hexagon:2611.01286v1

The Alon–Tarsi conjecture at orders 26, 94 and 118

Nils Juenemann
arxiv@nilsjuenemann.de

October 2026

Abstract

The Alon–Tarsi conjecture says that for every even n the numbers of even and odd Latin squares of order n differ. It is known for $n = p \pm 1$ with p an odd prime, and $n = 26$ has been the smallest open order. I prove it for $n = 26$, 94 and 118, so that it holds for all even $n \le 118$. For $n = p + 3$ the conjecture follows whenever $4K_6(p) \not\equiv 5 \pmod p$, where $K_6(p) = \sum_{j<p} j!\,6^{-j}$; below 10^6 this fails only for $p = 59729$. For $n = p+m$ I reduce the next p-adic digit to a signed count of Latin rectangles with m rows and write this count as a pairing in an algebra with commuting and anticommuting variables. For $m = 5$ a computer-assisted closed form gives a Kurepa-type criterion, which settles $n = 94$ and $n = 118$ and, with Glynn's theorem for one exceptional prime, all $n = p + 5$ with $7 \le p \le 300\,000$.

Contents

1 Introduction **2**
1.1 Historical context . . . 2
1.2 Results . . . 3
1.3 The proof and its main ingredients . . . 4
1.4 Organisation . . . 6

2 The circuit partition polynomial **6**

3 A congruence modulo p **9**

4 The second digit sits at a ladder value **11**

5 Ladder values **12**
5.1 Ladder values as sums of determinants . . . 12
5.2 Sign cancellation in sums over partial derangements . . . 13
5.3 The value $g_n(-2)$ . . . 15
5.4 The components in the proof of Theorem 5.5 . . . 17

6 The second digit modulo p **19**

7 Full layers and the orders 94 and 118 **20**
7.1 Reduction to full layers . . . 21
7.2 A pairing formula . . . 23
7.3 Five layers . . . 26

7.4 Pfaffian moments 27
7.5 The closed form for five layers 29

8 Computations **31**

9 Concluding remarks **33**

A The case $p+2$ **34**

B Computational details **35**

1 Introduction

The *sign* of a Latin square is the product of the signs of its n rows and its n columns, each read as a permutation, and L_n^e and L_n^o denote the numbers of Latin squares of order n with sign $+1$ and -1. Alon and Tarsi [1] conjectured that $L_n^e \neq L_n^o$ for every even n. They needed this for a statement on list colourings of graphs, and Huang and Rota [18] connected it with Rota's basis conjecture; the survey of Friedman and McGuinness [11] describes many equivalent forms. The form I use is the coefficient

$$D_n = [x_{11}x_{12}\cdots x_{nn}]\det(X)^n$$

of the product of all entries in the n-th power of the determinant of an $n \times n$ matrix X of indeterminates. Expanding the n factors into permutations shows that D_n is the number of Latin squares whose n symbol permutations have product of signs $+1$, minus the number of the others (Section 2). A Latin square is *row-even* if the product of the signs of its rows is $+1$, and L_n^{re}, L_n^{ro} count the row-even and row-odd squares. By conjugation $D_n = L_n^{re} - L_n^{ro}$, and by Janssen's identity [19, Theorem 3.2] (see also [31, Proposition 2] and [27, (1.2)]), the product of the row, column and symbol signs of a Latin square is $(-1)^{\binom{n}{2}}$ (Janssen writes $(-1)^{\lfloor n/2 \rfloor}$, which is the same sign), so that

$$L_n^e - L_n^o = (-1)^{\binom{n}{2}} D_n.$$

For odd $n \geq 3$, swapping two columns changes the sign of every row and shows $D_n = 0$; the conjecture is about even n.

1.1 Historical context

The conjecture is known for $n = p+1$ (Drisko [9, Theorem 9]) and for $n = p-1$ (Glynn [15]), where p is an odd prime. Glynn determines D_{p-1} modulo p; Drisko determines D_{p+1} modulo p^3, the first power of p that does not divide it. After his proof Drisko suggested trying the orders p^k+1, $p+3$ and $pq+1$ next [9, Section 5] (see also [27, p. 6]). Zappa [32] gave a doubling argument, from n to $2n$, on which Drisko [10] based the case $n = 2^r p$, but Glynn [15] found a gap in it (see also [27, p. 7]). The smallest even order not of the form $p \pm 1$ is 26, and $n = 26$ has been the smallest open case [15, Corollary 3.4], [11, Section 1.1]. Stones and Wanless [27] showed that Drisko's method cannot work for any of these: for every $t \leq n$ one has $D_{n+1} \equiv 0 \pmod{t^3}$ unless $t = n$ is an odd prime [27, Corollary 3.7]. For $n = p+3$ the number D_n is therefore divisible by p^3, and a proof along these lines needs the next p-adic digit. Berndsen [5, Section 2.9.4] took the next step for the unipotent version at $n = p+2$ (see below) and remarked that $p+3$, which would include $n = 26$, did not seem within reach of those techniques.

1.2 Results

The aim of this paper is to go one p-adic digit further. For $n = p + 3$ the next digit can be computed in closed form.

Theorem 1.1. *Let $p \geq 5$ be a prime and $n = p + 3$, and let*

$$K_6(p) = \sum_{j=0}^{p-1} j!\, 6^{-j} \pmod{p}.$$

Then $D_n = n!\,(n-1)!\,U_n$ with an integer $U_n \equiv 0 \pmod{p}$, and

$$\frac{U_n}{p} \equiv -6\,(4K_6(p) - 5) \pmod{p}.$$

In particular, if $4K_6(p) \not\equiv 5 \pmod{p}$, then D_n is divisible by exactly p^3, and the Alon–Tarsi conjecture holds for n.

Here U_n is the signed number of normalised unipotent Latin squares defined below; the factor $n!(n-1)!$ is divisible by exactly p^2, since $p \leq n - 1 < 2p$. For $p = 23$ one finds $K_6(23) \equiv 5$, so $4K_6(23) - 5 \equiv 15$.

Corollary 1.2. *The Alon–Tarsi conjecture holds for $n = 26$. More precisely, $D_{26} = L_{26}^{re} - L_{26}^{ro}$ satisfies*

$$\frac{D_{26}}{23^3} \equiv 1 \pmod{23}.$$

The condition of Theorem 1.1 is a congruence for a sum of factorials, of the same kind as Kurepa's left factorial hypothesis [21], which in its usual form (equivalent to Kurepa's original statement $\gcd(!n, n!) = 2$ for $n > 1$, see [24, Section 1]) asserts that $\sum_{j<p} j!$ is never divisible by an odd prime p; it is open and has been verified for all odd primes $p < 2^{40}$ [2], and a proof claimed in [3] was withdrawn [4]. I checked all primes $5 \leq p < 10^6$ and found exactly one with $4K_6(p) \equiv 5$, namely $p = 59729$. Hence the conjecture holds for all even $n = p + 3$ with $p < 10^6$, $p \neq 59729$. Up to 300 this adds the orders 26, 34, 50, 56, 64, 76, 86, 92, 116, 134, 142, 154, 160, 170, 176, 184, 202, 214, 236, 244, 254, 260, 266, 274, 286, 296 to the orders $p \pm 1$. Together with the theorems of Drisko and Glynn this gives the conjecture for all even $n \leq 92$.

The next open orders were $94 = 89 + 5$ and $118 = 113 + 5$. For $n = p + m$ with $m \geq 3$ the second p-adic digit turns out to depend only on a signed count of Latin rectangles with m rows (Section 7), which can be written as a pairing of two powers in an algebra with commuting and anticommuting variables. For $m = 5$ I evaluate this pairing in closed form: up to a rational factor, the generating function of these counts is the Euler series $\sum_N (N+4)!\, x^N$ at $x = u/(1+6u)^3$ (Theorem 7.13). The proof combines an elementary computation of Pfaffian moments with an exact computer elimination of the anticommuting variables. As for $p + 3$, the second digit becomes a Kurepa-type sum, now over the integer coefficients of a fixed power series that satisfies an explicit linear differential equation (Theorem 7.14).

Theorem 1.3 (computer-assisted)**.** *The Alon–Tarsi conjecture holds for $n = 94$ and $n = 118$. More precisely,*

$$\frac{D_{94}}{89^3} \equiv 1 \pmod{89}, \qquad \frac{D_{118}}{113^3} \equiv 96 \pmod{113}.$$

Hence the conjecture holds for all even $n \le 118$, and by a result of Huang and Rota [18] also Rota's basis conjecture in these dimensions over fields of characteristic zero. The smallest open order is now 120 (Corollary 8.1). The criterion of Theorem 7.14 holds for all primes $7 \le p \le 300\,000$ except $p = 4787$, whose order 4792 is covered by Glynn's theorem. Up to 300 this adds, besides 94 and 118, the orders 144, 186, 204, 216, 246, 288 and 298.

The same method applies to Zappa's extension of the conjecture [32]. A Latin square of order n is *unipotent* if all entries on its main diagonal are equal. Let U_n be the number of unipotent Latin squares with diagonal symbol 1 and first row $(1, 2, \dots, n)$, each counted with the product of the signs of its n symbol permutations (the permutation of symbol s maps each row to the column where s occurs). Equivalently, $(n-1)!\,U_n$ is the coefficient of the product of the off-diagonal entries in $\det(X)^{n-1}$ (Lemma 2.4). For even n one has $D_n = n!\,(n-1)!\,U_n$, which was used in Theorem 1.1. By Janssen's identity, $U_n = (-1)^{\binom{n}{2}}(U_n^e - U_n^o)$ in the notation of [27, Section 1], where the parity of a square is that of its rows and columns. The extended conjecture says that $U_n \neq 0$ for all n. For odd n it is known for $n = p$ (Drisko [10]). Stones and Wanless proved $R_n^e \equiv R_n^o \pmod p$ for reduced squares of order $n \ge p+2$ [27, Theorem 3.5] and remarked after that theorem, omitting the details, that the numbers R_n^π of reduced squares in the four parity classes π allowed by Janssen's identity are all congruent modulo p; together with their Table 1, which expresses U_n^e and U_n^o through these numbers, this gives $p \mid U_{p+2}$. Berndsen [5, Theorem 2.25] determined the next digit at $n = p+2$; up to the sign convention his result reads as follows in the present normalisation, and Appendix A gives a new proof.

Theorem 1.4 (Berndsen)**.** *Let $p \ge 3$ be a prime. Then $U_{p+2} \equiv 0 \pmod p$ and*

$$\frac{U_{p+2}}{p} \equiv \sum_{j=1}^{p-1} j!\,2^{-j} \pmod p.$$

Berndsen checked that the sum is nonzero modulo p for all primes $3 \le p < 2^{20}$ except $p = 234781$; my computation up to 10^6 agrees.

1.3 The proof and its main ingredients

The starting point is the *circuit partition polynomial* $j_n(t)$ of the complete directed graph K_n^* without loops: the sum of $t^{c(T)}$ over all ways T of decomposing the arcs into closed trails, where $c(T)$ is the number of trails. It is divisible by $t(t+1)\cdots(t+n-2)$, and the quotient $g_n(t)$ satisfies $U_n = (-1)^{n-1} g_n(1-n)$ for every n. Hence the conjecture asks that the integer polynomial g_n does not vanish at $t = 1-n$. The first new ingredient is a Lucas-type congruence modulo p for these polynomials (Theorem 3.1), proved by letting a cyclic group of order p act on p of the vertices. For $n = p+m$ it shows that g_n vanishes modulo p to order at least $m-1$ at $t \equiv 1-m$. This is the obstruction of Stones and Wanless in polynomial form, and it has a useful consequence: for $m \ge 3$ a Taylor expansion gives $g_n(1-n) \equiv g_n(1-m) \pmod{p^2}$. The second p-adic digit of U_n is therefore determined by the value of g_n at the small integer $1-m$, a *ladder value*. At $t = -k$ the polynomial is a determinant power with only k factors, and the ladder value becomes a sum over k partial derangements of the number of Eulerian circuits of the remaining graph. The BEST theorem and the matrix-tree theorem turn the circuit counts into determinants, and after expanding the determinants, a sign cancellation in sums over partial derangements (Lemma 5.4) collapses the sum to a short list of configurations. For $k = 1$ and $k = 2$ this gives closed formulas, and reducing them modulo p^2 gives the factorial sums above.

This explicit route stops at $k = 2$: the number of configurations grows quickly with k. For larger offsets the paper takes a second route, which only works modulo p^2 but avoids the classification. A cyclic group argument shows that modulo p^2 only k-tuples of derangements moving every vertex contribute, that is, Latin rectangles with $k+1$ rows (Lemma 7.1). For even k a Möbius inversion over set partitions turns their signed count into a pairing of two powers in an algebra whose number of variables depends only on k (Theorem 7.4). This pairing formula, and the congruence modulo p of Lucas type that it implies (Theorem 7.5), are the main structural results of the second part; the orders 94 and 118 are their first applications. Figure 1 shows how the parts of the proof fit together.

In combinatorial terms the pairing formula works as follows. Section 7 adds one more permutation π_0 to the rows $\pi_1, \dots, \pi_{k+1}$ of the rectangle. Lay the permutation matrices of $\pi_0, \dots, \pi_{k+1}$ on top of each other. Row v then has entries in the columns $\pi_0(v), \dots, \pi_{k+1}(v)$, and the condition on the tuple says, row by row, which of these columns coincide. By inclusion and exclusion over set partitions, as in Gessel's treatment of Latin rectangles [12], each row becomes a signed sum of patterns, and the N rows give an N-th power. The condition that every π_i is a permutation concerns the columns and gives a second N-th power. What remains is to glue the patterns of the rows to those of the columns, and the pairing counts these gluings. Draw the rows on one line and the columns on another, and join the glued pieces by lines. The sign of the tuple is then, up to signs that depend only on single rows and columns, (-1) to the number of crossings between lines that join pieces of odd size, and configurations with two such lines of the same type cancel in pairs. Anticommuting variables are a bookkeeping device for exactly this crossing parity, in the same way as the Pfaffian records signed perfect matchings. The gain is that N enters only as an exponent, while the number of variables stays fixed. For five layers this makes generating functions, Gaussian integrals and the symmetry of antisymmetric 6×6 matrices available.

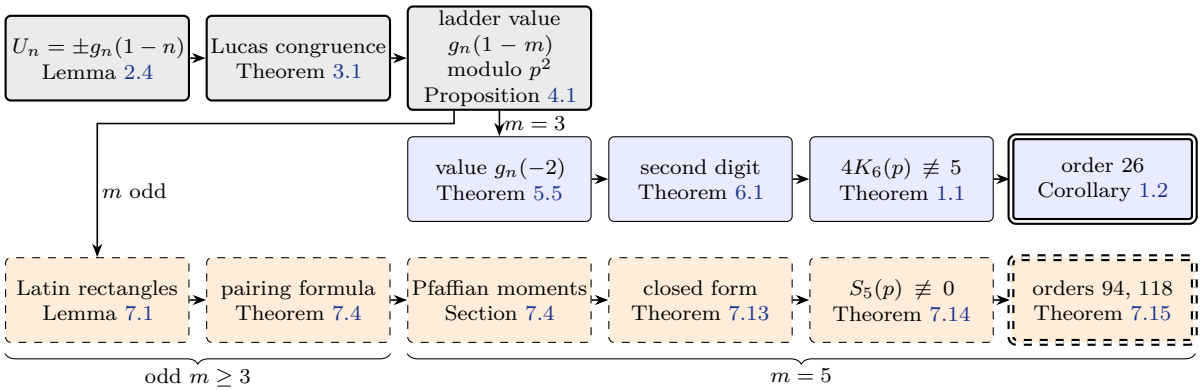

Figure 1: The structure of the proof for $n = p + m$ with a prime p. The common part reduces $g_n(1-n) = \pm U_n$ modulo p^2 to the ladder value $g_n(1-m)$. The common part uses Lemma 2.4, Theorem 3.1 with Corollary 3.2, and Proposition 4.1. The branch $m = 3$ evaluates this value in closed form (Lemmas 5.1 to 5.4 and Theorem 5.5), reduces it modulo p^2 (Theorem 6.1) and gives Theorem 1.1 and the order 26. The branch for odd m writes it modulo p^2 as a signed count of Latin rectangles (Lemma 7.1, Corollary 7.3) and evaluates the count for $m = 5$ (Theorem 7.4, Section 7.4, Theorems 7.13 to 7.15).

1.4 Organisation

Sections 2 to 6 follow the first route and prove Theorem 1.1, and Section 7 follows the second route and proves Theorem 1.3. Section 8 reports the computations and Section 9 the limits of the method. Appendix A treats the order $p+2$ (Theorem 1.4), and Appendix B describes the independent checks of the computations. Readers interested only in the order 26 need Sections 2 to 6 and the first paragraph of Section 8; anticommuting variables appear only in Section 7.

2 The circuit partition polynomial

Throughout, $V = [n]$ and arcs are ordered pairs (u, v) of vertices. Let K_n^* be the complete directed graph on V with the $n(n-1)$ arcs (u, v), $u \neq v$, and K_n° the complete directed graph with all n^2 arcs, loops included. A directed graph is *Eulerian* if every vertex has equal in-degree and out-degree. A *transition system* T of a directed graph G chooses at every vertex v a bijection from the arcs entering v to the arcs leaving v; it exists only if G is Eulerian. Following the chosen transitions decomposes the arcs of G into closed trails; let $c(T)$ be their number. The *circuit partition polynomial* of G is

$$j(G;t) = \sum_T t^{c(T)}.$$

(so $j(G;t) = 0$ if G is not Eulerian). It counts decompositions of the arc set into closed trails, weighted by t per trail; it is a directed relative of the Martin polynomial. I write $j_n(t) = j(K_n^*;t)$ and $J_n(t) = j(K_n^\circ;t)$. Since K_n^* has $\prod_v (n-1)!$ transition systems,

$$j_n(1) = ((n-1)!)^n. \tag{2.1}$$

Figure 2 shows a transition system of K_3^* and its closed trails.

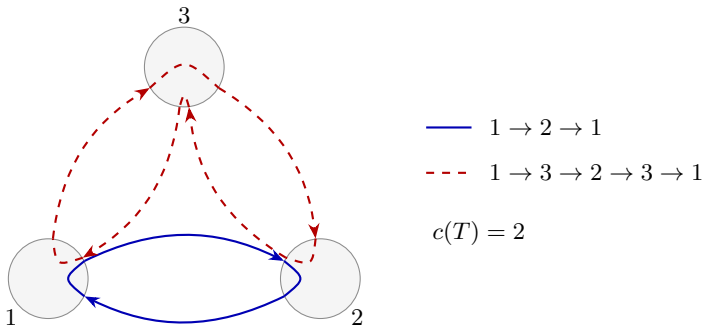

Figure 2: A transition system T of K_3^*. At each vertex the two entering arcs are paired with the two leaving arcs (curves inside the grey discs), and following these transitions gives the closed trails $1 \to 2 \to 1$ and $1 \to 3 \to 2 \to 3 \to 1$, so $c(T) = 2$. By (2.1), K_3^* has $(2!)^3 = 8$ transition systems.

The loops of K_n° only contribute a linear factor each.

