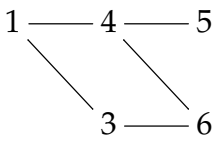
Math 4707 Spring 2018 (Darij Grinberg): homework set 5 with solutions [preliminary version]

Contents

For the notations that we will use, we refer to Spring 2017 Math 5707 Homework set #2 and to classwork. The word "graph" means "multigraph" unless it appears as part of "simple graph". Here are the notations that I did not introduce in class:

- A two-element set $\{u, v\}$ will be denoted by uv when no confusion can arise. This will be mostly used for two-element sets that appear as edges in simple graphs (or as images of edges in multigraphs). For example, the simple graph



  has edges $13, 14, 36, 45, 46$.

- The set of all vertices of a graph G is called the *vertex set* of G, and is denoted by $\mathrm{V}(G)$.

  The set of all edges of a graph G is called the *edge set* of G, and is denoted by $\mathrm{E}(G)$.

- If v is a vertex and e is an edge of a graph (V, E, φ), then we say that v *belongs to* e (or, equivalently, e *contains* v) if v is an endpoint of e (that is, $v \in \varphi(e)$).

0.1. Perfect matchings of a $2 \times n$ grid

Definition 0.1. Let $n \in \mathbb{N}$. Then, the *path graph* P_n is defined to be the simple graph whose vertices are the n numbers $1, 2, \ldots, n$, and whose edges are $\{1,2\}, \{2,3\}, \ldots, \{n-1, n\}$. Here is how it looks like:

$$1 \text{ —— } 2 \text{ —— } \cdots \text{ —— } n$$

Definition 0.2. Let G and H be two simple graphs. The *Cartesian product* of G and H is a new simple graph, denoted $G \times H$, which is defined as follows:

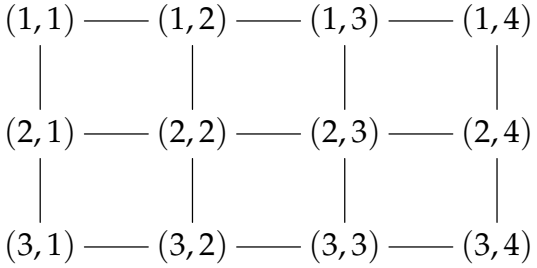
- The vertex set $\mathrm{V}(G \times H)$ of $G \times H$ is the Cartesian product $\mathrm{V}(G) \times \mathrm{V}(H)$. (So the vertices of $G \times H$ are all pairs of the form (v, w), where v is a vertex of G and w is a vertex of H.)
- A vertex (g, h) of $G \times H$ is adjacent to a vertex (g', h') of $G \times H$ if and only if we have

$$\textbf{either } \left(g = g' \text{ and } hh' \in \mathrm{E}(H)\right) \textbf{ or } \left(h = h' \text{ and } gg' \in \mathrm{E}(G)\right).$$

(In particular, exactly one of the two equalities $g = g'$ and $h = h'$ has to hold when (g, h) is adjacent to (g', h').)

Definition 0.3. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. The *grid graph* $G_{n,m}$ is defined to be the Cartesian product $P_n \times P_m$.

Here is how the grid graph $G_{3,4}$ looks like:



(Check that you understand how the definition of a Cartesian product of two graphs causes it to look like this.) For arbitrary $n, m \in \mathbb{N}$, the grid graph $G_{n,m}$ is the simple graph whose vertex set is $[n] \times [m]$, and whose edges have the form

$$\begin{aligned} &(i, j)\,(i+1, j) && \text{for } i \in [n-1] \text{ and } j \in [m], && \text{and} \\ &(i, j)\,(i, j+1) && \text{for } i \in [n] \text{ and } j \in [m-1]. \end{aligned}$$

Two edges of a graph G are said to be *disjoint* if they have no common endpoint. A *matching* of a graph G means a set of disjoint edges of G. A *perfect matching* of a graph G means a matching M of G such that each vertex of G belongs to exactly one edge in M. For example,

$$\{(1,1)\,(1,2),\ (1,3)\,(1,4),\ (2,1)\,(3,1),\ (2,2)\,(2,3),\ (3,2)\,(3,3),\ (2,4)\,(3,4)\}$$

is a perfect matching of the grid graph $G_{3,4}$ shown above; let me visualize this

matching by drawing only the edges of this matching (omitting all the other edges):

$$(1,1) \text{ —— } (1,2) \qquad (1,3) \text{ —— } (1,4)$$

$$\begin{array}{ccccc} (2,1) & & (2,2) \text{ —— } (2,3) & & (2,4) \\ | & & & & | \\ (3,1) & & (3,2) \text{ —— } (3,3) & & (3,4) \end{array}$$

Exercise 1. Let $n \in \mathbb{N}$. How many perfect matchings does the grid graph $G_{2,n}$ have?

[**Hint:** This is something you know in disguise.]

Hints to Exercise 1. We shall use the notations of Exercise 5 on homework set #1. In particular, we recall that $R_{n,2}$ denotes the set $[n] \times [2]$, regarded as a rectangle of width n and height 2. We know from class that the number of domino tilings of $R_{n,2}$ is the Fibonacci number f_{n+1}.

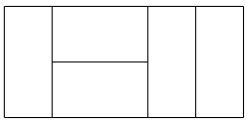
But there is a bijection

$$\{\text{perfect matchings of } G_{2,n}\} \to \{\text{domino tilings of } R_{n,2}\}.$$

(This bijection acts by replacing each edge $(i,j)\,(u,v)$ by the domino $\{(j,i),(v,u)\}$. For example, for $n = 5$, it maps the perfect matching

$$\begin{array}{cccccc} (1,1) & & (1,2) \text{ —— } (1,3) & & (1,4) & (1,5) \\ | & & & & | & | \\ (2,1) & & (2,2) \text{ —— } (2,3) & & (2,4) & (2,5) \end{array}$$

to the domino tiling



.)

This bijection shows that the number of perfect matchings of $G_{2,n}$ is the number of domino tilings of $R_{n,2}$. But the latter number is the Fibonacci number f_{n+1}. Hence, the number of perfect matchings of $G_{2,n}$ is f_{n+1}. □

0.2. Eulerian circuits of a windmill

The concept of a circuit in a graph is somewhat ambiguous: In the graph

$$\begin{array}{ccc} 1 & \overset{a}{\text{——}} & 2 \\ {\scriptstyle d}\,| & \diagdown\, {\scriptstyle c} & |\,{\scriptstyle b} \\ 4 & & 3 \end{array}, \tag{1}$$

do you consider $(1,a,2,b,3,c,1)$ and $(2,b,3,c,1,a,2)$ as the same circuit? What about $(1,a,2,b,3,c,1)$ and $(1,c,3,b,2,a,1)$? According to our definition of a circuit (we defined it as a specific kind of walk), the answer is "no" in both cases:

$$(2,b,3,c,1,a,2) \neq (1,a,2,b,3,c,1) \neq (1,c,3,b,2,a,1)\,.$$

But most people would like to equate $(1,a,2,b,3,c,1)$ with $(2,b,3,c,1,a,2)$, at the very least, since these are "the same circuit with different starting points". So they say "circuit" but really mean "equivalence class of circuits with respect to cyclic rotation (and perhaps mirror reflection)". This is all irrelevant as long as we just discuss the **existence** of circuits; but when we start **counting** circuits, it becomes important. Depending on how circuits are defined, the graph (1) has either 6 or 3 or 2 or 1 cycles (which, as you remember, are circuits satisfying some conditions). According to our definition (which I don't want to change), it has 6 cycles.

Definition 0.4. Let G be a graph.

(a) A walk $(v_0,e_1,v_1,e_2,v_2,\ldots,v_{k-1},e_k,v_k)$ of G is said to be *Eulerian* if each edge of G appears exactly once among the k edges $e_1,e_2,\ldots,e_k$.

(b) Let $\mathbf{w} = (v_0,e_1,v_1,e_2,v_2,\ldots,v_{k-1},e_k,v_k)$ be a walk of G. Then, k is called the *length* of $\mathbf{w}$. If $k>0$, then e_1 is called the *starting edge* of $\mathbf{w}$.

