Linear Algebra in Olympiad Maths

Krzysztof Karwik, Jakub Pieczonka

10.11.2024

1. Fundaments and Definitions

Vector

In linear algebra, a **vector** is an ordered list of numbers that represents a quantity with both magnitude and direction. Vectors are often written in the form:

$$\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

where each v_i is a component of the vector $\mathbf{v}$.

Vector Space

A **vector space** V over a field $\mathbb{F}$ (such as the field of real numbers $\mathbb{R}$ or complex numbers $\mathbb{C}$) is a set of vectors that satisfies certain properties under vector addition and scalar multiplication. For any vectors $\mathbf{u}, \mathbf{v} \in V$ and any scalar $c \in \mathbb{F}$, the following properties hold:

1. **Closure under addition**: $\mathbf{u} + \mathbf{v} \in V$.
2. **Closure under scalar multiplication**: $c\mathbf{u} \in V$.
3. **Commutativity**: $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.
4. **Associativity of addition**: $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$.
5. **Existence of an additive identity**: There exists a zero vector $\mathbf{0} \in V$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v} \in V$.
6. **Existence of additive inverses**: For each $\mathbf{v} \in V$, there exists a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.
7. **Associativity of scalar multiplication**: $a(b\mathbf{v}) = (ab)\mathbf{v}$.
8. **Distributive properties**: $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ and $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$.

Here are some examples of vector spaces to help you get the hang of them:

Example. The Space $\mathbb{R}^2$: (this is a very intuitive example) The set of all ordered pairs $\mathbb{R}^2 = \{(x, y) \,|\, x, y \in \mathbb{R}\}$ is a vector space over $\mathbb{R}$. For any two vectors $\mathbf{u} = (u_1, u_2)$ and $\mathbf{v} = (v_1, v_2)$ in $\mathbb{R}^2$, addition is defined as:

$$\mathbf{u} + \mathbf{v} = (u_1 + v_1, u_2 + v_2),$$

and for a scalar $c \in \mathbb{R}$, scalar multiplication is defined as:

$$c \cdot \mathbf{u} = (c \cdot u_1, c \cdot u_2).$$

It is easy to see that this satisfies all the vector space axioms. On the other hand, here is a much less intuitive example.

Example. The Space of Polynomials P_2: The set of all polynomials of degree at most 2, denoted $P_2 = \{a + bx + cx^2 \,|\, a, b, c \in \mathbb{R}\}$, is a vector space. Addition and scalar multiplication are defined by combining like terms and distributing scalars, respectively. For example, if $p(x) = 2 + 3x + x^2$ and $q(x) = -1 + 4x + 2x^2$, then:

$$p(x) + q(x) = (2 - 1) + (3 + 4)x + (1 + 2)x^2 = 1 + 7x + 3x^2.$$

Polynomials are going to be a recurring theme for this handout so it's worth to convince yourself that this is in fact a vector space.

Linear Independence

A set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ in a vector space V is said to be **linearly independent** if the only solution to the equation

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_k\mathbf{v}_k = \mathbf{0}$$

is $c_1 = c_2 = \cdots = c_k = 0$. In other words, no vector in the set can be written as a linear combination of the others. If there exists any other solution, the vectors are said to be **linearly dependent**.

Here are a few examples of linearly independent (or dependent) vectors:

Example. The vectors $\mathbf{v}_1 = (1, 0)$ and $\mathbf{v}_2 = (0, 1)$ in $\mathbb{R}^2$ are linearly independent because the only solution to $a_1(1, 0) + a_2(0, 1) = (0, 0)$ is $a_1 = 0$ and $a_2 = 0$. Neither vector can be written as a scalar multiple of the other.

Example. In P_2: In the space of polynomials P_2, the set $\{1, x, x^2\}$ is linearly independent. To show this, consider the equation:

$$a \cdot 1 + b \cdot x + c \cdot x^2 = 0.$$

Since this must hold for all values of x, we have $a = 0$, $b = 0$, and $c = 0$ as the only solution, which confirms the linear independence of $\{1, x, x^2\}$.

