Galois groups and real critical points of constrained permanents

Mantis Discovery

Abstract

We study the critical points of the three-by-three permanent under prescribed row and column sums. Their critical algebra is free of rank sixteen over the polynomial ring in the marginal parameters, and both its arithmetic and geometric Galois groups are S_{16}. The proof combines a Fourier normal form, a rational specialization, and a simple branch point at a positive matrix. Over the reals, the gradient has topological degree four. An explicit family with positive marginals develops an interior local minimum and a saddle at a fold; below the transition, every minimum on the transportation polytope lies on its boundary. Rational-univariate representations isolate all real and positive critical matrices, including at nonreduced fibers. For m constrained three-by-three matrices with quadratic interactions, the same argument gives critical length 16^m and between 4^m and 16^m real points in every nondegenerate fiber, with both bounds attained.

1 Introduction

For compatible vectors $r, s \in \mathbb{C}^3$, put

$$\mathcal{A}(r,s) = \{A \in \mathbb{C}^{3\times 3} : A\mathbf{1} = r,\ A^{\mathsf{T}}\mathbf{1} = s\}, \qquad \mathbf{1}^{\mathsf{T}} r = \mathbf{1}^{\mathsf{T}} s.$$

The space $\mathcal{A}(r,s)$ has dimension four. We study the critical points of the permanent restricted to this affine space, as the five independent marginal parameters vary. These are affine stationary points. They need not be nonnegative, and they do not include every boundary optimum of the transportation polytope $\mathcal{A}(r,s) \cap \mathbb{R}^{3\times 3}_{\geq 0}$.

Let $\mathcal{M}$ be the affine space of compatible marginal pairs and let $\mathcal{Z}$ be the critical scheme over $\mathcal{M}$. Its fiber is defined by the four first derivatives in any affine coordinates on $\mathcal{A}(r,s)$. The length of a fiber is the dimension of its coordinate algebra over $\mathbb{C}$, so it counts critical points with algebraic multiplicity.

Theorem 1.1. *The projection $\mathcal{Z} \to \mathcal{M}$ is finite and flat of degree sixteen. Every fiber has length sixteen, and the general fiber consists of sixteen distinct points. The arithmetic Galois group over the rational marginal function field and the geometric Galois group over $\mathbb{C}(\mathcal{M})$ are both S_{16}.*

The geometric group records the permutations obtained by continuing the sixteen critical matrices along loops outside the discriminant. Since it is S_{16}, the general critical matrix is not expressible by radicals in the marginals, even after adjoining complex constants. Exact computation remains possible through the fixed sixteen-dimensional algebra and a rational-univariate representation.

The degree statement and the Galois statement have different proofs. A Fourier transformation gives four monic quadratic equations with relatively prime leading monomials. This proves the uniform degree, including at degenerate marginal choices. For the arithmetic group we exhibit a rational fiber whose coordinate polynomial has three specified factorization types modulo primes.

To pass from arithmetic to geometric monodromy, we construct a simple fold at a positive real matrix and verify that no other critical point collides in the same fiber.

Every nondegenerate real fiber has signed Morse count four. At equal positive marginals all sixteen critical matrices are real, but only one is strictly positive. In a second one-parameter family, several critical matrices are positive before any interior local minimum exists. The convexity theorem of Ahmadi and Zhang for local minima of cubic polynomials [1] turns the transition point into a classification of local minima in this family.

The same highest-degree calculation extends to higher-dimensional models. If m constrained three-by-three permanents are coupled by any polynomial of degree at most two in their free entries, the critical algebra has length 16^m for every parameter choice. Its real gradient has degree 4^m. Both bounds are attained; see Section 6.

1.1 Relation to previous work

Permanent minimization on nonnegative matrices has a substantial literature, surveyed by Cheon and Wanless [3]. Gibson [6] studies subpolytopes on which the permanent is constant, including a classification of certain subpolytopes in order three. Moyls, Marcus and Minc [9] study linear permanent preservers on the doubly stochastic affine space. Our object instead includes every affine stationary point and varies both marginal vectors.

Nie and Ranestad [10] develop the algebraic degree of polynomial optimization under genericity assumptions. Four quadratic equations have the expected Bézout bound sixteen. The issue here is that their coefficients are linked by the permanent and by only five marginal parameters. The monic presentation below proves that no specialization of those parameters changes the scheme length.

Esterov [5] proves full symmetric monodromy for reduced irreducible systems with general coefficients. The coefficient relations in this marginal family prevent a direct application of a theorem for independent coefficients. Our S_{16} proof uses a specialization and a simple branch point within the actual five-parameter family. The field-theoretic tools are standard [12]; the explicit certificates are given in Section 3 and Section A.

Rational-univariate representations and trace-form methods are established tools for zero-dimensional systems [11, 2]. We use them for a uniform, fixed-size certificate rather than propose a new general solver. Similarly, the uniqueness consequences for local minima use [1]; the new calculation is the location and form of the transition for the permanent.

