilde{r}_j$. Then $t < \tilde{r}_j \leq j$, so $\mu_t = \mu_{t+1} = \mu_j$, and $\tilde{\mu}_t > \tilde{\mu}_j$ because t lies before the first row of $\tilde{\mu}$ of length $\tilde{\mu}_j$. By (T), $\tilde{\mu}_{t+1} \geq \mu_{t+1} = \mu_j = \mu_t \geq \tilde{\mu}_t \geq \tilde{\mu}_{t+1}$, so $\tilde{\mu}_t = \tilde{\mu}_{t+1} = \mu_j > \tilde{\mu}_j$. Every $\tilde{\mu}_s$ with $s > t$ is at most μ_j , and $\tilde{\mu}_j < \mu_j$, so $\sum_{s=t+1}^j \tilde{\mu}_s < (j-t)\mu_j = \sum_{s=t+1}^j \mu_s$. With tightness at t , $S_j(\tilde{\mu}) < S_j(\mu)$: a contradiction.

(c) *Middle against middle*. We need $S_t(\mu) + [t > \ell] \leq S_t(\tilde{\mu}) + [t > \tilde{\ell}]$. If $\ell \geq \tilde{\ell}$ this is immediate. If $\ell < \tilde{\ell}$ and $\ell < t \leq \tilde{\ell}$, the rows $\ell+1, \dots, t$ of $\tilde{\mu}$ are non-empty, so

$$S_t(\tilde{\mu}) \geq S_\ell(\tilde{\mu}) + (t-\ell) \geq S_\ell(\mu) + (t-\ell) = |\mu| + (t-\ell) \geq |\mu| + 1 = S_t(\mu) + 1. \quad (5.2)$$

Layout of the positions. If $\ell = \tilde{\ell}$ only (a), (b), (c) occur. If $\ell < \tilde{\ell}$, positions $\ell+1, \dots, \tilde{\ell}$ compare a middle option of μ with a removal of $\tilde{\mu}$ (case d1), and positions $L+1-j$ with $\ell < j \leq \tilde{\ell}$ compare a middle option of μ with an addition of $\tilde{\mu}$ (case d2). These positions are middle positions of μ because $\ell + \tilde{\ell} \leq 2h = L$. If $\ell > \tilde{\ell}$, the roles are reversed (cases e1, e2).

(d1) $\ell < p \leq \tilde{\ell}$: $\mu \sqcup 1$ against $\tilde{\mu} - e_p$. We need $S_t(\mu) + [t > \ell] \leq S_t(\tilde{\mu}) - [t \geq \tilde{r}_p]$. Here $\delta - \tilde{\delta}$ can be 2, so we check every t .

- $t \leq \ell$: both brackets vanish, since $\tilde{r}_p \geq p > \ell \geq t$.
- $t \geq \tilde{\ell}$: $S_t(\tilde{\mu}) = |\tilde{\mu}| \geq |\mu| + (\tilde{\ell} - \ell) \geq |\mu| + 1$ by (5.2) at $t = \tilde{\ell}$; by parity $|\tilde{\mu}| \geq |\mu| + 2$, which suffices.
- $\ell + 2 \leq t < \tilde{\ell}$: $S_t(\tilde{\mu}) \geq |\mu| + (t - \ell) \geq |\mu| + 2$ by (5.2).
- $t = \ell + 1 < \tilde{\ell}$: if $t < \tilde{r}_p$, (5.2) suffices. If $t \geq \tilde{r}_p$, then $\tilde{r}_p = p = \ell + 1$ and we need $S_{\ell+1}(\tilde{\mu}) \geq |\mu| + 2$. If $\tilde{\mu}_{\ell+1} \geq 2$ this holds, since $S_\ell(\tilde{\mu}) \geq |\mu|$. If $\tilde{\mu}_{\ell+1} = 1$, then row $\ell+2 \leq \tilde{\ell}$ of $\tilde{\mu}$ also has length 1, so $\tilde{r}_{\ell+1} \geq \ell+2 > t$, a contradiction.

(d2) $\ell < j \leq \tilde{\ell}$: $\mu \sqcup 1$ against $\tilde{\mu} + e_j$. We need $S_t(\mu) + [t > \ell] \leq S_t(\tilde{\mu}) + [t \geq \tilde{r}_j]$. For $t \leq \ell$ this is immediate. For $\ell < t \leq \tilde{\ell}$ it follows from (5.2), and for $t > \tilde{\ell}$ from $|\tilde{\mu}| \geq |\mu| + 1$.

(e1) $\tilde{\ell} < p \leq \ell$: $\mu - e_p$ against $\tilde{\mu} \sqcup 1$ (which exists because $\tilde{\ell} < \ell \leq h$). Here $\mu - e_p \preccurlyeq \mu \preccurlyeq \tilde{\mu} \preccurlyeq \tilde{\mu} \sqcup 1$.

(e2) $\tilde{\ell} < j \leq \ell$: $\mu + e_j$ against $\tilde{\mu} \sqcup 1$. We need $S_t(\mu) + [t \geq r_j] \leq S_t(\tilde{\mu}) + [t > \tilde{\ell}]$. For $t > \tilde{\ell}$ the right bracket is 1, so this is immediate. For $t \leq \tilde{\ell}$ with $t \geq r_j$ we need strictness. Suppose t is tight. Then $r_j \leq t \leq \tilde{\ell} < j$, so $\mu_t = \mu_{t+1} = \mu_j \geq 1$. By (T), $\tilde{\mu}_t \leq \mu_t = \mu_j$, so $\tilde{\mu}_s \leq \mu_j$ for every $s \geq t$. Moreover $\tilde{\mu}_j = 0$, since $j > \tilde{\ell}$. Hence $\sum_{s=t+1}^j \tilde{\mu}_s < (j-t)\mu_j = \sum_{s=t+1}^j \mu_s$, and with tightness $S_j(\tilde{\mu}) < S_j(\mu)$, a contradiction.

The positions $1, \dots, L$ are covered by (a)–(e) exactly once: removals occupy positions $\leq \ell$ or $\leq \tilde{\ell}$, additions the last ℓ or $\tilde{\ell}$ positions, and the middle the rest. The degenerate cases $\ell = 0$, $\ell = h$ (no middle positions) and $\tilde{\ell} = h$ are included. ■

5.7 (P3) Every tight pattern of a layer lies in the right slice

We need three identities of polynomials, all with integer coefficients, hence valid in C_m over any field.

Lemma 5.7 (identities over Z). (i) For $0 \leq t \leq q-2$: $[y_1^{q-2-t}]D(y_1, y_b) = (-1)^{t+1}y_b^t$. (ii) Let $S = \{b_1 < \dots < b_r\}$ and $\varepsilon_{b_c} := (-1)^{r+c}$. Then $\sum_{b \in S} \varepsilon_b \Delta(S \setminus b) y_b^t = 0$ for $0 \leq t \leq r-2$, and

$= \Delta(S)$ for $t = r - 1$. (iii) If $1 \notin B$ and $|B| \leq q - 2$, then $\Delta(B \cup \{1\}) = \prod_{c \in B} (y_c - y_1) \cdot \Delta(B)$ has y_1 -degree $|B|$ in C_m , with top coefficient $(-1)^{|B|} \Delta(B)$.

Proof. (i) The coefficient is $(-1)^{q-2-t} y_b^t$, and $q - 2$ is odd. (ii) The left side is the expansion, along its last row, of the Vandermonde matrix of S with its last row (y_b^{r-1}) replaced by (y_b^t) . For $t \leq r - 2$ two rows coincide. (iii) This is the factorisation of the Vandermonde determinant; $y_1^{|B|} \neq 0$ in C_m because $|B| \leq q - 2$. ■

Proposition 5.8 (linear algebra). *For every $i \in \{0, \dots, q - 2\}$: $V_{\Lambda_i} \subseteq W_{q-2-i}(V_\Lambda)$. Here $V_{\Lambda_i} \subseteq C_{m-1}$ is built on the indices $2, \dots, m$.*

Proof. Since $W_{q-2-i}(V_\Lambda)$ is an ideal (Lemma 5.1(i)), it suffices to treat a generator. Let $\mu \in \Lambda_i$, so $\Phi := F_\Lambda(\mu) \geq i + 1$, and let G be the product of a tight pattern of μ on $\{2, \dots, m\}$, with pairs P and column blocks B_c . By Lemma 5.1(ii) it is enough to show $G \in W_j(V_\Lambda)$ for some $j \leq q - 1 - \Phi$: then $j \leq q - 2 - i$. We use (5.1). Since $\Phi \geq 1$, at least one term of (5.1) is non-zero, and we split into three cases, which are mutually exclusive by construction: (α) j_0 exists; (β) j_0 does not exist and $\iota = 1$; (γ) neither, so that $\Phi = r \geq 1$. In case (β), $\iota = 1$ forces $\ell < h$, since $\mu \sqcup 1 \in \text{Par}_m$ requires $\ell(\mu) + 1 \leq h$.

(α) j_0 exists ($\lambda := \mu + e_{j_0} \in \Lambda$). The column $c^* := \mu_{j_0} + 1$ of μ has height $j_0 - 1$, because j_0 is the first row of its length; let $B := B_{c^*}$ (possibly empty). Put the index 1 into B . The result is a tight pattern of λ on $[m]$: column c^* of λ has height j_0 , and the number of pairs $(m - |\lambda|)/2 = ((m - 1) - |\mu|)/2$ is unchanged. Its product lies in V_Λ , has y_1 -degree $j_0 - 1$, and by Lemma 5.7(iii) its top y_1 -coefficient is $\pm G$ (note $|B| = j_0 - 1 \leq h - 1 \leq q - 2$). So $G \in W_{j_0-1}(V_\Lambda)$. By (5.1), $r = \ell$ here. If $\ell < h$, then $\iota = 1$ and $\Phi = \ell + (q - 1 - 2\ell) + (\ell - j_0 + 1) = q - j_0$. If $\ell = h$, then $q - 1 - 2\ell = 0$ and $\Phi = 2\ell - j_0 + 1 = q - j_0$. In both cases $j_0 - 1 = q - 1 - \Phi$.

(β) no j_0 , and $\iota = 1$ ($\lambda := \mu \sqcup 1 \in \Lambda$, $\ell < h$). Put the index 1 into the first column block B_1 , of height ℓ ; column 1 of λ has height $\ell + 1$, and the number of pairs is unchanged. The product has y_1 -degree $\ell \leq q - 2$ and top coefficient $\pm G$, so $G \in W_\ell(V_\Lambda)$. By (5.1), $r = \ell$ and $\Phi = q - 1 - \ell$, i.e. $\ell = q - 1 - \Phi$. (For $\mu = \emptyset$ the block is $\{1\}$, $\Delta = 1$, and the degree is 0.)

(γ) only removals ($\Phi = r \geq 1$, $\lambda := \mu - e_r \in \Lambda$). The column μ_r of μ has height r , because r is the last row of its length; call its block S , $|S| = r$, and write $G = \Delta(S) \cdot G'$, where G' involves no index of $S \cup \{1\}$. For $b \in S$, the pairs $P \cup \{(1, b)\}$ together with the blocks B_c ($c \neq \mu_r$) and $S \setminus \{b\}$ form a tight pattern of λ on $[m]$: column μ_r of λ has height $r - 1$, and the number of pairs $(m - |\lambda|)/2 = ((m - 1) - |\mu|)/2 + 1$ has grown by one. Hence

$$f := \sum_{b \in S} \varepsilon_b \Delta(S \setminus b) D(y_1, y_b) G' \in V_\Lambda.$$

By Lemma 5.7(i),(ii), $[y_1^{q-2-t}]f = (-1)^{t+1} (\sum_b \varepsilon_b \Delta(S \setminus b) y_b^t) G'$. This vanishes for $t \leq r - 2$ and equals $\pm \Delta(S) G' = \pm G$ for $t = r - 1$. So $\deg_{y_1} f \leq q - 1 - r$, with top coefficient $\pm G$, and $G \in W_{q-1-r}(V_\Lambda) = W_{q-1-\Phi}(V_\Lambda)$. ■

The three constructions land exactly in the slice $q - 1 - \Phi$, the largest index the proof can afford (see Remark 5.10(2)).

5.8 The induction

Proof of Theorem 5.3. Induction on m , with F , q and T fixed.

- **Base** $m = 0$. $\text{Par}_0 = \{\emptyset\}$. If $\Lambda = \{\emptyset\}$, then $V_\Lambda = C_0 = F$ (the empty product) and $Z_\Lambda = T^0$ is one point: $1 \geq 1$. If $\Lambda = \emptyset$, both sides are 0.

- **Relabelling.** A permutation of the index set sends every tight-pattern product to $\pm$ another one, since D and Δ are antisymmetric. Hence V_Λ is invariant under relabelling, and so is $|Z_\Lambda|$. So the statement for $m - 1$ variables applies to the variables $y_2, \dots, y_m$.
- **Step.** Let $m \geq 1$. By Lemma 5.1(iii), Proposition 5.8, the induction hypothesis, and Lemma 5.1(iv),

$$\dim V_\Lambda = \sum_{i=0}^{q-2} \dim W_{q-2-i}(V_\Lambda) \geq \sum_{i=0}^{q-2} \dim V_{\Lambda_i} \geq \sum_{i=0}^{q-2} |Z_{\Lambda_i}| = \sum_{i=0}^{q-2} |Z_{>i}| = |Z_\Lambda|.$$

The induction hypothesis applies because each Λ_i is a down-set of Par_{m-1} (Proposition 5.6). The identity $Z_{\Lambda_i} = Z_{>i}$ is §5.4. ■

5.9 Equality

For an ideal $I \subseteq F[y_1, \dots, y_m]$ let $\text{gr}(I)$ be the ideal of top-degree forms: its degree- d part consists of 0 and the homogeneous parts of degree d of the elements of I of degree exactly d . (It is an ideal: for $f, g \in I$ of degree d , the form $f^{\text{top}} + g^{\text{top}}$ is 0 or $(f + g)^{\text{top}}$, and $y_i f^{\text{top}} = (y_i f)^{\text{top}}$.)

Lemma 5.8' (top-degree forms). (i) If $I \subseteq F[y]$ is generated by $f_1, \dots, f_s$, then $\text{gr}(I) \supseteq (f_1^{\text{top}}, \dots, f_s^{\text{top}})$. (ii) If $\dim_F F[y]/I < \infty$, then $\dim_F F[y]/\text{gr}(I) = \dim_F F[y]/I$.

Proof. (i) $f_i \in I$, so $f_i^{\text{top}} \in \text{gr}(I)$. (ii) Fix a degree-compatible monomial order. For $f \neq 0$, the leading monomial of f is that of f^{top} . The ideal $\text{gr}(I)$ is homogeneous, so each of its non-zero elements g has $g^{\text{top}} \in \text{gr}(I)$, and $g^{\text{top}} = f^{\text{top}}$ for some $f \in I$. Hence $\text{gr}(I)$ and I have the same monomial ideal of leading monomials, and by Macaulay's basis theorem [CLO] the standard monomials are a basis of both quotients. ■

(The initial ideal of I is a monomial ideal and contains the leading monomials of the f_i , not the f_i ; it is $\text{gr}(I)$ that contains the forms themselves. Version 4 of this paper wrote «initial ideal» for gr in the proofs of Theorem 5.9 and Proposition 11.1.)

Theorem 5.9. If $\text{char } F$ does not divide $q - 1$, then $\dim_F V_\Lambda = |Z_\Lambda|$ for every $m \geq 0$ and every $\preceq$ -down-set $\Lambda \subseteq \text{Par}_m^{(h)}$. In particular, for such F , equality holds in Theorem B (for every field, see Theorem 5.9'), and $\dim_{F_p}(D_J : J \in \mathcal{J})C = Q_k(q)$ for $q = p^v$ without any appeal to topology.

Proof. By Theorem 5.3 it suffices to prove $\leq$. The generators of V_Λ have integer coefficients, so $\dim_F V_\Lambda$ does not change under extension of the field, and we may assume that F contains the group μ_{q-1} of $(q - 1)$ -th roots of unity. Since $\text{char } F \nmid q - 1$, the polynomial $y^{q-1} - 1$ is separable, $|\mu_{q-1}| = q - 1$, and $-1 \in \mu_{q-1}$ is not 1 (because $q - 1$ is even and $\text{char } F \neq 2$). So we may take $T := \mu_{q-1}$ with the involution $u \mapsto -u$, which has no fixed point.

Evaluation. For $a, b \in T$, the identity $(a + b)D(a, b) = b^{q-1} - a^{q-1} = 0$ shows $D(a, b) = 0$ unless $b = -a$, and $D(a, -a) = \sum_u (-1)^u (-1)^{q-2-u} a^{q-2} = -(q - 1)a^{q-2} \neq 0$. A Vandermonde determinant $\Delta(B)$ is non-zero at a point iff the values on B are pairwise distinct. So the product of a tight pattern $(P, B_1, \dots, B_{\lambda_1})$ of λ is non-zero at $M \in T^m$ iff every pair of P is a negation pair of M and every block B_c carries pairwise distinct values.

Support. Suppose such a product is non-zero at M . Let M' be the multiset of the $|\lambda|$ values of M outside P , and ν' its multiplicity partition. A value occurs at most once in each column block, so the t most frequent values of M' occupy at most $\min(t, \lambda'_c)$ places of column c ; summing over c , $S_t(\nu') \leq \sum_c \min(t, \lambda'_c) = S_t(\lambda)$, so $\nu' \preceq \lambda$. The pairs of P do not change the residue, and passing from M' to its residue replaces, in each class, the two multiplicities $a, \bar{a}$ by one part $|a - \bar{a}| \leq \max(a, \bar{a})$; so the parts of $\lambda(M)$ are bounded, one by one, by distinct parts of ν' , and $\lambda(M) \preceq \nu'$. Hence $\lambda(M) \preceq \lambda$, and if $\lambda \in \Lambda$ then $M \in Z_\Lambda$. So the union Σ of the supports of

the generators of V_Λ is contained in Z_Λ . (It is in fact equal: for $M \in Z_\Lambda$, take $\nu(M)$ disjoint negation pairs of M and put the residue into the columns of $\lambda(M)$, one value per row.)

Degeneration. Let $g_1, \dots, g_s$ be the generators of V_Λ , viewed as homogeneous polynomials in $F[y_1, \dots, y_m]$, and put $I := (g_1, \dots, g_s) + (y_1^{q-1} - 1, \dots, y_m^{q-1} - 1)$. Since $y^{q-1} - 1 = \prod_{u \in T} (y - u)$, the Chinese remainder theorem gives $F[y]/(y_i^{q-1} - 1) \cong F^{T^m}$, the ring of functions on T^m . In a finite product of fields, the ideal generated by some functions consists of the functions that vanish outside the union of their supports. So I is the ideal of the functions vanishing on $T^m \setminus \Sigma$, and $\dim_F F[y]/I = (q-1)^m - |\Sigma|$. The top-degree form of g_i is g_i and that of $y_i^{q-1} - 1$ is y_i^{q-1} . So, by Lemma 5.8'(i), $I' := (g_1, \dots, g_s) + (y_1^{q-1}, \dots, y_m^{q-1}) \subseteq \text{gr}(I)$, and by Lemma 5.8'(ii)

$$\dim_F C_m/V_\Lambda = \dim_F F[y]/I' \geq \dim_F F[y]/\text{gr}(I) = \dim_F F[y]/I = (q-1)^m - |\Sigma|,$$

that is, $\dim_F V_\Lambda \leq |\Sigma| \leq |Z_\Lambda|$. ■

Complement (the associated graded ring). Assume, as in the proof, that $\text{char } F \nmid q-1$ and $\mu_{q-1} \subseteq F$, and read $V_\Lambda + (y_i^{q-1})$ as the ideal $(g_i) + (y_i^{q-1})$ of $F[y_1, \dots, y_m]$. In the situation of the proof, Theorem 5.3 turns every inequality into an equality: $\Sigma = Z_\Lambda$ and $I' = \text{gr}(I)$. So $V_\Lambda + (y_1^{q-1}, \dots, y_m^{q-1})$ is the ideal of top-degree forms of the ideal of the finite set $T^m \setminus Z_\Lambda \subseteq \mu_{q-1}^m$, and C_m/V_Λ is the associated graded ring of the ring of functions on $T^m \setminus Z_\Lambda$, for the degree filtration. In other words, the tight-pattern products give a complete description of this associated graded ring. This is the same kind of statement as the Garsia–Procesi and Tanisaki descriptions of the associated graded rings of orbits [GP], [Ta], here for a new family of point sets, indexed by down-sets of partitions under weak dominance.

Theorem 5.9' (equality in every characteristic; freeness over Z). *For every field F , every odd $q \geq 3$, every $m \geq 0$ and every $\prec$ -down-set $\Lambda \subseteq \text{Par}_m^{(h)}$, $\dim_F V_\Lambda = |Z_\Lambda|$. Moreover, let $V_{\Lambda,Z}$ be the ideal of $C_{m,Z} := Z[y_1, \dots, y_m]/(y_1^{q-1}, \dots, y_m^{q-1})$ generated by the tight-pattern products of the elements of Λ . Then $C_{m,Z}/V_{\Lambda,Z}$ is a free abelian group of rank $(q-1)^m - |Z_\Lambda|$, each of its graded pieces is free, and the dimension over F of each graded piece of V_Λ does not depend on F .*

Proof. The ring $C_{m,Z}$ is free of rank $(q-1)^m$ on the monomials, and $V_{\Lambda,Z}$ is homogeneous, so $M := C_{m,Z}/V_{\Lambda,Z} = \bigoplus_d M_d$ with each M_d a finitely generated abelian group. The image of $V_{\Lambda,Z}$ in $C_{m,Z} \otimes F = C_m$ generates V_Λ (the generators have integer coefficients), so by right exactness of $\otimes$, $C_m/V_\Lambda \cong M \otimes F$, degree by degree. Write $M_d \cong Z^{\rho_d} \oplus (\text{finite})$. Then $\dim_F(M_d \otimes F) = \rho_d + c_d(F)$, where $c_d(F)$ is the number of cyclic factors of order divisible by $\text{char } F$ in the finite part ($c_d(F) = 0$ if $\text{char } F = 0$). With $F = Q$, where Theorem 5.9 applies because 0 does not divide $q-1$, $\sum_d \rho_d = \dim_Q C_{m,Q}/V_{\Lambda,Q} = (q-1)^m - |Z_\Lambda|$. So for every field F , $\dim_F C_m/V_\Lambda \geq (q-1)^m - |Z_\Lambda|$, that is, $\dim_F V_\Lambda \leq |Z_\Lambda|$, and Theorem 5.3 gives equality. Equality forces $c_d(F) = 0$ for every d . Taking $F = F_p$ for every prime p , no M_d has torsion, so M is free and $\dim_F(C_m/V_\Lambda)_d = \rho_d$ for every F . ■

Remark 5.10. (1) *Where the full family enters.* Only at the root, Lemma 5.2. The down-set closure of $\{(1)\}$ then carries the symmetry of $\mathcal{J}$ through every layer. §11 shows that no argument valid for all subfamilies can exist. (2) *No slack.* In Proposition 5.8 the slice $q-1-F$ cannot be lowered: replacing it by $q-2-F$ makes the statement false (§14, negative controls). (3) *The characteristic.* Theorem 5.3 and, by Theorem 5.9', equality hold over every field. Theorem 5.9 is needed only over Q . The earlier measurements of equality with $\text{char } F | q-1$ (§14) are instances of Theorem 5.9'. (4) *Leading monomials.* In the computed cells, the degree-lexicographic leading monomials of $(D_J)C$ are the reflection $e \mapsto (q-2) - e$ of the lexicographic standard monomials of Γ' in the sense of [CM] (§14). By the Complement to Theorem 5.9, the Hilbert function part of this statement holds in general: the graded dimensions of C_m/V_Λ are those of the degree filtration on the functions on $T^m \setminus Z_\Lambda$.

5.10 A worked example: $(q, m) = (9, 4)$

Here $h = 4$, T has 8 elements, and $\text{Par}_4^{(4)} = \{\emptyset, (2), (1, 1), (4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)\}$ has ten down-sets. Take $\Lambda := \{\emptyset, (1, 1), (2)\}$, the down-set generated by (2) . The tails have $m - 1 = 3$ coordinates, with shapes in $\text{Par}_3 = \{(1), (3), (2, 1), (1, 1, 1)\}$, and $|Z_{(1)}| = 168$, $|Z_{(3)}| = 8$, $|Z_{(2,1)}| = 144$, $|Z_{(1,1,1)}| = 192$ (total $8^3 = 512$).

tail shape μ	its chain (positions $1 \dots 8$)	options in Λ	$F_\Lambda(\mu)$	case of Prop. 5.8	slice $q - 1 - \Phi$
(1)	$\emptyset \cdot (1, 1) \times 6 \cdot (2)$	all	8	$(\alpha), j_0 = 1$	0
(3)	$(2) \cdot (3, 1) \times 6 \cdot (4)$	first	1	$(\gamma), r = 1$	7
(2, 1)	$(1, 1) \cdot (2) \cdot (2, 1, 1) \times 4 \cdot (2, 2) \cdot (3, 1)$	first two	2	$(\gamma), r = 2$	6
(1, 1, 1)	$(1, 1) \times 3 \cdot (1, 1, 1, 1) \times 2 \cdot (2, 1, 1) \times 3$	first three	3	$(\gamma), r = 3$	5

So $\Lambda_0 = \text{Par}_3$, $\Lambda_1 = \{(1), (2, 1), (1, 1, 1)\}$, $\Lambda_2 = \{(1), (1, 1, 1)\}$, and $\Lambda_i = \{(1)\}$ for $3 \leq i \leq 7$: all down-sets, as P2 says. Lemma 5.1(iv) gives $|Z_\Lambda| = 512 + 504 + 360 + 5 \cdot 168 = 2216$, and the computed dimension of V_Λ is 2216 (§14). For the down-set $\{\emptyset, (1, 1)\}$ the tail (1) has $F = 7$ (the addition (2) is missing) and falls into case (β) , with slice $\ell = 1 = q - 1 - F$; there $|Z_\Lambda| = 1896$. Case (β) needs a middle option in Λ and no addition, which is why it does not occur for the first down-set.

6. Odd degrees that are not prime powers: the colour reduction

In this section $m \geq 3$ is odd and p is a prime dividing m (the even degrees are treated in §9, which uses the lemmas of this section). Write $m = q \cdot r$ with $q = p^v$, $v \geq 1$, and $p \nmid r$; so r is odd, and $r = 1$ is the case treated in §2–§5. Put $F := \bar{F}_p$, $n = 2k$ with $k \geq 1$, $N = n + 2$,

$$F[G] := F[t_1, \dots, t_{n+1}] / (t_1^m - 1, \dots, t_{n+1}^m - 1),$$

$$I := (\bar{\psi}_J : J \in \mathcal{J}) \cdot F[G],$$

where $\bar{\psi}_J$ denotes the image of ψ_J in $F[G]$ (in §2 it denoted the image in $F_p[G]$; the ideal of $F[G]$ it generates is the extension of that ideal).

By Proposition 2.1, $\dim_{F_p} F_p[G] / (\bar{\psi}_J : J \in \mathcal{J}) \geq m^{n+1} - |\Gamma_{\mathcal{J}}|$ for every p , with equality at every $p|m$ if and only if $H_n(X)/L(X)$ is torsion free. The $\bar{\psi}_J$ have coefficients in F_p , so $(\bar{\psi}_J)F[G] = (\bar{\psi}_J)F_p[G] \otimes_{F_p} F$, and dimensions do not change under this extension of the field; so

$$\dim_F I \leq |\Gamma_{\mathcal{J}}|, \quad (6.1)$$

and **the Main Theorem at m is equivalent to $\dim_F I \geq |\Gamma_{\mathcal{J}}|$ for every prime $p|m$** . This section reduces that inequality to an inequality for one family of ideals in two sets of variables, the bipartite ideals; §7 proves it. All tensor products are over F , and a «unit» is an invertible element of the ring in which the statement is made. The idea is that $F[G]$ is a product of local rings indexed by the ways of colouring the coordinates with r -th roots of unity; on each factor the generators $\bar{\psi}_J$ either vanish or become pure tensors, and the pure tensors split along the colour classes.

6.1 The splitting

Lemma 6.1 (splitting). Put $R_c := \otimes_{i=1}^{n+1} F[t_i]/((t_i - c_i)^q)$ for $c = (c_1, \dots, c_{n+1}) \in \mu_r^{n+1}$, where $\mu_r \subseteq F^\times$ is the group of r -th roots of unity. Then the product of the quotient maps $\pi_c : F[G] \rightarrow R_c$ is an isomorphism $F[G] \cong \prod_{c \in \mu_r^{n+1}} R_c$, and for every ideal $I' \subseteq F[G]$, $\dim_F I' = \sum_c \dim_F \pi_c(I')$, where $\pi_c(I')$ is the ideal of R_c generated by the images of any set of generators of I' .

Proof. In characteristic p , $(t^r - 1)^q = t^m - 1$. The polynomial $t^r - 1$ is separable, since $r \neq 0$ in F , so $t^r - 1 = \prod_{\zeta \in \mu_r} (t - \zeta)$ with r distinct roots, and $t^m - 1 = \prod_{\zeta} (t - \zeta)^q$. The ideals $((t - \zeta)^q)$ are pairwise comaximal, and the Chinese remainder theorem gives $F[t]/(t^m - 1) \cong \prod_{\zeta} F[t]/((t - \zeta)^q)$. Now $F[G]$ is the tensor product of the $n + 1$ one-variable rings, and the tensor product over a field distributes over finite products of algebras. In a finite product of rings every ideal is the product of its images, which are generated by the images of its generators; dimensions add. ■

6.2 Which generators survive

Fix $c \in \mu_r^{n+1}$ and put $c_0 := (c_1 \cdots c_{n+1})^{-1}$, so that $\prod_{i=0}^{n+1} c_i = 1$. In R_c every $t_i - c_i$ is nilpotent, with $(t_i - c_i)^q = 0$.

Lemma 6.2. (i) For $1 \leq i \leq n + 1$: if $c_i \neq 1$, then $t_i - 1$ is a unit of R_c ; if $c_i = 1$, it is nilpotent. (ii) Let $1 \leq j < l \leq n + 1$ and $u := t_j t_l \in R_c$. If $c_j c_l \neq 1$, then $\varphi(u) = 0$ in R_c . If $c_j c_l = 1$, then $\varphi(u) = (\text{unit}) \cdot (u - 1)^{q-1}$. (iii) If some pair $\{j_i, k_i\}$ of J , $i \geq 1$, has $c_{j_i} c_{k_i} \neq 1$, then $\pi_c(\bar{\psi}_J) = 0$. If $c_{j_i} c_{k_i} = 1$ for $i = 1, \dots, k$, then also $c_0 c_{k_0} = 1$, and

$$\pi_c(\bar{\psi}_J) = (\text{unit}) \cdot (t_{k_0} - 1) \cdot \prod_{i=1}^k (t_{k_i} - 1)(t_{j_i} t_{k_i} - 1)^{q-1}. \quad (6.2)$$

Proof. (i) $t_i - 1 = (c_i - 1) + (t_i - c_i)$, a non-zero constant plus a nilpotent if $c_i \neq 1$. (ii) In $F[u]$, $(u - 1)\varphi(u) = u^m - 1 = \prod_{\xi \in \mu_r} (u - \xi)^q$, so $\varphi(u) = (u - 1)^{q-1} \cdot \prod_{\xi \neq 1} (u - \xi)^q$. In R_c , $t_j^q = c_j^q$ and $t_l^q = c_l^q$ (Frobenius), so $(u - c_j c_l)^q = 0$. If $\xi_0 := c_j c_l \neq 1$, then $\xi_0 \in \mu_r \setminus \{1\}$ and the factor $(u - \xi_0)^q$ vanishes. If $c_j c_l = 1$, then $u - 1$ is nilpotent and each $u - \xi = (1 - \xi) + (u - 1)$, $\xi \neq 1$, is a unit. (iii) The first sentence follows from (ii). For the second, $1 = \prod_{i=0}^{n+1} c_i = c_0 c_{k_0} \cdot \prod_{i \geq 1} c_{j_i} c_{k_i}$; then apply (ii) to each factor $\varphi(t_{j_i} t_{k_i})$. ■

6.3 Colour classes and the tensor decomposition

For $\zeta \in \mu_r$ put $\mathcal{C}_\zeta := \{i \in \{0, \dots, n + 1\} : c_i = \zeta\}$ (the index 0 carries the colour c_0). Since r is odd, $\zeta \neq \zeta^{-1}$ for $\zeta \neq 1$, and $\mu_r \setminus \{1\}$ splits into $(r - 1)/2$ pairs $\{\zeta, \zeta^{-1}\}$; fix a set $\mathcal{R}_r$ of representatives. The sets $\mathcal{C}_1$ and $\mathcal{C}_\zeta \cup \mathcal{C}_{\zeta^{-1}}$ ($\zeta \in \mathcal{R}_r$) partition $\{0, \dots, n + 1\}$; we call them the **blocks** of c . We say that $J \in \mathcal{J}$ is **compatible** with c if $c_a c_b = 1$ for every pair $\{a, b\}$ of J ; by Lemma 6.2(iii) this means $c_{j_i} c_{k_i} = 1$ for $i = 1, \dots, k$, and $\pi_c(\bar{\psi}_J) = 0$ unless J is compatible.

Lemma 6.3. A pair $\{a, b\}$ has $c_a c_b = 1$ iff $\{a, b\} \subseteq \mathcal{C}_1$, or $\{a, b\}$ meets both $\mathcal{C}_\zeta$ and $\mathcal{C}_{\zeta^{-1}}$ for some $\zeta \in \mathcal{R}_r$. Hence J is compatible with c iff it consists of a perfect matching P of $\mathcal{C}_1$ and, for each $\zeta \in \mathcal{R}_r$, of the pairs of a bijection $\sigma_\zeta : \mathcal{C}_\zeta \rightarrow \mathcal{C}_{\zeta^{-1}}$; and every such choice $(P, (\sigma_\zeta))$ is a compatible matching (it is a perfect matching of $\{0, \dots, n + 1\}$, hence an element of $\mathcal{J}$: this is where the full family is used, cf. Remark 6.10(3)). A compatible matching exists iff $|\mathcal{C}_1|$ is even and $|\mathcal{C}_\zeta| = |\mathcal{C}_{\zeta^{-1}}|$ for every ζ ; we then call c a **compatible colouring**. ■

Group the tensor factors of R_c by blocks: $R_c = R_{c,1} \otimes \otimes_{\zeta \in \mathcal{R}_r} R_{c,\zeta}$, where $R_{c,1} := \otimes_{i \in \mathcal{C}_1 \setminus \{0\}} F[t_i]/((t_i - 1)^q)$ and $R_{c,\zeta} := \otimes_{i \in (\mathcal{C}_\zeta \cup \mathcal{C}_{\zeta^{-1}}) \setminus \{0\}} F[t_i]/((t_i - c_i)^q)$ (an empty tensor product

is F ; the variable t_0 does not exist). Each factor of (6.2) involves the variables of one pair of J , and a pair of a compatible J lies in one block; the factor of the pair $\{0, k_0\}$ is $t_{k_0} - 1$, which lies in the block of k_0 . So, for a compatible $J = (P, (\sigma_\zeta))$,

$$\pi_c(\bar{\psi}_J) = (\text{unit}) \cdot g_P \otimes \otimes_{\zeta \in \mathcal{R}_r} g_{\sigma_\zeta},$$

where $g_P \in R_{c,1}$ and $g_{\sigma_\zeta} \in R_{c,\zeta}$ are the products of the factors of (6.2) belonging to the pairs of P and of σ_ζ (an empty product is 1; the unit of (6.2) is absorbed into one of them, and units do not change the ideals below). Put $I_{c,1} := (g_P : P)$ and $I_{c,\zeta} := (g_\sigma : \sigma)$, the ideals generated over all perfect matchings P of $\mathcal{C}_1$ and all bijections $\sigma : \mathcal{C}_\zeta \rightarrow \mathcal{C}_{\zeta^{-1}}$.

Lemma 6.4 (tensor products of ideals). *Let R, R' be finite-dimensional commutative F -algebras and $I = (g_\alpha)$, $I' = (g'_\beta)$ ideals. Then the ideal of $R \otimes R'$ generated by the $g_\alpha \otimes g'_\beta$ is $I \otimes I'$, and $\dim(I \otimes I') = \dim I \cdot \dim I'$.*

Proof. $I \otimes I'$ is an ideal of $R \otimes R'$ (pure tensors span, and $(r \otimes r')(x \otimes x') = rx \otimes r'x'$), and it contains the $g_\alpha \otimes g'_\beta$. Conversely, for $x = \sum_\alpha r_\alpha g_\alpha \in I$ and $x' = \sum_\beta r'_\beta g'_\beta \in I'$, $x \otimes x' = \sum_{\alpha,\beta} (r_\alpha \otimes r'_\beta)(g_\alpha \otimes g'_\beta)$. A basis of I tensored with a basis of I' is a basis of $I \otimes I'$. ■

Proposition 6.5 (tensor decomposition). *If c is not compatible, $\pi_c(I) = 0$. If c is compatible, $\pi_c(I) = I_{c,1} \otimes \otimes_{\zeta \in \mathcal{R}_r} I_{c,\zeta}$ and $\dim \pi_c(I) = \dim I_{c,1} \cdot \prod_\zeta \dim I_{c,\zeta}$.*

Proof. Units do not change the ideal generated, so by Lemmas 6.2 and 6.3 $\pi_c(I)$ is generated by the pure tensors $g_P \otimes \otimes_\zeta g_{\sigma_\zeta}$, over all independent choices of P and (σ_ζ) . Apply Lemma 6.4 repeatedly. ■

6.4 The block of colour 1

In $F[t]/((t-1)^q)$ put $y := t - t^{-1}$. Lemma 2.3 holds verbatim here: its proof uses only $(t-1)^q = 0$, $q = p^v$ and $2 \in F^\times$. So $R_{c,1} = F[y_i : i \in \mathcal{C}_1 \setminus \{0\}]/(y_i^q)$, with $y_i = (\text{unit}) \cdot (t_i - 1)$ and $t_i t_l - 1 = (\text{unit}) \cdot (y_i + y_l)$. By Lemma 2.4(i), for a pair $\{i < l\} \subseteq \mathcal{C}_1 \setminus \{0\}$, $(t_l - 1)(t_i t_l - 1)^{q-1} = (\text{unit}) \cdot y_i y_l \cdot D(y_i, y_l)$; if $0 \in \mathcal{C}_1$, the pair $\{0, k_0\}$ contributes $t_{k_0} - 1 = (\text{unit}) \cdot y_{k_0}$. The indices in these monomial factors are the elements of $\mathcal{C}_1 \setminus \{0\}$, each once, so $g_P = (\text{unit}) \cdot Y_1 \cdot D_P$ with $Y_1 := \prod_{i \in \mathcal{C}_1 \setminus \{0\}} y_i$ and D_P the product of the $D(y_i, y_l)$ over the pairs of P avoiding 0. By the argument of Proposition 2.5 (the kernel of multiplication by Y_1 on $R_{c,1}$ is exactly $(y_i^{q-1} : i \in \mathcal{C}_1 \setminus \{0\})$, so $f \mapsto Y_1 f$ induces an injective map from the quotient $C(\mathcal{C}_1 \setminus \{0\})$ into $R_{c,1}$),

$$\begin{aligned} \dim I_{c,1} &= \dim_F(D_P : P) \cdot C(\mathcal{C}_1 \setminus \{0\}), \\ C(S) &:= F[y_i : i \in S]/(y_i^{q-1} : i \in S). \end{aligned}$$

Let $N_1(c)$ be the number of tuples $(w_i)_{i \in \mathcal{C}_1 \setminus \{0\}} \in (\mu_q \setminus \{1\})^{\mathcal{C}_1 \setminus \{0\}}$ such that, with $w_0 := (\prod w_i)^{-1}$ if $0 \in \mathcal{C}_1$, the multiset $\{w_i : i \in \mathcal{C}_1\}$ lies in $\mu_q \setminus \{1\}$ and is closed under inversion. (For $|\mathcal{C}_1|$ even the condition $w_0 \neq 1$ is automatic: otherwise the other $|\mathcal{C}_1| - 1$ entries, an odd number, would form a multiset in $\mu_q \setminus \{1\}$ closed under the fixed-point-free inversion.)

Lemma 6.6. $\dim I_{c,1} \geq N_1(c)$.

Proof. If $|\mathcal{C}_1|$ is odd, both sides are 0: there is no perfect matching, and a multiset closed under the fixed-point-free inversion of $\mu_q \setminus \{1\}$ has even size. Let $|\mathcal{C}_1| = 2k'$.

- If $0 \in \mathcal{C}_1$, relabel $\mathcal{C}_1 \setminus \{0\}$ increasingly as $\{1, \dots, 2k' - 1\}$. Write $\mathcal{J}_j$ for the set $\mathcal{J}$ in dimension $2j$. The perfect matchings P of $\mathcal{C}_1$ are the matchings $J \in \mathcal{J}_{k'-1}$, and $D_P = \pm D_J$. So

$\dim I_{c,1} = \dim(D_J : J \in \mathcal{J}_{k'-1})C_{2k'-1} \geq Q_{k'-1}(q)$ by Lemma 5.2 and Theorem 5.3 (over every field, here F). By Lemma 2.2 (whose proof uses only that q is odd), $N_1(c) = Q_{k'-1}(q)$. (For $k' = 1$ both sides are $q - 1$.)

- If $0 \notin \mathcal{C}_1$, relabel $\mathcal{C}_1$ as $\{1, \dots, 2k'\}$. In $\text{Par}_{2k'}^{(h)}$ the set $\{\emptyset\}$ is a down-set, since $\lambda \preceq \emptyset$ forces $\lambda = \emptyset$. A tight pattern of $\emptyset$ on $[2k']$ has k' pairs and no blocks: it is a perfect matching P , with product D_P . So $(D_P : P)C_{2k'} = V_{\{\emptyset\}}$, and Theorem 5.3 gives $\dim \geq |Z_{\{\emptyset\}}|$, the number of $2k'$ -tuples in T whose multiset is closed under the involution. A bijection $\mu_q \setminus \{1\} \rightarrow T$ carrying inversion to $u \mapsto -u$ (both are sets of $q - 1$ elements with a fixed-point-free involution) identifies this number with $N_1(c)$. (For $k' = 0$, $I_{c,1} = R_{c,1} = F$ and $N_1(c) = 1$.) $\blacksquare$

6.5 The pair blocks

Fix $\zeta \in \mathcal{R}_r$, and put $A := \mathcal{C}_\zeta$, $B := \mathcal{C}_{\zeta^{-1}}$, $A^* := A \setminus \{0\}$, $B^* := B \setminus \{0\}$. For $i \in A^*$ put $x_i := \zeta^{-1}t_i - 1$, and for $l \in B^*$ put $z_l := (\zeta t_l)^{-1} - 1$.

Lemma 6.7. (i) $R_{c,\zeta} = F[x_i(i \in A^*), z_l(l \in B^*)]/(x_i^q, z_l^q)$. (ii) For $i \in A^*$, $l \in B^*$: $t_i t_l - 1 = (\text{unit}) \cdot (x_i - z_l)$. (iii) Let $\alpha := |A^*|$ and $\beta := |B^*|$ (the numbers of x - and z -variables, as in §7), and relabel $A^* = \{1, \dots, \alpha\}$, $B^* = \{1, \dots, \beta\}$. If $0 \notin A \cup B$ and $\alpha = \beta =: a$, then $I_{c,\zeta} \cong I_a^{\text{bal}} := (\prod_{i=1}^a (x_i - z_{\sigma(i)})^{q-1} : \sigma \in S_a)$. If $0 \in B$ and $\alpha = \beta + 1$, then $I_{c,\zeta} \cong I_\beta^{\text{ph}}$, where $I_a^{\text{ph}} := (\prod_{i \neq i_0} (x_i - z_{\sigma(i)})^{q-1} : i_0 \in [a+1], \sigma : [a+1] \setminus \{i_0\} \rightarrow [a] \text{ bijective})$; if $0 \in A$ and $\beta = \alpha + 1$, then $I_{c,\zeta} \cong I_\alpha^{\text{ph}}$, after exchanging the names x and z . In all other cases $I_{c,\zeta} = 0$.