Example. Dependent Set Example: The vectors $\{(1, 1), (2, 2)\}$ in $\mathbb{R}^2$ are *not* linearly independent because $(2, 2) = 2 \cdot (1, 1)$; hence, they are linearly dependent.

Dot Product

The **dot product** (or **scalar product**) of two vectors is an algebraic operation that takes two equal-length vectors and returns a single number. For two vectors $\mathbf{u} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}$ and $\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$, the dot product is defined as:

$$\mathbf{u} \cdot \mathbf{v} = \langle \mathbf{u}, \mathbf{v} \rangle = u_1v_1 + u_2v_2 + \cdots + u_nv_n = \sum_{i=1}^{n} u_iv_i.$$

Here are the most important properties of the dot product:

- **Commutativity**: $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$.
- **Distributive Property**: $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$.

2. More Properties of Vector Spaces

Basis of a Vector Space

A **basis** of a vector space V is a set of vectors that satisfies two key conditions:

1. **Spanning**: The basis vectors span the vector space, meaning any vector in V can be expressed as a linear combination of the basis vectors.
2. **Linear Independence**: The basis vectors are linearly independent, which implies that no vector in the basis can be written as a linear combination of the others.

More formally, a set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ in a vector space V is a basis if every vector $\mathbf{v} \in V$ can be uniquely represented as:

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n,$$

where $a_1, a_2, \ldots, a_n$ are scalars. The vectors in a basis provide the "building blocks" for all vectors in the space.

Example. Standard Basis in $\mathbb{R}^3$: In three-dimensional space, $\mathbb{R}^3$, a common basis is the set:

$$\{\mathbf{e}_1 = (1, 0, 0),\ \mathbf{e}_2 = (0, 1, 0),\ \mathbf{e}_3 = (0, 0, 1)\}.$$

This set is known as the *standard basis* for $\mathbb{R}^3$. Any vector $\mathbf{v} = (x, y, z)$ in $\mathbb{R}^3$ can be expressed as:

$$\mathbf{v} = x\mathbf{e}_1 + y\mathbf{e}_2 + z\mathbf{e}_3.$$

Example. Polynomial Basis: For the vector space P_2 of polynomials of degree at most 2, the set:

$$\{1, x, x^2\}$$

is a basis. Any polynomial $p(x) = a + bx + cx^2$ in P_2 can be written as:

$$p(x) = a \cdot 1 + b \cdot x + c \cdot x^2.$$

We will now be relying on the following.

Theorem

All bases of a vector space V have the same cardinality.

Dimension of a Vector Space

The **dimension** of a vector space V is the number of vectors in any basis of V. Since all bases of a vector space have the same number of elements, dimension is well-defined. If a vector space V has a basis with n vectors, we say that V is n-dimensional, denoted as $\dim(V) = n$.

Example. Dimension of $\mathbb{R}^3$: The vector space $\mathbb{R}^3$ has dimension 3, as its standard basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ contains three vectors.

Example. Dimension of P_2: The vector space P_2 of polynomials of degree at most 2 has dimension 3, with the basis $\{1, x, x^2\}$.

Now we introduce a theorem that will be the fundament of all solutions that involve dimensions.

Steinitz Exchange Lemma

Let N be a set of vectors spanning a vector space V and M be a set of linearly independent vectors in V. Then the following inequality holds

$$|M| \leqslant |N|$$

Proof. Suppose $N = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ and $M = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m\}$. Then $V = \operatorname{span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$. By way of contradiction assume $m > n$. Moreover,

$$\mathbf{u}_1 = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$$

for some scalars a_i. As $\mathbf{u}_1 \neq 0$ so not all of the a_i are zero, say without loss of generality $a_1 \neq 0$. Then $V = \operatorname{span}\{\mathbf{u}_1, \mathbf{v}_2, \mathbf{v}_3, \dots, \mathbf{v}_n\}$. Hence, write $\mathbf{u}_2 = b_1\mathbf{u}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 + \cdots + c_n\mathbf{v}_n$. Then some $c_i \neq 0$ because $\{\mathbf{u}_1, \mathbf{u}_2\}$ is independent; so, as before, $V = \operatorname{span}\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_3, \dots, \mathbf{v}_n\}$. This procedure continues until all the vectors $\mathbf{v}_i$ are replaced by the vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$. In particular, because $m > n$, we get

$$V = \operatorname{span}\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\}$$