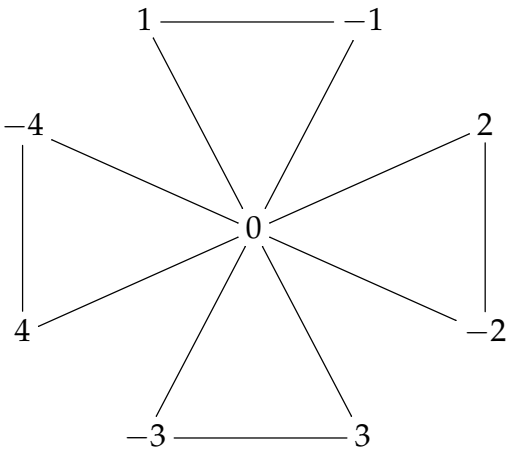
Counting all Eulerian circuits of a graph is usually difficult. For example, the number of Eulerian circuits in a complete graph K_n grows very fast with n and doesn't have a known expression (see sequence A007082 in the OEIS for the values when n is odd; of course, the values when n is even are 0).

Exercise 2. Let g be a positive integer. Let G be the simple graph whose vertices are the $2g+1$ integers $-g,-g+1,\ldots,g-1,g$, and whose edges are

$$\begin{aligned}
&\{0,i\} && \text{for all } i \in \{1,2,\ldots,g\}\,;\\
&\{0,-i\} && \text{for all } i \in \{1,2,\ldots,g\}\,;\\
&\{i,-i\} && \text{for all } i \in \{1,2,\ldots,g\}
\end{aligned}$$

(these are $3g$ edges in total).

[Here is how G looks like in the case when $g=4$:



(2)

]

(a) Find the number of Eulerian circuits of G whose starting point is 0 and whose starting edge is $\{0,1\}$.

(b) Find the number of Eulerian circuits of G whose starting point is 0.

Hints to Exercise 2. We shall refer to the g sets $\{0,1,-1\}$, $\{0,2,-2\}$, $\ldots$, $\{0,g,-g\}$ as the *triangles*.

(b) An Eulerian circuit of G whose starting point is 0 must have the following form: Start at 0, traverse some triangle, come back to 0, traverse another triangle, come back to 0, traverse another triangle, and so on, until each triangle has been traversed exactly once. (No other Eulerian circuits are possible, because there is no way to "escape" a triangle short of fully traversing it.)

Thus, in order to construct an Eulerian circuit of G whose starting point is 0, we need to decide in what order it should traverse the g triangles, and moreover, for each triangle $\{0,i,-i\}$, we need to decide whether it shall traverse it "clockwise" (that is, $0 \to i \to -i \to 0$) or "counterclockwise" (that is, $0 \to -i \to i \to 0$). The first of these decisions can be made in $g!$ many ways; the second in 2^g many ways (since there are two choices for each of the g triangles). Thus, the number of Eulerian circuits of G whose starting point is 0 is $g! \cdot 2^g$.

(a) The number of Eulerian circuits of G whose starting point is 0 and whose starting edge is $\{0,1\}$ is $(g-1)! \cdot 2^{g-1}$. Indeed, the same argument as used for part **(b)** applies here, except that we are somewhat restricted in our decision, since our circuit must begin with the triangle $\{0,1,-1\}$ and it must traverse this triangle "clockwise". □

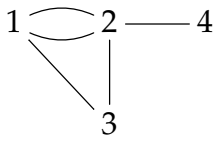
0.3. Counting walks in a graph

A graph always has a finite number of paths (since a path can never have more vertices than the graph has), but usually has an infinite number of walks (indeed, if the graph has a cycle, then you can build arbitrarily long walks by walking along this cycle over and over). Nevertheless, walks are much easier to count than paths. The next exercise states a formula for the number of walks of a given length between two given vertices in terms of the *adjacency matrix* of a graph. This matrix is an important representation of a graph.

Definition 0.5. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let A be an $n \times m$-matrix. Let $i \in [n]$ and $j \in [m]$. Then, $A_{i,j}$ will denote the (i,j)-th entry of A.

Definition 0.6. Let $G = (V, E, \varphi)$ be a graph. Assume that $V = [n]$ for some $n \in \mathbb{N}$. Then, the *adjacency matrix* of G is defined as the $n \times n$-matrix whose (i,j)-th entry (for each $i \in [n]$ and $j \in [n]$) is the number of edges whose endpoints are i and j.

For example, the graph



(3)

has adjacency matrix

$$\begin{pmatrix} 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Clearly, the adjacency matrix of a graph $G = (V, E, \varphi)$ with $V = [n]$ is symmetric. Furthermore, this adjacency matrix "encodes" the whole structure of G apart from the identities of the edges.

Exercise 3. Let $G = (V, E, \varphi)$ be a graph. Assume that $V = [n]$ for some $n \in \mathbb{N}$. Let A be the adjacency matrix of G. Let $i \in [n]$ and $j \in [n]$ and $k \in \mathbb{N}$. Prove that $\left(A^k\right)_{i,j}$ is the number of walks from i to j that have length k.

Exercise 3 is a fundamental result. For example, it appears in [Stanle13, Theorem 1.1]. The simplest proof uses induction:

Solution to Exercise 3 (sketched). Forget that we fixed i, j and k. We want to prove the following claim:

Claim 1: Let $i \in [n]$ and $j \in [n]$ and $k \in \mathbb{N}$. Then,

$$\left(A^k\right)_{i,j} = (\text{the number of walks from } i \text{ to } j \text{ that have length } k).$$

Before we prove this claim, let us recall that A is the adjacency matrix of G. Thus, for each $i \in [n]$ and $j \in [n]$, we have

$$A_{i,j} = (\text{the number of edges whose endpoints are } i \text{ and } j)$$

(by the definition of the adjacency matrix). Renaming i as w in this statement, we obtain the following: For each $w \in [n]$ and $j \in [n]$, we have

$$A_{w,j} = (\text{the number of edges whose endpoints are } w \text{ and } j). \tag{4}$$

Let us also recall that any two $n \times n$-matrices B and C satisfy

$$(BC)_{i,j} = \sum_{w=1}^{n} B_{i,w} C_{w,j} \tag{5}$$

for any $i \in [n]$ and $j \in [n]$. (Indeed, this is just the rule for how matrices are multiplied.)

We can now prove Claim 1:

[*Proof of Claim 1:* We shall prove Claim 1 by induction on k:

Induction base: We shall first prove Claim 1 for $k = 0$.

Indeed, let $i \in [n]$ and $j \in [n]$. For any two objects u and v, we let $\delta_{u,v} = [u = v]$ (where we are using the Iverson bracket notation). Then, the $n \times n$ identity matrix I_n satisfies $(I_n)_{i,j} = \delta_{i,j}$ (by the definition of the identity matrix). Hence, $(I_n)_{i,j} = \delta_{i,j} = [i = j]$ (by the definition of $\delta_{i,j}$). But the 0-th power of any $n \times n$-matrix is defined to be the $n \times n$ identity matrix I_n; thus, $A^0 = I_n$. Hence, $\left(A^0\right)_{i,j} = (I_n)_{i,j} = [i = j]$.

On the other hand, how many walks from i to j have length 0 ? A walk that has length 0 must consist of a single vertex, which is simultaneously the starting point and the ending point of this walk. Thus, a walk from i to j that has length 0 exists only when $i = j$, and in this case there is exactly one such walk (namely, the walk (i)). Hence,

$$(\text{the number of walks from } i \text{ to } j \text{ that have length } 0) = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j \end{cases} = [i = j] .$$

Comparing this with the equality $\left(A^0\right)_{i,j} = [i = j]$, we conclude that

$$\left(A^0\right)_{i,j} = (\text{the number of walks from } i \text{ to } j \text{ that have length } 0) . \tag{6}$$

Now, forget that we fixed i and j. We thus have proven (6) for any $i \in [n]$ and $j \in [n]$. In other words, Claim 1 holds for $k = 0$. Thus, the induction base is complete.

Induction step: Let g be a positive integer. Assume that Claim 1 holds for $k = g - 1$. We must show that Claim 1 holds for $k = g$ as well.