Proof. (i) $x_i = \zeta^{-1}(t_i - \zeta)$ is a unit multiple of the generator of the maximal ideal of the local ring $F[t_i]/((t_i - \zeta)^q)$, so $x_i^q = 0$ and $1, x_i, \dots, x_i^{q-1}$ is a basis. Similarly $\varepsilon_l := \zeta t_l - 1$ is nilpotent with $\varepsilon_l^q = 0$, and $z_l = (1 + \varepsilon_l)^{-1} - 1 = -\varepsilon_l(1 + \varepsilon_l)^{-1}$ is a unit multiple of ε_l . (ii) $t_i = \zeta(1 + x_i)$ and $t_l = \zeta^{-1}(1 + z_l)^{-1}$, so $t_i t_l - 1 = (x_i - z_l)(1 + z_l)^{-1}$. (iii) Every $t_s - 1$ with $s \in A^* \cup B^*$ is a unit (Lemma 6.2(i)), since $c_s \neq 1$. By (6.2) and (ii), the factor of a pair $\{i, l\}$, $i \in A^*$, $l \in B^*$, is $(\text{unit}) \cdot (x_i - z_l)^{q-1}$, and the factor of the pair $\{0, k_0\}$ is a unit. If $0 \notin A \cup B$, the bijections $A \rightarrow B$ are the $\sigma \in S_a$, $a = \alpha = \beta$. If $0 \in B$, a bijection $\sigma : A \rightarrow B$ sends exactly one $i_0 \in A$ to 0, and the other pairs give the product over $i \neq i_0$. If $0 \in A$, the same holds with the roles of A and B exchanged; since $(x - z)^{q-1} = \pm(z - x)^{q-1}$ and a sign does not change the ideal generated, exchanging the names of the variables carries this ideal onto I_a^{ph} . (Here q is odd and the sign is $+$; §9 uses the same argument with an even q .) If $|A| \neq |B|$, there is no bijection. (For $\alpha = \beta = 0$, $I_0^{\text{bal}} = (1)$ is the ring F ; for $\beta = 0$ in the second case, $I_0^{\text{ph}} = (1)$ is the ring $F[x_1]/(x_1^q)$; and in the third case with $\alpha = 0$, for instance $\mathcal{C}_\zeta = \{0\}$ and $\mathcal{C}_{\zeta^{-1}} = \{l\}$, it is the ring $F[z_1]/(z_1^q)$, of dimension q .) $\blacksquare$

6.6 The count factors in the same way

Let Ω be a set of q elements. For $a \geq 0$ put

$$N_{\text{bal}}(a, q) := \#\{(\xi, \eta) \in \Omega^a \times \Omega^a : \text{the multisets of } \xi \text{ and } \eta \text{ are equal}\} = \sum_{c_1 + \dots + c_q = a} (a! / (c_1! \cdots c_q!))^2,$$

$$N_{\text{ph}}(a, q) := \#\{(\xi, \eta) \in \Omega^{a+1} \times \Omega^a : \text{the multiset of } \eta \text{ is contained in that of } \xi\}.$$

Lemma 6.8. $|\Gamma_{\mathcal{J}}| = \sum_c N_1(c) \cdot \prod_{\zeta \in \mathcal{R}_r} N_\zeta(c)$, the sum over the compatible colourings, where $N_\zeta(c) := N_{\text{bal}}(\alpha, q)$ in the first case of Lemma 6.7(iii) and $N_\zeta(c) := N_{\text{ph}}(\min(\alpha, \beta), q)$ in the other two (α, β as there).

Proof. By the first paragraph of the proof of Lemma 2.2 (which uses nothing about m), $\Gamma_{\mathcal{J}}$ is the set of $g = (g_1, \dots, g_{n+1}) \in \mu_m^{n+1}$ such that, with $g_0 := (g_1 \cdots g_{n+1})^{-1}$, all $g_i \neq 1$ and the multiset $\{g_0, \dots, g_{n+1}\}$ splits into inverse pairs; since m is odd, inversion has no fixed point on $\mu_m \setminus \{1\}$, and «splits into inverse pairs» means «closed under inversion». Here $\mu_m \subset C$ is the group of complex m -th roots of unity (the rest of §6 works over $\bar{F}_p$). As $\gcd(q, r) = 1$, $\mu_m = \mu_q \times \mu_r$; write $g_i = c_i w_i$ with $c_i \in \mu_r$, $w_i \in \mu_q$ ($i = 0, \dots, n+1$). Then $c_0 = (c_1 \cdots c_{n+1})^{-1}$, $w_0 = (w_1 \cdots w_{n+1})^{-1}$, $g_i g_l = 1$ iff $c_i c_l = 1$ and $w_i w_l = 1$, and $g_i \neq 1$ iff $(c_i, w_i) \neq (1, 1)$. If $g \in \Gamma_{\mathcal{J}}$, its pairing into inverse pairs is a matching compatible with $c := (c_1, \dots, c_{n+1})$, so c is a compatible colouring. Fix a compatible c . By Lemma 6.3, a tuple g with colouring c lies in $\Gamma_{\mathcal{J}}$ iff (1) the multiset $\{w_i : i \in \mathcal{C}_1\}$ lies in $\mu_q \setminus \{1\}$ and is closed under inversion, and (2) for each $\zeta \in \mathcal{R}_r$ the multiset $\{w_i : i \in \mathcal{C}_{\zeta}\}$ equals the multiset $\{w_l^{-1} : l \in \mathcal{C}_{\zeta^{-1}}\}$. (Condition (2) allows the value $w_i = 1$, rightly: for $i \in \mathcal{C}_{\zeta} \cup \mathcal{C}_{\zeta^{-1}}$ one has $g_i \neq 1$ whatever w_i is, since $c_i \neq 1$.) Each condition involves the w_i of one block. The only coupling between blocks is w_0 : every block that satisfies its condition and does not contain 0 has $\prod w_i = 1$ over its indices, so, when all these blocks satisfy their conditions, $w_0 = (\prod_{i \in \mathcal{K} \setminus 0} w_i)^{-1}$ for the block $\mathcal{K} \ni 0$, a function of the w_i of $\mathcal{K}$ alone. Conversely, given w -values on each block that satisfy its condition, where for the block $\mathcal{K} \ni 0$ the value w_0 is computed from that block alone, the blocks not containing 0 have product 1, so this value is the true $(w_1 \cdots w_{n+1})^{-1}$ and the assembled tuple lies in $\Gamma_{\mathcal{J}}$. Hence the count over c is the product of the block counts. (For a compatible c , exactly one of the three cases of Lemma 6.7(iii) holds for each ζ .) The block $\mathcal{C}_1$ gives $N_1(c)$, and a balanced pair block gives $N_{\text{bal}}(\alpha, q)$ ($\Omega = \mu_q$, $\xi := (w_i)_{i \in \mathcal{C}_{\zeta}}$, $\eta := (w_l^{-1})_{l \in \mathcal{C}_{\zeta^{-1}}}$). For a pair block with $0 \in \mathcal{C}_{\zeta^{-1}}$, let ξ be the w_i on $\mathcal{C}_{\zeta}$ ($\beta + 1$ of them) and η the w_l^{-1} on $\mathcal{C}_{\zeta^{-1}} \setminus 0$; the condition says $\text{multiset}(\xi) = \text{multiset}(\eta) \cup \{w_0^{-1}\}$, with $w_0^{-1} = \prod \xi \cdot (\prod \eta)^{-1}$. If $\text{multiset}(\eta) \subseteq \text{multiset}(\xi)$, the difference is one element ξ^* and $\prod \xi \cdot (\prod \eta)^{-1} = \xi^*$, so the condition holds; conversely it implies $\text{multiset}(\eta) \subseteq \text{multiset}(\xi)$. So this block gives $N_{\text{ph}}(\beta, q)$, and so does the case $0 \in \mathcal{C}_{\zeta}$, by the symmetry $\xi \leftrightarrow \eta$, $w \mapsto w^{-1}$. ■

6.7 The reduction

Proposition 6.9 (colour reduction). *Let $k \geq 1$, let $m = q \cdot r$ be odd, $q = p^v$, $p \nmid r$, and suppose that $\dim_F I_a^{\text{bal}} \geq N_{\text{bal}}(a, q)$ and $\dim_F I_a^{\text{ph}} \geq N_{\text{ph}}(a, q)$ for every $a \geq 0$, where $F = \bar{F}_p$. Then $\dim_{F_p} F_p[G]/(\psi_J : J \in \mathcal{J}) = m^{n+1} - |\Gamma_{\mathcal{J}}|$, so $H_n(X)/L(X)$ has no p -torsion.*

Proof. By Lemma 6.1, Proposition 6.5, Lemmas 6.6 and 6.7 and the hypothesis, $\dim_F I = \sum_c \dim \pi_c(I) \geq \sum_c N_1(c) \cdot \prod_{\zeta} N_{\zeta}(c)$, the sum over the compatible colourings, and this is $|\Gamma_{\mathcal{J}}|$ by Lemma 6.8. With (6.1), $\dim_F I = |\Gamma_{\mathcal{J}}|$, and the per-prime clause of Proposition 2.1 concludes. ■

Remarks 6.10. (1) Only the inequality $\geq$ is needed on each block; the reverse inequality is global, (6.1). (2) For $r = 1$ there is one colouring, $\mathcal{C}_1 = \{0, \dots, n+1\}$, and Proposition 6.9 is Corollary 5.4. (3) For a subfamily $K \subsetneq \mathcal{J}$ the splitting of Lemma 6.1 still holds, but the matchings of K compatible with c are no longer a product set, and Proposition 6.5 fails; this is consistent with §11. (4) The splitting of Lemma 6.1 over F_p , with two factors per variable (the $(t-1)$ -primary part and the rest), was used earlier by the author as a memory-saving device for machine computations of these ranks, and to prove that any torsion is confined to one block [Rep, *The Localization Theorem, The Block Decomposition*]. Proposition 6.9 refines it over $\bar{F}_p$ to one factor per colouring and identifies every factor.

Example 6.11 ($k = 1$, $m = 15$). Here $N = 4$, $\mathcal{J}$ has three matchings, and $Q_1(15) = 3 \cdot 14 \cdot 13 = 546$. The compatible colourings, grouped by the shape of their blocks, contribute as follows (i, l, s are indices other than 0; $Q_0(q) = q - 1$):

blocks of the colouring	$p = 3$ ($q = 3, r = 5$): colourings $\times$ product	$p = 5$ ($q = 5, r = 3$): colourings $\times$ product
$\mathcal{C}_1 = \{0, 1, 2, 3\}$	$1 \times Q_1(3) = 6$	$1 \times Q_1(5) = 36$
$\mathcal{C}_1 = \{0, i\}$, and one balanced block $1 + 1$	$12 \times Q_0(3) \cdot N_{\text{bal}}(1, 3) =$ 12×6	$6 \times Q_0(5) \cdot N_{\text{bal}}(1, 5) = 6 \times 20$
$\mathcal{C}_1 = \{i, l\}$, and a phantom block $\{0\}$ against $\{s\}$	$12 \times Q_0(3) \cdot N_{\text{ph}}(0, 3) =$ 12×6	$6 \times Q_0(5) \cdot N_{\text{ph}}(0, 5) = 6 \times 20$
$\mathcal{C}_1 = \emptyset$, and one phantom block $2 + 2$ containing 0	$12 \times N_{\text{ph}}(1, 3) = 12 \times 15$	$6 \times N_{\text{ph}}(1, 5) = 6 \times 45$
$\mathcal{C}_1 = \emptyset$, a balanced block $1 + 1$ and a phantom block $\{0\}$ against $\{s\}$	$24 \times N_{\text{bal}}(1, 3) \cdot N_{\text{ph}}(0, 3) =$ 24×9	none (μ_3 has one pair of inverse colours)
total	61 colourings, 546	19 colourings, 546

At both primes the sum is $Q_1(15)$, as Lemma 6.8 says; the literal computation of §14.3 gives the same 546. (At $k = 1$ the Main Theorem is Degtyarev's theorem [De14]; the example only shows the bookkeeping.)

7. The bipartite count

This section proves the hypothesis of Proposition 6.9, and so completes the proof of the Main Theorem for odd m . The method is that of §5, with two changes: the box is q instead of $q - 1$, and the single partition of §5 is replaced by a *pair* of partitions, one for each of the two sets of variables. Throughout, $q \geq 2$ is an integer, odd or even, and F is a field in which the binomial coefficients $C(q - 1, t)$, $0 \leq t \leq q - 1$, are non-zero: for instance $\text{char } F = 0$, or $\text{char } F = p$ and $q = p^v$ for a prime p , the prime 2 included (then $C(q - 1, t) \equiv (-1)^t \pmod{p}$, because $(1 + u)^{q-1} = (1 + u^q)(1 + u)^{-1}$ in $F_p[[u]]$). The parity of q plays no role in this section: q enters only as the size of the box and of the set Ω , and the field only through the binomial coefficients, in case (γ) of Proposition 7.5. (Versions 6 to 10 of this paper stated the section for odd q , which is what §6 needs; §9 needs it for $q = 2^v$ in characteristic 2. The proofs are unchanged.) Let Ω be a set of q elements. For finite index sets A and B put $\alpha := |A|$, $\beta := |B|$ and

$$R_{A,B} := F[x_i(i \in A), z_l(l \in B)] / (x_i^q, z_l^q).$$

(The symbols $A, B, R_{A,B}$ are local to this section.) Points are pairs $(\xi, \eta) \in \Omega^A \times \Omega^B$.

THEOREM C (the bipartite count). *For every $a \geq 0$:*

$$\dim_F I_a^{\text{bal}} \geq N_{\text{bal}}(a, q) \text{ and } \dim_F I_a^{\text{ph}} \geq N_{\text{ph}}(a, q) = N_{\text{bal}}(a + 1, q),$$

where $I_a^{\text{bal}} \subseteq R_{[a],[a]}$ and $I_a^{\text{ph}} \subseteq R_{[a+1],[a]}$ are the ideals of Lemma 6.7(iii) and $N_{\text{bal}}, N_{\text{ph}}$ are the counts of §6.6.

Theorem C is the root case of Theorem 7.6 below. With Proposition 6.9 it gives the Main Theorem for m not a prime power (Corollary 7.7). Over $\bar{F}_p$ both inequalities are equalities (Corollary 7.8); in characteristic 0 they are strict in general (Remarks 7.9).

7.1 Peeling with the box q

Write $R_{A,B} = R_{A \setminus \{i_1\}, B}[w] / (w^q)$ with $w := x_{i_1}$ for some $i_1 \in A$. For an ideal $V \subseteq R_{A,B}$ and $0 \leq j \leq q - 1$ put $V_{\leq j} := \{f \in V : \deg_w f \leq j\}$ and $W_j(V) := \{[w^j]f : f \in V_{\leq j}\} \subseteq R_{A \setminus \{i_1\}, B}$.

Lemma 7.1 (peeling). (i) $W_j(V)$ is an ideal. (ii) $W_j(V) \subseteq W_{j+1}(V)$ for $0 \leq j < q-1$. (iii) $\dim V = \sum_{j=0}^{q-1} \dim W_j(V)$. (iv) For $Z \subseteq \Omega^A \times \Omega^B$ and a tail M' (the coordinates other than i_1) let $F(M') := \{u \in \Omega : (u, M') \in Z\}$ and $Z_{>i} := \{M' : |F(M')| > i\}$; then $|Z| = \sum_{i=0}^{q-1} |Z_{>i}|$.

Proof. As for Lemma 5.1, with q in place of $q-1$: in (ii) one uses $w^{j+1} \neq 0$, i.e. $j+1 \leq q-1$, and in (iv) $|F(M')| \leq q$. ■

7.2 Pairs of partitions and the bipartite down-set family

We use the partial sums S_t and the weak dominance order $\preceq$ of §5.2 (defined also between partitions of different sizes), and the rows $\bar{r}_j, \underline{r}_j$ of §5.5.

- **Residue shape.** For (ξ, η) , let X and Y be the multisets of values of ξ and η . Let R_+ keep, for each value u with $\text{mult}_X(u) > \text{mult}_Y(u)$, the difference $\text{mult}_X(u) - \text{mult}_Y(u)$ of copies of u , and let R_- be defined symmetrically. The **shape** of (ξ, η) is $\lambda(\xi, \eta) := (\lambda_+, \lambda_-)$, the multiplicity partitions of R_+ and R_- . Their supports are disjoint subsets of Ω , so $\ell(\lambda_+) + \ell(\lambda_-) \leq q$; moreover $|\lambda_+| - |\lambda_-| = \alpha - \beta$ and $|\lambda_+| + |\lambda_-| \leq \alpha + \beta$.
- $\text{BPar}_q(\alpha, \beta)$ is the set of pairs (λ_+, λ_-) of partitions with $|\lambda_+| - |\lambda_-| = \alpha - \beta$, $|\lambda_+| + |\lambda_-| \leq \alpha + \beta$ and $\ell(\lambda_+) + \ell(\lambda_-) \leq q$. It is ordered by the product order: $(\lambda_+, \lambda_-) \preceq (\mu_+, \mu_-)$ iff $\lambda_+ \preceq \mu_+$ and $\lambda_- \preceq \mu_-$. Every element of $\text{BPar}_q(\alpha, \beta)$ is the shape of some point (give the $\ell(\lambda_+) + \ell(\lambda_-) \leq q$ rows pairwise distinct values and the pairs arbitrary values); this is not used below.
- For a $\preceq$ -down-set $\Lambda \subseteq \text{BPar}_q(\alpha, \beta)$ put $Z_\Lambda := \{(\xi, \eta) \in \Omega^A \times \Omega^B : \lambda(\xi, \eta) \in \Lambda\}$.
- **Tight patterns.** A tight pattern of $\lambda = (\lambda_+, \lambda_-) \in \text{BPar}_q(\alpha, \beta)$ on (A, B) consists of a set P of $\alpha - |\lambda_+| = \beta - |\lambda_-|$ pairwise disjoint pairs $(i, l) \in A \times B$, of blocks $B_1^+, \dots, B_{\lambda_+,1}^+$ partitioning $A \setminus A(P)$ with $|B_c^+| = (\lambda_+)'_c$, and of blocks $B_1^-, \dots, B_{\lambda_-,1}^-$ partitioning $B \setminus B(P)$ with $|B_c^-| = (\lambda_-)'_c$. Its **product** is

$$\prod_{(i,l) \in P} (x_i - z_l)^{q-1} \cdot \prod_c \Delta(x_{B_c^+}) \cdot \prod_c \Delta(z_{B_c^-}),$$

with Δ the Vandermonde determinant of §5.2.

- $V_\Lambda \subseteq R_{A,B}$ is the ideal generated by the products of all tight patterns on (A, B) of all elements of Λ . For $\alpha = \beta = 0$ the empty product is 1.

Lemma 7.2 (the roots). (i) $\{(\emptyset, \emptyset)\}$ is a down-set of $\text{BPar}_q(a, a)$, $V_{\{(\emptyset, \emptyset)\}} = I_a^{\text{bal}}$, and $|Z_{\{(\emptyset, \emptyset)\}}| = N_{\text{bal}}(a, q)$. (ii) $\{((1), \emptyset)\}$ is a down-set of $\text{BPar}_q(a+1, a)$, $V_{\{((1), \emptyset)\}} = I_a^{\text{ph}}$, and $|Z_{\{((1), \emptyset)\}}| = N_{\text{ph}}(a, q)$. (iii) $N_{\text{ph}}(a, q) = N_{\text{bal}}(a+1, q)$.

Proof. (i) $\lambda_\pm \preceq \emptyset$ forces $\lambda_\pm = \emptyset$. A tight pattern of $(\emptyset, \emptyset)$ is a perfect matching of A with B , i.e. a bijection σ , with product $\prod_i (x_i - z_{\sigma(i)})^{q-1}$; and the shape is $(\emptyset, \emptyset)$ iff $X = Y$. (ii) In $\text{BPar}_q(a+1, a)$, $|\lambda_+| = |\lambda_-| + 1$; $\lambda_- \preceq \emptyset$ forces $\lambda_- = \emptyset$ and then $\lambda_+ \preceq (1)$ with $|\lambda_+| = 1$ forces $\lambda_+ = (1)$. A tight pattern has a pairs and one x -block of size 1 (with $\Delta = 1$), so its product is a generator of I_a^{ph} , and every generator arises. The shape is $((1), \emptyset)$ iff $Y \subseteq X$. (iii) Given $(\xi, \eta) \in \Omega^{a+1} \times \Omega^a$ with $Y \subseteq X$, append to η the one element of $X - Y$; given a balanced point in $\Omega^{a+1} \times \Omega^{a+1}$, delete the last coordinate of η . These maps are mutually inverse. ■

For instance, $N_{\text{bal}}(a, 3) = 3, 15, 93, 639, 4653$ and $N_{\text{bal}}(2, q) = 15, 45, 91, 153, 231$ for $a = 1, \dots, 5$ and $q = 3, 5, 7, 9, 11$.

Lemma 7.2' (§5.5 and §5.6 for arbitrary partitions). *Let $\lambda \preceq \tilde{\lambda}$ be partitions of arbitrary sizes and lengths. Then the identities of §5.5, the chain of Lemma 5.5 for the removals and the additions, (T) of §5.6, the inequality (5.2) of §5.6 (if $\ell(\lambda) < t \leq \ell(\tilde{\lambda})$, then $S_t(\tilde{\lambda}) \geq |\lambda| + (t - \ell(\lambda))$) and the comparisons (a), (b), (c), (e2) of §5.6, recalled in the proof of Proposition 7.4, hold for λ and $\tilde{\lambda}$.*

Proof. The identities of §5.5 and the chain are statements about one partition. The proofs of (T), (5.2), (a), (b), (c) and (e2) in §5.6 compare the partial sums S_t of the two partitions term by term and use only $\lambda \preceq \tilde{\lambda}$. In §5.6 the parity of $|\mu|$ is used only in case (d1), and the cap $\ell \leq h$ only in the layout of the positions and in case (e1); none of these is borrowed here. ■

7.3 (P1) Fibres and (Chain)

Fix a down-set $\Lambda \subseteq \text{BPar}_q(\alpha, \beta)$ with $\alpha \geq 1$, and peel $w = x_{i_1}$. Let M' be a tail with shape $\mu = (\mu_+, \mu_-) \in \text{BPar}_q(\alpha - 1, \beta)$, residual values $u_1, \dots, u_{\ell_+}$ of R_+ (u_j with multiplicity $\mu_{+,j}$) and $v_1, \dots, v_{\ell_-}$ of R_- . Adding the value u at the index i_1 changes the shape as follows:

- $u = v_j$: $(\mu_+, \mu_- - e_j)$ (one box removed from row j of μ_- , re-sorted);
- $u = u_j$: $(\mu_+ + e_j, \mu_-)$;
- u any of the $q - \ell_+ - \ell_-$ other values (the values whose multiplicities in the two coordinate sets of the tail agree, possibly $0 = 0$): $(\mu_+ \sqcup 1, \mu_-)$.

These are $q = |\Omega|$ values, and every resulting shape lies in $\text{BPar}_q(\alpha, \beta)$: one value is added to the x -side, and a middle value exists only when $\ell_+ + \ell_- < q$, which gives $\ell(\mu_+ \sqcup 1) + \ell(\mu_-) \leq q$. List them by position $p = 1, \dots, q$: $\text{opt}_p(\mu) := (\mu_+, \mu_- - e_p)$ for $p \leq \ell_-$; $(\mu_+ \sqcup 1, \mu_-)$ for $\ell_- < p \leq q - \ell_+$ (the **middle** positions); $(\mu_+ + e_{q+1-p}, \mu_-)$ for $p > q - \ell_+$. Hence $|F(M')| = F_\Lambda(\mu) := \#\{p : \text{opt}_p(\mu) \in \Lambda\}$, and $Z_{>i} = Z_{\Lambda_i}$ with $\Lambda_i := \{\mu \in \text{BPar}_q(\alpha - 1, \beta) : F_\Lambda(\mu) > i\}$.

Lemma 7.3 (chain). $\text{opt}_1(\mu) \preceq \text{opt}_2(\mu) \preceq \dots \preceq \text{opt}_q(\mu)$. *Hence the options lying in Λ form an initial segment, of length $F_\Lambda(\mu)$, and*

$$F_\Lambda(\mu) = r + (q - \ell_+ - \ell_-) \cdot \iota + (\ell_+ - j_0 + 1) \cdot [j_0 \text{ exists}], \quad (7.1)$$

where $r = 0$ or r is the last row of μ_- of its length (the removals in Λ are those at positions $\leq r$), $\iota := [(\mu_+ \sqcup 1, \mu_-) \in \Lambda]$ ($\iota := 0$ if $\ell_+ + \ell_- = q$), and j_0 , if it exists, is the first row of μ_+ of its length such that $(\mu_+ + e_j, \mu_-) \in \Lambda$ exactly for $j_0 \leq j \leq \ell_+$. If j_0 exists, then $r = \ell_-$, and either $\iota = 1$ or $\ell_+ + \ell_- = q$; if $\iota = 1$, then $r = \ell_-$.

Proof. By the identities of §5.5 (Lemma 7.2'), $\mu_- - e_1 \preceq \dots \preceq \mu_- - e_{\ell_-} \preceq \mu_-$ and $\mu_+ \preceq \mu_+ \sqcup 1 \preceq \mu_+ + e_{\ell_+} \preceq \dots \preceq \mu_+ + e_1$. Along the removals the first component is μ_+ , and along the middle and the additions the second component is μ_- ; so in the product order the list is weakly increasing, including the step from the last removal to the first middle or addition option. Since Λ is a down-set, the options in Λ form an initial segment. Rows of equal length give equal options, which gives the description of r and j_0 . ■

In particular, with $\Phi := F_\Lambda(\mu)$: $\Phi = q - j_0 + 1$ if j_0 exists, $\Phi = q - \ell_+$ if j_0 does not exist and $\iota = 1$, and $\Phi = r$ otherwise.

7.4 (P2) The layers are down-sets

Proposition 7.4 (inequality of pairs of partitions). *If $\mu, \tilde{\mu} \in \text{BPar}_q(\alpha - 1, \beta)$ and $\mu \preceq \tilde{\mu}$, then $\text{opt}_p(\mu) \preceq \text{opt}_p(\tilde{\mu})$ for every p . Hence $F_\Lambda(\mu) \geq F_\Lambda(\tilde{\mu})$ and every Λ_i is a down-set.*

Proof. The second sentence follows from the first as in Proposition 5.6. Write $\ell_{\pm} := \ell(\mu_{\pm})$, $\tilde{\ell}_{\pm} := \ell(\tilde{\mu}_{\pm})$. Since $|\mu_+| - |\mu_-| = |\tilde{\mu}_+| - |\tilde{\mu}_-|$, any strict inequality $|\tilde{\mu}_-| > |\mu_-|$ gives $|\tilde{\mu}_+| > |\mu_+|$. We use (T) of §5.6 and the inequality (5.2) (Lemma 7.2'): if $\lambda \preceq \tilde{\lambda}$ and $\ell(\lambda) < t \leq \ell(\tilde{\lambda})$, then $S_t(\tilde{\lambda}) \geq |\lambda| + (t - \ell(\lambda))$. We also use four comparisons of §5.6, valid for arbitrary partitions by Lemma 7.2': **(a)** $\lambda - e_p \preceq \tilde{\lambda} - e_p$ for $p \leq \min(\ell(\lambda), \ell(\tilde{\lambda}))$; **(b)** $\lambda + e_j \preceq \tilde{\lambda} + e_j$ for $j \leq \min(\ell(\lambda), \ell(\tilde{\lambda}))$; **(c)** $\lambda \sqcup 1 \preceq \tilde{\lambda} \sqcup 1$; **(e2)** $\lambda + e_j \preceq \tilde{\lambda} \sqcup 1$ for $\ell(\tilde{\lambda}) < j \leq \ell(\lambda)$. Each position p is a removal (R), a middle position (M) or an addition (A) for μ , and likewise for $\tilde{\mu}$, which gives nine cases; put $j := q + 1 - p$ when p is an addition.

case	the position p is	option of μ	option of $\tilde{\mu}$	used
RR	a removal for both	$(\mu_+, \mu_- - e_p)$	$(\tilde{\mu}_+, \tilde{\mu}_- - e_p)$	$\mu_+ \preceq \tilde{\mu}_+$; (a)
AA	an addition for both	$(\mu_+ + e_j, \mu_-)$	$(\tilde{\mu}_+ + e_j, \tilde{\mu}_-)$	(b); $\mu_- \preceq \tilde{\mu}_-$
MM	middle for both	$(\mu_+ \sqcup 1, \mu_-)$	$(\tilde{\mu}_+ \sqcup 1, \tilde{\mu}_-)$	(c); $\mu_- \preceq \tilde{\mu}_-$
RM, RA	a removal for μ	$(\mu_+, \mu_- - e_p)$	middle or addition	the chain through $\mu \preceq \tilde{\mu}$
AM	an addition for μ , middle for $\tilde{\mu}$	$(\mu_+ + e_j, \mu_-)$	$(\tilde{\mu}_+ \sqcup 1, \tilde{\mu}_-)$	(e2); $\mu_- \preceq \tilde{\mu}_-$
MA	middle for μ , an addition for $\tilde{\mu}$	$(\mu_+ \sqcup 1, \mu_-)$	$(\tilde{\mu}_+ + e_j, \tilde{\mu}_-)$	dominance, (5.2), sizes; $\mu_- \preceq \tilde{\mu}_-$
MR	middle for μ , a removal for $\tilde{\mu}$	$(\mu_+ \sqcup 1, \mu_-)$	$(\tilde{\mu}_+, \tilde{\mu}_- - e_p)$	(5.2) and the transfer of sizes
AR	an addition for μ , a removal for $\tilde{\mu}$	$(\mu_+ + e_j, \mu_-)$	$(\tilde{\mu}_+, \tilde{\mu}_- - e_p)$	(T), (5.2) and the transfer of sizes

The «transfer of sizes» is the one genuinely bipartite step: since $|\mu_+| - |\mu_-| = |\tilde{\mu}_+| - |\tilde{\mu}_-|$, a strict inequality on the z -side gives one on the x -side.

- **RR** ($p \leq \min(\ell_-, \tilde{\ell}_-)$): first components $\mu_+ \preceq \tilde{\mu}_+$; second components by (a).
- **AA** ($j \leq \min(\ell_+, \tilde{\ell}_+)$): (b), and $\mu_- \preceq \tilde{\mu}_-$.
- **MM**: (c), and $\mu_- \preceq \tilde{\mu}_-$.
- **RM**: $(\mu_+, \mu_- - e_p) \preceq \mu \preceq \tilde{\mu} \preceq (\tilde{\mu}_+ \sqcup 1, \tilde{\mu}_-)$.
- **RA**: $(\mu_+, \mu_- - e_p) \preceq \mu \preceq \tilde{\mu} \preceq (\tilde{\mu}_+ + e_j, \tilde{\mu}_-)$.
- **AM** ($j \leq \ell_+$ and $\tilde{\ell}_+ < j$): (e2), and $\mu_- \preceq \tilde{\mu}_-$.
- **MA** (p middle for μ , so $j > \ell_+$; addition for $\tilde{\mu}$, so $j \leq \tilde{\ell}_+$): we need $\mu_+ \sqcup 1 \preceq \tilde{\mu}_+ + e_j$. For $t \leq \ell_+$, $S_t(\mu_+ \sqcup 1) = S_t(\mu_+) \leq S_t(\tilde{\mu}_+) \leq S_t(\tilde{\mu}_+ + e_j)$. For $\ell_+ < t \leq \tilde{\ell}_+$, $S_t(\tilde{\mu}_+) \geq |\mu_+| + 1 = S_t(\mu_+ \sqcup 1)$ by (5.2). For $t > \tilde{\ell}_+ \geq j \geq r_j(\tilde{\mu}_+)$, $S_t(\tilde{\mu}_+ + e_j) = |\tilde{\mu}_+| + 1 \geq |\mu_+| + 1$. The second components are $\mu_- \preceq \tilde{\mu}_-$.
- **MR** (p middle for μ , so $p > \ell_-$; removal for $\tilde{\mu}$, so $p \leq \tilde{\ell}_-$): by (5.2) at $t = \tilde{\ell}_-$, $|\tilde{\mu}_-| \geq |\mu_-| + 1$, hence $|\tilde{\mu}_+| \geq |\mu_+| + 1$. *First components*: $\mu_+ \sqcup 1 \preceq \tilde{\mu}_+$: for $t \leq \ell_+$ this is dominance; for $t > \ell_+$ we need $S_t(\tilde{\mu}_+) \geq |\mu_+| + 1$, which holds by (5.2) if $t < \tilde{\ell}_+$ and by $|\tilde{\mu}_+| \geq |\mu_+| + 1$ if $t \geq \tilde{\ell}_+$. *Second components*: $\mu_- \preceq \tilde{\mu}_- - e_p$: for $t < \tilde{r}_p(\tilde{\mu}_-)$ this is dominance; for $t \geq \tilde{r}_p(\tilde{\mu}_-) \geq p > \ell_-$, $S_t(\mu_-) = |\mu_-|$, while the rows $\ell_- + 1, \dots, p$ of $\tilde{\mu}_-$ are non-empty, so $S_t(\tilde{\mu}_-) \geq S_{\ell_-}(\tilde{\mu}_-) + 1 \geq |\mu_-| + 1$.
- **AR** (p addition for μ , so $j \leq \ell_+$; removal for $\tilde{\mu}$, so $p \leq \tilde{\ell}_-$): since $\ell_+ + \ell_- \leq q$ and $\tilde{\ell}_+ + \tilde{\ell}_- \leq q$, we have $\ell_- \leq q - \ell_+ < p$ and $\tilde{\ell}_+ \leq q - p = j - 1$. *Second components*: exactly as in MR, $\mu_- \preceq \tilde{\mu}_- - e_p$ and $|\tilde{\mu}_-| \geq |\mu_-| + 1$, so $|\tilde{\mu}_+| \geq |\mu_+| + 1$. *First components*: we need $S_t(\mu_+) + [t \geq r_j(\mu_+)] \leq S_t(\tilde{\mu}_+)$. This is dominance for $t < r_j(\mu_+)$, and it follows from $|\tilde{\mu}_+| \geq |\mu_+| + 1$ for $t \geq \tilde{\ell}_+$. It remains to show $S_t(\mu_+) < S_t(\tilde{\mu}_+)$ for $r_j(\mu_+) \leq t < \tilde{\ell}_+$.

Suppose t is tight. The rows $\underline{r}_j(\mu_+), \dots, j$ of μ_+ have the same length $c := \mu_{+,j} \geq 1$, and $t < t+1 \leq \tilde{\ell}_+ \leq j-1$, so $\mu_{+,t} = \mu_{+,t+1} = c$. By (T), $c = \mu_{+,t} \geq \tilde{\mu}_{+,t} \geq \tilde{\mu}_{+,t+1} \geq \mu_{+,t+1} = c$, so every row of $\tilde{\mu}_+$ after the t -th has length $\leq c$. As $\tilde{\mu}_+$ has only $\tilde{\ell}_+ \leq j-1$ rows, $S_j(\tilde{\mu}_+) \leq S_t(\mu_+) + (j-1-t)c < S_t(\mu_+) + (j-t)c = S_j(\mu_+)$, contradicting $\mu_+ \preceq \tilde{\mu}_+$.

For each of μ and $\tilde{\mu}$ the three types partition $\{1, \dots, q\}$, so the nine cases cover every position. ■

7.5 (P3) Every tight pattern of a layer lies in the right slice

Proposition 7.5. *For every $i \in \{0, \dots, q-1\}$, $V_{\Lambda_i} \subseteq W_{q-1-i}(V_\Lambda)$, where $V_{\Lambda_i} \subseteq R_{A \setminus \{i_1\}, B}$.*

Proof. It suffices to treat a generator G : the product of a tight pattern $(P, (B_c^+), (B_c^-))$ of some $\mu \in \Lambda_i$, so that $\Phi := F_\Lambda(\mu) \geq i+1$. By Lemma 7.1(ii) it is enough to find $f \in V_\Lambda$ with $\deg_w f \leq q - \Phi$ and $[w^{q-\Phi}]f = \pm \kappa \cdot G$ for a non-zero constant κ ; then $G \in W_{q-\Phi}(V_\Lambda) \subseteq W_{q-1-i}(V_\Lambda)$. By (7.1) exactly one of the following holds.

- (α) j_0 exists and $\lambda := (\mu_+ + e_{j_0}, \mu_-) \in \Lambda$, $\Phi = q - j_0 + 1$. The column $c^* := \mu_{+,j_0} + 1$ of μ_+ has height $j_0 - 1$, because j_0 is the first row of its length; let $S := B_{c^*}^+$ (if $j_0 = 1$, c^* is a new column and $S = \emptyset$). Putting i_1 into S gives a tight pattern of λ : column c^* of λ_+ has height j_0 , and the number of pairs $\alpha - |\lambda_+| = (\alpha - 1) - |\mu_+|$ is unchanged. Its product lies in V_Λ ; by the factorisation $\Delta(x_{S \cup i_1}) = \pm \prod_{s \in S} (w - x_s) \cdot \Delta(x_S)$ it has w -degree $|S| = j_0 - 1 = q - \Phi \leq q - 1$ (so $w^{|S|} \neq 0$ in the box) and top coefficient $\pm G$.
- (β) j_0 does not exist, $\iota = 1$, $\lambda := (\mu_+ \sqcup 1, \mu_-) \in \Lambda$, $\Phi = q - \ell_+$. Put i_1 into B_1^+ , of height ℓ_+ (empty if $\mu_+ = \emptyset$): this is a tight pattern of λ , whose product has w -degree $\ell_+ = q - \Phi \leq q - 1$ (a middle value exists, so $\ell_+ < q$) and top coefficient $\pm G$.
- (γ) j_0 does not exist, $\iota = 0$, and $\Phi = r \geq 1$, $\lambda := (\mu_+, \mu_- - e_r) \in \Lambda$. The column $c_0 := \mu_{-,r}$ of μ_- has height r , because r is the last row of its length; let $S := B_{c_0}^-$ and write $G = \Delta(z_S) \cdot G'$. For $b \in S$, the pairs $P \cup \{(i_1, b)\}$, the blocks B_c^+ , the blocks B_c^- ($c \neq c_0$) and $S \setminus \{b\}$ form a tight pattern of λ : column c_0 of λ_- has height $r - 1$, and the number of pairs grows by one, as $\alpha - |\lambda_+| = ((\alpha - 1) - |\mu_+|) + 1$. So, with the signs ε_b of Lemma 5.7(ii),

$$f := \sum_{b \in S} \varepsilon_b \Delta(z_{S \setminus b}) \cdot (w - z_b)^{q-1} \cdot G' \in V_\Lambda.$$

Expanding, $[w^{q-1-t}]f = C(q-1, t)(-1)^t \cdot (\sum_{b \in S} \varepsilon_b \Delta(z_{S \setminus b}) z_b^t) \cdot G'$, which is 0 for $t \leq r-2$ and $\pm C(q-1, r-1) \cdot G$ for $t = r-1$, by Lemma 5.7(ii) (an identity over Z , valid in $R_{A \setminus \{i_1\}, B}$). So $\deg_w f \leq q - r = q - \Phi$, and the top coefficient is $\pm C(q-1, r-1) \cdot G$ with $C(q-1, r-1) \neq 0$ in F (here $r \leq \ell_- \leq q$). ■

The three constructions land exactly in the slice $q - \Phi$, and in general the slice cannot be lowered: the statement with W_{q-2-i} in place of W_{q-1-i} fails at the cells of §14.4, for some generators G .

7.6 The induction

Theorem 7.6 (bipartite down-set theorem). *For all $\alpha, \beta \geq 0$ and every $\preceq$ -down-set $\Lambda \subseteq \text{BPar}_q(\alpha, \beta)$, $\dim_F V_\Lambda \geq |Z_\Lambda|$.*

Proof. Induction on $\alpha + \beta$. **Base:** $\text{BPar}_q(0, 0) = \{(\emptyset, \emptyset)\}$; for $\Lambda = \emptyset$ both sides are 0, and for $\Lambda = \{(\emptyset, \emptyset)\}$, $V_\Lambda = F$ and Z_Λ is one point. **Symmetry:** the isomorphism $R_{A,B} \cong R_{B,A}$

that exchanges the names x and z carries tight-pattern products of (λ_+, λ_-) on (A, B) to tight-pattern products of (λ_-, λ_+) on (B, A) (as $(x - z)^{q-1} = (-1)^{q-1}(z - x)^{q-1}$, and a sign does not change the ideal), and $(\xi, \eta) \mapsto (\eta, \xi)$ exchanges λ_+ and λ_- . A relabelling of A or B changes each product by a sign and preserves $|Z_\Lambda|$. So we may assume $\alpha \geq 1$ and peel any x -variable. **Step:** by Lemma 7.1(iii), Proposition 7.5, the induction hypothesis (each Λ_i is a down-set of $\text{BPar}_q(\alpha - 1, \beta)$ by Proposition 7.4), §7.3 and Lemma 7.1(iv),

$$\dim V_\Lambda = \sum_{i=0}^{q-1} \dim W_{q-1-i}(V_\Lambda) \geq \sum_{i=0}^{q-1} \dim V_{\Lambda_i} \geq \sum_{i=0}^{q-1} |Z_{\Lambda_i}| = \sum_{i=0}^{q-1} |Z_{>i}| = |Z_\Lambda|. \quad \blacksquare$$

Proof of Theorem C. Lemma 7.2 and Theorem 7.6. $\blacksquare$

7.7 Consequences

Corollary 7.7 (Main Theorem' and the Main Theorem, odd degrees). *For odd $m \geq 3$, Main Theorem' holds, and Conjecture 1.2 of [DS] holds in every even dimension.*

Proof. Let m be odd and $k \geq 1$. For every prime $p|m$, $\dim_{F_p} F_p[G]/(\bar{\psi}_J : J \in \mathcal{J}) = m^{n+1} - |\Gamma_{\mathcal{J}}|$: for $m = p^v$ by Corollary 5.4 and Proposition 2.5; otherwise by Proposition 6.9, whose hypothesis is Theorem C over $F = \bar{F}_p$, $q = p^v$. For $p \nmid m$ the same equality is Theorem 0(b) with $K_p = \bar{F}_p$. The rank of $R/(\psi_J : J \in \mathcal{J})$ is $m^{n+1} - |\Gamma_{\mathcal{J}}|$ (Theorem 0(b) with $p = 0$), and $|\Gamma_{\mathcal{J}}| = Q_k(m)$ (Lemma 2.2, valid for odd m); so $R/(\psi_J : J \in \mathcal{J})$ has no torsion, which is Main Theorem'. No step of this uses topology. With Theorem 0(a) (Proposition 2.1) it gives the Main Theorem; for $k = 0$ the Main Theorem is trivial. $\blacksquare$

Corollary 7.8 (equality over $\bar{F}_p$). *Let $q = p^v$ with p odd. Then $\dim_{\bar{F}_p} I_a^{\text{bal}} = N_{\text{bal}}(a, q)$ and $\dim_{\bar{F}_p} I_a^{\text{ph}} = N_{\text{ph}}(a, q)$ for every $a \geq 0$. (For $p = 2$ see Corollary 9.12.)*

Proof. For $a = 0$, $I_0^{\text{bal}} = F$ and $I_0^{\text{ph}} = F[x_1]/(x_1^q)$ have dimensions $1 = N_{\text{bal}}(0, q)$ and $q = N_{\text{ph}}(0, q)$. Let $a \geq 1$, choose an odd prime $r \neq p$ and put $m := qr$ and $n := 2a$, so that $k = a \geq 1$ and (6.1) applies. Colour a coordinates by a primitive r -th root ζ , a coordinates by ζ^{-1} , and one coordinate s by 1; then $c_0 = 1$, the block $\mathcal{C}_1 = \{0, s\}$ contributes $\dim I_{c,1} = q - 1 = N_1(c)$, and the pair block contributes $\dim I_a^{\text{bal}}$. If $\dim I_a^{\text{bal}} > N_{\text{bal}}(a, q)$, this colouring has $\dim \pi_c(I) > N_1(c) \cdot N_{\text{bal}}(a, q)$, while every other compatible colouring has $\dim \pi_c(I) \leq N_1(c) \cdot \prod_{\zeta} N_{\zeta}(c)$ (Proposition 6.5, Lemmas 6.6 and 6.7, and Theorem C for every $a \leq n$). Summing, $\dim_F I > |\Gamma_{\mathcal{J}}|$ by Lemma 6.8, contradicting (6.1). For I_a^{ph} , take $n := 2a$, colour $a + 1$ coordinates by ζ and a coordinates by ζ^{-1} ; then $c_0 = \zeta^{-1}$, $\mathcal{C}_1 = \emptyset$, and the only block is I_a^{ph} . $\blacksquare$

Remarks 7.9. (1) Corollary 7.8 is an algebraic statement with an algebraic proof: the upper bound (6.1) is Theorem 0(b), a Chinese-remainder count. The proof is global, through the sum over the colourings of $F[G]$; we do not know a direct proof of $\leq$ on one block: the evaluation argument of Theorem 5.9 fails, because $(x - z)^{q-1}$ vanishes at $x = z$ rather than off it. (2) In characteristic 0 the inequalities of Theorem C are strict in general: $\dim_Q((x - z)^2) = 4 > 3 = N_{\text{bal}}(1, 3)$ in $Q[x, z]/(x^3, z^3)$, and $\dim_Q I_2^{\text{bal}} = 24 > 15$ at $q = 3$ (§14). So, unlike Theorem 5.9', in these cells (where Corollary 7.8 gives $\dim_{F_3} I_a^{\text{bal}} = N_{\text{bal}}(a, 3) < \dim_Q I_a^{\text{bal}}$) the quotient of the integral box ring by the bipartite ideal has 3-torsion: the bipartite ideals are genuinely of characteristic p . (3) By Lemma 7.2(iii) the phantom and balanced counts are related. On the ideal side, if $\sigma \in S_{a+1}$ and $i_0 := \sigma^{-1}(a + 1)$, the generator $\prod_i (x_i - z_{\sigma(i)})^{q-1}$ of I_{a+1}^{bal} has z_{a+1} -degree $q - 1$, with top coefficient the generator of I_a^{ph} indexed by (i_0, σ) , so the top slice $W_{q-1}(I_{a+1}^{\text{bal}})$ (peeling z_{a+1} , that is, Lemma 7.1 with the names x and z exchanged, as in the symmetry step of Theorem 7.6) contains I_a^{ph} . With Corollary 7.8, $W_j(I_{a+1}^{\text{bal}}) = 0$ for $j < q - 1$, and $f \mapsto [z_{a+1}^{q-1}]f$ is an isomorphism of graded vector spaces $I_{a+1}^{\text{bal}} \rightarrow I_a^{\text{ph}}$ of degree $-(q - 1)$ over $\bar{F}_p$.

