

Extending OpenAI's cubic lower bound for the permanent to odd characteristic, Pfaffian representations, and polynomial entries

Karthik Sheshadri

October 28, 2026

Abstract

OpenAI's Sep 2026 preprint introduced the first cubic lower bound on the border DC of the permanent. Their preprint generalizes the method I introduced in my June 2026 preprint (<https://arxiv.org/abs/2606.15970>; see also TR26-275). However, their proof only applies over $\mathbb{C}$.

In this note, I prove that the cubic lower bound holds over every algebraically closed field of odd characteristic p . Therefore, the cubic bound no longer depends on characteristic zero. I further prove the bound for Pfaffians. Recall that lower bounds for Pfaffians imply the same bounds for determinants. Finally, I prove the bound for matrices whose entries are polynomials of degree at most a . All three results come from the same lower bound for smooth hypersurfaces. Its proof involves counting intersection points together with their multiplicities, and applies to every characteristic.

This article was written by the human author.

1 Introduction

The permanent of an $n \times n$ matrix Y is defined as

$$\text{per}_n(Y) = \sum_{\sigma} \prod_{i=1}^n Y_{i,\sigma(i)},$$

where σ runs over the permutations of $\{1, \dots, n\}$. The determinant is the same sum with the sign of σ attached to each term. Whereas the determinant can be computed quickly by Gaussian elimination, no fast method is known for the permanent.

Valiant's landmark work [6] turns this gap into a question about matrices. A determinantal representation of a polynomial F is a square matrix whose determinant is F and whose entries are affine linear forms in the variables of F , i.e., polynomials of degree at most one. The determinantal complexity $\text{dc}(F)$ is the smallest order of such a matrix. Valiant shows that a polynomial computed by a formula of size s has a determinantal representation of order linear in s . He also shows that the permanent is complete for VNP, an algebraic analogue of NP, in characteristic other than two. He conjectured that the permanent is harder than the determinant, in the sense that $\text{dc}(\text{per}_n)$ grows faster than any polynomial in n .

The border determinantal complexity $\overline{\text{dc}}(F)$ also allows approximation. It is the smallest m such that F is a limit of determinants of $m \times m$ matrices with affine linear entries. Here the limit is taken coefficient by coefficient. Every representation is also such a limit. Hence $\overline{\text{dc}}(F) \leq \text{dc}(F)$, and a lower bound on $\overline{\text{dc}}(F)$ is the stronger statement.

In their famous result, Mignon and Ressayre [3] show that $\text{dc}(\text{per}_n) \geq n^2/2$ in characteristic zero. Cai, Chen and Li [1] extend this quadratic bound to every characteristic other than two. Recall that in characteristic two, the permanent is the determinant, so no bound beyond n is possible. OpenAI's September 2026 [4] manuscript gives the first cubic bound, $\overline{\text{dc}}_{\mathbb{C}}(\text{per}_n) = \Omega(n^3)$. Its proof has two parts. First, it restricts the permanent to a linear subspace. On this subspace, the permanent becomes a smooth hypersurface of degree about $n/3$ in about $n^2/100$ variables. Secondly, as in my June preprint, it shows that a smooth hypersurface of degree d in N variables has border determinantal complexity at least $(N-1)(d-1)/(4e)$.

Both parts of that proof use characteristic zero. The first part uses factorials as weights in order to select one coefficient inside a permanent. However, since in characteristic p , every factorial $j!$ with $j \geq p$ is zero, this selection breaks down. In the second part, the proof counts the points where the hypersurface meets several of its first derivatives. It assumes that these points are simple.

However, in positive characteristic, this can fail. For example, in characteristic p every first derivative of $x_1^{p+1} + \dots + x_N^{p+1}$ is the p th power of a linear form. Hence every intersection point is repeated.

I also consider two variations of Valiant's model. Both are at least as powerful as the original, so a lower bound in either one also holds for determinants.

The first variation uses Pfaffians. A square matrix M is alternating if $M^T = -M$ and its diagonal is zero. Its Pfaffian $\text{Pf } M$ is a polynomial in the entries whose square is $\det M$. A Pfaffian representation of F is an alternating matrix with affine linear entries whose Pfaffian is F . Such a matrix has even order $2m$, and I measure it by m , its half order. Since a determinant of order m is the Pfaffian of an alternating matrix of order $2m$, I count m rather than $2m$ ((1) below). I write $\overline{\text{pc}}(F)$ for the border complexity of Pfaffian representations.

The second variation lets each entry be a polynomial of degree at most a , instead of at most one. For $a = 1$ this is Valiant's model. For a equal to the degree of F , the 1×1 matrix $[F]$ is already a representation. I add a subscript a for this model, writing $\overline{\text{dc}}_a(F)$ for determinants and $\overline{\text{pc}}_a(F)$ for Pfaffians.

To the best of my knowledge, nothing in the published literature addresses the cubic bound in positive characteristic, for Pfaffians, or for polynomial entries.

My contributions are three cubic lower bounds. Firstly, the cubic bound holds over every algebraically closed field of odd characteristic p , with a constant that depends on p . Secondly, it holds for Pfaffian representations, both over $\mathbb{C}$ and in odd characteristic. Thirdly, it holds for representations whose entries have degree at most a , divided by a .

The order of the permanent in the first result matters. Valiant's completeness theorem already makes a determinant of order k a restriction of a permanent of order polynomial in k . However, a permanent of order k^c would only give a bound of order $n^{3/c}$. My construction has order linear in k for each fixed p . Its also cogent to point out that the third result does not follow from the first. An entry of degree two can have many terms. For example, the 1×1 matrix $[x_1^2 + \dots + x_N^2]$ has one entry of degree two. Whereas, every representation of $x_1^2 + \dots + x_N^2$ with affine entries has order at least $(N-1)/(4e)$ in characteristic other than two, by Theorem 3.1.

The precise statements use the constant $B_p = 5p + 38$.

Theorem 1.1. *Let p be an odd prime and K an algebraically closed field of characteristic p . For every $n \geq 128B_p$,*

$$\overline{\text{dc}}_K(\text{per}_n) \geq \frac{n^3}{270 e B_p^3}, \quad \overline{\text{pc}}_K(\text{per}_n) \geq \frac{n^3}{540 e B_p^3}.$$

Over $\mathbb{C}$, $\overline{\text{pc}}_{\mathbb{C}}(\text{per}_n) \geq n^3/(8.8 \cdot 10^6 e)$ for every $n \geq 1408$. The same bounds hold for the exact complexities.

Theorem 1.2. *Let $k = \lfloor n/11 \rfloor$ over $\mathbb{C}$ and $k = \lfloor n/B_p \rfloor$ in odd characteristic p , and suppose $k \geq 128$. For every integer $1 \leq a \leq k/6$, over $\mathbb{C}$,*

$$\overline{\text{dc}}_a(\text{per}_n) \geq \frac{\log(4/3)}{9600} \cdot \frac{k^3}{a}, \quad \overline{\text{pc}}_a(\text{per}_n) \geq \frac{\log(4/3)}{19200} \cdot \frac{k^3}{a},$$

In characteristic p , the same bounds hold with 1008 and 2016 instead of 9600 and 19200. Hence both are $\Omega(n^3/a)$ over $\mathbb{C}$ for $a \leq n/72$, and $\Omega_p(n^3/a)$ in characteristic p for $a \leq n/(12B_p)$.

The constants are poor and depend on p . I note that some bound on a in Theorem 1.2 is necessary. In fact, the 1×1 matrix $[\text{per}_n]$ is a representation with one entry of degree n .

All three results rely on one lower bound for smooth hypersurfaces, Theorem 3.1. This holds in every characteristic. Its proof involves the following. I intersect the hypersurface with $N - 2$ general first derivatives of its equation. The intersection is a finite set of points with multiplicities, and the sum of the multiplicities is $d(d-1)^{N-2}$. I follow this sum through the limit. I then bound it from above by a Bézout count on a larger space, which also records the kernel vectors of the matrix. Since the count uses multiplicities throughout, repeated points do no harm.

For Pfaffians I don't need a second argument. Let M be alternating of order $2m$. Let E be its submatrix on the rows and columns $3, \dots, 2m$. Let M' be M with its first row and second column deleted. Then $\det M' = -\text{Pf}(E) \text{Pf}(M)$ (Lemma A.2). After a constant change of coordinates, $\text{Pf } E$ is nonzero at every point of the count. Hence near these points the count for determinants applies, because $\text{Pf } M$ is a nonzero multiple of a determinant of order $2m - 1$.