Lemma 2.1. *Let G be a directed graph, and let the vertex v of in-degree d carry a loop ℓ. Then $j(G;t) = (t+d-1)\, j(G-\ell;t)$. In particular $J_n(t) = (t+n-1)^n j_n(t)$.*

Proof. Fix a transition system of G. Either it maps ℓ to itself, and then ℓ is a closed trail of its own and the rest is a transition system of $G-\ell$; this gives $t\, j(G-\ell;t)$. Or it maps some

arc $e \neq \ell$ entering v to ℓ and ℓ to some arc f leaving v. Replacing the passage $e \to \ell \to f$ by the transition $e \to f$ gives a transition system of $G - \ell$ with the same number of closed trails. Conversely, each transition system of $G - \ell$ arises in this way from exactly $d - 1$ systems of G, one for each choice of the arc e among the $d - 1$ arcs entering v in $G - \ell$. (If G is not Eulerian, neither is $G - \ell$, and both sides vanish.) The vertices of K_n° have in-degree n, which gives the second statement. □

The polynomial has a determinant formula, which is a form of MacMahon's master theorem for the α-permanent of Vere-Jones [30, (3)]. I give the short proof, since its ingredients are used later. Let $X = (x_{uv})$ be the $n \times n$ matrix with $x_{uu} = 0$ and independent indeterminates x_{uv} for $u \neq v$, one for each arc of K_n^*. For a set F of arcs write $x^F = \prod_{e \in F} x_e$, and let E be the set of all arcs of K_n^*. It is convenient to work in the ring $R = \mathbb{Q}[x_e : e \in E]/(x_e^2 : e \in E)$, in which a monomial survives only if it uses each arc at most once. A *partial derangement* is a permutation σ of a subset $S_\sigma \subseteq V$ without fixed points; it is the set of arcs $(v, \sigma(v))$, $v \in S_\sigma$, and $c(\sigma)$ denotes its number of cycles. Since $\operatorname{sgn}\sigma = (-1)^{|S_\sigma| - c(\sigma)}$, the expansion of $\det(I - X)$ into principal minors reads

$$\det(I - X) = \sum_{\sigma} (-1)^{c(\sigma)} x^\sigma, \tag{2.2}$$

the sum over all partial derangements. Each monomial on the right uses at most one arc leaving each vertex.

Lemma 2.2. *In R one has $\log\det(I - X) = -\sum_H \operatorname{ec}(H)\, x^H$, where H runs over the nonempty sets of arcs that form a connected Eulerian graph and $\operatorname{ec}(H)$ is the number of Eulerian circuits of H, counted as cyclic sequences of arcs. Consequently, for every integer $a \geq 0$ and every set $F \subseteq E$ of arcs,*

$$[x^F]\det(I - X)^a = j(F; -a), \qquad \textit{in particular} \quad [x^E]\det(I - X)^a = j_n(-a),$$

where $j(F; t)$ is the circuit partition polynomial of the graph (V, F).

Proof. As formal power series, $\log\det(I - X) = \operatorname{tr}\log(I - X) = -\sum_{k \geq 1} \operatorname{tr}(X^k)/k$. The trace $\operatorname{tr}(X^k)$ is the sum of x over the closed walks of length k with a marked starting arc. In R only walks with k distinct arcs survive. Such a walk is an Eulerian circuit of its arc set H, with $|H| = k$ and a marked start, and each Eulerian circuit has exactly k starting arcs. This proves the first statement. Hence $\det(I - X)^a = \exp(a \log\det(I - X)) = \exp(-a \sum_H \operatorname{ec}(H) x^H)$ in $R[a]$, a polynomial identity in a because the exponent is nilpotent. The coefficient of x^F on the right is the sum, over all partitions of F into blocks $H_1, \dots, H_k$ that are connected Eulerian graphs, of $(-a)^k \prod_i \operatorname{ec}(H_i)$. Choosing an Eulerian circuit in each block is the same as choosing a transition system with k closed trails, so the coefficient is $\sum_T (-a)^{c(T)} = j(F; -a)$. For integers $a \geq 0$ the left side is an honest polynomial, and its image in R has the same coefficient of x^F. □

The formula shows at once that j_n has many integer roots, and it identifies the value at $t = 1 - n$. For an $n \times n$ $(0,1)$-matrix M and $k \geq 1$ let $c_k(M) = [x^M]\det(X')^k$, where X' is a matrix of n^2 independent indeterminates and x^M is the product of the entries in the support of M. Expanding each of the k factors by the Leibniz formula, $c_k(M)$ is the sum of $\prod_{i=1}^k \operatorname{sgn}\sigma_i$ over the ordered decompositions of M into k permutation matrices $P_{\sigma_1}, \dots, P_{\sigma_k}$. Let J be the all-ones matrix.

Lemma 2.3. *For $0 \le a \le n-2$ one has $j_n(-a) = 0$, and $j_n(1-n) = c_{n-1}(J-I)$. Consequently*

$$j_n(t) = t(t+1)\cdots(t+n-2)\, g_n(t)$$

with $g_n \in \mathbb{Z}[t]$ of degree $\binom{n-1}{2}$, and $c_{n-1}(J-I) = (-1)^{n-1}(n-1)!\, g_n(1-n)$.

Proof. By (2.2), every monomial of $\det(I-X)^a$ uses at most a arcs leaving each vertex. Every vertex has $n-1$ arcs leaving it, so $[x^E]\det(I-X)^a = 0$ for $a \le n-2$, and Lemma 2.2 gives the roots. For $a = n-1$ each of the $n-1$ factors must contribute exactly one arc leaving every vertex, that is, a derangement σ_i of all of V, and the $n-1$ derangements must partition E. The coefficient of such a term is $\prod_i (-1)^{c(\sigma_i)} = \prod_i (-1)^n \operatorname{sgn}\sigma_i = \prod_i \operatorname{sgn}\sigma_i$, since $n(n-1)$ is even. Summing over all ordered decompositions of $J-I$ into $n-1$ permutation matrices gives $c_{n-1}(J-I)$. The polynomial j_n has integer coefficients and the distinct roots $0, -1, \ldots, -(n-2)$, so the monic polynomial $t(t+1)\cdots(t+n-2)$ divides it in $\mathbb{Z}[t]$ and $g_n \in \mathbb{Z}[t]$. Its degree is $\binom{n-1}{2}$, since a transition system has at most $\binom{n}{2}$ closed trails (each has length at least 2) and the decomposition into 2-cycles attains this. Finally, $(1-n)(2-n)\cdots(-1) = (-1)^{n-1}(n-1)!$. □

The next lemma connects these quantities with Latin squares. An ordered decomposition $(P_1, \ldots, P_n)$ of J into permutation matrices is the same thing as a Latin square, with symbol s in the cells of P_s; P_s is the matrix of the *symbol permutation* of s, which maps each row to the column where s occurs. Thus $D_n = c_n(J)$ is the sum over all Latin squares of order n of the product of the signs of their symbol permutations. Figure 3 shows a Latin square of order 4 and its symbol permutations.

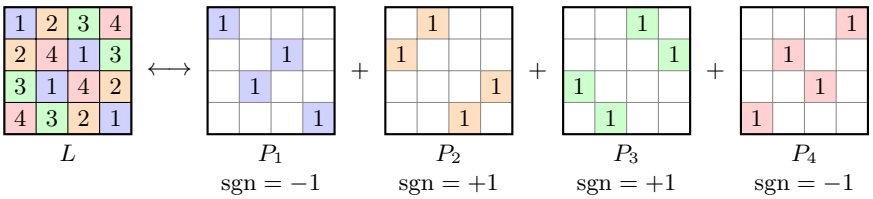

Figure 3: A Latin square L of order 4 and the matrices P_s of its symbol permutations: P_s has its entries 1 in the cells of the symbol s, and $P_1 + P_2 + P_3 + P_4 = J$.

Lemma 2.4. *1. $D_n = L_n^{re} - L_n^{ro}$.*

2. $c_{n-1}(J-I) = (n-1)!\, U_n$, with U_n as in Section 1, and hence $U_n = (-1)^{n-1} g_n(1-n)$.

3. If n is even, then $D_n = n!\, c_{n-1}(J-I) = n!\,(n-1)!\, U_n$.

Proof. (1) Exchanging the roles of rows and symbols, $(r, c, s) \mapsto (s, c, r)$, is a bijection on Latin squares. It turns the symbol permutation of s into the inverse of the permutation of row s (as a map from columns to symbols), which has the same sign.

(2) The decompositions of $J-I$ into $n-1$ permutation matrices $P_2, \ldots, P_n$ are the unipotent Latin squares with diagonal symbol 1, where $P_1 = I$ has sign $+1$. Relabelling the symbols $2, \ldots, n$ permutes the P_s and does not change the product of their signs. Each orbit has $(n-1)!$ elements and contains exactly one square with first row $(1, 2, \ldots, n)$. The second statement follows from Lemma 2.3.

(3) Let $(P_1, \ldots, P_n)$ be a decomposition of J and $P_1 = P_\pi$. Multiplying every P_s on the right by P_π^{-1} gives a decomposition with first matrix I, and it changes the product of the signs

by $(\operatorname{sgn}\pi)^n = 1$. This is a bijection between the decompositions with $P_1 = P_\pi$ and those with $P_1 = I$, for each of the $n!$ permutations π. The decompositions with $P_1 = I$ are counted by $c_{n-1}(J - I)$. □

Part (3) is Zappa's reduction to unipotent squares; for odd $n \geq 3$ the same map multiplies the sign by $\operatorname{sgn}\pi$, and since $\sum_\pi \operatorname{sgn}\pi = 0$ this gives $D_n = 0$. In the remaining sections I work with g_n. By Lemma 2.4, the Alon–Tarsi conjecture for even n and Zappa's extended conjecture for all n both say that $g_n(1-n) \neq 0$.

Remark 2.5. For $n = 4$ one finds $j_4(t) = t(t+1)(t+2)\,(t^3 + 13t^2 + 74t + 128)$, so $g_4(-3) = -4$ and $U_4 = 4$, $D_4 = 4!\,3! \cdot 4 = 576$. For $n = 5$ the polynomial $g_5(t) = t^6 + 34t^5 + 570t^4 + 6032t^3 + 38069t^2 + 125070t + 162000$ gives $U_5 = g_5(-4) = -24$.

3 A congruence modulo p

The following congruence describes J_n modulo p in terms of smaller orders. It is the polynomial behind the divisibility results of Stones and Wanless [26, 27] and behind the cases of Drisko and Glynn. Put $J_0 = 1$.

Theorem 3.1. *Let p be a prime and $m \geq 0$. Then, coefficientwise modulo p,*

$$J_{p+m}(t) \equiv J_p(t+m)\,J_m(t)\,(t^p - t)^m \pmod p.$$

Moreover $J_p(t) \equiv \sum_\tau \prod_C f(V_C) \pmod p$, where τ runs over the permutations of $\mathbb{Z}_p$, C over the cycles of τ, $V_C \in \mathbb{Z}_p$ is the sum of the elements of C, and $f(V) = t^p$ if $V = 0$ and $f(V) = t$ otherwise.

The idea is to let a cyclic group of order p rotate p of the vertices. Orbits of length p vanish modulo p, and the fixed transition systems have a simple structure: the remaining m vertices behave like an independent copy of K_m°, and each of them contributes a factor $t^p - t$ after summing over a shift in $\mathbb{Z}_p$. Figure 4 shows the contraction of the arcs through M for $p = 5$ and $m = 2$.

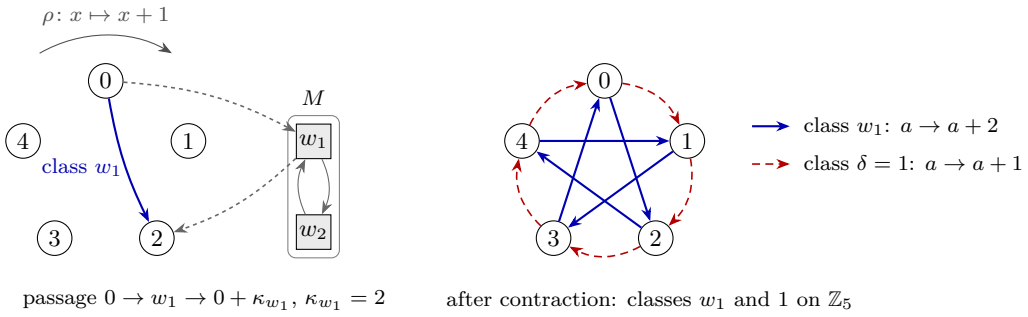

Figure 4: The fixed transition systems in the proof of Theorem 3.1 for $p = 5$ and $m = 2$. Left: the vertices of $\mathbb{Z}_5$, rotated by ρ, and $M = \{w_1, w_2\}$; a fixed system maps (a, w_1) to $(w_1, a + \kappa_{w_1})$, and the passage $0 \to w_1 \to 2$ (dotted, $\kappa_{w_1} = 2$) is replaced by one arc of class w_1. Right: after the contraction every vertex of $\mathbb{Z}_5$ has one entering and one leaving arc of each class, shown here for the class w_1 and the class $\delta = 1$.

Proof. Let $V = \mathbb{Z}_p \sqcup M$ with $|M| = m$, and let $A = V \times V$ be the arc set of K°_{p+m}. A transition system is a permutation Φ of A such that each arc $e = (u, v)$ is mapped to an arc leaving v, and $c(\Phi)$ is its number of cycles. Let ρ act on V by $x \mapsto x + 1$ on $\mathbb{Z}_p$ and trivially on M. It acts on A, and by conjugation on transition systems, preserving the number of cycles. Orbits have length 1 or p, so $J_{p+m}(t)$ is congruent modulo p to the sum of $t^{c(\Phi)}$ over the systems with $\rho\Phi\rho^{-1} = \Phi$.

Let Φ be fixed by ρ. The arcs fixed by ρ are those of $A_M = M \times M$. If $e \in A_M$, then $\Phi(e)$ is fixed by ρ, so Φ maps A_M to itself, and its restriction is an arbitrary transition system of K°_m on M. The other arcs are permuted among themselves. For $w \in M$, the arcs (a, w) with $a \in \mathbb{Z}_p$ are mapped to arcs (w, c) with $c \in \mathbb{Z}_p$, and $\Phi(a + 1, w) = \rho\Phi(a, w)$ forces $\Phi(a, w) = (w, a + \kappa_w)$ for some $\kappa_w \in \mathbb{Z}_p$. At the vertices of $\mathbb{Z}_p$, Φ is determined by its bijection at the vertex 0, which is arbitrary. Replace each passage $a \to w \to a + \kappa_w$ by a single arc of *class* w from a to $a + \kappa_w$, and give the arc $(a, a + \delta)$ with $\delta \in \mathbb{Z}_p$ the class δ. This does not change the number of cycles. Every vertex of $\mathbb{Z}_p$ now has one entering and one leaving arc of each class in $\Gamma = \mathbb{Z}_p \sqcup M$, and the bijection at 0 is a permutation π of Γ. Thus the fixed systems correspond to the triples (system on K°_m, $\kappa \in \mathbb{Z}_p^M$, $\pi \in \mathrm{Sym}(\Gamma)$); conversely each triple defines a fixed system, and different triples give different systems. The cycle count is the sum of the counts of the two parts.

Give the class x the displacement $\delta_x = x$ for $x \in \mathbb{Z}_p$ and $\delta_w = \kappa_w$ for $w \in M$. A cycle $(x_1, \dots, x_l)$ of π with total displacement $V = \sum_i \delta_{x_i}$ describes the walks that start at some vertex b with class x_1 and return to class x_1 at the vertex $b + V$. The pl arcs with these classes therefore form p cycles if $V = 0$, and, since p is prime and so V generates $\mathbb{Z}_p$, one cycle of length pl otherwise; the contribution is $f(V)$. Hence

$$J_{p+m}(t) \equiv J_m(t) \sum_{\kappa \in \mathbb{Z}_p^M} \sum_{\pi} \prod_{C} f(V_C) \pmod p. \tag{3.1}$$

For $m = 0$ this is the second statement of the theorem; call its right side $Z(t)$.

Now sum over κ. Consider a cycle of π that contains $k \geq 1$ classes from M. Its displacement is a fixed element of $\mathbb{Z}_p$ plus the sum of the k shifts κ_w of its classes, so it takes every value of $\mathbb{Z}_p$ exactly p^{k-1} times. The cycle contributes $p^{k-1}(t^p + (p-1)t)$, which is $\equiv t^p - t$ if $k = 1$ and $\equiv 0$ if $k \geq 2$. Different cycles involve different shifts, so modulo p only the permutations π survive in which the m classes of M lie in different cycles, and each of these m cycles gives $t^p - t$. Such a π is described by the set $U \subseteq \mathbb{Z}_p$ of elements lying in the cycles through M, by the distribution of U onto these m cycles, and by a permutation τ of $\mathbb{Z}_p \setminus U$. Each cycle through $w \in M$ is w followed by a list of elements of U, and there are $m(m+1)\cdots(m+|U|-1)$ ways to distribute U onto m labelled lists. Hence the double sum in (3.1) is congruent to $(t^p - t)^m\, Y$ with

$$Y = \sum_{U \subseteq \mathbb{Z}_p} m(m+1)\cdots(m+|U|-1) \sum_{\tau \in \mathrm{Sym}(\mathbb{Z}_p \setminus U)} \prod_{C} f(V_C).$$

It remains to show $Y \equiv Z(t+m)$. Modulo p one has $(t+m)^p \equiv t^p + m$, so the function f for the variable $t + m$ is $f + m$. Expanding,

$$Z(t+m) \equiv \sum_{\tau \in \mathrm{Sym}(\mathbb{Z}_p)} \prod_{C} (f(V_C) + m) = \sum_{\tau} \sum_{\mathcal{A}} m^{|\mathcal{A}|} \prod_{C \notin \mathcal{A}} f(V_C),$$

where $\mathcal{A}$ runs over the sets of cycles of τ. Group the terms by the union U of the cycles in $\mathcal{A}$. The cycles in $\mathcal{A}$ form a permutation of U, and $\sum_{\sigma \in \mathrm{Sym}(U)} m^{c(\sigma)} = m(m+1)\cdots(m+|U|-1)$. This gives Y. Since $J_p \equiv Z$ as polynomials, $J_p(t+m) \equiv Z(t+m) \equiv Y$, and the theorem follows. □

For g_n the theorem reads as follows. Put $g_1 = g_2 = 1$; this agrees with Lemma 2.3, since $j_1 = 1$ and $j_2 = t$.

Corollary 3.2. *Let p be a prime and $m \geq 1$. Then in $\mathbb{F}_p[t]$*

$$(t+m-1)\, g_{p+m}(t) = g_p(t+m)\, g_m(t)\, (t^p - t)^m.$$

In particular, the polynomial g_{p+m} is divisible by $(t+m-1)^{m-1}$ modulo p.

Proof. By Lemmas 2.1 and 2.3, $J_n = (t+n-1)^n (t)_{n-1} g_n$ with $(t)_k = t(t+1)\cdots(t+k-1)$. Modulo p, with $n = p+m$, one has $t+n-1 \equiv t+m-1$ and $(t)_{n-1} = (t)_{m-1}\,(t+m-1)\,(t+m)(t+m+1)\cdots(t+m+p-2)$. Inserting this into Theorem 3.1 and cancelling the common nonzero factors $(t+m-1)^n (t)_{m-1}(t+m)\cdots(t+m+p-2)$ in the domain $\mathbb{F}_p[t]$ gives the identity. The factor $t^p - t = \prod_{c \in \mathbb{F}_p} (t-c)$ contains $t+m-1$ once, so $(t^p-t)^m/(t+m-1)$ is divisible by $(t+m-1)^{m-1}$. □

At $t \equiv 1-n \equiv 1-m$ the corollary gives $g_n(1-n) \equiv 0 \pmod p$ for $m \geq 2$, that is, $p \mid U_n$. For reduced squares this divisibility is [27, Theorem 3.5], and for unipotent squares it follows from the remark after that theorem together with [27, Table 1] (Section 1); Corollary 3.2 gives a different proof. At the other end, for $n = p$ one has $1-p \equiv 1$, so $U_p = (-1)^{p-1} g_p(1-p) \equiv g_p(1) = ((p-1)!)^{p-1} \equiv 1 \pmod p$ by (2.1) and Wilson's theorem; this is Drisko's theorem for unipotent squares of prime order [10]. The congruence of Corollary 3.2 is a statement about polynomials, not only about values, and the next section uses this to go one step further.