We have assumed that Claim 1 holds for $k = g - 1$. In other words, for any $i \in [n]$ and $j \in [n]$, we have

$$\left(A^{g-1}\right)_{i,j} = (\text{the number of walks from } i \text{ to } j \text{ that have length } g - 1) .$$

Renaming j as w in this statement, we obtain the following: For any $i \in [n]$ and $w \in [n]$, we have

$$\left(A^{g-1}\right)_{i,w} = (\text{the number of walks from } i \text{ to } w \text{ that have length } g - 1) . \tag{7}$$

Each walk from i to j that has length g has the form $\left(v_0, e_1, v_1, e_2, v_2, \ldots, e_{g-1}, v_{g-1}, e_g, v_g\right)$ for some vertices $v_0, v_1, \ldots, v_g$ of G and some edges $e_1, e_2, \ldots, e_g$ of G satisfying $v_0 = i$, $v_g = j$ and $(\varphi(e_h) = \{v_{h-1}, v_h\}$ for all $h \in [g])$. Thus, each such walk can be constructed by the following algorithm:

- First, we choose a vertex w of G to serve as the vertex v_{g-1} (that is, as the penultimate vertex of the walk). This vertex w must belong to $V = [n]$.

- Now, we choose the vertices $v_0, v_1, \ldots, v_{g-1}$ (that is, all vertices of our walk except for the last one) and the edges $e_1, e_2, \ldots, e_{g-1}$ (that is, all edges of our walk except for the last one) in such a way that $v_{g-1} = w$. This is tantamount to choosing a walk $\left(v_0, e_1, v_1, e_2, v_2, \ldots, e_{g-1}, v_{g-1}\right)$ from i to w that has length $g-1$. This choice can be made in $\left(A^{g-1}\right)_{i,w}$ many ways (because (7) shows that the number of walks from i to w that have length $g-1$ is $\left(A^{g-1}\right)_{i,w}$).
- We have now determined all but the last vertex and all but the last edge of our walk $\left(v_0, e_1, v_1, e_2, v_2, \ldots, e_g, v_g\right)$. We set the last vertex v_g of our walk to be j. (This is the only possible option, since our walk $\left(v_0, e_1, v_1, e_2, v_2, \ldots, e_{g-1}, v_{g-1}, e_g, v_g\right)$ has to be a walk from i to j.)
- We choose the last edge e_g of our walk. This edge e_g must have endpoints v_{g-1} and v_g; in other words, it must have endpoints w and j (since $v_{g-1} = w$ and $v_g = j$). Thus, we need to choose an edge whose endpoints are w and j. This choice can be made in $A_{w,j}$ many ways (because (4) shows that the number of edges whose endpoints are w and j is $A_{w,j}$).

Conversely, of course, this algorithm always constructs a walk from i to j that has length g, and different choices in the algorithm lead to distinct walks. Thus, the total number of walks from i to j that have length g equals the total number of choices in the algorithm. But the latter number is $\sum\limits_{w \in [n]} \left(A^{g-1}\right)_{i,w} A_{w,j}$ (since the algorithm first chooses a $w \in [n]$, then involves a step with $\left(A^{g-1}\right)_{i,w}$ choices, and then involves a step with $A_{w,j}$ choices). Hence, the total number of walks from i to j that have length g is $\sum\limits_{w \in [n]} \left(A^{g-1}\right)_{i,w} A_{w,j}$. In other words,

$$\left(\text{the number of walks from } i \text{ to } j \text{ that have length } g\right) = \sum_{w \in [n]} \left(A^{g-1}\right)_{i,w} A_{w,j}.$$

Comparing this with

$$\begin{aligned}
\left(\underbrace{A^g}_{=A^{g-1}A}\right)_{i,j} &= \left(A^{g-1}A\right)_{i,j} = \sum_{w=1}^{n} \left(A^{g-1}\right)_{i,w} A_{w,j} \\
&\qquad \Big(\text{by (5) (applied to } B = A^{g-1} \text{ and } C = A)\Big) \\
&= \sum_{w \in [n]} \left(A^{g-1}\right)_{i,w} A_{w,j},
\end{aligned}$$

we obtain

$$\left(A^g\right)_{i,j} = \left(\text{the number of walks from } i \text{ to } j \text{ that have length } g\right). \tag{8}$$

Now, forget that we fixed i and j. We thus have proven (8) for any $i \in [n]$ and $j \in [n]$. In other words, Claim 1 holds for $k = g$. Thus, the induction step is complete. Hence, Claim 1 is proven by induction.]

Exercise 3 follows immediately from Claim 1. □

Remark 0.7. There is an analogue of Exercise 3 for multidigraphs. If D is a multidigraph with vertices $1, 2, \ldots, n$, then the *adjacency matrix* A of D is defined to be the $n \times n$-matrix whose (i, j)-th entry (for each $i \in [n]$ and $j \in [n]$) is the number of arcs with source i and target j. In general, this adjacency matrix A is not symmetric. Now, if $D = (V, A, \phi)$ is a multidigraph with $V = [n]$ for some $n \in \mathbb{N}$ and with adjacency matrix A, and if $i \in [n]$ and $j \in [n]$ and $k \in \mathbb{N}$ are arbitrary, then $\left(A^k\right)_{i,j}$ is the number of walks from i to j that have length k. The proof of this is completely analogous to the solution of Exercise 3.

0.4. Your friends have more friends than you (the "friendship paradox")

If G is a graph, and if v is a vertex of G, then $\deg v$ denotes the degree of v (that is, the number of edges of G that contain v).

Exercise 4. Let $G = (V, E, \varphi)$ be a graph.

If $v \in V$ and $e \in E$ are such that $v \in \varphi(e)$ (that is, the edge e contains the vertex v), then we let e/v denote the endpoint of e distinct from v. For each $v \in V$, we define a rational number q_v by

$$q_v = \sum_{\substack{e \in E; \\ v \in \varphi(e)}} \frac{\deg(e/v)}{\deg v}.$$

(Note that the denominator $\deg v$ on the right hand side is nonzero whenever the sum is nonempty!)

[Roughly speaking, q_v is the average degree of the neighbors of v. But to be more precise, this is an average over all **edges** containing v, not just over all **neighbors** of v; the degree of a neighbor of v will factor in the stronger the more edges join this neighbor to v. When v is an isolated vertex – i.e., when $\deg v = 0$ –, the number q_v is 0.]

Prove that

$$\sum_{v \in V} q_v \geq \sum_{v \in V} \deg v. \tag{9}$$

If the graph G is a social network (vertices being people, and edges being friendships), then the inequality (9) (when divided by $|V|$) can be construed as saying "the average person is unpopular", where being "unpopular" means that your average friend has at least as many friends as you do. This is a slippery statement

(involving an average within an average) and needs to be interpreted correctly: For example, in the graph (2), the vertex 0 has degree 8, while all other vertices have degree 2; the corresponding numbers q_v are $q_0 = 2$ and $q_v = 5$ (for $v \neq 0$), respectively. Thus, (9) says that

$$2+5+5+5+5+5+5+5+5 \geq 8+2+2+2+2+2+2+2+2,$$

which indeed holds (fairly strongly). The vertex 0, of course, is popular (having $\deg 0 = 8$ friends, whereas its average friend has $q_0 = 2$ friends), but this is balanced out by the unpopularity of all the other vertices.

Note that (9) does **not** mean that most vertices are unpopular. For example, if G is the simple graph with 5 vertices $1,2,3,4,5$ and all the $\binom{5}{2} = 10$ possible edges between them except for the edge $\{4,5\}$, then the vertices $1,2,3$ of G are popular (a majority), while the vertices $4,5$ are unpopular. Nevertheless, (9) holds here, since the popularity of $1,2,3$ "outweighs" the unpopularity of $4,5$ when the appropriate averages are added. See the Wikipedia page for the friendship paradox for further discussion.

The solution to Exercise 4 relies on the following basic inequality:

Lemma 0.8. Let x and y be two positive reals. Then, $\dfrac{x}{y} + \dfrac{y}{x} \geq 2$.