I need two more ingredients for the permanent in characteristic p . Firstly, the smooth hypersurface is a general linear section of $G_D(X) = [s^q t^q] \det(X + sI + tD)$, which is the coefficient of $s^q t^q$ in a determinant. This section is smooth, because the set of matrices X where every derivative of G_D vanishes is small (for a proof in every characteristic, refer to Theorem 3.2). Secondly, G_D must be a restriction of a permanent of order linear in k . Recall that $p - 1 = -1$ in characteristic p . This implies that if a permanent gives each cycle of a permutation one of $p - 1$ colours, it counts the permutation $(-1)^c$ times (where c is its number of cycles). Up to sign, this is the determinant. A permanent that forces exactly q of L marked entries to be used then extracts the coefficient (Theorem 4.3).

The remainder of this paper is organized as follows. Section 2 fixes the representations. Section 3 states the two geometric results that the proof needs. Section 4 builds the permanents in characteristic p , and Section 5 proves Theorems 1.1 and 1.2. Appendices A and B prove the two geometric results, whereas Appendix C builds the selectors. A reader who accepts the geometric results can skip the appendices.

2 Representations, limits and Pfaffians

In this section, I fix the matrices that are allowed and say what it means for a polynomial to be a limit of their determinants (or Pfaffians).

Notation. Throughout the article, K is an algebraically closed field of any characteristic (unless explicitly stated otherwise), and $e = \exp(1)$. For a form F in N variables, $V(F) \subset \mathbb{P}^{N-1}$ is its zero scheme, i.e., its zero set together with multiplicities.

For $w \in K^N$, the first polar $\partial_w F = \sum_j w_j \partial F / \partial x_j$ is the derivative of F in the direction w .

A bracket such as $[s^i t^j]P$ denotes the coefficient of $s^i t^j$ in P .

A zero dimensional scheme is a finite set of points and each of them has a finite dimensional local ring. Its length is the dimension of its coordinate ring over K . The length of a point is the

dimension of its local ring. For a set of simple points, the length is just the number of points. Finally, e_r is the elementary symmetric polynomial of degree r .

Definition 2.1. Fix an integer $a \geq 1$, the largest degree allowed in an entry. Consider all $m \times m$ matrices whose entries are polynomials in $x_1, \dots, x_N$ of degree at most a . Their determinants form a set of polynomials, which I call $D_{m,a}$. In the same way, the Pfaffians of alternating matrices of order $2m$ with such entries form the set $P_{2m,a}$. Every term of such a determinant or Pfaffian is a product of m entries. So both sets lie in the space of polynomials of degree at most am , and I take Zariski closures there. Over $\mathbb{C}$, the Zariski closure of either set is the set of all limits of its elements, taken coefficient by coefficient. Put

$$\overline{\text{dc}}_a(F) = \min\{m : F \in \overline{D_{m,a}}\}, \quad \overline{\text{pc}}_a(F) = \min\{m : F \in \overline{P_{2m,a}}\}.$$

The exact complexities dc_a and pc_a are defined in the same way without the closure. For $a = 1$ I drop the subscript.

Later, I will use three simple facts about these classes. I list them here for reference. Firstly, an affine substitution $x \mapsto \Lambda x + x_0$ keeps entry degrees at most a . Secondly, a nonzero scalar can be absorbed into one row of a determinant, or into an alternating matrix by a constant congruence. Thirdly, for every $m \times m$ matrix M over a commutative ring,

$$\text{Pf} \begin{pmatrix} 0 & M \\ -M^T & 0 \end{pmatrix} = (-1)^{m(m-1)/2} \det M. \quad (1)$$

Hence all four complexities can only decrease under affine restriction, so $\overline{\text{pc}}_a \leq \overline{\text{dc}}_a$. Note also that per_r is an affine restriction of per_n for $r \leq n$. To obtain this one only has to put an identity block in one corner.

3 The two geometric ingredients

The proof needs two results from algebraic geometry. The first is a lower bound for smooth hypersurfaces. The second gives a smooth hypersurface with many variables and large degree. I state both here, so that the rest of the paper can be read without their proofs. Appendix A proves the first, and Appendix B proves the second.

3.1 A lower bound for smooth hypersurfaces

Let F be a form of degree $d \geq 2$ in $N \geq 2$ variables. I say that $V(F)$ is smooth if the partial derivatives of F have no common zero on $V(F)$. The proof of the next theorem is in Appendix A. The idea is as follows. Firstly, the hypersurface meets $N - 2$ general first polars in a finite scheme of length $d(d - 1)^{N-2}$. Secondly, suppose that F is a determinant. At each point of this scheme the matrix loses rank, and the vanishing of a polar there becomes a condition on the left and right kernel vectors of the matrix. Thirdly, I add the kernel vectors as new coordinates. The scheme then becomes a set of isolated points of a system of equations of low degree. A Bézout count bounds the total length of these points by a coefficient that grows only polynomially with the order of the matrix.

Theorem 3.1. *Let F be a form of degree $d \geq 2$ in $N \geq 2$ variables over an algebraically closed field of any characteristic, with $V(F)$ smooth.*

(i) If $\overline{\text{dc}}(F) \leq m$, then $d(d-1)^{N-2} \leq 2^{N-2} \binom{2m-1}{N-1}$, and if $\overline{\text{pc}}(F) \leq m$, the same holds with $4m-3$ in place of $2m-1$. Consequently

$$\overline{\text{dc}}(F) \geq \frac{(N-1)(d-1)}{4e} + \frac{1}{2}, \quad \overline{\text{pc}}(F) \geq \frac{(N-1)(d-1)}{8e} + \frac{3}{4}.$$

(ii) If $0 < c < 1$ and $a \leq cd$, then with $L_c = \log(2/(1+c))$,

$$\overline{\text{dc}}_a(F) \geq \frac{(N-1)(1-c)L_c}{8} \cdot \frac{d}{a} + \frac{1}{2}, \quad \overline{\text{pc}}_a(F) \geq \frac{(N-1)(1-c)L_c}{16} \cdot \frac{d}{a} + \frac{3}{4}.$$

In addition, $\overline{\text{dc}}_a(F)$ and $\overline{\text{pc}}_a(F)$ are at least $\lceil d/a \rceil$.

Proposition A.9 in Appendix A shows that these bounds have the right order of growth.

3.2 A smooth hypersurface of large degree

Theorem 3.1 applies to any smooth hypersurface. To reach the permanent, I need one particular smooth hypersurface with large Nd that is a restriction of a small permanent. It comes from the polynomial G_D below, restricted to a general linear subspace. Such a restriction is smooth when the critical set of G_D is small. Here the critical set is the set of points at which every partial derivative of G_D vanishes. Theorem 3.2 below bounds the dimension of the critical set in every characteristic. Its proof in Appendix B follows the determinant side of [4]. The only outside input is a dimension bound for plane curves of given genus [2].

Fix $k \geq 2$ and put

$$q = \left\lfloor \frac{k-1}{3} \right\rfloor, \quad d = k - 2q, \quad c = d - 1, \quad T = \binom{q+2}{2},$$

so that $2q + c = k - 1$ and $c \geq q$. I choose distinct $\theta_1, \dots, \theta_k \in K$ and let $D = \text{diag}(\theta_1, \dots, \theta_k)$. Define

$$G_D(X) = [s^q t^q] \det(X + sI_k + tD), \quad \Gamma_D = \{X \in \text{Mat}_k(K) : \nabla G_D(X) = 0\},$$

where the gradient is taken with respect to all k^2 entries of X .

Theorem 3.2. *In every characteristic, $\dim \Gamma_D \leq k^2 + k - T$.*

The idea of the proof is as follows. To each matrix X I attach a plane curve C_X of degree k . Its normalisation defect $\delta(C_X)$ measures its singularities. It is the length of $\nu_* \mathcal{O}_{\tilde{C}} / \mathcal{O}_C$, where $\nu : \tilde{C} \rightarrow C$ is the normalisation, i.e., the smooth curve that maps onto C and is an isomorphism over the smooth points of C . For example, a node contributes one to δ . Firstly, if $X \in \Gamma_D$, then $\delta(C_X) \geq T$. Secondly, the curves of degree k with $\delta \geq T$ form a set of codimension at least T . Thirdly, the matrices with a given curve form a set of dimension at most $k(k-1)/2$.

I now use Theorem 3.2 to obtain the smooth hypersurface. Since Γ_D has codimension at least $T - k$, a general linear section can have up to $T - k$ variables and still be smooth. I take all of them.

Corollary 3.3. *Let $k \geq 128$, let q, d and T be as above, and put $N = T - k$. For a general linear map $\Lambda : K^N \rightarrow \text{Mat}_k(K)$, the form $F = G_D \circ \Lambda$ is nonzero of degree d , and $V(F) \subset \mathbb{P}^{N-1}$ is smooth. Moreover*

$$N - 1 \geq \frac{k^2}{21}, \quad d - 1 \geq \frac{k - 1}{3}, \quad d \geq \frac{k}{3}. \quad (2)$$

Appendix B proves Theorem 3.2 and Corollary 3.3.