2 A critical algebra of constant length

Let ω be a primitive cube root of unity and set

$$e = (1,1,1)^{\mathsf{T}}, \quad u = (1,\omega,\omega^2)^{\mathsf{T}}, \quad v = (1,\omega^2,\omega)^{\mathsf{T}}.$$

There are unique parameters $h, \rho_1, \rho_2, \kappa_1, \kappa_2$ with

$$r = 3he + 3\rho_1 u + 3\rho_2 v, \qquad s = 3he + 3\kappa_1 u + 3\kappa_2 v. \tag{1}$$

In particular, $h = (\mathbf{1}^{\mathsf{T}} r)/9$. Every $A \in \mathcal{A}(r,s)$ has a unique expression

$$A = A_0 + auu^{\mathsf{T}} + buv^{\mathsf{T}} + cvu^{\mathsf{T}} + dvv^{\mathsf{T}}, \tag{2}$$

where

$$A_0 = hee^{\mathsf{T}} + \rho_1 ue^{\mathsf{T}} + \rho_2 ve^{\mathsf{T}} + \kappa_1 eu^{\mathsf{T}} + \kappa_2 ev^{\mathsf{T}}, \qquad (A_0)_{ij} = \frac{r_i + s_j}{3} - h.$$

The vectors e, u, v are a basis, and the last four outer products span the matrices with zero row and column sums.

Lemma 2.1. *For $W = [e\ u\ v]$ and $Z = (z_{ij})_{0\le i,j\le 2}$,*

$$\operatorname{per}(WZW^{\mathsf{T}}) = 6\sum_{i,j} z_{ij}^3 - 18\sum_i \prod_j z_{ij} - 18\sum_j \prod_i z_{ij} + 9\operatorname{per} Z. \tag{3}$$

Proof. Write $w_0 = e, w_1 = u, w_2 = v$. The permanent of a matrix with three columns chosen from these vectors vanishes unless their subscripts sum to zero modulo three: a cyclic row permutation multiplies that permanent by the corresponding power of ω. The surviving cases are

$$\operatorname{per}[w_i\ w_i\ w_i] = 6, \qquad \operatorname{per}[w_0\ w_1\ w_2] = -3.$$

Expand $WZW^{\mathsf{T}} = \sum_{i,j} z_{ij} w_i w_j^{\mathsf{T}}$ by multilinearity. The contribution of an ordered triple of outer products is the product of its two column permanents, divided by 3! when all ordered triples are summed. If both triples of subscripts are constant, the result is $6z_{ij}^3$. If exactly one is constant, the contribution is -18 times a row or column product of Z. If both triples have distinct subscripts, the contribution is $9\operatorname{per} Z$. These are all the surviving terms. □

Apply Lemma 2.1 to

$$Z = \begin{pmatrix} h & \kappa_1 & \kappa_2 \\ \rho_1 & a & b \\ \rho_2 & c & d \end{pmatrix}.$$

Up to a term depending only on the marginals, the restricted permanent is

$$\begin{aligned} \Phi_\theta = {} & 6(a^3+b^3+c^3+d^3) + 9h(ad+bc) \\ & - 18(\rho_1 ab + \kappa_1 ac + \kappa_2 bd + \rho_2 cd) \\ & + 9(\kappa_2\rho_2 a + \kappa_1\rho_2 b + \kappa_2\rho_1 c + \kappa_1\rho_1 d) + C(\theta), \end{aligned} \tag{4}$$

where

$$C(\theta) = 6(h^3 + \rho_1^3 + \rho_2^3 + \kappa_1^3 + \kappa_2^3) - 18h(\rho_1\rho_2 + \kappa_1\kappa_2).$$

Dividing its four derivatives by 18 gives

$$\begin{aligned} F_a &= a^2 - \rho_1 b - \kappa_1 c + \tfrac{h}{2} d + \tfrac{1}{2}\kappa_2\rho_2, \\ F_b &= b^2 - \rho_1 a + \tfrac{h}{2} c - \kappa_2 d + \tfrac{1}{2}\kappa_1\rho_2, \\ F_c &= c^2 - \kappa_1 a + \tfrac{h}{2} b - \rho_2 d + \tfrac{1}{2}\kappa_2\rho_1, \\ F_d &= d^2 + \tfrac{h}{2} a - \kappa_2 b - \rho_2 c + \tfrac{1}{2}\kappa_1\rho_1. \end{aligned} \tag{5}$$

Proposition 2.2. *Let $R = \mathbb{C}[h, \rho_1, \rho_2, \kappa_1, \kappa_2]$. The critical algebra*

$$\mathcal{B} = R[a,b,c,d]/(F_a, F_b, F_c, F_d)$$

is a free R-module with basis

$$E = \{a^{\varepsilon_1} b^{\varepsilon_2} c^{\varepsilon_3} d^{\varepsilon_4} : \varepsilon_i \in \{0,1\}\}. \tag{6}$$

Every marginal fiber has length sixteen. The homogenized equations have no common point at infinity.

Proof. Use any graded monomial order in a, b, c, d, treating the marginal parameters as coefficients. The four equations are monic with leading monomials a^2, b^2, c^2, d^2. These monomials are pairwise relatively prime, so Buchberger's product criterion gives a Gröbner basis. The criterion and division algorithm work over R because the leading coefficients are one; see [4]. The standard monomials are exactly (6), and monic division proves both spanning and uniqueness over R.