But then $\mathbf{u}_{n+1}$ is a linear combination of $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$, contrary to the independence of the $\mathbf{u}_i$. Hence, the assumption $m > n$ cannot be valid, so $m \leqslant n$ $\square$

Exercise. Using the Steinitz Exchange Lemma prove that every two bases of a vector space V have the same cardinality.

Assuming additionally that N is the basis of V we get the following.

Corollary

If M is a set of linearly independent vectors in a vector space V then

$$|M| \leqslant \dim(V)$$

3. Applications in Problems Involving Sets

Sets as Vectors over $\mathbb{Z}_2$

Let us consider problems of the following type: we have a family of sets and certain information about the parity of the sizes of these sets and their intersections; we want to estimate their quantity. A subset $A \subseteq [n]$ can be identified with a vector $v \in \mathbb{F}^n$, which has 1 in the i-th coordinate if $i \in A$, and 0 otherwise. If parity is relevant, a good choice of field $\mathbb{F}$ could be $\mathbb{Z}_2$. Notice that if $A \sim v$ and $B \sim w$, then $\langle v, w\rangle = |A \cap B|$ (the equalities hold in the field over which the vectors are considered), so assumptions about the sizes of sets and their intersections translate well into the language of linear algebra. For example, proving that there are at most n sets satisfying certain properties reduces to showing the linear independence of the corresponding system of vectors.

Problem 1. Let sets $A_1, \dots, A_m$ be subsets of the set $[n]$, such that $|A_i|$ is an odd number for each i, and $|A_i \cap A_j|$ is an even number for any $i \neq j$. Find the maximum possible value of m as a function of n.

Problem 2. Let n be an odd number, and let sets $A_1, \dots, A_m$ be subsets of the set $[n]$, such that $|A_i|$ is an even number for each i, and $|A_i \cap A_j|$ is an odd number for any $i \neq j$. Find the maximum possible value of m as a function of n.

Problem 3. Let n be an even number, and let sets $A_1, \dots, A_m$ be subsets of the set $[n]$, such that $|A_i|$ is an even number for each i, and $|A_i \cap A_j|$ is an odd number for any $i \neq j$. Find the maximum possible value of m as a function of n.

Problem 4. Let sets $A_1, \dots, A_m$ be pairwise distinct subsets of the set $[n]$, such that $|A_i \cap A_j|$ is an even number for any i, j (including the case $i = j$). Find the maximum possible value of m as a function of n.

Sets as Vectors over $\mathbb{R}$

If we do not have any information about parity, then $\mathbb{Z}_2$ is not the most useful field. If there is no indication otherwise, then the field $\mathbb{Z}_p$ for some prime number p would not bring anything interesting to the problem, so it is easiest to consider vectors and matrices over the field $\mathbb{R}$, which is the most intuitive.

Problem 5. Students in a school go for ice cream in groups of at least two. After $k > 1$ groups have gone, every two students have gone together exactly once. Prove that the number of students in the school is at most k.

Problem 6. Let $1 \leqslant k \leqslant n$. Let sets $A_1, \ldots, A_m$ be pairwise distinct subsets of the set $[n]$, such that $|A_i \cap A_j| = k$ for any $i \neq j$. Prove that $m \leqslant n$.