Proof of Lemma 0.8. Straightforward computations reveal that $\dfrac{x}{y} + \dfrac{y}{x} - 2 = \dfrac{(x-y)^2}{xy}$. But $(x-y)^2 \geq 0$ (since the square of a real number is always ≥ 0), and thus $\dfrac{(x-y)^2}{xy} \geq 0$ (since x and y are positive). Thus, $\dfrac{x}{y} + \dfrac{y}{x} - 2 = \dfrac{(x-y)^2}{xy} \geq 0$, so that $\dfrac{x}{y} + \dfrac{y}{x} \geq 2$. This proves Lemma 0.8. □

Solution to Exercise 4 (sketched). We first observe that every $e \in E$ satisfies

$$\sum_{v \in \varphi(e)} \frac{\deg(e/v)}{\deg v} \geq 2. \tag{10}$$

[*Proof of (10):* Let $e \in E$. Recall that $\varphi(e)$ is a 2-element subset of V. Thus, we can write $\varphi(e)$ in the form $\varphi(e) = \{p, q\}$ for two distinct elements p and q of V. Consider these p and q. Thus, p and q are the endpoints of the edge e. Hence, $e/p = q$ (due to how we defined e/p) and $e/q = p$ (similarly). Also, the vertex p of V belongs to at least one edge (namely, to the edge e); thus, its degree is ≥ 1. In other words, $\deg p \geq 1 > 0$. Similarly, $\deg q > 0$. Thus, Lemma 0.8 (applied to $x = \deg q$ and $y = \deg p$) yields $\dfrac{\deg q}{\deg p} + \dfrac{\deg p}{\deg q} \geq 2$.

But recall that $\varphi(e) = \{p, q\}$, with p and q being distinct. Hence,

$$\begin{aligned}\sum_{v \in \varphi(e)} \frac{\deg(e/v)}{\deg v} &= \frac{\deg(e/p)}{\deg p} + \frac{\deg(e/q)}{\deg q} \\ &= \frac{\deg q}{\deg p} + \frac{\deg p}{\deg q} \qquad (\text{since } e/p = q \text{ and } e/q = p) \\ &\geq 2.\end{aligned}$$

This proves (10).]

On the other hand, the handshaking lemma (Proposition 6.3 in the classwork from April 2nd) yields

$$\sum_{v \in V} \deg v = 2|E|. \tag{11}$$

Now,

$$\begin{aligned}\sum_{v \in V} \underbrace{q_v}_{\substack{= \sum\limits_{\substack{e \in E; \\ v \in \varphi(e)}} \frac{\deg(e/v)}{\deg v} \\ (\text{by the definition of } q_v)}} &= \underbrace{\sum_{v \in V} \sum_{\substack{e \in E; \\ v \in \varphi(e)}} \frac{\deg(e/v)}{\deg v}}_{= \sum\limits_{e \in E} \sum\limits_{\substack{v \in V; \\ v \in \varphi(e)}}} = \sum_{e \in E} \underbrace{\sum_{\substack{v \in V; \\ v \in \varphi(e)}} \frac{\deg(e/v)}{\deg v}}_{\substack{= \sum\limits_{v \in \varphi(e)} \\ (\text{since } \varphi(e) \text{ is a subset of } V)}} \\ &= \sum_{e \in E} \underbrace{\sum_{v \in \varphi(e)} \frac{\deg(e/v)}{\deg v}}_{\substack{\geq 2 \\ (\text{by (10)})}} \geq \sum_{e \in E} 2 = |E| \cdot 2 = 2|E| = \sum_{v \in V} \deg v\end{aligned}$$

(by (11)). This solves Exercise 4. □

0.5. When do transpositions generate all permutations?

Exercise 5. Let $G = (V, E, \varphi)$ be a connected graph.

For each $e = \{u, v\} \in \mathcal{P}_2(V)$, we let t_e be the permutation of V that swaps u with v while leaving all other elements of V unchanged.

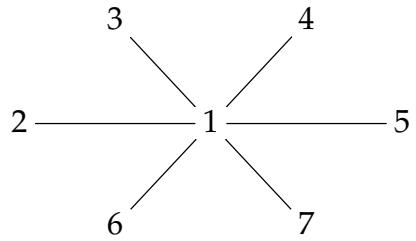
An *E-transposition* shall mean a permutation of the form t_e for some $e \in \varphi(E)$.

Prove that every permutation of V can be written as a composition of some E-transpositions.

Remark 0.9. In Exercise 5, we can WLOG assume (by relabeling the vertices) that $V = [n]$ for some $n \in \mathbb{N}$. Thus, Exercise 5 makes a statement about permutations of $[n]$.

For instance, if we apply Exercise 5 to the connected simple graph $P_n = ([n], \{\{1,2\}, \{2,3\}, \ldots, \{n-1,n\}\})$ (for some $n > 0$), then we obtain the well-known fact that every permutation of $[n]$ can be written as a composition of some simple transpositions (because the E-transpositions in this case are precisely the simple transpositions $s_1, s_2, \ldots, s_{n-1}$).

For another example, we can apply Exercise 5 to the connected simple graph $([n], \{\{1,2\}, \{1,3\}, \ldots, \{1,n\}\})$ (for some $n > 0$); this graph is called a "star", because here is how it looks like for $n = 7$:



Thus, Exercise 5 shows that every permutation of $[n]$ can be written as a composition of some transpositions, each of which swaps 1 with one of the numbers $2, 3, \ldots, n$. (This fact was Exercise 3 on Fall 2017 Math 4990 homework set #7.)

Exercise 5 also has a converse: If $G = (V, E, \varphi)$ is a graph such that every permutation of V can be written as a composition of some E-transpositions, then G is connected or V is empty. This is not hard to prove[1].

Our solution of Exercise 5 relies on the following notation:

Definition 0.10. Let V be any set. Let u and v be two distinct elements of V. Then, $t_{u,v}$ shall denote the permutation of V that swaps u with v while leaving all other elements of V unchanged. This permutation $t_{u,v}$ is called a *transposition* of V.

Lemma 0.11. Let V be a set. Let i, p and q be three distinct elements of V. Then,

$$t_{i,q} = t_{p,q} \circ t_{i,p} \circ t_{p,q}.$$

Proof of Lemma 0.11 (sketched). This is straightforward: We just need to show that $t_{i,q}(x) = \left(t_{p,q} \circ t_{i,p} \circ t_{p,q}\right)(x)$ for each $x \in V$. This can be shown by considering the cases $x = i$, $x = p$, $x = q$ and $x \notin \{i, p, q\}$ separately; in the first three cases, the verification is a straightforward computation, whereas in the fourth case, the claim follows from $t_{i,q}(x) = x$ and $\left(t_{p,q} \circ t_{i,p} \circ t_{p,q}\right)(x) = x$. □

[1] *Hint:* Show that if a composition of some E-transpositions maps a vertex $u \in V$ to a vertex $v \in V$, then there exists a walk from u to v in G.

Solution to Exercise 5 (sketched). Recall that every permutation of V is a composition of transpositions[2]. We now focus on proving the following fact:

> *Statement 1:* Let i and j be two distinct elements of V. Then, the transposition $t_{i,j}$ of V can be written as a composition of some E-transpositions.

[*Proof of Statement 1:* Since G is connected, there is a path $\left(k_0, e_1, k_1, \ldots, e_p, k_p\right)$ from i to j in G (with $k_0 = i$ and $k_p = j$). Consider such a path. For each $r \in [p]$, the transposition t_{k_{r-1},k_r} is an E-transposition (since it can be written as t_{e_r}). Thus, in particular, t_{k_0,k_1} is an E-transposition. Note that the path $\left(k_0, e_1, k_1, \ldots, e_p, k_p\right)$ has length > 0 (since $i \neq j$). In other words, $p > 0$. Hence, $p \in [p]$.

We *claim* that t_{i,k_r} is a composition of some E-transpositions for each $r \in \{1, 2, \ldots, p\}$. Indeed, this can be proven by induction on r: The base case ($r = 1$) is clear, since $t_{i,k_1} = t_{k_0,k_1}$ is itself an E-transposition. For the induction step, let $r \in \{1, 2, \ldots, p\}$ be such that $r > 1$, and assume that $t_{i,k_{r-1}}$ is a composition of some E-transpositions; we must show that t_{i,k_r} is a composition of some E-transpositions. But the vertices k_0, k_{r-1}, k_r of V are distinct (since they are three different vertices of the path $\left(k_0, e_1, k_1, \ldots, e_p, k_p\right)$). In other words, the vertices i, k_{r-1}, k_r of V are distinct (since $k_0 = i$). Hence, Lemma 0.11 (applied to k_{r-1} and k_r instead of p and q) yields $t_{i,k_r} = t_{k_{r-1},k_r} \circ t_{i,k_{r-1}} \circ t_{k_{r-1},k_r}$. But the right hand side of this equality is a composition of some E-transpositions (since $t_{i,k_{r-1}}$ is a composition of some E-transpositions, whereas t_{k_{r-1},k_r} is itself an E-transposition). Hence, so is the left hand side. In other words, t_{i,k_r} is a composition of some E-transpositions. That completes the induction. Now, applying our claim to $r = p$, we conclude that t_{i,k_p} is a composition of some E-transpositions. Since $k_p = j$, this means that $t_{i,j}$ is a composition of some E-transpositions. This proves Statement 1.]