4 Permanents in odd characteristic

Corollary 3.3 gives a smooth restriction of G_D . However, G_D is not yet a restriction of a permanent. Over $\mathbb{C}$, the manuscript [4] selects the coefficient of $s^q t^q$ inside a permanent, using factorials as weights. In characteristic p this fails once $p \leq q$. In this section, I replace that step by two constructions. The first is a permanent of linear order that forces exactly q of L marked entries to be used. The second writes the determinant of order k as a permanent of order $(5p - 4)k$. From now on, p is an odd prime and K has characteristic p .

Consider a matrix as a weighted bipartite graph between its rows and its columns. A perfect matching would pair every row with a distinct column. Further, its weight is the product of the entries that it uses. The permanent is the sum of the weights of all such perfect matchings. A marked entry is an entry that I single out, and its selection bit shows whether a given matching uses it or not. If a marked entry is part of an entry's sum, only that summand is meant. All constants below lie in $\mathbb{Z}[1/2]$. Hence every identity below holds in every odd characteristic.

For our purpose, both constructions need a way to force two marked entries to be either (i) used together or (ii) not at all. This is carried out by the equality gadget. It does so by adding three new rows and three new columns, and is shown in Appendix C.

4.1 A selector of linear order

Here I describe my selector. The selector must check that exactly q of L bits are equal to one. I do so using standard binary addition. A circuit of full adders adds the bits, and its output is fixed to the binary digits of q . Appendix C builds the circuit and proves the following proposition.

Proposition 4.1. *For $L \geq 1$ and $0 \leq q \leq L$ there is a matrix $E_{L,q}(z)$ of order at most $17L$, with entries in $\mathbb{Z}[1/2] \cup \{z_1, \dots, z_L\}$, such that $\text{per } E_{L,q} = e_q(z_1, \dots, z_L)$. Each z_i occurs in one entry, and no row or column contains two of them.*

Remark 4.2. Let $e_1, \dots, e_L$ be marked entries of weights w_i in some matrix. Couple each e_i by an equality gadget to the z_i entry of a disjoint copy of $E_{L,q}$, with z_i set to 1. The permanent of the result is the sum of the weights of the matchings of the original matrix that use exactly q of the e_i . The order grows by at most $20L$.

4.2 The determinant as a permanent

I now write the determinant as a permanent. Recall that $p - 1 = -1$ in characteristic p . Suppose that each cycle of a permutation $\sigma \in S_k$ receives one of $r = p - 1$ colours. Then σ is counted $r^{\text{cyc}(\sigma)} = (-1)^{\text{cyc}(\sigma)}$ times, where $\text{cyc}(\sigma)$ is the number of cycles of σ . Since $(-1)^{\text{cyc}(\sigma)} = (-1)^k \text{sgn } \sigma$, this count gives the determinant up to sign. I use r copies of the matrix, one for each colour. A small gate ensures that each index appears in exactly one copy. The count gate is

$$C_r(z) = \begin{pmatrix} \text{diag}(z_1, \dots, z_r) & \mathbf{1} \\ \mathbf{1}^T & 0 \end{pmatrix}, \quad \text{per } C_r(z) = e_{r-1}(z).$$

The formula emerges from the observation that a perfect matching leaves out exactly one diagonal entry (say the j th). It is then completed in one way, through the last row to column j and from row j to the last column.

Theorem 4.3. *Let p be an odd prime and $r = p - 1$.*

- (i) *For every $k \times k$ matrix A over a commutative K -algebra there is a matrix $B(A)$ of order $(5p - 4)k$, whose entries are entries of A or constants, with $\text{per } B(A) = (-1)^k \det A$.*

(ii) For $q = \lfloor (k-1)/3 \rfloor$, the polynomial $(-1)^k G_D(X)$ is the permanent of a matrix of order at most $(5p+38)k$ whose entries are entries of X or constants. In particular, G_D is an affine restriction of $\text{per}_{n'}$ for some $n' \leq (5p+38)k$.

Proof. For (i), I take r disjoint copies of A , with rows and columns (c, i) in copy c . I add to each diagonal entry (c, i) a marked summand 1, called the bypass. For each index i , I add a count gate, and I couple the bypass at (c, i) to the c th diagonal entry of that gate by an equality gadget, for $c = 1, \dots, r$. The gate makes exactly $r-1$ of the bypasses at i be used. Hence exactly one copy has the index i free for the entries of A . Let J_c be the set of indices that are free in copy c . Then $(J_1, \dots, J_r)$ runs over the ordered partitions of $\{1, \dots, k\}$, with empty parts allowed, and

$$\text{per } B(A) = \sum_{J_1 \sqcup \dots \sqcup J_r = \{1, \dots, k\}} \prod_{c=1}^r \text{per } A_{J_c, J_c} = \sum_{\sigma \in S_k} r^{\text{cyc}(\sigma)} \prod_i A_{i, \sigma(i)}.$$

The second equality holds because a term on the left is a permutation together with a colour for each of its cycles. In characteristic p the right side is $(-1)^k \det A$. The order is rk for the copies, $(r+1)k$ for the gates and $3rk$ for the gadgets, which is $(5r+1)k$ in all.

For (ii), I apply (i) to X . For each i , I add two vertices s_i and t_i , each with its own row and column, carrying marked loops of weights z_i and w_i . For every copy c , I add the entries 1 from (c, i) to s_i and back, θ_i from (c, i) to t_i , and 1 from t_i to (c, i) . A new vertex can attach only to the copy in which i is free. There, it serves as an extra diagonal entry, equal to 1 for s_i and to θ_i for t_i . Otherwise it uses its loop. Note that s_i and t_i cannot both attach at i . With all $z_i = z$ and all $w_i = w$, the colouring count of (i) gives

$$H(X, z, w) = (-1)^k z^k w^k \det(X + z^{-1}I + w^{-1}D), \quad [z^{k-q} w^{k-q}]H = (-1)^k G_D(X).$$

Remark 4.2, applied to the loops z_i with $E_{k, k-q}$ and to the loops w_i with a second copy, selects this coefficient. The order is at most $(5r+1)k + 2k + 2 \cdot 20k = (5p+38)k$. Finally, a row scaling removes the sign. $\square$

The identities for J , the eight minors of C used in Appendix C, (7), Lemma A.2 in orders 2, 4 and 6, part (i) over $\mathbb{Q}$ for $(p, k) = (3, 2), (3, 1), (5, 1)$, and the formula for H with $p = 3$ and $k \leq 2$ were all checked by computing them exactly. The proofs do not depend on these checks.

5 Proofs of the main theorems

In this section, I combine the smooth restriction of Section B, its realisation as a permanent from Section 4, and the bounds of Section A.3. I begin with the smooth restriction in each characteristic. In odd characteristic p and for $k \geq 128$, Corollary 3.3 gives a form $F = G_D \circ \Lambda$ with $V(F)$ smooth and the parameters (2). By Theorem 4.3(ii), F is an affine restriction of $\text{per}_{n'}$ with $n' \leq B_p k$. Over $\mathbb{C}$, the construction of [4] gives a smooth form of the same degree d in $N_{\mathbb{C}} = \lfloor k^2/100 \rfloor$ variables as an affine restriction of per_n whenever $n \geq 11k$. Here $N_{\mathbb{C}} - 1 \geq k^2/200$. Whereas that construction selects a coefficient inside a permanent and moves the critical set bound to the permanent through characteristic two, the construction in characteristic p uses G_D directly and then Theorem 4.3. In particular, no bound over $\mathbb{C}$ is reduced modulo p .

Proof of Theorem 1.1. In characteristic p , (2) gives $(N-1)(d-1) \geq k^2(k-1)/63 \geq k^3/64$. Hence Theorem 3.1(i) gives $\overline{\text{dc}}(F) \geq k^3/(256e)$ and $\overline{\text{pc}}(F) \geq k^3/(512e)$. The restrictions are fixed before

any representation is chosen, and affine restriction preserves the closures of the classes. Hence these bounds hold for per_n whenever F is a restriction of per_n .

I take $k = \lfloor n/B_p \rfloor$. If $n \geq 128B_p$, then $k \geq 128$ and $k \geq n/B_p - 1 \geq \frac{127}{128} \cdot \frac{n}{B_p}$. Padding with an identity block makes the permanent of order at most $B_p k \leq n$ a restriction of per_n . Since $256 \cdot (128/127)^3 < 270$, this gives the two bounds.