4 The second digit sits at a ladder value

Corollary 3.2 says more than $p \mid g_n(1-n)$: modulo p, the whole polynomial g_n vanishes to order at least $m-1$ at $t \equiv 1-m$. The points $1-n$ and $1-m$ differ by p, and a Taylor expansion between them turns the order of vanishing into a congruence modulo p^2. I call the values $g_n(-k)$ at the integers $1 \leq k \leq n-2$ the *ladder values*; they lie at the forced roots of j_n. Figure 5 shows their positions and the step from $1-m$ to $1-n$.

Proposition 4.1. *Let p be a prime and $n = p+m$ with $m \geq 3$. Then $g_n(1-m) \equiv 0 \pmod p$ and $g_n(1-n) \equiv g_n(1-m) \pmod{p^2}$.*

Proof. Write $g_n(1-m-p) = \sum_{k \geq 0} c_k (-p)^k$ with the integers $c_k = g_n^{(k)}(1-m)/k!$. The terms with $k \geq 2$ are divisible by p^2. If $m \geq 3$, Corollary 3.2 shows that g_n vanishes modulo p to order at least 2 at $1-m$, so $c_0 = g_n(1-m) \equiv 0$ and $c_1 \equiv 0 \pmod p$, and the term with $k=1$ is divisible by p^2 as well. □

For $n = p+m$ with $2 \leq m < p$ one has $v_p(n!\,(n-1)!) = 2$, where $v_p(x)$ is the exponent of the largest power of p dividing x. By Lemma 2.4 and Corollary 3.2, D_n (for even n) is divisible by p^3, and it is divisible by exactly p^3 if and only if $g_n(1-n) \not\equiv 0 \pmod{p^2}$. For $m \geq 3$ this is the condition $g_n(1-m) \not\equiv 0 \pmod{p^2}$ on a ladder value. The question has moved from the point $1-n$, where nothing is known, to a point where only few factors of the determinant power are involved: by Lemma 2.2, j_n near $t = -k$ is governed by $\det(I-X)^k$, and Lemma 5.1 below writes the ladder value $g_n(-k)$, through $j_n'(-k)$, as a sum over k partial derangements. For $m = 3$ there are two. (For $m = 2$ the Taylor expansion has one more term; this case is treated in Appendix A.)

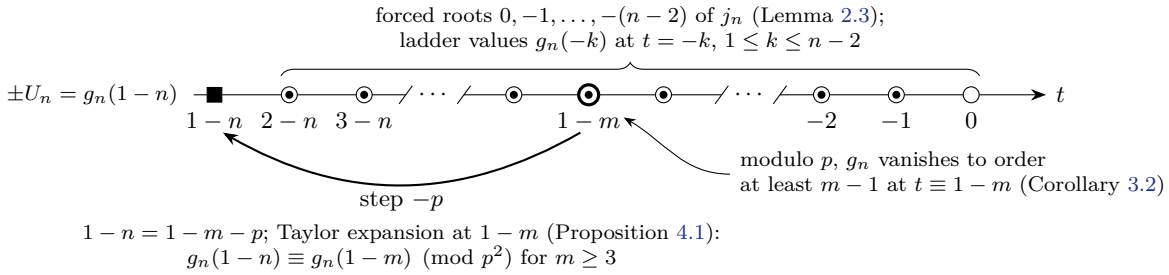

Figure 5: The ladder values of g_n for $n = p + m$ (schematic; rings mark the forced roots of j_n, dots the ladder values). Modulo p the points $1-n$ and $1-m$ coincide, and g_n vanishes there to order at least $m-1$; for $m \ge 3$ the Taylor expansion over the step of length p gives $g_n(1-n) \equiv g_n(1-m) \pmod{p^2}$.

5 Ladder values

This section computes $g_n(-2)$ in closed form (the simpler value $g_n(-1)$, needed only for $n = p+2$, is computed in Appendix A). The first two lemmas express a ladder value as a sum over k partial derangements of a determinant; they use only classical results. Lemma 5.3 expands the determinant into forests and is used for $k = 1$ in Appendix A. Lemma 5.4, an elementary sign cancellation, reduces these sums to a short list of configurations.

5.1 Ladder values as sums of determinants

For partial derangements $\sigma_1, \dots, \sigma_k$ that are pairwise arc-disjoint, let $F = \sigma_1 \cup \dots \cup \sigma_k$ and let d_v be the number of i with $v \in S_{\sigma_i}$, so that d_v is the out-degree (and the in-degree) of v in F. For a directed multigraph F on V let $L_F = D_F - A_F$ be its Laplacian, where D_F is the diagonal matrix of the out-degrees and A_F the adjacency matrix (with multiplicities), and for a directed graph G let $t(G)$ be the number of spanning arborescences of G oriented towards a fixed vertex. Put

$$\lambda(d) = \prod_{i=1}^{d} \frac{1}{n-1-i}, \qquad \text{so } \lambda(0) = 1,\ \lambda(1) = \frac{1}{n-2},\ \lambda(2) = \frac{1}{(n-2)(n-3)}.$$

Lemma 5.1. *Let $0 \le k \le n-2$. Then*

$$g_n(-k) = \frac{(-1)^k\,((n-2)!)^n}{n^2\,k!\,(n-2-k)!}\; S_n^{(k)}$$

with

$$S_n^{(k)} = \sum_{(\sigma_1,\dots,\sigma_k)} \prod_{i=1}^{k} (-1)^{c(\sigma_i)} \prod_{v \in V} \lambda(d_v)\, \det(nI - L_F),$$

where the sum runs over all k-tuples of pairwise arc-disjoint partial derangements of V.

Proof. Since $t = -k$ is a simple root of $t(t+1)\cdots(t+n-2)$, one has $g_n(-k) = j_n'(-k) / \prod_{i \ne k}(i-k)$, with i running over $0, \dots, n-2$, and $\prod_{i \ne k}(i-k) = (-1)^k k!\,(n-2-k)!$. In the ring R of Section 2, $\det(I-X)^{-t} = \exp(-t \log\det(I-X))$, so by the proof of Lemma 2.2, which gives $j_n(t) = [x^E] \exp(t \sum_H \mathrm{ec}(H) x^H)$,

$$j_n'(-k) = [x^E]\Big(\det(I-X)^k \cdot \sum_H \mathrm{ec}(H)\, x^H\Big).$$

Expanding the k factors by (2.2), a term survives if and only if the k partial derangements are pairwise arc-disjoint and the complement $E \setminus F$ is one of the sets H. The complement is Eulerian, and if it is not connected, its number of Eulerian circuits is 0. Hence $j'_n(-k) = \sum \prod_i (-1)^{c(\sigma_i)} \operatorname{ec}(K_n^* - F)$. Every vertex has out-degree $n-1-d_v \geq n-1-k \geq 1$ in $K_n^* - F$, and by the BEST theorem [29, Theorem 6 and (6.4)], $\operatorname{ec}(K_n^* - F) = t(K_n^* - F) \prod_v (n-2-d_v)!$, and $t(K_n^* - F)$ does not depend on the chosen vertex (it is 0 if $K_n^* - F$ is not connected, so the formula also covers that case). Finally $\prod_v (n-2-d_v)! = ((n-2)!)^n \prod_v \lambda(d_v)$, and Lemma 5.2 gives $t(K_n^* - F) = \det(nI - L_F)/n^2$. □

Lemma 5.2. *For every Eulerian graph $F \subseteq K_n^*$, $t(K_n^* - F) = \det(nI - L_F)/n^2$.*

Proof. Let $G = K_n^* - F$ and L_G its Laplacian. The Laplacian of K_n^* is $nI - J$, so $L_G = nI - J - L_F$. Since G is Eulerian, L_G has zero row sums and zero column sums. Hence $\det L_G = 0$, and $L_G \operatorname{adj}(L_G) = \operatorname{adj}(L_G) L_G = 0$. If L_G has rank $n-1$, its kernel and its left kernel are spanned by $\mathbf{1}$, so the columns and the rows of $\operatorname{adj}(L_G)$ are constant; otherwise $\operatorname{adj}(L_G) = 0$. In both cases all cofactors of L_G are equal. By the matrix-tree theorem for directed graphs [29, Theorem 7] the diagonal cofactors are $t(G)$, so the adjugate of L_G is $t(G)\, J$. With $J = \mathbf{1}\mathbf{1}^T$ the matrix determinant lemma, in the form $\det(A + \mathbf{u}\mathbf{v}^T) = \det A + \mathbf{v}^T \operatorname{adj}(A)\, \mathbf{u}$ valid for every square A, gives $\det(L_G + J) = 0 + \mathbf{1}^T \operatorname{adj}(L_G)\, \mathbf{1} = n^2\, t(G)$. Here $L_G + J = nI - L_F$. □

The determinant $\det(nI - L_F)$ couples the k partial derangements. For $k = 1$ the next lemma, a signed form of the matrix-forest theorem (see [7, (2)] for the general all-minors version), makes it a sum of local terms; for $k = 2$ the Leibniz formula is used instead (proof of Theorem 5.5). A *forest* in a directed multigraph F is a set Φ of arcs of F with at most one arc leaving each vertex and no directed cycle.

Lemma 5.3. *For every directed multigraph F on V without loops and every number c,*

$$\det(cI - L_F) = \sum_{\Phi} (-1)^{|\Phi|}\, c^{\,n-|\Phi|},$$

the sum over all forests Φ of F (parallel arcs are distinguished).

Proof. Row v of $cI - L_F$ is $ce_v - \sum_{(v,w)\in F} (e_v - e_w)$, where e_v is the unit row vector. Expanding the determinant by multilinearity in the rows, each vertex v chooses either ce_v or one arc (v,w) of F with the row $e_w - e_v$. The chosen arcs form a set Φ with at most one arc leaving each vertex. If Φ contains a directed cycle, the rows of its vertices sum to 0, and the determinant vanishes. Otherwise order the vertices so that every chosen arc points to an earlier vertex; then the matrix is triangular with diagonal entries c (unchosen vertices) and -1 (chosen vertices), and the determinant is $(-1)^{|\Phi|} c^{n-|\Phi|}$. □

5.2 Sign cancellation in sums over partial derangements

The following lemma is the source of all simplifications below. It evaluates a weighted sum over all partial derangements that contain a prescribed set of arcs, and it shows that the sum vanishes as soon as two paths are prescribed. Each vertex v carries two weights, $w_1(v)$ if the partial derangement moves v and $w_0(v)$ if it fixes v.

Lemma 5.4. *Let P be a set of arcs of K_n^* forming vertex-disjoint directed paths and cycles, with q paths, $c(P)$ cycles and vertex set $V(P)$, and let w_0, w_1 be weights on V. The sum*

$$\Lambda_w(P) := \sum_{\sigma \supseteq P} (-1)^{c(\sigma)} \prod_{v \in S_\sigma} w_1(v) \prod_{v \notin S_\sigma} w_0(v),$$

where σ runs over the partial derangements of V containing P, satisfies

$$\Lambda_w(P) = (-1)^{c(P)+q} \prod_{v \in V(P)} w_1(v) \cdot \begin{cases} \prod_{v \in R} \omega(v) - \sum_{u \in R} w_1(u) \prod_{v \in R \setminus \{u\}} \omega(v) & \text{if } q = 0, \\ \prod_{v \in R} \omega(v) & \text{if } q = 1, \\ 0 & \text{if } q \geq 2, \end{cases}$$

where $R = V \setminus V(P)$ and $\omega(v) = w_0(v) + w_1(v)$. If two arcs of a set P of arcs leave the same vertex or enter the same vertex, the sum over $\sigma \supseteq P$ is empty.

Proof. Every vertex of $V(P)$ lies in S_σ, and the cycles of P are cycles of σ. Contract each path of P, from its first vertex to its last, to a single element. Then σ corresponds to a permutation π of the set Y of the q contracted paths and the vertices outside $V(P)$: $\pi(y)$ is the element of Y that contains σ of the last vertex of y, and conversely σ is determined by π and P. A fixed point of π is a vertex outside S_σ, or a path closed into a cycle of σ. Each cycle of π that is not a fixed vertex corresponds to a cycle of σ. Give the elements of Y the weights $f(u) = w_1(u)$ for vertices and $f = 1$ for paths (the factors w_1 of the path vertices are taken out in front). Then $(-1)^{c(\sigma)} \prod_v w(v) = (-1)^{c(P)} \prod_{v \in V(P)} w_1(v) \prod_C \mathrm{wt}(C)$ over the cycles C of π, where the weight $\mathrm{wt}(C)$ is $-\prod_{y \in C} f(y)$, except for fixed points: a fixed vertex u has weight $w_0(u) = -w_1(u) + \omega(u)$, and a fixed path has weight -1. Hence the weight of every cycle is $-\prod_{y \in C} f(y)$ plus a correction $r(y)$ for fixed points, with $r(u) = \omega(u)$ for vertices and $r = 0$ for paths. Expanding the product of the corrections,

$$\Lambda_w(P) = (-1)^{c(P)} \prod_{v \in V(P)} w_1(v) \sum_{A \subseteq Y} \prod_{y \in A} r(y) \prod_{y \notin A} f(y) \sum_{\pi \in \mathrm{Sym}(Y \setminus A)} (-1)^{c(\pi)}.$$

Here $c(\pi)$ counts all cycles of π, fixed points included, so the inner sum is the value of $x(x+1)\cdots(x+N-1)$ at $x = -1$, that is, $(-1) \cdot 0 \cdot 1 \cdots (N-2)$ for $N = |Y \setminus A|$, that is, 1 for $N = 0$, -1 for $N = 1$ and 0 for $N \geq 2$. Paths have $r = 0$ and must lie outside A, so $q \geq 2$ gives 0. For $q = 1$ the only term is $Y \setminus A = \{\text{the path}\}$. For $q = 0$ one gets the term $A = Y$ and the terms with one vertex outside A. The last statement is clear, since a partial derangement has one arc leaving and one arc entering each moved vertex. □

It is convenient to read the bracket as a sum over *marks*. For $q = 0$ a layer may carry no mark or one mark on a vertex $u \notin V(P)$; for $q = 1$ it carries no mark. Every vertex then has a *layer factor*: $w_1(v)$ on $V(P)$, $\omega(v)$ off $V(P)$ and unmarked, and $-w_1(v)$ on the marked vertex. The bracket is the sum over the allowed marks of the product of the layer factors off $V(P)$. With this reading, each prescribed path costs a factor -1, and each layer carries at most one path or one mark.

For $k = 2$ the weight of a vertex depends on both partial derangements, and Lemma 5.4 is applied in the following form. A layer factor is a linear function of the pair $(w_0(v), w_1(v))$: write it as $\varphi_v(0)w_0(v) + \varphi_v(1)w_1(v)$, so that $\varphi_v = (0,1)$ on $V(P)$, $(1,1)$ off $V(P)$ and unmarked, and

$(0,-1)$ on the marked vertex. Let P, P' be two arc sets as in Lemma 5.4 and let $h_v(s,t)$, for $s,t\in\{0,1\}$, be numbers. Then

$$\sum_{\sigma\supseteq P,\ \tau\supseteq P'}(-1)^{c(\sigma)+c(\tau)}\prod_v h_v(s_v,t_v)=(-1)^{c(P)+q+c(P')+q'}\sum_{\mu,\mu'}\prod_v\psi_v, \tag{5.1}$$

with $\psi_v=\sum_{s,t\in\{0,1\}}\varphi_v(s)\,\varphi'_v(t)\,h_v(s,t)$, where $s_v=[v\in S_\sigma]$, $t_v=[v\in S_\tau]$, μ and μ' run over the allowed marks of the two layers, and φ, φ' are the coefficients of the layer factors of (P,μ) and (P',μ'). Indeed, both sides are linear in each of the functions h_v, so it suffices to take $h_v(s,t)=w_v(s)\,w'_v(t)$, and then the left side is $\Lambda_w(P)\,\Lambda_{w'}(P')$.

5.3 The value $g_n(-2)$

For $k=2$ Lemmas 5.1, 5.2 and 5.4 lead to a generating function. Put

$$a=\frac{1}{n-2},\quad \alpha=\frac{1}{n-3},\quad \beta=\frac{1}{(n-2)(n-3)},\quad x=\alpha z,\quad y=\beta z,$$

so that $\alpha=a+\beta=(n-2)\beta$.

Theorem 5.5. *For $n\ge 4$,*

$$g_n(-2)=\frac{((n-2)!)^n}{2n^2(n-4)!}\,S_n,\qquad S_n=n!\,[z^n]\,e^{\frac{n(n-1)}{n-3}z}\,\frac{1-2y}{(1+x)^3}\,\mathcal{D}(z),$$

where

$$\begin{aligned}
&\mathcal{D}=(1+M+M'+C)^2+J,\\
&M=-nx+(n-1)y,\qquad M'=-\frac{xy}{1+x},\qquad C=\frac{2y^2}{(1+x)(1-2y)},\\
&J=x-\frac{y^2}{(1+x)^2(1-2y)^2}-\frac{x^2}{1+x}.
\end{aligned}$$

In the proof the determinant is expanded by the Leibniz formula; with the common arcs of σ and τ this gives disjoint cycles and paths on V, and each term of $\mathcal{D}$ is the contribution of one kind of these components.

Proof. By Lemma 5.1, $S_n=S_n^{(2)}$ is the sum over arc-disjoint pairs (σ,τ) of the terms

$$(-1)^{c(\sigma)+c(\tau)}\prod_v\lambda(d_v)\det(nI-L_F),\qquad F=\sigma\cup\tau.$$

Step 1: the Leibniz expansion. For arc-disjoint σ,τ, the matrix $nI-L_F$ has the diagonal entries $n-d_v$ and the off-diagonal entries $[\sigma(v)=w]+[\tau(v)=w]$. By the Leibniz formula, $\det(nI-L_F)=\sum_\pi\operatorname{sgn}\pi\prod_v(nI-L_F)_{v,\pi(v)}$, the sum over all permutations π of V. For a vertex moved by π, expand the factor $[\sigma(v)=\pi(v)]+[\tau(v)=\pi(v)]$ by choosing whether the arc $(v,\pi(v))$ is used by σ or by τ; let $B\subseteq S_\pi$ be the set of vertices whose π-arc is used by σ. Put $s_v=[v\in S_\sigma]$ and $t_v=[v\in S_\tau]$, so $d_v=s_v+t_v$, and

$$h_v(s,t)=\lambda(s+t)\,(n-s-t)\quad\text{if }\pi(v)=v,\qquad h_v(s,t)=\lambda(s+t)\quad\text{if }\pi(v)\ne v.$$

Step 2: disjointness. Write $\pi|_X$ for the set of arcs $(v, \pi(v))$, $v \in X$. For all pairs (σ, τ) define

$$T(\sigma,\tau) = (-1)^{c(\sigma)+c(\tau)} \sum_{\pi,B} \operatorname{sgn}\pi \prod_v h_v(s_v, t_v),$$

the sum over the pairs (π, B) with $\pi|_B \subseteq \sigma$ and $\pi|_{S_\pi \setminus B} \subseteq \tau$; for arc-disjoint pairs $T(\sigma,\tau)$ is the term of S_n. Multiply it by $\sum_E (-1)^{|E|}$ over the sets E of arcs common to σ and τ; this factor is 1 if the pair is arc-disjoint and 0 otherwise. Exchanging the order of summation,

$$S_n = \sum_{E,\pi,B} (-1)^{|E|} \operatorname{sgn}\pi \sum_{\sigma \supseteq P_\sigma,\ \tau \supseteq P_\tau} (-1)^{c(\sigma)+c(\tau)} \prod_v h_v(s_v, t_v),$$

where $P_\sigma = E \cup \pi|_B$ and $P_\tau = E \cup \pi|_{S_\pi \setminus B}$.