8. The odd box: Theorem O

Theorem B is a count at the **even** box $q - 1$, on a grid without zero. The even degrees need the same count at an **odd** box, on a grid with one zero. This is problem 7 of version 10 of this paper; this section proves it. Throughout the section, $r = 2h + 1 \geq 3$ is odd, F is an arbitrary field, and

$$C_m := F[y_1, \dots, y_m] / (y_1^r, \dots, y_m^r)$$

(in this section the box is r ; in §5 the ring C_m had the box $q - 1$). T is a set of r elements with an involution $u \mapsto -u$ that has exactly one fixed point, written 0; so $T \setminus \{0\}$ consists of h classes $\{u, -u\}$. As in §5, the field carries the ideals and T carries the point sets, and the two are compared only through dimensions and cardinalities. Put

$$D(a, b) := \sum_{u=0}^{r-1} (-1)^u a^u b^{r-1-u},$$

$$D^-(a, b) := \sum_{u=0}^{r-2} (-1)^u a^u b^{r-2-u},$$

two polynomials with integer coefficients: D is the D_r of Proposition 10.5, and D^- is the D of §2.3 for the odd number $q = r$. For a matching $J \in \mathcal{J}$, $D_J := \prod D(y_a, y_b)$, the product over the k pairs of J that avoid 0; and, as in §10,

$$N_r(n) := n! \cdot [x^n] e^x \cdot I_0(2x)^h,$$

the number of n -tuples in T in which, for every class $\{u, -u\}$, the values u and $-u$ occur equally often (the zeros are free). For even n the number of zeros of such a tuple is even, and e^x may be replaced by $\cosh x$.

THEOREM O (the odd box). *For every field F , every odd $r \geq 3$ and every $k \geq 0$,*

$$\dim_F(D_J : J \in \mathcal{J}) \cdot C_{2k+1} = N_r(2k + 2).$$

Moreover the quotient of $Z[y_1, \dots, y_{2k+1}] / (y_i^r)$ by the ideal generated by the D_J is a free abelian group, and the dimension of each graded piece of $(D_J : J \in \mathcal{J})C_{2k+1}$ does not depend on F .

For $k = 0$ the ideal is the whole ring $F[y_1] / (y_1^r)$, of dimension $r = N_r(2)$. The inequality $\geq$ is the root case of Theorem 8.11 below, a statement about a family of ideals indexed by «interlaced pairs» of down-sets, proved by peeling one variable as in §5. The inequality $\leq$ is elementary (Corollary 8.13). The plan is that of §5, with two changes. First, a point may have one unpaired **zero**, so a shape is a partition together with a mark $\delta \in \{0, 1\}$, and the down-sets of §5 become pairs of down-sets that must be interlaced. Second, the generators attached to a marked shape are not products of divided differences and Vandermonde determinants any more: one of their factors is a **bordered Pfaffian**, and the place of Lemma 5.7(ii) is taken, in one of the seven cases, by a membership lemma (Lemma 8.7), which is proved by a rank-two update of bordered Pfaffians (§8.5).

8.1 Elementary identities and peeling

In $Z[a, b]$:

- **(8.1)** $D(b, a) = D(a, b)$ and $D^-(b, a) = -D^-(a, b)$ (substitute $w = r - 1 - u$, respectively $w = r - 2 - u$; $r - 1$ is even and $r - 2$ is odd).
- **(8.2)** $D(a, b) = b^{r-1} - a \cdot D^-(a, b)$. (Indeed $-a \cdot D^-(a, b) = \sum_{w=1}^{r-1} (-1)^w a^w b^{r-1-w}$.)
- **(8.3)** $(a + b) \cdot D(a, b) = a^r + b^r$ and $(a + b) \cdot D^-(a, b) = b^{r-1} - a^{r-1}$ (telescoping).
- **(8.4)** For $0 \leq u \leq r - 1$, the coefficient of a^{r-1-u} in $D(a, b)$ is $(-1)^u b^u$. For $0 \leq u \leq r - 2$, the coefficient of a^{r-2-u} in $D^-(a, b)$ is $-(-1)^u b^u$.

For a set P of pairwise disjoint pairs of indices, $D_P := \prod_{(a,b) \in P} D(y_a, y_b)$; by (8.1) it does not depend on the order inside the pairs. For a finite set S of indices, $\Delta(S)$ is the Vandermonde determinant of §5.2 ($\Delta(\emptyset) = \Delta(\{s\}) = 1$).

Peeling. Write $C_m = C_{m-1}[y_1]/(y_1^r)$, with C_{m-1} in the variables $y_2, \dots, y_m$. For an ideal $V \subseteq C_m$ and $0 \leq j \leq r - 1$ put $W_j(V) := \{[y_1^j]f : f \in V, \deg_{y_1} f \leq j\}$. By Lemma 7.1 (with one set of variables, the box r and $\Omega = T$): $W_j(V)$ is an ideal of C_{m-1} , $W_j(V) \subseteq W_{j+1}(V)$, $\dim V = \sum_{j=0}^{r-1} \dim W_j(V)$, and for $Z \subseteq T^m$, with $Z_{>i}$ the set of the tails $M' \in T^{m-1}$ that have more than i completions in Z , $|Z| = \sum_{i=0}^{r-1} |Z_{>i}|$.

8.2 Points: shapes, interlaced pairs, layers

Shapes. Let $\mathcal{P}_n := \text{Par}_n^{(h)}$, the set of partitions λ with at most h parts, $|\lambda| \leq n$ and $|\lambda| \equiv n \pmod{2}$ (§5.2; $\mathcal{P}_n = \emptyset$ for $n < 0$). For $M \in T^m$: in each class with multiplicities $a, \bar{a}$ keep the number $|a - \bar{a}|$; $\lambda(M)$ is the partition formed by the non-zero ones, and $\delta(M) \in \{0, 1\}$ is the parity of the number of entries of M equal to 0. The **shape** of M is $(\lambda(M), \delta(M))$. Since m is twice the number of disjoint pairs $\{u, -u\}$, $\{0, 0\}$ of M plus $|\lambda(M)| + \delta(M)$, the shape lies in

$$\text{Sh}_m := \{(\lambda, 0) : \lambda \in \mathcal{P}_m\} \cup \{(\lambda, 1) : \lambda \in \mathcal{P}_{m-1}\}.$$

We call δ the **mark**; a shape $(\lambda, 1)$ is **marked**. $\preceq, \lambda - e_j, \lambda + e_j, \lambda \sqcup 1$ and $\ell = \ell(\lambda)$ are as in §5.2 and §5.4. A row of a partition is a labelled part: lowering or raising two different rows commutes, so $(\lambda - e_i) - e_j = (\lambda - e_j) - e_i$, and so on, as partitions.

Lemma 8.1 (options; this is (P1)). *Let $M' \in T^{m-1}$ have shape (μ, δ) , $\ell = \ell(\mu)$, with residual values $u_1, \dots, u_\ell$ (u_j of multiplicity μ_j). The r values $y \in T$ give the following shapes of (y, M') :*

- $y = -u_j$: $(\mu - e_j, \delta)$; $y = u_j$: $(\mu + e_j, \delta)$ ($j = 1, \dots, \ell$);
- $y \neq 0$ in one of the $h - \ell$ classes absent from the residue: $(\mu \sqcup 1, \delta)$ ($2(h - \ell) = r - 1 - 2\ell$ values);
- $y = 0$: $(\mu, 1 - \delta)$.

All of them lie in Sh_m .

Proof. For $y \neq 0$ this is §5.4; a new zero changes the parity of the number of zeros and nothing else. The count is $2\ell + 2(h - \ell) + 1 = r$. For the last sentence: if $\delta = 0$ then $\mu \in \mathcal{P}_{m-1}$, so $\mu \pm e_j, \mu \sqcup 1 \in \mathcal{P}_m$ (the last one exists only if $\ell < h$) and $(\mu, 1) \in \text{Sh}_m$; if $\delta = 1$ then $\mu \in \mathcal{P}_{m-2}$, so $\mu \pm e_j, \mu \sqcup 1 \in \mathcal{P}_{m-1}$ and $\mu \in \mathcal{P}_m$. ■

For $\Lambda \subseteq \text{Sh}_m$ put $\Lambda^0 := \{\lambda : (\lambda, 0) \in \Lambda\} \subseteq \mathcal{P}_m$, $\Lambda^1 := \{\lambda : (\lambda, 1) \in \Lambda\} \subseteq \mathcal{P}_{m-1}$ and $Z_\Lambda := \{M \in T^m : \text{the shape of } M \text{ lies in } \Lambda\}$. For $\sigma = (\mu, \delta) \in \text{Sh}_{m-1}$ let $F_\Lambda(\sigma)$ be the number of $y \in T$ such that the shape of (y, M') lies in Λ , for any M' of shape σ ; it is well defined by Lemma 8.1, and

$$F_\Lambda(\mu, \delta) = F_{\Lambda^\delta}^*(\mu) + [\mu \in \Lambda^{1-\delta}], \quad (8.5)$$

$$F_{\Lambda'}^*(\mu) := \#\{j : \mu - e_j \in \Lambda'\} + \#\{j : \mu + e_j \in \Lambda'\} + (r - 1 - 2\ell) \cdot [\mu \sqcup 1 \in \Lambda'].$$

Here $F_{\Lambda'}^*$ is exactly the function $F_{\Lambda'}$ of §5.4 for the odd number $q = r$ (there T has $q - 1 = r - 1$ elements and h classes).

Definition 8.2. $\Lambda \subseteq \text{Sh}_m$ is an *interlaced pair* if

- (D1) Λ^0 is a $\preceq$ -down-set of $\mathcal{P}_m$ and Λ^1 is a $\preceq$ -down-set of $\mathcal{P}_{m-1}$;
- (D2) if $(\nu, \delta) \in \Lambda$ and $1 \leq j \leq \ell(\nu)$, then $(\nu - e_j, 1 - \delta) \in \Lambda$.

($(\nu - e_j, 1 - \delta)$ is a shape of level m : its size has the required parity.) In words: removing one box from a shape of Λ and switching the mark stays in Λ . On points, (D2) says: replacing one unpaired non-zero value by 0 stays in Z_Λ .

Lemma 8.3 (chain). Let Λ be an interlaced pair of level m and $(\mu, \delta) \in \text{Sh}_{m-1}$, $\ell = \ell(\mu)$. List the r options of Lemma 8.1 as

$$(\mu - e_1, \delta), \dots, (\mu - e_\ell, \delta); \quad (\mu, 1 - \delta); \quad (\mu \sqcup 1, \delta)[r - 1 - 2\ell \text{ times}]; \quad (\mu + e_\ell, \delta), \dots, (\mu + e_1, \delta).$$

Then the options lying in Λ form an initial segment of this list, of length $F_\Lambda(\mu, \delta)$.

Proof. Among the removals, among the additions, and from the middle option to the additions, this is Lemma 5.5 applied to the down-set Λ^δ : $\mu - e_j \preceq \mu - e_{j+1}$, $\mu \sqcup 1 \preceq \mu + e_\ell$ and $\mu + e_{j+1} \preceq \mu + e_j$. If $(\mu, 1 - \delta) \in \Lambda$, then by (D2) every $(\mu - e_j, \delta) \in \Lambda$. If $(\mu \sqcup 1, \delta) \in \Lambda$, then by (D2), removing the new row, $(\mu, 1 - \delta) \in \Lambda$. If $(\mu + e_j, \delta) \in \Lambda$, then by (D2), removing the box just added, $(\mu, 1 - \delta) \in \Lambda$. ■

As in §5.5, rows of equal length give equal options. So the removals in Λ are those of the rows $1, \dots, \rho$, where $\rho = 0$ or ρ is the last row of its length, and the additions in Λ are those of the rows $j_0, \dots, \ell$, where j_0 is the first row of its length.

Lemma 8.4 (layers; this is (P2)). Let Λ be an interlaced pair of level $m \geq 1$, and for $0 \leq i \leq r - 1$ let $\Lambda_i := \{\sigma \in \text{Sh}_{m-1} : F_\Lambda(\sigma) > i\}$. Then Λ_i is an interlaced pair of level $m - 1$, and $(Z_\Lambda)_{>i} = Z_{\Lambda_i}$.

Proof. The last assertion is Lemma 8.1.

(D1). Let $\mu \preceq \tilde{\mu}$ in $\mathcal{P}_{m-1}$. By Proposition 5.6 (for $q = r$, the down-set $\Lambda^0 \subseteq \text{Par}_m^{(h)}$, tails in $\text{Par}_{m-1}^{(h)}$), $F_{\Lambda^0}^*(\mu) \geq F_{\Lambda^0}^*(\tilde{\mu})$; and $[\mu \in \Lambda^1] \geq [\tilde{\mu} \in \Lambda^1]$ because Λ^1 is a down-set of $\mathcal{P}_{m-1}$. By (8.5), $F_\Lambda(\mu, 0) \geq F_\Lambda(\tilde{\mu}, 0)$. In the same way, for $\mu \preceq \tilde{\mu}$ in $\mathcal{P}_{m-2}$: Proposition 5.6 for the down-set $\Lambda^1 \subseteq \text{Par}_{m-1}^{(h)}$, with tails in $\text{Par}_{m-2}^{(h)}$, gives $F_{\Lambda^1}^*(\mu) \geq F_{\Lambda^1}^*(\tilde{\mu})$, and $[\mu \in \Lambda^0] \geq [\tilde{\mu} \in \Lambda^0]$ because $\mathcal{P}_{m-2} \subseteq \mathcal{P}_m$ and Λ^0 is a down-set of $\mathcal{P}_m$; so $F_\Lambda(\mu, 1) \geq F_\Lambda(\tilde{\mu}, 1)$. Hence both components of Λ_i are down-sets.

(D2). Let $(\nu, \delta) \in \text{Sh}_{m-1}$, $1 \leq j \leq \ell := \ell(\nu)$, $\nu' := \nu - e_j$, and write $A := \Lambda^\delta$, $A' := \Lambda^{1-\delta}$. We must show $F_\Lambda(\nu', 1 - \delta) \geq F_\Lambda(\nu, \delta)$, that is, by (8.5),

$$F_{A'}^*(\nu') + [\nu' \in A] \geq F_A^*(\nu) + [\nu \in A'].$$

By (D2) for Λ : if a partition κ lies in A , then κ minus a box in any of its rows lies in A' ; and symmetrically with A and A' exchanged.

Case $\nu_j \geq 2$. The rows of ν' are the rows of ν , with the same labels. If $\nu - e_i \in A$, lower the row j (it is still non-empty, also when $i = j$): $(\nu - e_i) - e_j = \nu' - e_i \in A'$. If $\nu + e_i \in A$, lower the row j : $(\nu + e_i) - e_j = \nu' + e_i \in A'$. If $\nu \sqcup 1 \in A$, lower the row j : $\nu' \sqcup 1 \in A'$; and $\ell(\nu') = \ell$, so the middle options of ν and ν' have the same multiplicity. So $F_{A'}^*(\nu') \geq F_A^*(\nu)$. Finally $\nu \in A'$ implies $\nu' = \nu - e_j \in A$.

Case $\nu_j = 1$. Then ν' has the rows of ν other than j , $\ell(\nu') = \ell - 1$, and $\nu' \sqcup 1 = \nu$. For $i \neq j$: $\nu - e_i \in A$ implies $\nu' - e_i \in A'$, and $\nu + e_i \in A$ implies $\nu' + e_i \in A'$, as before. The removal of the row j of ν is ν' , and $[\nu - e_j \in A] = [\nu' \in A]$. What remains on the right is $(r - 1 - 2\ell)[\nu \sqcup 1 \in A] + [\nu + e_j \in A] + [\nu \in A']$, and what remains on the left is the middle term of ν' , namely $(r - 1 - 2(\ell - 1))[\nu' \sqcup 1 \in A'] = (r + 1 - 2\ell)[\nu \in A']$. If $\nu \in A'$, the right-hand remainder is at most $(r - 1 - 2\ell) + 1 + 1$. If $\nu \notin A'$, it is 0: $\nu \sqcup 1 \in A$ would give, removing the new row, $\nu \in A'$; and $\nu + e_j \in A$ would give, removing the box just added, $\nu \in A'$. ■

Lemma 8.5 (the root; the only place where the full family enters). *For $m = 2k + 1$, $\Lambda_{\text{root}} := \{((1), 0), (\emptyset, 1)\}$ is an interlaced pair, and $|Z_{\Lambda_{\text{root}}}| = N_r(2k + 2)$. For $m = 2k + 2$, $\{(\emptyset, 0)\}$ is an interlaced pair, and $|Z_{\{(\emptyset, 0)\}}| = N_r(2k + 2)$.*

Proof. $\{(1)\}$ is a down-set of $\mathcal{P}_{2k+1}$ (Lemma 5.2), $\{\emptyset\}$ is a down-set of $\mathcal{P}_{2k}$ and of $\mathcal{P}_{2k+2}$, and $(1) - e_1 = \emptyset$. $Z_{\Lambda_{\text{root}}}$ is the set of the $(2k + 1)$ -tuples with exactly one unpaired value, zero or not. Appending the opposite of that value is a bijection onto the set of the $(2k + 2)$ -tuples that split into pairs $\{u, -u\}$ and $\{0, 0\}$: the inverse deletes the last entry. The latter set is $Z_{\{(\emptyset, 0)\}}$ at level $2k + 2$, and it has $N_r(2k + 2)$ elements. ■

8.3 Bordered Pfaffians

Let $A = (a_{xy})$ be an alternating matrix ($a_{xx} = 0$, $a_{yx} = -a_{xy}$) over a commutative ring, indexed by a totally ordered finite set X , and write $p_x \in \{0, 1, 2, \dots\}$ for the position of $x \in X$, counted from 0. The **Pfaffian** of A is $\text{Pf}(A) := \sum_{\pi} \text{sgn}(\pi) \cdot \prod_{\{x < y\} \in \pi} a_{xy}$, the sum over the perfect matchings π of X , where $\text{sgn}(\pi)$ is the sign of the permutation that lists the pairs of π one after the other, each pair in increasing order (it does not depend on the order of the pairs, and it is (-1) to the number of crossings of π). So $\text{Pf}(A) = 1$ for $X = \emptyset$ and $\text{Pf}(A) = 0$ for $|X|$ odd. Three properties follow from the definition ([Knu, (0.1)], [Oka, (2.1)]); (i) and (iii) are classical [Knu, (0.4), (2.0)], [Oka, (2.3), (2.4)], and (ii), for two distinct indices with equal rows, is proved below in every commutative ring:

- (i) a simultaneous permutation of rows and columns multiplies Pf by the sign of the permutation;
- (ii) if two indices $x \neq x'$ have equal rows, then $\text{Pf}(A) = 0$: exchanging x and x' is an involution of the matchings that do not pair them, which changes the sign and keeps the product, and a matching that pairs them has the factor $a_{xx'} = a_{x'x'} = 0$;
- (iii) for a fixed index x , $\text{Pf}(A) = \sum_{z \neq x} \varepsilon(x, z) \cdot a_{xz} \cdot \text{Pf}(A^{x,z})$, where $A^{x,z}$ is A without the indices x, z , and $\varepsilon(x, z) = (-1)^{p_x + p_z + 1}$ if $x < z$, $\varepsilon(x, z) = (-1)^{p_x + p_z}$ if $z < x$. In particular Pf is additive in the row-and-column of x .

None of them needs a division or a hypothesis on 2-torsion: they hold over every commutative ring, characteristic 2 included. All the rings below are polynomial rings over Z and their quotients, and the identities are proved there and then reduced to any field.

Definition. *Let a be an alternating matrix indexed by a finite ordered set N of n indices, and $c = (c_1, \dots, c_s)$ a list of «border columns», each a function from N to the ring. $\text{Pf}(a; c)$ is the*

Pfaffian of the alternating matrix indexed by $N \sqcup \{1, \dots, s\}$ (first N , then the borders) whose block on N is a , whose entry in the row of $i \in N$ and the column of the border k is $c_k(i)$, and whose block on the borders is 0. For a set N of indices of variables, $a_N := (D^-(y_i, y_j))_{i,j \in N}$ (alternating, by (8.1)), $\text{Pf}(N; c) := \text{Pf}(a_N; c)$, and, for a finite set $E = \{e_1 < \dots < e_s\}$ of exponents, $\text{Pf}_E(N) := \text{Pf}(N; y^{e_1}, \dots, y^{e_s})$, where y^e is the column $i \mapsto y_i^e$.

In (F1)–(F7), $n = |N|$, s is the number of borders, and $a^{(b)}$ is a without the index b , the columns being restricted to $N \setminus b$.

- (F1) $\text{Pf}(a; c)$ changes sign under a transposition of two indices of N together with the corresponding entries of the borders, and under a transposition of two border columns (by (i)).
- (F2) $\text{Pf}(a; c)$ is additive and homogeneous in each border column, and it vanishes if two border columns are equal (by (iii) and (ii)). Expanding along the last border: $\text{Pf}(a; c_1, \dots, c_s) = \sum_{b \in N} \eta_b \cdot c_s(b) \cdot \text{Pf}(a^{(b)}; c_1, \dots, c_{s-1})$ with $\eta_b := (-1)^{n+s+p_b}$.
- (F3) If $n = s$, then $\text{Pf}(a; c) = (-1)^{s(s-1)/2} \cdot \det(c_k(i))_{i \in N, k \leq s}$ (rows indexed by N in its order); it does not depend on a . In particular $\text{Pf}_{\{0,1,\dots,s-1\}}(N) = (-1)^{s(s-1)/2} \cdot \Delta(N)$ for $|N| = s$. (A matching with a non-zero product pairs every border with an element of N , so it is a bijection from N to the borders.)
- (F4) *Expansion along an index $x \in N$.* Split the row-and-column of x into its entries against $N \setminus x$ and its entries against the borders. By (iii),

$$\text{Pf}(a; c) = \vartheta \cdot \text{Pf}(a^{(x)}; c, a_x) + \sum_{k=1}^s (-1)^{p_x+n+k} \cdot c_k(x) \cdot \text{Pf}(a^{(x)}; c \text{ without } c_k),$$

$$\vartheta := (-1)^{p_x+n+s},$$

where a_x is the border column $b \mapsto a_{xb}$ on $N \setminus x$; for $a = a_N$ it is $D^-(y_x, \cdot)$, the column $b \mapsto D^-(y_x, y_b)$. (In the first part, x is moved to the last place and becomes a border.)

- (F5) By (8.4) and (F2), for a set E of exponents:

$$\text{Pf}(N'; y^E, D^-(y_x, \cdot)) = - \sum_{u=0}^{r-2} (-1)^u y_x^{r-2-u} \cdot \text{Pf}(N'; y^E, y^u),$$

$$\text{Pf}(N'; y^E, D(y_x, \cdot)) = \sum_{u=0}^{r-1} (-1)^u y_x^{r-1-u} \cdot \text{Pf}(N'; y^E, y^u),$$

and $\text{Pf}(N'; y^E, y^u) = 0$ if $u \in E$, while it is $(-1)^{\#\{e \in E: e > u\}} \cdot \text{Pf}_{E \cup \{u\}}(N')$ if $u \notin E$. By (8.2), $\text{Pf}(N'; y^E, D(y_x, \cdot)) = \text{Pf}(N'; y^E, y^{r-1}) - y_x \cdot \text{Pf}(N'; y^E, D^-(y_x, \cdot))$.

- (F6) (Lemma 5.7(ii).) For $S = \{b_1 < \dots < b_\rho\}$ and $\varepsilon_{b_c} := (-1)^{\rho+c}$: $\sum_{b \in S} \varepsilon_b \Delta(S \setminus b) y_b^u$ is 0 for $0 \leq u \leq \rho - 2$ and $\Delta(S)$ for $u = \rho - 1$.
- (F7) *Laplace.* For an alternating matrix a on N and $n = s + 2\kappa$,

$$\text{Pf}(a; c) = (-1)^{s(s-1)/2} \cdot \sum_{S \subseteq N, |S|=s} \text{sgn}(S) \cdot \det(c_k(i))_{i \in S, k \leq s} \cdot \text{Pf}(a|_{N \setminus S}),$$

where $\text{sgn}(S) = (-1)^{\sum_{i \in S} p_i - s(s-1)/2}$ is the sign of the shuffle that puts S before $N \setminus S$, and $a|_{N \setminus S}$ is the restriction of a . This is the case of [Oka, Proposition 2.3] in which the block on the borders is 0. (A matching with a non-zero product consists of a bijection from a subset S of N onto the borders and of a perfect matching of $N \setminus S$.)

The signs in (iii) and (F2)–(F7) are those of the Lean proof (§14.8); only their form matters below, except where the text says otherwise.

8.4 Patterns and the ideals V_Λ

For a partition λ , λ'_c is the length of its c -th column ($\lambda'_1 = \ell(\lambda)$). For $\ell \geq 0$ put

$E_0 := \{r-1\}$, $E_\ell := \{0, 1, \dots, \ell-2\}$ for $\ell \geq 1$ (so $E_1 = \emptyset$).

Definition 8.6 (patterns). Let I be a set of m indices and $(\lambda, \delta) \in \text{Sh}_m$, $\ell = \ell(\lambda)$.

- $\delta = 0$: a pattern consists of a set P of $(m - |\lambda|)/2$ pairwise disjoint pairs of I and of pairwise disjoint blocks $B_1, \dots, B_{\lambda_1}$ with $|B_c| = \lambda'_c$ covering the rest. Its **product** is $D_P \cdot \prod_c \Delta(B_c)$. (These are the tight patterns of §5.2, with D in the place of the divided difference of §2.3.)
- $\delta = 1$: a pattern consists of a set P of pairwise disjoint pairs, of pairwise disjoint blocks $B_2, \dots, B_{\lambda_1}$ with $|B_c| = \lambda'_c$, and of a **marked block** B_0 with $|B_0| = \ell + 1 + 2t$ for some $t \geq 0$, which together partition I . Its product is $D_P \cdot \text{Pf}_{E_\ell}(B_0) \cdot \prod_{c \geq 2} \Delta(B_c)$.

On the side of the points, the marked block carries the unpaired zero, the ℓ values of the first column of λ , and t «absorbed» pairs. (Some of these products are 0, by §8.5, Remark (2); this does no harm.) The sizes are consistent: a pattern of $(\lambda, 1)$ uses $2|P| + (|\lambda| - \ell) + (\ell + 1 + 2t)$ indices, so $|P| + t = (m - 1 - |\lambda|)/2$, an integer because $\lambda \in \mathcal{P}_{m-1}$; and the matrix of $\text{Pf}_{E_\ell}(B_0)$ has $(\ell + 1 + 2t) + |E_\ell|$ indices, an even number in both cases.

For $\Lambda \subseteq \text{Sh}_m$, $V_\Lambda \subseteq C_m$ is the ideal generated by the products of all the patterns on $\{1, \dots, m\}$ of all the shapes of Λ . All these products have integer coefficients. A permutation of the indices maps every product to $\pm$ a product of a pattern of the same shape (by (8.1), (F1) and the antisymmetry of Δ), so V_Λ is stable under relabelling.

Examples. $(\emptyset, 1)$ on one index: y^{r-1} . $(\emptyset, 1)$ on three indices: $y_c^{r-1} D(y_a, y_b)$ ($t = 0$) and $\text{Pf}_{\{r-1\}}(\{1, 2, 3\}) = \pm(y_3^{r-1} D^-(y_1, y_2) - y_2^{r-1} D^-(y_1, y_3) + y_1^{r-1} D^-(y_2, y_3))$ ($t = 1$). $((1), 1)$ on two indices: $D^-(y_1, y_2)$. $((1, 1), 1)$ on three indices: $\pm(D^-(y_1, y_2) - D^-(y_1, y_3) + D^-(y_2, y_3))$.

8.5 The membership lemma

Lemma 8.7. Let $\ell \geq 0$, $t \geq 0$, and let B_0 be a set of $\ell + 1 + 2t$ indices. In $Z[y_i : i \in B_0]/(y_i^r)$,

$$\text{Pf}_{E_\ell}(B_0) \in \mathfrak{U}_\ell(B_0) := (\Delta(S) \cdot D_Q : S \subseteq B_0, |S| = \ell + 1, Q \text{ a perfect matching of } B_0 \setminus S).$$

We prove a more general statement, in which the borders are arbitrary powers. For a finite set N of indices, $\mathfrak{U}_\ell(N)$ is defined in the same way, with $|S| = \ell + 1$.

Lemma 8.7' (the membership lemma, any exponents). Let N be a set of n indices, $t \geq 0$, and $e_1, \dots, e_s \geq 0$ any exponents. In $Z[y_i : i \in N]/(y_i^r)$:

- (a) if $n = s + 2(t + 1)$, then $\text{Pf}(N; y^{e_1}, \dots, y^{e_s}) \in \mathfrak{U}_{s+1}(N)$;
- (b) if $n = s + 1 + 2t$, then $\text{Pf}(N; y^{e_1}, \dots, y^{e_s}, y^{r-1}) \in \mathfrak{U}_s(N)$.

Lemma 8.7 is the case $s = \ell - 1$, $(e_1, \dots, e_s) = (0, 1, \dots, \ell - 2)$ of (a) for $\ell \geq 1$, and the case $s = 0$ of (b) for $\ell = 0$. The proof takes the rest of this subsection; the symbols ω_s , Ev , Od , W_σ , H and the variable ζ are local to it.

(a) Three polynomials. For odd s , $1 \leq s \leq 2r - 3$, put $\omega_s(a, b) := \sum (-1)^u a^u b^{s-u}$, the sum over the u with $0 \leq u \leq r - 1$ and $0 \leq s - u \leq r - 1$. The set of these u is stable under $u \mapsto s - u$, which exchanges the terms of $\omega_s(a, b)$ and of $\omega_s(b, a)$ and changes the sign $(-1)^u$, because s is odd; so $\omega_s(b, a) = -\omega_s(a, b)$, and $\omega_s(a, a) = 0$ (the terms u and $s - u \neq u$ cancel; no division by 2 is involved).

- $\omega_{r-2} = D^-$ (for $s = r - 2$ the conditions are $0 \leq u \leq r - 2$).
- For odd i , $1 \leq i \leq r - 2$: $\omega_{r-1+i}(a, b) = b^i \cdot D(a, b)$ modulo (a^r, b^r) . (In $b^i D(a, b) = \sum_u (-1)^u a^u b^{r-1-u+i}$ the terms with $u < i$ have b -exponent at least r ; the others are the terms of ω_{r-1+i} .)
- In $Z[a, b][\zeta]$, with $\text{Ev}(a) := \sum_{\alpha=0}^h \zeta^\alpha a^{2\alpha}$ and $\text{Od}(a) := \sum_{\beta=0}^{h-1} \zeta^\beta a^{2\beta+1}$:

$$\sum_{\sigma=0}^{2h-1} \zeta^\sigma \omega_{2\sigma+1}(a, b) = \text{Ev}(a) \cdot \text{Od}(b) - \text{Ev}(b) \cdot \text{Od}(a). \quad (8.6)$$

Indeed, in $\omega_{2\sigma+1}(a, b)$ the terms with $u = 2\alpha$ even have b -exponent $2\beta + 1$ with $\alpha + \beta = \sigma$, and the sign $+$; the terms with $u = 2\beta + 1$ odd have b -exponent 2α , and the sign $-$. Every pair (α, β) with $0 \leq \alpha \leq h$, $0 \leq \beta \leq h - 1$ occurs exactly once, with $\sigma = \alpha + \beta$.

So the matrix $(\sum_{\sigma} \zeta^\sigma \omega_{2\sigma+1}(y_i, y_j))_{i,j}$ has rank two: it is $\text{Ev} \cdot \text{Od}^T - \text{Od} \cdot \text{Ev}^T$ for the columns $\text{Ev} = (\text{Ev}(y_i))_i$ and $\text{Od} = (\text{Od}(y_i))_i$. This is the one fact behind the lemma.

Lemma 8.8 (two operations on bordered Pfaffians). *Let a be an alternating matrix on N , $c = (c_1, \dots, c_s)$ border columns, and E, O two more columns, over a commutative ring.*

- (i) (border shift) For every function λ on N and every $k \leq s$: $\text{Pf}(a'; c) = \text{Pf}(a; c)$, where $a'_{ij} := a_{ij} + \lambda_i c_k(j) - \lambda_j c_k(i)$.
- (ii) (rank-two update) $\text{Pf}(a + E \cdot O^T - O \cdot E^T; c) = \text{Pf}(a; c) - \text{Pf}(a; c, E, O)$.

Proof. We use one elementary operation: for two indices $x \neq w$ of an alternating matrix A and an element λ , adding λ times the row of x to the row of w , and λ times the column of x to the column of w , does not change $\text{Pf}(A)$. Indeed, by the additivity of (iii) in the row-and-column of w , the Pfaffian changes by $\lambda \cdot \text{Pf}(A'')$, where A'' is A with the row and the column of w replaced by those of x (and $A''_{ww} = 0$); the rows of w and x in A'' are equal, so $\text{Pf}(A'') = 0$ by (ii).

(i) In the bordered matrix of $(a; c)$, the row of the border k is $-c_k$ on N and 0 on the borders. For each $w \in N$, add $-\lambda_w$ times the row and the column of the border k to those of w : the entry (w, j) , $j \in N$, becomes $a_{wj} + \lambda_w c_k(j)$, the entry (i, w) becomes $a_{iw} - \lambda_w c_k(i)$, and the border columns do not change. After all w the matrix is the bordered matrix of $(a'; c)$.

(ii) Let X_θ be the bordered matrix of $(a; c, E, O)$ with the entry θ in the row of the border E and the column of the border O (and $-\theta$ in the symmetric place). Expanding along the index O by (iii), the only term that contains θ is the one of $z = E$, with $\varepsilon(O, E) = -1$ (the borders E and O are the last two indices), and it is $\theta \cdot \text{Pf}(a; c)$; so $\text{Pf}(X_\theta) = \text{Pf}(a; c, E, O) + \theta \cdot \text{Pf}(a; c)$. Now take $\theta = 1$ and, for each $w \in N$, add E_w times the row and the column of O to those of w . The row of O is $-O$ on N , 0 on the borders of c and -1 at E ; so the block on N becomes $a - E \cdot O^T + O \cdot E^T$, the entry of w in the column of E becomes $E_w - E_w = 0$, and nothing else changes. Then the row of E is 0 except for the entry 1 at O ; for each $w \in N$, adding $-O_w$ times the row and the column of E to those of w clears the column of O on N . The final matrix is the bordered matrix of $(a - E \cdot O^T + O \cdot E^T; c)$ together with the block $[[0, 1], [-1, 0]]$ on the last two indices, and its Pfaffian, expanded along O , is $\text{Pf}(a - E \cdot O^T + O \cdot E^T; c)$. Hence $\text{Pf}(a - E \cdot O^T + O \cdot E^T; c) = \text{Pf}(a; c) + \text{Pf}(a; c, E, O)$; replacing O by $-O$ and using (F2) gives (ii). ■

There is no sign that depends on n or s . Two more facts follow at once from the definition of the Pfaffian as a sum over matchings, in which a matching with a non-zero product uses one entry of each border and $\kappa := (n - s)/2$ entries of a : **(homogeneity)** $\text{Pf}(\tau \cdot a; c) = \tau^\kappa \cdot \text{Pf}(a; c)$ for every scalar τ ; and **(top coefficients)** if a and c have entries in a polynomial ring $A[\zeta]$, those of a of degree at most d and those of the border c_k of degree at most d_k , then $\text{Pf}(a; c)$ has degree at most $\kappa d + \sum_k d_k$ in ζ , and its coefficient there is $\text{Pf}(a^{\text{top}}; c^{\text{top}})$, the bordered Pfaffian of the coefficients of the degrees d and d_k .

Corollary 8.9 (the closed forms). *Let A be a commutative ring, $y_i \in A$ ($i \in N$), $W_\sigma := (\omega_{2\sigma+1}(y_i, y_j))_{i,j \in N}$, $H := \sum_{\tau=0}^{h-1} \zeta^\tau W_{h+\tau}$ over $A[\zeta]$, and Ev, Od the columns of (8.6) at the y_i . For border columns $c = (c_1, \dots, c_s)$ over A :*

- (a) if $n = s + 2(t + 1)$, then $\text{Pf}(N; c) = (-1)^{t+1} \cdot [\zeta^{h-1-t}] \text{Pf}(H; c, \text{Ev}, \text{Od})$ for $t \leq h - 1$, and $\text{Pf}(N; c) = 0$ for $t \geq h$;
- (b) if $n = s + 1 + 2t$, then $\text{Pf}(N; c, y^{r-1}) = (-1)^t \cdot [\zeta^{h-t}] \text{Pf}(H; c, \text{Ev})$ for $t \leq h$, and $\text{Pf}(N; c, y^{r-1}) = 0$ for $t > h$.

Proof. Put $L := \sum_{\sigma=0}^{h-1} \zeta^\sigma W_\sigma$. By (8.6), $L + \zeta^h H = \text{Ev} \cdot \text{Od}^T - \text{Od} \cdot \text{Ev}^T$, entry by entry. The entries of L have degree at most $h - 1$ in ζ , with top coefficient $W_{h-1} = a_N$. (a) By Lemma 8.8(ii) with $a := -\zeta^h H$ and homogeneity,

$$\text{Pf}(L; c) = \text{Pf}(-\zeta^h H; c) - \text{Pf}(-\zeta^h H; c, \text{Ev}, \text{Od}) = (-\zeta^h)^{t+1} \cdot \text{Pf}(H; c) - (-\zeta^h)^t \cdot \text{Pf}(H; c, \text{Ev}, \text{Od}).$$

Take the coefficient of $\zeta^{(h-1)(t+1)}$: on the left it is $\text{Pf}(a_N; c) = \text{Pf}(N; c)$, by the top coefficients; the first term on the right is a multiple of $\zeta^{h(t+1)}$, so it contributes 0; the second contributes $(-1)^{t+1} \cdot [\zeta^{h-1-t}] \text{Pf}(H; c, \text{Ev}, \text{Od})$ if $ht \leq (h - 1)(t + 1)$, i.e. $t \leq h - 1$, and 0 otherwise. (b) By Lemma 8.8(i), applied to $a := -\zeta^h H$, the last border Ev and $\lambda := -\text{Od}$, $\text{Pf}(-\zeta^h H; c, \text{Ev}) = \text{Pf}(-\zeta^h H + \text{Ev} \cdot \text{Od}^T - \text{Od} \cdot \text{Ev}^T; c, \text{Ev}) = \text{Pf}(L; c, \text{Ev})$; and $\text{Pf}(-\zeta^h H; c, \text{Ev}) = (-\zeta^h)^t \cdot \text{Pf}(H; c, \text{Ev})$. The border Ev has degree h with top coefficient $y^{2h} = y^{r-1}$; take the coefficient of $\zeta^{(h-1)t+h}$: on the left it is $\text{Pf}(N; c, y^{r-1})$, and on the right $(-1)^t \cdot [\zeta^{h-t}] \text{Pf}(H; c, \text{Ev})$ if $t \leq h$, and 0 otherwise. $\blacksquare$

Proof of Lemma 8.7'. Work in $A := Z[y_i : i \in N]/(y_i^r)$. Since $2(h + \tau) + 1 = (r - 1) + (2\tau + 1)$, the second item of (a) gives $H_{ij} = \sum_\tau \zeta^\tau y_j^{2\tau+1} D(y_i, y_j) = D(y_i, y_j) \cdot \text{Od}(y_j)$ in $A[\zeta]$. By the definition of the Pfaffian as a sum over matchings, $\text{Pf}(H|_{N'})$ therefore lies, for every subset N' , in the ideal of $A[\zeta]$ generated by the products D_Q , Q a perfect matching of N' . (a) Expand $\text{Pf}(H; y^{e_1}, \dots, y^{e_s}, \text{Ev}, \text{Od})$ by (F7). Its $s + 2$ borders are values $P_k(y_i)$ of polynomials $P_k \in Z[\zeta][T]$ in one variable; so for each $S \subseteq N$ with $|S| = s + 2$, $\det(P_k(y_i))_{i \in S}$ is an alternating polynomial in the variables y_i , $i \in S$, and hence a multiple of $\Delta(S)$ in $Z[\zeta][y_i : i \in S]$. So every coefficient of every power of ζ in $\text{Pf}(H; y^{e_1}, \dots, y^{e_s}, \text{Ev}, \text{Od})$ is a combination of products $\Delta(S) \cdot D_Q$, with $|S| = s + 2$ and Q a perfect matching of $N \setminus S$: it lies in $\mathfrak{U}_{s+1}(N)$. By Corollary 8.9(a), so does $\text{Pf}(N; y^{e_1}, \dots, y^{e_s})$. (b) The same with the $s + 1$ borders $y^{e_1}, \dots, y^{e_s}, \text{Ev}$ and Corollary 8.9(b). $\blacksquare$

Remarks. (1) The smallest non-trivial case of Lemma 8.7, $(\ell, t) = (0, 1)$, says $y_3^{r-1} D^-(y_1, y_2) - y_2^{r-1} D^-(y_1, y_3) + y_1^{r-1} D^-(y_2, y_3) \in (D(y_1, y_2), D(y_1, y_3), D(y_2, y_3))$; for $r = 3$ it reads $\Delta(y_1, y_2, y_3) = y_1 D(y_1, y_2) - y_1 D(y_1, y_3) + y_2 D(y_2, y_3)$ modulo the cubes. (2) *Some patterns are zero.* By Corollary 8.9, $\text{Pf}_{E_\ell}(B_0) = 0$ when $\ell \geq 1$ and $\ell + t \geq h + 1$, and when $\ell = 0$ and $t > h$. For $\ell = 1$ the first condition is $t \geq h$. For $\ell \geq 2$, expand the bordered Pfaffian of Corollary 8.9(a) by multilinearity in its last two border columns: the coefficient of ζ^α in Ev is $y^{2\alpha}$ and that of ζ^β in Od is $y^{2\beta+1}$; a term in which one of them is a border y^e , $e \leq \ell - 2$, has two equal border columns and vanishes (F2), and every other term has degree at least $\lceil (\ell - 1)/2 \rceil + \lceil (\ell - 2)/2 \rceil = \ell - 1$ in ζ , which exceeds $h - 1 - t$. (The case $\ell = 2$, $t = h - 1$ was found by the cold reader of §14.6.)

These conditions are sufficient; we do not claim that they list all zero patterns. Such patterns of Definition 8.6 contribute nothing, and do no harm. (3) *The border y^{r-1} in (b) cannot in general be replaced by another power:* at $r = 5$, $n = 3$, $\text{Pf}(N; y^2)$ does not lie in $\mathfrak{U}_0(N)$ (§14.9). (In the cells tried by the cold reader, the replacement never broke the membership at $r = 3$.) (4) *Version 11* proved Lemma 8.7 in the exterior algebra on a free module with basis $v_0, \dots, v_{r-1}$, with divided powers of 2-forms, by showing that the divided powers γ_n of the generating 2-form vanish for $n \geq 2$ and by a recursion. In that language our (8.6) says that the generating function of the 2-forms of the ω_s is the product of two 1-forms, and our Lemma 8.8(ii) corresponds to the formula $\gamma_\kappa(\varphi + E \wedge O) = \gamma_\kappa(\varphi) + \gamma_{\kappa-1}(\varphi) \wedge E \wedge O$ for the divided powers γ_κ of a 2-form φ and two 1-forms E, O . The proof printed here is the one that was formalized (§14.8); it uses no exterior algebra, no divided powers and no torsion-freeness, and it proves Lemma 8.7', the statement for other border sets that problem 7(c) of version 11 asked for.

8.6 (P3) Every pattern of a layer lies in the right slice

Proposition 8.10. *Let Λ be an interlaced pair of level $m \geq 1$ and $0 \leq i \leq r - 1$. Then $V_{\Lambda_i} \subseteq W_{r-1-i}(V_\Lambda)$, where $V_{\Lambda_i} \subseteq C_{m-1}$ is built on the indices $2, \dots, m$.*

Proof. $W_{r-1-i}(V_\Lambda)$ is an ideal, so it suffices to treat a generator: let $\sigma = (\mu, \delta) \in \Lambda_i$, $\ell = \ell(\mu)$, $\Phi := F_\Lambda(\sigma) \geq i + 1$, and let G be the product of a pattern of σ on $\{2, \dots, m\}$. Since the slices are nested and $r - \Phi \leq r - 1 - i$, it is enough to find $f \in V_\Lambda$ with $\deg_{y_1} f \leq r - \Phi$ and $[y_1^{r-\Phi}]f = \pm G$, or to show otherwise that $G \in W_{r-\Phi}(V_\Lambda)$. Write $G = D_P \cdot \Delta(B_1) \cdot R$ if $\delta = 0$ and $G = D_P \cdot \text{Pf}_{E_\ell}(B_0) \cdot R$ if $\delta = 1$, where $R := \prod_{c \geq 2} \Delta(B_c)$. By Lemma 8.3 the options in Λ are an initial segment of the chain, of length Φ ; we split according to the last one.