Specializing the marginals leaves the same leading monomials and the same monic division. Hence the basis persists at every fiber. On the hyperplane at infinity, the homogenized equations reduce to $a^2 = b^2 = c^2 = d^2 = 0$, which has no projective solution. Freeness implies finite flatness of degree sixteen. □

At zero marginals the entire fiber is supported at the zero matrix, with algebra

$$\mathbb{C}[a, b, c, d]/(a^2, b^2, c^2, d^2).$$

Thus a constant scheme length is not a constant number of distinct points.

2.1 The discriminant

For $g \in \mathcal{B}$, write m_g for multiplication by g in the basis E. Define

$$\Delta(\theta) = \det\big(\mathrm{Tr}(m_{ef})\big)_{e,f\in E}. \tag{7}$$

Proposition 2.3. *The polynomial Δ is nonzero and homogeneous of degree 64. A marginal fiber has sixteen distinct points if and only if $\Delta \neq 0$. On the equal-marginal line,*

$$\Delta(h, 0, 0, 0, 0) = \frac{3^{24}}{2^{64}} h^{64}. \tag{8}$$

Proof. The standard trace-pairing criterion for finite-dimensional commutative $\mathbb{C}$-algebras says that the trace pairing is nondegenerate exactly when the algebra is reduced; see [2]. This proves the assertion about fibers.

Assign degree one to a, b, c, d and to all five marginal parameters. The relations (5) are homogeneous of degree two. If basis monomials e, f have degrees p, q, then $\mathrm{Tr}(m_{ef})$ is homogeneous of degree $p + q$. Indeed, reducing efg back to its coefficient on a basis vector g leaves a parameter coefficient of that degree. Every term of (7) therefore has degree

$$2\sum_{e\in E} \deg e = 2\sum_{j=0}^{4} j\binom{4}{j} = 64.$$

For (8), put $u_0 = h/2$. The algebra specializes to the tensor product of two copies of

$$D = \mathbb{C}[x, y]/(x^2 + u_0 y,\ y^2 + u_0 x).$$

Its trace matrix in the basis $(1, x, y, xy)$ is

$$\begin{pmatrix} 4 & 0 & 0 & 3u_0^2 \\ 0 & 0 & 3u_0^2 & 0 \\ 0 & 3u_0^2 & 0 & 0 \\ 3u_0^2 & 0 & 0 & 3u_0^4 \end{pmatrix},$$

with determinant $-27u_0^8$. The trace matrix of the tensor product is the Kronecker product of the two trace matrices. Its determinant is $(-27u_0^8)^8$, proving (8) and nonvanishing. □

The degree 64 refers to this trace discriminant. No assertion that it is squarefree or irreducible is needed. Its zero set is the branch locus relevant to the critical-point cover.

3 The full symmetric Galois group

We first compute an arithmetic specialization. We then exhibit a geometric transposition. Both steps are necessary: a full arithmetic group alone would not determine the geometric group.

Lemma 3.1. *For $r = (2, 3, 7)$ and $s = (1, 5, 6)$, the sixteen critical points are distinct. Their splitting field over $\mathbb{Q}$ has Galois group S_{16}.*

Proof. Use the first two entries of the first two rows as coordinates:

$$A = \begin{pmatrix} x_1 & x_2 & r_1 - x_1 - x_2 \\ x_3 & x_4 & r_2 - x_3 - x_4 \\ s_1 - x_1 - x_3 & s_2 - x_2 - x_4 & r_3 - s_1 - s_2 + x_1 + x_2 + x_3 + x_4 \end{pmatrix}. \tag{9}$$

In the critical algebra, multiplication by x_4 has characteristic polynomial $P(T)/408146688$, where the integer polynomial P is displayed in Section A. This is an exact determinant identity in a sixteen-dimensional algebra: form the four derivatives of (9), reduce products in the quotient, and take the characteristic polynomial of multiplication by x_4. The verifier repeats these rational operations directly from the derivatives.

The reductions of P at three primes are squarefree and have irreducible factor degrees

Prime	Factor degrees
29	16
73	2, 7, 7
97	1, 15

The factors and finite-field irreducibility checks are in Section A. Irreducibility modulo 29 implies that P is irreducible over $\mathbb{Q}$. Squarefreeness implies that its sixteen roots are distinct. As the critical algebra has dimension sixteen, x_4 separates the critical points and generates their algebra.

By the factorization–cycle correspondence for good primes [12], the Galois group is transitive, contains a permutation of type $(1, 15)$, and contains one of type $(2, 7, 7)$. The 15-cycle fixing a point makes that point stabilizer transitive on the other fifteen points. Together with transitivity, this gives double transitivity. The seventh power of the $(2, 7, 7)$ permutation is a transposition. A doubly transitive group containing one transposition contains every transposition by conjugation, and is therefore S_{16}. □

Lemma 3.2. *At*

$$(h, \rho_1, \rho_2, \kappa_1, \kappa_2) = (10, 1, 1, 2, 2)$$

the critical scheme has one point of length two and fourteen reduced points. The length-two point has Fourier coordinates $a = b = c = d = -1$, corresponding to

$$A_* = \begin{pmatrix} 12 & 12 & 12 \\ 15 & 6 & 6 \\ 15 & 6 & 6 \end{pmatrix}, \qquad r = (36, 27, 27), \quad s = (42, 24, 24). \tag{10}$$

Varying h transversely through this parameter gives a simple fold. A small complex loop around the fold exchanges exactly two critical points.