Problem 7. Let $A_1, A_2, \ldots, A_{n+1}$ be non-empty subsets of $\{1, 2, \ldots, n\}$. Prove that there exists nonempty disjoint subsets $I, J \subset \{1, 2, \ldots, n+1\}$ such that

$$\bigcup_{k \in I} A_k = \bigcup_{k \in J} A_k.$$

Problem 8. Let $A_1, A_2, \ldots, A_{n+2}$ be non-empty subsets of $\{1, 2, \ldots, n\}$. Prove that there exists nonempty disjoint subsets $I, J \subset \{1, 2, \ldots, n+2\}$ such that

$$\bigcup_{k \in I} A_k = \bigcup_{k \in J} A_k, \quad \text{and} \quad \bigcap_{k \in I} A_k = \bigcap_{k \in J} A_k.$$

Problem 9. Let sets $A_1, \ldots, A_m$ be subsets of the set $[n]$, such that there is no two-coloring of the elements of $[n]$ in which each set A_i contains elements of both colors, but after removing any one of the sets A_i, such a coloring exists. Prove that $m \geqslant n'$, where $n' = |\bigcup_{i=1}^{m} A_i|$.

4. A Word or Two on Multivariate Polynomials

All of the techniques and tricks shown above can also be applied to polynomials vector spaces. Here is a prime example.

Problem 10. Do there exist polynomials $a(x), b(x), c(y), d(y)$ with real coefficients such that

$$1 + xy + x^2y^2 = a(x)c(y) + b(x)d(y)$$

holds for all $x, y \in \mathbb{R}$?

Basis and Dimension of a Polynomial Vector Space

As you have seen before polynomials with multiple variables can be interpreted within a vector space, allowing us to apply linear algebra tricks to analyze and manipulate them. Consider a polynomial in two variables x and y:

$$p(x, y) = a_{00} + a_{10}x + a_{01}y + a_{11}xy + a_{20}x^2 + a_{02}y^2 + \cdots.$$

Each polynomial can be represented as a linear combination of terms $x^i y^j$ with coefficients a_{ij}.

Example. The polynomial $p(x, y) = 2 + 3x + 4y + 5xy$ can be viewed as a vector of coefficients:

$$\mathbf{p} = \begin{bmatrix} 2 & 3 & 4 & 5 \end{bmatrix}^T.$$

This is true for any n-variable polynomials in general, as you can check in the next lemma.

Lemma

Let V be a vector space of n-variable polynomials with a maximum degree k of each variable. Then

$$S = \{x_1^{\alpha_1} \ldots x_n^{\alpha_n} \mid \text{for all permutations } (\alpha_1, \ldots, \alpha_n) \text{ of } \{0, 1, \ldots, k\}\}$$

is a basis of space V.

Proof. Left as an exercise.

Moreover, we can now derive the following corollary.

Corollary

If V is a vector space of n-variable polynomials with a maximum degree k of each variable then
$$\dim(V) = (k+1)^n$$

Degree of a Multivariate Polynomial

Let P be a polynomial in n variables such that
$$P(x_1, \ldots, x_n) = \sum_i p_i \left(x_1^{\alpha_{i,1}} x_2^{\alpha_{i,2}} \ldots\ x_n^{\alpha_{i,n}}\right)$$
Then the **degree of polynomial P** is defined as
$$\deg(P) = \max_i(\alpha_{i,1} + \ldots + \alpha_{i,n})$$

Exercise. Find the dimension of the vector space of polynomials of two variables of degree at most m.

Exercise. Generalize the above to polynomials with n variables. That is, find the dimension of a vector space of polynomials of n variables of degree at most m

Polynomials are a tool for writing into linear algebra more complicated conditions (just like we did in the problems that considered sets). A common motive in solving following problems will be to firstly find a specific set of polynomials, then find the dimension of the vector space that we're dealing with, and finally, apply the **Exchange Lemma Corollary** to receive a cardinality bound.