Over $\mathbb{C}$, I take $k = \lfloor n/11 \rfloor$. If $n \geq 1408$, then $k \geq 128$ and $k \geq \frac{127}{128} \cdot \frac{n}{11}$. Further, $(N_{\mathbb{C}} - 1)(d - 1) \geq (k^2/200)(k/4) = k^3/800$, so $\overline{\text{pc}}_{\mathbb{C}}(\text{per}_n) \geq k^3/(6400e)$. Since $11^3 \cdot 6400 \cdot (128/127)^3 < 8.8 \cdot 10^6$, this gives the bound over $\mathbb{C}$. Finally, exact complexity is at least border complexity. $\square$

Proof of Theorem 1.2. I use the same F . Since $d \geq k/3$, the condition $a \leq k/6$ gives $a \leq d/2$. Hence Theorem 3.1(ii) with $c = 1/2$ gives $\overline{\text{dc}}_a(F) \geq \log(4/3)(N - 1)d/(16a)$ and $\overline{\text{pc}}_a(F) \geq \log(4/3)(N - 1)d/(32a)$. In characteristic p , (2) gives $(N - 1)d \geq k^3/63$. Over $\mathbb{C}$, $(N_{\mathbb{C}} - 1)d \geq k^3/600$. Affine restriction keeps entry degrees, so the bounds pass to per_n . The ranges in n follow from $k \geq n/12$ and $k \geq n/(2B_p)$. $\square$

I end with the limits of these results. The constants in characteristic p depend on p through B_p^3 . Hence the bounds improve on the quadratic bound of [1] only when p is small compared with $n^{1/3}$. I claim nothing that is uniform in p . I also claim nothing in characteristic two. Further, the cubic order is the limit of this method. A preliminary manuscript by Sheshadri [5] shows that arguments which read an invariant of a hypersurface through a corank one kernel system cannot prove more than a constant times Nd for a form of degree d in N variables. For the restrictions used here, Nd is of order n^3 .

6 Use of artificial intelligence

The mathematics was developed with ChatGPT Astra during a discussion on OpenAI's cubic bound. Some proofs were later refined in conversation with Claude Opus 5.5

A Proof of the bound for smooth hypersurfaces

In this appendix, I prove Theorem 3.1. I begin by realising a border representation by a single matrix, and I prove two identities for Pfaffians.

A.1 Limits and Pfaffians

A border representation is a limit of matrices, and I want a single matrix that represents it. The next lemma provides one, with entries in a field of Laurent series.

Lemma A.1. *If $F \in \overline{D_{m,a}}$, respectively $F \in \overline{P_{2m,a}}$, then there is a matrix $M(t, x)$, square of order m , respectively alternating of order $2m$, with entries in $K((t))[x]$ of x -degree at most a , such that $P = \det M$, respectively $P = \text{Pf } M$, lies in $K[[t]][x]$ and $P(0, x) = F$.*

Proof. The class is the image of a space of matrices under a polynomial map. Hence its closure is irreducible, and it contains a curve through F on which the image is dense. I lift this curve to a curve of matrices, complete the normalisation of the lifted curve, and choose a point over F . After replacing the uniformiser by one of its roots if necessary, the completed local ring at this point is $K[[t]]$. The matrix entries then become Laurent series in t . The coefficients of the image polynomial are regular at the chosen point, and there they equal the coefficients of F . $\square$

I write $\mathbb{L}$ for an algebraic closure of $K((t))$. Points over the field $K((t))$ are taken over $\mathbb{L}$, and lengths are compared over $K[[t]]$.

I now turn to Pfaffians. The Pfaffian of an alternating matrix M of order $2m$ is a signed sum over the perfect matchings of $\{1, \dots, 2m\}$. A perfect matching splits these indices into m pairs, and its term is the product of the entries M_{ij} over its pairs $\{i, j\}$ with $i < j$. The Pfaffian has integer coefficients, so it makes sense in every characteristic. The matchings that contain a fixed pair $\{i, j\}$ contribute M_{ij} times the Pfaffian of the remaining indices, with one common sign. Therefore, as a polynomial in the independent entries M_{ij} with $i < j$,

$$\frac{\partial \text{Pf } M}{\partial M_{ij}} = \pm \text{Pf } M_{ij}, \quad (3)$$

where M_{ij} is M with rows and columns i and j removed.

The next identity lets me reduce Pfaffians to determinants. It writes a Pfaffian, up to a factor, as the determinant of a submatrix of one order less.

Lemma A.2. *Let M be an alternating matrix of order $2m \geq 2$ over a commutative ring. Let E be its principal submatrix on the indices $3, \dots, 2m$, with $\text{Pf } E = 1$ when $m = 1$, and let M' be the matrix of order $2m - 1$ obtained from M by deleting row 1 and column 2. Then*

$$\det M' = -\text{Pf}(E) \text{Pf}(M).$$

Proof. Both sides are polynomials with integer coefficients in the entries M_{ij} with $i < j$. Hence I may take these entries to be independent indeterminates over $\mathbb{Q}$. Then E is invertible. Write

$$M = \begin{pmatrix} A & B \\ -B^T & E \end{pmatrix}$$

with A of order two, and let B_1 and B_2 be the rows of B . Put $\Sigma = A + BE^{-1}B^T$ and $G = \begin{pmatrix} I_2 & 0 \\ E^{-1}B^T & I \end{pmatrix}$. Since $E^T = -E$, multiplying out gives $G^T M G = \Sigma \oplus E$. Since $\det G = 1$, it follows that $\text{Pf } M = \Sigma_{12} \text{Pf } E$. On the other hand,

$$M' = \begin{pmatrix} M_{21} & B_2 \\ -B_1^T & E \end{pmatrix}.$$

The Schur complement formula therefore gives $\det M' = \det E \cdot (M_{21} + B_2 E^{-1} B_1^T) = \det E \cdot \Sigma_{21}$. Finally, $\det E = (\text{Pf } E)^2$ and $\Sigma_{21} = -\Sigma_{12}$. Hence $\det M' = -(\text{Pf } E)^2 \Sigma_{12} = -\text{Pf}(E) \text{Pf}(M)$. $\square$

Note that the congruence in this proof also proves the identity $\text{Pf } M = \text{Pf } E \cdot \Sigma_{12}$ in general.

A.2 The count for smooth hypersurfaces

In this subsection, I prove the count for smooth hypersurfaces that all three results rest on. Throughout, $F \in K[x_1, \dots, x_N]$ is a form of degree $d \geq 2$ with $N \geq 2$, and $V(F) \subset \mathbb{P}^{N-1}$ is smooth, i.e., the partial derivatives of F have no common zero on $V(F)$.

Two lemmas make this count survive the passage to a limit. The first says that an isolated point of a limit does not disappear before the limit. Instead, its length is shared among isolated points of the family over $K((t))$.

Lemma A.3. *Let Y be a smooth variety of dimension r over an algebraically closed field, and let $\mathcal{Z} \subset Y \times \operatorname{Spec} K[[t]]$ be cut out locally by r equations. Let b be an isolated point of the special fibre $\mathcal{Z}_0$, i.e., of the member at $t = 0$, and let $\ell(b)$ be its length. Then the generic fibre $\mathcal{Z}_\eta$, i.e., the member over $K((t))$, has a finite set $S(b)$ of isolated points over $\mathbb{L}$ whose lengths add up to $\ell(b)$. The sets $S(b)$ for different b are disjoint. Further, a function on $\mathcal{Z}$ that does not vanish at b vanishes at no point of $S(b)$.*

Proof. In local coordinates u on Y at b , the completed local ring of $\mathcal{Z}$ is $B = K[[t, u]]/(f_1, \dots, f_r)$. The ring B/tB is Artinian of length $\ell(b)$. Hence $t, f_1, \dots, f_r$ is a system of parameters of a regular local ring, and therefore a regular sequence in any order. In particular, t is a nonzerodivisor on B . Since B is complete in the t -adic topology and B/tB is finite, B is a free $K[[t]]$ -module of rank $\ell(b)$. Since b is isolated in its fibre and $K[[t]]$ is henselian, $\operatorname{Spec} B$ is an open and closed part of a neighbourhood of b that is finite over $K[[t]]$. Its generic fibre consists of isolated points of $\mathcal{Z}_\eta$ of total length $\ell(b)$, and I let $S(b)$ be the set of these points. A point of a finite $K[[t]]$ -scheme specialises to exactly one closed point, which gives disjointness. Finally, a unit of B stays a unit after t is inverted. $\square$

The second lemma is a form of Bézout's theorem that counts only isolated points. It allows the intersection to have extra components, which I cannot rule out.