Step 3: the common arcs. If an arc of E has an end in S_π and is not an arc of π, then P_σ or P_τ has two arcs leaving or entering the same vertex, and the inner sum is empty by Lemma 5.4. Hence $E = \pi|_D \cup E_0$, where $D \subseteq S_\pi$ and E_0 is a set of arcs between fixed points of π, and E determines (D, E_0); for the inner sum not to vanish, E_0 consists of vertex-disjoint paths and cycles, and then so do P_σ and P_τ, since the arcs of π form disjoint cycles on S_π. For $v \in D$ the arc $(v, \pi(v))$ lies in P_σ and in P_τ whether or not $v \in B$, so the two choices give the same term: a factor 2 for each $v \in D$.

Local weights. By (5.1), the inner sum is $(-1)^{c(P_\sigma)+q_\sigma+c(P_\tau)+q_\tau}$ times a sum over marks of $\prod_v \psi_v$. Call the *status* of a vertex in a layer A (in $V(P)$), N (outside $V(P)$, unmarked) or K (marked). The vertex factors h_v take the values $h_v(0,0) = n$, $h_v(1,0) = h_v(0,1) = a(n-1)$, $h_v(1,1) = \alpha$ if $\pi(v) = v$, and 1, a, β if $\pi(v) \neq v$. A vertex moved by π lies in $V(P_\sigma)$ or in $V(P_\tau)$, since its π-arc lies in one of them, and a vertex fixed by π lies in both or in neither. With $\alpha = a + \beta$ one gets the local factors

vertex	statuses in the two layers	ψ_v
fixed by π	(N,N)	$n + 2a(n-1) + \alpha$
fixed by π	(K,N) or (N,K)	$-(a(n-1)+\alpha)$
fixed by π	(K,K) or (A,A)	α
moved by π	(A,A)	β
moved by π	(A,N) or (N,A)	α
moved by π	(A,K) or (K,A)	$-\beta$

Altogether,

$$S_n = \sum_{\pi,B,D,E_0} \operatorname{sgn}\pi\, (-2)^{|D|} (-1)^{|E_0|} (-1)^{c(P_\sigma)+q_\sigma+c(P_\tau)+q_\tau} \sum_{\mu_\sigma,\mu_\tau} \prod_v \psi_v, \tag{5.2}$$

where B now runs over the subsets of $S_\pi \setminus D$.

The exponential formula. The cycles of π and the components of E_0 (paths, cycles and isolated vertices fixed by π) partition V, and the summand of (5.2) is a product over these components, except for the condition that each layer carries in total at most one path start or mark. Introduce variables ε and ε' with $\varepsilon^2 = \varepsilon'^2 = 0$, and give each path start and each mark of the layer of σ the factor ε, and those of τ the factor ε'. Then (5.2) is the sum of the coefficients of 1, ε, ε', $\varepsilon\varepsilon'$ in the unrestricted sum. A configuration $(\pi, B, D, E_0, \mu_\sigma, \mu_\tau)$ is the same as a set partition of V together with one connected structure on each block, and its weight is the product of the weights of the structures. Giving each vertex the factor z, the exponential formula for

labelled structures, which holds for weights in any commutative $\mathbb{Q}$-algebra, shows that $S_n/n!$ is the coefficient of z^n in

$$\exp(F + (\varepsilon + \varepsilon')\Gamma + \varepsilon\varepsilon' J) = e^F(1 + (\varepsilon + \varepsilon')\Gamma + \varepsilon\varepsilon'(\Gamma^2 + J)),$$

where F, $\varepsilon\Gamma$ and $\varepsilon\varepsilon' J$ are the exponential generating functions of the components without path start and mark, with the path start or the mark of the layer of σ only, and with both (by the symmetry between σ and τ, the components of the layer of τ give $\varepsilon'\Gamma$). The sum of the four coefficients is $e^F((1+\Gamma)^2 + J)$. Section 5.4 lists the components and shows that $e^F = e^{n(n-1)z/(n-3)}(1-2y)/(1+x)^3$, $\Gamma = M + M' + C$ and that J is as stated. □

I checked the theorem independently: it gives the values

$$g_4(-2) = 24, \quad g_5(-2) = 23976, \quad g_6(-2) = 1185546240, \quad g_7(-2) = 4575483936000000,$$

which agree with the polynomials g_n computed by a transfer-matrix method for $n \le 10$ and with a direct evaluation of the sum in Lemma 5.1 over all pairs (σ, τ) for $n \le 12$ (Section 8). The direct evaluation does not use Lemma 5.4 or the classification.

5.4 The components in the proof of Theorem 5.5

This subsection completes the proof of Theorem 5.5. Each vertex carries the factor z, so a vertex with local factor α or β contributes x or y. On a cycle of π of length l, write the letter σ at a vertex $v \in B$, the letter τ at $v \in S_\pi \setminus (B \cup D)$ and the letter b at $v \in D$; reading the letters along the cycle gives a cyclic word. The arcs of P_σ on the cycle are those at the letters σ and b, and those of P_τ are at τ and b. Hence the cycle is a cycle of P_σ if it has no letter τ, and otherwise each maximal block of letters σ and b is a path of P_σ; similarly for τ. A vertex of the cycle lies in $V(P_\sigma)$ if its own letter or the letter of its predecessor is σ or b. The signs are $(-1)^{l-1}$ from $\operatorname{sgn}\pi$, -2 for each letter b, -1 for each cycle of P_σ or P_τ, -1 for each path and -1 for each arc of E_0. A connected structure on l labelled vertices contributes its weight divided by $l!$ to the exponential generating function. A cycle of length l has $(l-1)!$ cyclic orders of its vertices; a cyclic word without rotational symmetry can be placed in l ways, so it has $l!$ labelled versions, and a word with all letters equal has $(l-1)!$. A non-constant word with a rotational symmetry repeats each of its blocks, so it carries two paths of one layer and contributes 0; the surviving non-constant words below have no rotational symmetry. A path of E_0 on $k+1$ vertices has $(k+1)!$ labelled versions.

Components without path start and mark. A cycle of π that contains both letters σ and τ carries a path of each layer, and a cycle with letters σ and b only, both present, carries a path of τ. The components without path start and mark are:

- a vertex fixed by π outside E_0, statuses (N,N): $(n + 2a(n-1) + \alpha)z$;
- a cycle of π with all letters σ (or all τ): a cycle of P_σ, statuses (A,N), weight $(-1)^{l-1}(-1)\alpha^l$, so $\sum_{l\ge2}(-x)^l/l$ each;
- a cycle of π with all letters b: a cycle of both layers, statuses (A,A), weight $(-1)^{l-1}(-2)^l\beta^l$, so $-\sum_{l\ge2}(2y)^l/l$;
- a cycle of E_0 of length $l \ge 2$: statuses (A,A) at fixed points, weight $(-1)^l\alpha^l$, so $\sum_{l\ge2}(-x)^l/l$.

Hence

$$e^F = \exp\Big((n + 2a(n-1) + \alpha)z + 3\sum_{l\ge 2}\frac{(-x)^l}{l} - \sum_{l\ge 2}\frac{(2y)^l}{l}\Big) = e^{(n+2a(n-1)+4\alpha+2\beta)z}\,\frac{1-2y}{(1+x)^3}$$

and $n + 2a(n-1) + 4\alpha + 2\beta = n(n-1)/(n-3)$.

Components with the path start or the mark of one layer. Take the layer of σ. A mark of σ sits on a vertex outside $V(P_\sigma)$, that is, on a vertex fixed by π outside E_0, or on a cycle of π with all letters τ: a mark is only allowed when the layer has no path, and a cycle with a letter σ or b either lies in $V(P_\sigma)$ or carries a path of σ. A path of σ alone lies on a cycle of π with letters τ and b only. This gives three kinds:

- a marked fixed vertex, statuses (K, N): $-(a(n-1)+\alpha)z = -nx + (n-1)y = M$;
- a cycle τ^l with one marked vertex: the mark replaces one factor α by $-\beta$, with l choices of the vertex; the signs are $(-1)^{l-1}$, -1 for the cycle of P_τ and -1 from $-\beta$, so $\sum_{l\ge 2}(-1)^{l-1}\alpha^{l-1}\beta z^l = \sum_{l\ge 2} y(-x)^{l-1} = M'$;
- a cycle $\tau^c\mathsf{b}^i$ $(i, c \ge 1)$: a cycle of P_τ whose b-block is the path of σ. The $i+1$ vertices of this path lie in both $V(P)$, the other $c-1$ vertices only in $V(P_\tau)$. The signs are $(-1)^{i+c-1}$, $(-2)^i$, -1 for the cycle and -1 for the path, so the contribution is $\sum_{i,c\ge 1}(-1)^{c-1}2^i\beta^{i+1}\alpha^{c-1}z^{i+c} = \sum_{i,c\ge 1} y(2y)^i(-x)^{c-1} = C$.

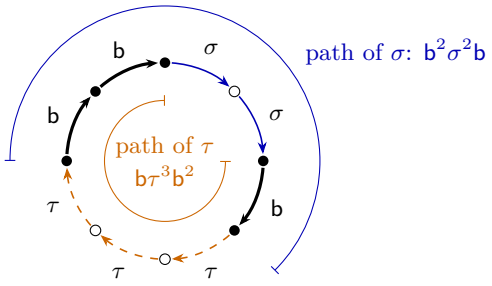

Figure 6: A cycle of π with the word $\sigma^2\mathsf{b}\,\tau^3\mathsf{b}^2$ ($a = 2$, $i = 1$, $c = 3$, $j = 2$), read clockwise; each arc carries the letter of its tail. The arcs with letters σ and b form the path of σ, those with letters τ and b the path of τ. The $i + j + 2 = 5$ filled vertices lie on both paths, the other $a + c - 2 = 3$ on one.

Components with both layers. A component carries a path start or mark of each layer in three ways:

- a fixed vertex outside E_0 with both marks, statuses (K, K): $\alpha z = x$;
- a cycle of π with both letters σ and τ. Its maximal blocks of letters σ and b are paths of σ, and there is only one; so all letters σ lie in one such block, and so do all letters τ in one block of letters τ and b. A block of letters b between two letters σ would be a second path of τ, and symmetrically, so the letters σ, and the letters τ, are contiguous. Hence the word is $\sigma^a\mathsf{b}^i\tau^c\mathsf{b}^j$ with $a, c \ge 1$, $i, j \ge 0$ (Figure 6). The paths are the blocks

$\mathsf{b}^j\sigma^a\mathsf{b}^i$ and $\mathsf{b}^i\tau^c\mathsf{b}^j$, so $i+j+2$ vertices lie in both $V(P)$ and $a+c-2$ in one. The signs are $(-1)^{a+i+c+j-1}$, $(-2)^{i+j}$ and $(-1)^2$ for the two paths, so the contribution is $\sum(-1)^{a+c-1}2^{i+j}\beta^{i+j+2}\alpha^{a+c-2}z^{a+i+c+j} = -y^2/((1+x)^2(1-2y)^2)$;

- a path of E_0 with $k \geq 1$ arcs: a path of both layers on $k+1$ fixed points of π, statuses (A,A), signs $(-1)^k$ and $(-1)^2$, so $\sum_{k\geq 1} x(-x)^k = -x^2/(1+x)$.

The sum is J. A component cannot carry two path starts or marks of the same layer, and the components above exhaust the cycles of π (by their words), the components of E_0 (isolated vertices, cycles, paths) and the possible positions of marks. This completes the proof of Theorem 5.5.

6 The second digit modulo p

This section reduces the formula of Section 5 modulo p^2 for $n = p+3$ (the case $n = p+2$ is in Appendix A). The falling factorials in the coefficient extraction contribute exactly one factor p for all but a few indices, and Fermat's and Wilson's theorems turn the remaining sum into a factorial sum. For a prime p and an integer c prime to p put

$$K_c(p) = \sum_{j=0}^{p-1} j!\, c^{-j} \pmod p.$$

By Wilson's theorem, $j!\,(p-1-j)! \equiv (-1)^{j+1}$, so $K_c(p) \equiv -\sum_{i<p}(-c)^i/i!$, and since $(p-1)!\sum_{i\leq p-1}(y-1)^i/i!$ is the sum of $y^{\mathrm{fix}(\pi)}$ over $\pi \in S_{p-1}$, one also has

$$K_c(p) \equiv \sum_{\pi\in S_{p-1}} (1-c)^{\mathrm{fix}(\pi)} \pmod p.$$

For $c = 1$ this is Kurepa's left factorial $!p$ [21].

Theorem 6.1. *For every prime $p \geq 5$, $g_{p+3}(-2) \equiv 6p\,(4K_6(p) - 5) \pmod{p^2}$.*

Proof. Let $n = p+3$; then $a = 1/(p+1)$, $\alpha = 1/p$, $\beta = 1/(p(p+1))$, and the exponent in Theorem 5.5 is cz with $c = (p+2)(p+3)/p$. Let $H(z) = (1-2y)\,\mathcal{D}(z)/(1+x)^3$ and $h_j = [z^j]H$, so that $S_n = \sum_{j=0}^{n}(n)_j\, c^{n-j}h_j$. Substitute $z = p\,w$. Then $x = w$, $y = w/(p+1)$ and $n = p+3$, so $H(pw)$ is a power series in w whose coefficients $\eta_j = p^j h_j$ are, after expanding $1/(1+w)$ and $1/(1-2w/(p+1))$, polynomials with integer coefficients in p and $1/(p+1)$; in particular they are p-integral, and reducing modulo p amounts to setting $p = 0$, so $\eta_j \equiv \eta_j^{(0)} \pmod p$, where $\eta_j^{(0)}$ are the coefficients of the series $H_0(w)$ obtained by setting $p = 0$. A direct simplification of the formulas of Theorem 5.5 with $x = w$, $y = w$, $n = 3$ (the values at $p = 0$) gives

$$H_0(w) = -\frac{(2w-1)(4w^3+1)}{(1+w)^4} = -8 + \frac{36}{1+w} - \frac{60}{(1+w)^2} + \frac{42}{(1+w)^3} - \frac{9}{(1+w)^4};$$

the pole at $w = 1/2$ cancels. Now

$$S_n = p^{-n}\Sigma, \qquad \Sigma = \sum_{j=0}^{n}(n)_j\,\big((p+2)(p+3)\big)^{n-j}\eta_j,$$

and by Theorem 5.5, $g_n(-2) = (p+1)^{p+3}((p-1)!)^{p+2}\,\Sigma/(2(p+3)^2)$, where the factor in front of Σ is a p-adic unit (as $p \nmid 18$) and, by Wilson's theorem and since $p+2$ is odd, is $\equiv -1/18 \pmod p$.

For $j \geq 4$ the falling factorial $(n)_j = (p+3)(p+2)(p+1)p(p-1)\cdots(p+4-j)$ contains exactly one factor p, with quotient $\equiv 6(-1)^{j-4}(j-4)! \pmod p$, and $((p+2)(p+3))^{n-j} \equiv 6^{4-j}$. From the partial fractions, $\eta_j^{(0)} = (-1)^j q(j)$ for $j \geq 1$, with $q(j) = 36 - 60(j+1) + 21(j+1)(j+2) - \frac{3}{2}(j+1)(j+2)(j+3)$. Writing $i = j-4$,

$$\frac{1}{p}\sum_{j\geq 4}(n)_j((p+2)(p+3))^{n-j}\eta_j \equiv 6\sum_{i=0}^{p-1} i!\,6^{-i}\,q(i+4) \pmod p.$$

Here $q(i+4) = 36+18(i+1)+3(i+1)(i+2)-\frac{3}{2}(i+1)(i+2)(i+3)$, and $\sum_{i<p} i!\,6^{-i}(i+1)\cdots(i+r) \equiv 6^r\,(K_6(p) - \sum_{l<r} l!\,6^{-l})$, since the terms with $i+r \geq p$ vanish. This evaluates the sum to $6(-72K_6(p)+162) = -432K_6(p)+972$.

For $j \leq 3$ the factors are units. Using $\eta_0 = 1$, $\eta_1 = -2(p+3)$, $\eta_2 = (p+3)(p^2+8p+6)/(p+1)$, $\eta_3 = -(p+3)(p+6)(3p+2)/(p+1)$ and $((p+2)(p+3))^{n-j} \equiv 6^{p-1}\,6^{4-j}(1+\frac{5}{6}(3-j)p) \pmod{p^2}$ (since $(p+2)(p+3) = 6(1+\frac{5}{6}p+\frac{1}{6}p^2)$ and $n-j = p+3-j$), the four terms are, up to the common factor 6^{p-1} and modulo p^2,

$$(1296+3240p) + (-3888-9072p) + (3888+9072p) + (-1296-3672p) = -432p.$$

Since this is divisible by p, the factor $6^{p-1} \equiv 1 \pmod p$ may be dropped. Altogether $\Sigma/p \equiv -432-432K_6(p)+972 = 540-432K_6(p)$, and $g_n(-2)/p \equiv -\frac{1}{18}(540-432K_6(p)) = 24K_6(p)-30 = 6(4K_6(p)-5) \pmod p$. □

Proof of Theorem 1.1. For $n = p+3$, Proposition 4.1 and Theorem 6.1 give $g_n(1-n) \equiv 6p(4K_6(p)-5) \pmod{p^2}$, and $U_n = -g_n(1-n)$ by Lemma 2.4, since n is even. This is the congruence of Theorem 1.1, and $D_n = n!(n-1)!\,U_n$ by Lemma 2.4(3). Since $v_p(n!(n-1)!) = 2$ (Section 4) and $p \nmid 6$, the condition $4K_6(p) \not\equiv 5$ gives $v_p(D_n) = 3$; in particular $D_n \neq 0$, and $L_n^e \neq L_n^o$ by Janssen's identity. □

As a check, $p = 5$ gives $K_6(5) \equiv \sum_{j<5} j! = 34 \equiv 4$ and $4K_6(5) - 5 \equiv 1$, so $v_5(U_8) = 1$; and $p = 7$ gives $K_6(7) \equiv \sum_{j<7}(-1)^j j! = 620 \equiv 4$ and $4K_6(7) - 5 \equiv 4$, so $v_7(U_{10}) = 1$. Both agree with the values $U_8 = 6210846720 = 2^{17}\cdot 3^6 \cdot 5 \cdot 13$ and $U_{10} = -27369126116720640000$, which is divisible by 7 exactly once.

7 Full layers and the orders 94 and 118

For $n = p+m$ with $m \geq 3$, Proposition 4.1 moves the second p-adic digit to the ladder value $g_n(-k)$ with $k = m-1$, and Lemma 5.1 writes it as a sum over k partial derangements. Section 5 evaluated this sum for $k \leq 2$ by a classification of configurations, which becomes unmanageable for larger k. This section shows that modulo p^2 the sum has a much simpler structure: only tuples of derangements that move every vertex contribute, and their sum is a signed count of Latin rectangles. For even k this count is a pairing of two powers in an algebra with commuting and anticommuting variables (Theorem 7.4). For $k = 4$, that is $n = p+5$, I evaluated the pairing by computer, and this settles the orders $94 = 89+5$ and $118 = 113+5$.

7.1 Reduction to full layers

For $k \geq 0$, $N \geq 0$ and an integer a let

$$A_k(N,a) = \sum_{(\sigma_1,\dots,\sigma_k)} \prod_{i=1}^{k} (-1)^{c(\sigma_i)} \det(aI + P_{\sigma_1} + \cdots + P_{\sigma_k}),$$

where the sum runs over the k-tuples of pairwise arc-disjoint derangements of $[N]$ (each σ_i moves every vertex) and P_σ is the permutation matrix of σ; $A_k(0,a) = 1$ and $A_0(N,a) = a^N$. The determinants are polynomials in a with integer coefficients, so $A_k(N,a) \in \mathbb{Z}[a]$.