(A) The last option in Λ is an addition. Let j_0 be the smallest j with $(\mu + e_j, \delta) \in \Lambda$; it is the first row of its length, and $\Phi = \ell + 1 + (r - 1 - 2\ell) + (\ell - j_0 + 1) = r - j_0 + 1$. The column $c^* := \mu_{j_0} + 1 \geq 2$ of μ has height $j_0 - 1$; put the index 1 into its block B_{c^*} (a new block if c^* is a new column). This is a pattern of $(\mu + e_{j_0}, \delta)$: the number of pairs is unchanged, and for $\delta = 1$ the first column, hence ℓ , E_ℓ and the marked block, are untouched because $c^* \geq 2$. By the factorisation $\Delta(B \cup \{1\}) = \pm \prod_{c \in B} (y_c - y_1) \cdot \Delta(B)$ of the Vandermonde determinant, its product is $\pm G \cdot \prod_{c \in B_{c^*}} (y_c - y_1)$: its y_1 -degree is $j_0 - 1 = r - \Phi$ (and $y_1^{j_0-1} \neq 0$ in the box, as $j_0 - 1 < r$), and its top coefficient is $\pm G$.

(M) The last option in Λ is the middle one (so $\ell < h$ and $\Phi = \ell + 1 + (r - 1 - 2\ell) = r - \ell$).

- $\delta = 0$: put the index 1 into B_1 (of height ℓ): a pattern of $(\mu \sqcup 1, 0)$, whose product has y_1 -degree $\ell = r - \Phi$ and top coefficient $\pm G$.
- $\delta = 1$: here $(\mu \sqcup 1, 1) \in \Lambda$ and $(\mu, 0) \in \Lambda$ (the zero option precedes the middle one). Put $E^+ := E_{\ell+1} = \{0, \dots, \ell - 1\}$ and

$$f := (y_1 \cdot \text{Pf}_{E^+}(B_0 \cup \{1\}) + \vartheta \cdot \text{Pf}(B_0; y^{E^+}, D(y_1, \cdot))) \cdot D_P \cdot R,$$

with $\vartheta = \pm 1$ the sign of (F4) for $N = B_0 \cup \{1\}$, $x = 1$. $f \in V_\Lambda$. $\text{Pf}_{E^+}(B_0 \cup \{1\}) \cdot D_P \cdot R$ is the product of a pattern of $(\mu \sqcup 1, 1)$: its marked block $B_0 \cup \{1\}$ has size $(\ell + 1) + 1 + 2t$, its borders are $E_{\ell+1}$, and the columns $c \geq 2$ and the pairs are those of μ . By (F2), $\text{Pf}(B_0; y^{E^+}, D(y_1, \cdot)) = \sum_{b \in B_0} \eta_b D(y_1, y_b) \cdot \text{Pf}_{E^+}(B_0 \setminus b)$. If $t \geq 1$, $D(y_1, y_b) \cdot \text{Pf}_{E^+}(B_0 \setminus b) \cdot D_P \cdot R$ is the product of a pattern of $(\mu \sqcup 1, 1)$ with marked block $B_0 \setminus b$ (of size $(\ell + 2) + 2(t - 1)$) and pairs $P \cup \{(1, b)\}$. If $t = 0$, then $|B_0 \setminus b| = \ell = |E^+|$ and $\text{Pf}_{E^+}(B_0 \setminus b) = \pm \Delta(B_0 \setminus b)$ by (F3), so it is $\pm$ the product of a pattern of $(\mu, 0)$: first block $B_0 \setminus b$, pairs $P \cup \{(1, b)\}$. *Degree.* By (F4), $\text{Pf}_{E^+}(B_0 \cup \{1\}) = \vartheta \cdot \text{Pf}(B_0; y^{E^+}, D^-(y_1, \cdot)) + \sum_{e \in E^+} \pm y_1^e \text{Pf}_{E^+ \setminus e}(B_0)$, and by (F5), $\text{Pf}(B_0; y^{E^+}, D(y_1, \cdot)) = \text{Pf}(B_0; y^{E^+}, y^{r-1}) - y_1 \text{Pf}(B_0; y^{E^+}, D^-(y_1, \cdot))$. So the two terms with $D^-(y_1, \cdot)$ cancel, whatever the value of ϑ :

$$f/(D_P R) = \sum_{e \in E^+} \pm y_1^{e+1} \text{Pf}_{E^+ \setminus e}(B_0) + \vartheta \cdot \text{Pf}(B_0; y^{E^+}, y^{r-1}).$$

The last term does not contain y_1 . If $\ell \geq 1$, the y_1 -degree is ℓ , with top coefficient $\pm \text{Pf}_{E^+ \setminus \{\ell-1\}}(B_0) = \pm \text{Pf}_{E_\ell}(B_0)$. If $\ell = 0$, then $E^+ = \emptyset$ and $f/(D_P R) = \vartheta \cdot \text{Pf}_{\{r-1\}}(B_0) = \pm \text{Pf}_{E_0}(B_0)$. In both cases $\deg_{y_1} f = \ell = r - \Phi$ and the top coefficient is $\pm G$.

(Z) The last option in Λ is the zero option ($\Phi = \ell + 1$).

- $\delta = 0$: here $(\mu, 1) \in \Lambda$. If $\ell = 0$, $f := y_1^{r-1} \cdot G$ is the product of a pattern of $(\emptyset, 1)$ with marked block $\{1\}$ ($\text{Pf}_{\{r-1\}}(\{1\}) = y_1^{r-1}$), of y_1 -degree $r - 1 = r - \Phi$. If $\ell \geq 1$, $f := \text{Pf}_{E_\ell}(B_1 \cup \{1\}) \cdot D_P \cdot R$ is the product of a pattern of $(\mu, 1)$ with marked block $B_1 \cup \{1\}$ (of size $\ell + 1$, so $t = 0$). By (F4) and (F5),

$$\text{Pf}_{E_\ell}(B_1 \cup \{1\}) = \mp \sum_{u=0}^{r-2} (-1)^u y_1^{r-2-u} \text{Pf}(B_1; y^{E_\ell}, y^u) + \sum_{e \in E_\ell} \pm y_1^e \text{Pf}_{E_\ell \setminus e}(B_1).$$

$\text{Pf}(B_1; y^{E_\ell}, y^u) = 0$ for $u \leq \ell - 2$, and for $u = \ell - 1$ it is $\pm \text{Pf}_{\{0, \dots, \ell-1\}}(B_1) = \pm \Delta(B_1)$ by (F3). So the first sum has y_1 -degree $r - 2 - (\ell - 1) = r - \ell - 1$, with top coefficient $\pm \Delta(B_1)$; the second has y_1 -degree at most $\ell - 2 < r - \ell - 1$ (as $\ell \leq h$). So $\deg_{y_1} f = r - \ell - 1 = r - \Phi$, with top coefficient $\pm G$.

- $\delta = 1$: here $(\mu, 0) \in \Lambda$. For $S \subseteq B_0$ with $|S| = \ell + 1$ and a perfect matching Q of $B_0 \setminus S$ put, with the signs of (F6),

$$f_{S,Q} := \sum_{b \in S} \varepsilon_b \Delta(S \setminus b) \cdot D(y_1, y_b) \cdot D_Q \cdot D_P \cdot R.$$

Each summand is the product of a pattern of $(\mu, 0)$: first block $S \setminus b$ (of size ℓ), blocks B_c ($c \geq 2$), pairs $P \cup Q \cup \{(1, b)\}$ (their number is $|P| + t + 1 = (m - |\mu|)/2$). So $f_{S,Q} \in V_\Lambda$. By (8.4) and (F6), $[y_1^{r-1-u}]f_{S,Q} = (-1)^u (\sum_b \varepsilon_b \Delta(S \setminus b) y_b^u) \cdot D_Q D_P R$ vanishes for $u \leq \ell - 1$ and is $\pm \Delta(S) \cdot D_Q \cdot D_P R$ for $u = \ell$. Hence $\Delta(S) D_Q \cdot D_P R \in W_{r-1-\ell}(V_\Lambda)$ for all S, Q . As $W_{r-1-\ell}(V_\Lambda)$ is an ideal, it contains the image of $\mathfrak{U}_\ell(B_0)$ in C_{m-1} times $D_P R$, and by **Lemma 8.7** — a membership over Z , which therefore holds for the images in C_{m-1} over every field — it contains $\text{Pf}_{E_\ell}(B_0) \cdot D_P R = G$. And $r - 1 - \ell = r - \Phi$.

(R) The last option in Λ is a removal. Then the removals in Λ are those of the rows $1, \dots, \rho$, with $\rho \geq 1$ the last row of its length, and $\Phi = \rho$.

- $\delta = 0$, or $\delta = 1$ and $\mu_\rho \geq 2$: the column $c_0 := \mu_\rho$ of μ has height ρ , and its block $S := B_{c_0}$ is an ordinary block ($c_0 \geq 2$ if $\delta = 1$). Write $G = \Delta(S) \cdot G'$. As in case (γ) of Proposition 5.8, $f := \sum_{b \in S} \varepsilon_b \Delta(S \setminus b) \cdot D(y_1, y_b) \cdot G'$ is a sum of products of patterns of $(\mu - e_\rho, \delta)$ (pairs $P \cup \{(1, b)\}$, the block of the column c_0 replaced by $S \setminus b$; for $\delta = 1$ the first column, hence the marked block, is unchanged). By (8.4) and (F6), $[y_1^{r-1-u}]f$ vanishes for $u \leq \rho - 2$ and is $\pm G$ for $u = \rho - 1$: $\deg_{y_1} f = r - \rho = r - \Phi$.
- $\delta = 1$ and $\mu_\rho = 1$: then $\rho = \ell$. Put $E' := E_{\ell-1}$ and $f := \text{Pf}_{E'}(B_0 \cup \{1\}) \cdot D_P \cdot R$. It is the product of a pattern of $(\mu - e_\ell, 1)$: the first column of $\mu - e_\ell$ has $\ell - 1$ rows, the marked block $B_0 \cup \{1\}$ has size $((\ell - 1) + 1) + 2(t + 1)$, and the other columns are those of μ . By (F4) and (F5),

$$\text{Pf}_{E'}(B_0 \cup \{1\}) = \mp \sum_{u=0}^{r-2} (-1)^u y_1^{r-2-u} \text{Pf}(B_0; y^{E'}, y^u) + \sum_{e \in E'} \pm y_1^e \text{Pf}_{E' \setminus e}(B_0).$$

If $\ell \geq 2$: $E' = \{0, \dots, \ell - 3\}$; the first sum vanishes for $u \leq \ell - 3$, and for $u = \ell - 2$ it gives $\pm y_1^{r-\ell} \text{Pf}_{E_\ell}(B_0)$; the second sum has y_1 -degree at most $\ell - 3 < r - \ell$. If $\ell = 1$: $E' = \{r - 1\}$; the first sum has y_1 -degree at most $r - 2$, and the second is $\pm y_1^{r-1} \text{Pf}_\emptyset(B_0) = \pm y_1^{r-1} \text{Pf}_{E_1}(B_0)$. In both cases $\deg_{y_1} f = r - \ell = r - \Phi$, with top coefficient $\pm G$.

The four kinds of last option exhaust $\Phi \geq 1$. ■

In every case the construction lands exactly in the slice $r - \Phi$. The absorbed pairs ($t \geq 1$) are produced by the second case of (R): a removal that empties the first column of a marked tail turns a pair D outside the marked block into a pair D^- inside it.

8.7 The theorem

Theorem 8.11 (interlaced down-set theorem). *For every field F , every odd $r \geq 3$, every $m \geq 0$ and every interlaced pair $\Lambda \subseteq \text{Sh}_m$, $\dim_F V_\Lambda \geq |Z_\Lambda|$.*

Proof. Induction on m . For $m = 0$, $\text{Sh}_0 = \{(\emptyset, 0)\}$: if $\Lambda = \emptyset$ both sides are 0; otherwise $V_\Lambda = F$ (the empty product) and Z_Λ is one point. Let $m \geq 1$. By the peeling lemma, Proposition 8.10, the induction hypothesis applied to the interlaced pairs Λ_i (Lemma 8.4; V_{Λ_i} is stable under relabelling, so the variables $y_2, \dots, y_m$ may be used), and Lemma 8.4 again,

$$\dim V_\Lambda = \sum_{i=0}^{r-1} \dim W_{r-1-i}(V_\Lambda) \geq \sum_i \dim V_{\Lambda_i} \geq \sum_i |Z_{\Lambda_i}| = \sum_i |(Z_\Lambda)_{>i}| = |Z_\Lambda|. \quad \blacksquare$$

Proof of Theorem O, the inequality $\geq$. Take $m = 2k + 1$ and $\Lambda = \Lambda_{\text{root}}$ (Lemma 8.5). The patterns of $((1), 0)$ consist of k disjoint pairs and one block of one element; their products are the D_P , that is, the D_J , $J \in \mathcal{J}$ (D is symmetric). The patterns of $(\emptyset, 1)$ have products $\text{Pf}_{\{r-1\}}(B_0) \cdot D_{P'}$ with $|B_0| = 1 + 2t$; by Lemma 8.7 with $\ell = 0$ (a membership over Z , hence also in C_{2k+1} over every field), $\text{Pf}_{\{r-1\}}(B_0)$ lies in the ideal generated by the D_Q , Q a perfect matching of B_0 minus one index (here $\Delta(S) = 1$, as $|S| = 1$); since $|Q| + |P'| = t + (k - t) = k$, the product lies in $(D_J : J \in \mathcal{J})$. Hence $V_{\Lambda_{\text{root}}} = (D_J : J \in \mathcal{J}) \cdot C_{2k+1}$, and Theorem 8.11 gives $\dim \geq |Z_{\Lambda_{\text{root}}}| = N_r(2k + 2)$. ■

Lemma 8.12 (the two forms). *Let $N = 2k + 2$, write the variables as $x_0, y_1, \dots, y_{2k+1}$, and put $\mathcal{M} := \sum_P D_P \cdot C_N$, the sum over the perfect matchings P of the N variables (the ideal $V_{\{(\emptyset, 0)\}}$ of level N). Then $\theta : \mathcal{M} \rightarrow C_{2k+1}$, $f \mapsto [x_0^{r-1}]f$, is injective, and its image is $(D_J : J \in \mathcal{J})C_{2k+1}$.*

Proof. By (8.3), $(x_a + x_b) \cdot D(x_a, x_b) = 0$ in the box, so every D_P is killed by $e_1 = x_0 + s$, $s := \sum_i y_i$ (sum over the pairs of P). Write $f = \sum_{u=0}^{r-1} x_0^u f_u$ with $f_u \in C_{2k+1}$; comparing the coefficients of x_0^u in $x_0 f = -sf$ gives $f_{u-1} = -sf_u$ for $u \geq 1$. So f is determined by f_{r-1} , and θ is injective. If k_0 is the partner of 0 in P , the coefficient of x_0^{r-1} in $D(x_0, y_{k_0})$ is 1, so $\theta(D_P \cdot g) = D_J \cdot g$ for $g \in C_{2k+1}$, where J is P read as a matching of $\{0, \dots, 2k + 1\}$. Moreover $x_0 \cdot D_P = -y_{k_0} D_P$, so $\mathcal{M} = \sum_P D_P \cdot C_{2k+1}$. Hence $\theta(\mathcal{M}) = (D_J : J \in \mathcal{J})C_{2k+1}$. ■

(The same proof works for every $r \geq 2$, with $(-1)^{r-1}$ in the place of 1; for the even box it is the proof of Corollary 10.6(i).)

Corollary 8.13 (equality; freeness over Z). *For every field F , every odd $r \geq 3$ and every $k \geq 0$: $\dim_F \sum_P D_P \cdot C_{2k+2} = N_r(2k + 2)$ and $\dim_F (D_J : J \in \mathcal{J}) \cdot C_{2k+1} = N_r(2k + 2)$. Both quotients of the integral box rings are free abelian groups, and the dimensions of the graded pieces of the two ideals do not depend on F . In particular Theorem O holds.*

Proof. By Lemma 8.12 the two dimensions are equal, and each is at least $N_r(2k + 2)$: the second by the part of Theorem O already proved, the first by Theorem 8.11 for the interlaced pair $\{(\emptyset, 0)\}$ of level $2k + 2$ (Lemma 8.5), whose patterns are the perfect matchings. For the upper bound, let first $F = Q$ and $T := \{-h, \dots, h\} \subset Q$, and put $I_P := (x_a + x_b : \{a, b\} \in P)$

and $\mathcal{M} := \sum_P D_P \cdot C_N$. On C_N let $\langle f, g \rangle$ be the coefficient of $\prod_i x_i^{r-1}$ in fg ; as in the proof of Proposition 2.6 the pairing is perfect, so $\dim V + \dim V^\perp = \dim C_N$ for every subspace V , and the annihilator of an ideal is contained in its orthogonal. By (8.3), $(x_a + x_b) \cdot D(x_a, x_b) = 0$ in the box, so $I_P \cdot C_N$ annihilates D_P , and $\bigcap_P I_P \cdot C_N$ annihilates $\mathcal{M}$. Hence $\dim \mathcal{M} \leq \dim C_N - \dim \bigcap_P I_P \cdot C_N = \dim Q[x] / \bigcap_P (I_P + (x_i^r))$. Let $\Gamma \subseteq T^N$ be the set of the points of $\bigcup_P V(I_P)$ in T^N , that is, the set of the N -tuples that split into pairs $\{u, -u\}$; $|\Gamma| = N_r(N)$. With $g(x) := \prod_{u \in \Gamma} (x - u)$, an odd monic polynomial of degree r , the ideal of the finite set $V(I_P) \cap T^N$ is $I_P + (g(x_i) : i)$, and its ideal of top-degree forms is $I_P + (x_i^r)$ (it contains it, and both quotients have dimension r^{k+1} ; Lemma 5.8'). Since $I(\Gamma) = \bigcap_P I(V(I_P) \cap T^N)$ and gr of an intersection is contained in the intersection of the gr 's, $\text{gr}(I(\Gamma)) \subseteq \bigcap_P (I_P + (x_i^r))$, whence $\dim Q[x] / \bigcap_P (I_P + (x_i^r)) \leq \dim Q[x] / \text{gr}(I(\Gamma)) = |\Gamma|$. So $\dim_Q \sum_P D_P \cdot C_N \leq N_r(N)$. Over an arbitrary field F , the ideal $\sum_P D_P \cdot C_N$ is spanned by the images of the vectors $D_P \cdot x^\alpha$, which have integer coordinates, and the rank of an integer matrix over F is at most its rank over Q . This gives the two equalities over every field. The integral statement follows as in the proof of Theorem 5.9': the quotient M of the integral box ring by the ideal generated by the D_P (respectively the D_J) is a graded, finitely generated abelian group, $M \otimes F$ is the quotient over F , and the dimension of $M \otimes F$ is the same for $F = Q$ and for every $F = F_p$; so no graded piece of M has torsion. ■

Remarks 8.14. (1) *Where the full family enters.* Only at the root (Lemma 8.5 and the proof of Theorem O), as in §5. With one matching removed the dimension drops in every cell we computed, also in characteristic 2 (§14.9). (2) *No slack.* In Proposition 8.10 the slice $r - 1 - i$ cannot be lowered: with $r - 2 - i$ the containment fails in every cell tested (§14.9). (3) *Equality for every interlaced pair* is measured, not proved: $\dim V_\Lambda = |Z_\Lambda|$ held for every interlaced pair of every cell computed, and for pairs of down-sets that satisfy (D1) but not (D2) the two numbers differ (§14.9). (4) *The marked shapes are needed.* Without the bordered Pfaffians — with the patterns $t = 0$ only — the equality of (3) fails for 15 of the 163 interlaced pairs of the auditor's run (§14.9): the absorbed pairs are part of the ideal. (5) *Characteristic.* Unlike the bipartite ideals of §7, the ideals V_Λ of this section are defined over Z , and Theorem 8.11 holds over every field with no condition; in particular over F_2 , which is where §9 uses it for the degrees 2^v .

8.8 The case $r = 3$, without Pfaffians

For $r = 3$ ($h = 1$) the theory collapses to a family with one parameter, and every step is a one-line identity. This gives a proof of Theorem O at $r = 3$ that uses nothing from §8.2–§8.7; with §9 it suffices for the degrees $m = 4, 6$ and 12 . Here $T = \{-1, 0, 1\}$, $C_m = F[y_1, \dots, y_m] / (y_i^3)$ and $D(a, b) = a^2 - ab + b^2$. The shape of $M \in T^m$ is determined by $j(M) := |\sum_i M_i|$ (the mark is the parity of $m - j$), and the interlaced pairs are the sets $\{j \leq J\}$. For $0 \leq J \leq m$ put $Z_J^{(m)} := \{M \in \{-1, 0, 1\}^m : |\sum M_i| \leq J\}$, and define an ideal $I(m, J) \subseteq C_m$ as follows, where P, P^+, P' denote sets of pairwise disjoint pairs of indices and a, b, c distinct indices outside them:

- if $J \equiv m \pmod{2}$: $I(m, J) := (D_P : |P| = (m - J)/2)$;
- if $J \not\equiv m \pmod{2}$ and $J \geq 1$: $I(m, J) := ((y_b - y_a) \cdot D_P : |P| = (m - 1 - J)/2; \quad D_{P^+} : |P^+| = (m + 1 - J)/2)$;
- if $J = 0$ and m is odd: $I(m, 0) := (y_c^2 \cdot D_P : P \text{ a perfect matching of the other indices}; \quad \Delta(y_a, y_b, y_c) \cdot D_{P'} : P' \text{ a perfect matching of the other indices})$.

Theorem 8.15. $\dim_F I(m, J) \geq |Z_J^{(m)}|$ for every field F and all $0 \leq J \leq m$. In particular $I(2k + 1, 1)$ is the ideal generated by the D_J , $J \in \mathcal{J}$, in C_{2k+1} , and $|Z_1^{(2k+1)}| = N_3(2k + 2)$: this is Theorem O, $\geq$, at $r = 3$.

Proof. Induction on m ; $I(0,0) = F$. For $J = m$ the ideal is the unit ideal and Z is everything. A tail with $|\Sigma| = j'$ has 3 completions in $Z_J^{(m)}$ if $j' \leq J - 1$, 2 if $j' = J \geq 1$, 1 if $j' = J + 1$ or $j' = J = 0$, and none otherwise. So $|Z_J^{(m)}| = |Z_{J+1}^{(m-1)}| + |Z_J^{(m-1)}| + |Z_{J-1}^{(m-1)}|$ for $J \geq 1$, and $|Z_0^{(m)}| = |Z_1^{(m-1)}|$ (with $Z_J^{(m-1)}$ everything and $I(m-1, J)$ the unit ideal for $J \geq m-1$). By peeling and induction it suffices to show, for the slices of $I(m, J)$:

$W_2 \supseteq I(m-1, J+1)$, $W_1 \supseteq I(m-1, J)$, $W_0 \supseteq I(m-1, J-1)$ for $J \geq 1$; $W_2 \supseteq I(m-1, 1)$ for $J = 0$.

Write $D(1, b)$ for $D(y_1, y_b) = y_1^2 - y_1 y_b + y_b^2$; the sets of pairs below lie in $\{2, \dots, m\}$, and «free» means an index of $\{2, \dots, m\}$ outside them.

Case I: $J \equiv m$, $1 \leq J \leq m-2$, $p := (m-J)/2 \geq 1$; $I(m, J) = (D_P : |P| = p)$.

- $W_2 \supseteq I(m-1, J+1) = (D_{P'} : |P'| = p-1)$: there are $J+1 \geq 2$ free indices; for a free b , $D(1, b) \cdot D_{P'} \in I(m, J)$ has y_1^2 -coefficient $D_{P'}$.
- $W_1 \supseteq I(m-1, J) = ((y_b - y_a)D_{P'} : |P'| = p-1; \quad D_{P''} : |P''| = p) : (D(1, b) - D(1, a)) \cdot D_{P'} = (-y_1(y_b - y_a) + y_b^2 - y_a^2) \cdot D_{P'} \in I(m, J)$; and $D_{P''} \in I(m, J)$ does not contain y_1 .
- $W_0 \supseteq I(m-1, J-1) = (D_{P''} : |P''| = p)$: these are generators of $I(m, J)$ without y_1 .

Case II: $J \not\equiv m$, $1 \leq J \leq m-1$, $p := (m-1-J)/2$; $I(m, J) = ((y_b - y_a)D_P : |P| = p; \quad D_{P^+} : |P^+| = p+1)$.

- $W_2 \supseteq I(m-1, J+1)$. If $p = 0$ this is the unit ideal, and $D(1, b) \in I(m, J)$ has y_1^2 -coefficient 1. If $p \geq 1$ its generators are $(y_b - y_a)D_{P'}$ ($|P'| = p-1$) and D_P ($|P| = p$); there is a free index c besides a, b in the first case and a free b in the second, and $D(1, c)(y_b - y_a)D_{P'}$, $D(1, b)D_P$ lie in $I(m, J)$ with y_1^2 -coefficients the generators.
- $W_1 \supseteq I(m-1, J) = (D_P : |P| = p)$: for a free b , $(y_b - y_1) \cdot D_P \in I(m, J)$ has y_1 -coefficient $-D_P$.
- $W_0 \supseteq I(m-1, J-1)$. If $J \geq 2$, its generators $(y_b - y_a)D_P$ ($|P| = p$), D_{P^+} ($|P^+| = p+1$) are generators of $I(m, J)$ without y_1 . If $J = 1$ (m even), it is $I(m-1, 0) = (y_c^2 D_P, \Delta(y_a, y_b, y_c)D_{P'})$, and

$$y_c^2 = y_1 \cdot (y_c - y_1) + D(1, c),$$

$$\Delta(y_a, y_b, y_c) = D(1, a)(y_c - y_b) - D(1, b)(y_c - y_a) + D(1, c)(y_b - y_a)$$

(in the second identity the coefficients of y_1^2 and of y_1 cancel, and the constant term is $y_a^2(y_c - y_b) - y_b^2(y_c - y_a) + y_c^2(y_b - y_a) = \Delta(y_a, y_b, y_c)$). So $y_c^2 D_P$ and $\Delta \cdot D_{P'}$ lie in $I(m, 1)$ and do not contain y_1 .

Case III: $J = 0$. If m is even, $I(m, 0) = (D_{P^+} : P^+ \text{ a perfect matching})$ and $I(m-1, 1) = (D_{P'} : |P'| = (m-2)/2)$: with the free index b , $D(1, b)D_{P'}$ has y_1^2 -coefficient $D_{P'}$. If m is odd, $I(m-1, 1) = ((y_b - y_a)D_{P'}; \quad D_{P^+})$ with P^+ a perfect matching of $\{2, \dots, m\}$ and P' one of $\{2, \dots, m\} \setminus \{a, b\}$: $y_1^2 \cdot D_{P^+} \in I(m, 0)$, and $\Delta(y_1, y_a, y_b) \cdot D_{P'} = (y_a - y_1)(y_b - y_1)(y_b - y_a)D_{P'} \in I(m, 0)$ has y_1^2 -coefficient $(y_b - y_a)D_{P'}$.

For the last sentence of the theorem: the D_P with $|P| = k$ in $2k+1$ variables are the D_J ; and deleting the last entry is a bijection from the $(2k+2)$ -tuples in $\{-1, 0, 1\}$ of sum 0 onto $Z_1^{(2k+1)}$.

■

8.9 A worked example: $r = 3, k = 1$

Here $m = 3$, the three generators are $D(y_2, y_3)$, $D(y_1, y_3)$, $D(y_1, y_2)$ in $F[y_1, y_2, y_3]/(y_i^3)$, a ring of dimension 27, and $N_3(4) = 19$: the 4-tuples in $\{-1, 0, 1\}$ of sum 0 number $1 + 12 + 6$. The root is $\Lambda = \{((1), 0), (\emptyset, 1)\}$. The tails have two coordinates, with shapes in $\text{Sh}_2 = \{(\emptyset, 0), ((2), 0), ((1), 1)\}$, and $|Z_{(\emptyset, 0)}| = 3$, $|Z_{((2), 0)}| = 2$, $|Z_{((1), 1)}| = 4$ (total 9).

tail shape	its chain (positions 1, 2, 3)	options in Λ	F_Λ	case of Prop. 8.10	slice $r - \Phi$
$(\emptyset, 0)$	$(\emptyset, 1) \cdot ((1), 0) \cdot ((1), 0)$	all	3	(M), $\delta = 0$	0
$((1), 1)$	$(\emptyset, 1) \cdot ((1), 0) \cdot ((2), 1)$	first two	2	(Z), $\delta = 1$	1
$((2), 0)$	$((1), 0) \cdot ((2), 1) \cdot ((3), 0)$	first	1	(R)	2

So $\Lambda_0 = \text{Sh}_2$, $\Lambda_1 = \{(\emptyset, 0), ((1), 1)\}$ and $\Lambda_2 = \{(\emptyset, 0)\}$, all interlaced, and $|Z_\Lambda| = 9 + 7 + 3 = 19$. On the side of the ideal: $W_0 \ni D(y_2, y_3)$ (the generator of V_{Λ_2}); W_1 contains $y_3 - y_2$, from $D(y_1, y_2) - D(y_1, y_3) = -y_1(y_2 - y_3) + y_2^2 - y_3^2$, which is the case (Z) with $B_0 = \{2, 3\}$, $\ell = 1$, $t = 0$; and $W_2 \ni 1$, from $D(y_1, y_2)$. The dimensions of the three slices are 3, 7 and 9.

9. Even degrees

In this section $m \geq 4$ is even, $k \geq 1$, $n = 2k$ and $N = n + 2$, except in §9.2, which also allows the degree 2 and $k \geq 0$ (Lemma 9.10 uses it in that generality). Nothing in §2.1 or in Appendix B uses the parity of m : Theorem 0 and Proposition 2.1 hold for every $m \geq 3$, and [DS] themselves compute even cells ([DS, Remark 4.4] and [DS, §5]). So, as for odd m , the conjecture at (k, m) is the equality $\dim_{F_p}(\bar{\psi}_J : J \in \mathcal{J})F_p[G] = |\Gamma_{\mathcal{J}}|$ for every prime p dividing m , and $\leq$ always holds. What changes is everything after §2.1. Inversion on $\mu_m \setminus \{1\}$ now has the fixed point -1 , so the count is different (§9.1). At the prime 2, the element 2 is not a unit and the coordinate $y = t - t^{-1}$ of Lemma 2.3 does not exist: for $m = 2^v$ we pass to the ideal of leading forms, which contains $s_1 \cdots s_{2k+1}$ times the ideal of Theorem O for the box $2^v - 1$ in characteristic 2, an isomorphic copy of it in another ring (§9.2). For the other even degrees the colour reduction of §6 applies at each prime (§9.3), with two new kinds of block: at an odd prime the cofactor is even, the colour -1 is its own inverse, and its block is the ideal of Theorem O for the box p^v (§9.4); at the prime 2 the block of colour 1 is the problem for the degree 2^v again, and the pair blocks are bipartite ideals with an even box.

In this section the letter r is the odd box of §8, and the cofactor of a prime power in m , which §6 calls r , is written r' . The count $N_r(n)$ of §8 makes sense for $r = 1$ ($h = 0$): $N_1(n) = 1$, the only tuple being $(0, \dots, 0)$; it is used in that sense in §9.2 and §9.4.

9.1 The count

Lemma 9.1. *For every $m \geq 3$, $\Gamma_{\mathcal{J}}$ is in bijection with the set of N -tuples in $\mu_m \setminus \{1\}$ that can be split into pairs of mutually inverse entries. For even m their number is*

$$|\Gamma_{\mathcal{J}}| = N_{m-1}(N) = N! \cdot [x^N] \cosh(x) \cdot I_0(2x)^{(m-2)/2}.$$

Proof. The first paragraph of the proof of Lemma 2.2 uses nothing about m : for $a \in \Gamma_{\mathcal{J}}$, with a matching J , put $a_0 := (a_1 \cdots a_{n+1})^{-1}$; then $a_0 = a_{k_0}^{-1} \neq 1$, and every pair of J is a pair of inverse entries of $(a_0, \dots, a_{n+1})$. Conversely a tuple that splits into inverse pairs has product 1,

so its entry at 0 is determined by the others, which lie in $\Gamma_{\mathcal{J}}$ through the same matching. For even m , inversion on $\mu_m \setminus \{1\}$ has the single fixed point -1 and $(m-2)/2$ orbits $\{c, c^{-1}\}$. A tuple splits into inverse pairs if and only if, for every orbit, c and c^{-1} occur equally often, and -1 occurs an even number of times. Each orbit contributes the exponential generating function $I_0(2x)$, and the value -1 contributes $\cosh x$. A bijection $\mu_m \setminus \{1\} \rightarrow T$ that carries inversion to $u \mapsto -u$ and -1 to 0 (with $r = m-1$) identifies these tuples with the tuples counted by $N_{m-1}(N)$ in §8. $\blacksquare$

We extend the notation of §1.2: for even m , $Q_k(m) := N_{m-1}(2k+2)$. So $Q_k(m) = |\Gamma_{\mathcal{J}}|$ for every $m \geq 3$. The first values are

$m \setminus k$	1	2	3	4	5
4	19	141	1 107	8 953	73 789
6	61	1 001	18 733	375 745	7 858 225
8	127	3 301	103 279	3 595 177	133 789 789
10	217	7 761	345 465	17 605 249	980 612 161
12	331	15 101	876 331	59 415 961	4 481 629 021
16	631	41 301	3 529 863	361 612 105	42 214 788 925

For $k = 1$, $Q_1(m) = 3m^2 - 9m + 7$, and the values for $k = 2, 3$ are those of the polynomials displayed in [DS, Remark 4.4] for even m (with their $\delta_m = 1$); for instance 141, 1001 and 1107 at $(n, m) = (4, 4), (4, 6), (6, 4)$. For $m = 4$ the numbers are the central trinomial coefficients, the constant terms of $(x + 1 + x^{-1})^{2k+2}$. In general, for even m the rank $Q_k(m) + 1$ of $L(X)$ is one more than the count $N_{m-1}(2k+2)$ of Theorem A at the odd number $m-1$ (§10).

9.2 Degree 2^v : leading forms

Let $q = 2^v$ with $v \geq 1$, $k \geq 0$, and let F be a field of characteristic 2. Put $s_i := t_i + 1$. Since $t^q - 1 = (t + 1)^q$,

$$F[G] = F[t_1, \dots, t_{2k+1}]/(t_i^q - 1) = F[s_1, \dots, s_{2k+1}]/(s_i^q) =: B,$$

a graded ring. Let $I := (\bar{\psi}_J : J \in \mathcal{J})B$, where $\bar{\psi}_J$ is the image of the generator ψ_J of §2 for the degree $m = q$.

Proposition 9.2. $\dim_F I \geq N_{q-1}(2k+2)$. Hence, for $v \geq 2$ and $k \geq 1$, $\dim_{F_2}(\bar{\psi}_J : J \in \mathcal{J})F_2[G] = |\Gamma_{\mathcal{J}}|$, and $H_{2k}(X; Z)/L(X)$ is torsion free for the Fermat variety of degree 2^v and dimension $2k$.

Proof. The $\bar{\psi}_J$ have coefficients in F_2 , so the dimension does not depend on F ; let $F = F_2$.

Step 1: the generators. In $F_2[u]$, $(u+1)\varphi(u) = u^q + 1 = (u+1)^q$, so $\varphi(u) = (u+1)^{q-1}$. For $u = t_j t_l$, $u+1 = (1+s_j)(1+s_l) + 1 = s_j + s_l + s_j s_l$. So

$$\bar{\psi}_J = \prod_{i=0}^k s_{k_i} \cdot \prod_{i=1}^k (s_{j_i} + s_{k_i} + s_{j_i} s_{k_i})^{q-1},$$

and, as a polynomial, its homogeneous component of lowest degree is $L_J := \prod_{i=0}^k s_{k_i} \cdot \prod_{i=1}^k (s_{j_i} + s_{k_i})^{q-1}$, of degree $(k+1) + k(q-1)$.

Step 2: leading forms. For $0 \neq f \in B$ let $\text{in}(f)$ be its homogeneous component of lowest degree, and let $\text{in}(I)$ be the span of the $\text{in}(f)$, $0 \neq f \in I$. Let $I_{\geq d}$ be the set of the elements of I with

no component of degree less than d . The map $I_{\geq d} \rightarrow B_d$ that takes the component of degree d has kernel $I_{\geq d+1}$, and its image is $\text{in}(I) \cap B_d$. Summing over d , $\dim \text{in}(I) = \dim I$. Moreover $\text{in}(I)$ is an ideal: for a monomial x and $f \in I$, $x \cdot \text{in}(f)$ is 0 or $\text{in}(xf)$. Since the ideal (s_i^q) is homogeneous, the image of L_J in B is 0 or $\text{in}(\psi_J)$. Hence

$$\dim I = \dim \text{in}(I) \geq \dim(L_J : J \in \mathcal{J})B.$$

Step 3: the odd box. Put $r := q - 1$. In $F_2[a, b]$, $(a + b) \cdot \sum_{u=0}^{q-1} a^u b^{q-1-u} = a^q + b^q = (a + b)^q$, so $(a + b)^{q-1} = \sum_{u=0}^{q-1} a^u b^{q-1-u}$. Multiply by b and drop b^q : $b(a + b)^{q-1} = ab \cdot \sum_{w=0}^{q-2} a^w b^{q-2-w}$ in $F_2[a, b]/(b^q)$, and the last sum is the polynomial $D(a, b) = D_r(a, b)$ of §8 over F_2 , where the signs disappear. The indices k_0 and j_i, k_i ($i \geq 1$) are $1, \dots, 2k + 1$, each once; so $L_J = Y \cdot D_J$ in B , with $Y := s_1 \cdots s_{2k+1}$ and $D_J := \prod_{i=1}^k D(s_{j_i}, s_{k_i})$. Multiplication by Y on B kills exactly the monomials with some exponent at least $q - 1$, so it induces an injective map $F_2[s]/(s_i^r) \rightarrow B$, which carries the ideal $(D_J : J \in \mathcal{J}) \cdot F_2[s]/(s_i^r)$ onto $(L_J : J \in \mathcal{J})B$. The former is the ideal of Theorem O at (k, r, F_2) .

Conclusion. If $q \geq 4$, then $r = 2^v - 1 \geq 3$ is odd and Theorem O gives $\dim(L_J)B \geq N_r(2k + 2)$. If $q = 2$, then $r = 1$, $L_J = Y \neq 0$ for every J , and $\dim(L_J)B = 1 = N_1(2k + 2)$. With Step 2 this is the inequality. For $k \geq 1$ and $m = q \geq 4$, Proposition 2.1 and Lemma 9.1 give $\dim I \leq |\Gamma_{\mathcal{J}}| = N_{q-1}(2k + 2)$, so there is equality at the only prime dividing m . ■

Remarks 9.3. (1) The proof shows more: $\text{in}(I) = (L_J : J \in \mathcal{J})B$. The generators $\bar{\psi}_J$ are a standard basis of I for the filtration by the order of vanishing, in the sense that their leading forms generate the ideal of leading forms. (2) The inequality of Step 2 is where information could be lost; Theorem O says that none is. The statement « $\dim_{F_2}(D_J) \cdot F_2[s]/(s_i^r) \geq N_r(2k + 2)$ for $r = 2^v - 1$ » is, on its face, stronger than the conjecture at $(k, 2^v)$: it is the conjecture together with (1). (3) For $q = 2$, $\bar{\psi}_J = Y$ for every J (in Step 1, $s_l(s_j + s_l + s_j s_l) = s_j s_l$, because $s_l^2 = 0$), and I is the socle of B .

9.3 The colour reduction for an even degree

Let p be a prime dividing m , and write $m = q \cdot r'$ with $q = p^v$ and $p \nmid r'$. Put $F := \bar{F}_p$, $F[G] := F[t_1, \dots, t_{n+1}]/(t_i^m - 1)$ and $I := (\bar{\psi}_J : J \in \mathcal{J})F[G]$, as in §6. By Proposition 2.1 and Lemma 9.1, exactly as in §6,

$$\dim_F I \leq |\Gamma_{\mathcal{J}}| = Q_k(m), \quad (9.1)$$

and the conjecture at (k, m) is equivalent to $\dim_F I \geq Q_k(m)$ for every prime p dividing m .

Lemma 9.4 (splitting and survival, for every prime). *Lemmas 6.1 and 6.2 hold as stated, with r' in the place of r , for every prime p dividing m and every $m \geq 3$.*

Proof. The proof of Lemma 6.1 uses that $(t^{r'} - 1)^q = t^m - 1$ in characteristic p and that $t^{r'} - 1$ is separable, because $r' \neq 0$ in F . The proof of Lemma 6.2 uses the factorisation $(u - 1)\varphi(u) = \prod_{\xi \in \mu_{r'}} (u - \xi)^q$ in $F[u]$ and the Frobenius identity $(t_j t_l - c_j c_l)^q = t_j^q t_l^q - c_j^q c_l^q = 0$ in R_c . Neither uses the parity of p , of q or of r' . ■

Blocks (this replaces Lemma 6.3, which uses that the cofactor is odd). Fix a colouring $c \in \mu_{r'}^{n+1}$, with $c_0 := (c_1 \cdots c_{n+1})^{-1}$ and the colour classes $\mathcal{C}_{\zeta} \subseteq \{0, \dots, n + 1\}$. The colours equal to their inverses are 1 and, when r' is even (so p is odd), -1 . The other colours split into pairs $\{\zeta, \zeta^{-1}\}$; fix a set $\mathcal{R}$ of representatives. The **blocks** of c are $\mathcal{C}_1, \mathcal{C}_{-1}$ (empty if r' is odd) and the sets $\mathcal{C}_{\zeta} \cup \mathcal{C}_{\zeta^{-1}}$, $\zeta \in \mathcal{R}$. A pair $\{a, b\}$ has $c_a c_b = 1$ if and only if it lies in $\mathcal{C}_1$, or it lies in $\mathcal{C}_{-1}$, or it meets both $\mathcal{C}_{\zeta}$ and $\mathcal{C}_{\zeta^{-1}}$ for some $\zeta \in \mathcal{R}$. So the matchings compatible with c are the choices

of a perfect matching P_1 of $\mathcal{C}_1$, a perfect matching P_{-1} of $\mathcal{C}_{-1}$ and a bijection $\sigma_\zeta : \mathcal{C}_\zeta \rightarrow \mathcal{C}_{\zeta^{-1}}$ for each $\zeta \in \mathcal{R}$, made independently; every such choice is an element of $\mathcal{J}$ (this is where the full family is used), and c is **compatible** if $|\mathcal{C}_1|$ and $|\mathcal{C}_{-1}|$ are even and $|\mathcal{C}_\zeta| = |\mathcal{C}_{\zeta^{-1}}|$ for every ζ . Group the tensor factors of R_c accordingly, $R_c = R_{c,1} \otimes R_{c,-1} \otimes \otimes_{\zeta \in \mathcal{R}} R_{c,\zeta}$, and define g_{P_1} , $g_{P_{-1}}$, g_{σ_ζ} and the ideals $I_{c,1}$, $I_{c,-1}$, $I_{c,\zeta}$ as in §6.3: the products of the factors of (6.2) that belong to the pairs of one block, and the ideals they generate.

Lemma 9.5 (tensor decomposition). *If c is not compatible, $\pi_c(I) = 0$. If c is compatible, $\pi_c(I) = I_{c,1} \otimes I_{c,-1} \otimes \otimes_{\zeta \in \mathcal{R}} I_{c,\zeta}$, and its dimension is the product of the dimensions of the factors.*

Proof. As for Proposition 6.5: by (6.2) the image of a compatible $\bar{\psi}_J$ is a unit times a pure tensor along the blocks, the choices in the blocks are independent, and Lemma 6.4 applies. ■

Lemma 9.6 (the count factors). *For a compatible colouring c let $N_1(c)$ be the number of tuples $(w_i)_{i \in \mathcal{C}_1}$ in $\mu_q \setminus \{1\}$ that split into inverse pairs, $N_{-1}(c)$ the number of tuples $(w_i)_{i \in \mathcal{C}_{-1}}$ in μ_q that split into inverse pairs, and $N_\zeta(c) := N_{\text{bal}}(|\mathcal{C}_\zeta|, q)$ (§6.6). Then*

$$Q_k(m) = |\Gamma_{\mathcal{J}}| = \sum_c N_1(c) \cdot N_{-1}(c) \cdot \prod_{\zeta \in \mathcal{R}} N_\zeta(c),$$

the sum over the compatible colourings. Moreover: $N_1(c) = (2k')! \cdot [x^{2k'}]I_0(2x)^{(q-1)/2}$ if p is odd and $N_1(c) = N_{q-1}(2k')$ if $p = 2$, where $|\mathcal{C}_1| = 2k'$; $N_{-1}(c) = N_q(|\mathcal{C}_{-1}|)$; and $N_{\text{bal}}(a, q) = N_{\text{ph}}(a-1, q)$ for $a \geq 1$.