Problem 11. Let S be a set of n-tuples of complex numbers (or remainders mod p) and fix $K \neq 0$. If for every two n-tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ in S there is an index i with $a_i = b_i + K$, then prove $|S| \leqslant 2^n$.

Problem 12. Let n be a given positive integer. A set S of points in the plane has the following properties:

- It is not possible to cover all elements of the set S with n lines.
- For any point $A \in S$, the set $S \setminus \{A\}$ can be covered by n lines.

Determine the largest possible value of $|S|$.

Problem 13. Given two real numbers α, β and a set of N points in $\mathbb{R}^n$ with the property that the distance between any two of them is either α or β prove that
$$N \leqslant \frac{(n+1)(n+2)}{2}$$
(*Hint: Start by proving the weaker bound* $N \leqslant \frac{(n+1)(n+4)}{2}$)

Problem 14. Let $P(x)$ and $Q(x)$ be arbitrary polynomials with real coefficients, and let d be the degree of $P(x)$. Assume that $P(x)$ is not the zero polynomial. Prove that there exist polynomials $A(x)$ and $B(x)$ such that

1. Both A and B have degree at most $d/2$,
2. At most one of A and B is the zero polynomial,
3. P divides $A + Q \cdot B$.

Problem 15 (Multivariable Lagrange interpolation)**.** Let $S \subset \mathbb{Z}^2$ be a set of n lattice points. Prove that there exists a nonzero two-variable polynomial p with real coefficients, of degree at most $\sqrt{2n}$, such that $p(x, y) = 0$ for every $(x, y) \in S$.

Problem 16. Let $A_1, A_2, \ldots, A_m$ be distinct subsets of $\{1, 2, \ldots, n\}$. Let L be the set of numbers that occur as $|A_i \cap A_j|$ for some $i \neq j$. Prove that

$$m \leqslant \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{|L|}$$

Problem 17. Let p be a prime and S be a subset of $\{0, 1, \ldots, p-1\}$. Suppose $\{A_1, A_2, \ldots, A_m\}$ are subsets of $\{1, 2, \ldots, n\}$ so that $|A_i| \notin S \pmod p$ for all i and $|A_i \cap A_j| \in S \pmod p$ for $i \neq j$. Prove that

$$m \leqslant \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{|S|}$$

Problem 18. Let $0 < k \leqslant n$ be positive integers and suppose $\{A_1, A_2, \ldots, A_m\}$ are distinct k-element subsets of $\{1, 2, \ldots, n\}$. Let T be the set of numbers that occur as $|A_i \cap A_j|$ for some $i \neq j$. Show that

$$m \leqslant \binom{n}{|T|}$$

5. A Closer Look at Matrices

Here we make an extensive use of the following properties.

Matrix Rank Properties

Let A be a $n \times m$ matrix with $n < m$. Then

$$A\mathbf{v} = \mathbf{0}$$

has a nonzero solution Let B be a $n \times n$ matrix with $\det(B) = 0$. Then

$$B\mathbf{v} = \mathbf{0}$$

has a nonzero solution.

Those properties are corollaries of the fact that if the rank, or the dimension of the set of rows, or the dimension of the set of columns is less than the dimension of $\mathbf{v}$. Then

$$A\mathbf{v} = \mathbf{0}$$

has a nonzero solution.

Problem 19. Let $a_1, a_2, \ldots, a_{2n+1}$ be real numbers, such that for any $1 \leqslant i \leqslant 2n+1$, we can remove a_i and separate the remaining $2n$ numbers into two groups of n numbers with equal sums. Show that $a_1 = a_2 = \cdots = a_{2n+1}$.

Problem 20. Show that the complete graph with n vertices, K_n, cannot be covered by fewer than $n-1$ complete bipartite graphs so that each edge of K_n is covered exactly once.

Problem 21. A contest with n questions was taken by m contestants. Each question was worth a certain (positive) number of points, and no partial credits were given. After all the papers have been graded, it was noticed that by reassigning the scores of the questions, any desired ranking of the contestants could be achieved. What is the largest possible value of m?