Lemma 7.1. *Let p be a prime, $1 \leq m < p$, $n = p + m$ and $k = m - 1$. Then*

$$g_n(-k) \equiv \frac{(-1)^k\,((p-1)!)^{n-1}}{n^2\,k!}\, A_k(n, p+1) \pmod{p^2}.$$

Proof. By the proof of Lemma 5.1, with $n - 2 - k = p - 1$,

$$g_n(-k) = \frac{(-1)^k}{k!\,(p-1)!} \sum_{(\sigma_1,\dots,\sigma_k)} w(\sigma_1,\dots,\sigma_k), \qquad w = \prod_i (-1)^{c(\sigma_i)}\, t(K_n^* - F) \prod_v (n-2-d_v)!,$$

where $t(K_n^* - F) = \det(nI - L_F)/n^2$ is an integer by Lemma 5.2. Call a vertex *full* if $d_v = k$. For a full vertex, $(n-2-d_v)! = (p-1)!$ is prime to p. For $d_v < k$ one has $p \leq n-2-d_v \leq p+k-1 < 2p$, so $(n-2-d_v)!$ is divisible by p. Hence tuples with two or more vertices that are not full contribute 0 modulo p^2.

Fix a vertex u and let T_u be the set of tuples in which u is the only vertex that is not full. The weight w is invariant under relabelling the vertices, and a relabelling that fixes u maps T_u to itself, and w/p is an integer on T_u. Let Z be a set of p vertices not containing u (possible since $n - 1 \geq p$), ρ a cyclic permutation of Z fixing $W = [n] \setminus Z$ pointwise, and let ρ act on T_u by conjugation. Orbits have length 1 or p, so $\sum_{T_u} w/p$ is congruent modulo p to the sum over the fixed tuples. Suppose $\rho\sigma_i\rho^{-1} = \sigma_i$ for all i. For $v \in W$, $\sigma_i(v) = \sigma_i(\rho v) = \rho\,\sigma_i(v)$, so σ_i maps $W \cap S_{\sigma_i}$ into W. Now $|W| = n - p = k + 1$. Every $v \in W \setminus \{u\}$ is full, so $\sigma_1(v), \dots, \sigma_k(v)$ are k distinct elements of $W \setminus \{v\}$, which has k elements; hence $\sigma_i(v) = u$ for exactly one i. Since each σ_i is injective, the k vertices of $W \setminus \{u\}$ use k different indices i. Hence u is in the image of every σ_i, at some $v \neq u$, so every σ_i moves u and $d_u = k$, a contradiction. There are no fixed tuples, and the tuples in T_u contribute 0 modulo p^2.

It remains to sum over the tuples in which all vertices are full, that is, over k-tuples of pairwise arc-disjoint derangements of $[n]$. For these $D_F = kI$, so $nI - L_F = (n-k)I + A_F = (p+1)I + A_F$ with $A_F = P_{\sigma_1} + \cdots + P_{\sigma_k}$, and $\prod_v (n-2-d_v)! = ((p-1)!)^n$. This gives the formula. □

For full derangements $(-1)^{c(\sigma)} = (-1)^N \operatorname{sgn}\sigma$, so for even k the sign in $A_k(N,a)$ is $\prod_i \operatorname{sgn}\sigma_i$. In this case the sum has a symmetric form. For $N \geq 0$ and $k \geq 0$ let $S_k(N)$ be the sum of $\prod_{i=0}^{k+1} \operatorname{sgn}\pi_i$ over the tuples $(\pi_0, \pi_1, \dots, \pi_{k+1})$ of permutations of $[N]$ such that for every $v \in [N]$ the values $\pi_1(v), \dots, \pi_{k+1}(v)$ are distinct and $\pi_0(v)$ is one of them. In other words, $(\pi_1, \dots, \pi_{k+1})$ are the rows of a $(k+1) \times N$ Latin rectangle (written columnwise), and π_0 is a permutation contained in its support. Figure 7 shows an example with $k = 2$ and $N = 4$.

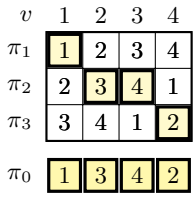

Figure 7: A Latin rectangle with rows π_1, π_2, π_3 and $N = 4$ columns, and a permutation π_0 with $\pi_0(v) \in \{\pi_1(v), \pi_2(v), \pi_3(v)\}$ for every v (highlighted cells); the tuple $(\pi_0, \dots, \pi_3)$ is one of the tuples counted by $S_2(4)$.

Lemma 7.2. *Let k be even and $N \geq 0$.*

1. $N!\, A_k(N, 1) = S_k(N)$.
2. $\frac{\partial}{\partial a} A_k(N, a)\big|_{a=1} = \frac{N}{k+1}\, A_k(N, 1)$.
3. $A_k(k+2, 1) = -(k+1)\, D_{k+2}/(k+2)!$.

Proof. (1) The matrix $I + P_{\sigma_1} + \cdots + P_{\sigma_k}$ is a $(0,1)$-matrix, so its determinant is the sum of $\operatorname{sgn}\pi_0$ over the permutations π_0 with $\pi_0(v) \in \{v, \sigma_1(v), \dots, \sigma_k(v)\}$ for all v. With $\pi_1 = \mathrm{id}$ and $\pi_{i+1} = \sigma_i$ the summands of $A_k(N, 1)$ are exactly the summands of $S_k(N)$ with $\pi_1 = \mathrm{id}$, since the values $v, \sigma_1(v), \dots, \sigma_k(v)$ are distinct for all v exactly when the σ_i are pairwise arc-disjoint derangements. For an arbitrary tuple in $S_k(N)$, replacing every π_i by $\pi_i \pi_1^{-1}$ gives a tuple with $\pi_1 = \mathrm{id}$ (the condition at v becomes the condition at $\pi_1(v)$) and multiplies the sign by $(\operatorname{sgn}\pi_1)^{k+2} = 1$. This is a bijection between the tuples with a given π_1 and those with $\pi_1 = \mathrm{id}$, for each of the $N!$ permutations π_1.

(2) Here $M = P_{\sigma_1} + \cdots + P_{\sigma_k}$ has zero diagonal. Differentiating

$$\det(aI + M) = \sum_{\pi} \operatorname{sgn}\pi \prod_{v} (a[\pi(v) = v] + M_{v,\pi(v)})$$

at $a = 1$ gives the sum of $\operatorname{sgn}\pi_0$ times the number of fixed points of π_0. Under the bijection of (1), the fixed points of $\pi_0\pi_1^{-1}$ correspond to the vertices v with $\pi_0(v) = \pi_1(v)$. Hence $N!\, \partial_a A_k(N, 1)$ is the signed sum of N_1 over the tuples of $S_k(N)$, where N_i is the number of v with $\pi_0(v) = \pi_i(v)$. Exchanging π_1 and π_i is a sign-preserving bijection on these tuples, so the signed sums of $N_1, \dots, N_{k+1}$ agree, and $N_1 + \cdots + N_{k+1} = N$ for every tuple.

(3) For $N = k+2$, for every v one of the N values is missing among $\pi_1(v), \dots, \pi_{k+1}(v)$; call it $\pi_{k+2}(v)$. Every value is taken exactly once by each of $\pi_1, \dots, \pi_{k+1}$, hence missed for exactly one v, so π_{k+2} is a permutation and $(\pi_1, \dots, \pi_{k+2})$ is a Latin square of order $k+2$ in the sense of Section 2. The sum over π_0 is $\det(J - P_{\pi_{k+2}}) = \det(J - I)\operatorname{sgn}\pi_{k+2} = -(k+1)\operatorname{sgn}\pi_{k+2}$. Hence $S_k(k+2) = -(k+1)D_{k+2}$, and (1) gives the claim. □

Corollary 7.3. *Let p be a prime, m odd with $3 \leq m < p$, $n = p + m$, and $A = A_{m-1}(n, 1)$. Then $p \mid A$ and*

$$\frac{U_n}{p} \equiv \frac{1}{m^2(m-1)!}\,\frac{A}{p}, \qquad \frac{D_n}{p^3} \equiv \frac{(m-1)!}{m}\,\frac{A}{p} \pmod{p}.$$

In particular, if $A \not\equiv 0 \pmod{p^2}$, then D_n is divisible by exactly p^3 and the Alon–Tarsi conjecture holds for n.

Proof. Let $k = m-1$, which is even. Since $A_k(n,a) \in \mathbb{Z}[a]$, Lemma 7.2(2) gives $A_k(n,p+1) \equiv A\,(1+pn/m) \pmod{p^2}$, and n/m is p-integral. By Corollary 3.2, $g_n(-k) \equiv 0 \pmod{p}$, so Lemma 7.1 gives $p \mid A$ and then $A_k(n,p+1) \equiv A \pmod{p^2}$. Modulo p the factor in Lemma 7.1 is $-1/(m^2(m-1)!)$, by Wilson's theorem and since $n-1$ is odd. With $U_n = -g_n(1-n) \equiv -g_n(-k) \pmod{p^2}$ (Lemma 2.4 and Proposition 4.1) this gives the first congruence. Finally $n!/p \equiv -m!$ and $(n-1)!/p \equiv -(m-1)!$ modulo p, and $D_n = n!\,(n-1)!\,U_n$. □

For $m = 3$, the corollary and Theorem 1.1 give $A_2(p+3,1)/p \equiv -108\,(4K_6(p) - 5) \pmod{p}$, a congruence for a signed count of Latin rectangles with three rows.

7.2 A pairing formula

Let $k \geq 0$, $q = k+2$, and let $\mathcal{I} = \{0, 1, \ldots, k+1\}$ be the set of indices of the permutations $\pi_0, \ldots, \pi_{k+1}$ in $S_k(N)$. For every nonempty $B \subseteq \mathcal{I}$ take a variable z_B: if $|B|$ is even, $z_B = y_B$ is an ordinary (commuting) variable; if $|B|$ is odd, $z_B = \theta_B$ is a Grassmann variable, so that $\theta_B\theta_C = -\theta_C\theta_B$ and $\theta_B^2 = 0$, and the y_B commute with everything. Fix a total order of the nonempty subsets of $\mathcal{I}$. For a set partition τ of $\mathcal{I}$ let z^τ be the product of the variables of its blocks in this order, let $\varepsilon(\tau)$ be the sign of the permutation of $\mathcal{I}$ obtained by writing the blocks of τ in this order, each block in increasing order, and let $\mu(\tau) = \prod_{B\in\tau}(-1)^{|B|-1}(|B|-1)!$ be the Möbius function of the partition lattice (see [12, p. 80] for this product formula) from the partition into singletons to τ. Put

$$P = -\sum_{\tau:\ \{0\}\notin\tau} \mu(\tau)\,\varepsilon(\tau)\,z^\tau, \qquad Q = \sum_{\tau} \varepsilon(\tau)\,z^\tau,$$

the first sum over the partitions in which 0 is not a singleton. If q is even, every partition of $\mathcal{I}$ has an even number of odd blocks, so all monomials of P and Q commute with each other; for odd q this fails, and P^N, Q^N are the powers in the (noncommutative) algebra. In the application in Section 7.3, $k = 4$ and $q = 6$ is even. The algebra is the tensor product of $\mathbb{Z}[y_B]$ with the exterior algebra over $\mathbb{Z}$ on the θ_B, so the normal monomials below form a $\mathbb{Z}$-basis. Every product of variables is 0 or $\pm$ a *normal monomial* $y^\alpha\theta_{\mathcal{J}}$, where $\mathcal{J}$ is a set of odd blocks and $\theta_{\mathcal{J}}$ is the product of its variables in increasing order. Define a bilinear pairing by

$$\langle y^\alpha\theta_{\mathcal{J}},\, y^\beta\theta_{\mathcal{J}'}\rangle = [\alpha=\beta]\,[\mathcal{J}=\mathcal{J}']\prod_B \alpha_B!.$$

On the commuting variables this is the Fischer inner product $\langle f, g\rangle = f(\partial)\,g\,|_{y=0}$.

Theorem 7.4. *For every $k \geq 0$ and $N \geq 0$, $S_k(N) = \langle P^N, Q^N\rangle$. For even k, hence, $A_k(N,1) = \langle P^N, Q^N\rangle/N!$.*

Proof. Step 1: rows. For a tuple $\pi = (\pi_0, \ldots, \pi_{k+1})$ and a vertex v, let $\tau_v(\pi)$ be the partition of $\mathcal{I}$ into the classes of equal values $\pi_i(v)$. The condition on row v in $S_k(N)$ is $f(\tau_v(\pi)) = 1$, where $f(\tau) = 1$ if the indices $1, \ldots, k+1$ lie in different blocks of τ and 0 is not a singleton, and $f(\tau) = 0$ otherwise. Write $\tau' \leq \tau$ if τ' refines τ, and $\hat{0}$ for the partition into singletons. If $1, \ldots, k+1$ lie in different blocks, then either 0 shares its block with exactly one of them or $\tau = \hat{0}$; so $f = h - \delta$ with $h(\tau) = [1, \ldots, k+1 \text{ in different blocks}]$ and $\delta(\tau) = [\tau = \hat{0}]$. I claim that $f(\tau) = \sum_{\tau'\leq\tau} g(\tau')$ with

$$g(\tau') = -\mu(\tau')\,[\{0\} \notin \tau'].$$

Indeed $\sum_{\tau' \le \tau} \mu(\tau') = \delta(\tau)$ by the definition of the Möbius function, and the partitions $\tau' \le \tau$ in which $\{0\}$ is a singleton correspond to the partitions of $\{1, \dots, k+1\}$ refining the restriction of τ, with the same value of μ, so their sum is $h(\tau)$. Inserting this,

$$S_k(N) = \sum_{(\tau'_v)_{v \in [N]}} \prod_v g(\tau'_v) \sum_\pi \prod_i \operatorname{sgn} \pi_i,$$

where the inner sum runs over the tuples with $\pi_i(v) = \pi_j(v)$ whenever i and j lie in a common block of τ'_v, for all v.

Step 2: tokens. Fix (τ'_v). Call a pair (v, B) with $B \in \tau'_v$ a *token* sent by v. A tuple π in the inner sum assigns to each token a column $c(v, B)$ (the common value $\pi_i(v)$, $i \in B$), and the condition that every π_i is a permutation says that the tokens received by each column c form a partition σ_c of $\mathcal{I}$. Grouping by $(\sigma_c)_{c \in [N]}$, the tuple is given by a bijection β_B, for every block B, from the e_B tokens of type B sent by the rows to the e_B tokens of type B received by the columns (the numbers must agree). Conversely, partitions (σ_c) with the same numbers e_B and bijections (β_B) determine a unique tuple π compatible with (τ'_v). Hence

$$S_k(N) = \sum_{(\tau'_v),\,(\sigma_c)} \prod_v g(\tau'_v) \sum_{(\beta_B)} \prod_i \operatorname{sgn} \pi_i.$$

Step 3: the sign. Let $X = [N] \times \mathcal{I}$ and $\Theta(v, i) = (\pi_i(v), i)$. Then Θ is a permutation of X acting on $[N] \times \{i\}$ as π_i, so $\operatorname{sgn} \Theta = \prod_i \operatorname{sgn} \pi_i$. To compute it, order the source X by rows, and within row v by the tokens of v in the order of their blocks, each token by increasing i; this differs from the lexicographic order of X by the permutation with sign $\prod_v \varepsilon(\tau'_v)$. Order the target X in the same way by columns and received tokens; this costs $\prod_c \varepsilon(\sigma_c)$. With respect to these two orders, Θ maps each token, as a consecutive segment, onto its image token, preserving the order inside the segment. A permutation that moves consecutive segments of lengths $b_1, b_2, \dots$ as wholes has sign $\prod (-1)^{b_j b_l}$ over the pairs of segments whose order is reversed, and only pairs of odd tokens contribute. Hence

$$\prod_i \operatorname{sgn} \pi_i = \prod_v \varepsilon(\tau'_v) \prod_c \varepsilon(\sigma_c)\ \kappa,$$

where κ is the sign of the permutation that takes the odd tokens from their order on the row side to their order on the column side.

Step 4: the bijections. Changing β_B by a transposition swaps the values of two rows in each π_i, $i \in B$, and multiplies $\prod_i \operatorname{sgn} \pi_i$ by $(-1)^{|B|}$. For even $|B|$ all $e_B!$ bijections therefore give the same sign. For odd $|B|$ and $e_B \ge 2$, the bijections come in pairs of opposite sign and cancel. Only terms with $e_B \le 1$ for all odd B remain, and each of them is counted $\prod_{|B| \text{ even}} e_B!$ times with the sign of Step 3.

Step 5: the pairing. Expanding P^N as an ordered product of N factors, one for each row, gives $\sum_{(\tau'_v)} \prod_v g(\tau'_v) \varepsilon(\tau'_v) \cdot z^{\tau'_1} \cdots z^{\tau'_N}$, and the product of the variables is 0 if an odd variable repeats and otherwise $\kappa_R\, y^\alpha \theta_{\mathcal{J}}$, where $\alpha_B = e_B$ and κ_R is the sign that sorts the odd variables from their row order. The same holds for Q^N with the columns, weights $\varepsilon(\sigma_c)$ and a sign κ_C. The pairing of the two normal monomials is [equal] $\prod_B e_B!$, and $\kappa_R \kappa_C = \kappa$. Comparing with Steps 2 to 4 gives $S_k(N) = \langle P^N, Q^N \rangle$, and Lemma 7.2(1) gives the second statement. □

The smallest case shows the mechanism. For $k = 0$ the condition says $\pi_0 = \pi_1$, so $S_0(N) = N!$. Here $\mathcal{I} = \{0, 1\}$; write $y = y_{\{0,1\}}$, $\theta_0 = \theta_{\{0\}}$, $\theta_1 = \theta_{\{1\}}$ and order the subsets as $\{0\}, \{1\}, \{0, 1\}$.

The only partition in which 0 is not a singleton is $\{\{0,1\}\}$, with $\mu = -1$, so $P = y$ and $Q = y + \theta_0\theta_1$. Since $(\theta_0\theta_1)^2 = 0$, one has $Q^N = y^N + Ny^{N-1}\theta_0\theta_1$, and $\langle P^N, Q^N\rangle = \langle y^N, y^N\rangle = N!$. In the language of the proof, every row sends one token of type $\{0,1\}$, so every column must receive one, and the $N!$ bijections between them are the $N!$ choices of $\pi_0 = \pi_1$. The term with $\theta_0\theta_1$ describes columns that receive two separate tokens, which no row sends, and it pairs to zero. Figure 8 shows Steps 1 to 4 for $k = 2$, where the signs matter, and Table 1 summarises the translation between the count and the algebra.

the count $S_k(N)$	the pairing $\langle P^N, Q^N\rangle$
row v	one factor P of P^N
column c	one factor Q of Q^N
a token of type B (indices with equal values)	the variable z_B
inclusion and exclusion over the condition on a row	the coefficients $-\mu(\tau)$ in P
the $e_B!$ bijections between tokens of type B	the factor $\alpha_B!$ in the pairing
two lines of odd type cross, the sign changes	$\theta_B\theta_C = -\theta_C\theta_B$
two tokens of the same odd type cancel (Step 4)	$\theta_B^2 = 0$

Table 1: The translation in the proof of Theorem 7.4. Lines join the tokens sent by the rows to the tokens received by the columns, as in Figure 8.