Lemma A.4. *Let $Y = \mathbb{P}^{b_1} \times \dots \times \mathbb{P}^{b_c}$ over an algebraically closed field, let $r = \dim Y$, and let $D_1, \dots, D_r$ be effective divisors with multidegrees $\delta_1, \dots, \delta_r \in \mathbb{Z}_{\geq 0}^c$. Then the isolated points of $D_1 \cap \dots \cap D_r$ have total length at most the coefficient β of $H_1^{b_1} \dots H_c^{b_c}$ in $\prod_{i=1}^r (\delta_{i1} H_1 + \dots + \delta_{ic} H_c)$. This holds whatever the rest of the intersection looks like.*

Proof. Suppose first that r divisors of these multidegrees meet in a finite scheme. Then their equations form a regular sequence at each point, and the local lengths are intersection multiplicities. Hence the total length is the intersection number β , computed in $\mathbb{Z}[H_1, \dots, H_c]/(H_1^{b_1+1}, \dots, H_c^{b_c+1})$. The systems $|\mathcal{O}_Y(\delta_i)|$ are base point free, so general members D'_i meet in a finite scheme. Let s_i and s'_i be sections defining D_i and D'_i , and let $D_i(\lambda)$ be the divisor of $s_i + \lambda s'_i$. These divisors meet in a finite scheme at $\lambda = 1$. Hence they also meet in a finite scheme over the generic point of the λ -line, and there the total length is β . By Lemma A.3, with λ in place of t , each isolated point of $D_1 \cap \dots \cap D_r$ accounts for a separate part of that total, equal to its own length. $\square$

I now return to F . The next lemma gives the scheme that I count.

Lemma A.5. *For general $w_1, \dots, w_{N-2} \in K^N$, the scheme $Z = V(F, \partial_{w_1} F, \dots, \partial_{w_{N-2}} F) \subset \mathbb{P}^{N-1}$ is finite of length $\mu = d(d-1)^{N-2}$.*

Proof. Since $V(F)$ is smooth, the polars $\partial_w F$ have no common zero on $V(F)$. Hence they form a base point free system on $V(F)$, and general members cut $V(F)$ properly. Bézout's theorem for this proper intersection gives the length. $\square$

Note that Z need not be reduced. In characteristic p it can have fewer points than its length. I never pass from Z to its set of points.

Now suppose that F lies in $\overline{D_{m,a}}$ or in $\overline{P_{2m,a}}$, and let $P = \det M$ or $P = \operatorname{Pf} M$ be as in Lemma A.1. I choose coordinates in which x_N vanishes at no point of Z , and I put $\Pi = \{x_N = 1\} \subset \mathbb{A}^N$. Let

$$\mathcal{Z} = V(P, \partial_{w_1} P, \dots, \partial_{w_{N-2}} P) \subset \Pi \times \operatorname{Spec} K[[t]].$$

Here each derivative is taken on $\mathbb{A}^N$ in the direction $w_j \in K^N$, and then restricted to Π . The special fibre of $\mathcal{Z}$ is Z .

Lemma A.6. *The generic fibre $\mathcal{Z}_\eta$ has a finite set S of isolated points over $\mathbb{L}$ whose lengths add up to μ . At each $z \in S$ there is $w_0 \in K^N$ with $\partial_{w_0} P(z) \neq 0$.*

Proof. I apply Lemma A.3 to the $N - 1$ equations on Π at every point b of Z , and I let S be the union of the sets $S(b)$. Since $V(F)$ is smooth, there is w_0 with $\partial_{w_0} F(b) \neq 0$. Since $\partial_{w_0} P$ specialises to $\partial_{w_0} F$, the last part of Lemma A.3 gives $\partial_{w_0} P(z) \neq 0$ for $z \in S(b)$. $\square$

The next lemma lifts the points of S to a space that also records kernel vectors. I state it for any square matrix whose determinant is a nonzero multiple of P near S . This is all that the Pfaffian case needs.

Lemma A.7. *Let M' be a square matrix of order h whose entries are polynomials in x of degree at most a with coefficients in $K((t))$. Suppose that $\det M' = gP$ for a polynomial g that vanishes at no point of S . Then*

$$d(d-1)^{N-2} \leq \beta_a(h) := [H^{N-1}U^{h-1}V^{h-1}] (aH + V)^h (aH + U)^{h-1} ((a-1)H + U + V)^{N-2}. \quad (4)$$

Proof. Let $z \in S$. Since $P(z) = 0$, the derivative of $\det M'$ at z in the direction w_0 is $g(z) \partial_{w_0} P(z)$, which is nonzero. The derivative of a determinant with respect to an entry is a cofactor. Hence some cofactor of $M'(z)$ is nonzero, and $M'(z)$ has rank exactly $h - 1$. Its right and left kernels are lines $[v_z]$ and $[u_z]$, and $\text{adj } M'(z) = c v_z u_z^T$ with $c \neq 0$. A constant change of basis in the column space multiplies $\det M'$ by a nonzero constant. Hence I may assume that the last coordinate of every v_z is nonzero.

I homogenise the entries of M' to degree a with x_N , and those of $M'_w = \partial_w M'$ to degree $a - 1$. On $Y = \mathbb{P}^{N-1} \times \mathbb{P}_u^{h-1} \times \mathbb{P}_v^{h-1}$ consider

$$M'v = 0, \quad (u^T M')_j = 0 \quad (j < h), \quad u^T M'_{w_i} v = 0 \quad (1 \leq i \leq N-2). \quad (5)$$

These are h , $h-1$ and $N-2$ equations of multidegrees $(a, 0, 1)$, $(a, 1, 0)$ and $(a-1, 1, 1)$, so there are $\dim Y$ equations in all. I claim that $\zeta_z = (z, [u_z], [v_z])$ is an isolated point of (5), and that its local scheme is isomorphic to that of $\mathcal{Z}_\eta$ at z . The points ζ_z are distinct, since their first coordinates are. Hence the claim, Lemma A.6 and Lemma A.4 give $\mu \leq \beta_a(h)$.

To prove the claim, I work in the local ring of Y at ζ_z , on the charts $x_N = 1$, $v_h = 1$ and $u_i = 1$ for an index i with $(u_z)_i \neq 0$. The identity

$$v_h(u^T M')_h = u^T(M'v) - \sum_{j < h} v_j(u^T M')_j$$

puts the omitted equation $(u^T M')_h = 0$ in the ideal of (5). The (i, h) cofactor of $M'(z)$ is $c(v_z)_h(u_z)_i$, which is nonzero. Hence, after moving row i and column h to the front, I can write

$$M' = \begin{pmatrix} \alpha & \rho \\ \gamma & E' \end{pmatrix}, \quad u = \begin{pmatrix} 1 \\ u' \end{pmatrix}, \quad v = \begin{pmatrix} 1 \\ v' \end{pmatrix},$$

with E' invertible near z . The kernel equations say that $v' = -E'^{-1}\gamma$, that $u'^T = -\rho E'^{-1}$, and that $\sigma = 0$, where $\sigma = \alpha - \rho E'^{-1}\gamma$. Differentiating gives $\partial_w \sigma = u'^T(\partial_w M')v$ for every direction w . Therefore, after u' and v' are eliminated, the system on the base is $\sigma = \partial_{w_1} \sigma = \dots = \partial_{w_{N-2}} \sigma = 0$. Finally, $\det M' = \pm \det E' \cdot \sigma = gP$, where $\det E'$ and g are units. Hence σ is a unit multiple of P , and the ideals $(\sigma, \partial_{w_1} \sigma, \dots)$ and $(P, \partial_{w_1} P, \dots)$ coincide. $\square$

Proposition A.8. *If $\overline{\text{dc}}_a(F) \leq m$, then $d(d-1)^{N-2} \leq \beta_a(m)$. If $\overline{\text{pc}}_a(F) \leq m$, then $d(d-1)^{N-2} \leq \beta_a(2m-1)$.*

Proof. For determinants, I take $M' = M$ and $g = 1$ in Lemma A.7. For Pfaffians, fix $z \in S$. Since $\partial_{w_0} P(z) \neq 0$, the chain rule and (3) give indices $i < j$ with $\text{Pf } M_{ij}(z) \neq 0$. Replacing M by $Q^T M Q$ for a constant $Q \in GL_{2m}(K)$ multiplies P by $\det Q$. This changes none of the schemes above, and it keeps the entry degrees. For each z , the Pfaffian of the principal submatrix of $Q^T M(z) Q$ on the indices $3, \dots, 2m$ is a polynomial in Q . It does not vanish at a permutation matrix that sends i and j to 1 and 2. Since S is finite, one Q makes all of these Pfaffians nonzero. With this Q , let E be that principal submatrix and M' the matrix M with row 1 and column 2 deleted. By Lemma A.2, $\det M' = -\text{Pf}(E) P$. Hence Lemma A.7 applies with $h = 2m - 1$ and $g = -\text{Pf } E$. $\square$

A.3 Numerical bounds and sharpness

Proposition A.8 is an inequality between d , N and the order of the matrix. In this subsection, I solve it for the order, which proves Theorem 3.1. I then check on Fermat forms that the answer has the right size. For affine linear entries, the coefficient $\beta_1(h)$ is bounded by a single binomial coefficient.