Proof. At these parameters, (5) becomes

$$a^2 - b - 2c + 5d + 1 = 0, \quad b^2 - a + 5c - 2d + 1 = 0,$$

$$c^2 - 2a + 5b - d + 1 = 0, \quad d^2 + 5a - 2b - c + 1 = 0.$$

Substitution verifies the point. The Jacobian at $(-1,-1,-1,-1)$ is

$$J_* = \begin{pmatrix} -2 & -1 & -2 & 5 \\ -1 & -2 & 5 & -2 \\ -2 & 5 & -2 & -1 \\ 5 & -2 & -1 & -2 \end{pmatrix}. \tag{11}$$

Its eigenvalues are $0, 6, -6, -8$, and its kernel is spanned by $e_4 = (1,1,1,1)^{\mathsf{T}}$. If $F = (F_a, F_b, F_c, F_d)^{\mathsf{T}}$, then

$$e_4^{\mathsf{T}} D^2 F[e_4, e_4] = 8 \neq 0, \qquad e_4^{\mathsf{T}} \partial_h F = -2 \neq 0. \tag{12}$$

The first nonzero quantity is the quadratic term along the kernel; the second shows transversality in the parameter h.

The nondegeneracy and transversality conditions in (12) are the standard criterion for a fold singularity; see [7]. Thus the germ is analytically equivalent, up to nonvanishing factors and changes of local coordinates, to $z^2 - \tau = 0$, with τ a local parameter. The local algebra has length two, and a loop around $\tau = 0$ interchanges its two branches.

We must also exclude a simultaneous collision elsewhere. Reduction using the four displayed quadratic relations gives

$$\begin{aligned} \det(TI - m_a) = (T+1)^2 (T^2 - 6T + 25)(T^2 - 4T + 13) \\ \cdot (T^2 + 8T + 25) Q_8(T), \end{aligned} \tag{13}$$

where

$$\begin{aligned} Q_8(T) = T^8 + 4T^6 + 384T^5 - 582T^4 - 272T^3 \\ + 34652T^2 - 84432T + 128853. \end{aligned}$$

The quotient of (13) by $(T+1)^2$ is squarefree and takes the value 2563467264 at $T = -1$. These polynomial identities are checked in the supplied certificate. In the decomposition into local algebras, the multiplicity of an eigenvalue of m_a is the sum of the lengths of the local factors with that a-coordinate. The fourteen remaining simple eigenvalues therefore come from distinct reduced critical points, while the double eigenvalue is accounted for by the local algebra at A_*. These fourteen points continue as separate analytic branches and are fixed by a small loop around the fold. □

Proof of Theorem 1.1. Propositions 2.2 and 2.3 give the finite flat cover and a nonempty open set of sixteen distinct points. Take its arithmetic group over $\mathbb{Q}(r_1, r_2, r_3, s_1, s_2)$, with $s_3 = \sum r_i - s_1 - s_2$. The characteristic polynomial of the generic coordinate x_4 has coefficients in this rational function field. The specialization of Lemma 3.1 is separable of degree sixteen, so x_4 generates the generic algebra as well. The specialization theorem for Galois groups at a separable fiber places its specialized S_{16} inside the generic arithmetic group [12]. Hence the arithmetic group is S_{16}.

The geometric group is a normal subgroup of the arithmetic group: it is the kernel of the action on the algebraic constant field in the splitting field. By Lemma 3.2 it contains a transposition. The normal closure of a transposition in S_{16} is S_{16} itself. Thus the geometric group is also S_{16}. □

4 Real critical points and an interior transition

For real marginals, h is real, $\rho_2 = \overline{\rho_1}$ and $\kappa_2 = \overline{\kappa_1}$. The matrix in (2) is real exactly when $d = \bar{a}$ and $c = \bar{b}$. Write

$$a = x + iy, \qquad b = z + it$$

as real affine coordinates.

Theorem 4.1. *At every real marginal pair with $\Delta \neq 0$, let N_j be the number of real critical points of Morse index j. Then*

$$\sum_{j=0}^{4} (-1)^j N_j = 4. \tag{14}$$

The number of real critical points is even and lies between four and sixteen. Every real marginal pair, including those on the discriminant, has at least one real critical point.

Proof. The highest-degree part of the real restricted permanent is $12(x^3 - 3xy^2 + z^3 - 3zt^2)$. Its gradient is

$$Q(x, y, z, t) = 36(x^2 - y^2, -2xy, z^2 - t^2, -2zt).$$

It satisfies

$$\|Q(x, y, z, t)\|^2 = 36^2((x^2 + y^2)^2 + (z^2 + t^2)^2) \geq \frac{36^2}{2}\|(x, y, z, t)\|^4.$$

The full gradient differs from Q by an affine map. The straight homotopy between them is uniformly proper, since the quadratic lower bound dominates all affine terms outside a fixed ball.