Statement 1 shows that each transposition of V can be written as a composition of some E-transpositions. We thus know that every permutation of V is a composition of transpositions, each of which can in turn be written as a composition of some E-transpositions. Hence, every permutation of V is a composition of compositions of E-transpositions. But this means that every permutation of V can be written as a composition of E-transpositions. This solves Exercise 5. □

0.6. Latin rectangles and squares

Definition 0.12. Let $n \in \mathbb{N}$ and $r \in \mathbb{N}$. A *Latin $r \times n$-rectangle* is an $r \times n$-matrix with the following properties:

- Each row contains the integers $1, 2, \ldots, n$ in some order.
- No number appears more than once in a column.

[2]This is proven, e.g., in [Grinbe16, Exercise 5.15 **(b)**] (but also follows easily from what we have done in class).

For example, $\begin{pmatrix} 1 & 4 & 2 & 3 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ is a Latin 2×4-rectangle, and $\begin{pmatrix} 4 & 3 & 1 & 5 & 2 \\ 1 & 2 & 5 & 4 & 3 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$ is a Latin 3×5-rectangle, whereas $\begin{pmatrix} 1 & 4 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ is not a Latin 2×4-rectangle (as the number 1 appears twice in the first column) and $\begin{pmatrix} 1 & 3 & 2 \\ 2 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ is not a Latin 3×3-rectangle (since the second row is $2, 2, 3$, which is not a rearrangement of $1, 2, 3$).

Clearly, a Latin $r \times n$-rectangle can only exist if $r \leq n$.

Definition 0.13. Let $n \in \mathbb{N}$. A *Latin square of size n* means a Latin $n \times n$-rectangle.

Latin squares are another classical combinatorial object whose number has not been expressed to a reasonable standard; see the Wikipedia page for what is known and why people care.

Exercise 6. Let $r \in \mathbb{N}$ and $n \in \mathbb{N}$ be such that $r \leq n$. Let A be a Latin $r \times n$-rectangle. Show that A can be extended to a Latin square of size n by appending $n - r$ extra rows.

[**Hint:** By induction, it suffices to show that, as long as $r < n$, you can extend A to a Latin $(r+1) \times n$-rectangle by appending one extra row. You can use Hall's marriage theorem without proof here, even though we have not shown it in class.]

Exercise 6 is a famous result in the theory of Latin squares, due to Marshall Hall in 1945 (see [Hall45]). His proof derives it rather quickly from Hall's marriage theorem (restated in terms of systems of distinct representatives). For a readable writeup of this proof, see [Bartle12, Latin Squares, Lecture 2, §2.2]. Note that the Hall who discovered Hall's marriage theorem is a Philip Hall; thus, it makes sense to call Exercise 6 the "Hall-Hall theorem".

See [HilVau11, Theorem 1] for a generalization (from which you can obtain Exercise 6 by setting $s = n$ and observing that $\nu(\sigma) = r$).

0.7. Latin squares and signs

Exercise 7. Let $n \in \mathbb{N}$. Let A be a Latin square of size n. Recall Definition 0.5.

For each $i \in [n]$, let r_i be the permutation of $[n]$ whose one-line notation is the i-th row of A (that is, which satisfies $r_i(j) = A_{i,j}$ for each $j \in [n]$).

For each $j \in [n]$, let c_j be the permutation of $[n]$ whose one-line notation is the j-th column of A (that is, which satisfies $c_j(i) = A_{i,j}$ for each $i \in [n]$).

For each $k \in [n]$, let z_k be the permutation of $[n]$ such that for each $i \in [n]$, we have $A_{i,z_k(i)} = k$. (Thus, the permutation z_k sends each $i \in [n]$ to the position of

the entry k in the i-th row of A. This is indeed a permutation, as follows easily from the definition of a Latin square and from the pigeonhole principle.)

Prove that

$$\left(\prod_{i=1}^{n}(-1)^{r_i}\right)\left(\prod_{j=1}^{n}(-1)^{c_j}\right)\left(\prod_{k=1}^{n}(-1)^{z_k}\right) = (-1)^{n(n-1)/2}.$$

Example 0.14. For this example, let $n = 4$ and $A = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 2 & 1 & 3 & 4 \end{pmatrix}$. Then, A is a Latin square of size 4. The permutations r_i, c_j, z_k of Exercise 7 then look as follows in one-line notation:

$$\begin{array}{llll} r_1 = [4,3,1,2], & r_2 = [1,2,4,3], & r_3 = [3,4,2,1], & r_4 = [2,1,3,4]; \\ c_1 = [4,1,3,2], & c_2 = [3,2,4,1], & c_3 = [1,4,2,3], & c_4 = [2,3,1,4]; \\ z_1 = [3,1,4,2], & z_2 = [4,2,3,1], & z_3 = [2,4,1,3], & z_4 = [1,3,2,4]. \end{array}$$

Exercise 7 is Wilson's sign identity for Latin squares. For solutions, see [Glynn10, proof of Theorem 2.1], [Jansse95, proof of Theorem 3.2] or [Bernds12, proof of Theorem 2.4].

Hints to Exercise 7. Step 1: Let us introduce some notations.

Let S be the set of all triples $\left(i, j, A_{i,j}\right) \in [n]^3$ for $i \in [n]$ and $j \in [n]$. In other words,

$$S = \left\{(i,j,k) \in [n]^3 \mid k = A_{i,j}\right\}.$$

Notice that you can visualize the set $[n]^3$ as an $n \times n \times n$-cube built out of $1 \times 1 \times 1$-blocks – like a Rubik's cube –, and then S is a set of n^2 blocks of this cube such that each strip parallel to one of the three coordinate axes contains exactly one block from S. In other words, if you fix two entries of a triple $(i,j,k) \in [n]^3$, then there exists exactly one value for the third entry that causes the triple to belong to S. More precisely:

- For each pair $(i,j) \in [n]^2$, there is exactly one $k \in [n]$ such that $(i,j,k) \in S$. (Namely, this k is $A_{i,j}$.)
- For each pair $(i,k) \in [n]^2$, there is exactly one $j \in [n]$ such that $(i,j,k) \in S$. (This j is the index of the entry k in the i-th row of A; in other words, j is such that $A_{i,j} = k$.)

- For each pair $(j,k) \in [n]^2$, there is exactly one $i \in [n]$ such that $(i,j,k) \in S$. (This i is the index of the entry k in the j-th column of A; in other words, i is such that $A_{i,j} = k$.)

(Notice that these three conditions characterize sets $S \subseteq [n]^3$ that come from Latin squares; thus, they can be viewed as a more symmetric definition of a Latin square.)

Now, whenever α, β and γ are three binary relations on the set $[n]$ (for example, α can be any of the relations $=$, $<$, $>$ and $\neq$, and so can be β and γ), we define the set $N(\alpha,\beta,\gamma)$ by

$$N(\alpha,\beta,\gamma) = \left\{ \left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x \alpha x' \text{ and } y \beta y' \text{ and } z \gamma z' \right\}.$$

For example,

$$N(<,>,=) = \left\{ \left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x < x' \text{ and } y > y' \text{ and } z = z' \right\}$$

and

$$N(>,=,=) = \left\{ \left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x > x' \text{ and } y = y' \text{ and } z = z' \right\}.$$

Step 2: We have

$$|N(<,<,>)| = |N(>,>,<)| \quad \text{and} \tag{12}$$
$$|N(<,>,<)| = |N(>,<,>)| \quad \text{and} \tag{13}$$
$$|N(>,<,<)| = |N(<,>,>)|. \tag{14}$$

[*Proof:* The map

$$N(<,<,>) \to N(>,>,<),$$
$$\left((x,y,z),\left(x',y',z'\right)\right) \mapsto \left(\left(x',y',z'\right),(x,y,z)\right)$$

is a bijection. Thus, $|N(<,<,>)| = |N(>,>,<)|$. Similarly, $|N(<,>,<)| = |N(>,<,>)|$ and $|N(>,<,<)| = |N(<,>,>)|$.]