Proof of Theorem 3.1. Put $r = N - 1$ and $\kappa = 2h - 1$. All coefficients of the polynomial in (4) are nonnegative. Hence setting $U = V$ and then dehomogenising can only increase the coefficient, and

$$\beta_a(h) \leq [t^r] (1 + at)^\kappa (2 + (a - 1)t)^{r-1}.$$

For $a = 1$ the right hand side is $2^{r-1} \binom{\kappa}{r}$. With $h = m$ for determinants and $h = 2m - 1$ for Pfaffians, Proposition A.8 gives the two inequalities in (i). Note that $d(d - 1)^{r-1} \geq (d - 1)^r$ and $\binom{\kappa}{r} \leq (e\kappa/r)^r$. Hence the inequalities imply $d - 1 \leq 2^{(r-1)/r} e\kappa/r \leq 2e\kappa/r$, i.e., $\kappa \geq r(d - 1)/(2e)$. Substituting $\kappa = 2m - 1$ and $\kappa = 4m - 3$ gives the bounds on $\overline{dc}$ and $\overline{pc}$.

For (ii), nonnegativity gives $[t^r]f(t) \leq f(\tau)/\tau^r$ for every $\tau > 0$. I take $\tau = 4/(d - a)$, which is positive because $a \leq cd < d$. Then $a - 1 + 2/\tau = (d + a - 2)/2$, and rearranging gives

$$\kappa \log \left(1 + \frac{4a}{d - a} \right) \geq (N - 2) \log \frac{2(d - 1)}{d + a - 2} + \log \frac{4d}{d - a}.$$

Since $a \leq cd$, it follows that $2(d - 1)/(d + a - 2) \geq 2/(1 + c)$. Further, the last term is at least $\log 4$, which is at least L_c , and the left side is at most $4a\kappa/((1 - c)d)$. Hence $\kappa \geq (N - 1)(1 - c)L_c d/(4a)$, which is (ii). The bound $\lceil d/a \rceil$ holds because a determinant of order m , or a Pfaffian of half order m , with entries of degree at most a has degree at most am , and so do its limits. $\square$

I now show that these bounds have the right order of growth. To do so, I use the Fermat forms.

Proposition A.9. *If the characteristic does not divide d , the Fermat form $F_{N,d} = x_1^d + \dots + x_N^d$ defines a smooth hypersurface, and both $\overline{dc}_a(F_{N,d})$ and $\overline{pc}_a(F_{N,d})$ are at most $N(\lceil d/a \rceil - 1) + 1$. So Theorem 3.1(i) is tight up to the factor $4e$ for determinants and $8e$ for Pfaffians, and (ii) is tight up to a constant depending on c .*

Proof. The gradient $(dx_i^{d-1})_i$ vanishes only at the origin, so $V(F_{N,d})$ is smooth. Let $h = \lceil d/a \rceil$. Take N directed paths of h edges from a source to a sink that share no other vertices. Label the i th path by $h - 1$ copies of x_i^a and one copy of $x_i^{d-a(h-1)}$. Then the sum over the paths of the products of their labels is $F_{N,d}$. Let A_G be the adjacency matrix of this graph in a topological order. Then $\det(I - A_G) = 1$, and the (source, sink) entry of $(I - A_G)^{-1}$ is $F_{N,d}$. By the cofactor formula, deleting the row of the sink and the column of the source gives, up to sign, a determinantal representation of order $N(h - 1) + 1$ with entries of degree at most a . Equation (1) gives the Pfaffian bound. $\square$

Recall the forms $\sum_i x_i^{p+1}$ from the introduction. More generally, in characteristic p the forms $\sum_i x_i^{p^b+1}$ are smooth, and their general polars are p^b th powers of linear forms. Hence their polar scheme has $p^b + 1$ points, but its length is $(p^b + 1)p^{b(N-2)}$. Note that a count of points instead of lengths would lose the factor $p^{b(N-2)}$ here. Theorem 3.1 applies to these forms, and by Proposition A.9 it is tight on them.

B Proof of the critical set bound

In this appendix, I prove Theorem 3.2 and Corollary 3.3. I keep the notation of Section 3.

The spectral curve. For a matrix X , let

$$M = sI_k + tD + uX, \quad F_X(s, t, u) = \det M, \quad C_X = V(F_X) \subset \mathbb{P}^2.$$

Note that $\det(X + sI + tD) = F_X(s, t, 1)$, and that the coefficient of $s^q t^q$ there has degree d in X . Hence $G_D(X) = [s^q t^q u^d] F_X$. I need three properties of $C = C_X$. Firstly, C is reduced. Indeed, on the line $u = 0$ the form F_X equals $\prod_i (s + t\theta_i)$, a product of distinct linear forms. A repeated factor of F_X would either be divisible by u or restrict to a repeated factor on $u = 0$. Hence F_X has no repeated factor. Secondly, every component of C passes through one of the points $P_i = [-\theta_i : 1 : 0]$. At P_i the matrix M is diagonal with exactly one zero entry, so it has rank $k - 1$. Thirdly, F_X is monic in s . Hence the projection $\pi : C \rightarrow \mathbb{P}^1$, $[s : t : u] \mapsto [t : u]$, is finite and flat of degree k , and $\pi_* \mathcal{O}_C = \bigoplus_{j=0}^{k-1} \mathcal{O}_{\mathbb{P}^1}(-j)$. A general fibre of π consists of k distinct points, because the discriminant in s does not vanish at $u = 0$. I put $\mathcal{E} = \pi_* \mathcal{O}_C(k - 1) = \bigoplus_j \mathcal{O}_{\mathbb{P}^1}(k - 1 - j)$.

The adjugate scheme. Consider the matrix of cofactors and transpose it. This matrix, M , is the adjugate, so $M \operatorname{adj} M = \det M \cdot I$. Observe that its entries are forms of degree $k - 1$. Let $\mathcal{J} \subseteq \mathcal{O}_C$ consist of all sums obtained by multiplying the entries of $\operatorname{adj} M$ by functions on C . Let $Z = V_C(\mathcal{J})$ be the scheme where all these entries vanish. We keep track of the full scheme structure, including multiplicities. Since $\operatorname{adj} M$ is nonzero at the points P_i , the scheme Z is finite. I keep its full scheme structure.

The next lemma shows that every form of degree $k - 1$ vanishing on Z is a linear combination of the entries of $\operatorname{adj} M$.

Lemma B.1. *Every form of degree $k - 1$ in s, t, u that vanishes on Z is a K -linear combination of the entries of $\operatorname{adj} M$.*

Proof. Put $A = tD + uX$, and let $\psi : \operatorname{Mat}_k(\mathcal{O}_{\mathbb{P}^1}) \rightarrow \mathcal{E}$ send Y to $\operatorname{tr}(Y \operatorname{adj} M)$. On C , $M \operatorname{adj} M = 0$, so $s \operatorname{adj} M = -A \operatorname{adj} M$. On each chart, consider all linear combinations of the entries of $\operatorname{adj} M$. I allow coefficients that are functions on the chart. Note here that multiplying any such combination by s gives another combination of the same kind.

Every function on C over this chart can be expressed using s and functions on the chart. Hence these combinations are closed under multiplication by any function on C . Therefore, these form the ideal generated by the entries of $\operatorname{adj} M$. Here, an ideal simply means a collection that is closed under addition and multiplication by functions on C .

It follows that

$$\operatorname{im} \psi = \pi_*(\mathcal{J}(k - 1)).$$

Here, $\operatorname{im} \psi$ means all the outputs of ψ . The notation π_* means that I view sections on C as sections over the base. The $(k - 1)$ records the degree shift.

Next, consider $\ker \psi$. This is the set of inputs that ψ sends to zero.

Take any $Y \in \text{Mat}_k(\mathcal{O}(-1))$. This is a $k \times k$ matrix whose entries have the prescribed degree shift -1 . The matrix $AY - YA$ belongs to $\ker \psi$. Such a difference is called a commutator. It belongs to the kernel because A commutes with $\text{adj } M$. In other words, $A \text{adj } M = (\text{adj } M)A$.

At the point $[t : u] = [1 : 0]$, the matrix A becomes D . The commutators therefore have the form $DY - YD$. Since D has distinct diagonal entries, these matrices can have arbitrary entries outside the diagonal. Their diagonal entries are always zero. There are $k^2 - k$ positions outside the diagonal. Hence these commutators form a vector space of dimension $k^2 - k$. At the same point ψ has rank k . Indeed, it sends the diagonal matrix units to the polynomials $\prod_{j \neq i}(y + \theta_j)$, which are linearly independent modulo $\prod_j(y + \theta_j)$. Hence the sheaf $\mathcal{I}$ of commutators and $\ker \psi$ have the same generic rank, and $\ker \psi / \mathcal{I}$ is a torsion sheaf. As a quotient of $\mathcal{O}(-1)^{k^2}$, the sheaf $\mathcal{I}$ satisfies $H^1(\mathcal{I}) = 0$. Hence $H^1(\ker \psi) = 0$ as well. Therefore the constant matrices map onto $H^0(\mathbb{P}^1, \text{im } \psi) = H^0(C, \mathcal{J}(k-1))$.