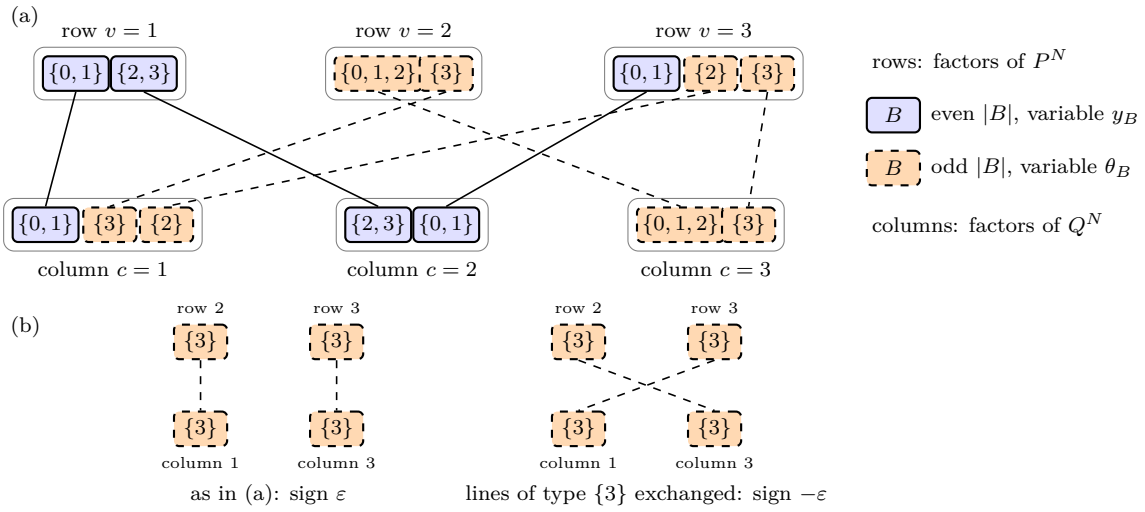

Figure 8: Steps 1 to 4 of the proof of Theorem 7.4 for $k = 2$, $\mathcal{I} = \{0,1,2,3\}$ and $N = 3$. Row v sends one token for each block of its partition τ'_v, in which 0 is not a singleton; column c receives tokens that form a partition σ_c of $\mathcal{I}$, and the lines are the bijections β_B between tokens of the same type B. (a) The odd type $\{3\}$ occurs twice. (b) Exchanging the two lines of type $\{3\}$ swaps the values of rows 2 and 3 in π_3 and changes the sign of the term, so the two terms cancel (Step 4).

For unsigned counts of Latin rectangles, Steps 1, 2 and 5 have a precursor: Gessel [12] weights the colour classes of the edges between two vertices by Möbius functions of partition lattices, cuts the edges into half-edge blocks and pairs blocks of the same type, which gives a formula for the number of $k \times n$ Latin rectangles and shows that it is P-recursive in n for fixed k. Expressions of such counts by symmetric functions in several sets of variables go back to MacMahon [14,

Section 10]; Gessel [13, Sections 8–11] develops them. The new features of Theorem 7.4 are the signs (Steps 3 and 4), which the Grassmann variables carry, and the extra permutation π_0; for six indices, Theorem 7.13 below gives the corresponding P-recursiveness for the signed count.

The theorem turns a signed count of Latin rectangles with an extra permutation into an algebraic expression in a fixed number of variables, $2^{k+2}-1$, which depends on k but not on N; the work needed to evaluate $\langle P^N, Q^N\rangle$ still grows with N. Its first consequence is a congruence modulo p of Lucas type.

Theorem 7.5. *Let $m \geq 1$ be odd, $k = m-1$, p a prime and $0 \leq a < p$. Then*

$$A_k(p+a,1) \equiv m!\, A_k(a,1) \pmod{p}.$$

In particular $p \mid A_k(p+m,1)$ if $3 \leq m < p$, since then $A_k(m,1) = 0$.

Proof. All coefficients of P and Q are integers, and the monomials of P commute, so in the ring of integral combinations of normal monomials $P^p = \sum_M c_M^p M^p + p\Delta$ with $P = \sum_M c_M M$ and integral Δ. A monomial with an odd variable has $M^p = 0$, and $c_M^p \equiv c_M \pmod{p}$. The same holds for Q. Let $N = p + a$. In a normal monomial $M = y^\alpha \theta_{\mathcal{J}}$ of P^N every $\alpha_B \leq N < 2p$, so $\prod_B \alpha_B!$ is divisible by p exactly $h(M)$ times, where $h(M)$ is the number of B with $\alpha_B \geq p$. In $P^N = P^a P^p$, the part $P^a \sum c_M M^p$ only has monomials with $h \geq 1$. Hence monomials with $h(M) = 0$ have coefficients divisible by p in P^N and in Q^N and contribute 0 modulo p^2 to $\langle P^N, Q^N\rangle$, and monomials with $h(M) \geq 2$ contribute 0 modulo p^2 as well. If $h(M) = 1$, then modulo p the coefficient of M comes from a term $c_{M'} M'^p$, where $M' = z^\tau$ for a partition τ of $\mathcal{I}$; since M'^p has exponent at least p at every block of τ, the partition τ has a single block, so $M' = y_{\mathcal{I}}$, whose coefficient is $-\mu(\{\mathcal{I}\}) = (q-1)! = m!$ in P and 1 in Q. Writing $M = y_{\mathcal{I}}^p M_0$, where M_0 is a monomial of P^a with $y_{\mathcal{I}}$-exponent $b \leq a$, the factor $\prod \alpha_B!$ of M is that of M_0 times $(p+b)!/b! = (b+1)\cdots(b+p) \equiv -p \pmod{p^2}$ (the factor p occurs once, since $b < p$, and the other $p-1$ factors run through the nonzero residues modulo p, whose product is -1 by Wilson's theorem). Altogether $\langle P^N, Q^N\rangle \equiv -p\, m!\, \langle P^a, Q^a\rangle \pmod{p^2}$, and $N! \equiv -p\, a! \pmod{p^2}$. Dividing, Theorem 7.4 gives the congruence. For $N = m$, the identity and k arc-disjoint derangements fill the all-ones matrix J of order m, so every determinant in $A_k(m,1)$ is $\det J = 0$. □

For unsigned counts, Stones and Wanless [26] prove congruences of the same shape for the numbers $R_{k,n}$ of reduced $k \times n$ Latin rectangles, by letting a cyclic group act on blocks of columns; among them $R_{k,n+p} \equiv (-1)^{k-1}(k-1)!\, R_{k,n} \pmod{p}$ for primes $p \geq k$. Theorem 7.5 is a signed analogue for the counts A_k, which carry the extra permutation π_0 and the determinant.

Together with Lemma 7.1 and $g_n(1-n) \equiv g_n(1-m) \pmod{p}$, this gives once more the divisibility $p \mid U_{p+m}$ for odd m with $3 \leq m < p$, without Corollary 3.2.

7.3 Five layers

For $k = 4$ there are six indices, and the blocks are the 15 pairs, the 15 sets of size 4 and the whole set $\mathcal{I}$ (even), and the 6 singletons, the 20 sets of size 3 and the 6 sets of size 5 (odd). The partitions of $\mathcal{I}$ into even blocks have the types $2+2+2$, $4+2$ and 6, with coefficients 1, -6 and 120 in P (times ε) and 1 in Q. For the type $2+2+2$, $\sum_\tau \varepsilon(\tau) z^\tau$ is the Pfaffian $\operatorname{pf}(Y)$ of the antisymmetric 6×6 matrix Y with entries $Y_{ij} = y_{\{i,j\}}$ for $i < j$: the shuffle sign of a perfect matching is the sign of the word $i_1 j_1 i_2 j_2 i_3 j_3$ with $i_r < j_r$, which does not depend on the order of the pairs, and this is the sign in the usual definition of the Pfaffian.

Lemma 7.6. *For $k = 4$, as formal power series in s and t with $u = st$,*

$$\langle e^{sP}, e^{tQ}\rangle = e^{120u}\,\mathbb{E}\Big[e^{-6u|Y|^2} e^{s\,\mathrm{pf}(Y)+t\,\mathrm{pf}(\overline{Y})}\prod_i (1+S_i)\Big],$$

where $|Y|^2 = \sum_e |Y_e|^2$ over the 15 pair variables, the expectation acts on the pair variables as the expectation for independent standard complex Gaussians Y_e and on the Grassmann variables by the pairing of Section 7.2, and the S_i are finitely many explicit terms that contain Grassmann variables (listed in Appendix B). Moreover, for polynomials f, g in the pair variables that are homogeneous of the same degree D,

$$\mathbb{E}[e^{-c|Y|^2} f(Y)\, g(\overline{Y})] = (1+c)^{-15-D}\,\langle f, g\rangle.$$

Proof. For polynomials in commuting variables, $\langle f, g\rangle = \mathbb{E}\,[f(Y)\, g(\overline{Y})]$ for independent standard complex Gaussians, since $\mathbb{E}\, Y^a \overline{Y}^b = [a = b]\, a!$; all identities hold coefficientwise in s and t, where they are finite. If a commuting variable y occurs only linearly, as $s\alpha y$ in the exponent on one side and $t\beta y$ on the other, with even α, β free of y, then $\mathbb{E}\, e^{\lambda Y + \nu\overline{Y}} = e^{\lambda\nu}$ gives the factor $e^{st\alpha\beta}$. The variable $y_{\mathcal{I}}$ occurs only in the terms $120\, y_{\mathcal{I}}$ of P and $y_{\mathcal{I}}$ of Q, which gives e^{120u}. A set B of size 4 occurs only together with its complementary pair $\{i, j\}$, in the types $4+2$ and $4+1+1$; its contraction gives the scalar factor $e^{-6u|y_{ij}|^2}$ times a factor whose exponent contains Grassmann variables. The terms of type $2+2+2$ add up to $\mathrm{pf}(Y)$. All remaining terms of P and Q, and the Grassmann parts of the contractions, contain Grassmann variables; they are even and square to zero, so their exponentials are $1 + S_i$. Finally $\mathbb{E}[e^{-c|Y|^2} Y^a \overline{Y}^b] = [a = b]\, a!\,(1+c)^{-|a|-15}$ for the 15 pair variables. □

For the part without Grassmann variables, Lemma 7.6 and the antisymmetric Cayley identity $\mathrm{pf}(\partial)\,\mathrm{pf}(Y)^s = s(s+2)(s+4)\,\mathrm{pf}(Y)^{s-1}$ [6, Theorem 2.3] already give a closed formula. The Grassmann variables and the pair variables with insertions remain. To evaluate the pairing I first compute the moments of the Pfaffian exactly, using only elementary identities and one classical fact about representations of GL_6.

Representation theory enters through a symmetry. The 15 pair variables are the entries of the antisymmetric matrix Y, and GL_6 acts on Y by $Y \mapsto gYg^T$, which multiplies $\mathrm{pf}(Y)$ by $\det g$. Because of this symmetry, the pairing of powers of the Pfaffian with other polynomials need not be computed monomial by monomial: it suffices to know it on one polynomial f_λ for each partition λ with at most three parts (Proposition 7.11). Section 7.5 then reduces the resulting series to the Euler series of factorials. Theorem 7.14 and the orders 94 and 118 use only the statement of Theorem 7.13.

7.4 Pfaffian moments

Write $\partial_e = \partial/\partial y_e$ for the 15 pair variables and $\mathrm{pf}(\partial)$ for the Pfaffian of the antisymmetric matrix of these derivatives. Let $\mathrm{pf}_2 = y_{01}$, $\mathrm{pf}_4 = y_{01}y_{23} - y_{02}y_{13} + y_{03}y_{12}$ and $\mathrm{pf}_6 = \mathrm{pf}(Y)$ be the leading principal sub-Pfaffians, and for a partition $\lambda = (\lambda_1 \ge \lambda_2 \ge \lambda_3 \ge 0)$ put

$$f_\lambda = \mathrm{pf}_2^{\lambda_1-\lambda_2}\,\mathrm{pf}_4^{\lambda_2-\lambda_3}\,\mathrm{pf}_6^{\lambda_3}, \qquad \kappa_\lambda(K) = \prod_{i=1}^{3}\frac{(\lambda_i + K + s_i)!}{(\lambda_i + s_i)!}, \quad s = (4, 2, 0).$$

Let V_D be the space of homogeneous polynomials of degree D in the pair variables. For $g \in \mathrm{GL}_6(\mathbb{C})$ write $c_g(Y) = gYg^T$.

Lemma 7.7. *1. $\langle y_e f, h\rangle = \langle f, \partial_e h\rangle$; hence $\langle \mathrm{pf}\cdot f, h\rangle = \langle f, \mathrm{pf}(\partial)h\rangle$.*

2. For every polynomial φ and $g \in \mathrm{GL}_6$, $\mathrm{pf}(\partial)(\varphi \circ c_g) = \det(g)\,(\mathrm{pf}(\partial)\varphi)\circ c_g$.

3. For $K \geq 0$ the operator $\Delta_K = \mathrm{pf}(\partial)^K \circ \mathrm{pf}^K$ maps V_D to V_D and commutes with the action of the Lie algebra $\mathfrak{gl}_6$ by the derivations $X_A\varphi(Y) = \frac{d}{d\epsilon}\varphi((1+\epsilon A)Y(1+\epsilon A)^T)|_{\epsilon=0}$.

Proof. (1) On monomials both sides are $[\alpha + e = \beta]\,\beta!$. (2) With $\langle Z, Y\rangle = \sum_{i<j} z_{ij}y_{ij}$ one has $\langle Z, gYg^T\rangle = \langle g^T Z g, Y\rangle$ and $\mathrm{pf}(\partial)e^{\langle Z,Y\rangle} = \mathrm{pf}(Z)e^{\langle Z,Y\rangle}$, so $\mathrm{pf}(\partial)e^{\langle Z,gYg^T\rangle} = \mathrm{pf}(g^TZg)e^{\langle g^TZg,Y\rangle} = \det(g)\,\mathrm{pf}(Z)e^{\langle Z,gYg^T\rangle}$; comparing coefficients of the monomials in Z gives the claim. (3) Since $\mathrm{pf}(gYg^T) = \det(g)\,\mathrm{pf}(Y)$, $[X_A, \mathrm{pf}^K] = K\,\mathrm{tr}(A)\,\mathrm{pf}^K$, and differentiating (2) at $g = 1+\epsilon A$ gives $[X_A, \mathrm{pf}(\partial)] = -\,\mathrm{tr}(A)\,\mathrm{pf}(\partial)$. Hence $[X_A, \Delta_K] = \mathrm{pf}(\partial)^K[X_A, \mathrm{pf}^K] + [X_A, \mathrm{pf}(\partial)^K]\,\mathrm{pf}^K = 0$. □

Lemma 7.8. *Let B be the group of lower triangular matrices in $\mathrm{GL}_6(\mathbb{C})$ and $Y_0 = \mathrm{diag}(J, J, J)$ with $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0\end{smallmatrix}\right)$.*

1. For $g \in B$, $\mathrm{pf}_{2r}(c_g(Y)) = g_{00}g_{11}\cdots g_{2r-1,2r-1}\,\mathrm{pf}_{2r}(Y)$.

2. Every Y with $\mathrm{pf}_2\,\mathrm{pf}_4\,\mathrm{pf}_6(Y) \neq 0$ is $c_g(Y_0)$ for some $g \in B$.

3. If a polynomial φ satisfies $\varphi(c_g(Y)) = \chi(g)\varphi(Y)$ for all $g \in B$, where χ is the character $(g_{00}g_{11})^{a+b+c}(g_{22}g_{33})^{b+c}(g_{44}g_{55})^c$ of $T = \mathrm{pf}_2^a\,\mathrm{pf}_4^b\,\mathrm{pf}_6^c$, then $\varphi = \varphi(Y_0)\,T$.

Proof. (1) The leading $2r \times 2r$ block of gYg^T is $g'Y'g'^T$ with the leading blocks g', Y'. (2) By induction: if $y_{01} \neq 0$, then $Y = L\,\mathrm{diag}(y_{01}J, S)L^T$ with a lower unitriangular L and the antisymmetric Schur complement S, whose leading sub-Pfaffians are $\mathrm{pf}_{2r}(Y)/y_{01} \neq 0$ by (1); and $y_{01}J = c_d(J)$ with $d = \mathrm{diag}(y_{01}, 1)$. (3) T has the same character and $T(Y_0) = 1$, so $\varphi = \varphi(Y_0)T$ on the dense set of (2), hence everywhere. □

Lemma 7.9. *For integers $a, b \geq 0$ and $c \geq 1$,*

$$\mathrm{pf}(\partial)(\mathrm{pf}_2^a\,\mathrm{pf}_4^b\,\mathrm{pf}_6^c) = c\,(b+c+2)\,(a+b+c+4)\;\mathrm{pf}_2^a\,\mathrm{pf}_4^b\,\mathrm{pf}_6^{c-1}\,.$$

Consequently $\Delta_K f_\lambda = \kappa_\lambda(K) f_\lambda$ for every partition λ with at most three parts.

Proof. Let $F = \mathrm{pf}_2^a\,\mathrm{pf}_4^b\,\mathrm{pf}_6^c$, $A = a+b+c$, $B' = b+c$. By Lemma 7.8(1) and Lemma 7.7(2), $\mathrm{pf}(\partial)F$ satisfies the hypothesis of Lemma 7.8(3) for $T = \mathrm{pf}_2^a\,\mathrm{pf}_4^b\,\mathrm{pf}_6^{c-1}$, so $\mathrm{pf}(\partial)F = e\,T$, where e is the coefficient of $m^* = y_{01}^{A-1}y_{23}^{B'-1}y_{45}^{c-1}$ in $\mathrm{pf}(\partial)F$. Call $01, 23, 45$ the diagonal pairs. Every term of pf_2, pf_4, pf_6 contains 0, 2 or 3 non-diagonal variables, never exactly one. The coefficient of m^* in $\mathrm{pf}(\partial)F$ is the sum over the 15 perfect matchings μ of $\mathrm{sgn}\,\mu$ times the coefficient of m^*y_μ in F times the product of the exponents of the three variables of μ in m^*y_μ. The diagonal matching gives $AB'c$. The four matchings with the diagonal pair 01 or 23 and two non-diagonal pairs meeting $\{4,5\}$ take these from one of the c factors pf_6 and give cA (twice) and cB' (twice). The two matchings with 45 take the non-diagonal pair from one of the b factors pf_4 or one of the c factors pf_6, with the same sign, and give cB' each. The eight matchings without diagonal pairs come from a single term of one factor pf_6 and give c each. Hence $e = AB'c + 2cA + 4cB' + 8c = c(A+4)(B'+2)$. Iterating with $c = \lambda_3 + K, \ldots, \lambda_3 + 1$ gives $\kappa_\lambda(K)$. □

For $\lambda = 0$ this is the antisymmetric Cayley identity [6, Theorem 2.3]. Identities of this kind are known in greater generality: Caracciolo, Sokal and Sportiello [6, Section 2.6] point to generalisations of the Cayley identity in which both the determinant and the differential operator are replaced by products of leading principal minors. Lemma 7.9 is a case of the eigenvalue formula of Kostant and Sahi [20, (4.4)] for the operators $\varphi^m \partial(\varphi)^m$ on symmetric tube domains: for the cone of positive definite quaternionic Hermitian 3×3 matrices the complexification is the space of 6×6 antisymmetric matrices, the principal minors are the leading sub-Pfaffians and the root multiplicity is $d = 4$ [20, Section 5, type D], and the shifts $s_i = 2(3 - i)$ in κ_λ come from $d/2 = 2$. Rubenthaler and Schiffmann [23, Lemme 5.6, Théorème 5.7] compute the b-functions of the fundamental relative invariants of these prehomogeneous spaces in general. I include the short algebraic proof of the case needed here. The extension from the vectors f_λ to all polynomials uses one classical fact, the multiplicity-free decomposition of the polynomials on antisymmetric matrices under GL_6: each irreducible representation occurs at most once, and those that occur in degree D correspond to the partitions of D into at most three parts (Schmid [25, p. 63, assertion c)] for all Hermitian symmetric spaces; for antisymmetric matrices Howe [16, Proposition 2] and Howe and Umeda [17, (11.3.2)], who also give the Pfaffian highest weight vectors [17, (11.3.3)]; Kostant and Sahi [20, Theorem 0] state it with the products of principal minors as extremal weight vectors). I sketch the part of the argument that is used.