Problem 22. Does there exist a configuration of 22 distinct circles and 22 distinct points on the plane, such that every circle contains at least 7 points and every point belongs at least to 7 circles?

Problem 23. Let J_m be an $m \times m$ matrix with all entries equal to 1, and let I_m be the $m \times m$ identity matrix. Determine the rank of the matrix $J_m - I_m$ over the field $\mathbb{Z}_2$.

Eigenvalues

Let A be an $n \times n$ matrix, and let I be the $n \times n$ identity matrix. We define the **characteristic polynomial** of matrix A as

$$p_A(x) = \det(xI - A)$$

and its **eigenvalues** $\lambda_1, \ldots, \lambda_n$ as (possibly complex) roots of the characteristic polynomial.

Trace

The **trace** of an $n \times n$ matrix A is the sum of the elements on its main diagonal. It is denoted by $\mathrm{Tr}(A)$ and defined as:

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii}$$

Equivalently, $\mathrm{Tr}(A)$ is the sum of all eigenvalues of A, taking multiplicities into account.

It is clear that if λ is a real number, then it is an eigenvalue of A if and only if there exists a non-zero vector v such that $Av = \lambda v$ (we call v an eigenvector). This definition does not provide information about the multiplicity of λ and excludes the case of non-real roots. It is easy to see that the characteristic polynomial of A does not change under the transformation $A \mapsto CAC^{-1}$, where C is an invertible matrix. It is also apparent that the coefficient of x^{n-1} in the characteristic polynomial is equal to $-\mathrm{Tr}(A)$. What is more, of course the determinant of a matrix is the products of its eigenvalues counting multiplicity
We now proceed to a theorem that is the main focus of any serious course in linear algebra. However, due to its level of complexity, we present a simplified version here, which is sufficient for our purposes, without proof.

Simplified Jordan Theorem

Let A be an $n \times n$ matrix with eigenvalues $\lambda_1, \ldots, \lambda_n$. Then there exists a matrix (possibly complex) C such that C is invertible, J is upper triangular with the eigenvalues $\lambda_1, \ldots, \lambda_n$ on the diagonal, and

$$A = CJC^{-1}$$

In the full formulation, much more is proven about the matrix J than just its upper triangular form. Since $p_A(x) = p_J(x)$, it also follows that $\mathrm{Tr}(A) = \mathrm{Tr}(J) = \sum_{i=1}^{n} \lambda_i$. From the triangular form of J, it follows that the eigenvalues of the matrix A^k are the numbers λ_i^k.

Theorem

Let A be a symmetric $n \times n$ matrix. Then all eigenvalues of A are real.

Graph Adjacency Matrix

A graph G with n vertices can be associated with an adjacency matrix M, having dimensions $n \times n$ and defined by $M_{u,v} = 1$ if there is an edge from u to v in G, and $M_{u,v} = 0$ otherwise. This definition applies to both directed and undirected graphs, where for undirected graphs, the adjacency matrix is symmetric. The following exercise provides the simplest example of how to encode certain properties of a graph using matrix operations.

Exercise. Let G be a directed graph with n vertices (allowing loops and multiple edges) and let M be the adjacency matrix of G. Prove that $(M^k)_{u,v}$ is equal to the number of paths of length k from u to v (we allow repetition of edges and vertices on the path). Deduce that $\mathrm{Tr}(M^k)$ is equal to the number of closed paths of length k in G.

With all this knowledge we can attempt to solve one very difficult problem from the Polish MO.

Problem 24. Given a graph with $n \geqslant 2$ vertices, k edges, and t triangles, prove that

$$9t^2 < 2k^3.$$

Problem 25. There are 2007 senators in a senate. Each senator has enemies within the senate. Prove that there is a non-empty subset K of senators such that for every senator in the senate, the number of enemies of that senator in the set K is an even number.