Step 3: Let $*$ be the binary relation on $[n]$ such that **every** pair (i,j) satisfies $i * j$. (The "joker relation".) Show that

$$|N(*,<,>)| = \left(n(n-1)/2\right)^2 \quad \text{and} \tag{15}$$
$$|N(<,>,*)| = \left(n(n-1)/2\right)^2 \quad \text{and} \tag{16}$$
$$|N(>,*,<)| = \left(n(n-1)/2\right)^2. \tag{17}$$

[*Proof:* The definition of $N(*,<,>)$ yields

$$\begin{aligned} &N(*,<,>) \\ &= \left\{ \left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid \underbrace{x * x'}_{\substack{\text{this always} \\ \text{holds}}} \text{ and } y < y' \text{ and } z > z' \right\} \\ &= \left\{ \left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid y < y' \text{ and } z > z' \right\}. \end{aligned} \tag{18}$$

Thus, the elements of $N(*,<,>)$ are simply the pairs $((x,y,z),(x',y',z')) \in S \times S$ satisfying $y < y'$ and $z > z'$. We can construct any such pair by the following algorithm:

- Choose two elements $y, y' \in [n]$ satisfying $y < y'$. Note that there are $\binom{n}{2} = n(n-1)/2$ ways to do this.
- Then choose $z, z' \in [n]$ satisfying $z > z'$. Again, there are $\binom{n}{2} = n(n-1)/2$ ways to do this.
- Find the unique $x \in [n]$ such that $(x,y,z) \in S$. (This is indeed unique, because for each pair $(j,k) \in [n]^2$, there is exactly one $i \in [n]$ such that $(i,j,k) \in S$.)
- Find the unique $x' \in [n]$ such that $(x',y',z') \in S$. (Again, this is unique for the same reason.)

Hence, altogether, there are $(n(n-1)/2)^2$ such pairs (because we had $n(n-1)/2$ choices in the first step of the above algorithm, and then again $n(n-1)/2$ choices in the second step, and no further choices). Thus,

$$\left|\left\{\left((x,y,z),(x',y',z')\right) \in S \times S \mid y < y' \text{ and } z > z'\right\}\right| = (n(n-1)/2)^2.$$

In view of (18), this rewrites as $|N(*,<,>)| = (n(n-1)/2)^2$. This proves (15). Similarly, (16) and (17) can be shown.]

Step 4: We have

$$|N(=,<,>)| + |N(<,<,>)| + |N(>,<,>)| = |N(*,<,>)|; \tag{19}$$
$$|N(>,=,<)| + |N(>,<,<)| + |N(>,>,<)| = |N(>,*,<)|; \tag{20}$$
$$|N(<,>,=)| + |N(<,>,<)| + |N(<,>,>)| = |N(<,>,*)|. \tag{21}$$

[*Proof:* The definition of $N(*,<,>)$ yields

$$\begin{aligned} & N(*,<,>) \\ &= \left\{ \left((x,y,z),(x',y',z')\right) \in S \times S \mid \underbrace{x * x'}_{\substack{\text{this always} \\ \text{holds}}} \text{ and } y < y' \text{ and } z > z' \right\} \\ &= \left\{\left((x,y,z),(x',y',z')\right) \in S \times S \mid y < y' \text{ and } z > z'\right\}. \end{aligned}$$

Clearly, each element $((x,y,z),(x',y',z'))$ of $N(*,<,>)$ satisfies either $x = x'$ or $x < x'$ or $x > x'$ (but not more than one of these relations); and, correspondingly, it belongs to either $N(=,<,>)$ or $N(<,<,>)$ or $N(>,<,>)$. Thus, the set

$N(*,<,>)$ is the union of its three disjoint subsets $N(=,<,>)$, $N(<,<,>)$ and $N(>,<,>)$. Hence,

$$|N(*,<,>)| = |N(=,<,>)| + |N(<,<,>)| + |N(>,<,>)|.$$

This proves (19). Analogous arguments prove (20) and (21).]

Step 5: Adding the equalities (19), (20) and (21) together, we obtain

$$\begin{aligned}
&|N(=,<,>)| + |N(<,<,>)| + |N(>,<,>)| \\
&\quad + |N(>,=,<)| + |N(>,<,<)| + |N(>,>,<)| \\
&\quad + |N(<,>,=)| + |N(<,>,<)| + |N(<,>,>)| \\
&= \underbrace{|N(*,<,>)|}_{\substack{=(n(n-1)/2)^2 \\ \text{(by (15))}}} + \underbrace{|N(>,*,<)|}_{\substack{=(n(n-1)/2)^2 \\ \text{(by (17))}}} + \underbrace{|N(<,>,*)|}_{\substack{=(n(n-1)/2)^2 \\ \text{(by (16))}}} \\
&= (n(n-1)/2)^2 + (n(n-1)/2)^2 + (n(n-1)/2)^2 \\
&= 3(n(n-1)/2)^2 \equiv (n(n-1)/2)^2 \equiv n(n-1)/2 \bmod 2
\end{aligned}$$

(since $m^2 \equiv m \bmod 2$ for each integer m (because $\dfrac{m^2-m}{2} = \dbinom{m}{2}$ is an integer)). Comparing this with

$$\begin{aligned}
&|N(=,<,>)| + \underbrace{|N(<,<,>)|}_{\substack{=|N(>,>,<)| \\ \text{(by (12))}}} + |N(>,<,>)| \\
&\quad + |N(>,=,<)| + \underbrace{|N(>,<,<)|}_{\substack{=|N(<,>,>)| \\ \text{(by (14))}}} + |N(>,>,<)| \\
&\quad + |N(<,>,=)| + \underbrace{|N(<,>,<)|}_{\substack{=|N(>,<,>)| \\ \text{(by (13))}}} + |N(<,>,>)| \\
&= |N(=,<,>)| + |N(>,>,<)| + |N(>,<,>)| \\
&\quad + |N(>,=,<)| + |N(<,>,>)| + |N(>,>,<)| \\
&\quad + |N(<,>,=)| + |N(>,<,>)| + |N(<,>,>)| \\
&= |N(=,<,>)| + |N(<,>,=)| + |N(>,=,<)| \\
&\quad + 2(|N(>,>,<)| + |N(>,<,>)| + |N(<,>,>)|) \\
&\equiv |N(=,<,>)| + |N(<,>,=)| + |N(>,=,<)| \bmod 2,
\end{aligned}$$

we obtain

$$\begin{aligned}
&|N(=,<,>)| + |N(<,>,=)| + |N(>,=,<)| \\
&\equiv n(n-1)/2 \bmod 2. \qquad (22)
\end{aligned}$$

Step 6: We have

$$\prod_{i=1}^{n}(-1)^{r_i} = (-1)^{|N(=,<,>)|} \qquad \text{and} \tag{23}$$

$$\prod_{j=1}^{n}(-1)^{c_j} = (-1)^{|N(>,=,<)|} \qquad \text{and} \tag{24}$$

$$\prod_{k=1}^{n}(-1)^{z_k} = (-1)^{|N(<,>,=)|}. \tag{25}$$

[*Proof:* We begin by proving (23). For each $i \in [n]$, the length $\ell(r_i)$ of the permutation $r_i \in S_n$ is given by

$$\begin{aligned}
\ell(r_i) &= (\text{the number of inversions of } r_i) \\
&\qquad (\text{by the definition of the length of a permutation}) \\
&= \Big(\text{the number of all } (u,v) \in [n]^2 \text{ satisfying } u < v \text{ and } r_i(u) > r_i(v)\Big) \\
&\qquad (\text{by the definition of an inversion}) \\
&= \left|\left\{(u,v) \in [n]^2 \mid u < v \text{ and } r_i(u) > r_i(v)\right\}\right| \\
&= \left|\left\{(y,y') \in [n]^2 \mid y < y' \text{ and } r_i(y) > r_i(y')\right\}\right|
\end{aligned} \tag{26}$$

(here, we have renamed the index (u,v) as (y,y')).