Lemma 7.10. *$V_D = \sum_\lambda U(\mathfrak{gl}_6) f_\lambda$, the sum over the partitions λ of D into at most three parts.*

Proof. GL_6 acts on V_D by $(\rho(g)\varphi)(Y) = \varphi(g^T Y g)$, a polynomial representation. By complete reducibility and the theorem of the highest weight, V_D is spanned by the $U(\mathfrak{gl}_6)$-modules generated by vectors v that are eigenvectors of the upper triangular Borel subgroup with dominant polynomial weights. Such a $v \neq 0$ satisfies $v(Y_0) \neq 0$, since otherwise it vanishes on the dense set of Lemma 7.8(2), so its character is trivial on the stabiliser of Y_0 in the diagonal torus and v satisfies the hypothesis of Lemma 7.8(3); dominance gives $\alpha \geq \beta \geq \gamma \geq 0$ for its exponents, and v is a multiple of $f_{(\alpha,\beta,\gamma)}$. So $U(\mathfrak{gl}_6) f_\lambda$ is the irreducible representation with highest weight $(\lambda_1, \lambda_1, \lambda_2, \lambda_2, \lambda_3, \lambda_3)$, and since its highest weight vectors form the line spanned by f_λ, it occurs in V_D exactly once. □

Proposition 7.11. *Let $f, h \in V_D$ and $h = \sum_\lambda h_\lambda$ with $h_\lambda \in U(\mathfrak{gl}_6) f_\lambda$. Then for every $K \geq 0$, $\langle \mathrm{pf}^K f, \mathrm{pf}^K h \rangle = \sum_\lambda \kappa_\lambda(K) \langle f, h_\lambda \rangle$.*

Proof. By Lemma 7.7(1) the left side is $\langle f, \Delta_K h \rangle$; by Lemma 7.7(3) and Lemma 7.9, Δ_K acts on $U(\mathfrak{gl}_6) f_\lambda$ by $\kappa_\lambda(K)$. □

7.5 The closed form for five layers

Start from Lemma 7.6. Every Grassmann variable occurs at most once in a nonzero monomial. Expanding the product and pairing the Grassmann variables gives a finite sum $C = \sum c\, s^a t^b\, y^\gamma \otimes \overline{y}^{\gamma'}$ of monomials in the pair variables on the two sides; for six indices it has 1 651 018 terms, which I computed in exact integer arithmetic. Group them by $G = (a, b, d, d')$ with $d = |\gamma|$, $d' = |\gamma'|$, put $\delta = |d - d'|/3$, $D = \max(d, d')$, and (for $d \geq d'$; otherwise exchange the sides) $h = \mathrm{pf}^\delta\, y^{\gamma'} \in V_D$. With a decomposition $h = \sum_\lambda h_\lambda$ as in Lemma 7.10 put

$$W_{G,\lambda} = \sum_{\text{terms of } G} c\, \langle y^\gamma, h_\lambda \rangle .$$

By Proposition 7.11 the moments $m_j = \sum c\,\langle y^\gamma, \Delta_1^j h\rangle$ equal $\sum_\lambda W_{G,\lambda}\kappa_\lambda(1)^j$. For each fixed degree $D \le 7$ the numbers $\kappa_\lambda(1) = (\lambda_1+5)(\lambda_2+3)(\lambda_3+1)$ are pairwise distinct for the partitions λ of D into at most three parts (across different degrees they can coincide, for instance for $(1,1,0)$ and $(3,0,0)$). Every group G has a single degree D, and $D \le 7$ for all groups, so the $W_{G,\lambda}$ are determined by finitely many moments; they do not depend on the decomposition. I computed them exactly: there are 361 nonzero weights, all integers. With the identity for the mass term in Lemma 7.6 and Proposition 7.11 one obtains the coefficient formula

$$H(u) := e^{-120u}\sum_N A_4(N,1)\frac{u^N}{N!}$$
$$= \sum_{G,\lambda} W_{G,\lambda}\, u^{\max(a,b)}(1+6u)^{-15-D}\sum_{j\ge 0}\frac{\kappa_\lambda(j)}{j!\,(j+\delta)!}\,x^j, \qquad x = \frac{u}{(1+6u)^3}. \tag{7.1}$$

The inner series are hypergeometric. For $\alpha \in \mathbb{Z}^3_{\ge 0}$ and $\delta \in \mathbb{Z}$ put

$$\Phi_{\alpha,\delta}(x) = \sum_{N\ge 0}\frac{(N+\alpha_1)!\,(N+\alpha_2)!\,(N+\alpha_3)!}{N!\,(N+\delta)!}\,x^N$$

(with $1/(N+\delta)! = 0$ for $N+\delta < 0$) and $\theta = x\,d/dx$.

Lemma 7.12. *As formal power series, $(\theta+\alpha_i+1)\Phi_{\alpha,\delta} = \Phi_{\alpha+e_i,\delta}$ and $(\theta+\delta)\Phi_{\alpha,\delta} = \Phi_{\alpha,\delta-1}$. The series $\Phi_0 = \Phi_{(0,2,4),2} = \sum_N (N+4)!\,x^N$ satisfies $\theta\Phi_0 = (x^{-1}-5)\Phi_0 - 24x^{-1}$. Consequently, for $\alpha \ge (0,2,4)$ componentwise and $\delta \le 2$, $\Phi_{\alpha,\delta} = r\Phi_0 + s$ with Laurent polynomials $r, s \in \mathbb{Q}[x, x^{-1}]$.*

Proof. The first two identities hold coefficientwise, since $(N+\alpha_i+1)(N+\alpha_i)! = (N+\alpha_i+1)!$ and $(N+\delta)/(N+\delta)! = 1/(N+\delta-1)!$ (both sides 0 if $N+\delta \le 0$). The coefficient of x^N in $x(\theta+5)\Phi_0$ is $(N+4)!$ for $N \ge 1$ and 0 for $N = 0$, so $\Phi_0 - x(\theta+5)\Phi_0 = 24$. Starting from Φ_0, apply the first two identities and replace $\theta\Phi_0$ after each step: $(\theta+c)(r\Phi_0+s) = (\theta r + cr - 5r + r/x)\Phi_0 + (\theta s + cs - 24r/x)$. □

Theorem 7.13 (computer-assisted)**.** *There are integer polynomials N_A, N_B of degree 31 (listed in the code repository of Section 8; $N_A = 5u^6 - 95u^7 + \dots$, $N_B = -120u^6 + 1680u^7 - \dots$) such that*

$$H(u) = \frac{N_A(u)\,\Phi_0(x) + N_B(u)}{48\,u^{10}(1+6u)^{15}}, \qquad x = \frac{u}{(1+6u)^3}.$$

H satisfies a linear differential equation $p_1H' + p_0H = q$ with integer polynomials p_1, p_0, q of degrees 34, 35, 35, $u^2 \mid p_1$ and $p_0(0) = -1$. Consequently the coefficients H_k of H satisfy an integer recurrence expressing H_k through $H_0, \dots, H_{k-1}$; all H_k are integers, and $H_k = (-120)^k/k!$ for $k \le 5$.

Proof. In (7.1), $\kappa_\lambda(j)/(j!(j+\delta)!)$ is the coefficient of x^j in $\Phi_{\alpha,\delta}/\prod_i(\lambda_i+s_i)!$ with $\alpha = (\lambda_3, \lambda_2+2, \lambda_1+4) \ge (0,2,4)$, and $\delta \le 2$. Lemma 7.12 turns every term into $r\Phi_0 + s$; summing the 361 terms in exact rational arithmetic gives N_A and N_B. For $G(u) = \Phi_0(x(u))$ one has $x'/x = (1-12u)/(u(1+6u))$, so Lemma 7.12 gives $u^2(1+6u)G' = (1-12u)\big[((1+6u)^3-5u)G - 24(1+6u)^3\big]$. Eliminating G from this and the closed form (exact polynomial arithmetic, then division by the greatest common divisor) gives the differential equation. Comparing coefficients of u^k, the term $-H_k$ comes from $p_0(0) = -1$, and $u^2 \mid p_1$ means that p_1H' involves only $H_0, \dots, H_{k-1}$. Finally $A_4(0,1) = 1$ and $A_4(N,1) = 0$ for $1 \le N \le 5$ (for $N \le 4$ there are no four arc-disjoint derangements, and for $N = 5$ every determinant is $\det J = 0$), so $H = e^{-120u} + O(u^6)$. □

The only non-rational ingredient of H is the Euler series Φ_0 of factorials. This explains why the second digit for $n = p + 5$ is again a sum of Kurepa type.

Theorem 7.14. *For a prime $p \geq 7$ put, modulo p,*

$$S_5(p) = -\frac{120^6}{5} + \sum_{i=6}^{p+5} (-1)^{i-6} (i-6)!\, 120^{7-i} H_i.$$

Then $A_4(p+5, 1) \equiv p\, S_5(p) \pmod{p^2}$ and $D_{p+5}/p^3 \equiv \frac{24}{5} S_5(p) \pmod{p}$. In particular, if $S_5(p) \not\equiv 0 \pmod{p}$, then D_{p+5} is divisible by exactly p^3 and the Alon–Tarsi conjecture holds for $n = p+5$.

Proof. Let $N = p+5$. Then $A_4(N, 1) = \sum_{i=0}^{N} (N)_i 120^{N-i} H_i$ with integers H_i. For $i \geq 6$ the falling factorial $(N)_i$ contains p exactly once and $(N)_i/p \equiv 5!\,(-1)^{i-6}(i-6)!$, while $120^{N-i} \equiv 120^{6-i} \pmod{p}$. For $i \leq 5$, $H_i = (-120)^i / i!$ and the sum is $120^N \sum_{i \leq 5} (-1)^i \binom{N}{i} = -120^N \binom{N-1}{5} = -120^N p(p+1)(p+2)(p+3)(p+4)/120 \equiv -p\, 120^6/5 \pmod{p^2}$. Corollary 7.3 with $m = 5$ gives the rest. □

Theorem 7.15 (computer-assisted)**.** *$S_5(89) \equiv 41 \pmod{89}$ and $S_5(113) \equiv 20 \pmod{113}$. Hence $A_4(94, 1) \equiv 89 \cdot 41 \pmod{89^2}$, $A_4(118, 1) \equiv 113 \cdot 20 \pmod{113^2}$, $D_{94}/89^3 \equiv 1 \pmod{89}$ and $D_{118}/113^3 \equiv 96 \pmod{113}$, and the Alon–Tarsi conjecture holds for $n = 94$ and $n = 118$.*

Proof. The values H_k for $k \leq 118$ follow from the recurrence of Theorem 7.13; then Theorem 7.14 gives $\frac{24}{5} \cdot 41 \equiv 1 \pmod{89}$ and $\frac{24}{5} \cdot 20 \equiv 96 \pmod{113}$. This also proves Theorem 1.3. □

8 Computations

The order 26. For $p = 23$ the partial sums of $j!\, 6^{-j}$ modulo 23 give $K_6(23) \equiv 5$, so $4K_6(23) - 5 \equiv 15$ and Theorem 1.1 gives $U_{26}/23 \equiv -6 \cdot 15 \equiv 2 \pmod{23}$. Since $26!/23 \equiv -6$ and $25!/23 \equiv -2$ modulo 23 by Wilson's theorem, $D_{26}/23^3 \equiv 12 \cdot 2 \equiv 1 \pmod{23}$. This proves Corollary 1.2. As a check of the reduction in Theorem 6.1, I also evaluated the generating function of Theorem 5.5 exactly for $n = 26$ in rational arithmetic; it gives $g_{26}(-2) \equiv 483 = 23 \cdot 21 \pmod{23^2}$, and indeed $6(4 \cdot 5 - 5) = 90 \equiv 21 \pmod{23}$. The independent checks of Theorem 5.5 are described in Appendix B.

The orders $p+3$ and $p+2$. I computed $K_6(p)$ and $K_2(p)$ for all primes $p < 10^6$ (each in $O(p)$ operations). The congruence $4K_6(p) \equiv 5$ holds only for $p = 59729$, and $K_2(p) \equiv 1$ only for $p = 234781$; the latter agrees with Berndsen's search below 2^{20} [5]. Heuristically, if the residues behaved like random elements of $\mathbb{F}_p$, one would expect about $\sum_p 1/p$ exceptions below x, which grows like $\log\log x$; the two single exceptions are consistent with this. The theorem of Glynn covers $n = p - 1$ and the theorem of Drisko covers $n = p + 1$, and Theorem 1.1 covers $n = p + 3$ unless $p = 59729$.

The orders $p+5$. Theorem 7.13 rests on exact computations: the elimination of the Grassmann variables (1 651 018 terms, exact integers), the 361 weights $W_{G,\lambda}$ (exact solution of the Vandermonde systems), the reduction of the occurring hypergeometric series to Φ_0 by Lemma 7.12, the polynomials N_A, N_B, and the elimination giving the differential equation (exact polynomial arithmetic). The programs that carry out the whole chain, starting from the definition of P and Q in Theorem 7.4 (export of the summands of the pairing, elimination of the Grassmann variables,

moments, Vandermonde systems, weights, N_A, N_B and the differential equation), are available at https://github.com/totallyunknown/alon-tarsi-orders-code (tag `alon-tarsi-26-v1`); the elimination takes about two minutes and 6 GB of memory. In addition there is a short stand-alone program that reads only the 361 weights and the polynomials and checks the closed form, the differential equation and the recurrence, and recomputes the residues for $n = 94$ and $n = 118$ and Table 2.

p	A/p	D/p^3	p	A/p	D/p^3	p	A/p	D/p^3
7	3	6	37	27	26	71	17	39
11	4	6	41	22	40	73	42	41
13	7	5	43	30	15	79	36	78
17	3	11	47	15	25	83	37	78
19	16	16	53	27	13	89	41	1
23	13	21	59	11	41	97	72	74
29	2	27	61	22	8	101	55	62
31	19	23	67	15	5	103	27	6
						107	89	42
						109	70	9
						113	20	96

Table 2: The residues of $A/p = S_5(p)$ and D/p^3 modulo p, where $A = A_4(p+5, 1)$ and $D = D_{p+5}$, for $7 \le p \le 113$.

I checked these computations in several independent ways, among them a second evaluation of the pairing that does not use Section 7.4 and gives the same polynomials N_A, N_B; see Appendix B.

With the recurrence of Theorem 7.13, $S_5(p)$ costs $O(p)$ operations. I computed it for all primes $7 \le p \le 300\,000$. It vanishes only for $p = 4787$; the order $4792 = 4787 + 5$ is covered by Glynn's theorem (4793 is prime). As for $p + 3$, one or two exceptions in this range are what one would expect from random residues ($\sum 1/p \approx 1.8$ over these primes). Table 2 lists $S_5(p) = A_4(p + 5, 1)/p$ and D_{p+5}/p^3 modulo p for $p \le 113$. All these orders except 94 and 118 were already covered by Drisko, Glynn or Theorem 1.1.

Combining the families $p - 1$, $p + 1$, $p + 3$ with Theorem 7.15 gives the following.

Corollary 8.1. *The Alon–Tarsi conjecture holds for all even $n \le 118$. The smallest even order for which it is open is* 120.

Indeed, every even n with $12 \le n \le 116$, $n \ne 94$, has $n - 1$, $n + 1$ or $n - 3$ prime, the orders 94 and 118 are covered by Theorem 7.15, and none of 119, 121, 117 and 115 is prime. Adding the orders $p + 5$ with $p \le 300\,000$, $p \ne 4787$, the even orders up to 300 that remain open are 120, 122, 124, 146, 188, 206, 208, 218, 220, 248, 290, 300; up to 1000 and 2000 there are 62 and 182 of them, against 109 and 280 without the orders $p + 5$. Figure 9 shows which family covers each even order up to 300. Huang and Rota [18, Section 3] showed that the Alon–Tarsi conjecture for an even n implies Rota's basis conjecture in dimension n over fields of characteristic zero (see also [27, p. 2]), so Corollary 8.1 also gives Rota's basis conjecture in these dimensions over such fields. Over a field of characteristic p this argument needs $D_n \not\equiv 0 \pmod p$, which fails here for the prime p used.

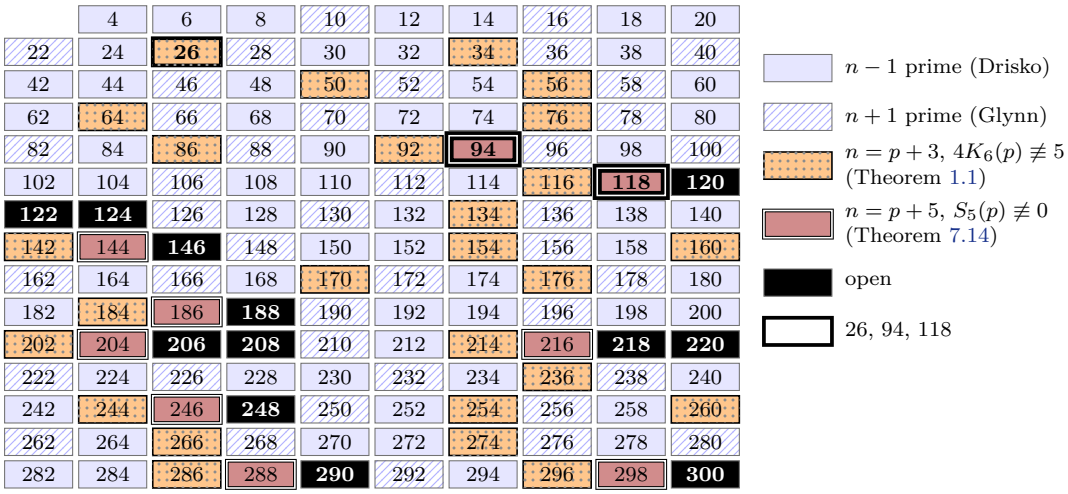

Figure 9: The even orders $4 \le n \le 300$, each marked by the first family that covers it: $n-1$ prime (Drisko), $n+1$ prime (Glynn), $n = p+3$ with a prime $p \ge 5$, $p \ne 59729$ (Theorem 1.1), and $n = p+5$ with a prime $7 \le p \le 300\,000$, $p \ne 4787$ (Theorem 7.14). The orders $n \le 10$ are all of the form $p \pm 1$, the twelve black cells are the open orders, and the orders 26, 94 and 118 are framed.

9 Concluding remarks

The main limitation of the method is the evaluation of the pairing in Theorem 7.4. For an even order $n = p + m$ with $3 \le m < p$, Lemma 7.1 and Corollary 7.3 reduce the second p-adic digit to the signed count $A_{m-1}(n, 1)$ of Latin rectangles with m rows modulo p^2, and Theorem 7.4 turns this count into a pairing in a number of variables that depends on m but not on p (the cost of evaluating it grows with p). For a single order there are many primes p between $n/2$ and $n-3$, and each of them could be used.

For $m = 2$ and $m = 3$ the second digit is an explicit factorial sum (Theorems 1.1 and 1.4). The exceptional primes, at which the sum takes the forbidden value, are rare in the range I examined (one each below 10^6), and I see no way to describe them in general; the situation is analogous to Kurepa's left factorial hypothesis [21]. For $m = 5$, Theorem 7.14 is a criterion of the same kind, with the integer coefficients H_k of the series of Theorem 7.13 in place of the powers of a fixed number; below 300 000 the only exceptional prime is 4787. I do not know whether $S_5(p)$ can be expressed through finitely many sums $K_c(p)$; the closed form shows at least that the Euler series $\sum (N+4)!\, x^N$ is its only non-rational ingredient. For $m = 7$, which is the next case and would give the order $120 = 113 + 7$, the pairing has eight indices; partitions with two blocks of size 4 occur, and the contraction used in Lemma 7.6 no longer separates the variables. The pairing is still a finite object, and the methods of Sections 7.4 and 7.5 (Pfaffian moments and contiguity of hypergeometric series) may extend to it, with eight indices and more Pfaffian minors; carrying this out is the next challenge. It would go a long way: every even $n \le 10^4$ except 9584 has a prime p with $n - p \in \{-1, 1, 3, 5, \dots, 31\}$, and 9584 needs the offset 33. A method for general odd m would settle the conjecture far beyond the present range, up to isolated exceptional primes.