Proof. Work with the complex roots of unity, as in Lemma 6.8, and fix an isomorphism of groups between the complex r' -th roots of unity and those of F ; it preserves 1, -1 and inversion, hence the blocks of a colouring and their sizes. $\mu_m = \mu_{r'} \times \mu_q$, $g_i = c_i w_i$ for $i = 0, \dots, n+1$; $g_a g_b = 1$ iff $c_a c_b = 1$ and $w_a w_b = 1$; and $g_i \neq 1$ iff $(c_i, w_i) \neq (1, 1)$. By Lemma 9.1, $\Gamma_{\mathcal{J}}$ is in bijection with the N -tuples $(g_0, \dots, g_{n+1})$ in $\mu_m \setminus \{1\}$ that split into inverse pairs, and the colours of such a tuple are (c_0, c) with $c_0 = (c_1 \cdots c_{n+1})^{-1}$. A matching that splits the tuple is compatible with c , so each of its pairs lies in one block; hence the tuple splits if and only if its restriction to each block does. On $\mathcal{C}_1$: $g_i = w_i$, and the condition is that (w_i) lies in $\mu_q \setminus \{1\}$ and splits into inverse pairs. On $\mathcal{C}_{-1}$: $g_i = -w_i$, which is never 1 because q is odd, and $g_i g_l = w_i w_l$; the condition is that (w_i) splits into inverse pairs in μ_q . On $\mathcal{C}_\zeta \cup \mathcal{C}_{\zeta^{-1}}$: every $g_i \neq 1$, a splitting is a bijection $\sigma : \mathcal{C}_\zeta \rightarrow \mathcal{C}_{\zeta^{-1}}$ with $w_{\sigma(i)} = w_i^{-1}$, and one exists if and only if the multiset of the w_i , $i \in \mathcal{C}_\zeta$, equals the multiset of the w_l^{-1} , $l \in \mathcal{C}_{\zeta^{-1}}$: this is $N_{\text{bal}}(|\mathcal{C}_\zeta|, q)$. The conditions concern disjoint sets of coordinates, so the count is the product. The closed forms: on $\mu_q \setminus \{1\}$ inversion has no fixed point if q is odd (Lemma 2.2) and one fixed point if q is even (Lemma 9.1); on μ_q , q odd, it has the single fixed point 1, which gives N_q ; and $N_{\text{bal}}(a, q) = N_{\text{ph}}(a-1, q)$ is Lemma 7.2(iii). ■

(In this count the index 0 is a coordinate like the others. On the side of the ideals it is not: the variable t_0 does not exist, and the block that contains 0 has one variable less. This is the difference between the balanced and the phantom bipartite ideals, between the two cases of Lemma 6.6, and between the two forms of Lemma 8.12.)

9.4 The blocks

Lemma 9.7 (pair blocks). *For every prime $p|m$ and every $\zeta \in \mathcal{R}$, with $a := |\mathcal{C}_\zeta| = |\mathcal{C}_{\zeta^{-1}}|$: $I_{c,\zeta} \cong I_a^{\text{bal}}$ if $0 \notin \mathcal{C}_\zeta \cup \mathcal{C}_{\zeta^{-1}}$, and $I_{c,\zeta} \cong I_{a-1}^{\text{ph}}$ otherwise, with the box $q = p^v$. In both cases $\dim_F I_{c,\zeta} \geq N_\zeta(c)$.*

Proof. Lemma 6.7 and its proof hold for every prime p and every r' : they use only $c_s \neq 1$ for the indices s of the block, and, in the case $0 \in \mathcal{C}_\zeta$, the equality of the ideals generated by $(x-z)^{q-1}$

and by $(z - x)^{q-1}$, which holds for every q . The inequality is Theorem C for the box $q = p^v$ over $F = \bar{F}_p$; its hypothesis holds for every prime p , 2 included, because $C(q-1, t) \equiv (-1)^t \pmod{p}$. For $p = 2$ this is Theorem C at an **even** box. ■

Lemma 9.8 (the block of colour 1 at an odd prime). *If p is odd, $\dim_F I_{c,1} \geq N_1(c)$.*

Proof. This is Lemma 6.6: §6.4 uses only $(t_i - 1)^q = 0$, $q = p^v$ and $2 \in F^\times$. The number $N_1(c)$ of §6.4 is the one of Lemma 9.6: if $0 \notin \mathcal{C}_1$ the two definitions coincide, and if $0 \in \mathcal{C}_1$ a tuple $(w_i)_{i \in \mathcal{C}_1}$ that splits into inverse pairs has product 1, so its entry w_0 is the one that §6.4 computes from the others, and deleting it is a bijection between the two sets of tuples. ■

Lemma 9.9 (the block of colour -1). *Let p be odd, r' even and $|\mathcal{C}_{-1}| = 2a$. Then $\dim_F I_{c,-1} \geq N_q(2a) = N_{-1}(c)$. More precisely, in suitable coordinates y_i with $R_{c,-1} = F[y_i : i \in \mathcal{C}_{-1} \setminus \{0\}]/(y_i^q)$: if $0 \in \mathcal{C}_{-1}$, $I_{c,-1}$ is the ideal $(D_J : J \in \mathcal{J})$ of Theorem O for the box $r = q$ in $2a - 1$ variables; if $0 \notin \mathcal{C}_{-1}$, it is the ideal $\sum_P D_P \cdot C_{2a}$ of Lemma 8.12.*

Proof. For $i \in \mathcal{C}_{-1} \setminus \{0\}$ put $u_i := -t_i$. In R_c , $(u_i - 1)^q = -(t_i + 1)^q = 0$, because q is odd. So Lemma 2.3 applies to u_i (it needs $(u - 1)^q = 0$, $q = p^v$ and $2 \in F^\times$): with $y_i := u_i - u_i^{-1}$, the factor of i is $F[y_i]/(y_i^q)$, and $t_i t_l - 1 = u_i u_l - 1 = (\text{unit}) \cdot (y_i + y_l)$. Moreover $t_i - 1 = -(u_i + 1) = -(2 + (u_i - 1))$ is a unit. So in (6.2) a pair $\{i < l\} \subseteq \mathcal{C}_{-1} \setminus \{0\}$ contributes a unit times $(y_i + y_l)^{q-1}$, and the pair $\{0, k_0\}$, if $0 \in \mathcal{C}_{-1}$, contributes a unit. In characteristic p , $(a + b)^{q-1} = \sum_u (-1)^u a^u b^{q-1-u}$ (proof of Lemma 2.4(i)), which is the polynomial $D(a, b)$ of §8 for $r = q$. Hence g_P is a unit times the product of the $D(y_i, y_l)$ over the pairs of P that avoid 0. If $0 \in \mathcal{C}_{-1}$, the perfect matchings of $\mathcal{C}_{-1}$ are the matchings $J \in \mathcal{J}$ of dimension $2(a - 1)$, and Theorem O gives $\dim \geq N_q(2a)$. If $0 \notin \mathcal{C}_{-1}$, the ideal is $V_{\{(\emptyset, 0)\}}$ of level $2a$, and Theorem 8.11 with Lemma 8.5 gives the same bound. (For $a = 0$ the block is empty, the ideal is F and $N_q(0) = 1$.) ■

Lemma 9.10 (the block of colour 1 at the prime 2). *Let $p = 2$ and $|\mathcal{C}_1| = 2k'$. Then $\dim_F I_{c,1} \geq N_{q-1}(2k') = N_1(c)$.*

Proof. Here $q = 2^v$, $R_{c,1} = F[t_i : i \in \mathcal{C}_1 \setminus \{0\}]/(t_i^q - 1)$, a group algebra, and for $u = t_i t_l$ in it, $(u - 1)^{q-1} = \varphi_q(u) := 1 + u + \dots + u^{q-1}$ (in $F[u]$, $(u - 1)\varphi_q(u) = u^q - 1 = (u - 1)^q$). For $k' = 0$ the block is empty and both sides are 1.

$0 \in \mathcal{C}_1$. By (6.2), $g_P = (\text{unit}) \cdot (t_{k_0} - 1) \cdot \prod (t_l - 1)\varphi_q(t_i t_l)$, the product over the pairs $\{i < l\}$ of P that avoid 0, where k_0 is the partner of 0. After the increasing relabelling of $\mathcal{C}_1 \setminus \{0\}$ as $\{1, \dots, 2k' - 1\}$, these are exactly the generators $\bar{\psi}_J$ of §2 for the degree q and the dimension $2(k' - 1)$. So $I_{c,1}$ is the ideal of Proposition 9.2 at $(k' - 1, q)$ over F , and that proposition gives $\dim \geq N_{q-1}(2k')$.

$0 \notin \mathcal{C}_1$. Now $g_P = \prod_{\{i < l\} \in P} (t_l - 1)\varphi_q(t_i t_l)$, over the perfect matchings P of the $2k' \geq 2$ indices of $\mathcal{C}_1$; let $\mathcal{M}$ be the ideal they generate. Let $i_1 := \min \mathcal{C}_1$, let H' be the group on the other indices, and write each $f \in R_{c,1}$ as $f = \sum_{j \in \mathcal{Z}/q} t_{i_1}^j f_j$ with $f_j \in F[H']$. The map $\theta : \mathcal{M} \rightarrow F[H']$, $f \mapsto f_0$, is $F[H']$ -linear. If $\{i_1, l\} \in P$, the coefficient of $t_{i_1}^0$ in $\varphi_q(t_{i_1} t_l)$ is 1, and no other factor of g_P contains t_{i_1} ; so $\theta(g_P) = (t_l - 1) \cdot \prod (t_{l'} - 1)\varphi_q(t_{i'} t_{l'})$, the product over the other pairs: the generator of the previous case, with i_1 in the role of 0. So $\theta(\mathcal{M})$ contains the ideal of the previous case in $2k' - 1$ variables, and $\dim \mathcal{M} \geq \dim \theta(\mathcal{M}) \geq N_{q-1}(2k')$. ■

(Version 11 proved in addition that θ is injective on $\mathcal{M}$. No conclusion uses it: the equality block by block is Corollary 9.12(i), which follows from the inequalities alone. The proof printed here is the one that was formalized, §14.8.)

9.5 The theorem

Theorem 9.11 (even degrees). *Let $m \geq 4$ be even and $k \geq 1$. Then $\dim_{F_p} F_p[G]/(\bar{\psi}_J : J \in \mathcal{J}) = m^{2k+1} - Q_k(m)$ for every prime p ; the group $R/(\psi_J : J \in \mathcal{J})$ is free abelian of rank*

$m^{2k+1} - Q_k(m)$; and $H_{2k}(X; Z)/L(X)$ is torsion free for the Fermat variety X of degree m and dimension $2k$.

Proof. Let p be a prime dividing m , $m = q \cdot r'$ as in §9.3. By Lemma 9.4 (Lemma 6.1), Lemma 9.5, Lemmas 9.7–9.10 and Lemma 9.6,

$$\dim_F I = \sum_c \dim \pi_c(I) = \sum_c \dim I_{c,1} \cdot \dim I_{c,-1} \cdot \prod_{\zeta} \dim I_{c,\zeta} \geq \sum_c N_1(c) \cdot N_{-1}(c) \cdot \prod_{\zeta} N_{\zeta}(c) = Q_k(m),$$

the sums over the compatible colourings: the block of colour 1 is Lemma 9.8 if p is odd and Lemma 9.10 if $p = 2$; the block of colour -1 (present only if p is odd) is Lemma 9.9; the pair blocks are Lemma 9.7. (If $r' = 1$, that is, $m = 2^v$, there is one colouring, and the inequality is Proposition 9.2.) With (9.1), $\dim_F I = Q_k(m)$, and dimensions do not change from F_p to F . For $p \nmid m$ the equality of the statement is Theorem 0(b). So $R/(\psi_J : J \in \mathcal{J})$, whose rank is $m^{2k+1} - Q_k(m)$ by Theorem 0(b) at $p = 0$, has no p -torsion for any prime p : it is free. No step of this uses topology. Theorem 0(a) then gives the last assertion. ■

With Corollary 7.7, this proves the Main Theorem and Main Theorem' of §1.2 for every $m \geq 3$.

Corollary 9.12. (i) In the proof of Theorem 9.11 every block has exactly the dimension of its count: $\dim I_{c,1} = N_1(c)$, $\dim I_{c,-1} = N_{-1}(c)$ and $\dim I_{c,\zeta} = N_{\zeta}(c)$ for every compatible colouring c . (ii) For $q = 2^v$, $v \geq 1$, and every $a \geq 0$: $\dim_{\bar{F}_2} I_a^{\text{bal}} = N_{\text{bal}}(a, q)$ and $\dim_{\bar{F}_2} I_a^{\text{ph}} = N_{\text{ph}}(a, q)$. So Corollary 7.8 holds for $p = 2$ as well.

Proof. (i) The sum of the products of the dimensions equals the sum of the products of the counts, each dimension is at least its count, and every count of a compatible colouring is positive. (ii) For $a = 0$ see the proof of Corollary 7.8. For $a \geq 1$ take $m := 3q$, $p = 2$, $r' = 3$, $n := 2a$, and ζ a primitive cube root of unity. Colour a coordinates by ζ , a by ζ^{-1} and one coordinate s by 1: then $c_0 = 1$, $\mathcal{C}_1 = \{0, s\}$, and the pair block is I_a^{bal} . Colour $a + 1$ coordinates by ζ and a by ζ^{-1} : then $c_0 = \zeta^{-1}$, $\mathcal{C}_1 = \emptyset$, and the only block is I_a^{ph} . Apply (i). ■

9.6 Two examples

Example 9.13 (quartics). For $m = 4$ the only prime is 2, $q = 4$, and $r = 3$: the proof is Proposition 9.2 and the elementary Theorem 8.15 over F_2 ; no Pfaffian and no colouring is involved. At $k = 1$: $B = F_2[s_1, s_2, s_3]/(s_i^4)$, the three leading forms are $s_1 s_2 s_3 \cdot (s_a^2 + s_a s_b + s_b^2)$, and the ideal generated by the three polynomials $s_a^2 + s_a s_b + s_b^2$ in $F_2[s_1, s_2, s_3]/(s_i^3)$ has dimension $19 = N_3(4)$ (§8.9). So $\text{rank } L(X) = 20$, the Picard number of the Fermat quartic surface. In general, for the Fermat quartic of dimension $2k$, $L(X)$ is primitive of rank one more than the central trinomial coefficient of $2k + 2$: $20, 142, 1108, 8954, \dots$

Example 9.14 ($k = 1$, $m = 6$). Here $N = 4$, $Q_1(6) = 61$, and both kinds of prime occur. At $p = 3$ ($q = 3$, $r' = 2$) the colours are ± 1 , all 8 colourings are compatible, and there are no pair blocks. At $p = 2$ ($q = 2$, $r' = 3$) the colours are the cube roots of unity, 19 of the 27 colourings are compatible, and every block of colour 1 contributes 1 (Remark 9.3(3)).

$p = 3$: sizes ($ \mathcal{C}_1 , \mathcal{C}_{-1} $)	colourings $\times N_1 \cdot N_{-1}$	$p = 2$: sizes ($ \mathcal{C}_1 , \mathcal{C}_{\zeta} , \mathcal{C}_{\zeta^{-1}} $)	colourings $\times N_1 \cdot N_{\zeta}$
(4, 0)	$1 \times 6 \cdot 1$	(4, 0, 0)	$1 \times 1 \cdot 1$
(2, 2)	$6 \times 2 \cdot 3$	(2, 1, 1)	$12 \times 1 \cdot 2$
(0, 4)	$1 \times 1 \cdot 19$	(0, 2, 2)	$6 \times 1 \cdot 6$

$p = 3$: sizes ($ \mathcal{C}_1 , \mathcal{C}_{-1} $)	colourings $\times N_1 \cdot N_{-1}$	$p = 2$: sizes ($ \mathcal{C}_1 , \mathcal{C}_\zeta , \mathcal{C}_{\zeta^{-1}} $)	colourings $\times N_1 \cdot N_\zeta$
total	$6 + 36 + 19 = 61$	total	$1 + 24 + 36 = 61$

At $p = 3$ the blocks of colour 1 are instances of Theorem B at $q = 3$ ($Q_1(3) = 6$, $Q_0(3) = 2$) and the blocks of colour -1 are instances of Theorem O at $r = 3$ ($N_3(2) = 3$, $N_3(4) = 19$). At $p = 2$ the pair blocks are bipartite ideals with the box 2 ($N_{\text{bal}}(1, 2) = 2$, $N_{\text{bal}}(2, 2) = 6$). (At $k = 1$ the theorem is Degtyarev's [De14]; the example only shows the bookkeeping.)

Remarks 9.15. (1) *What each degree uses.* For $m = 4$: Theorem 8.15 over F_2 . For $m \equiv 2 \pmod{4}$: at the prime 2, Theorem C at the box 2 and Remark 9.3(3); at the odd primes p , Theorems B and C at p^v and Theorem O at $r = p^v$. For $m = 6$ and $m = 12$ every box that occurs is 2, 3 or 4, and the proof uses, of §8, only §8.8. The bordered Pfaffians are first needed at $m = 8$ ($r = 7$) and $m = 10$ ($r = 5$). (2) *The list of boxes.* Theorem 9.11 uses Theorem O — or, in Lemma 9.9 when $0 \notin \mathcal{C}_{-1}$, Theorem 8.11 at the second root $\{(\emptyset, 0)\}$ — exactly at the boxes $r = p^v$ in characteristic p , for the odd primes p with $p^v \parallel m$, and $r = 2^v - 1$ in characteristic 2, if $2^v \parallel m$ with $v \geq 2$. (3) *Subfamilies.* As in §6, the proof uses the product structure of the compatible matchings (Lemma 9.5) and the roots of Lemma 8.5 and Lemma 7.2, which need the full family $\mathcal{J}$; and with one matching removed the dimension of the ideal of Theorem O drops, also over F_2 (§14.9).

10. A different count: Theorem A

For a finite set L of variables over a field F and an odd $q \geq 1$, put $I_q(L) := (e_j(L) : j \text{ odd}) + (x^q : x \in L)$ and

$$N_q(n) := n! \cdot [y^n] e^y I_0(2y)^{(q-1)/2}.$$

Theorem A. *Let F be a field with $\text{char } F \neq 2$, let $q \geq 1$ be odd, and let $|L| = n$. Then $\dim_F F[L]/I_q(L) = N_q(n)$.*

The proof is in Appendix A. The lower bound degenerates the ideal of an explicit finite set of points. The upper bound is an induction on n over a family of ideals $K_\mu(L)$ indexed by partitions μ ; the ideals are built from the coefficients of one generating function, and each inductive step shifts one index in that function. The proof uses the characteristic only through $2 \in F^\times$, and it uses no relation between q and $\text{char } F$.

Corollary 10.1. *Let p be an odd prime and $q = p^v$. For every $k \geq 0$, $A_k(q) := \dim F_p[x_0, \dots, x_{2k+1}]/(E + (x_0^q, \dots, x_{2k+1}^q)) = P_k(q)$, where $P_k(q)$ is the number of points of F_q^{2k+2} at which every odd elementary symmetric polynomial vanishes, i.e. the number of F_q -points of $\bigcup_{J \in \mathcal{J}} V(I_J)$.*

Corollary 10.2. *For every odd q and every n , the finitely generated abelian group $M := Z[x_1, \dots, x_n]/(e_j : j \text{ odd}; x_i^q)$ has rank $N_q(n)$, and its torsion subgroup is a 2-group.*

Remarks 10.3. (1) In characteristic 2 the statement fails: at $n = 4$ the dimensions are 21, 65, 133, 225 for $q = 3, 5, 7, 9$, against $N_q(4) = 19, 61, 127, 217$. (2) For $q = 3$ and all k , Corollary 10.1 was known earlier through Steinberg modules and tilting theory [Jan, II.4.16], [Mat, Theorem 1(1)], [DCP, Theorems 5.6–5.7]; for $k \leq 4$ and all $q = 3^v$ it was known through case-by-case arguments in earlier notes of this project. Theorem A contains all of these, in every characteristic $\neq 2$ and for every odd q . **As a count, however, Theorem A is not new: it follows from a theorem of Kostant in characteristic 0 and from a proposition of**

Bezrukavnikov, Riche and Rider in odd characteristic (Remark 10.4). (3) **Theorem A is not used anywhere in the proof of the Main Theorem, and it does not imply it (§11).**

Remark 10.4 (the centralizer of a regular unipotent element; as a count, Theorem A is not new). Let $q = 2h + 1 \geq 3$, so that $h = (q - 1)/2$ as in §1.9. In this remark and in Remark 10.7 the letters G , T , W , K , ℓ and u have the meaning that they have in the sources quoted, not that of §2 and §11; $\mathcal{Z}$ is the centralizer defined in (1).

(1) *A dictionary.* Let F be a field of characteristic $\neq 2$, and let $V := F[x]/(x^q)$ with the bilinear form $\langle x^a, x^b \rangle := (-1)^a$ if $a + b = q - 1$, and 0 otherwise. The form is nondegenerate, and it is symmetric because $a + b$ is even. Multiplication by x , which we call e , satisfies $\langle eu, v \rangle = -\langle u, ev \rangle$, and it is nilpotent with a single Jordan block. An endomorphism of V that commutes with e is a polynomial $f(e)$, and $f(e)$ preserves the form exactly when $f(e)f(-e) = 1$; the constant term of this identity gives $f(0) = \pm 1$, so the determinant of $f(e)$ is $f(0)^q = f(0)$. So the centralizer of e in $\mathrm{SO}(V) \cong \mathrm{SO}_{2h+1}$ is the commutative unipotent group

$$\mathcal{Z} := \{f(e) : f(e)f(-e) = 1, f(0) = 1\}.$$

For $t \in F$ the Cayley transform $g_t := (1 + te)(1 - te)^{-1}$ lies in $\mathcal{Z}$, and for $t \neq 0$ it has a single Jordan block: it is a regular unipotent element of $\mathrm{SO}(V)$, and $\mathcal{Z}$ is its centralizer. The ring $F[L]/(x^q : x \in L)$ is $V^{\otimes n}$, and $f(e) \in \mathcal{Z}$ acts on it as multiplication by $\prod_{x \in L} f(x)$. In particular g_t acts as $E(t)/E(-t)$, where $E(t) := \prod_{x \in L} (1 + tx) = \sum_j e_j(L)t^j$. Since $E(t) - E(-t) = 2 \sum_{j \text{ odd}} e_j(L)t^j$ and $E(-t)$ is invertible, the elements $E(t)/E(-t) - 1$ lie in the ideal $(e_j(L) : j \text{ odd})$, and when F is infinite they generate it (they are polynomials in t whose coefficients generate it). For a general $f(e) \in \mathcal{Z}$ put $\varphi := 1 + f$; then $\varphi(0) = 2$ is a unit, $f(x) = \varphi(x)/\varphi(-x)$, and $\prod_x f(x) - 1 = (H - H^-)/H^-$ with $H := \prod_x \varphi(x)$ and $H^- := \prod_x \varphi(-x)$. Here $H - H^-$ is twice the sum of the homogeneous components of odd degree of the symmetric polynomial H , and a symmetric polynomial of odd degree lies in $(e_j(L) : j \text{ odd})$. Hence, for F infinite,

$$F[L]/I_q(L) = V^{\otimes n} / \langle (g - 1)v : g \in \mathcal{Z}, v \in V^{\otimes n} \rangle,$$

the coinvariants of the centralizer of a regular unipotent element on the n -th tensor power of the vector representation of SO_{2h+1} . The hypothesis that F is infinite cannot be dropped: over F_3 the coinvariants of the finite group $\mathcal{Z}$ have dimension 9, 27 and 19 at $(q, n) = (3, 3), (3, 4)$ and $(5, 3)$, against 7, 19 and 13 for the ring (§14.5). Over a finite field the statement holds for the centralizer as an algebraic group, that is, after extension of scalars to an infinite field. Since $V^{\otimes n}$ is isomorphic to its dual as a representation of $\mathcal{Z}$, the space of coinvariants has the dimension of the invariants $(V^{\otimes n})^{\mathcal{Z}}$. In characteristic 0 the invariants of $\mathcal{Z}$ are those of its Lie algebra, which has basis $e, e^3, \dots, e^{2h-1}$; e^j acts as multiplication by the power sum $p_j(L)$, and $(p_j(L) : j \text{ odd}) = (e_j(L) : j \text{ odd})$ by Newton's identities.

(2) *Characteristic 0: Kostant's theorem.* Let G be a connected semisimple group over C and W a finite-dimensional rational G -module whose weights lie in the root lattice. Then $x \mapsto \dim W^{\mathfrak{g}^x}$ is constant on the regular elements of $\mathfrak{g}$ [Kos]; we quote the statement from [Gin, Proposition 4.2]. At a regular semisimple x the centralizer $\mathfrak{g}^x$ is a Cartan subalgebra, and $W^{\mathfrak{g}^x}$ is the zero weight space of W . The weights of V are $0, \pm \varepsilon_1, \dots, \pm \varepsilon_h$, which span the root lattice of $\mathfrak{so}_{2h+1}$. So $\dim(V^{\otimes n})^{\mathfrak{g}^e}$ is the dimension of the zero weight space of $V^{\otimes n}$: the number of closed walks of length n on the lattice $\mathbb{Z}^h$ with steps $0, \pm \varepsilon_i$, which is $N_q(n)$. **So in characteristic 0, Theorem A follows from Kostant's theorem and (1).**

(3) *Odd characteristic: a proposition of Bezrukavnikov, Riche and Rider.* Let K be an algebraically closed field of characteristic ℓ , and let G be a connected reductive group over K

with simply connected derived subgroup, such that ℓ is good for G and $X^*(T)/ZR$ has no ℓ -torsion (T a maximal torus, R the roots). Then [BRR, Proposition 2.12]: *for every finite-dimensional G -module W which admits a good filtration and every regular unipotent element $u \in G$, $\dim W^{Z_G(u)} = \dim W^T$.* We read this statement and its proof in the arXiv version of 4 July 2024; the proof rests on the vanishing theorem and the good filtration of [KLT]. Take $G = \text{Spin}_{2h+1}$ and ℓ odd. Then ℓ is good for G (the only bad prime of type B_h , $h \geq 2$, is 2, and type A_1 has none), and $X^*(T)/ZR \cong \mathbb{Z}/2$, so the hypotheses hold. The vector representation V is the Weyl module of highest weight ε_1 ; it is simple for $\ell \neq 2$, hence tilting ([BRR, proof of Lemma 2.13] for $h \geq 2$; for $h = 1$, $G = \text{SL}_2$ and V is the Weyl module of highest weight 2), and a tensor product of modules with a good filtration has a good filtration [Jan, II.4.21], [Mat]. The group scheme $Z_G(u)$ is smooth [BRR, Proposition 2.2], so its invariants are those of its group of K -points. The centre of G acts trivially on V , and the image of $Z_G(u)$ in $\text{SO}(V)$ is the centralizer of the image of u : if $g \in \text{SO}(V)$ commutes with it, a lift $\tilde{g}$ satisfies $\tilde{g}u\tilde{g}^{-1} = \pm u$, and $-u$ is not unipotent. Finally $(V^{\otimes n})^T$ is the zero weight space. So for $F = K$, $\dim F[L]/I_q(L) = \dim (V^{\otimes n})^{\mathbb{Z}} = N_q(n)$; the dimension does not change under extension of scalars, so the same holds over every field of odd characteristic. **So in odd characteristic, too, Theorem A follows from the literature, through (1): from [BRR, Proposition 2.12].** Corollary 10.2 then follows as in Appendix A.8. Version 9 of this paper said: «we do not know a version of Kostant’s theorem in positive characteristic that gives this». There is one; we had not read it. The count of Theorem A should be credited to Kostant in characteristic 0 and to [BRR] in odd characteristic. (Logically, the case of characteristic 0 also follows from the case of one odd prime p : the ring over Q is $M \otimes Q$ for the abelian group M of Corollary 10.2, so its dimension is at most that of $M \otimes F_p$, and Proposition A.5 gives the lower bound. We keep the reference to Kostant, whose theorem is the origin of the statement.) A related paper, [Ric], extends Kostant’s results on the centralizers of regular elements to positive characteristic and to integral coefficients; it describes the centralizer group scheme, and we did not find the count in it (we read its introduction and §2.2, and searched its source). We have not found the dictionary (1), or the statement of Theorem A for this ring, in the literature. For $q = 3$ the statement is the one recalled in Remark 10.3(2).

(4) *What Appendix A contributes.* The proof of Appendix A is a second, independent proof of the count. It is elementary and self-contained: it uses no algebraic groups, no good filtrations and no Frobenius splitting, only $2 \in F^\times$. It also gives slightly more than the count: to every partition μ with at most h parts, read as the dominant weight $\sum \mu_i \varepsilon_i$, it attaches an explicit ideal $K_\mu(L)$, with $K_\emptyset(L) = I_q(L)$, such that $\dim F[L]/K_\mu(L)$ is the multiplicity $N_\mu(n)$ of the weight μ in $V^{\otimes n}$ (Theorem A.15 and Corollary A.17; computed independently at 178 cells, §14.5), and each row of $K_\mu(L \cup z)$ is the ideal of the corresponding neighbouring weight (Theorem A.12 and Corollary A.17). The lower bound (Proposition A.5) is the classical method of degenerating the ideal of a finite set of points (the «orbit harmonics» of [GP]).

(5) *Computed, not claimed.* In the 27 cells (q, n) that we computed ($3 \leq q \leq 13$, $n \leq 9$), the Hilbert series of $F[L]/I_q(L)$ is $\sum_\lambda c_\lambda \cdot t^{mn} m_\lambda^0(t^{-1})$, where λ runs over the irreducible constituents V_λ of $V^{\otimes n}$ in characteristic 0, c_λ is the multiplicity, and m_λ^0 is Lusztig’s t -analogue of the zero weight multiplicity [Lus]; in 56 cases the same holds for the graded character of the symmetric group (pairs of a cell with $q \in \{3, 5\}$, $n \leq 6$ and a cycle type), with the multiplicity spaces in place of the c_λ . In characteristic 0 this is what the theory of generalized exponents and of the Brylinski–Kostant filtration predicts [Bry]; for tilting modules in good characteristic see [Liu]. Of these sources we have read only the introduction of [Liu], and we record the statement as a computation (§14.5).

(6) *Even q .* For even q the form of (1) is alternating, and the same dictionary holds with $\text{Sp}(V) \cong \text{Sp}_q$: the centralizer of the regular unipotent element g_1 is $\{\pm 1\} \times \mathbb{Z}$, and -1 acts on $V^{\otimes n}$ as $(-1)^n$. The group Sp_q is simply connected, every odd prime is good for it, $X^*(T)/ZR \cong \mathbb{Z}/2$,

and V is a simple Weyl module in every characteristic. So for **even** n and every field of characteristic $\neq 2$, [Kos] and [BRR, Proposition 2.12] give

$$\dim F[x_1, \dots, x_n]/(e_1, e_3, \dots; x_1^q, \dots, x_n^q) = n! \cdot [y^n] I_0(2y)^{q/2},$$

the number of closed walks of length n on the lattice $Z^{q/2}$ with steps $\pm \varepsilon_i$. (In characteristic 0 the reference to [Kos] can again be avoided: the dimension over Q is at most the dimension over F_3 , and Proposition 10.5(iii) with Corollary 10.6(i), applied to the odd number $q+1$, gives the lower bound.) Version 9 listed this as an open problem; for even n it is a consequence of the literature. For odd n the zero weight space is 0 and the proposition says nothing about the invariants of $\mathcal{Z}$ alone. In 8 cells (q, n) with $q \in \{2, 4, 6, 8\}$, of both parities of n , the dimension in characteristics 3, 5 and 7 equals the dimension in characteristic 0, and for odd n it is the number of such walks from 0 to ε_1 ; in characteristic 2 it is larger in all 8 cells. The case of odd n is not proved (§15).

Proposition 10.5 (the invariant copairing). *Let F be a field, $r \geq 2$, $N = 2s \geq 2$, and $C_r := F[x_1, \dots, x_N]/(x_1^r, \dots, x_N^r)$. Put $D_r(a, b) := \sum_{u=0}^{r-1} (-1)^u a^u b^{r-1-u}$, and for a perfect matching J of $\{1, \dots, N\}$ put $D_{r,J} := \prod_{\{a,b\} \in J} D_r(x_a, x_b)$ and $I_J := (x_a + x_b : \{a, b\} \in J)$. Then:*

- (i) $(x_a + x_b) \cdot D_r(x_a, x_b) = 0$ in C_r , and $\text{ann}_{C_r}(D_{r,J}) = I_J C_r$;
- (ii) $\dim_F \sum_J D_{r,J} C_r = \dim_F F[x_1, \dots, x_N]/\bigcap_J (I_J + (x_i^r))$;
- (iii) $e_j \cdot D_{r,J} = 0$ for every odd j . So $\sum_J D_{r,J} C_r \subseteq \text{ann}_{C_r}(e_j : j \text{ odd})$, and $\dim_F \sum_J D_{r,J} C_r \leq \dim_F F[x_1, \dots, x_N]/((e_j : j \text{ odd}) + (x_i^r))$.

Proof. (i) The product $(a+b) \cdot \sum_u (-1)^u a^u b^{r-1-u}$ telescopes to $b^r + (-1)^{r-1} a^r$, which is 0 in the box. In $F[a, b]/(a^r, b^r)$, multiplication by $D_r(a, b)$ therefore factors through the quotient by $(a+b)$, which is $F[b]/(b^r)$, of dimension r . The elements $D_r(a, b) \cdot b^i$, $0 \leq i \leq r-1$, are non-zero (the term $u = r-1$ survives) and homogeneous of different degrees, so the image has dimension at least r . Hence the annihilator of $D_r(a, b)$ is exactly $(a+b)$. The ring C_r is the tensor product, over the pairs of J , of such rings, and $D_{r,J}$ is the tensor product of the elements D_r ; the kernel of a tensor product of linear maps is the sum of the kernels in each factor, which gives $\text{ann}(D_{r,J}) = I_J C_r$. (ii) Let $\langle f, g \rangle$ be the coefficient of $\prod_i x_i^{r-1}$ in fg ; as in the proof of Proposition 2.6, the pairing is non-degenerate, $\dim \text{ann}(I) = \dim C_r - \dim I$ for every ideal I , and the annihilator of a sum of ideals is the intersection of their annihilators. So $\dim \sum_J D_{r,J} C_r = \dim C_r - \dim \bigcap_J I_J C_r$. (iii) By (i), $x_a D_{r,J} = -x_b D_{r,J}$ for each pair, so $\prod_i (1 + x_i t) \cdot D_{r,J} = \prod_{\{a,b\} \in J} (1 - x_b^2 t^2) \cdot D_{r,J}$, which is even in t . The last inequality is $\dim \text{ann}(I) = \dim C_r - \dim I$ for $I = (e_j : j \text{ odd}) C_r$. ■

Corollary 10.6 (Theorem B at $2k+2$ variables; both ends of the sandwich). *Let $q \geq 3$ be odd, $k \geq 0$, $N = 2k+2$, and $r = q-1$.*

- (i) For every field F , $\dim_F \sum_J D_{q-1,J} C_{q-1} = Q_k(q)$.
- (ii) Modulo [BRR, Proposition 2.12]: if $\text{char } F \neq 2$, then $\sum_J D_{q-1,J} C_{q-1} = \text{ann}_{C_{q-1}}(e_j : j \text{ odd})$, $\bigcap_J (I_J + (x_i^{q-1})) = (e_j : j \text{ odd}) + (x_i^{q-1})$, and $\dim_F F[x_1, \dots, x_N]/((e_j : j \text{ odd}) + (x_i^{q-1})) = Q_k(q)$. So both inequalities of Proposition 11.1 are equalities.

Proof. (i) Write the variables as $x_0, y_1, \dots, y_{2k+1}$, and let C be the ring of Theorem B in the y_i . Every element f of $\mathcal{M} := \sum_J D_{q-1,J} C_{q-1}$ is killed by $e_1 = x_0 + \sigma$, $\sigma := \sum_i y_i$, by Proposition 10.5(iii). Write $f = \sum_{u=0}^{r-1} x_0^u f_u$ with $f_u \in C$; comparing the coefficients of x_0^u in $x_0 f = -\sigma f$ gives $f_{u-1} = -\sigma f_u$ for $u \geq 1$. So f is determined by f_{r-1} , and the linear map $\theta : \mathcal{M} \rightarrow C$, $f \mapsto f_{r-1}$, is injective. If k_0 is the partner of 0 in J , the coefficient of x_0^{r-1} in $D_{q-1}(x_0, y_{k_0})$ is $(-1)^{r-1}$,

so $\theta(D_{q-1,J} \cdot g) = \pm D_J \cdot g$ for $g \in C$, with D_J as in §2.3. Moreover $x_0 \cdot D_{q-1,J} = -y_{k_0} D_{q-1,J}$, so $\mathcal{M} = \sum_J D_{q-1,J} C$. Hence $\theta(\mathcal{M}) = (D_J : J \in \mathcal{J})C$, and $\dim \mathcal{M} = Q_k(q)$ by Theorem B. (ii) By Proposition 10.5(iii) and (i), $\mathcal{M}$ is a subspace of $\text{ann}(e_j : j \text{ odd})$, of dimension $Q_k(q)$; so $\dim F[x]/((e_j : j \text{ odd}) + (x_i^{q-1})) \geq Q_k(q)$ over every field. If $\text{char } F$ is odd, this dimension is $N! \cdot [y^N] I_0(2y)^{(q-1)/2} = Q_k(q)$ by Remark 10.4(6), which rests on [BRR, Proposition 2.12]. If $\text{char } F = 0$, the ring is obtained by extension of scalars from the finitely generated abelian group $Z[x]/((e_j : j \text{ odd}) + (x_i^{q-1}))$, so its dimension is the rank of this group, which is at most the dimension of its reduction modulo 3, that is, $Q_k(q)$; so [Kos] is not needed. In both cases $\mathcal{M}$ and $\text{ann}(e_j : j \text{ odd})$ have the same dimension, so they are equal. Taking annihilators, $\bigcap_J I_J C_{q-1} = (e_j : j \text{ odd}) C_{q-1}$. ■

Remark 10.7 (what this says). (1) *Invariant tensors.* Let $V_r := F[x]/(x^r)$ with the form $\langle x^a, x^b \rangle = (-1)^a [a + b = r - 1]$, which is symmetric for odd r and alternating for even r . Then $D_r(a, b) = \sum_u x^u \otimes (-1)^u x^{r-1-u}$ is the element of $V_r \otimes V_r$ dual to the form, so every $D_{r,J}$ is a tensor of $V_r^{\otimes N}$ invariant under the whole group of isometries (Sp_r for even r , O_r for odd r). The ring C_r acts on $V_r^{\otimes N}$ through the N commuting copies of e , one in each factor. In these terms, Corollary 10.6 reads: **Theorem B says that the invariant tensors $D_{q-1,J}$ of Sp_{q-1} generate, under the commuting copies of a regular nilpotent element, a space of the dimension of the zero weight space of $V^{\otimes(2k+2)}$, over every field; in characteristic $\neq 2$, and modulo [BRR, Proposition 2.12], that space is the whole space of invariants of the centralizer of a regular unipotent element** (of the centralizer as an algebraic group; equivalently, over an infinite field). By Proposition 2.5 and Theorem 0, for degree p^v and $k \geq 1$, Conjecture 1.2 of [DS] is equivalent to the first half of this statement (the dimension count) over F_p , for Sp_{p^v-1} . We did not find this formulation in the literature, and we do not know whether Theorem B in odd characteristic can be derived from the theory of modules with a good filtration.

(2) *Characteristic 0.* There the equality $\sum_J D_{r,J} C_r = \text{ann}_{C_r}(e_j : j \text{ odd})$ can be derived from classical invariant theory, for both parities of r and even N . We give the argument as a sketch; we have not read its sources in the original, and nothing in this paper uses it. Let G be SO_r for odd r and Sp_r for even r , with Lie algebra $\mathfrak{g}$, and let $W := V_r^{\otimes N}$. By Kostant's theorem the evaluation at a regular nilpotent e maps the G -equivariant polynomial maps $\mathfrak{g} \rightarrow W$ onto the invariants W^{G^e} of the centralizer of e in G [Kos]. These are the invariants of $\mathfrak{g}^e$: for SO_r the group G^e is connected, and for Sp_r it is the product of $\{\pm 1\}$ and a connected group, and -1 acts trivially on W because N is even. By the first fundamental theorem, the equivariant maps $\mathfrak{g} \rightarrow W$ of degree d are spanned by the complete contractions of $V_r^{\otimes N} \otimes \mathfrak{g}^{\otimes d}$ with the form (for odd r , $O_r = \{\pm 1\} \times \text{SO}_r$, and -1 acts trivially on this tensor power, whose degree $N + 2d$ is even; so the invariants of SO_r in it are those of O_r). Evaluated at e , a contraction is a product, over the pairs $\{a, b\}$ of some matching, of elements $x_a^j \cdot D_r(x_a, x_b)$, times traces of powers of e , which vanish. Over the rationals the dimension of $\sum_J D_{r,J} C_r$ is therefore that of the zero weight space; for even r this agrees with Theorem B over $\mathbb{Q}$.

(3) *The odd box.* For odd r the corresponding statement is Theorem O, proved in §8: $\dim_F \sum_J D_{r,J} C_r = N_r(N)$ over every field (Corollary 8.13). Version 10 of this paper stated it as an open problem. With Theorem A it gives the equality of the two ideals in characteristic $\neq 2$ (Corollary 10.8). In characteristic 2 the two ideals differ: their colengths are 19 and 21 at $(r, N) = (3, 4)$. The statement cannot follow from Theorem A by an argument that is valid for subfamilies of matchings: for 14 of the 15 matchings at $r = 3$, $k = 2$, over F_3 , the sum count is 141, the number of points, and the intersection count is 140 (computed in the earlier notes of this project [Rep]; recomputed in §14.9).

Corollary 10.8 (the odd box; both ends of the sandwich). *Let $r \geq 3$ be odd, $k \geq 0$, $N = 2k + 2$, and let F be a field of characteristic $\neq 2$. Then, in the notation of Proposition 10.5,*

$\sum_J D_{r,J} C_r = \text{ann}_{C_r}(e_j : j \text{ odd})$ and $\bigcap_J (I_J + (x_i^r)) = (e_j : j \text{ odd}) + (x_i^r)$,

and both quotients $F[x_1, \dots, x_N] / \bigcap_J (I_J + (x_i^r))$ and $F[x_1, \dots, x_N] / ((e_j : j \text{ odd}) + (x_i^r))$ have dimension $N_r(N)$. In particular, for an odd prime p and $q = p^v$: $\dim F_p[x_0, \dots, x_{2k+1}] / \bigcap_{J \in \mathcal{J}} (I_J + (x_i^q)) = P_k(q) = A_k(q)$.

Proof. By Proposition 10.5(iii), $\sum_J D_{r,J} C_r \subseteq \text{ann}_{C_r}(e_j : j \text{ odd})$, and the dimension of the right-hand side is $\dim F[x] / ((e_j : j \text{ odd}) + (x_i^r)) = N_r(N)$ by Theorem A. By Corollary 8.13 the left-hand side has dimension $N_r(N)$ too; so they are equal. Take annihilators in C_r , with the pairing of the proof of Proposition 10.5(ii), for which $\dim \text{ann}(I) = \dim C_r - \dim I$, so that $\text{ann}(\text{ann}(I)) = I$ for every ideal I : by Proposition 10.5(i), $\text{ann}(\sum_J D_{r,J} C_r) = \bigcap_J I_J C_r$, and $\text{ann}(\text{ann}((e_j : j \text{ odd}) C_r)) = (e_j : j \text{ odd}) C_r$. The last sentence is the case $F = F_p$, $r = q$, with Corollary 10.1. ■

Unlike Corollary 10.6(ii), this does not depend on [BRR]: Theorem A is proved in Appendix A. In the language of Remarks 10.4 and 10.7(1): for odd r and $\text{char } F \neq 2$, the tensors $D_{r,J}$, which are invariant under the orthogonal group of the form on V_r , generate, under the commuting copies of a regular nilpotent element, the whole space of invariants of the centralizer of a regular unipotent element of SO_r in $V_r^{\otimes N}$ (of the centralizer as an algebraic group; equivalently, over an infinite field). And the two counts of §1.6 and §11.1, the sum count $A_k(q)$ and the intersection count at the odd box, do coincide for the full family of matchings; they are both different from Conjecture 1.2 at the degree q , which lives at the even box $q - 1$ (§11), and they are the count of Conjecture 1.2 at the **even** degree $q + 1$ (Lemma 9.1).

11. Why the full family is needed

11.1 Two counts

Let p be an odd prime, $q = p^v$, $S := F_p[x_0, \dots, x_{2k+1}]$, $N = 2k+2$ and $I_J := (x_a + x_b : \{a, b\} \in J)$. The ideal E vanishes on $\bigcup_J V(I_J)$: a point lies there iff its multiset of coordinates is closed under negation iff $\prod_i (1 + x_i t)$ is even in t (unique factorisation in $\bar{F}_p[t]$). By Proposition 2.6, (S) says

$$b_k(q - 1) := \dim S / \bigcap_{J \in \mathcal{J}} (I_J + (x_i^{q-1})) = Q_k(q),$$

an **intersection** at the **even** box $q - 1$, counting the points of the union of the matching spaces on the **zero-free** grid T^N . Corollary 10.1 says $\dim S / (E + (x_i^q)) = P_k(q)$, a **sum** at the **odd** box q , counting points on the grid **with** 0.

Proposition 11.1 (the sandwich). $b_k(q - 1) \leq Q_k(q) \leq \dim S / (E + (x_i^{q-1}))$.