Each two-dimensional factor of Q is a positive multiple of $z \mapsto \bar{z}^2$, a proper map of topological degree -2. The product has degree four. Homotopy invariance gives degree four for the full gradient; we use the standard degree properties in [8]. If $\Delta \neq 0$, all zeros are nondegenerate and their local degrees are the signs of the Hessian determinants, namely $(-1)^j$. This proves (14). The upper bound is the algebraic length sixteen; the signed sum gives the lower bound and parity. Without nondegeneracy, the nonzero degree still forces a zero. □

4.1 Equal positive marginals

Proposition 4.2. *For $r = s = (1, 1, 1)^{\mathsf{T}}$, all sixteen critical matrices are real and nondegenerate. They are:*

1. *$J/3$, of value $2/9$ and Morse index zero;*
2. *the six matrices $(J - P)/2$, where P is a permutation matrix, of value $1/4$ and Morse index one;*
3. *the nine matrices obtained by choosing (i, j), placing $-1/3$ there, $2/3$ in the other entries of its row and column, and $1/6$ in the remaining four entries, of value $5/18$ and Morse index two.*

Only $J/3$ is strictly positive. All sixteen points remain real and nondegenerate under sufficiently small real marginal perturbations.

Proof. Here $h = 1/3$ and the other Fourier parameters vanish. The equations split into

$$a^2 + d/6 = d^2 + a/6 = 0, \qquad b^2 + c/6 = c^2 + b/6 = 0.$$

Each pair has the zero solution and the three solutions $(-\omega^j/6, -\omega^{2j}/6)$, $j = 0, 1, 2$. They satisfy the required conjugacy conditions. Substitution into (2) gives the three matrix types: respectively neither, one, or both pairs nonzero.

On the real locus the permanent is

$$\frac{2}{9} + 12\Re(a^3 + b^3) + 3(|a|^2 + |b|^2).$$

For one variable $a = x + iy$, the Hessian of $12\Re(a^3) + 3|a|^2$ is

$$\begin{pmatrix} 6 + 72x & -72y \\ -72y & 6 - 72x \end{pmatrix}.$$

At zero it has eigenvalues $6, 6$; at each nonzero critical point it has eigenvalues $18, -6$. The two summands use disjoint variables, proving the stated indices and nondegeneracy. Each nonzero pair adds $1/36$ to the critical value. Finally, the real implicit function theorem continues all sixteen simple points. The constant fiber length leaves no room for additional points. □

The affine Morse indices do not assert boundary optimality of the six matrices with zero entries.

4.2 Local minima

Ahmadi and Zhang prove that the local minima of a cubic polynomial form a convex set [1, Theorem 4.3]. They also show that a null direction of the Hessian at a local minimum gives a line of critical points [1, Lemma 4.2]. Since our critical sets are finite, these facts imply that there is at most one real local minimum and, when it exists, its Hessian is positive definite. This is an application of their cubic optimization theory.

There is a further simple restriction in the permanent family. In the real coordinates above, the quadratic terms have Hessian trace $72h$; the cubic and mixed quadratic terms have zero trace. Thus if $h > 0$ there is no real local maximum. If $h < 0$ there is no real local minimum. At $h = 0$, the finiteness of the critical set and the same Hessian facts exclude both.

We now locate the local-minimum transition in a family with all marginals positive. For $h > 2$, let

$$r(h) = (3h + 6, 3h - 3, 3h - 3), \qquad s(h) = (3h + 12, 3h - 6, 3h - 6). \tag{15}$$

These correspond to $\rho_1 = \rho_2 = 1$ and $\kappa_1 = \kappa_2 = 2$.

Theorem 4.3. *For the real affine permanent with marginals* (15)*, a local minimum exists if and only if $h > 10$. It is unique and strictly positive. For $h > 10$, put*

$$D = (h - 10)(h - 2), \qquad t_\pm = \frac{6 - h \pm \sqrt{D}}{4},$$

and define

$$A(h, t) = \begin{pmatrix} h + 6 + 4t & h - 2t & h - 2t \\ h + 3 - 2t & h - 3 + t & h - 3 + t \\ h + 3 - 2t & h - 3 + t & h - 3 + t \end{pmatrix}. \tag{16}$$

The local minimum is $A(h, t_+)$. If $10 < h < 6 + 4\sqrt{10}$, then $A(h, t_-)$ is also strictly positive and is a saddle of Morse index one. At $h = 10$ they meet at the fold (10)*. For $2 < h \le 10$, every global minimum on the transportation polytope lies on its boundary.*

Proof. The marginal vectors and objective are invariant under independently swapping the last two rows and the last two columns. If a local minimum exists, its uniqueness forces it to be fixed by these swaps. Such a matrix has the form (16), or equivalently $a = b = c = d = t \in \mathbb{R}$. The four critical equations then coincide:

$$t^2 + (h/2 - 3)t + 1 = 0. \tag{17}$$

For $2 < h < 10$ its discriminant is negative, so no local minimum exists. At $h = 10$ its only root is $t = -1$, but along the line (16) the derivative of the permanent is $72(t + 1)^2$. This point is not a local extremum.