Problem 26. Each square of a $(2^n-1)\times(2^n-1)$ board contains either 1 or -1. Such an arrangement is called *successful* if each number is the product of its neighbors. Find the number of successful arrangements.

Advanced techniques

Null Space

The **null space** (or **kernel**) of a matrix A, denoted $\mathrm{null}(A)$, is the set

$$\mathrm{null}(A) = \{\mathbf{v} : A\mathbf{v} = \mathbf{0}\}$$

Image

The **image** (or **range**) of a matrix A, denoted $\mathrm{im}(A)$, is the set

$$\mathrm{im}(T) = \{A\mathbf{v} : \mathbf{v} \in V\}$$

Orthogonal Complement

The **orthogonal complement** of a set S, denoted $S^\perp$, is the set

$$S^\perp = \{\mathbf{w} \in V : \langle \mathbf{w}, \mathbf{v}\rangle = 0 \text{ for all } \mathbf{v} \in S\}$$

In other words, the orthogonal complement is the set of all vectors which are perpendicular (that is - their dot product is zero) to **all** elements of S.

Fundamental Theorem of Symmetric Matrices

For a symmetric matrix A

$$\mathrm{im}(A) = (\mathrm{null}(A))^\perp$$

An interesting fact which we state without proof that for all subspaces V: $\dim V + \dim V^\perp = n$, where n is the dimension of the original space. With those definitions we shall examine the following lemma.

Lemma

Let $A \in \mathbb{F}_2^{n\times n}$ be a symmetric matrix. Then

$$\mathrm{diag}(A) \in \mathrm{im}(A)$$

Where $\mathrm{diag}(A)$ is the vector made out of the main diagonal of A.

Proof. From the facts stated above we know that

$$\mathrm{im}(A) = (\mathrm{null}(A))^\perp$$

Therefore we shall prove

$$\mathrm{diag}(A) \in (\mathrm{null}(A))^\perp$$

This is equivalent to proving that for each $\mathbf{v}$ such that $A\mathbf{v} = \mathbf{0}$ it holds

$$\langle \mathrm{diag}(A), \mathbf{v}\rangle = \mathbf{0}$$

This follows since

$$\mathbf{0} = \mathbf{v}^{\perp} A \mathbf{v} = \sum_{i,j} a_{ij} v_i v_j = \sum_{i=1}^{n} a_{i,i} v_i^2 + 2 \sum_{i<j} a_{ij} v_i v_j = \langle \mathrm{diag}(A), \mathbf{v} \rangle \quad \square$$

All this knowledge is sufficient to solve the following difficult problem.

Problem 27. Let G be a finite simple graph, and there is a light bulb at each vertex of G. Initially, all the lights are off. Each step we are allowed to chose a vertex and toggle the light at that vertex as well as all its neighbors'. Show that we can get all the lights to be on at the same time.

Problem 28. Given a positive integer n, a collection $\mathcal{S}$ of $n-2$ unordered triples of integers in $\{1, 2, \ldots, n\}$ is n-*admissible* if for each $1 \leqslant k \leqslant n-2$ and each choice of k distinct $A_1, A_2, \ldots, A_k \in \mathcal{S}$ we have

$$|A_1 \cup A_2 \cup \cdots \cup A_k| \geqslant k+2.$$

Is it true that for all $n > 3$ and for each n-admissible collection $\mathcal{S}$, there exist pairwise distinct points $P_1, P_2, \ldots, P_n$ in the plane such that the angles of the triangle $P_i P_j P_k$ are all less than $61°$ for any triple $\{i, j, k\} \in \mathcal{S}$?

Sources and Links to Solutions

[1] For problems 1-6 see this blog.

[2] For problem 26 see AOPS.

[3] For the other matrices problems see this handout and this blog.

[4] For problem 10 see this handout.

[5] For problem 11 and twelve see page 156 of this book

[6] For problems 11 and 13 see this brochure under the section *Consider the Polynomial*.

[7] For problems 16, 17 and 18 see this paper.

[8] For problem 28 check this AOPS post.