Proof. Dimensions do not change under extension of scalars, so we may work over F_q . Let $\Gamma \subseteq T^N$ be the set of zero-free points of $\bigcup_J V(I_J)$; $|\Gamma| = Q_k(q)$ by Lemma 2.2, and $S/I(\Gamma)$ has dimension $|\Gamma|$. We use Lemma 5.8' (with N variables). The ideal $I'' := E + (x_i^{q-1} - 1)$ is contained in $I(\Gamma)$, and $\text{gr}(I'') \supseteq E + (x_i^{q-1})$ because E is homogeneous; so $\dim S / (E + (x_i^{q-1})) \geq \dim S / \text{gr}(I'') = \dim S / I'' \geq |\Gamma|$, the right-hand inequality. For each J , the ideal of the finite set $V(I_J) \cap T^N$ is $I_J + (x_i^{q-1} - 1)$: modulo I_J one free variable per pair remains, and $x^{q-1} - 1$ is separable with roots exactly T . Its gr contains $I_J + (x_i^{q-1})$, and is equal to it, since both quotients have dimension $(q - 1)^{k+1}$. Finally $I(\Gamma) = \bigcap_J I(V(I_J) \cap T^N)$, and gr of an intersection is contained in the intersection of the gr's, so $\text{gr}(I(\Gamma)) \subseteq \bigcap_J (I_J + (x_i^{q-1}))$, which gives the left-hand inequality. ■

So the Main Theorem is the **left** equality. It is not a consequence of Corollary 10.1, which is an equality of the right-hand kind at a different box. The right-hand inequality is in fact an equality too: it is the analogue of Theorem A at the even box $q - 1$, which follows from [BRR, Proposition 2.12] (Remark 10.4(6)). So the two ideals $\bigcap_J (I_J + (x_i^{q-1}))$ and $E + (x_i^{q-1})$ coincide (Corollary 10.6(ii)). This does not make the Main Theorem a consequence of a count of the kind of Theorem A: the count gives the right-hand equality only, and the equality of the two ideals is what the Main Theorem adds to it.

11.2 A counterexample for subfamilies

Proposition 2.1 and Proposition 2.5 hold for every non-empty $K \subseteq \mathcal{J}$. So, for a subfamily, $L_K(X)$ is primitive iff $\dim(D_J : J \in K)C = |\Gamma_K|$.

Fact 11.2 (computed; not used in any proof). *Let $q = 9$, $k = 2$, and let $K := \mathcal{J} \setminus \{[[0, 1], [2, 3], [4, 5]], [[0, 2], [1, 5], [3, 4]]\}$ (13 of the 15 matchings). Then $\dim(D_J : J \in K)C = 4730 < 4736 = |\Gamma_K|$. So $H_4(X)/L_K(X)$ has 3-torsion for the Fermat fourfold of degree 9. For the same K , the sum-type count holds: with $E_K := \bigcap_{J \in K} I_J$, $\dim S/(E_K + (x_i^9)) = 7089$, which is the number of F_9 -points of $\bigcup_{J \in K} V(I_J)$.*

The value 4730 was obtained by four independent routes (§14): the literal form of [DS] in the ring $F_3[G]$ ($\dim F_3[G]/(\bar{\psi}_J : J \in K) = 54319 = 9^5 - 4730$, against $9^5 - |\Gamma_K| = 54313$), the y -form of §2, the intersection form of Proposition 2.6, and an engine written separately (a kernel basis $D \cdot y_a^i$ per pair, exact rank modulo 3 degree by degree). $|\Gamma_K| = 4736$ was obtained by direct enumeration.

At $q = 3$, $k = 2$, the analogue of (S) fails for 800 of the 32767 non-empty subfamilies (worst deficit 2, e.g. $18 < 20$), while every subfamily satisfies $\leq$. So 3-torsion for subfamilies occurs already for the cubic fourfold.

Consequences.

- Any argument that proves the analogue of (S) for every subfamily proves a false statement. A proof of the Main Theorem must use a property of the full family $\mathcal{J}$; in §5 this property enters at the root (Lemma 5.2), and in §6–§7 through the product structure of the compatible matchings (Proposition 6.5) and the roots of Lemma 7.2.
- $A = P$ cannot imply the Main Theorem through any argument that is valid for subfamilies.
- This is the natural first guess, and it is the error described in §1.8.

12. The integral Hodge conjecture

In this section $k \geq 1$, $n = 2k$, $m \geq 3$, and $X \subset P^{n+1}$ is the Fermat variety of degree m .

12.1 Classical facts

- (H1) **Integral cohomology.** $H^*(X; Z)$ is torsion free and vanishes in odd degrees. By the Lefschetz hyperplane theorem [Mil, §7], $H^{2j}(X; Z) = Z \cdot h^j$ for $2j < n$, where h is the hyperplane class, and $H_{2l}(X; Z) \rightarrow H_{2l}(P^{n+1}; Z) \cong Z$ is an isomorphism for $2l < n$.
- (H2) **Hodge classes.** Through Poincaré duality we call a class in $H_n(X; Z)$ a Hodge class if its dual lies in $H^{k,k}(X)$, and write $\text{Hdg}(X) \subseteq H_n(X; Z)$ for the group of Hodge classes. It is the set of integral classes on which every class of $F^{k+1}H^n(X, C)$ integrates to zero, so it is

a primitive subgroup. The class of an algebraic subvariety of dimension k is a Hodge class, so $L(X) \subseteq \text{Hdg}(X)$. The class P_X of Appendix B, Step 3 (the dual of h^k) is a Hodge class, and $H^n(X; Q) = H_{\text{prim}}^n(X; Q) \oplus Q \cdot h^k$.

- (H3) Characters [SK], [Shi79], [Ran, Proposition 1.7].** Let $\mathfrak{A}$ be the set of $\alpha = (a_0, \dots, a_{n+1}) \in (Z/m \setminus \{0\})^{n+2}$ with $a_0 + \dots + a_{n+1} = 0$, and for $\alpha \in \mathfrak{A}$ put $|\alpha| := \sum_i \langle a_i \rangle / m$, where $\langle a \rangle \in \{1, \dots, m-1\}$ is the representative of a . Under the action of μ_m^{n+2} on the coordinates, $H_{\text{prim}}^n(X; C) = \bigoplus_{\alpha \in \mathfrak{A}} V(\alpha)$ with every $V(\alpha)$ of dimension one, and $(H^{k,k}(X) \cap H_{\text{prim}}^n(X; Q)) \otimes C = \bigoplus_{\alpha \in \mathfrak{B}} V(\alpha)$, where $\mathfrak{B} := \{\alpha \in \mathfrak{A} : |t\alpha| = k+1 \text{ for every } t \in (Z/m)^\times\}$ is the set of **Hodge characters**. So $\text{rank Hdg}(X) = |\mathfrak{B}| + 1$. An element $\alpha \in \mathfrak{A}$ is of **pair type** if the multiset $\{a_0, \dots, a_{n+1}\}$ splits into pairs $\{a, -a\}$; we write $\mathfrak{D} \subseteq \mathfrak{A}$ for the set of these.
- (H4) Prime degree [Ran, Proposition 1.8(i)], based on [KO].** If m is prime, every Hodge character is of pair type. We include a short proof, so that (H4) does not depend on [Ran] or [KO].
- **(H4') Degree 4.** If $m = 4$, every Hodge character is of pair type. The proof is three lines, given below; it is also the case $m = 4$ of (H5).
- (H5) Aoki's theorem [Aok, Theorem A, p. 24].** $\mathfrak{B} = \mathfrak{D}$ if and only if m is a prime or 4, or every prime divisor of m is greater than $n+2$. (Aoki's sets $\mathfrak{A}_m^n, \mathfrak{B}_m^n, \mathfrak{D}_m^n$ [Aok, §0] are the sets $\mathfrak{A}, \mathfrak{B}, \mathfrak{D}$ above, with $a_i \in \{1, \dots, m-1\}$ and $\sum a_i \equiv 0 \pmod{m}$; the proof of his Theorem A is in [Aok, §7], pp. 41–43, and the erratum [Aok] concerns only his Theorem B.) For odd m and even n , «greater than $n+2$ » means «at least $2k+3$ ». For even m and $n \geq 2$, the conditions hold only for $m = 4$.

Proof of (H4). Let $m = p$ and $\alpha \in \mathfrak{B}$, and for $c \in F_p^\times$ let $N(c)$ be the number of i with $a_i = c$. Then $|t\alpha| = \sum_c N(c) \langle tc \rangle / p = k+1$ for every $t \in F_p^\times$. Let χ be an odd character of $F_p^\times$, that is, $\chi(-1) = -1$. Multiply by $\chi(t)$ and sum over t . The constant contributes 0, and the substitution $u = tc$ gives $B_{1,\chi} \cdot \sum_c N(c) \bar{\chi}(c) = 0$, where $B_{1,\chi} = (1/p) \sum_{u=1}^{p-1} \chi(u)u$. An odd character is non-principal, hence primitive with conductor p since p is prime; so $B_{1,\chi} \neq 0$, by the classical formula $L(1, \bar{\chi}) = \pi i \tau(\bar{\chi}) B_{1,\chi} / p$ together with $L(1, \bar{\chi}) \neq 0$ [Was, Theorem 4.9]. Hence $\sum_c N(c) \bar{\chi}(c) = 0$ for every odd χ . The function $f(c) = N(c) - N(-c)$ is odd, so $\sum_c f(c) \bar{\chi}(c)$ equals $2 \sum_c N(c) \bar{\chi}(c) = 0$ for odd χ , and vanishes trivially for even χ . By Fourier inversion on $F_p^\times$, $f = 0$. Since p is odd, $c \neq -c$, and the entries split into pairs $\{c, -c\}$. ■ (We also checked numerically that $B_{1,\chi} \neq 0$ for all 2090 odd characters of the odd primes $p < 200$.)

Proof of (H4'). Let $m = 4$, $\alpha \in \mathfrak{B}$, and let $N(c)$ be the number of i with $a_i = c$, for $c = 1, 2, 3$. Then $N(1) + N(2) + N(3) = 2k+2$ and $|\alpha| = (N(1) + 2N(2) + 3N(3))/4 = k+1$. Subtracting twice the first equation from four times the second, $N(3) - N(1) = 0$. Then $N(2) = 2k+2 - 2N(1)$ is even. So the entries split into pairs $\{1, 3\}$ and $\{2, 2\}$. ■

12.2 Pair-type characters

Lemma 12.1. (i) Every pair-type $\alpha \in \mathfrak{A}$ is a Hodge character: $\mathfrak{D} \subseteq \mathfrak{B}$. (ii) $|\mathfrak{D}| = Q_k(m)$.

Proof. (i) For $t \in (Z/m)^\times$ and $a \neq 0$, $ta \neq 0$ and $\langle ta \rangle + \langle -ta \rangle = m$. Summing over the $k+1$ pairs, $|t\alpha| = k+1$. (ii) Identify Z/m with μ_m by $a \mapsto e^{2\pi i a/m}$. The pair-type elements of $\mathfrak{A}$ become the N -tuples in $\mu_m \setminus \{1\}$ that split into pairs of inverse entries; the condition $\sum a_i = 0$ is then automatic. By Lemma 2.2 for odd m and Lemma 9.1 for even m , there are $Q_k(m)$ of them. ■

12.3 Proof of Corollary H

By (H3), (H2), Theorem 0(c) and Lemmas 2.2, 9.1 and 12.1, $\text{rank Hdg}(X) = |\mathfrak{B}| + 1$ and $\text{rank } L(X) = |\Gamma_{\mathcal{J}}| + 1 = |\mathfrak{D}| + 1$, with $L(X) \subseteq \text{Hdg}(X)$ and $\mathfrak{D} \subseteq \mathfrak{B}$.

(ii). $\text{Hdg}(X)/L(X)$ is a subgroup of $H_n(X; Z)/L(X)$, which is finitely generated and torsion free by the Main Theorem; so $\text{Hdg}(X)/L(X)$ is free, of rank $|\mathfrak{B}| - |\mathfrak{D}| = |\mathfrak{B}| - Q_k(m)$. It is zero iff $\mathfrak{B} = \mathfrak{D}$, which by (H5) happens iff m is prime, or $m = 4$, or every prime factor of m is at least $2k + 3$. (For prime m and for $m = 4$, (H4) and (H4') give $\mathfrak{B} = \mathfrak{D}$ without appeal to [Aok].)

(i). Under the hypothesis of (i), $\text{Hdg}(X) = L(X)$ by (ii). (Only the primitivity of $L(X)$ is used here; that $\text{Hdg}(X)$ is primitive is not needed.) For the other degrees, by (H1) (the Lefschetz hyperplane theorem) and Poincaré duality: odd degrees vanish; for $2j < n$, $H^{2j}(X; Z)$ is generated by h^j , the class of the intersection of X with j general hyperplanes; for $2j > n$, $H^{2j}(X; Z) \cong H_{2l}(X; Z) \cong Z$ with $l = n - j < k$, and it is generated by the class of any linear subspace $P^l \subseteq X$, whose image in $H_{2l}(P^{n+1}; Z)$ is a generator. Such subspaces exist, since X contains the k -spaces $L_{J,\beta}$. So every integral Hodge class of X , in every degree, is the class of an algebraic cycle with integer coefficients. ■

Remark 12.2. (1) Under the hypothesis of (i), Corollary H says more than the integral Hodge conjecture for X : the integral Hodge classes of middle degree are generated by the $(2k+1)!! \cdot m^{k+1}$ standard k -spaces alone. (2) In the same degrees, the elementary divisors and the discriminant of the lattice of integral Hodge classes of middle degree, computed in [AMV] for small (n, m) , are those of the lattice generated by the standard spaces. For $k = 1$ and $m = p \geq 5$ prime, closed forms are given by the author's *Watermark* and *Double Ladder* theorems [WDL], which are cited and not proved here (both are proved for every such prime and verified in Lean 4 in [WDL]; they have not been refereed): $|\text{disc}| = p^{3(p-3)^2}$, and the discriminant group is $(Z/p)^{3p^2-24p+59} \times (Z/p^2)^{3p-16}$ for $p \geq 7$ and $(Z/5)^{10} \times Z/25$ for $p = 5$. They agree with the surface rows $m = 5, 7, 11, 13$ of [AMV, Table 1]. For $k \geq 2$ and $m = p$ prime, the sequel note [WED] gives a formula for $|\text{disc Hdg}(X)|$ through the Hilbert function of the ring of Theorem A at the even box $p - 1$, modulo [BRR, Proposition 2.12] (without it, as a lower bound); the elementary divisors are open (§15).

Remark 12.3 (the degrees excluded by (i)). When m is neither prime nor 4 and has a prime factor $p \leq 2k + 1$, Corollary H(ii) says that $L(X)$ is a primitive sublattice of $\text{Hdg}(X)$ of corank $|\mathfrak{B}| - Q_k(m) > 0$, so the standard linear cycles do not generate the integral Hodge classes, and other algebraic cycles would be needed (for $k = 1$ they exist, by the Lefschetz (1, 1) theorem); we do not claim that any particular construction supplies them. Counting $\mathfrak{B}$ directly (§14), $|\mathfrak{B}| - Q_k(m)$ is 48, 2880 and 152880 for $m = 9$ and $k = 1, 2, 3$; it is 192 for $(k, m) = (1, 27)$, 624 for $(1, 81)$, 288 for $(1, 15)$, 432 for $(1, 21)$, 528 for $(1, 45)$, 2880 for $(2, 25)$, 4320 for $(2, 35)$ and 45360 for $(2, 15)$; and it is 0 for $(k, m) = (1, 25), (1, 35), (1, 49), (1, 55), (1, 77), (1, 121)$, as (H5) predicts. For even m : $|\mathfrak{B}| - Q_k(m)$ is 24, 750 and 19432 for $m = 6$ and $k = 1, 2, 3$; 48, 2580 and 116592 for $m = 8$; 144 and 12120 for $m = 10$ and $k = 1, 2$; 312 and 37890 for $m = 12$; and it is 0 for $m = 4$ and $k \leq 5$, as (H4') says. (At $k = 1$ the ranks $|\mathfrak{B}| + 1$ are 20, 86, 176, 362, 644 for $m = 4, 6, 8, 10, 12$, the Picard numbers of these Fermat surfaces.) For $m = 9$ the count has a closed form.

Lemma 12.4 ($m = 9$). *For $m = 9$ and every $k \geq 1$, $|\mathfrak{B}| = C(2k + 2, k + 1)^3$. Hence $\text{Hdg}(X)/L(X)$ is free of rank $C(2k + 2, k + 1)^3 - Q_k(9)$ (48, 2880, 152880, 8064000 for $k = 1, 2, 3, 4$).*

Proof. Since $(Z/9)^\times = \{\pm 1, \pm 2, \pm 4\}$ and $\langle -x \rangle = 9 - \langle x \rangle$, the condition $|t\alpha| = k + 1$ for t implies it for $-t$, and $\alpha \in \mathfrak{A}$ is a Hodge character iff $\sum_i \delta(a_i) = 0$, where $\delta(a) := (2\langle a \rangle - 9, 2\langle 2a \rangle - 9, 2\langle 4a \rangle - 9) \in Z^3$ (note $\sum_i 9 = 9N = 18(k + 1)$). Let $s(a) \in \{\pm 1\}^3$ be the vector of signs of $\delta(a)$. Then $\delta(1) = (-7, -5, -1)$, $\delta(2) = (-5, -1, 7)$, $\delta(4) = (-1, 7, 5)$, $\delta(3) = (-3, 3, -3)$, and

$\delta(-a) = -\delta(a)$; so $a \mapsto s(a)$ is a bijection from $Z/9 \setminus \{0\}$ onto $\{\pm 1\}^3$, and $\delta(a) = M \cdot s(a)$ for the matrix M with rows $(4, 2, 1)$, $(-1, 4, 2)$, $(-2, -1, 4)$ (check on $a = 1, 2, 4, 3$, then use $\delta(-a) = -\delta(a)$). As $\det M = 81 \neq 0$, $\sum_i \delta(a_i) = 0$ iff $\sum_i s(a_i) = 0$ in Z^3 , i.e. iff each of the three coordinates of the sign vectors is balanced over the N entries. The condition $\sum a_i = 0$ follows from $\sum \langle a_i \rangle = 9(k+1)$. So $|\mathfrak{B}|$ is the number of N -tuples of sign vectors with three balanced coordinates, $C(N, N/2)^3$. $\blacksquare$

(The direct counts 216, 8000, 343000 at $k = 1, 2, 3$ suggested the lemma; the direct count at $k = 4$, 16003008 = 252^3 , agrees with it, §14.)

13. Partial Fermat varieties

In this section $m \geq 3$ and $0 \leq s \leq d$. We prove Corollary W of §1.4. For $d = 0$ both statements are trivial (X and W_0 are sets of m points), so let $d \geq 1$.

Proof of Corollary W(ii). Let X be the Fermat variety of dimension $2d$, $R = Z[t_1, \dots, t_{2d+1}]/(t_i^m - 1)$, and $K := \mathcal{J}(s, d)$. A matching $J \in K$ is $J = J' \sqcup \{\{2i, 2i+1\} : s < i \leq d\}$ with J' a matching of $\{0, \dots, 2s+1\}$, and $J' \mapsto J$ is a bijection from $\mathcal{J}$ in dimension $2s$ onto K . By §2,

$$\psi_J = \psi_{J'} \cdot \prod_{i=s+1}^d g_i, \quad g_i := (t_{2i+1} - 1) \cdot \varphi(t_{2i}t_{2i+1}),$$

where $\psi_{J'}$ is the generator of [DS] in dimension $2s$, a polynomial in $t_1, \dots, t_{2s+1}$. Let p be a prime and $F := F_p$. The ring $R \otimes F$ is the tensor product of $F[t_1, \dots, t_{2s+1}]/(t_i^m - 1)$ and the rings $F[t_{2i}, t_{2i+1}]/(t_{2i}^m - 1, t_{2i+1}^m - 1)$, $i > s$. By Lemma 6.4 (which holds over any field), the ideal generated by the ψ_J , $J \in K$, is $I_{2s} \otimes \otimes_{i>s} (\bar{g}_i)$, where I_{2s} is the ideal of Conjecture 1.2 in dimension $2s$, and its dimension is the product of the dimensions. In $F[t_{2i}, t_{2i+1}]/(t^m - 1)$, put $u := t_{2i}t_{2i+1}$; the ring is $F[u, t_{2i+1}]/(u^m - 1, t_{2i+1}^m - 1)$, and $\bar{g}_i = (t_{2i+1} - 1) \cdot \varphi(u)$. The ideal $(\varphi(u))$ of $F[u]/(u^m - 1)$ is the line spanned by $\varphi(u)$, since $u\varphi(u) = \varphi(u)$; the ideal $(t - 1)$ of $F[t]/(t^m - 1)$ has dimension $m - 1$. By Lemma 6.4 again, $\dim(\bar{g}_i) = m - 1$, over every field. Hence

$$\dim_{F_p}(\bar{\psi}_J : J \in K) = \dim_{F_p} I_{2s} \cdot (m - 1)^{d-s}.$$

By the Main Theorem in dimension $2s$ and Proposition 2.1, $\dim_{F_p} I_{2s} = |\Gamma_{\mathcal{J}}^{(2s)}| = Q_s(m)$ for every prime p dividing m (for $s = 0$, $I_0 = (t_1 - 1)$ has dimension $m - 1 = Q_0(m)$ directly). On the other hand $|\Gamma_K| = Q_s(m)(m - 1)^{d-s}$: by [DS, Definition 1.3], a tuple $(a_1, \dots, a_{2d+1})$ lies in Γ_K iff $(a_1, \dots, a_{2s+1}) \in \Gamma_{\mathcal{J}}^{(2s)}$ and each pair (a_{2i}, a_{2i+1}) , $i > s$, is (a, a^{-1}) with $a \neq 1$. So $\dim_{F_p}(\bar{\psi}_J : J \in K) = |\Gamma_K|$ at every $p|m$, and by Proposition 2.1 (which holds for every non-empty $K \subseteq \mathcal{J}$) $H_{2d}(X)/L_K(X)$ is torsion free. Its rank is $|\Gamma_K| + 1$ by Theorem 0(c). $\blacksquare$

Proof of Corollary W(i). Consider the family of hypersurfaces $f_0(z_0, z_1) + \dots + f_d(z_{2d}, z_{2d+1}) = 0$ with $f_0 = \dots = f_s = x^m + y^m$ and $f_{s+1}, \dots, f_d$ binary forms of degree m without repeated factors. By Euler's identity its members are smooth; its parameter space is the complement of a discriminant hypersurface in an affine space, hence connected; it contains X (all $f_i = x^m + y^m$) and W_s ; and along it the m roots of each f_i , $i > s$, move continuously. The path must stay in this subfamily: the spaces $L_{J,\beta}$ whose first $2s+2$ coordinates are paired by a matching other than $\{0, 1\}, \dots, \{2s, 2s+1\}$ involve $f_0, \dots, f_s$ and need not deform if these forms move. By [DS, §4.6], along such a path from the Fermat variety X to W_s , the subspaces $L_{J,\beta}$ with $J \in \mathcal{J}(s, d)$ deform to the d -spaces of W_s , and parallel transport (constant with respect to

the Gauss–Manin connection) carries $L_{\mathcal{J}(s,d)}(X)$ onto the subgroup of $H_{2d}(W_s; Z)$ generated by these d -spaces; transport preserves rank and primitivity. So (i) follows from (ii), with the same rank $Q_s(m)(m-1)^{d-s} + 1$. ([DS, §4.6] reach the same point through the module $\bar{\mathcal{M}}_{\mathcal{J}_s}(2d) = \bar{\mathcal{M}}_{\mathcal{J}(2s)}(2s) \otimes_Z \bar{S}(s, d)$ of their Theorem 1.1(d), which is free «if and only if Conjecture 1.2 holds for Fermat varieties of dimension $2s$ ».) ■

Remarks 13.1. (1) We have read the argument of [DS, §4.6] in the original and made the choice of the path explicit, but we have not re-derived the transport statement (the continuity of the family of subspaces and the invariance of primitivity under parallel transport), on which Corollary W(i) depends; part (ii) is proved above from Theorem 0, Proposition 2.1, Lemma 6.4 and the Main Theorem. (2) The rank in (ii), $Q_s(m)(m-1)^{d-s} + 1$, was also checked by enumerating Γ_K from [DS, Definition 1.3] at $m = 3, 5$ and $d \leq 3$ (14 cells; the enumeration is in the repository [Rep]). (3) We make no claim about the Hodge classes of W_s : its rational Hodge classes are not computed here, so Corollary W is a primitivity statement only.

14. Verification record

No step of the proofs of the Main Theorem, Theorem B, Theorem C, Theorem O or Theorem A uses a computer. The computations below are corroboration: a proof that has never been confronted with data has not been tested. Every run was made inside a memory and time watchdog. All engines and logs are in the repository [Rep]. Main Theorem' and Theorem O have, in addition, been verified by a proof assistant for every degree (§14.8). The computations for the odd box and the even degrees are in §14.9.

14.1 Direct computations of (S)

(k, q) , field	$Q_k(q)$	graded ranks of $(D_J)C$ from degree $k(q-2)$	independent engines
$(1, 3), F_3$	6	2, 3, 1	5 (sum form; literal t -form; y -form; intersection form; rank engine)
$(2, 3), F_3$	20	5, 9, 5, 1	5
$(3, 3), F_3$	70	14, 28, 20, 7, 1	6
$(4, 3), F_3$	252	42, 90, 75, 35, 9, 1	4
$(5, 3), F_3$	924	132, 297, 275, 154, 54, 11, 1	4
$(6, 3), F_3$	3 432	429, 1001, 1001, 637, 273, 77, 13, 1	3
$(1, 9), F_3$	168	3, 6, 9, 12, 15, 18, 20, 21, 18, 15, 12, 9, 6, 3, 1	5
$(2, 9), F_3$	5 120	15, 45, 90, 150, 224, 310, 395, 470, 515, 530, 516, 475, 411, 329, 245, 170, 110, 65, 34, 15, 5, 1	5
$(1, 27), F_3$	1 950	3, 6, ..., 72, 74, 75, 72, ..., 3, 1	4
$(3, 9), F_3$	190 120	—	1
$(1, 5), F_5$	36	—	3, and the literal form of [DS]
$(2, 5), F_5$	400	—	3, and the literal form of [DS]
$(3, 5), F_5$	4 900	—	3
$(1, 25), F_5$	1 656	—	3

(k, q) , field	$Q_k(q)$	graded ranks of $(D_J)C$ from degree $k(q-2)$	independent engines
$(2, 25), F_5$	182 400	—	1
$(1, 125), F_5$	45 756	—	1
$(1, 7), F_7$	90	—	3, and the literal form of [DS]
$(2, 7), F_7$	1 860	—	3
$(1, 49), F_7$	6 768	—	2
$(3, 7), F_7$	44 730	—	1
$(2, 11), F_{11}$	10 900	—	1
$(2, 13), F_{13}$	19 920	—	1

The literal form of [DS] (the ring $F_p[t]/(t_i^q - 1)$ modulo the $\bar{\psi}_J$) gives $q^{2k+1} - Q_k(q)$: 21, 223, 2117 at $(1, 3), (2, 3), (3, 3)$ over F_3 , and 89, 2725, 253 at $(1, 5), (2, 5), (1, 7)$ over F_5, F_5, F_7 . The cell $(2, 25)$ is the Fermat fourfold of degree 25, which lies outside the range computed in [DS]. The cell $(3, 9)$ was computed in May 2026, four months before the proof existed, as the F_3 -rank 190120 of the generators ρ_J of [DS, §5] in their ring $\bar{R} = F_3[t_1, \dots, t_7]/(\varphi(t_i))$; in the same line of work, the cell $(5, 3)$ gave $1124 = 2^{11} - 924$ for the quotient of $\bar{R}$. Equality was also measured over fields whose characteristic is not the one attached to q : at $q = 5$ over F_3 and $q = 9$ over F_5 , which Theorem 5.9 covers, and at $q = 7$ over F_3 , where $3|q-1$; these are instances of Theorem 5.9'. Over Z , the integer Smith normal form of the literal ring $A_{\mathcal{J}} = R/(\psi_J)$ has no torsion and rank $q^{2k+1} - Q_k(q)$ at five cells, and the quotient $C_Z/V_{\Lambda, Z}$ of Theorem 5.9' is free of rank $(q-1)^m - |Z_{\Lambda}|$ at the root for $(k, q) = (1, 5), (1, 7), (2, 3), (1, 9)$ and for every down-set at $(q, m) = (5, 3), (7, 3), (9, 3), (5, 4)$. For composite odd q (Theorem B is a statement about every odd q), it was confirmed at $k = 1$ for $q = 15, 21, 45$ over several fields. The degrees m of the Main Theorem that are not prime powers are treated in §14.3.

14.2 The ingredients of §5

- **Every down-set, pure combinatorics.** All $\preceq$ -down-sets of Par_m (not a sample) at $(q, m) = (3; 4, 6, 8, 12), (9; 3, \dots, 11), (27; 4, 5, 8, 9), (81; 4, 7), (243; 6)$, up to 940 down-sets per cell: P1, P2 and P3 hold, with 0 failures. The counts $\#\{M : \lambda(M) = \lambda\}$ were obtained by a class-by-class recursion, a route different from the fibres, with the check $\Sigma_{\lambda} = (q-1)^m$. P1 and (5.1) were also checked by brute force over all tails at seven cells up to $(27, 4)$ (238257 tests), and P2 on all comparable pairs with h up to 60 and $m \leq 12$.
- **Every down-set, algebra.** $\dim V_{\Lambda} = |Z_{\Lambda}|$ for every down-set at $(q, m) = (3, 4), (3, 5), (3, 6), (9, 2), (9, 3), (9, 4)$ over F_3 (at $(9, 4)$: 0, 168, 1896, 2216, 2280, 2600, 3752, 3896, 4088, 4096), at $(27, 3)$ and $(81, 2)$, and at $q = 5$ and $q = 7$ over F_3, F_5, F_7 . The membership of every generator of every layer in its slice (Proposition 5.8) was checked at $(3, 3), (9, 3), (9, 4), (27, 2), (27, 3), (81, 2)$.
- **Theorem 5.9, its two ingredients.** The evaluation of D on $T \times T$ over F_5, F_7 and F_9 , and the support statement (a non-zero pattern of λ at M forces $\lambda(M) \preceq \lambda$, and the pattern of $\lambda(M)$ is non-zero at M) on every $M \in T^m$ for $(q, m) = (5, 3), (5, 4), (7, 3), (9, 3), (9, 4)$: 0 failures.
- **Theorem 5.9'.** $\dim V_{\Lambda} = |Z_{\Lambda}|$ for every down-set at $(q, p, m) = (5, 2, 3), (5, 2, 4), (7, 2, 3), (7, 3, 3), (7, 2, 4), (9, 2, 3)$, all with $p|q-1$ (34 down-sets, 0 failures); a second reader measured equality at 42 (cell, characteristic) pairs with $\text{char } F|q-1$. The graded dimensions of $(D_J)C_F$ at $(q, 2k+1) = (5, 3), (7, 3), (5, 5)$ coincide for $\text{char } F = 2, 3, 5, 7, 10007$ (totals 36, 90, 400).

- **Hodge characters (§12).** The sets $\mathfrak{B}$ were counted by enumerating multisets at 19 cells (m, n) , and again, with a separate program, at the cells of Remark 12.3. For the ten cells with m prime — $(3, 2), (5, 2), (7, 2), (3, 4), (5, 4), (7, 4), (11, 4), (3, 6), (5, 6), (3, 8)$ — $|\mathfrak{B}|$ equals the number of pair-type characters, $Q_k(m)$. For prime powers the numbers are those of Remark 12.3, and no pair-type character failed to be a Hodge character (Lemma 12.1(i)). At $(k, m) = (1, 35), (1, 55), (1, 77)$, and at the prime cells $(k, m) = (3, 7), (3, 11), (2, 13)$, $|\mathfrak{B}| = Q_k(m)$, and at $(1, 15), (1, 21), (1, 45), (2, 15), (2, 35)$, $|\mathfrak{B}| > Q_k(m)$, as (H5) predicts. For $m = 9$ the direct counts are 216, 8000, 343000, 16003008 for $k = 1, \dots, 4$ (Lemma 12.4).
- **Negative controls, which fire as they should.** Counting one copy of $\mu \sqcup 1$ per empty class instead of two gives 27 failures of P1 and 61 of P2 at $(9, 6)$. Tightening P3 by one slice gives 604 failures at $(9, 7)$ and fails at every tested cell with $m \geq 2$. In characteristic 2, Theorem A fails in 8 of 12 cells.
- **The cubic case.** The ballot basis of Theorem 4.1 was recomputed as the set of lexicographic leading monomials for $k \leq 7$ (certificate) and $k \leq 6$ (echelon form), and the Specht identification of Remark 4.2(3) at $N = 4, 6, 8$.

14.3 Degrees that are not prime powers

Two engines were used, written separately: the constructor's (numpy, incremental echelon forms) and the auditor's (Singular). The auditor's predictions were computed from the closed forms and recorded before each run.

- **The literal ring of [DS], $k = 1$.** $\dim_{F_p} F_p[t_1, t_2, t_3]/(t_i^m - 1, \bar{\psi}_J) = m^3 - Q_1(m)$ at $m = 15, 21, 33, 35, 39, 45, 55$, each over both primes dividing m (14 runs), and at $m = 15, 21$ over F_3, F_5, F_{31} and F_3, F_7, F_{43} by the other engine. At $k = 1$ this is Degtyarev's theorem [De14]; the runs check our conventions for ψ_J at composite m .
- **The Fermat fourfolds of degree 15 and 21.** For every colouring $c \in \mu_r^5$ the ideal generated by the images of the literal generators ψ_J in R_c was computed directly, over a field containing μ_r ; this uses only Lemma 6.1. At $(k, m) = (2, 15)$ the sum over the colourings is $32900 = Q_2(15)$ both at $p = 3$ (over F_{81} , 3125 colourings, 1001 with non-zero image) and at $p = 5$ (over F_{25} , 243 colourings, 141 with non-zero image). At $(2, 21)$ it is $102800 = Q_2(21)$ at $p = 3$ (over F_{729} , 16807 colourings, 3301 with non-zero image) and at $p = 7$ (over F_7 , 243 colourings, 141 with non-zero image). So $H_4(X; Z)/L(X)$ is torsion free for these two fourfolds, independently of §6–§7. They lie outside the range of [DS, §5]. The author's earlier computations [Rep] had decided the characteristic-5 half of the degree-15 fourfold and had stopped on the characteristic-3 half at a memory limit. At $k = 1$ the colourings with non-zero image are exactly the compatible colourings (61 and 19 at $m = 15, 19$ at $(21, 7)$).
- **The ingredients of §6.** Lemma 6.8 (the count factors) was checked by enumerating $\Gamma_{\mathcal{J}}$ at $(m, n) = (15, 2), (21, 2), (45, 2), (15, 4)$ against the sums of products of block counts, for both primes of each m (8 sums), and Proposition 6.5 with Lemmas 6.6–6.7 by computing every block ideal directly at $(15; 3, 5)$ and $(21; 3, 7)$, $k = 1$: incompatible colourings give the zero ideal, and each compatible colouring gives exactly its block count.
- **Main Theorem' at $k = 1$, every characteristic.** In the literal ring $F_p[t_1, t_2, t_3]/(t_i^m - 1)$, the quotient by the $\bar{\psi}_J$ has dimension $m^3 - Q_1(m)$ for $m = 3, 5, 7, 9$ over F_2 and over primes dividing and not dividing m (12 cells, a third engine).
- **Controls.** The literal engine gives $5120 = Q_2(9)$ at $(k, m) = (2, 9)$, and it detects torsion when there is torsion: for the subfamily of Fact 11.2 it gives $4730 < 4736 = |\Gamma_K|$.

- **Corollary W(ii).** In the literal ring at $(d, s) = (2, 1)$, with the three matchings containing $\{4, 5\}$, the ideal has dimension $144 = Q_1(5) \cdot 4$ at $m = 5$ and $1344 = Q_1(9) \cdot 8$ at $m = 9$, the values of §13.

14.4 The bipartite count

- **The roots (Theorem C).** Over F_p , $\dim I_a^{\text{bal}} = N_{\text{bal}}(a, q)$ at the 18 cells $(a, q) = (1, 3), \dots, (5, 3), (2, 5), (3, 5), (4, 5), (2, 7), (3, 7), (2, 9), (3, 9), (2, 11), (2, 13), (1, 25), (2, 25), (1, 27), (2, 27)$, and $\dim I_a^{\text{ph}} = N_{\text{ph}}(a, q)$ at the 14 cells $(1, 3), \dots, (4, 3), (1, 5), (2, 5), (3, 5), (2, 7), (1, 9), (2, 9), (2, 11), (2, 13), (1, 25), (1, 27)$; for instance $\dim I_5^{\text{bal}} = \dim I_4^{\text{ph}} = 4653$ at $q = 3$, $\dim I_4^{\text{bal}} = 7885$ at $q = 5$, and $\dim I_2^{\text{ph}} = 11713$ at $q = 13$. Twelve of these cells are new to this record, and their values were predicted before they were computed. In the 9 pairs measured, the graded ranks of I_a^{ph} and I_{a+1}^{bal} coincide after a shift of $q - 1$ (Remark 7.9(3)).
- **Theorem 7.6, every down-set.** $\dim V_\Lambda = |Z_\Lambda|$ for every down-set $\Lambda \subseteq \text{BPar}_q(\alpha, \beta)$ (equality, not only $\geq$) at the 18 cells $(\alpha, \beta, q) = (1, 1, 3), (2, 1, 3), (2, 2, 3), (3, 2, 3), (3, 3, 3), (4, 3, 3), (4, 4, 3), (5, 4, 3), (2, 1, 5), (2, 2, 5), (3, 2, 5), (3, 3, 5), (2, 1, 7), (2, 2, 7), (2, 2, 9), (3, 1, 9), (3, 2, 9), (2, 2, 25)$: 220 down-sets, 0 failures (auditor's engine; the constructor's engine, run separately, reported equality for 142 down-sets at 11 cells).
- **(P1), (Chain), (P2).** The chain property and the membership of the options in $\text{BPar}_q(\alpha, \beta)$ for every tail shape, and Proposition 7.4 on every comparable pair of tail shapes, at 16 cells up to $(8, 7, 5), (6, 6, 9), (7, 5, 27)$ and $(3, 3, 81)$ (up to 7214 comparable pairs); (P1) by brute force over every tail at 8 cells up to $(2, 2, 27)$ (19683 tails): 0 failures.
- **(P3).** Every generator of every layer lies in its slice (Proposition 7.5), 3428 memberships at 7 cells. Negative control: lowering the slice by one gives 17, 58 and 10 failures at $(3, 2, 3), (3, 3, 3)$ and $(2, 2, 5)$.
- **The characteristic.** In characteristic 0, $\dim I_a^{\text{bal}} = 4, 24, 169$ for $a = 1, 2, 3$ at $q = 3$ (against 3, 15, 93), $\dim I_a^{\text{ph}} = 18, 126$ for $a = 1, 2$ (against 15, 93), and $\dim I_2^{\text{bal}} = 129, 416, 1025$ at $q = 5, 7, 9$ (against 45, 91, 153): Theorem C holds with strict inequality (Remark 7.9(2)).
- **The full family is needed.** With a single bijection instead of all of S_2 , the ideal at $(a, q) = (2, 3)$ has dimension $9 < 15$.

14.5 Theorem A

$\dim F_p[L]/K_\mu(L) = N_\mu(n)$ at 178 cells; Theorem A in characteristics 0, 3, 5, 7, 11 for $n = 2, 4, 6$ and $q = 3, 5, 7, 9$ (60 of 60 cells); the row inclusions of Theorem A.12 as ideal memberships at 7 parents; the case bookkeeping of Theorem A.12 for all μ with $|\mu| \leq 14$ at $q = 3, 9, 27, 81$ (1673721 objects); the identities of Lemmas A.8–A.10 exactly at 166 random instances; and two negative controls (Remark A.14). For Remark 10.4(5)–(6): the Hilbert series against Lusztig's t -analogues at 27 cells and the graded characters of the symmetric group at 56 cycle types ($q = 3, 5, n \leq 6$); the even- q rings at 8 cells in characteristics 0, 3, 5, 7 (equal dimensions) and 2 (larger in all 8). For Corollary 10.6 and Remark 10.7(3): $\dim \sum_J D_{r,J} C_r$ against the number of closed walks at 13 cells $(r, N) \rightarrow r \in \{3, 5, 7, 9\}$ and $r \in \{2, 4, 6\}$, $N \in \{2, 4, 6\}$ — in characteristics 3, 5, 7, 32003 (50 of 50, with (5, 6) in characteristics 3 and 5 only) and at 9 cells in characteristic 2 (9 of 9). One run of the first engine was stopped by the memory guard at the cell (5, 6) and rerun with a corrected engine. For the last sentences of Remark 10.4(1): the coinvariants of the group of F_p -points of the centralizer at $(p, q, n) = (3, 3, 3), (3, 3, 4), (3, 5, 3)$ (9, 27, 19 against 7, 19, 13),

computed by the cold reader and again by the author with separate code; at $(5, 3, 3)$ and $(5, 5, 3)$ the two numbers agree. Engines and logs: [Rep], [engines/theorem-a-kostant/](#).

14.6 Independent readings, and their limits

The proofs of §2, §5 and Appendix A were checked in a first pass, then re-derived cold, step by step, by a separate reader with its own code, before this paper was written. An earlier version of this paper (for $m = 3^v$) was then read cold by three further readers, independently, each with a list of attacks and its own engines. None found a fatal error, a gap or a mathematical error; all their findings were of presentation, and they are incorporated here. One of them audited the proofs inside [DS] of the results collected in Theorem 0, from the source of arXiv:1405.4683v3, and found them sound for every $m \geq 3$ and every even $n \geq 2$; the Picard number of the cubic surface independently confirms the signs of [DS, Theorem 2.2] (with $1 + t$ in place of $1 - t$ in ψ_J the rank at $(n, m) = (2, 3)$ would be 20, not 7).

The version for odd prime powers was read cold by a further reader of the same system and, for the first time, by AI systems of two other providers (ChatGPT, OpenAI; Gemini, Google). None found a fatal error. Two of them found, independently, that one sentence in the proof of Theorem 5.9, and the same phrase twice in the proof of Proposition 11.1, was literally false: an initial ideal is a monomial ideal and does not contain the non-monomial generators. One classified this as a gap and the other as an error of wording, and both gave the argument used here (Lemma 5.8'). Two readers also pointed out Theorem 5.9' and Corollary H. ChatGPT then read the Hodge part of the version with Corollary H (§1.3, §8 and §11 there) and found one error, a novelty claim contradicted by the cells of [DS, §5]; it is corrected here (§1.3).

The part of this version on the degrees that are not prime powers (§6–§7) was constructed by one instance of the same system, with its own engines, and then audited cold by another, which re-derived every step, including the nine cases of Proposition 7.4 and the three constructions of Proposition 7.5, compared the colour reduction with the author's earlier block decomposition [Rep], and ran separate engines with predictions recorded before the runs (§14.3–§14.4). The new sections (§6, §7, §12, §13) were then read cold by a further instance, which re-derived them and recomputed the counts with its own code; it found no fatal error, no gap and no mathematical error, and its findings of presentation are incorporated. A further cold reader then read the whole of §6, §7, §12, §13 and the chain of the Main Theorem, with eleven section-referees and adversarial verifiers of its own. It recomputed the Fermat fourfolds of degree 15 and 21 at both primes from the literal generators of [DS], colouring by colouring, and checked Theorem 7.6 at 117 down-sets of 11 cells and Theorem C at 10 new root cells. It found no fatal error and no gap in the proofs; one error of self-description (the upper bound of Proposition 2.1 is algebraic, which is now stated in §1.2 as Main Theorem'); one sentence missing in the deformation argument of Corollary W(i), now supplied; and items of presentation, incorporated. ChatGPT (OpenAI) then read the previous version (v7) cold, attacking the new parts with its own computations and with the source of [DS]. It found no fatal error, no gap and no mathematical error; its one point of presentation is incorporated here (the proof of Lemma 6.8).

Version 11: the odd box and the even degrees (§8–§9). They were found and proved on 2 October 2026 by one instance of the system (the constructor), working alone in one session from a written mission, with its own engines. The mission had been written by the auditing instance, which had first measured, in seven cells with $m = 2^v$, that the leading forms of the generators span an ideal of the right dimension, and, in eighteen cells, that the count at the odd box holds. The two documents of the constructor were then audited cold by the auditing instance: every step of what is now §8 and §9 was written again in its own words and marked, the translation was re-read in the original of [DS] for even m , §7 was re-read with an even q , and gates were run with code of its own (§14.9). It found no error and no gap, and four points

of presentation. The documents were then read cold by a third instance, which had only those two documents, version 10 of this paper and the source of [DS], and no access to the work of the other two. It wrote its verdict item by item (29 items) before running any computation, and then made 19 logged runs with its own code, with 14 predictions recorded in advance (§14.9). Its verdict was «holds», with no error and no gap, and 17 points of presentation, which are incorporated here; among them: that §7 should be *stated* for every q , so that the even box is a case of the theorem and not a re-reading of its proof; the labelling of the rows in the proof of Lemma 8.4; and the observation that Lemma 8.7 holds for more border sets than it states. Two of its own negative controls did not behave as it had predicted — one was badly conceived, and the other could not fire and was replaced by one that does — and it says so. Its session record shows that it used no other agent and opened nothing outside its folder. The auditing instance graded the report, checked eight of its hand computations and repeated six of its runs with its scripts, with identical output. The text of §8 and §9 printed here was written by the auditing instance from those documents and readings, and it differs from them in notation and in three places of substance: the upper bound of Theorem O is proved here without Theorem A (Corollary 8.13); the count of §9 treats the index 0 as an ordinary coordinate (Lemma 9.6), which removes the per-colouring upper bound that the constructor had proved with p -adic integers; and Corollary 10.8 is new. **The limits of this part of the record:** the three instances are of the same system; the cold reader computed no cell of the literal ring of [DS] beyond those already known; the printed text of §8–§9, as distinct from the documents it was written from, was at first re-read and gated by its writer only (§14.9, last item; it was then read cold, see the next paragraph); and nothing in §8–§9 was formalized (it now is, §14.8). The documents, the audit, the report of the cold reader, its grading and all the code are in [Rep], **record/even-degrees/**.