For $h > 10$, the roots are $t_\pm$. In real Fourier coordinates, the Hessian at $a = b = t \in \mathbb{R}$ splits into the $(\Re a, \Re b)$ and $(\Im a, \Im b)$ blocks. Its eigenvalues are

$$18(h + 4t - 6), \quad 18(h + 4t + 6), \quad 18(h - 4t - 2), \quad 18(h - 4t + 2). \tag{18}$$

At t_+ the first two are $18\sqrt{D}$ and $18(12 + \sqrt{D})$. The smaller of the last two is $18(2h - 8 - \sqrt{D}) > 0$, since $\sqrt{D} < h - 2$ for $h > 10$. Thus $A(h, t_+)$ is a strict local minimum. Its entries are positive: its top-left entry is $12 + \sqrt{D}$, and the other entries in (16) are positive after the same inequality $\sqrt{D} < h - 2$ is used.

At t_-, the first eigenvalue is negative. The other three are positive exactly while $\sqrt{D} < 12$. The same inequality is precisely positivity of its top-left entry $12 - \sqrt{D}$; its remaining entries are positive for $h > 10$. Hence the stated interval is $10 < h < 6 + 4\sqrt{10}$ and the index is one there.

Finally, the positive marginals make the transportation polytope nonempty and compact, with a nonempty positive relative interior. Any minimum in that interior would be a real affine local minimum. None exists for $2 < h \leq 10$, so every global minimum is on the boundary. □

The theorem identifies an interior local minimum for $h > 10$; it does not assert that this point beats every boundary matrix in that range.

5 Exact certificates for real and positive points

The Galois group rules out general radical formulas, but the fixed algebra allows exact root isolation. We describe the certificate in rational coordinates and include nonreduced fibers.

Fix rational marginals and use the matrix-entry chart (9). Write B for the resulting sixteen-dimensional rational critical algebra. In any basis E_0, the rank of the trace matrix

$$\big(\mathrm{Tr}(m_{ef})\big)_{e,f \in E_0}$$

is the number r_0 of distinct complex points. This is the trace-pairing criterion from Proposition 2.3, applied to the local-algebra decomposition.

Proposition 5.1. *Let $x_1, \ldots, x_4$ be the rational coordinates in* (9)*. Among the* 361 *linear forms*

$$\ell_t = x_1 + tx_2 + t^2x_3 + t^3x_4, \qquad t = 0, 1, \ldots, 360,$$

at least one separates the distinct complex critical points. It can be recognized by

$$\deg \mathrm{sqfree} \det(TI - m_{\ell_t}) = r_0. \tag{19}$$

For a separating form, put

$$P = \det(TI - m_\ell), \quad D = \gcd(P, P'), \quad p = P/D, \quad q = P'/D,$$

and

$$Q_j(T) = \operatorname{Tr}\big(m_{x_j} \operatorname{adj}(TI - m_\ell)\big).$$

Then D divides every Q_j, q is invertible modulo p, and the distinct complex critical points are exactly

$$\big(R_1(\lambda), \dots, R_4(\lambda)\big), \qquad p(\lambda) = 0, \qquad R_j \equiv (Q_j/D)q^{-1} \pmod{p}. \tag{20}$$

This formula remains valid when the critical algebra is not reduced.

Proof. For two distinct points, equality of their values under ℓ_t is a nonzero polynomial condition of degree at most three in t. There are at most $\binom{16}{2} = 120$ pairs, so at most 360 values of t fail to separate some pair. This proves existence. The distinct eigenvalues of m_ℓ are the values of ℓ at the distinct points, which proves (19).

For the formula, extend scalars to $\mathbb{C}$ and decompose B into its local algebras. Write $\lambda_z = \ell(z)$ and μ_z for the length at a point z. Then

$$P(T) = \prod_z (T - \lambda_z)^{\mu_z}, \qquad \frac{Q_j(T)}{P(T)} = \sum_z \frac{\mu_z x_j(z)}{T - \lambda_z}.$$

To see the second identity, use $\operatorname{adj}(TI - m_\ell) = P(T)(TI - m_\ell)^{-1}$ over $\mathbb{C}(T)$. In a local algebra, multiplication by an element is its residue value times the identity plus a nilpotent operator. The nilpotent terms in this trace vanish, leaving $\mu_z x_j(z)/(T - \lambda_z)$.

Since the λ_z are distinct,

$$D = \prod_z (T - \lambda_z)^{\mu_z - 1}, \qquad P'/D = \sum_z \mu_z \prod_{y \neq z} (T - \lambda_y).$$

Thus D divides Q_j. Evaluating the second expression at λ_z gives

$$(P'/D)(\lambda_z) = \mu_z \prod_{y \neq z} (\lambda_z - \lambda_y) \neq 0,$$

and the ratio $(Q_j/D)/(P'/D)$ is $x_j(z)$. This proves invertibility of q modulo p and (20). All operations have rational coefficients, so the representation descends to $\mathbb{Q}$. □

This is the trace-based rational-univariate representation of [11], with a fixed separating search bound for the present four-coordinate algebra. Its advantage here is validity at every marginal specialization, rather than only on a generic locus where a predetermined coordinate separates the points.