Now let P be a form of degree $k-1$ that vanishes on Z . Then P is a section of $\mathcal{J}(k-1)$, so it agrees on C with a constant combination of adjugate entries. Their difference is a form of degree $k-1$ that is divisible by F_X , which has degree k . Hence the difference is zero. $\square$

The next lemma is where the condition $X \in \Gamma_D$ enters. It shows that Z is large.

Lemma B.2. *If $X \in \Gamma_D$, then $\text{length } Z \geq T$.*

Proof. The derivative of a determinant with respect to an entry is a cofactor. Hence $\partial F_X / \partial X_{ij} = u(\text{adj } M)_{ji}$ over any ring. Consider the linear functional $\lambda(P) = [s^q t^q u^c]P$ on forms of degree $k-1$. The equations of Γ_D say that λ kills every adjugate entry. By Lemma B.1, λ therefore kills every form of degree $k-1$ that vanishes on Z .

Now let $P = \sum a_{ij\ell} s^i t^j u^\ell$ be a form of degree q that vanishes on Z , and fix an exponent (i, j, ℓ) . The form $s^{q-i} t^{q-j} u^{c-\ell} P$ has degree $2q + c = k-1$, and it vanishes on Z . Note that its exponents are nonnegative, since $c \geq q$. Its value under λ is $a_{ij\ell}$, which must therefore be zero. Hence $P = 0$. In other words, the forms of degree q restrict injectively to Z . They form a space of dimension T , so $T \leq \text{length } Z$. Note that this argument never divides by an integer. $\square$

The scheme Z lies over the singular points of C . The next lemma bounds its length by the normalisation defect.

Lemma B.3. $\text{length } Z \leq \delta(C)$.

Proof. Both sides are sums of contributions over the points of $\mathbb{P}^1$, so I may work over one point. Let S be the local ring of $\mathbb{P}^1$ at that point. It is a discrete valuation ring with residue field K . Over S the curve is $\text{Spec } B$, where $B = S[y]/(f)$ and $f = \det(yI + A_0)$ for some $A_0 \in \text{Mat}_k(S)$. Further, $\mathcal{O}_C/\mathcal{J}$ becomes B/J , where J is the ideal generated by the entries of $\text{adj}(yI + A_0)$. Let R be the normalisation of B . It is finite over S , since f has distinct roots over the fraction field of S . The conductor $\mathfrak{c} = \{x \in B : xR \subseteq B\}$ is the largest ideal of R that lies in B . It suffices to show that $\mathfrak{c} \subseteq J$ and that $\text{length}_S(B/\mathfrak{c}) = \text{length}_S(R/B)$.

I begin with the inclusion. Let $\mathcal{L}$ be the cokernel of $yI + A_0$ on B^k . Since f has distinct roots over the fraction field of S , $\mathcal{L}$ is a torsion free B -module of rank one. A B -linear map $\mathcal{L} \rightarrow B$ is a row b with $b(yI + A_0) \equiv 0$ modulo f . Lifting b to $S[y]$ and multiplying by the adjugate shows that b is a combination of the rows of $\text{adj}(yI + A_0)$. Hence J is the image of the evaluation map $\text{Hom}_B(\mathcal{L}, B) \otimes \mathcal{L} \rightarrow B$. Since K is infinite, some $\ell_0 \in \mathcal{L}$ generates $R\mathcal{L}$ at every maximal ideal of R . Then $\mathcal{L}' = \ell_0^{-1}\mathcal{L}$ satisfies $B \subseteq \mathcal{L}' \subseteq R$. For $x \in \mathfrak{c}$, multiplication by x maps $\mathcal{L}' \cong \mathcal{L}$ into B and sends 1 to x . Hence $x \in J$.

For the lengths, let $\lambda_0 : B \rightarrow S$ read off the coefficient of y^{k-1} in the remainder modulo f . In the basis $1, y, \dots, y^{k-1}$, the pairing $(x, x') \mapsto \lambda_0(xx')$ has a Gram matrix that is zero above the antidiagonal and equal to one on it. Hence the pairing identifies B with its dual over S . Under this identification, $\text{Hom}_B(R, B)$ becomes the dual of R . Further, evaluation at 1 identifies $\text{Hom}_B(R, B)$ with $\mathfrak{c}$. Comparing the elementary divisors of $B \subseteq R$ now gives $\text{length}(B/\mathfrak{c}) = \text{length}(R/B)$. $\square$

The next lemma counts the curves with a large defect. It is the only place where I use an outside result.

Lemma B.4. *In $\mathbb{P}H^0(\mathbb{P}^2, \mathcal{O}(k))$, the reduced curves C with $\delta(C) \geq T$ form a constructible set of dimension at most $k(k+3)/2 - T$.*

Proof. In every characteristic, the integral plane curves of degree b whose normalisation has genus g form a locally closed set. When this set is nonempty, its dimension is $3b + g - 1$ [2]. Now consider a reduced curve of degree k with components of degrees b_i and normalisation genera g_i , for $1 \leq i \leq \alpha$. Comparing the Euler characteristics of $\mathcal{O}_C$ and $\nu_*\mathcal{O}_{\tilde{C}}$ gives $\delta(C) = \frac{(k-1)(k-2)}{2} - \sum_i g_i + \alpha - 1$. By multiplying equations, the reduced curves of a given type form a set of dimension at most $\sum_i (3b_i + g_i - 1) = 3k + \sum_i g_i - \alpha$. This number equals $k(k+3)/2 - \delta(C)$. Since there are finitely many types, the lemma follows. $\square$

Finally, I show that few matrices share the same curve.

Lemma B.5. *For a fixed curve C , the matrices X with $C_X = C$ form a set of dimension at most $N_0 = k(k-1)/2$.*

Proof. Let $r_X = (1, \dots, 1) \text{ adj } M$, a row of k forms of degree $k-1$, and let $Z'_X \subset C$ be the subscheme where its entries vanish. I first show that Z'_X has length N_0 and that it determines X . The row defines a map $\rho_X : \mathcal{O}_{\mathbb{P}^1}^k \rightarrow \mathcal{E}$. At $[1 : 0]$ this map sends the i th basis vector to $\prod_{j \neq i} (y + \theta_j)$. This is an isomorphism, and it does not depend on X . Hence ρ_X is injective, and its cokernel has length $\chi(\mathcal{E}) - k = N_0$. As in the proof of Lemma B.1, $sr_X = -r_X(tD + uX)$ on C . Therefore the image of ρ_X is π_* of the twisted ideal of Z'_X , and $\text{length } Z'_X = N_0$. Now suppose that $Z'_X = Z'_{X'}$. Then ρ_X and $\rho_{X'}$ have the same image, so they differ by a constant automorphism of $\mathcal{O}^k$. This automorphism is the identity, because the two maps agree at $[1 : 0]$. Hence $r_X = r_{X'}$. Subtracting the relations $sr = -r(tD + uX)$ for X and for X' gives $ur_X(X - X') = 0$. Since ρ_X is injective, $X = X'$.

It remains to show that $\dim \text{Hilb}_{N_0}(C) \leq N_0$, where $\text{Hilb}_{N_0}(C)$ is the space of subschemes of C of length N_0 . Consider a subscheme of $\mathbb{A}^2$ of length ℓ supported at one point, together with a basis of its coordinate ring. These data determine two commuting nilpotent $\ell \times \ell$ matrices, namely multiplication by the two coordinates, and a cyclic vector, namely the image of 1. Conversely, the matrices and the vector determine the subscheme and the basis. Now let A be nilpotent with a centraliser of dimension j . Its conjugacy class has dimension $\ell^2 - j$. The nilpotent matrices that commute with A satisfy $\det = 0$, which is a nontrivial equation on the centraliser. Hence these triples form a set of dimension at most $\ell^2 - 1 + \ell$. The basis accounts for ℓ^2 of these dimensions, so the subschemes form a family of dimension at most $\ell - 1$. Adding one parameter for each support point on C gives $\dim \text{Hilb}_{N_0}(C) \leq N_0$. Finally, the pairs (X, Z') with $r_X|_{Z'} = 0$ form a closed set. This set maps onto $\{X : C_X = C\}$. It has at most one point over each Z' , since $Z' \subseteq Z'_X$ and both have length N_0 . $\square$

Proof of Theorem 3.2. By Lemmas B.2 and B.3, the map $X \mapsto C_X$ sends Γ_D into the set of reduced curves with $\delta \geq T$. By Lemma B.4, this set has dimension at most $k(k+3)/2 - T$.

By Lemma B.5, the fibres of the map have dimension at most $k(k-1)/2$. Hence $\dim \Gamma_D \leq k(k+3)/2 - T + k(k-1)/2 = k^2 + k - T$. $\square$

Note that none of these steps depends on the characteristic. The k distinct points of a general fibre of π come from the fixed fibre at $u = 0$. The pairing in Lemma B.3 uses a coefficient and not a trace. Lemma B.5 uses a fixed basis at $[1 : 0]$ and Jordan forms.