The printed text of version 11, and version 12. The printed text of version 11 was read cold on 2 October 2026 by a further instance of the same system, which had the paper, the original of [DS] and the pages of [Aok] that it needed, and nothing else. It wrote its verdict item by item before running anything (37 items: §1, §2, Appendix B, §5, §6, all of §7, §8 and §9, Corollary 10.8, §12, §13 and §16), re-derived every step of the chain for even m by hand, and made logged runs with its own code, among them the dimension of the literal ideal of [DS] in 16 cells (k, m, p) with $p|m$. Its verdict was «holds», with no error and no gap; its 18 notes of presentation and three observations (some patterns are zero; the border of Lemma 8.7 for $\ell = 0$; the odd-box formula at an even box) are incorporated in this version. It did not read Appendix A or §4, did not re-prove the topology or (H1)–(H3), and did not open the pdf; Corollary 10.8 is in its reading «holds, given Theorem A». Its session record shows that it used no other agent and opened nothing outside its folder. The auditing instance graded the report, checked its hand computations and repeated six of its runs with its scripts, with identical output. **The changes of version 12.** Version 12 is new in the writing in these places: the proof of §8.5 (Lemmas 8.7', 8.8 and Corollary 8.9); the upper bound of Corollary 8.13; the proof of Lemma 9.10 in the case $0 \notin \mathcal{C}_1$; the proof of property (ii) and the explicit signs of §8.3; the base change in case (Z) of Proposition 8.10; the proofs of Lemmas 6.7(iii) and 9.8; and §1.0, §1.8–§1.10, §14.8, §14.9 and §16. Before the version was made public, these passages were read cold on 4 October 2026 by a further instance of the same system, which had the paper, version 11 for comparison and the originals of [DS], [Knu], [Oka], [MMRV] and [FK], and nothing else. It re-derived by hand every sign of §8.3 and §8.5, the proof of Lemma 8.7' (with the Vandermonde divisibility over $Z[\zeta][y]$), the upper bound of Corollary 8.13 step by step, the short route of Lemma 9.10 and the equivalence of the two forms of the degree condition, and made eleven logged runs with its own code, among them the proof of Lemma 8.7' run as an explicit certificate over Z in 33 cells, and Corollary 8.13 over five fields with the intersection computed independently. Its verdict was «holds», with no error and no gap; its 17 notes of presentation are incorporated in this version, and its one mathematical observation (a further zero pattern) is part of §8.5, Remark (2), which the auditing instance generalized and checked with its own code. It did not read §3, §4, the

proofs of §5–§7, §10, §11 or the appendices, and could not read the Lean project; it states that it launched no other agent, and every file it produced is in its own folder. The auditing instance graded the report, checked every line it cites and repeated five of its runs with its scripts, with identical output. Reports, gradings and code: [Rep], `record/cold-readings/`.

The limits of this record must be stated plainly.

- **All these readers are AI systems** (Claude, Anthropic, for all but four readings; Chat-GPT for three of them and Gemini for one; see the note at the end). They worked separately and without access to each other’s code, but they are not independent in the way that different human experts are.
- **No human expert has refereed this work.**
- **Pham’s theorem [Ph] is not re-proved here**, and neither are the intersection numbers [DS, Theorem 2.2]; Appendix B reduces Theorem 0 to these two results.
- The numbering of [DS] was checked against arXiv:1405.4683v3, not against the printed version.
- **Versions 9 and 10.** The new material of versions 9 and 10 (Remark 10.4, Proposition 10.5, Corollary 10.6 and Remark 10.7) and the supplementary note [Note] were read cold on 1 October 2026 by a separate instance of the same system, working alone and with its own code. Its verdict was «holds», with one gap (the inequality of Remark 10.7(3) in characteristic 2, repaired there), three errors (a false sentence in the sketch of Remark 10.7(2); the hypothesis of [Gin, Proposition 4.2], which is stated for semisimple groups; one imprecise identification in the note) and thirteen points of presentation. One of these was an under-claim, which became Corollary A.17; another was the observation that the dictionary of Remark 10.4(1) fails for the points of the centralizer over a finite field. All the findings are incorporated, with the texts and the arguments that the reader proposed; in particular the argument of Corollary A.17 is the reader’s. The reader re-derived Proposition 10.5 and Corollary 10.6 by hand, checked them at 14 cells in characteristics 2, 3, 5 and 1000003, and checked the quotation and the hypotheses of [BRR, Proposition 2.12] against the arXiv source; it did not re-audit §2–§7 or the proofs of Appendix A, which the earlier readings covered. Report, grading and code: [Rep], `record/cold-readings/12_internal-reader_on-v10/`. Kostant’s theorem is quoted from [Gin, Proposition 4.2]; [Kos] was not read in the original. [BRR, §2.1–§2.6] and the introduction and §2.2 of [Ric] were read in the arXiv sources; [KLT], [Bry] and [Lus] were not read.
- **The Lean proof covers Main Theorem’ and Theorem O** (§14.8), for every degree; it does not cover the topology, Theorem A or Corollaries H and W. Its proofs were written by an AI system and are checked by the Lean kernel; that the Lean statements say what the paper says is an audit, set out line by line in [LC, §1.2–§1.3], which a reader can repeat on about fifteen short definitions for Main Theorem’ and seventeen more for Theorem O, printed in [LC, §1.2–§1.4]. Version 2 of the certificate was read cold on 4 October 2026, before this version was made public, by a further instance of the same system, which had the certificate, this paper, the original of [DS], the pieces and the compiled Lean project, and nothing else. It printed the final statement and its definitions from the compiled project and compared them with this paper and with [DS], evaluated $Q_k(m)$ in the kernel against a direct count of $\Gamma_{\mathcal{J}}$, re-elaborated five files of the chain from their sources, recounted every number of the certificate, followed the chain of the final theorem in the sources, and re-submitted to the Lean kernel, from the compiled files, every one of the 4 669 project declarations on which the final theorem and Theorem O depend, with a negative control. Its verdict was «HOLDS AS FAR AS I CAN CHECK»; its findings concerned the certificate, not the proofs, and are incorporated in it. Report, grading and code: [Rep], `record/`

14.7 A referee's guide

The joints deserve attention in this order.

1. **Proposition 5.6 (P2)** and **Proposition 7.4**, the only case analyses in the proof that are not one-line identities. A sceptical reader should try long, very uneven partitions at $q = 3$ ($h = 1$) and $q = 9$ ($h = 4$), where lengths hit the cap $\ell \leq h$, and, for Proposition 7.4, the cases AR and MR, where a removal of one pair of partitions is compared with an option of another kind.
2. **The translation (§2)**: the conventions of [DS] ($j_0 = 0$, the variable t_0 never appears, $N = 2k + 2$) and Lemma 2.4.
3. **The colour reduction (§6)**: Proposition 6.5 (the surviving generators are pure tensors; this is where the full family is used, as Lemma 5.2 is in §5) and Lemma 6.8, where the index 0 couples the blocks only through w_0 ; and Corollary 7.8, whose proof passes through the sum over the colourings.
4. **The coverage formulas (5.1) and (7.1), and Propositions 5.8 and 7.5**, which have no slack (Remark 5.10(2), §14.4).
5. **Theorem 0** and Appendix B. Only Theorem 0(a), (c) and (d) are topological; Theorem 0(b), which carries every upper bound of the paper, is a Chinese-remainder count.
6. **Corollary H**: the classical input (H3) and Aoki's theorem (H5) of §12.1, which are quoted and not re-proved here; (H4) is proved in §12.1.
7. **The odd box (§8)**: Lemma 8.4, part (D2), in the case $\nu_j = 1$; Lemma 8.7': the identity (8.6), the two operations of Lemma 8.8 and the powers of ζ in Corollary 8.9 (all of them checked in Lean, §14.8); and, in Proposition 8.10, the case (M) with $\delta = 1$, where two Pfaffians are combined so that the terms with $D^-(y_1, \cdot)$ cancel, and the case (Z) with $\delta = 1$, where Lemma 8.7 is used.
8. **The even degrees (§9)**: Step 2 of Proposition 9.2 (the leading forms); §7 read with an even q (the only use of the field is $C(q-1, r-1) \neq 0$ in case (γ) of Proposition 7.5); Lemma 9.9 (the substitution $u = -t$) and Lemma 9.10 (the map θ); and Lemma 9.6, where the index 0 is a coordinate of the count but not of the ideals.

14.8 A machine-checked proof of Main Theorem' and of Theorem O

Main Theorem' has been proved, for every degree, in the proof assistant Lean 4 [dMU] with the Mathlib library [Mlib]; the certificate is [LC]. The final theorem, `EvenAll.mainTheorem'`, states: *for every $m \geq 1$ and every $k \geq 0$, $R/(\psi_J : J \in \mathcal{J})$ is a free abelian group of rank $m^{2k+1} - Q_k(m)$, and for every field F , $\dim_F F[G]/(\bar{\psi}_J : J \in \mathcal{J}) = m^{2k+1} - Q_k(m)$ and $\dim_F (\bar{\psi}_J : J \in \mathcal{J}) = Q_k(m)$.* This is slightly more general than Main Theorem' as stated in §1.2 ($m \geq 3$, $k \geq 1$, prime fields). In Lean, $Q_k(m)$ is defined by the formulas of §1.2, with the parity split, and lemmas identify it with the numbers of tuples of Lemmas 2.2 and 9.1 and with $|\Gamma_{\mathcal{J}}|$. Theorem O is proved with equality over every field and with the freeness over Z (`OddEquality.D1`, `OddEquality.D2_DJ`; for the ideal $\mathcal{M}$ of Lemma 8.12, `OddEquality.D2_M`).

- **What was formalized.** For odd m (version 1 of the certificate, 29 September 2026): Lemma 2.2 and the translation of §2 in its local form (Lemmas 2.3, 2.4 and Proposition 2.5); Theorem 5.3 and the induction of §5; the colour reduction of §6; Theorems 7.6 and

C; and the upper bound [DS, Claim 4.3] (Theorem 0(b), Appendix B, Step 6), which is algebraic. For every degree, in twenty further pieces: §7 for every box $q \geq 2$, and at $q = p^v$ in characteristic p , 2 included; Lemma 9.1 and the upper bound for even m ; all of §8 — the shapes and interlaced pairs, Lemmas 8.3–8.5, the Pfaffians and bordered Pfaffians of §8.3 over any commutative ring with the signs given there, Lemmas 8.7, 8.7' and 8.8 and Corollary 8.9 in the form printed in §8.5, Definition 8.6, the seven cases of Proposition 8.10, Theorem 8.11, Theorem O, Lemma 8.12 in the direction used and Corollary 8.13 — and all of §9, with Lemmas 9.4–9.10 for every prime and every cofactor. Theorem 4.1, Theorems 5.9 and 5.9', Corollaries 7.8 and 9.12, Theorem 8.15 and the equality in Theorem O were formalized too, although Main Theorem' does not need them.

- **How.** The Lean proofs were written by the AI system Aristotle (Harmonic), in 49 pieces (29 for the odd degrees, 20 for the rest), each a short text written from this paper. Every returned module that holds a theorem was compiled again on the author's machine (the two modules of numeric checks, and the two files that only import them, exceed the memory cap of the local builds; they contain no theorem used elsewhere, [LC, §2 item 4]) (Lean v4.28.0, Mathlib at the tag v4.28.0) and audited against the paper before the next piece was sent: the difference with the previous project (no piece changed a file of an earlier one), a search for forbidden constructs, the build, the statements as Lean prints them, and their axioms. Before a piece was sent, its statements were tested by exact computation, with negative controls (33731 checks for the twenty pieces of the even degrees, with no failure).
- **Result.** 233 files, 41243 lines, 1859 theorems and lemmas. There is no `sorry`, admit, `native_decide` or added axiom, and every main theorem depends only on the axioms `propext`, `Classical.choice` and `Quot.sound`. A rebuild from source on the author's machine compiled 229 of the 233 modules; the other four — two modules of numeric checks, whose evaluation by the kernel needs more memory than the cap of the local builds, and the two modules that only import them — compiled, as Aristotle reports, on its machines (this was not checked on the author's machine), and no theorem used elsewhere is in them. A program that collects the declarations used by the final theorem finds 4412 of them, in 180 of the 233 modules.
- **What is not formalized.** Theorem 0(a), (c) and (d): the topology of [DS] that identifies the torsion of $R/(\psi_J)$ with that of $H_{2k}(X; Z)/L(X)$ and gives the rank of $L(X)$. Mathlib has no singular homology of complex Fermat varieties. So the Main Theorem, as a statement about homology, is machine-checked only in its algebraic form. Theorem A, Corollaries H and W, §11, the graded refinements of Theorems B and O, and the computations of §14.1–§14.5 and §14.9 are not formalized either.
- **Where.** The certificate [LC] (read cold before release, §14.6) gives the Lean statements and definitions verbatim, compares them with this paper line by line, and lists the trust base, the data of every piece and how to reproduce the build. The Lean project, the pieces, the checks and every log are in [Rep], folder `lean/`.

14.9 The odd box and the even degrees

Three sets of engines were used, written separately and without access to each other: the constructor's, the auditor's (with Singular for the literal ring) and the cold reader's. In the last two, the predictions were recorded before the runs. None of these computations is used in a proof.

- **Theorem O at the root.** $\dim(D_J)C_{2k+1} = N_r(2k+2)$ at $(k, r) = (1, 3), \dots, (1, 11), (2, 3), \dots, (2, 9), (3, 3)$ over F_2 ; at $(1, 3), (2, 3), (3, 3), (1, 5), (2, 5), (1, 9), (2, 9)$ over F_3 ; at

$(1, 5), (2, 5)$ over F_5 and $(1, 7), (2, 7)$ over F_7 ; and at $(k, r, p) = (4, 3, 2), (3, 5, 2), (2, 15, 2), (2, 11, 11)$, predicted before the run (constructor). The cold reader recomputed $(2, 7, 2), (2, 7, 7), (1, 15, 2), (1, 25, 5), (1, 27, 3), (1, 13, 13)$: 3301, 3301, 631, 1801, 2107, 469. With one matching removed the dimension drops: $15 < 19, 140 < 141, 45 < 61, 976 < 1001, 91 < 127, 153 < 217, 231 < 331$ at $(k, r) = (1, 3), (2, 3), (1, 5), (2, 5), (1, 7), (1, 9), (1, 11)$.

- **Theorem 8.11, every interlaced pair.** With V_Λ built from Definition 8.6 (the Pfaffian from its definition) and Z_Λ counted point by point: $\dim V_\Lambda = |Z_\Lambda|$ for all 163 interlaced pairs of 26 cells (r, m, p) with $r \leq 9$ and $m \leq 6$ (auditor), and for the 133 interlaced pairs of 18 cells $(r, m) = (3, 1 \dots 7), (5, 1 \dots 5), (7, 1 \dots 4), (9, 3), (11, 3)$, in 400 triples of a pair, a cell and a characteristic among 2, 3, 5, 7, 101 (cold reader). Without the marked patterns with absorbed pairs ($t \geq 1$) the dimension falls below $|Z_\Lambda|$ in 15 of the 163. For every pair of down-sets that satisfies (D1) but not (D2), in every cell, $\dim V_\Lambda > |Z_\Lambda|$ and the chain of Lemma 8.3 breaks (for instance 19 against 12 for $\{((1), 0)\}$ at $(r, m) = (3, 3)$).
- **Lemmas 8.3 and 8.4.** In the same cells: the number of completions of a tail depends only on its shape and is given by (8.5); the options in Λ form an initial segment; every layer is an interlaced pair; $\Sigma_i |Z_{\Lambda_i}| = |Z_\Lambda|$. No failure.
- **Proposition 8.10.** With the slices computed from the ideal itself (elimination ordered by the degree in y_1): every pattern product of every layer lies in its slice, 12530 memberships (auditor) and 1849 containments $V_{\Lambda_i} \subseteq W_{r-1-i}(V_\Lambda)$ (cold reader), with no failure; moreover $\dim W_{r-1-i}(V_\Lambda) = |Z_{\Lambda_i}|$ in every case. With the slice lowered by one, 540 of 1327 containments fail, in every cell. The seven constructions of the proof, as written, were checked on every pattern of every tail shape of every interlaced pair (membership in V_Λ , degree in y_1 , top coefficient): 2513 cases in 19 cells (r, m, p) with $r \leq 9, m \leq 5$ (constructor) and 3595 cases in 13 cells (r, m) (cold reader), with no failure, every one of the seven cases occurring (359 in the case (M) with $\delta = 1$, of which 96 with absorbed pairs; 235 in the case (Z) with $\delta = 1$; 31 in the second case of (R)); with deliberately wrong border sets the top coefficient is wrong in 49 cases of 49.
- **Lemma 8.7.** The membership, with the Pfaffian computed from its definition, over F_p for $p = 2, 3, 5, 7, 101$: at $r = 3, (\ell, t) = (0, 1)$; $r = 5: (0, 1), (1, 1), (0, 2)$; $r = 7: (0, 1), (1, 1), (2, 1), (0, 2)$; $r = 9: (0, 1), (1, 1)$ (50 memberships, cold reader; 17 instances, auditor; 46, constructor). With the generators of one set S removed the membership fails in every case. The identities of the exterior-algebra proof of version 11 were checked with exact integers for $r = 3, 5, 7, 9, 11$. The proof printed in §8.5 was checked, before it was sent to Lean, with exact integer arithmetic: the rank-two update and the closed forms of Corollary 8.9 (1718 checks), and Lemma 8.7' with the explicit certificate that its proof produces, in 70 cells with $r = 3, \dots, 11$ and up to six variables (840 checks), with controls that fail as they should. The cold reader of the printed text of version 11 found that for $\ell = 0, t = 1$ and $r = 5$ the border y^2 in place of y^{r-1} gives a Pfaffian outside $\mathfrak{U}_0(N)$ (§8.5, Remark (3)).
- **Theorem 8.15.** $\dim I(m, J) = |Z_J^{(m)}|$ for all $0 \leq J \leq m$ and $1 \leq m \leq 7$ over F_2, F_3, F_{101} (35 ideals; three engines), with every slice containment of the proof. With the signs of D removed, the dimensions are 18 and 138 instead of 19 and 141 over F_3 .
- **§7 at an even box.** $\dim V_\Lambda = |Z_\Lambda|$ at every down-set of $\text{BPar}_q(\alpha, \beta)$ over F_2 for $q = 2$ (nine cells, up to $\alpha + \beta = 6$), $q = 4$ (four cells) and $q = 8$ (two cells): 51 down-sets of 51 (auditor); the cold reader found equality at every down-set of its cells over F_2 ($q = 2, 4, 8$), and $\dim V_\Lambda \geq |Z_\Lambda|$, strict at the roots ($58 > 28, 174 > 66$), for $q = 4$ over F_5 and $q = 6$ over F_7 , where the binomial coefficients are non-zero (22 cells in all). The constructor had measured the roots at 15 cells over F_2 . In two fields where a binomial coefficient vanishes ($q = 4$ over $F_3, q = 6$ over F_2) the inequality held as well (§15, problem 7). With one

bijection, or all but one, instead of all, the dimension falls below the count ($4 < 6$, $16 < 28$, $232 < 256$, $64 < 120$).

- **The counts.** $|\Gamma_{\mathcal{J}}|$ from [DS, Definition 1.3], the number of tuples that split into inverse pairs, the formula of Lemma 9.1 and the polynomials of [DS, Remark 4.4] agree at $(k, m) = (1, 4), (1, 6), \dots, (1, 14), (2, 4), (2, 6), (2, 8), (3, 4)$. Forbidding the value -1 gives the numbers $Q_k(m-1)$ instead.
- **The colour reduction for even m , from the literal generators of [DS].** For every colouring, the ideal generated in R_c by the images of the ψ_J was computed and compared with the product of block counts of Lemma 9.6; the sums were compared with $Q_k(m)$. No mismatch: at the prime 2, $(k, m) = (1, 6), (2, 6), (1, 12), (2, 12), (1, 14), (2, 14), (1, 20), (1, 24)$; at an odd prime, $(k, m, p) = (1, 6, 3), (2, 6, 3), (3, 6, 3), (1, 10, 5), (2, 10, 5), (1, 12, 3), (2, 12, 3), (1, 14, 7), (1, 18, 3), (1, 20, 5), (1, 30, 5), (1, 42, 7)$. In the colouring «all -1 » the dimension is $N_q(2k+2)$, and in the colouring «all 1 » at the prime 2 it is $N_{q-1}(2k+2)$. Both kinds of block of colour 1 of Lemma 9.10 occur and agree; at $q = 2$ every block of colour 1 has dimension 1.
- **Cells of Conjecture 1.2 that are not in [DS, §5], in the literal ring.** By the splitting of Lemma 6.1 and Gröbner bases, at every prime dividing m , with no use of Theorem O or of the block theory: $(n, m) = (4, 14)$: 26041; $(4, 18)$: 61601; $(4, 20)$: 87661; $(4, 28)$: 263901; $(4, 30)$: 329561; $(6, 12)$: 876331 (auditor); and $(6, 6)$: 18733 (constructor). In each, the dimension of the ideal equals $Q_k(m)$ at each prime.
- **Hodge characters for even m** (§12): $|\mathfrak{B}|$ and $|\mathfrak{D}|$ were counted by enumerating multisets at $(k, m) = (1 \dots 5, 4), (1 \dots 3, 6), (1 \dots 3, 8), (1, 10), (2, 10), (1, 12), (2, 12), (1, 14), (1, 16), (1, 18), (1, 20)$; in each, $|\mathfrak{D}| = Q_k(m)$, and $|\mathfrak{B}| = |\mathfrak{D}|$ exactly for $m = 4$.
- **What was not done.** No cell of the literal ring for a pure power of 2 outside [DS, §5] (the runs at $(n, m) = (4, 16)$ and $(8, 4)$ were stopped by the memory guard). The family runs of Theorem 8.11 stop at $r = 11$ and at seven variables. As a membership, Lemma 8.7 was tested by machine over prime fields only; its proof was run as an explicit certificate over Z in small cells (the bullet «Lemma 8.7» above, and the cold reading of §14.6), and over Z it is proved in Lean (§14.8).
- **The printed text.** After §8–§10 were written in their present form, the statements that are new in the writing were computed again from the text, with a separate script (34 checks, no failure): the slices 3, 7, 9 of §8.9, in characteristics 2, 3, 5; Lemma 8.12 and Corollary 8.13 (the two dimensions, the injectivity of θ and its image) at $(k, r) = (1, 3), (2, 3), (1, 5)$ in characteristics 2, 3, 5; Corollary 10.8, as two equalities of ideals, at $(r, N) = (3, 4), (3, 6), (5, 4)$ in characteristics 3, 5, 7, and in characteristic 2 the colengths 19, 141, 61 of the intersection against 21, 183, 65 of the ideal of the odd elementary symmetric polynomials; at $r = 3$, $k = 2$, for each of the 15 matchings removed, the dimension 140 in characteristics 2 and 3, and (Singular) the sum count 141 over F_3 (Remark 10.7(3)); Proposition 9.2 at $(k, q) = (1, 4), (2, 4), (1, 8)$: the formula of Step 1, $\text{in}(\bar{\psi}_J) = L_J = Y \cdot D_J$, and the equality of the Hilbert functions of $\text{in}(I)$ and of $(L_J)B$ (3, 6, 6, 3, 1; 15, 36, 40, 29, 15, 5, 1; 3, 6, 9, 12, 15, 18, 18, 15, 12, 9, 6, 3, 1); and the tables of §9.1 and of Example 9.14, the latter by enumeration.
- **The printed text of version 12.** The statements that are new in the writing of version 12 were computed again from the printed text in the same way, with a separate script (4831 checks, no failure): the explicit signs of (iii), (F2), (F3), (F4) and (F7), and property (ii), on random integer matrices with up to eight indices; (8.1)–(8.4) and (F5) at $r = 3, 5, 7$; (8.6), the two items of (a) and the antisymmetry of ω_s for $h = 1, \dots, 4$; Lemma 8.8 (i) and (ii), with a control (the opposite sign in (ii) fails); Corollary 8.9 (a) and (b) for $h = 1, 2$ and

$n \leq 5$, as identities over $Z[\zeta]$; Lemma 8.7' as a membership over F_{10007} , in 25 cells with $r = 3, 5, 7, 9$ and up to six variables (16 of them with a non-zero Pfaffian); Remark (2) in eight cells where the Pfaffian is identically 0, among them $(r, \ell, t) = (5, 2, 1), (7, 2, 2), (7, 3, 1)$, with four controls where it is not; Remark (3); and, for $k \leq 11$ and $3 \leq m < 400$, the equality of the conditions $\gcd(m, (n+1)!) = 1$ and $\gcd(m, (n+2)!) = 1$ of §1.3.

15. Open problems

1. **Equality for every interlaced pair.** Prove $\dim V_\Lambda = |Z_\Lambda|$ for every interlaced pair Λ of Theorem 8.11 (it is proved at the two roots, Corollary 8.13, and measured in every cell we computed, §14.9), and describe C_m/V_Λ as an associated graded ring, as in the Complement to Theorem 5.9. The evaluation argument of Theorem 5.9 does not apply as it stands: on a grid with 0 the polynomial $D_r(a, b)$ does not vanish off the pairs $b = -a$. (In version 10 this item was «Even degrees»; it is now Theorem 9.11.)
2. **The remaining integral Hodge classes.** When m is neither prime nor 4 and has a prime factor at most $2k+1$, find generators of $\text{Hdg}(X)$ beyond $L(X)$. By Corollary H(ii) the missing part is a free group of rank $|\mathfrak{B}| - Q_k(m)$ (Remark 12.3, Lemma 12.4), and the integral question is whether algebraic cycles fill it. For $k = 1$ they do, by the Lefschetz (1,1) theorem; the question is for $k \geq 2$. The rational Hodge conjecture for these X is known in many cases [Shi79], [Aok], [Jum].
3. **Elementary divisors.** For $m = p$ prime and $k \geq 2$, compute the elementary divisors of $\text{Hdg}(X) = L(X)$; [AMV, Table 1] gives the data for small cells. For $k = 1$ they are the author's *Watermark* and *Double Ladder* theorems [WDL]; for $k \geq 2$, the discriminant is given by the sequel note [WED], modulo [BRR, Proposition 2.12] (Remark 12.2).
4. **A direct proof of Corollary 7.8.** Prove $\dim_{\bar{F}_p} I_a^{\text{bal}} \leq N_{\text{bal}}(a, q)$ on the bipartite block itself, without passing through the sum over the colourings of §6; since the dimension over Q is larger (Remark 7.9(2)), such a proof must use the characteristic. Equality $\dim V_\Lambda = |Z_\Lambda|$ for every down-set of Theorem 7.6, measured at every down-set we tested (§14.4) and never contradicted, would give it.
5. **Representation theory.** The Specht module route at $q = 3$ (Remark 4.2(3)), and more generally a representation-theoretic description of the rings C_m/V_Λ (Complement to Theorem 5.9) and of the bipartite quotients.
6. **Theorem A for even q and odd n .** Prove that for every field of characteristic $\neq 2$, every even q and every odd n , $\dim F[x_1, \dots, x_n]/(e_1, e_3, \dots; x_1^q, \dots, x_n^q)$ is the number of walks of length n on the lattice $Z^{q/2}$ with steps $\pm \varepsilon_i$ from 0 to ε_1 . For even n the corresponding statement (closed walks) follows from [BRR, Proposition 2.12] (Remark 10.4(6)); for odd n the weights are not in the root lattice, and the statement is computed in a few cells only. The proof of Theorem A uses the value 0 of the grid, which an even q does not have.
7. **Around the odd box.** Problem 7 of version 10 is Theorem O. What remains: (a) derive Theorem B and Theorem O in positive characteristic from the theory of modules with a good filtration, as [BRR] derive the count of Theorem A; (b) Theorem C over an arbitrary field: in the cells where a binomial coefficient $C(q-1, t)$ vanishes that we computed ($q = 4$ over F_3 , $q = 6$ over F_2), the inequality of Theorem 7.6 still holds at every down-set, although the proof of Proposition 7.5 does not apply (§14.9); (c) Lemma 8.7' gives the membership for any exponents in its case (a), and in its case (b) with the border y^{r-1} , which cannot be dropped (§8.5, Remark (3)): describe all the border sets for which it holds.
8. **What is not formalized.** Main Theorem' and Theorem O are formalized for every degree

(§14.8; this was problem 8 of version 11). Formalize the topology of Theorem 0 (Mathlib has no singular homology of complex Fermat varieties), Theorem A, Corollaries H and W, and the graded refinements of Theorems B and O.

9. **The leading forms.** By Remark 9.3(1) the generators $\bar{\psi}_J$ at $m = 2^v$ are a standard basis for the order filtration. Is the same true of the generators at an odd prime power, for the filtration by the powers of the augmentation ideal, and does it give a proof of Theorem B that avoids the coordinate $y = t - t^{-1}$?

16. Exact status

- **PROVED, with no topology:** Main Theorem' — for every $m \geq 3$ and every $k \geq 1$, the group $R/(\psi_J : J \in \mathcal{J})$ of [DS] is free abelian of rank $m^{2k+1} - Q_k(m)$. For odd m it uses §5–§7; for even m , §6 (Lemmas 6.1, 6.2, 6.4 and 6.7, at every prime, the prime 2 included), §7, §8, §9 and, at the odd primes, §5; in both cases [DS, Claim 4.3], a Chinese-remainder count re-proved in Appendix B, Step 6.
- **MACHINE-CHECKED in Lean 4 with Mathlib (§14.8), for every degree:** Main Theorem', for every $m \geq 1$ and every $k \geq 0$, over Z and over every field; and Theorem O, with equality over every field and the freeness over Z . No `sorry`, and no axiom beyond `propext`, `Classical.choice`, `Quot.sound`. Not formalized: the topology of Theorem 0(a), (c) and (d), Theorem A, Corollaries H and W, and the graded refinements of Theorems B and O.
- **PROVED, modulo Pham's theorem [Ph] and the intersection numbers [DS, Theorem 2.2]:** the Main Theorem, i.e. Conjecture 1.2 of Degtyarev–Shimada for the Fermat varieties of every degree $m \geq 3$ and every even dimension. Through Theorem 0 it uses [DS, Theorem 1.1(a), Claim 4.3, Theorem 1.4, Corollary 1.5], which Appendix B re-derives from those two results and classical topology, for every $m \geq 3$.
- **PROVED, modulo in addition the standard topological facts (H1)–(H2), the classical description of Hodge classes (H3) [SK], [Shi79], [Ran], and Aoki's theorem (H5) [Aok] (for prime m and for $m = 4$, (H4) and (H4') replace (H5); the proof of (H4) uses the formula for $B_{1,\chi}$ and Dirichlet's theorem $L(1, \chi) \neq 0$ [Was]):** Corollary H — for every $m \geq 3$, $L(X)$ is a primitive sublattice of $\text{Hdg}(X)$ with free quotient of rank $|\mathfrak{B}| - Q_k(m)$, and the integral Hodge conjecture holds for X when m is prime, or $m = 4$, or every prime factor of m is at least $2k + 3$. In the prime cells computed in [DS, §5], in the cells $(k, m) = (2, 4), (3, 4)$ computed there, and in the cell $(2, 4)$ of [AMV], it was already known (§1.3).
- **PROVED, modulo the same two results as the Main Theorem:** Corollary W(ii), for every $m \geq 3$, and, modulo in addition the transport argument of [DS, §4.6], Corollary W(i).
- **PROVED:** Theorem B (the dimension count, with equality over every field and for every odd q , and the freeness over Z), Theorems 5.3, 5.9 and 5.9', Theorem 4.1; the colour reduction (Proposition 6.9); Theorem C and Theorem 7.6, for every integer $q \geq 2$ and every field in which the binomial coefficients $C(q-1, t)$ are non-zero; Corollary 7.8; Lemma 12.4.
- **PROVED:** Theorem O (the count at the odd box, with equality over every field and for every odd $r \geq 3$, and the freeness over Z), Theorem 8.11, Lemmas 8.7 and 8.7', Theorem 8.15; Proposition 9.2, Theorem 9.11 and Corollary 9.12 (in Proposition 9.2 and Theorem 9.11, the last clause, that $H_{2k}(X; Z)/L(X)$ is torsion free, is modulo the same two results

as the Main Theorem).

- **PROVED:** Theorem A, for every field of characteristic $\neq 2$, every odd q and every n , with Corollaries 10.1 and 10.2. It is a different statement from the Main Theorem. **As a count it is not new:** it follows from Kostant’s theorem [Kos] in characteristic 0 and from [BRR, Proposition 2.12] in odd characteristic, through the dictionary of Remark 10.4. What this paper adds is that dictionary and the elementary proof of Appendix A, with its ideals K_μ and the equality $\dim F[L]/K_\mu(L) = N_\mu(n)$ for every μ (Corollary A.17).
- **PROVED:** Proposition 10.5 and Corollary 10.6(i) (Theorem B in $2k+2$ variables); Corollary 10.8 (at every odd box and in characteristic $\neq 2$, the intersection of the matching ideals and the ideal of the odd elementary symmetric polynomials coincide; it uses Theorem O and Theorem A, and not [BRR]). **PROVED, modulo [BRR, Proposition 2.12]:** Corollary 10.6(ii) (the same at the even box $q-1$), and the analogue of Theorem A for even q and even n (Remark 10.4(6)).
- **CITED, NOT PROVED HERE:** the author’s *Watermark* and *Double Ladder* theorems (the case $k=1$ of problem 3 of §15), proved for every prime $m \geq 5$ and verified in Lean 4 in [WDL] (Remark 12.2).
- **MEASURED, NOT CLAIMED:** the leading-monomial description of Remark 5.10(4) outside $q=3$; the Specht-module route of Remark 4.2(3); equality $\dim V_\Lambda = |Z_\Lambda|$ in Theorem 7.6 for down-sets other than the roots, and in Theorem 8.11 for interlaced pairs other than the two roots; the inequality of Theorem 7.6 in fields where a binomial coefficient $C(q-1, t)$ vanishes; the Hilbert series of the ring of Theorem A as a sum of Lusztig’s t -analogues (Remark 10.4(5)); the analogue of Theorem A for even q and odd n (Remark 10.4(6)).
- **COMPUTED EXACTLY (finite enumerations, §14):** the counts of Hodge characters of Remark 12.3; the cells of §14.9.
- **FALSE:** the analogue of the Main Theorem for arbitrary subfamilies $K \subseteq \mathcal{J}$ (Fact 11.2); the identification «Conjecture 1.2 at the degree $q \iff A_k(q) = P_k(q)$ »; the equality $\text{Hdg}(X) = L(X)$ for m neither prime nor 4 with a prime factor at most $2k+1$ (Corollary H(ii)).
- **OPEN:** the problems of §15.
- **READ COLD, for the even degrees:** the documents of the proof, twice, by the auditing instance and by a separate cold reader, with separate code; the printed text of version 11, by a further cold reader, «holds» (§14.6). The passages that are new in the writing of this version (§14.6) — among them the proof of §8.5, the upper bound of Corollary 8.13 and the proof of Lemma 9.10 — are checked by the Lean kernel and were read cold before the version was made public: «holds».
- **NOT YET REFEREED by a human expert.**

Acknowledgements and use of AI

The mathematics of this paper was developed with extensive use of Claude, an AI system made by Anthropic, working under the author’s direction in separate roles: instances that proposed and wrote proofs, instances that re-derived them cold and ran their own checks, and instances that read the finished text as referees. The previous versions were also read by AI systems of two

other providers (ChatGPT, OpenAI; Gemini, Google). The degrees that are not prime powers (§6–§7) were constructed by one instance and audited cold by another. The even degrees and the odd box (§8–§9) were constructed by one instance in a single session, from a mission written by an auditing instance that had first measured the leading-form inequality of §9.2 in seven cells; they were then audited cold by that auditing instance, step by step and with its own code, and read cold by a third instance, which had no access to the work of the other two (§14.6). The printed text of version 11 was read cold by a further instance (§14.6). The Lean 4 proofs of Main Theorem' and of Theorem O (§14.8) were written by Aristotle, an AI system made by Harmonic, from pieces written from this paper, and were compiled and audited on the author's machine. The author directed the project and takes responsibility for the content.

The work took more than two and a half months. It went through several hundred written working sessions, recorded more than three hundred unsuccessful routes together with the reason each one failed, and produced more than two hundred standalone write-ups of intermediate results. The full record — the engines and their logs, the audits and the cold readings, the dead routes, and the history of the project — is public at github.com/tretoef-estrella/chaise-longue-theorem [Rep]. Every result of the author on which this paper relies or which it cites — the earlier block decomposition quoted in §6, the *Watermark* and *Double Ladder* theorems quoted in §12, and the computer verdicts quoted in §1.3 and §14 — is deposited in that repository, together with every engine and log behind §14 and the Lean project of §14.8. The sequel note [WED], cited in Remark 12.2 and §15, is deposited at Zenodo and in the repository of the *Watermark* theorem, and a copy is in [Rep].

Appendix A. Proof of Theorem A

This appendix is independent of §2–§5. **Its symbols are local:** here L is a finite set of variables, A and B are subsets of L , C is a set of field elements (Lemma A.4), J is an ideal (Proposition A.5), $R_a(G)$ are the «rows» of Lemma A.6, $K_\mu(L)$ are ideals, and Θ is a generating function (it has nothing to do with Γ_K of [DS]).

A.0 Conventions

- F is a field with $2 \in F^\times$, $q \geq 1$ is odd, and $h = (q - 1)/2$.
- For $X \subseteq L$, $E_X(t) := \prod_{x \in X} (1 + xt)$ and $e_j(X) := [t^j]E_X(t)$, so $e_0 = 1$ and $e_j = 0$ for $j < 0$ or $j > |X|$. $I_q(L) := (e_j(L) : j \text{ odd}) + \text{box}_L$ with $\text{box}_L := (x^q : x \in L)$.
- $[t^D]$ of a power series is 0 when $D < 0$.
- $I_d(2y) := \sum_{b \geq 0} y^{2b+d} / (b!(b+d)!)$ for $d \geq 0$, and $N_q(n) := n! \cdot [y^n]e^y I_0(2y)^h$.
- A **partition** is a finite multiset of positive integers $\mu_1 \geq \dots \geq \mu_\ell$, with $\ell = \ell(\mu)$ and $|\mu| = \sum \mu_i$. For $w \geq 0$, $\beta_w(\mu) := \sum_i \max(\mu_i - w, 0)$ (the number of boxes of the Young diagram to the right of column w), and $c_w(\mu) := \beta_w(\mu) - \beta_{w+1}(\mu) = \#\{i : \mu_i \geq w + 1\}$. So $\beta_0(\mu) = |\mu|$, $c_0(\mu) = \ell(\mu)$, and $c_w(\mu) \leq \ell(\mu)$ for all w .

Strategy. Adjoin one variable z to L . Every ideal G of $F[L \cup z]$ containing z^q has q rows $R_0(G) \subseteq \dots \subseteq R_{q-1}(G)$, and $\dim F[L \cup z]/G = \sum_a \dim F[L]/R_a(G)$ (Lemma A.6). The count satisfies the matching recursion $N_\mu(n+1) = \sum_a N_{\text{child}_a(\mu)}(n)$ (Lemma A.3), which is the derivative of a product of Bessel functions. So it suffices to attach to each μ an ideal $K_\mu(L)$ with $K_\emptyset(L) = I_q(L)$

such that every row of $K_\mu(L \cup z)$ contains the ideal of the corresponding child (Theorem A.12). The ideals come from one generating function Θ , and adjoining z to one of three sets shifts an index of Θ in a controlled way (Lemma A.8). This is the same peeling idea as §5.1, with the box q in place of $q - 1$.

A.1 The count and the dictionary

For a partition μ with $\ell(\mu) \leq h$, put $F_\mu(y) := e^y \cdot \prod_{i=1}^\ell I_{\mu_i}(2y) \cdot I_0(2y)^{h-\ell}$ and $N_\mu(n) := n! \cdot [y^n]F_\mu(y)$, so that $N_q(n) = N_\emptyset(n)$.

Lemma A.1. For $d \geq 1$, $(d/dy)I_d(2y) = I_{d-1}(2y) + I_{d+1}(2y)$, and $(d/dy)I_0(2y) = 2I_1(2y)$.

Proof. Termwise, with $(2b + d) = b + (b + d)$:

$$\sum_b (2b + d)y^{2b+d-1}/(b!(b+d)!) = \sum_{b \geq 1} y^{2b+d-1}/((b-1)!(b+d)!) + \sum_b y^{2b+d-1}/(b!(b+d-1)!).$$

The first sum is $I_{d+1}(2y)$ (substitute $b \mapsto b + 1$). The second is $I_{d-1}(2y)$ if $d \geq 1$, and for $d = 0$ it is again $I_1(2y)$. $\blacksquare$

Definition A.2 (the dictionary). Let $\ell = \ell(\mu) \leq h$. For $a \in \{0, \dots, q - 1\}$, $\text{child}_a(\mu)$ is the partition:

- **lower**, $0 \leq a \leq \ell - 1$: μ with one copy of μ_{a+1} replaced by $\mu_{a+1} - 1$; parts are lowered **largest first**, and a part 0 is deleted;
- **value-0**, $a = \ell$: μ ;
- **new-class**, $\ell + 1 \leq a \leq q - \ell - 1$: $\mu \cup (1)$;
- **raise**, $a = q - j$ with $1 \leq j \leq \ell$: μ with one copy of μ_j replaced by $\mu_j + 1$; row $q - 1$ raises the largest part.

New-class rows exist iff $\ell + 1 \leq q - \ell - 1$, i.e. iff $\ell + 1 \leq h$. Hence every child has at most h parts.

Lemma A.3. $N_\mu(0) = [\mu = \emptyset]$, and $N_\mu(n + 1) = \sum_{a=0}^{q-1} N_{\text{child}_a(\mu)}(n)$ for every $n \geq 0$.

Proof. The first claim holds because $F_\mu(0) = [\mu = \emptyset]$. For the second, $N_\mu(n + 1) = n! \cdot [y^n]F'_\mu$. By the product rule and Lemma A.1, F'_μ is a sum of:

- F_μ , from e^y ;
- for each i , F of μ with μ_i replaced by $\mu_i - 1$, plus F of μ with μ_i replaced by $\mu_i + 1$ (a part 0 is a factor I_0);
- $2(h - \ell)$ copies of $F_{\mu \cup (1)}$, from $I_0^{h-\ell}$.

These are exactly the $\ell + 1 + 2(h - \ell) + \ell = q$ children of Definition A.2. $\blacksquare$

Lemma A.4. Let C be a set of q elements of a field of characteristic $\neq 2$ with $0 \in C = -C$. Then $N_q(n)$ is the number of $c \in C^n$ such that $\#\{i : c_i = v\} = \#\{i : c_i = -v\}$ for every $v \in C \setminus \{0\}$.

Proof. $C \setminus \{0\}$ splits into h pairs $\{v, -v\}$ with $v \neq -v$. By the exponential formula:

- the zero coordinates contribute the factor e^y ;
 - each pair with b coordinates equal to v and b equal to $-v$ contributes $\sum_b y^{2b}/(b! \cdot b!) = I_0(2y)$.
- $\blacksquare$

A.2 The lower bound

Proposition A.5. $\dim_F F[L]/I_q(L) \geq N_q(|L|)$.

Proof.

Reduction to a large field. Let F' be an infinite extension of F . The dimension is unchanged by extension of scalars, because $F'[L]/I_q(L)F'[L] = (F[L]/I_q(L)) \otimes_F F'$. Choose $c_1, \dots, c_h \in F'^\times$ with $c_i \neq \pm c_j$ for $i \neq j$, and put $C := \{0, \pm c_1, \dots, \pm c_h\}$. These are q distinct elements, since $c \neq -c$ for $c \neq 0$.

A radical ideal with the right count. Let $f(x) := \prod_{c \in C} (x - c)$ and $J := (e_j(L) : j \text{ odd}) + (f(x) : x \in L)$.

- By the Chinese remainder theorem, $F'[L]/(f(x) : x \in L) \cong F'^{C^L}$, a product of copies of F' .
- Every quotient of a finite product of fields by an ideal is the product over a subset of the factors. Hence $F'[L]/J \cong F'^Z$, where Z is the set of $c \in C^L$ at which every odd e_j vanishes.
- For such c , all odd $e_j(c)$ vanish iff $\prod_x (1 + c_x t)$ is an even polynomial, i.e. $\prod_x (1 + c_x t) = \prod_x (1 - c_x t)$.
- By unique factorisation in $F'[t]$, this holds iff the multiset $\{c_x \neq 0\}$ is closed under negation.
- So $\dim F'[L]/J = |Z| = N_q(n)$ by Lemma A.4.

Degeneration. Let $\text{in}(J)$ be the span of the top-degree forms of the elements of J .

- $(e_j : j \text{ odd}) \subseteq \text{in}(J)$, since the e_j are homogeneous.
- $x^q \in \text{in}(J)$, since x^q is the top form of $f(x)$.