The second p-adic digit can vanish, and then the method needs the third digit. This happens for $n = 59732 = 59729 + 3$ and $n = 234783 = 234781 + 2$. It also happens in a structured way

for $n = 2p$: there $m = p$, Proposition 4.1 gives only $g_{2p}(1-2p) \equiv g_{2p}(1-p) \pmod{p^2}$, and for $p = 3, 5$ one has $v_p(U_{2p}) = p-1$. The fixed points of the cyclic group in Theorem 3.1 account for only part of this valuation. For $n = 26 = 2 \cdot 13$ this route would require control modulo a high power of 13, which is why the prime $23 = 26 - 3$ is the natural one to use.

It would be interesting to know whether Theorem 3.1 has a p-adic refinement, that is, an expression for J_{p+m} modulo p^2 in terms of J_p, J_m and their derivatives. Such a refinement would give the second digit for all m at once; Theorem 7.5 is its analogue modulo p for the counts A_k. I also do not know a combinatorial interpretation of the factorial sums $K_6(p)$ in terms of Latin squares; by Section 6 they count permutations of $p-1$ points weighted by $(-5)^{\text{number of fixed points}}$.

Theorem 7.13 uses, besides paper proofs, the exact computations listed in Section 8 and the classical Lemma 7.10; Theorem 7.15, the orders $p+5$ and Table 2 depend on it.

Formalisation. The numbered results of Sections 2 to 6, Lemmas 7.1 and 7.2, Corollary 7.3, Theorems 7.4 and 7.5 and Proposition A.1, and with them Theorem 1.1 and Corollary 1.2 (also in the form $L^e_{26} \neq L^o_{26}$, with Janssen's identity), are formalised in Lean 4 [8], version 4.34.0, with Mathlib [28], release v4.34.0, and checked by the kernel. The formal statement for the order 26 is $L^e_{26} \neq L^o_{26}$, with the sign of a Latin square defined by its rows and columns as in Section 1; the chain to it runs through D_n as the signed count of Latin squares by symbol permutations, so the coefficient forms of D_n in Section 1 and of $c_{n-1}(J-I)$ in Section 2 are not needed; the formalisation works with the signed counts of the corresponding decompositions, and it proves Janssen's identity as well. In Sections 2 to 6 the exceptions are the logarithmic identity in Lemma 2.2 and Remark 2.5; in the formalisation the sum (5.2) is evaluated through powers of transfer matrices instead of the list of components in Section 5.4. For Theorem 1.3 the formalisation derives $D_{94} \neq 0$ and $D_{118} \neq 0$ from the two residues of A_4 in Theorem 7.15; these residues, Section 7.4, Lemmas 7.6 and 7.12, Theorems 7.13 and 7.14, Section 8, Appendix A beyond Proposition A.1 and the second statement of Theorem 1.4 are not formalised. The Lean sources are available at `https://github.com/totallyunknown/latin-squares-lean` (tag `alon-tarsi-26-v1`); `lake build` in the repository checks all proofs.

Use of AI

AI tools (Claude by Anthropic and Codex by OpenAI) were used in the course of this research to explore mathematical ideas, develop and check proofs, implement and test computations, and prepare the manuscript. The author critically reviewed the mathematical arguments and references, cross-checked the computer-assisted results as described in Section 8, and takes full responsibility for the content.

A The case $p+2$

This appendix proves Berndsen's Theorem 1.4 with the methods of Sections 3 to 6. It is not needed for the orders 26, 94 and 118.

Proposition A.1. *Let p be a prime and $n = p+2$. Then $g_n(1-n) \equiv g_n(-1) - p \pmod{p^2}$.*

Proof. The Taylor expansion in the proof of Proposition 4.1, with $m = 2$, gives $g_n(1-n) \equiv g_n(-1) - p\, g_n'(-1) \pmod{p^2}$, and it remains to show $g_n'(-1) \equiv 1 \pmod{p}$. Corollary 3.2 with $g_2 = 1$ gives $(t+1)\, g_n(t) = g_p(t+2)\,(t^p - t)^2$ in $\mathbb{F}_p[t]$. Write $t^p - t = (t+1)\, Q(t)$; then

$g_n = g_p(t+2)\,(t+1)\,Q(t)^2$ and $g_n'(-1) = g_p(1)\,Q(-1)^2$. Here $Q(-1)$ is the derivative of $t^p - t$ at -1, which is -1 in $\mathbb{F}_p$, and $g_p(1) = ((p-1)!)^{p-1} \equiv 1$ by (2.1) and Wilson's theorem. □

For $k = 1$, Lemmas 5.1, 5.3 and 5.4 give a finite formula. Write $(n)_r = n(n-1)\cdots(n-r+1)$.

Theorem A.2. *For $n \geq 4$ and $a = 1/(n-2)$,*

$$g_n(-1) = -\frac{((n-2)!)^n}{n^2(n-3)!}\,T_n,$$

where

$$T_n = n^n(1+a)^{n-1}(1-(n-1)a) - \sum_{r=1}^{n-1}(n)_{r+1}(-1)^r n^{n-r} a^{r+1}(1+a)^{n-r-1}.$$

Proof. By Lemmas 5.1 and 5.3, with $\lambda(d_v) = a^{d_v}$, $T_n := S_n^{(1)} = \sum_\Phi (-1)^{|\Phi|} n^{n-|\Phi|}\,\Lambda_w(\Phi)$ with $w_0 = 1$, $w_1 = a$, where Φ runs over the forests of K_n^* that consist of disjoint paths (a forest contained in a partial derangement has in-degrees at most 1). By Lemma 5.4 only $\Phi = \emptyset$ and the single paths contribute. The empty forest gives $n^n((1+a)^n - na(1+a)^{n-1})$. A path with $r \geq 1$ arcs can be chosen in $(n)_{r+1}$ ways and gives $(-1)^r n^{n-r} \cdot (-a^{r+1}(1+a)^{n-r-1})$. □

For example, $n = 5$ gives $g_5(-1) = 69504$, in agreement with Remark 2.5.

Theorem A.3. *For every prime $p \geq 3$, $g_{p+2}(-1) \equiv p\,K_2(p) \pmod{p^2}$.*

Proof. Let $n = p+2$, so $a = 1/p$ in Theorem A.2. Multiplying by p^{p+2},

$$p^{p+2}T_n = -n^n(p+1)^{p+1} - \sum_{r=1}^{p+1}(n)_{r+1}(-1)^r n^{n-r}(p+1)^{p+1-r}.$$

The term $r = 1$ equals $n(n-1)\,n^{n-1}(p+1)^p = n^n(p+1)^{p+1}$ and cancels the first term. For $2 \leq r \leq p+1$ the falling factorial $(n)_{r+1} = (p+2)(p+1)p(p-1)\cdots(p+2-r)$ contains exactly one factor p, and modulo p the quotient is $2\,(-1)^{r-2}(r-2)!$. Also $n^{n-r} \equiv 2^{p+2-r} \equiv 2^{3-r}$ by Fermat's theorem. Hence

$$\frac{p^{p+2}T_n}{p} \equiv -\sum_{r=2}^{p+1} 2^{4-r}(r-2)! = -4K_2(p) \pmod{p}.$$

By Theorem A.2, $g_n(-1) = -((p-1)!)^{p+1}\,p^{p+2}T_n/(p+2)^2$, and $((p-1)!)^{p+1} \equiv 1$, $(p+2)^2 \equiv 4$ modulo p, which gives the claim. □

Proof of Theorem 1.4. For $n = p+2$, Proposition A.1 and Theorem A.3 give $g_n(1-n) \equiv p\,(K_2(p)-1) \pmod{p^2}$, and $U_n = g_n(1-n)$ since n is odd (Lemma 2.4). Finally $K_2(p) - 1 = \sum_{j=1}^{p-1} j!\,2^{-j}$. □

B Computational details

Independent checks of Theorem 5.5. Theorem 5.5 rests on the classification of the components in Section 5.4, so I checked it by two computations that do not use it.

1. A transfer-matrix computation of the polynomials g_n for $n \le 10$, based on Lemma 2.3 and a decomposition by closing the vertices one at a time. It reproduces the values $(-1)^{\binom{n}{2}} U_n$, $n \le 10$, which Berndsen computed by a different method [5, Table 2.2] (the value for $n = 10$ was new there; U_9 also appears in [27, Table 3]) and which are listed in [22]; in the present sign convention $U_9 = 2086844497920$ and $U_{10} = -27369126116720640000$, and its values $g_n(-2)$, $4 \le n \le 10$, agree with Theorem 5.5.

2. A direct evaluation of the sum in Lemma 5.1 for $k = 2$, where σ runs over representatives of the conjugacy classes of partial derangements (weighted by the class size) and τ over all partial derangements arc-disjoint from σ, with exact integer determinants. This uses only the BEST theorem and Lemma 5.2. It agrees with Theorem 5.5 for $4 \le n \le 12$; for $n = 12$ both give the same 82-digit integer.

The values $n = 11$ and $n = 12$ were not used in finding the formula. Similarly, Theorem A.2 agrees with the transfer-matrix values $g_n(-1)$ for $4 \le n \le 10$, and the reductions of Theorems A.3 and 6.1 agree with the exact values of $g_{p+2}(-1)$ for all $p < 200$ and of $g_{p+3}(-2)$ for all $p < 140$.

Checks of the computations for five layers. I checked the computations behind Theorem 7.13 in several independent ways.

1. The first values are $A_4(N, 1) = 1, 0, 0, 0, 0, 0, 1382400, -663552000, -10450944000$ for $N = 0, \dots, 8$. For $N \le 7$ they agree with a direct enumeration of the quadruples of arc-disjoint derangements with exact determinants ($4.06 \cdot 10^9$ quadruples for $N = 7$), which does not use Theorem 7.4, and for $N = 6$ with Lemma 7.2(3) and $D_6 = -199065600$. The same programs with four indices reproduce the values of $A_2(N, 1)$ obtained by direct enumeration for $N \le 8$.

2. A second evaluation of the pairing, developed and programmed separately, does not use Section 7.4: it averages the distinguished index over all six indices, contracts all blocks other than the pairs, and integrates the pair variables over the singular values of a complex antisymmetric Gaussian matrix, which gives a finite sum with 608 integer coefficients. It leads to the same polynomials N_A, N_B, and to the same values of $A_4(p + 5, 1)$ modulo p^2 for all 27 primes $7 \le p \le 113$.

3. A direct evaluation of $A_4(p + 5, 1)$ modulo p^2 from the 361 weights, without the closed form, agrees with Theorem 7.14 for all 2257 primes $13 \le p \le 20\,000$.

4. The exact value $D_{12} = 2035029864867295940706311266594330749645619200000000$, which I computed separately by a recursion for the coefficients of powers of the determinant that uses no result of this paper, gives $D_{12}/7^3 \equiv 6 \pmod 7$, the entry for $p = 7$ in Table 2. This checks the whole chain from Lemma 7.1 to Theorem 7.14, including Theorem 7.4, at $N = 12$.

The evaluations in items 2 and 3 start from Theorem 7.4, so they guard against errors in the evaluation, not against an error in the pairing formula itself; the latter is checked by the direct enumeration for $N \le 7$ and by item 4.

The terms S_i of Lemma 7.6. For six indices the terms S_i are of three kinds. (i) For every partition τ of $\mathcal{I}$ that has an odd block and no block of size 4 or 6, the term $s\,c_P(\tau)\,\varepsilon(\tau)\,z^\tau$ of P, where $c_P(\tau) = -\mu(\tau)$ is -24, -4, 2, -2, -1, 1 for the types $5+1$, $3+3$, $3+2+1$, $3+1+1+1$, $2+2+1+1$, $2+1+1+1+1$, and 0 if $\{0\}$ is a block. (ii) The terms $t\,\varepsilon(\tau)\,z^\tau$ of Q for the same types and for the type $1+\cdots+1$, except those in which $\{0\}$ is a block (they cannot be paired, since $\theta_{\{0\}}$ does not occur in P). (iii) For each set B of size 4 with complement $\{i,j\}$, the variable y_B occurs in the terms of types $4+2$ and $4+1+1$, with coefficients -6 and 6 in P and 1 and 1 in Q (times the shuffle signs); writing $s\alpha_B y_B$ and $t\beta_B y_B$ for these terms, the contraction gives $e^{st\alpha_B\beta_B}$, whose exponent is $-6st\,|y_{ij}|^2$ plus monomials containing $\theta_{\{i\}}\theta_{\{j\}}$. Each monomial of (i), (ii) and of the non-scalar part of (iii) is one S_i; all are even and square to zero. The elimination of the Grassmann variables expands $\prod_i(1+S_i)$ in this form.

References

[1] Noga Alon and Michael Tarsi. Colorings and orientations of graphs. *Combinatorica*, 12(2):125–134, 1992. doi:10.1007/BF01204715.

[2] Vladica Andrejić, Alin Bostan, and Milos Tatarevic. Improved algorithms for left factorial residues. *Information Processing Letters*, 167:106078, 2021. doi:10.1016/j.ipl.2020.106078.

[3] Daniel Barsky and Bénali Benzaghou. Nombres de Bell et somme de factorielles. *Journal de Théorie des Nombres de Bordeaux*, 16(1):1–17, 2004. doi:10.5802/jtnb.432.

[4] Daniel Barsky and Bénali Benzaghou. Erratum à l'article Nombres de Bell et somme de factorielles. *Journal de Théorie des Nombres de Bordeaux*, 23(2):527, 2011. doi:10.5802/jtnb.775.

[5] Jochem Berndsen. Three problems in algebraic combinatorics. Master's thesis, Eindhoven University of Technology, 2012. URL: https://pure.tue.nl/ws/portalfiles/portal/47046131/739259-1.pdf.

[6] Sergio Caracciolo, Alan D. Sokal, and Andrea Sportiello. Algebraic/combinatorial proofs of Cayley-type identities for derivatives of determinants and pfaffians. *Advances in Applied Mathematics*, 50(4):474–594, 2013. doi:10.1016/j.aam.2012.12.001.

[7] Seth Chaiken. A combinatorial proof of the all minors matrix tree theorem. *SIAM Journal on Algebraic and Discrete Methods*, 3(3):319–329, 1982. doi:10.1137/0603033.

[8] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, volume 12699 of *Lecture Notes in Computer Science*, pages 625–635. Springer, 2021. doi:10.1007/978-3-030-79876-5_37.

[9] Arthur A. Drisko. On the number of even and odd Latin squares of order $p+1$. *Advances in Mathematics*, 128(1):20–35, 1997. doi:10.1006/aima.1997.1623.

[10] Arthur A. Drisko. Proof of the Alon–Tarsi conjecture for $n = 2^r p$. *The Electronic Journal of Combinatorics*, 5:Research Paper 28, 1998. doi:10.37236/1366.

[11] Benjamin Friedman and Sean McGuinness. The Alon–Tarsi conjecture: a perspective on the main results. *Discrete Mathematics*, 342(8):2234–2253, 2019. doi:10.1016/j.disc.2019.04.018.

[12] Ira M. Gessel. Counting Latin rectangles. *Bulletin of the American Mathematical Society (N.S.)*, 16(1):79–82, 1987. doi:10.1090/S0273-0979-1987-15465-6.

[13] Ira M. Gessel. Enumerative applications of symmetric functions. In *Actes du 17e Séminaire Lotharingien de Combinatoire*, volume B17a of *Séminaire Lotharingien de Combinatoire*, pages 5–21. Publ. I.R.M.A. Strasbourg, 1987. URL: https://www.mat.univie.ac.at/~slc/opapers/s17gessel.html.

[14] Ira M. Gessel. Symmetric functions and P-recursiveness. *Journal of Combinatorial Theory, Series A*, 53(2):257–285, 1990. doi:10.1016/0097-3165(90)90060-A.

[15] David G. Glynn. The conjectures of Alon–Tarsi and Rota in dimension prime minus one. *SIAM Journal on Discrete Mathematics*, 24(2):394–399, 2010. doi:10.1137/090773751.

[16] Roger Howe. Remarks on classical invariant theory. *Transactions of the American Mathematical Society*, 313(2):539–570, 1989. doi:10.1090/S0002-9947-1989-0986027-X.

[17] Roger Howe and Tōru Umeda. The Capelli identity, the double commutant theorem, and multiplicity-free actions. *Mathematische Annalen*, 290(1):565–619, 1991. doi:10.1007/BF01459261.

[18] Rosa Huang and Gian-Carlo Rota. On the relations of various conjectures on Latin squares and straightening coefficients. *Discrete Mathematics*, 128(1–3):225–236, 1994. doi:10.1016/0012-365X(94)90114-7.

[19] Jeannette C. M. Janssen. On even and odd Latin squares. *Journal of Combinatorial Theory, Series A*, 69(1):173–181, 1995. doi:10.1016/0097-3165(95)90115-9.

[20] Bertram Kostant and Siddhartha Sahi. The Capelli identity, tube domains, and the generalized Laplace transform. *Advances in Mathematics*, 87(1):71–92, 1991. doi:10.1016/0001-8708(91)90062-C.

[21] Đuro Kurepa. On the left factorial function $!n$. *Mathematica Balkanica*, 1:147–153, 1971.

[22] OEIS Foundation Inc. Sequence A065711, The On-Line Encyclopedia of Integer Sequences. https://oeis.org/A065711. Accessed 13 October 2026.

[23] Hubert Rubenthaler and Gérard Schiffmann. Opérateurs différentiels de Shimura et espaces préhomogènes. *Inventiones Mathematicae*, 90(2):409–442, 1987. doi:10.1007/BF01388712.

[24] Zoran Šami. On generalization of functions $n!$ and $!n$. *Publications de l'Institut Mathématique (Beograd) (N.S.)*, 60(74):5–14, 1997.

[25] Wilfried Schmid. Die Randwerte holomorpher Funktionen auf hermitesch symmetrischen Räumen. *Inventiones Mathematicae*, 9(1):61–80, 1969. doi:10.1007/BF01389889.

[26] Douglas S. Stones and Ian M. Wanless. Divisors of the number of Latin rectangles. *Journal of Combinatorial Theory, Series A*, 117(2):204–215, 2010. doi:10.1016/j.jcta.2009.03.019.

[27] Douglas S. Stones and Ian M. Wanless. How not to prove the Alon–Tarsi conjecture. *Nagoya Mathematical Journal*, 205:1–24, 2012. doi:10.1215/00277630-1543769.

[28] The mathlib Community. The Lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, pages 367–381. ACM, 2020. doi:10.1145/3372885.3373824.

[29] Tatyana van Aardenne-Ehrenfest and Nicolaas G. de Bruijn. Circuits and trees in oriented linear graphs. *Simon Stevin*, 28:203–217, 1951.

[30] David Vere-Jones. A generalization of permanents and determinants. *Linear Algebra and its Applications*, 111:119–124, 1988. doi:10.1016/0024-3795(88)90053-5.

[31] Ian M. Wanless. Cycle switches in Latin squares. *Graphs and Combinatorics*, 20(4):545–570, 2004. doi:10.1007/s00373-004-0567-7.

[32] Paolo Zappa. The Cayley determinant of the determinant tensor and the Alon–Tarsi conjecture. *Advances in Applied Mathematics*, 19(1):31–44, 1997. doi:10.1006/aama.1996.0522.