To certify positivity, substitute the four polynomials R_j into the nine affine matrix entries and reduce modulo p. Isolate the real roots of the squarefree polynomial p by rational intervals. At each real root, evaluate the signs of those nine entry polynomials. A common-root test by a greatest common divisor detects an entry equal to zero; otherwise interval refinement certifies its sign. Standard univariate real-root methods guarantee termination [2]. All nine signs must be positive for a strictly positive matrix.

The program `critical_solver.py` implements these steps using rational arithmetic, including the nonreduced fibers in Table 1. It verifies the four critical equations in $\mathbb{Q}[T]/(p)$ and emits isolating intervals and all nine entry signs. No numerical continuation or tolerance-based root merging is used for the table.

r	s	Distinct complex	Real	Strictly positive
$(0,0,0)$	$(0,0,0)$	1	1	0
$(1,1,1)$	$(1,1,1)$	16	16	1
$(2,3,7)$	$(1,5,6)$	16	6	0
$(33,24,24)$	$(39,21,21)$	16	12	4
$(36,27,27)$	$(42,24,24)$	15	13	5
$(39,30,30)$	$(45,27,27)$	16	14	6

Table 1: Exact rational-univariate certificates. Every fiber has scheme length sixteen; the table counts distinct points. The last three rows are $h = 9, 10, 11$ in (15). The positive critical points at $h = 9$ are not local minima.

6 Quadratically coupled permanent models

The normal form also gives a family with an arbitrary number of variables. Fix compatible real marginals for m three-by-three matrices $A_1, \dots, A_m$. On the product of their affine spaces, consider

$$\Psi(A_1, \dots, A_m) = \sum_{i=1}^{m} \operatorname{per}(A_i) + Q(A_1, \dots, A_m), \tag{21}$$

where Q is any real polynomial of degree at most two in the free entries. It may couple different matrices and need not be convex. Linear penalties and quadratic interactions therefore change the lower-degree terms but not the highest-degree part of the critical system.

For the universal algebraic statement, regard the compatible marginal coordinates and the coefficients of a general quadratic polynomial Q as indeterminates, and let R_m be the resulting polynomial ring over $\mathbb{C}$.

Theorem 6.1. *For* (21)*, the complex critical algebra is free of rank* 16^m *over* R_m*. Every specialized critical scheme has length* 16^m*, with no point at infinity. The real gradient is proper of topological degree* 4^m*. Hence every nondegenerate real fiber satisfies*

$$\sum_{j=0}^{4m} (-1)^j N_j = 4^m, \tag{22}$$

and has between 4^m *and* 16^m *real critical points. Both endpoint counts occur in this family. At arbitrary real parameters there is at least one real critical point.*

Proof. Apply (2) separately to each matrix. Over $\mathbb{C}$, the highest-degree part is $6 \sum_{j=1}^{4m} z_j^3$. After division by 18, the gradient equations have the form

$$z_j^2 + L_j(z_1, \dots, z_{4m}) = 0 \qquad (1 \le j \le 4m),$$

where each L_j is affine in the variables. The coefficients may depend polynomially on all marginal and coupling parameters. Their leading monomials z_j^2 are relatively prime. The same monic Gröbner argument as in Proposition 2.2 gives the standard monomial basis of size $2^{4m} = 16^m$ over R_m. Homogenization gives only the equations $z_j^2 = 0$ at infinity.

On the real locus, pair the Fourier coordinates into $2m$ conjugate pairs. The highest-degree part becomes $12 \sum_{j=1}^{2m} \Re(\zeta_j^3)$. Its gradient is the product of $2m$ copies of $36\bar{\zeta}_j^2$, and

$$\|Q_2(\zeta)\|^2 = 36^2 \sum_{j=1}^{2m} |\zeta_j|^4 \ge \frac{36^2}{2m} \|\zeta\|^4.$$

The remaining gradient terms are affine. Properness and homotopy invariance therefore give degree $(-2)^{2m} = 4^m$. The local-degree argument from Theorem 4.1 proves (22), the real lower bound and existence. The upper bound is the scheme length.

For the upper endpoint, take $Q = 0$ and all marginals equal to $(1, 1, 1)$. The product of the fibers in Proposition 4.2 has 16^m nondegenerate real points. For the lower endpoint, subtract the lower-degree part after the real Fourier change and add a linear term so that the real objective is

$$12 \sum_{j=1}^{2m} (\Re(\zeta_j^3) - 3\Re\zeta_j).$$

The Fourier change is real-linear on the real locus, so the subtracted lower-degree part pulls back to a real polynomial of degree at most two in the original affine entries and is an admissible choice of Q. For one complex coordinate $\zeta = x + iy$, its real critical equations are $x^2 - y^2 = 1$ and $xy = 0$, with precisely the two real solutions $(1, 0), (-1, 0)$. Both have a nonsingular Hessian of index one. The two remaining complex solutions, $(0, i)$ and $(0, -i)$, are also simple. The product fiber is therefore reduced and has exactly $2^{2m} = 4^m$ real points. □

The freeness argument is an application of monic division, and the real count uses standard topological degree. Their applicability here comes from the fixed Fourier form of the constrained permanent. By [1] and the finite critical set, every model (21) has at most one real local minimum, which is nondegenerate when it exists; the same holds for a local maximum. Thus exponentially many critical points need not mean many local minima.