Hence $I_q(L) \subseteq \text{in}(J)$. For a degree-compatible monomial order, $\text{LM}(g) = \text{LM}(\text{top}(g))$. Moreover, for fixed d the non-zero top forms of degree- d elements of J form, with 0, a vector space. So $\text{LM}(J) = \text{LM}(\text{in}(J))$, and by Macaulay's basis theorem $\dim F'[L]/\text{in}(J) = \dim F'[L]/J$. Therefore

$$\dim F'[L]/I_q(L) \geq \dim F'[L]/\text{in}(J) = N_q(n). \quad \blacksquare$$

A.3 Rows

Lemma A.6. Let $z \notin L$, and let $G \subseteq F[L \cup z]$ be an ideal with $z^q \in G$. For $0 \leq a \leq q-1$ put

$$R_a(G) := \{f \in F[L] : z^a f \in G + z^{a+1}F[L \cup z]\}.$$

Then:

- each $R_a(G)$ is an ideal of $F[L]$;
- $R_a(G) \subseteq R_{a+1}(G)$;
- $\dim_F F[L \cup z]/G = \sum_{a=0}^{q-1} \dim_F F[L]/R_a(G)$, in $N \cup \{\infty\}$.

Proof.

- **Ideal:** $R_a(G)$ is an additive group, and for $g \in F[L]$ we have $z^a g f = g \cdot z^a f$.

- **Monotone:** multiplying $z^a f \in G + (z^{a+1})$ by z gives $z^{a+1} f \in G + (z^{a+2})$.
- **Dimension:** put $G_a := G + z^a F[L \cup z]$. Then $G_0 = F[L \cup z]$ and $G_q = G$. The map $F[L] \rightarrow G_a/G_{a+1}$, $f \mapsto z^a f$, is surjective because $z^a F[L \cup z] = z^a F[L] + z^{a+1} F[L \cup z]$, and its kernel is $R_a(G)$. Summing over a gives the formula. ■

A.4 The generating function

Fix disjoint $A, B \subseteq L$. Put:

- $P := L \setminus (A \cup B)$;
- $r := |A|$;
- $w := |B| - |A|$, the imbalance.

For $a \in A$ let $\varphi_a(t) := (1 - at)/(1 + at) = 1 + \sum_{i \geq 1} 2(-1)^i a^i t^i$.

Definition A.7. For $s \in \mathbb{Z}$, let $D_L(A, B; s) := r(q - 1) + |P| + 1 - s$ and

$$\Theta_L^s(A; B) := [t^{D_L(A, B; s)}] E_P(-t) \cdot \prod_{a \in A} \varphi_a(t) \in F[L].$$

We call s the **level**.

Remark. With $H_{A;B}(t) := \prod_{a \in A} (1 + at)^{-1} \prod_{b \in B} (1 - bt)^{-1}$ one has $E_L(-t) H_{A;B}(t) = E_P(-t) \prod_{a \in A} \varphi_a(t)$: the factors of B cancel. So B enters Θ only through P , that is, through the degree D .

Lemma A.8 (the three moves, and vanishing). Let $z \notin L$ and $L^+ := L \cup \{z\}$. For disjoint $A, B \subseteq L$ and $s \in \mathbb{Z}$:

- (P) $\Theta_{L^+}^s(A; B) = \Theta_L^{s-1}(A; B) - z \cdot \Theta_L^s(A; B)$;
- (B) $\Theta_{L^+}^s(A; B \cup \{z\}) = \Theta_L^s(A; B)$;
- (A) $\Theta_{L^+}^s(A \cup \{z\}; B) = \Theta_L^{s-q+1}(A; B) + \sum_{i \geq 1} 2(-1)^i z^i \cdot \Theta_L^{s-q+1+i}(A; B)$, a finite sum;
- (V) if $s \leq 0$, then $\Theta_L^s(A; B) \in \text{box}_A$, and $\Theta_L^s(A; B) = 0$ if $A = \emptyset$.

Proof.

- (P) In L^+ , z lies in the set $P^+ = P \cup \{z\}$, and $E_{P^+}(-t) = E_P(-t)(1 - zt)$. Since $D_{L^+}(A, B; s) = D_L(A, B; s - 1)$ and $D_{L^+}(A, B; s) - 1 = D_L(A, B; s)$, the identity follows.
- (B) Neither P nor D changes.
- (A) One more factor $\varphi_z(t)$, and $D_{L^+}(A \cup z, B; s) = D_L(A, B; s) + (q - 1)$. The coefficient of $z^i t^i$ in φ_z is 1 for $i = 0$ and $2(-1)^i$ for $i \geq 1$. Finally, level u of $(A; B)$ in L has degree $D_L(A, B; s) + (q - 1) - i$ exactly when $u = s - q + 1 + i$.
- (V) $\Theta_L^s(A; B) = \sum_p (-1)^p e_p(P) \cdot [t^{D-p}] \prod_A \varphi_a$. The coefficient of t^m in $\prod_A \varphi_a$ is homogeneous of degree m in the r letters of A . For $s \leq 0$ every $p \leq |P|$ gives $D - p \geq r(q - 1) + 1$. So every monomial has some exponent $\geq q$ when $r \geq 1$, and $[t^{D-p}]1 = 0$ when $r = 0$. ■

Lemma A.9 (descent). For $a \geq 0$:

$$z^a \cdot \Theta_L^s(A; B) = \Theta_{L^+}^{s-a}(A; B \cup \{z\}) - \sum_{i=1}^a z^{i-1} \cdot \Theta_{L^+}^{s-a+i}(A; B).$$

Proof. The case $a = 0$ is (B). By (P) and (B), $z \cdot \Theta_L^s(A; B) = \Theta_{L^+}^{s-1}(A; B \cup z) - \Theta_{L^+}^s(A; B)$, and applying (B) again to the first term gives $z\Theta_L^s = \Theta_L^{s-1}(A; B) - \Theta_{L^+}^s(A; B)$. Hence

$$z^a \Theta_L^s = z^{a-1} \Theta_L^{s-1}(A; B) - z^{a-1} \Theta_{L^+}^s(A; B),$$

and the formula follows by induction on a . ■

Lemma A.10 (the odd identity). *Let $|A| = |B| = r$, let $c \in Z$, $M := D_L(A, B; c)$, and $h_m := [t^m]H_{A;B}(t)$. For every $\ell \geq 0$,*

$$z^{\ell+1} \Theta_L^{c+1}(A; B) \equiv \Omega - \frac{1}{2} \cdot z^\ell \cdot ((-1)^M \Theta_L^c(B; A) - \Theta_L^c(A; B)) \pmod{z^{\ell+2} F[L^+]},$$

where $\Omega := z^\ell \sum_{j \text{ odd}} e_j(L^+) h_{M-j} - z^{\ell+1} \sum_{j \text{ odd}} e_j(L^+) h_{M-1-j}$ lies in $(e_j(L^+) : j \text{ odd})$.

Proof. Put $\alpha_m := [t^m]E_L(t)H_{A;B}(t)$ and $\beta_m := [t^m]E_L(-t)H_{A;B}(t)$. By definition and the Remark after Definition A.7, $\beta_M = \Theta_L^c(A; B)$ and $\beta_{M-1} = \Theta_L^{c+1}(A; B)$.

Next, $E_L(t)H_{A;B}(t) = E_P(t) \prod_B (1+bt)/(1-bt)$, which at $t = -u$ is $E_L(-u)H_{B;A}(u)$. Since $|A| = |B|$, the degree M corresponds to the same level c for $(B; A)$, so $\alpha_M = (-1)^M \Theta_L^c(B; A)$.

Let $X_m := [t^m]O(t)H_{A;B}(t)$ with $O(t) := \sum_{j \text{ odd}} e_j(L^+) t^j = \frac{1}{2}(E_{L^+}(t) - E_{L^+}(-t))$, so that $\Omega = z^\ell X_M - z^{\ell+1} X_{M-1}$. From $E_{L^+}(\pm t) = E_L(\pm t)(1 \pm zt)$:

$$X_m = \frac{1}{2}(\alpha_m + z\alpha_{m-1} - \beta_m + z\beta_{m-1}).$$

Hence

$$\Omega = \frac{1}{2}z^\ell(\alpha_M - \beta_M) + z^{\ell+1}\beta_{M-1} - \frac{1}{2}z^{\ell+2}(\alpha_{M-2} + \beta_{M-2}).$$

Rearranging gives the claim. ■

A.5 The ideals

Definition A.11. For a partition μ with $\ell(\mu) \leq h$ and a finite set L ,

$$K_\mu(L) := I_q(L) + (\Theta_L^s(A; B) : A, B \subseteq L \text{ disjoint}, w = |B| - |A| \geq 0, 1 \leq s \leq \beta_w(\mu)).$$

Remarks.

1. $K_\emptyset(L) = I_q(L)$, since $\beta_w(\emptyset) = 0$.
2. If $\mu \neq \emptyset$ and $L = \emptyset$, then $\Theta_\emptyset^1(\emptyset; \emptyset) = [t^0]1 = 1$, so $K_\mu(\emptyset) = F$.
3. For $A = \emptyset$, the generators are $\pm e_{|S|+1-s}(S)$ with $S = L \setminus B$, allowed for $s \leq \beta_{n-|S|}(\mu)$. For $S \subsetneq L$ this is Tanisaki's rule for the partition $\mu \cup (1^{n-|\mu|})$ of n [Ta], [GP]; for $S = L$ it adds the $e_j(L)$ with $j \geq n - |\mu| + 1$.
4. The case $s = 1$, $A \neq \emptyset$ gives $\pm 2^r (\prod_A a^{q-1}) \cdot \prod_P x$ modulo box.
5. The generators with $A \neq \emptyset$ and higher s are not suggested by Tanisaki's rule. They were first found by computation, as the corrections needed for $\mu = (1, 1)$, $(1, 1, 1)$ and $(2, 2)$, and the generating function Θ organises them.

A.6 The row inclusions

Theorem A.12. Let μ be a partition with $\ell := \ell(\mu) \leq h$, L a finite set, $z \notin L$ and $K^+ := K_\mu(L \cup z)$. For every $a \in \{0, \dots, q-1\}$:

$$R_a(K^+) \supseteq K_{\text{child}_a(\mu)}(L).$$

Lemma A.13. Let $A, B \subseteq L$ be disjoint with $w := |B| - |A| \geq 0$.

- (i) If $s \geq 1$ and $s+1 \leq \beta_w(\mu)$, then $\Theta_L^s(A; B) \in R_0(K^+)$.
- (ii) If $s \in \mathbb{Z}$, $s \leq \beta_w(\mu)$, $a \geq 0$ and $s-a \leq \beta_{w+1}(\mu)$, then $z^a \cdot \Theta_L^s(A; B) \in K^+$. (For $s \leq 0$ this holds already by (V).)
- (iii) $I_q(L) \subseteq R_0(K^+)$.

Proof.

- (i) $\Theta_{L^+}^{s+1}(A; B)$ is a generator of K^+ : its imbalance is w and its level $s+1 \leq \beta_w(\mu)$. By (P) it equals $\Theta_L^s(A; B) - z\Theta_L^{s+1}(A; B)$.
- (ii) Use Lemma A.9.
 - The first term has imbalance $w+1$ and level $s-a \leq \beta_{w+1}(\mu)$.
 - The terms of the sum have imbalance w and levels in $[s-a+1, s] \subseteq (-\infty, \beta_w(\mu)]$.
 - Each term is a generator of K^+ if its level is ≥ 1 , and lies in box by (V) otherwise.
- (iii) $e_j(L) = e_j(L^+) - z \cdot e_{j-1}(L)$, and $x^q \in K^+$ for $x \in L$. ■

Proof of Theorem A.12. By Lemma A.6 the rows increase, so it suffices to place every generator of $K_{\text{child}_a(\mu)}(L)$ in the row a assigned by the dictionary (or in an earlier row). Generators from $I_q(L)$ are handled by (iii). So consider a child generator $\Theta_L^s(A; B)$ with $w = |B| - |A| \geq 0$ and $1 \leq s \leq \beta_w(\text{child})$. Recall $\beta_w - \beta_{w+1} = c_w \leq \ell$.

Lower, $0 \leq a \leq \ell-1$. Here $\beta_w(\text{child}) = \beta_w(\mu) - [\mu_{a+1} > w]$.

- If $\mu_{a+1} > w$, then $s+1 \leq \beta_w(\mu)$, and (i) applies.
- If $\mu_{a+1} \leq w$, then all parts $> w$ are among $\mu_1, \dots, \mu_a$ (parts are ordered decreasingly), so $c_w(\mu) \leq a$. Hence $s-a \leq \beta_w(\mu) - c_w(\mu) = \beta_{w+1}(\mu)$, and (ii) gives $z^a \Theta_L^s \in K^+$.

Value-0, $a = \ell$. Here $s \leq \beta_w(\mu)$ and $s-\ell \leq \beta_w(\mu) - c_w(\mu) = \beta_{w+1}(\mu)$, so (ii) applies.

New-class, $\ell+1 \leq a \leq q-\ell-1$. Here $\beta_w(\mu \cup (1)) = \beta_w(\mu) + [w=0]$.

- Every generator other than $(w, s) = (0, |\mu|+1)$ is a generator of $K_\mu(L)$, hence lies in row $\ell \subseteq$ row a by the value-0 case.
- For $w=0$ (so $|A| = |B|$) and $s = |\mu|+1$, apply Lemma A.10 with $c = |\mu|$:
 - $\Omega \in K^+$;
 - by (ii) with $a = \ell$, both $z^\ell \Theta_L^{|\mu|}(A; B)$ and $z^\ell \Theta_L^{|\mu|}(B; A)$ lie in K^+ . The pairs $(A; B)$ and $(B; A)$ have imbalance 0; $|\mu| = \beta_0(\mu)$; and $|\mu| - \ell = \beta_0 - c_0 = \beta_1(\mu)$.
 - Hence $z^{\ell+1} \Theta_L^{|\mu|+1}(A; B) \in K^+ + (z^{\ell+2})$, i.e. the generator lies in $R_{\ell+1} \subseteq R_a$.

Raise, $a = q - j$, $1 \leq j \leq \ell$. Here $\beta_w(\text{child}) = \beta_w(\mu) + [\mu_j \geq w]$, and $q - j \geq q - \ell \geq \ell + 1$ because $2\ell \leq q - 1$.

- *Old levels*, $s \leq \beta_w(\mu)$: $s - (q - j) \leq \beta_w(\mu) - \ell - 1 < \beta_{w+1}(\mu)$, so (ii) applies.
- *New level at $w = 0$* , $s = |\mu| + 1$: the new-class argument places it in $R_{\ell+1} \subseteq R_{q-j}$.
- *New level at $w \geq 1$* (only when $\mu_j \geq w$): $s = t := \beta_w(\mu) + 1$. Put $s' := \beta_{w-1}(\mu)$ and consider $\Pi := \Theta_{L+}^{s'}(A \cup \{z\}; B)$.
 - Π has imbalance $w - 1 \geq 0$ and level $s' \geq c_{w-1}(\mu) \geq j \geq 1$, so it is a generator of K^+ .
 - By (A), $\Pi = \sum_{i \geq 0} \kappa_i z^i \Theta_L^{u_i}(A; B)$, with $u_i := s' - q + 1 + i$, $\kappa_0 = 1$ and $\kappa_i = 2(-1)^i$ for $i \geq 1$, all units.
 - Put $i^* := q - c_{w-1}(\mu)$. Then $u_{i^*} = \beta_w(\mu) + 1 = t$, and $i^* \leq q - j$ because $\mu_1, \dots, \mu_j \geq w$ gives $c_{w-1}(\mu) \geq j$.
 - For $i < i^*$: $u_i \leq \beta_w(\mu)$, and $u_i - i = s' - q + 1 = \beta_{w+1}(\mu) + c_w(\mu) + c_{w-1}(\mu) - (q - 1) \leq \beta_{w+1}(\mu)$, since $c_w + c_{w-1} \leq 2\ell \leq q - 1$. So $z^i \Theta_L^{u_i}(A; B) \in K^+$ by (ii), or lies in box if $u_i \leq 0$. (This includes $i = 0$, which matters when $s' \geq q$.)
 - Therefore $\kappa_{i^*} z^{i^*} \Theta_L^t(A; B) \in K^+ + (z^{i^*+1})$. Since κ_{i^*} is a unit, $\Theta_L^t(A; B) \in R_{i^*} \subseteq R_{q-j}$.

Remark A.14 (the order of the lower rows is used). The lower case uses «largest part first». With the opposite order, the inclusion fails already for $\mu = (3, 1)$, $q = 9$, $|L| = 5$: 65 generators of the child (3) lie outside row 0. The count of Lemma A.3 does not see the order; the inclusions do.

A.7 Proof of Theorem A

Theorem A.15. *For every $n \geq 0$, every set L of n variables and every partition μ with $\ell(\mu) \leq h$: $\dim_F F[L]/K_\mu(L) \leq N_\mu(n)$.*

Proof. Induction on n .

Base, $n = 0$. $F[\emptyset] = F$. For $\mu = \emptyset$, $K_\emptyset(\emptyset) = 0$ and $N_\emptyset(0) = 1$. For $\mu \neq \emptyset$, $K_\mu(\emptyset) = F$ (Remark 2 after Definition A.11) and $N_\mu(0) = 0$.

Step. Let $|L| = n$ and $z \notin L$. Then $z^q \in K_\mu(L \cup z)$, and:

$$\begin{aligned}
\dim F[L \cup z]/K_\mu(L \cup z) &= \sum_{a=0}^{q-1} \dim F[L]/R_a(K_\mu(L \cup z)) \quad (\text{Lemma A.6}) \\
&\leq \sum_a \dim F[L]/K_{\text{child}_a(\mu)}(L) \quad (\text{Theorem A.12}) \\
&\leq \sum_a N_{\text{child}_a(\mu)}(n) \quad (\text{induction; every child has } \leq h \text{ parts}) \\
&= N_\mu(n + 1) \quad (\text{Lemma A.3}). \blacksquare
\end{aligned}$$

Proof of Theorem A. Take $\mu = \emptyset$ in Theorem A.15: $K_\emptyset(L) = I_q(L)$, so $\dim F[L]/I_q(L) \leq N_q(n)$. Combine with Proposition A.5. $\blacksquare$

A.8 Proofs of Corollaries 10.1 and 10.2

Corollary 10.1. Take $F = F_p$, $q = p^v$, $n = 2k + 2$. Then $A_k(q) = N_q(2k + 2)$ by Theorem A. Also $N_q(2k + 2) = P_k(q)$: in the proof of Proposition A.5 with $F' = \bar{F}_p$ and the set of values $C = F_q \subset F'$, the set Z is $\{x \in F_q^{2k+2} : e_j(x) = 0, j \text{ odd}\}$. ■

Corollary 10.2. M is spanned by the monomials with exponents $< q$, so it is finitely generated. Write $M \cong Z^\rho \oplus T$ with T finite. For a field F , $M \otimes F \cong F[L]/I_q(L)$, by right exactness of $\otimes$. So:

- $\rho = \dim_Q = N_q(n)$;
- for an odd prime p , $\dim_{F_p} = \rho + (\text{number of cyclic } p\text{-primary summands of } T) = N_q(n)$.

Hence T has no odd primary part. ■

Remark A.16. In characteristic 2 the statement fails, and the proof uses $\frac{1}{2}$ in exactly one place (Lemma A.10). The measured dimensions at $n = 4$ are 21, 65, 133, 225 for $q = 3, 5, 7, 9$, against $N_q(4) = 19, 61, 127, 217$.

A.9 Equality for every partition

Corollary A.17. *For every partition μ with $\ell(\mu) \leq h$, every finite set L and every $z \notin L$:*

- $\dim_F F[L]/K_\mu(L) = N_\mu(|L|)$;
- $R_a(K_\mu(L \cup z)) = K_{\text{child}_a(\mu)}(L)$ for every $a \in \{0, \dots, q-1\}$.

Proof. Let $P(\mu)$ be the statement « $\dim_F F[L]/K_\mu(L) = N_\mu(|L|)$ for every finite set L ». $P(\emptyset)$ is Theorem A. Suppose $P(\mu)$, and let $|L| = n$ and $z \notin L$. In the chain of the proof of Theorem A.15,

$$\begin{aligned} \dim F[L \cup z]/K_\mu(L \cup z) &= \sum_a \dim F[L]/R_a(K_\mu(L \cup z)) \leq \sum_a \dim F[L]/K_{\text{child}_a(\mu)}(L) \leq \\ &\sum_a N_{\text{child}_a(\mu)}(n) = N_\mu(n+1), \end{aligned}$$

the two ends are equal by $P(\mu)$, and all the numbers are finite. The first inequality is a sum of the inequalities $\dim F[L]/R_a \leq \dim F[L]/K_{\text{child}_a(\mu)}(L)$ given by the inclusions of Theorem A.12, and the second is a sum of the inequalities of Theorem A.15; so each of them is an equality. Hence $\dim F[L]/K_{\text{child}_a(\mu)}(L) = N_{\text{child}_a(\mu)}(n)$ for every a and every L , which is $P(\text{child}_a(\mu))$, and $R_a(K_\mu(L \cup z)) = K_{\text{child}_a(\mu)}(L)$, because one ideal contains the other and they have the same finite codimension. So $P(\mu)$ implies $P(\nu)$ for every child ν of μ , and the second claim for μ .

It remains to see that every partition $\nu \neq \emptyset$ with $\ell(\nu) \leq h$ is a child of a partition μ with $\ell(\mu) \leq h$ and $|\mu| = |\nu| - 1$; then $P(\nu)$ follows by induction on $|\nu|$. Let μ be ν with its smallest part lowered by 1 (and deleted if it becomes 0). If the smallest part of ν is 1, then $\nu = \mu \cup (1)$ and $\ell(\mu) + 1 = \ell(\nu) \leq h$, so ν is a new-class child of μ (Definition A.2). Otherwise $\ell(\mu) = \ell(\nu) =: \ell$ and ν is μ with μ_ℓ replaced by $\mu_\ell + 1$: the raise child $a = q - \ell$. ■

So the ideals $K_\mu(L)$ are graded models of all the weight spaces of $V^{\otimes n}$, and the q rows of $K_\mu(L \cup z)$ are exactly the ideals of the q neighbouring weights. We proved Theorem A.15 as an upper bound, which is all that Theorem A needs; that the bound is an equality was pointed out by the cold reader of this version (§14.6).

Appendix B. Theorem 0, modulo Pham's theorem and the intersection numbers

This appendix proves Theorem 0 for $n = 2k \geq 2$, $m \geq 3$ and $\emptyset \neq K \subseteq \mathcal{J}$. It follows [DS, §4] closely, with every step written out. We use, without proof:

- (T1) **Classical topology** [Mil, §7]. $H_*(X)$ and $H_*(Y_0)$ are torsion free, where $Y_0 := X \cap \{z_0 = 0\}$ is the Fermat hypersurface of dimension $n-1$ in P^n ; the intersection form $\langle, \rangle$ on $H_n(X)$ is unimodular; and by the Lefschetz hyperplane theorem $H_j(Y_0) \rightarrow H_j(P^n)$ is an isomorphism for $j < n-1$. We also use three standard facts: the Gysin map $H_n(X) \rightarrow H_{n-2}(Y_0)$ sends the class of a cycle meeting Y_0 transversally to the class of the intersection; two complex submanifolds of complementary dimension meeting transversally in one point have intersection number $+1$; and the action of G by holomorphic automorphisms preserves the intersection form and is compatible with Poincaré–Lefschetz duality [DS, §2].
- (T2) **Pham's theorem** [Ph], [DS, Theorem 2.1]. Let S be the Pham cycle of [DS, §2], an n -sphere in $X \setminus Y_0$, and let G act on $H_n(X \setminus Y_0)$. The map $R \rightarrow H_n(X \setminus Y_0)$, $1 \mapsto [S]$, is surjective.
- (T3) **The intersection numbers** [DS, Theorem 2.2]. Fix $\eta := e^{\pi i/m}$, and put $s(\eta) := 1$, $s(\eta^{-1}) := -1$, and $s(\beta) := 0$ for the other m -th roots β of -1 . Then $\langle L_{J,\beta}, S \rangle = \text{sgn}(\sigma_J) \cdot \prod_{i=0}^k s(\beta_i)$, where σ_J is the permutation $(0, 1, \dots, n+1) \mapsto (j_0, k_0, \dots, j_k, k_k)$.

The group G , generated by $\gamma_i : z_i \mapsto \zeta z_i$ ($\zeta := e^{2\pi i/m}$, $i = 1, \dots, n+1$), acts on X by holomorphic automorphisms; we identify R with its group ring through $t_i \mapsto \gamma_i$. For an R -module M put $M^\vee := \text{Hom}_Z(M, Z)$ with the contragredient action $(g \cdot \varphi)(x) = \varphi(g^{-1}x)$.

Step 1 (the Pham image is primitive, of corank 1). Let $V := \text{Im}(H_n(X \setminus Y_0) \rightarrow H_n(X))$. The cohomology sequence of the pair (X, Y_0) , with Poincaré–Lefschetz duality, gives an exact sequence of R -modules $H_n(X \setminus Y_0) \rightarrow H_n(X) \rightarrow H_{n-2}(Y_0)$ [DS, §2]. The second map is the Gysin map, which sends the class of a cycle meeting Y_0 transversally to the class of the intersection. By (T1), $H_{n-2}(Y_0) \cong H_{n-2}(P^n) \cong Z$ (note $n-2 < n-1$), so $H_n(X)/V$ embeds in Z : V is primitive. The map $H_n(X) \rightarrow Z$ is non-zero: a standard space $L_{J,\beta}$ meets Y_0 transversally in the linear $(k-1)$ -space $L_{J,\beta} \cap \{z_0 = 0\}$ (on $L_{J,\beta}$, $z_{k_0} = \beta_0 z_0$, and z_0 is a non-zero linear form). The intersection is transverse: at a point x , with $H := \{z_0 = 0\}$, $T_x Y_0 = T_x X \cap T_x H$, so $T_x L_{J,\beta} \cap T_x Y_0 = T_x L_{J,\beta} \cap T_x H$, of dimension $k-1$. Its class generates $H_{n-2}(Y_0)$, since its image in $H_{n-2}(P^n)$ is the class of a linear $(k-1)$ -space. Hence $\text{rank } V = \text{rank } H_n(X) - 1$. By (T2), $R \rightarrow V$, $1 \mapsto [S]$, is surjective.

Step 2 (duals of surjections). On R put $[t^\nu, t^{\nu'}] := \delta_{\nu, \nu'}$ ($\nu, \nu' \in (Z/m)^{n+1}$). This form is unimodular and G -invariant, so $x \mapsto [x, \cdot]$ is an isomorphism $R \cong R^\vee$ of R -modules. Let $f : R \rightarrow M$ be a *surjective* homomorphism of R -modules. Then $f^\vee : M^\vee \rightarrow R^\vee \cong R$ is injective, its image is the ideal $\text{Ker}(f)^\perp := \{x \in R : [x, y] = 0 \text{ for all } y \in \text{Ker } f\}$, and $R/\text{Ker}(f)^\perp$ is torsion free.² Indeed, an element of the image vanishes on $\text{Ker } f$; conversely, if $x \in \text{Ker}(f)^\perp$, then $[x, \cdot]$ vanishes on $\text{Ker } f$ and factors through $R/\text{Ker } f \cong M$, so it lies in the image. Finally, if $cx \in \text{Ker}(f)^\perp$ with $0 \neq c \in Z$, then $c[x, y] = 0$ for $y \in \text{Ker } f$, so $x \in \text{Ker}(f)^\perp$.

Apply this to the surjection $f : R \rightarrow V$ of Step 1. We obtain an ideal $V^\vee \subseteq R$ with $R/V^\vee$ torsion free. Explicitly, the composite $H_n(X) \cong H_n(X)^\vee \rightarrow V^\vee \subseteq R$, where the first map is the (G -invariant) intersection form and the second is restriction, sends τ to the element r_τ with $[r_\tau, t^\nu] = \langle \tau, f(t^\nu) \rangle$, that is

²As stated in [DS, §4.2], this description of the image of $f^\vee$ requires the additional hypothesis that $M/\text{Im } f$ be torsion free (for instance, f surjective); this hypothesis holds in the case where [DS] apply it, the surjection of Step 1, so the result we use is not affected.

$$r_\tau = \sum_{\nu \in (Z/m)^{n+1}} \langle \tau, \gamma^\nu[S] \rangle t^\nu.$$

Step 3 (the kernel is generated by the class of a linear section, which lies in L_K). The restriction $H_n(X)^\vee \rightarrow V^\vee$ is surjective, because V is a direct summand of $H_n(X)$ (a primitive subgroup of a free group); so $H_n(X) \rightarrow V^\vee$ is surjective with kernel $V^\perp$ (orthogonal for $\langle, \rangle$), which is primitive of rank 1. Let $P_X := [X \cap \Lambda]$ for a linear subspace $\Lambda \subset P^{n+1}$ of dimension $k+1$ meeting X properly; this class does not depend on Λ , since $[X \cap \Lambda] = h^k \cap [X]$ whenever the intersection is proper. Taking $\Lambda \subset \{z_0 = 0\}$ shows $P_X \perp V$, since every class of V is carried by a cycle in $X \setminus Y_0$. And $\langle P_X, [L] \rangle = 1$ for a standard space L , since P_X is the k -th power of the hyperplane class cut on X and L is a linear space of dimension k . So P_X is primitive and $V^\perp = Z \cdot P_X$. Now fix $J \in K$ and β with $\beta^m = -1$, and let $\Lambda_J := \{z_{k_i} = \beta z_{j_i} : i = 1, \dots, k\}$, of dimension $k+1$. On Λ_J one has $z_{j_i}^m + z_{k_i}^m = 0$ for $i \geq 1$, so $X \cap \Lambda_J = \{z_0^m + z_{k_0}^m = 0\} \cap \Lambda_J$, the reduced union of the m standard spaces $L_{J,(\beta_0, \beta, \dots, \beta)}$, $\beta_0^m = -1$. Hence $P_X \in L_K(X)$, and therefore

$$H_n(X)/L_K(X) \cong V^\vee/L'_K, \quad \text{rank } L_K(X) = \text{rank } L'_K + 1,$$

where $L'_K \subseteq V^\vee \subseteq R$ is the image of $L_K(X)$. Since the maps are R -linear and $L_K(X)$ is an R -submodule, L'_K is an ideal of R .

Step 4 (the image of L_J is generated by ψ_J). For $\nu \in (Z/m)^{n+1}$ write $\gamma^\nu := \prod \gamma_i^{\nu_i}$ and put $\nu_0 := 0$. Since γ^ν multiplies z_i by ζ^{ν_i} , one has $(\gamma^\nu)^{-1}(L_{J,\beta}) = L_{J,\beta'}$ with $\beta'_i = \zeta^{\nu_{j_i} - \nu_{k_i}} \beta_i$. For fixed J these translates exhaust all β (choose $\nu_{j_i} = 0$ and adjust ν_{k_i}), so $L_{\{J\}}(X)$ is the R -module generated by $[L_{J,\eta}]$, $\eta := (\eta, \dots, \eta)$. By Step 2 and (T3), its image is $\psi'_J := \sum_\nu a_\nu t^\nu$ with

$$a_\nu = \langle L_{J,\eta}, \gamma^\nu[S] \rangle = \langle (\gamma^\nu)^{-1} L_{J,\eta}, S \rangle = \text{sgn}(\sigma_J) \cdot \prod_{i=0}^k e(\nu_{k_i} - \nu_{j_i}),$$

where $e(c) := s(\zeta^{-c}\eta)$, that is $e(0) = 1$, $e(1) = -1$ (because $\zeta^{-1}\eta = \eta^{-1}$), and $e(c) = 0$ otherwise. The indices k_0 and j_i, k_i ($i \geq 1$) are $1, \dots, n+1$, each once, so the sum factorises, and $\sum_c e(c)t^c = 1 - t$ and $\sum_{c,c'} e(c' - c)t_j^c t_k^{c'} = (1 - t_k) \sum_c (t_j t_k)^c = (1 - t_k) \varphi(t_j t_k)$ give

$$\psi'_J = \text{sgn}(\sigma_J) \cdot (1 - t_{k_0}) \cdot \prod_{i=1}^k (1 - t_{k_i}) \varphi(t_{j_i} t_{k_i}) = \pm \psi_J.$$

Hence $L'_K = (\psi_J : J \in K)$.

Step 5 (torsion transfer): Theorem 0(a). The exact sequence $0 \rightarrow V^\vee/L'_K \rightarrow R/L'_K \rightarrow R/V^\vee \rightarrow 0$ has a torsion-free cokernel, so every torsion element of R/L'_K lies in $V^\vee/L'_K$, and the torsion subgroups of $V^\vee/L'_K$ and $R/L'_K = A_K$ coincide. With Step 3, $\text{Tors}(H_n(X)/L_K(X)) \cong \text{Tors}(A_K)$.

Step 6: Theorem 0(b)–(d). (b) If $\text{char } K_p = p$ with $p = 0$ or $p \nmid m$, then $t^m - 1$ is separable over K_p , so $R \otimes K_p \cong K_p^{\mu_m^{n+1}}$ is the ring of functions on μ_m^{n+1} , and $A_K \otimes K_p$ is the ring of functions on the common zeros of the ψ_J , $J \in K$. For $b \in \mu_m$, $\varphi(b) = m \neq 0$ if $b = 1$ and $\varphi(b) = 0$ otherwise. So $\psi_J(a) \neq 0$ iff $a_{k_i} \neq 1$ for all i and $a_{j_i} a_{k_i} = 1$ for $i \geq 1$; since then $a_{j_i} = a_{k_i}^{-1} \neq 1$, this says exactly $a \in \Gamma_J$. Hence $\dim(A_K \otimes K_p) = m^{n+1} - |\Gamma_K|$. (c) By Step 3 and (b) with $p = 0$, $\text{rank } L_K(X) = \text{rank } L'_K + 1 = (m^{n+1} - \text{rank } A_K) + 1 = |\Gamma_K| + 1$. (d) For

$p \nmid m$, (b) with $K_p = \bar{F}_p$ gives $\dim_{F_p}(A_K \otimes F_p) = \text{rank } A_K$, so A_K has no p -torsion, and by (a) neither has $H_n(X)/L_K(X)$. ■

References

- [AH] M. F. Atiyah, F. Hirzebruch, *Analytic cycles on complex manifolds*, Topology **1** (1962), 25–45. (§1.3 only.)
- [AMV] E. Aljovin, H. Movasati, R. Villafior Loyola, *Integral Hodge conjecture for Fermat varieties*, J. Symbolic Comput. **95** (2019), 177–184. doi:10.1016/j.jsc.2019.02.006; arXiv:1711.02628.
- [DS] A. Degtyarev, I. Shimada, *On the topology of projective subspaces in complex Fermat varieties*, J. Math. Soc. Japan **68** (2016), no. 3, 975–996. doi:10.2969/jmsj/06830975; arXiv:1405.4683 (v3, 14 July 2015). Theorems 1.1, 1.4, 2.1, 2.2, Conjecture 1.2, Definition 1.3, Corollaries 1.5–1.7, Claim 4.3, Remark 4.4, Lemma 4.5 and §4–§5 (including §4.6) were read in the original.
- [dMU] L. de Moura, S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Computer Science **12699**, Springer, 2021, 625–635. doi:10.1007/978-3-030-79876-5_37. (§14.8 only.)
- [De14] A. Degtyarev, *Lines generate the Picard groups of certain Fermat surfaces*, J. Number Theory **147** (2015), 454–477. doi:10.1016/j.jnt.2014.07.020; arXiv:1305.3073. (Cited in [DS] as reference [3], under a slightly different title.)
- [De15] A. Degtyarev, *Projective spaces in Fermat varieties*, arXiv:1512.06199 (19 December 2015). Conjecture 4.4, (4.5)–(4.6) and Corollaries 4.7–4.8 were read in the original.
- [Aok] N. Aoki, *On some arithmetic problems related to the Hodge cycles on the Fermat varieties*, Math. Ann. **266** (1983), 23–54; erratum Math. Ann. **267** (1984), 572. doi:10.1007/BF01458703. (§1.3, §12.1 (H5). Theorem A (p. 24), its proof (§7, pp. 41–43) and the definitions of §0 were read in the original; the erratum concerns only Theorem B.)
- [BRR] R. Bezrukavnikov, S. Riche, L. Rider, *Modular affine Hecke category and regular unipotent centralizer*, arXiv:2005.05583 (v2, 4 July 2024; the first version carried «, I» in the title). (§1.6, §1.8, §10, §11.1, §14.6, §15 and §16; §2.1–§2.6 were read in the arXiv source, in particular Proposition 2.12 and the proof of Lemma 2.13.)
- [Bry] R. K. Brylinski, *Limits of weight spaces, Lusztig’s q -analogs, and fiberings of adjoint orbits*, J. Amer. Math. Soc. **2** (1989), no. 3, 517–533. (Remark 10.4(5) only; not read in the original.)
- [CLO] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, Springer, 2nd ed., 1997. (Macaulay’s basis theorem: the standard monomials of an ideal form a basis of the quotient.)
- [CM] L. Cerlienco, M. Mureddu, *From algebraic sets to monomial linear bases by means of combinatorial algorithms*, Discrete Math. **139** (1995), 73–87. (Remark 5.10(4) only.)
- [DCP] C. De Concini, C. Procesi, *A characteristic free approach to invariant theory*, Adv. Math. **21** (1976), 330–354. (Remark 10.3(2) only.)
- [FK] D. Favero, T. L. Kelly, *The Chern character of a coherent sheaf on a smooth projective hypersurface*, arXiv:2609.12759 (11 September 2026). (§1.3 and §1.10 only; the abstract and §1 were read in the arXiv version.)
- [Gin] V. Ginzburg, *Loop Grassmannian cohomology, the principal nilpotent and Kostant theorem*, arXiv:math/9803141 (v2). (Remark 10.4 only; §4 was read in the arXiv source.)
- [GP] A. M. Garsia, C. Procesi, *On certain graded S_n -modules and the q -Kostka polynomials*, Adv. Math. **94** (1992), 82–138. (Remark 10.4(4); Appendix A, remark after Definition A.11; Complement to Theorem 5.9.)

- [Ham] R. Amichis Luengo, *The Hammock Theorem*, Zenodo (2026). doi:10.5281/zenodo.21382543. (§1.8 only.)
- [Jum] R. Jumagulov, *The Hodge conjecture for Fermat fourfolds of odd degree at most 199*, arXiv:2608.18134 (28 July 2026). (§1.3 and §15 only; cited for the statement in its abstract.)
- [Jam] G. D. James, *The Representation Theory of the Symmetric Groups*, Lecture Notes in Mathematics **682**, Springer, 1978. (Remark 4.2(3) only.)
- [Jan] J. C. Jantzen, *Representations of Algebraic Groups*, 2nd ed., Mathematical Surveys and Monographs **107**, American Mathematical Society, 2003. (Remarks 10.3(2) and 10.4(3) only.)
- [KO] N. Koblitz, A. Ogus, *Algebraicity of some products of values of the Γ function*, Proc. Sympos. Pure Math. **33**, Part 2, Amer. Math. Soc., 1979, 343–345. (Quoted through [Ran]; not read in the original.)
- [Kol] J. Kollár, *Trento examples*, in: Classification of irregular varieties (Trento, 1990), Lecture Notes in Math. **1515**, Springer, 1992, 134–139. (§1.3 only.)
- [KLT] S. Kumar, N. Lauritzen, J. F. Thomsen, *Frobenius splitting of cotangent bundles of flag varieties*, Invent. Math. **136** (1999), 603–621. (Remark 10.4(3) only; quoted through [BRR]; not read in the original.)
- [Knu] D. E. Knuth, *Overlapping Pfaffians*, Electron. J. Combin. **3** (1996), no. 2, #R5; arXiv:math/9503234. (§8.3 and §1.10; §0–§3 and §6 were read in the arXiv version.)
- [Kos] B. Kostant, *Lie group representations on polynomial rings*, Amer. J. Math. **85** (1963), 327–404. (§1.6, §10, §14.6 and §16; quoted through [Gin]; not read in the original.)
- [LC] R. Amichis Luengo, *The Chaise Longue Theorem — Lean certificate*, version 2 (3 October 2026, every degree, and Theorem O), doi:10.5281/zenodo.23129677, and in [Rep], folder `lean/`; version 1 (29 September 2026, odd degrees) is doi:10.5281/zenodo.23045371. Both versions were read cold before release. (§1.0, §14.6 and §14.8 only.)
- [Liu] L. Liu, *Filtrations of tilting modules and costalks of parity sheaves*, arXiv:2007.12444 (24 July 2020). (Remark 10.4(5) only; the introduction was read.)
- [Lus] G. Lusztig, *Singularities, character formulas, and a q -analog of weight multiplicities*, Astérisque **101–102** (1983), 208–229. (Remark 10.4(5) only; not read in the original.)
- [Mat] O. Mathieu, *Filtrations of G -modules*, Ann. Sci. École Norm. Sup. (4) **23** (1990), no. 4, 625–644. (Remarks 10.3(2) and 10.4(3) only.)
- [Note] R. Amichis Luengo, *The Chaise Longue Theorem and the centralizer of a regular unipotent element* (supplementary note, version 1, 1 October 2026), deposited with this version of the paper in the same Zenodo record, and in [Rep], `paper/`. (§1.8 and §14.6 only; not refereed.)
- [Mlib] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), 367–381. doi:10.1145/3372885.3373824. (§14.8 only.)
- [Mil] J. Milnor, *Morse Theory*, Annals of Mathematics Studies **51**, Princeton University Press, 1963. (§7, the Lefschetz theorem on hyperplane sections; used in §12.1 and Appendix B.)
- [Miz] M. Mizukami, *Birational mappings from quartic surfaces to Kummer surfaces* (in Japanese), Master’s thesis, University of Tokyo, 1975. (§1.3 and §1.10 only; quoted from [SSvL, §3 and §6]; not read.)
- [MMRV] M. Miranda, H. Movasati, L. Rufino, R. Villaflor, *Lengths of Hodge characters in Fermat varieties*, arXiv:2609.27301 (v2, 26 September 2026). (§1.3 and §1.10 only; the abstract and §1 were read in the arXiv version.)
- [Oka] S. Okada, *Pfaffian formulas and Schur Q -function identities*, Adv. Math. **353** (2019), 446–470. doi:10.1016/j.aim.2019.07.006; arXiv:1706.01029. (§8.3 and §1.10; §2, in particular Proposition 2.3 and its proof, was read in the arXiv version.)

- [Rep] R. Amichis Luengo, *The Chaise Longue Theorem — working record*, github.com/tretoef-estrella/chaise-longue-theorem (2026). Contains, among the author’s earlier documents, *The Localization Theorem* and *The Block Decomposition* (the splitting of the group ring over F_p into blocks, June 2026), *The Watermark Theorem* (4 June 2026) and *The Double Ladder Theorem* (5 June 2026), the machine verdicts of *The Hodge–Fermat Campaign*, and every engine and log of §14. These documents have not been refereed. The repository is public since 26 September 2026; it also contains the Lean 4 project of §14.8 (folder `lean/`).
- [Ph] F. Pham, *Formules de Picard–Lefschetz généralisées et ramification des intégrales*, Bull. Soc. Math. France **93** (1965), 333–367. (Appendix B only.)
- [Ran] Z. Ran, *Cycles on Fermat hypersurfaces*, Compositio Math. **42** (1980/81), no. 1, 121–142. (Numdam CM_1980__42_1_121_0. Proposition 1.7, Proposition 1.8(i) and Theorem 4.9 were read in the original.)
- [Ric] S. Riche, *Kostant section, universal centralizer, and a modular derived Satake equivalence*, arXiv:1411.3112 (v4, 19 May 2015). (Remark 10.4(3) only; the introduction and §2.2 were read in the arXiv source.)
- [Shi79] T. Shioda, *The Hodge conjecture for Fermat varieties*, Math. Ann. **245** (1979), no. 2, 175–184. doi:10.1007/BF01428804. (Quoted as in [DS] and [Ran]; not read in the original.)
- [SK] T. Shioda, T. Katsura, *On Fermat varieties*, Tôhoku Math. J. (2) **31** (1979), no. 1, 97–115. (Quoted as in [DS] and [Ran]; not read in the original.)
- [Sofa] R. Amichis Luengo, *The Sofa Theorem*, Zenodo (2026). doi:10.5281/zenodo.21288551. (§1.8 only.)
- [SSvL] M. Schütt, T. Shioda, R. van Luijk, *Lines on Fermat surfaces*, J. Number Theory **130** (2010), no. 9, 1939–1963. (§1.3 and §1.10; §3 and §6 were read in the arXiv source.)
- [Ta] T. Tanisaki, *Defining ideals of the closures of the conjugacy classes and representations of the Weyl groups*, Tôhoku Math. J. (2) **34** (1982), no. 4, 575–585. (Appendix A, remark after Definition A.11; Complement to Theorem 5.9.)
- [Voi] C. Voisin, *Abel–Jacobi map, integral Hodge classes and decomposition of the diagonal*, J. Algebraic Geom. **22** (2013), no. 1, 141–174. (§1.3 only; Theorem 2.11 is quoted as in [AMV, §1]; not read in the original.)
- [WDL] R. Amichis Luengo, *The Watermark and Double Ladder Theorems (Verified in Lean)*, Zenodo (2026). doi:10.5281/zenodo.23062529. (Remark 12.2, §15 and §16 only; not refereed.)
- [WED] R. Amichis Luengo, *The Watermark in Every Even Dimension*, Zenodo (2026). doi:10.5281/zenodo.23091046. (Remark 12.2 and §15 only; not refereed.)
- [Was] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, 1997. (§12.1 only; not read in the original.)