Proof of Corollary 3.3. Put $v = k^2$ and $\Delta = T - k = N$. The singular set of $V(G_D) \subset \mathbb{P}^{v-1}$ lies in the projectivisation of Γ_D . By Theorem 3.2, it has dimension at most $v - 1 - \Delta$. In the Grassmannian of N dimensional subspaces, the subspaces through a singular point form a set of dimension at most $N(v - N) + N - 1 - \Delta = N(v - N) - 1$. At a smooth point $[x]$, Euler's identity gives $x \in \ker dG_D(x)$ in every characteristic. Over all smooth points, the subspaces H with $x \in H \subseteq \ker dG_D(x)$ form a set of dimension at most $N(v - N) - 1$. Hence a general subspace meets $V(G_D)$ only at smooth points and is tangent nowhere. Therefore $V(F)$ is smooth. Further, $F \neq 0$, since otherwise the subspace would be tangent everywhere.

For (2), note that $3q \leq k - 1$ and $q + 1 \geq k/3$. Hence $T \geq (q + 1)^2/2 \geq k^2/18$, and $N - 1 \geq k^2/18 - k - 1 \geq k^2/21$, where the last step uses $k \geq 127$. Further, $d = k - 2q \geq (k + 2)/3$, which gives the other two inequalities. $\square$

C Construction of the selectors

In this appendix, I build the equality gadget and the selector of Section 4, and I prove Proposition 4.1.

C.1 An equality gadget

Take two marked entries of weights w and 1 in distinct rows and distinct columns. Delete them, and add three new rows and three new columns carrying

$$J = \begin{pmatrix} -1 & -1 & 1 \\ -1 & -1 & 1 \\ -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

I connect the row of the first marked entry to new column 1, and give this connection weight w . Similarly, connect the row of the second marked entry to new column 2, with weight 1.

Further, also connect the new row 1 to the column of the first marked entry, with weight -2 .

Finally, connect new row 2 to the column of the second marked entry, with weight 1.

I now check three properties of the matrix J . First, its permanent is 1:

$$\text{per } J = 1.$$

Second, consider deleting one of the first two rows and one of the first two columns. There are four ways to do this.

In each case, note that the remaining 2×2 matrix has permanent 0. Third, deleting both of the first two rows and columns leaves a single entry:

$$J_{33} = -\frac{1}{2}.$$

Now, fix a matching outside the gadget. A matching is a choice of entries with no two in the same row or column. Each matching contributes the product of its chosen entries to the permanent.

There are four possibilities for the two marked entries. If neither is chosen, the gadget contributes 1. If both are chosen, it contributes

$$w \cdot (-2) \cdot \left(-\frac{1}{2}\right) = w.$$

If exactly one is chosen, the contribution is 0.

Hence the gadget allows only two possibilities: either both marked entries are chosen, or neither is chosen.

In other words, their selection bits must agree (here, a selection bit is 1 if the entry is chosen and 0 otherwise).

The gadget also gives the required weight w when both entries are chosen. It introduces no extra factor.

These calculations depend only on the entries involved. I can therefore use several gadgets even when they share rows or columns outside the gadgets.

C.2 The full adder and the circuit

A full adder adds three bits a, b, c . It produces two bits s, u satisfying

$$a + b + c = s + 2u.$$

Here, each bit is either 0 or 1, and the addition is ordinary integer addition. The bit s records whether the sum is odd or even. The bit u records whether the sum is at least 2. My full adder is a permanent of order eleven, built from

$$C = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

For a set I of the first three columns and a set O of the first three rows, delete them from C . Suppose that O is one of $\emptyset, \{1\}, \{2, 3\}, \{1, 2, 3\}$, and that $|I| = |O|$. Then the permanent of what remains is 1. Read the deleted columns as the input bits a, b, c , and the deleted rows as the output bits (s, u, u) . Then these eight cases are exactly the solutions of $a + b + c = s + 2u$. Table 1 lists them.

Rows deleted	Columns deleted	$a + b + c$	(s, u)	Term in (7)
$\emptyset$	$\emptyset$	0	$(0, 0)$	1
$\{1\}$	one column	1	$(1, 0)$	sa, sb, sc
$\{2, 3\}$	two columns	2	$(0, 1)$	uab, uac, ubc
$\{1, 2, 3\}$	all three	3	$(1, 1)$	$suabc$

Table 1: The eight cases of the full adder.

To turn C into a full adder, I put a copy of C and a copy of C^T side by side. For $j = 1, 2, 3$, I join row j of the second copy to column j of the first by an input edge, and row j of the first copy to column j of the second by an output edge. The completions inside the two copies then contribute the square of a permanent of the kind above. I give the input edges the weights a, b, c

and output edge 1 the weight s . Finally, I couple output edges 2 and 3 by an equality gadget, with u on the first of them. In blocks of sizes 4, 4 and 3, the result is

$$\mathcal{A} = \begin{pmatrix} C & sE_{11} & U(u) \\ \Delta(a, b, c) & C^T & 0 \\ 0 & V & J \end{pmatrix}, \quad (6)$$

$$U(u) = \begin{pmatrix} 0 & 0 & 0 \\ u & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

where $\Delta(a, b, c) = \text{diag}(a, b, c, 0)$ and E_{11} is a 4×4 matrix unit. The gadget keeps only the four output sets listed above, and the row and column counts force $|I| = |O|$. Hence

$$\text{per } \mathcal{A} = 1 + s(a + b + c) + u(ab + bc + ca) + suabc. \quad (7)$$

Note that the five variables lie in five different rows and five different columns.

Next I describe the circuit. I put the L input bits in the column of weight 1, and I treat the columns from the lowest weight up. While a column holds at least three live bits, I feed three of them to a full adder. Its sum bit stays in the column, and its carry moves to the next column. Each adder removes one live bit, and every column ends with one or two bits. What remains are two binary numbers of some length H . A ripple carry adder of H further full adders turns them into the $H + 1$ binary digits of $y_1 + \dots + y_L$. If the first phase leaves $B \geq H$ bits, it has used $L - B$ adders. Hence there are at most L adders in all. Note that the circuit is acyclic, and that every intermediate bit is used exactly once.

Proof of Proposition 4.1. I replace each adder by a copy of $\mathcal{A}$, and I couple the two ends of every internal wire by an equality gadget. I delete the marked entries that carry a constant input 0 or an output digit 0 of q . I delete the row and column of each output digit 1 of q , which forces that entry to be used. Finally, I put z_i on the input entry of the bit y_i . By (7) and the gadget, an assignment of all selection bits has weight one if it is consistent at every adder and every wire, and weight zero otherwise. An input vector $y \in \{0, 1\}^L$ has exactly one consistent extension. This extension matches the fixed outputs exactly when y has q ones, and it then contributes $\prod_i z_i^{y_i}$. With at most L adders and $2L$ wires, the order is at most $11L + 6L$. $\square$

Table 2 lists the eight minors of C that the full adder uses, with their permanents.

References

- [1] J.-Y. Cai, X. Chen and D. Li. Quadratic lower bound for permanent vs. determinant in any characteristic. *Computational Complexity* 19 (2010), 37–56.
- [2] K. Christ, X. He and I. Tyomkin. On the Severi problem in arbitrary characteristic. *Publications Mathématiques de l’IHÉS* 137 (2023), 1–45.
- [3] T. Mignon and N. Ressayre. A quadratic bound for the determinant and permanent problem. *International Mathematics Research Notices* 2004, no. 79, 4241–4253.

Rows deleted	Columns deleted	Remaining matrix	Permanent
$\emptyset$	$\emptyset$	$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$	1
$\{1\}$	$\{1\}$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$	1
$\{1\}$	$\{2\}$	$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	1
$\{1\}$	$\{3\}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$	1
$\{2, 3\}$	$\{1, 2\}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	1
$\{2, 3\}$	$\{1, 3\}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	1
$\{2, 3\}$	$\{2, 3\}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	1
$\{1, 2, 3\}$	$\{1, 2, 3\}$	(1)	1

Table 2: The minors of C used by the full adder.

- [4] OpenAI. A cubic lower bound for border determinantal complexity of the permanent. Preprint, 24 September 2026. <https://github.com/openai/math/blob/fd4aeeb2ee4fc729c18d98444fed42fd0529eeeb/preprints/A-cubic-lower-bound-for-border-determinantal-complexity-of-the-permanent-September-24-2026/A-cubic-lower-bound-for-border-determinantal-complexity-of-the-permanent-September-24-2026.pdf>
- [5] K. Sheshadri. Conormal lower bounds for determinantal complexity: Fermat slices, tight bounds, and a ceiling. arXiv:2606.15970v2, 2026.
- [6] L. G. Valiant. Completeness classes in algebra. *Proceedings of the 11th ACM Symposium on Theory of Computing* (1979), 249–261.