But

$$N(=,<,>) = \left\{\left((x,y,z),(x',y',z')\right) \in S \times S \mid x = x' \text{ and } y < y' \text{ and } z > z'\right\}$$

and thus

$$\begin{aligned}
&|N(=,<,>)| \\
&= \left|\left\{\left((x,y,z),(x',y',z')\right) \in S \times S \mid x = x' \text{ and } y < y' \text{ and } z > z'\right\}\right| \\
&= \sum_{i \in [n]} \left|\left\{\left((x,y,z),(x',y',z')\right) \in S \times S \mid x = x' = i \text{ and } y < y' \text{ and } z > z'\right\}\right|.
\end{aligned} \tag{27}$$

But each $i \in [n]$ satisfies

$$\begin{aligned}
&\left|\left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x = x' = i \text{ and } y < y' \text{ and } z > z'\right\}\right| \\
&= \left|\left\{\left(y,z,y',z'\right) \in [n]^4 \mid \underbrace{(i,y,z) \in S}_{\substack{\iff \left(A_{i,y}=z\right) \\ \text{(by the definition of } S\text{)}}} \text{ and } \underbrace{\left(i,y',z'\right) \in S}_{\substack{\iff \left(A_{i,y'}=z'\right) \\ \text{(by the definition of } S\text{)}}} \text{ and } y < y' \text{ and } z > z'\right\}\right| \\
&\qquad \left(\begin{array}{c}\text{because the } ((x,y,z),(x',y',z')) \in S \times S \text{ satisfying } x = x' = i \text{ are} \\ \text{uniquely determined by their coordinates } y,z,y',z'\end{array}\right) \\
&= \left|\left\{\left(y,z,y',z'\right) \in [n]^4 \mid \underbrace{A_{i,y}}_{\substack{=r_i(y) \\ \text{(by the definition} \\ \text{of } r_i\text{)}}} = z \text{ and } \underbrace{A_{i,y'}}_{\substack{=r_i(y') \\ \text{(by the definition} \\ \text{of } r_i\text{)}}} = z' \text{ and } y < y' \text{ and } z > z'\right\}\right| \\
&= \left|\left\{\left(y,z,y',z'\right) \in [n]^4 \mid r_i(y) = z \text{ and } r_i\left(y'\right) = z' \text{ and } y < y' \text{ and } z > z'\right\}\right| \\
&= \left|\left\{\left(y,y'\right) \in [n]^2 \mid y < y' \text{ and } r_i(y) > r_i\left(y'\right)\right\}\right| \\
&\qquad \left(\begin{array}{c}\text{since the 4-tuples } (y,z,y',z') \in [n]^4 \text{ satisfying } r_i(y) = z \text{ and } r_i\left(y'\right) = z' \\ \text{are uniquely determined by their coordinates } y \text{ and } y'\end{array}\right) \\
&= \ell\left(r_i\right) \qquad \text{(by (26))}.
\end{aligned}$$

Thus, (27) becomes

$$\begin{aligned}
|N(=,<,>)| &= \sum_{i \in [n]} \underbrace{\left|\left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x = x' = i \text{ and } y < y' \text{ and } z > z'\right\}\right|}_{=\ell(r_i)} \\
&= \sum_{i \in [n]} \ell\left(r_i\right) = \sum_{i=1}^{n} \ell\left(r_i\right).
\end{aligned}$$

Thus,

$$(-1)^{|N(=,<,>)|} = (-1)^{\sum_{i=1}^{n} \ell(r_i)} = \prod_{i=1}^{n} \underbrace{(-1)^{\ell(r_i)}}_{\substack{=(-1)^{r_i} \\ \text{(since } (-1)^{r_i}=(-1)^{\ell(r_i)} \\ \text{(by the definition of } (-1)^{r_i}\text{))}}} = \prod_{i=1}^{n} (-1)^{r_i}.$$

This proves (23).

Next, we will prove (24). This proof is similar, but differs in some details, so we give it in full. For each $j \in [n]$, the length $\ell\left(c_j\right)$ of the permutation $c_j \in S_n$ is given

by

$$\begin{aligned}
\ell\left(c_j\right) &= \left(\text{the number of inversions of } c_j\right) \\
&\qquad \text{(by the definition of the length of a permutation)} \\
&= \Big(\text{the number of all } (u,v) \in [n]^2 \text{ satisfying } u < v \text{ and } c_j(u) > c_j(v)\Big) \\
&\qquad \text{(by the definition of an inversion)} \\
&= \left|\left\{(u,v) \in [n]^2 \mid u < v \text{ and } c_j(u) > c_j(v)\right\}\right| \\
&= \left|\left\{(u,v) \in [n]^2 \mid \underbrace{v < u}_{\iff (u>v)} \text{ and } \underbrace{c_j(v) > c_j(u)}_{\iff \left(c_j(u)<c_j(v)\right)}\right\}\right| \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } (v,u) \text{ for the index } (u,v), \\ \text{since the map } [n]^2 \to [n]^2,\ (u,v) \mapsto (v,u) \text{ is a bijection}\end{array}\right) \\
&= \left|\left\{(u,v) \in [n]^2 \mid u > v \text{ and } c_j(u) < c_j(v)\right\}\right| \\
&= \left|\left\{(x,x') \in [n]^2 \mid x > x' \text{ and } c_j(x) < c_j(x')\right\}\right| \qquad (28)
\end{aligned}$$

(here, we have renamed the index (u,v) as (x,x')).

But

$$N(>,=,<) = \left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x > x' \text{ and } y = y' \text{ and } z < z'\right\}$$

and thus

$$\begin{aligned}
&|N(>,=,<)| \\
&= \left|\left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x > x' \text{ and } y = y' \text{ and } z < z'\right\}\right| \\
&= \sum_{j \in [n]} \left|\left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x > x' \text{ and } y = y' = j \text{ and } z < z'\right\}\right|. \qquad (29)
\end{aligned}$$

But each $j \in [n]$ satisfies

$$\begin{aligned}
&\left|\left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x > x' \text{ and } y = y' = j \text{ and } z < z'\right\}\right| \\
&= \left|\left\{ \left(x,z,x',z'\right) \in [n]^4 \mid \underbrace{(x,j,z) \in S}_{\substack{\iff \left(A_{x,j}=z\right) \\ \text{(by the definition of } S\text{)}}} \text{ and } \underbrace{\left(x',j,z'\right) \in S}_{\substack{\iff \left(A_{x',j}=z'\right) \\ \text{(by the definition of } S\text{)}}} \text{ and } x > x' \text{ and } z < z' \right\}\right| \\
&\qquad \left(\begin{array}{c} \text{because the } ((x,y,z),(x',y',z')) \in S \times S \text{ satisfying } y = y' = j \text{ are} \\ \text{uniquely determined by their coordinates } x,z,x',z' \end{array} \right) \\
&= \left|\left\{ \left(x,z,x',z'\right) \in [n]^4 \mid \underbrace{A_{x,j}}_{\substack{=c_j(x) \\ \text{(by the definition} \\ \text{of } c_j\text{)}}} = z \text{ and } \underbrace{A_{x',j}}_{\substack{=c_j(x') \\ \text{(by the definition} \\ \text{of } c_j\text{)}}} = z' \text{ and } x > x' \text{ and } z < z' \right\}\right| \\
&= \left|\left\{ \left(x,z,x',z'\right) \in [n]^4 \mid c_j(x) = z \text{ and } c_j\left(x'\right) = z' \text{ and } x > x' \text{ and } z < z' \right\}\right| \\
&= \left|\left\{ \left(x,x'\right) \in [n]^2 \mid x > x' \text{ and } c_j(x) < c_j\left(x'\right) \right\}\right| \\
&\qquad \left(\begin{array}{c} \text{since the 4-tuples } (x,z,x',z') \in [n]^4 \text{ satisfying } c_j(x) = z \text{ and } c_j(x') = z' \\ \text{are uniquely determined by their coordinates } x \text{ and } x' \end{array} \right) \\
&= \ell\left(c_j\right) \qquad \text{(by (28))}.
\end{aligned}$$

Thus, (29) becomes

$$\begin{aligned}
|N(>,=,<)| &= \sum_{j \in [n]} \underbrace{\left|\left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \mid x > x' \text{ and } y = y' = j \text{ and } z < z'\right\}\right|}_{=\ell\left(c_j\right)} \\
&= \sum_{j \in [n]} \ell\left(c_j\right) = \sum_{j=1}^{n} \ell\left(c_j\right).
\end{aligned}$$

Thus,

$$(-1)^{|N(>,=,<)|} = (-1)^{\sum_{j=1}^{n} \ell\left(c_j\right)} = \prod_{j=1}^{n} \underbrace{(-1)^{\ell\left(c_j\right)}}_{\substack{=(-1)^{c_j} \\ \text{(since } (-1)^{c_j} = (-1)^{\ell\left(c_j\right)} \\ \text{(by the definition of } (-1)^{c_j}\text{))}}} = \prod_{j=1}^{n} (-1)^{c_j}.$$

This proves (24).