This extension does not give a uniform finite-fiber theorem for a single larger permanent. For $n \geq 4$, at zero marginals the critical locus already contains a linear space of dimension $(n-3)(n-1)$: allow only $n-2$ rows to be nonzero and retain zero row and column sums. Every deleted $(n-1)\times(n-1)$ submatrix then has a zero row, so every permanental cofactor vanishes. The coupled theorem preserves the three-by-three cubic part; it does not bypass this higher-order obstruction.

A The arithmetic certificate

For the marginals in Lemma 3.1, the integer characteristic polynomial is

$$\begin{aligned} P(T) = {} & 408146688T^{16} - 8707129344T^{15} + 86527097856T^{14} \\ & - 536455913472T^{13} + 2329062481152T^{12} - 7451502170112T^{11} \\ & + 17832473968896T^{10} - 31687859460096T^9 + 41014578486048T^8 \\ & - 38163217509376T^7 + 27153635566144T^6 - 19514196428288T^5 \\ & + 16713475641296T^4 - 11332168247040T^3 + 4055004716400T^2 \\ & - 526381200000T - 8005078125. \end{aligned}$$

The following lists give coefficients in descending order of the monic irreducible factors of P modulo each prime. The leading coefficient of P is nonzero at all three primes.

Prime	Coefficient lists
29	$(1, 27, 9, 25, 7, 20, 3, 3, 1, 17, 9, 5, 16, 28, 24, 22, 28)$
73	$(1, 2, 61)$; $(1, 4, 66, 51, 44, 7, 12, 27)$; $(1, 70, 22, 43, 0, 33, 47, 60)$
97	$(1, 43)$; $(1, 65, 36, 62, 18, 19, 47, 6, 56, 57, 18, 12, 30, 12, 12, 19)$

Their products equal the monic reductions of P, and the factors are distinct. Irreducibility of each monic degree-d factor f over $\mathbb{F}_p$ is certified by

$$T^{p^d} \equiv T \pmod{f}, \qquad \gcd(f, T^{p^{d/q}} - T) = 1 \quad \text{for every prime } q \mid d.$$

The script `verify_permanents.py` checks these identities by modular exponentiation and Euclidean division, rather than relying on a numerical Galois-group computation. It also reconstructs the rational multiplication matrix giving P, the fold multiplication matrix giving (13), the Jacobian tests (12), and the Hessian formulas (18). The JSON certificates contain exact rational coefficients and the real-root certificates used in Table 1; the displayed arithmetic polynomial is stored with integer coefficients.

References

[1] A. A. Ahmadi and J. Zhang, *Complexity aspects of local minima and related notions*, Adv. Math. **397** (2022), 108119. 10.1016/j.aim.2021.108119.

[2] S. Basu, R. Pollack and M.-F. Roy, *Algorithms in Real Algebraic Geometry*, 2nd ed., Algorithms and Computation in Mathematics 10, Springer, 2006. 10.1007/3-540-33099-2.

[3] G.-S. Cheon and I. M. Wanless, *An update on Minc's survey of open problems involving permanents*, Linear Algebra Appl. **403** (2005), 314–342. 10.1016/j.laa.2005.02.030.

[4] D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*, 2nd ed., Graduate Texts in Mathematics 185, Springer, 2005. 10.1007/b138611.

[5] A. Esterov, *Galois theory for general systems of polynomial equations*, Compositio Math. **155** (2019), no. 2, 229–245. 10.1112/S0010437X18007868. See also the addendum in arXiv:1801.08260v3.

[6] P. M. Gibson, *Permanental polytopes of doubly stochastic matrices*, Linear Algebra Appl. **32** (1980), 87–111. 10.1016/0024-3795(80)90009-9.

[7] M. Golubitsky and V. Guillemin, *Stable Mappings and Their Singularities*, Graduate Texts in Mathematics 14, Springer, New York, 1973. 10.1007/978-1-4615-7904-5.

[8] J. W. Milnor, *Topology from the Differentiable Viewpoint*, University Press of Virginia, Charlottesville, 1965.

[9] B. N. Moyls, M. Marcus and H. Minc, *Permanent preservers on the space of doubly stochastic matrices*, Canad. J. Math. **14** (1962), 190–194. 10.4153/CJM-1962-014-1.

[10] J. Nie and K. Ranestad, *Algebraic degree of polynomial optimization*, SIAM J. Optim. **20** (2009), no. 1, 485–502. 10.1137/080716670.

[11] F. Rouillier, *Solving zero-dimensional systems through the rational univariate representation*, Appl. Algebra Engrg. Comm. Comput. **9** (1999), no. 5, 433–461. 10.1007/s002000050114.

[12] J.-P. Serre, *Topics in Galois Theory*, 2nd ed., Research Notes in Mathematics 1, A K Peters, Wellesley, MA, 2008.