Finally, we need to prove (25). For each $k \in [n]$, the length $\ell(z_k)$ of the permutation $z_k \in S_n$ is given by

$$\begin{aligned}
\ell(z_k) &= (\text{the number of inversions of } z_k) \\
&\qquad (\text{by the definition of the length of a permutation}) \\
&= \Big(\text{the number of all } (u,v) \in [n]^2 \text{ satisfying } u < v \text{ and } z_k(u) > z_k(v)\Big) \\
&\qquad (\text{by the definition of an inversion}) \\
&= \left|\left\{(u,v) \in [n]^2 \mid u < v \text{ and } z_k(u) > z_k(v)\right\}\right| \\
&= \left|\left\{(x,x') \in [n]^2 \mid x < x' \text{ and } z_k(x) > z_k(x')\right\}\right| \qquad (30)
\end{aligned}$$

(here, we have renamed the index (u,v) as (x,x')).

But

$$N(<,>,=) = \left\{((x,y,z),(x',y',z')) \in S \times S \mid x < x' \text{ and } y > y' \text{ and } z = z'\right\}$$

and thus

$$\begin{aligned}
&|N(<,>,=)| \\
&= \left|\left\{((x,y,z),(x',y',z')) \in S \times S \mid x < x' \text{ and } y > y' \text{ and } z = z'\right\}\right| \\
&= \sum_{k \in [n]} \left|\left\{((x,y,z),(x',y',z')) \in S \times S \mid x < x' \text{ and } y > y' \text{ and } z = z' = k\right\}\right|. \qquad (31)
\end{aligned}$$

But each $k \in [n]$ satisfies

$$\begin{aligned}
&\left|\left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \;\mid\; x < x' \text{ and } y > y' \text{ and } z = z' = k\right\}\right| \\
&= \left|\left\{ \left(x,y,x',y'\right) \in [n]^4 \;\mid\; \underbrace{(x,y,k) \in S}_{\substack{\iff \left(A_{x,y}=k\right) \\ \text{(by the definition of } S\text{)}}} \text{ and } \underbrace{\left(x',y',k\right) \in S}_{\substack{\iff \left(A_{x',y'}=k\right) \\ \text{(by the definition of } S\text{)}}} \text{ and } x < x' \text{ and } y > y' \right\}\right| \\
&\qquad \left(\begin{array}{c} \text{because the } \left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \text{ satisfying } z = z' = k \text{ are} \\ \text{uniquely determined by their coordinates } x,y,x',y' \end{array} \right) \\
&= \left|\left\{ \left(x,y,x',y'\right) \in [n]^4 \;\mid\; \underbrace{A_{x,y} = k}_{\substack{\iff (y=z_k(x)) \\ \text{(by the definition} \\ \text{of } z_k\text{)}}} \text{ and } \underbrace{A_{x',y'} = k}_{\substack{\iff (y'=z_k(x')) \\ \text{(by the definition} \\ \text{of } z_k\text{)}}} \text{ and } x < x' \text{ and } y > y' \right\}\right| \\
&= \left|\left\{ \left(x,y,x',y'\right) \in [n]^4 \;\mid\; y = z_k\left(x\right) \text{ and } y' = z_k\left(x'\right) \text{ and } x < x' \text{ and } y > y' \right\}\right| \\
&= \left|\left\{ \left(x,x'\right) \in [n]^2 \;\mid\; x < x' \text{ and } z_k\left(x\right) > z_k\left(x'\right) \right\}\right| \\
&\qquad \left(\begin{array}{c} \text{since the 4-tuples } \left(x,y,x',y'\right) \in [n]^4 \text{ satisfying } y = z_k\left(x\right) \text{ and } y' = z_k\left(x'\right) \\ \text{are uniquely determined by their coordinates } x \text{ and } x' \end{array} \right) \\
&= \ell\left(z_k\right) \qquad \text{(by (30))}\,.
\end{aligned}$$

Thus, (31) becomes

$$\begin{aligned}
|N(<,>,=)| &= \sum_{k \in [n]} \underbrace{\left|\left\{\left((x,y,z),\left(x',y',z'\right)\right) \in S \times S \;\mid\; x < x' \text{ and } y > y' \text{ and } z = z' = k\right\}\right|}_{=\ell(z_k)} \\
&= \sum_{k \in [n]} \ell\left(z_k\right) = \sum_{k=1}^{n} \ell\left(z_k\right).
\end{aligned}$$

Thus,

$$(-1)^{|N(<,>,=)|} = (-1)^{\sum_{k=1}^{n} \ell(z_k)} = \prod_{k=1}^{n} \underbrace{(-1)^{\ell(z_k)}}_{\substack{=(-1)^{z_k} \\ \text{(since } (-1)^{z_k}=(-1)^{\ell(z_k)} \\ \text{(by the definition of } (-1)^{z_k}\text{))}}} = \prod_{k=1}^{n} (-1)^{z_k}.$$

This proves (25).]

Step 7: Multiplying the three equalities (23), (24) and (25), we obtain

$$\begin{aligned}
&\left(\prod_{i=1}^{n}(-1)^{r_i}\right)\left(\prod_{j=1}^{n}(-1)^{c_j}\right)\left(\prod_{k=1}^{n}(-1)^{z_k}\right) \\
&= (-1)^{|N(=,<,>)|}(-1)^{|N(>,=,<)|}(-1)^{|N(<,>,=)|} \\
&= (-1)^{|N(=,<,>)|}(-1)^{|N(<,>,=)|}(-1)^{|N(>,=,<)|} \\
&= (-1)^{|N(=,<,>)|+|N(<,>,=)|+|N(>,=,<)|} = (-1)^{n(n-1)/2}
\end{aligned}$$

(by (22)). This solves Exercise 7. □

References

[Bartle12] Padraic Bartlett, *Notes from the 2012 Canada/USA Mathcamp*. `http://web.math.ucsb.edu/~padraic/mathcamp_2012/mathcamp_2012.html`

[Bernds12] Jochem Berndsen, *Three problems in algebraic combinatorics*, master's thesis, Eindhoven 2012. `http://repository.tue.nl/fc05ed79-5969-47ce-adaa-bf2d59a3cecc`

[Glynn10] David G. Glynn, *The conjectures of Alon-Tarsi and Rota in dimension prime minus one*, SIAM J. Discrete Math., Vol. 24, No. 2, pp. 394–399. `https://doi.org/10.1137/090773751`

[Grinbe16] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019. `http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf` The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see `https://github.com/darijgr/detnotes/releases/tag/2019-01-10` .

[Hall45] Marshall Hall, *An existence theorem for Latin squares*, Bull. Amer. Math. Soc., Volume 51, Number 6, Part 1 (1945), pp. 387–388.

[HilVau11] A. J. W. Hilton, E. R. Vaughan, *Hall's Condition for Partial Latin Squares*, arXiv:1107.2639v1.

[Jansse95] Jeannette C. M. Janssen, *On even and odd latin squares*, Journal of Combinatorial Theory, Series A, Volume 69, Issue 1, January 1995, pp. 173–181. `https://doi.org/10.1016/0097-3165(95)90115-9`

[Stanle13] Richard Stanley, *Algebraic Combinatorics: Walks, Trees, Tableaux, and More*, Springer 2013. See `http://www-math.mit.edu/~rstan/algcomb/` for a draft version.