International Mathematics Competition for University Students
July 25–30 2009, Budapest, Hungary
Day 2

Problem 1.
Let ℓ be a line and P a point in $\mathbb{R}^3$. Let S be the set of points X such that the distance from X to ℓ is greater than or equal to two times the distance between X and P. If the distance from P to ℓ is $d>0$, find the volume of S.

Solution. We can choose a coordinate system of the space such that the line ℓ is the z-axis and the point P is $(d,0,0)$. The distance from the point (x,y,z) to ℓ is $\sqrt{x^2+y^2}$, while the distance from P to X is $|PX| = \sqrt{(x-d)^2+y^2+z^2}$. Square everything to get rid of the square roots. The condition can be reformulated as follows: the square of the distance from ℓ to X is at least $4|PX|^2$.

$$x^2+y^2 \ge 4((x-d)^2+y^2+z^2)$$

$$0 \ge 3x^2-8dx+4d^2+3y^2+4z^2$$

$$\left(\frac{16}{3}-4\right)d^2 \ge 3\left(x-\frac{4}{3}d\right)^2+3y^2+4z^2$$

A translation by $\frac{4}{3}d$ in the x-direction does not change the volume, so we get

$$\frac{4}{3}d^2 \ge 3x_1^2+3y^2+4z^2$$

$$1 \ge \left(\frac{3x_1}{2d}\right)^2+\left(\frac{3y}{2d}\right)^2+\left(\frac{\sqrt{3}z}{d}\right)^2,$$

where $x_1 = x-\frac{4}{3}d$. This equation defines a solid ellipsoid in canonical form. To compute its volume, perform a linear transformation: we divide x_1 and y by $\frac{2d}{3}$ and z by $\frac{d}{\sqrt{3}}$. This changes the volume by the factor $\left(\frac{2d}{3}\right)^2\frac{d}{\sqrt{3}} = \frac{4d^3}{9\sqrt{3}}$ and turns the ellipsoid into the unit ball of volume $\frac{4}{3}\pi$. So before the transformation the volume was $\frac{4d^3}{9\sqrt{3}}\cdot\frac{4}{3}\pi = \frac{16\pi d^3}{27\sqrt{3}}$.

Problem 2.
Suppose $f\colon \mathbb{R}\to\mathbb{R}$ is a two times differentiable function satisfying $f(0)=1$, $f'(0)=0$, and for all $x\in[0,\infty)$,

$$f''(x)-5f'(x)+6f(x)\ge 0.$$

Prove that for all $x\in[0,\infty)$,

$$f(x)\ge 3e^{2x}-2e^{3x}.$$

Solution. We have $f''(x)-2f'(x)-3(f'(x)-2f(x))\ge 0$, $x\in[0,\infty)$.

Let $g(x)=f'(x)-2f(x)$, $x\in[0,\infty)$. It follows that

$$g'(x)-3g(x)\ge 0,\ x\in[0,\infty),$$

hence

$$(g(x)e^{-3x})'\ge 0,\quad x\in[0,\infty),$$

therefore

$$g(x)e^{-3x}\ge g(0)=-2,\ x\in[0,\infty) \text{ or equivalently}$$
$$f'(x)-2f(x)\ge -2e^{3x},\ x\in[0,\infty).$$

Analogously we get

$$(f(x)e^{-2x})'\ge -2e^{x},\ x\in[0,\infty) \text{ or equivalently}$$
$$(f(x)e^{-2x}+2e^{x})'\ge 0,\ x\in[0,\infty).$$

It follows that

$$f(x)e^{-2x}+2e^{x}\ge f(0)+2=3,\ x\in[0,\infty) \text{ or equivalently}$$
$$f(x)\ge 3e^{2x}-2e^{3x},\ x\in[0,\infty).$$

Problem 3.
Let $A, B \in M_n(\mathbb{C})$ be two $n \times n$ matrices such that

$$A^2B + BA^2 = 2ABA.$$

Prove that there exists a positive integer k such that $(AB - BA)^k = 0$.

Solution 1. Let us fix the matrix $A \in M_n(\mathbb{C})$. For every matrix $X \in M_n(\mathbb{C})$, let $\Delta X := AX - XA$. We need to prove that the matrix ΔB is nilpotent.

Observe that the condition $A^2B + BA^2 = 2ABA$ is equivalent to

$$\Delta^2 B = \Delta(\Delta B) = 0. \tag{1}$$

Δ is linear; moreover, it is a derivation, i.e. it satisfies the Leibniz rule:

$$\Delta(XY) = (\Delta X)Y + X(\Delta Y), \quad \forall X, Y \in M_n(\mathbb{C}).$$

Using induction, one can easily generalize the above formula to k factors:

$$\Delta(X_1 \cdots X_k) = (\Delta X_1)X_2 \cdots X_k + \cdots + X_1 \cdots X_{j-1}(\Delta X_j)X_{j+1} \cdots X_k + X_1 \cdots X_{n-1}\Delta X_k, \tag{2}$$

for any matrices $X_1, X_2, \ldots, X_k \in M_n(\mathbb{C})$. Using the identities (1) and (2) we obtain the equation for $\Delta^k(B^k)$:

$$\Delta^k(B^k) = k!(\Delta B)^k, \quad \forall k \in \mathbb{N}. \tag{3}$$

By the last equation it is enough to show that $\Delta^n(B^n) = 0$.

To prove this, first we observe that equation (3) together with the fact that $\Delta^2 B = 0$ implies that $\Delta^{k+1}B^k = 0$, for every $k \in \mathbb{N}$. Hence, we have

$$\Delta^k(B^j) = 0, \quad \forall k, j \in \mathbb{N},\ j < k. \tag{4}$$

By the Cayley–Hamilton Theorem, there are scalars $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{C}$ such that

$$B^n = \alpha_0 I + \alpha_1 B + \cdots + \alpha_{n-1}B^{n-1},$$

which together with (4) implies that $\Delta^n B^n = 0$.

Solution 2. Set $X = AB - BA$. The matrix X commutes with A because

$$AX - XA = (A^2B - ABA) - (ABA - BA^2) = A^2B + BA^2 - 2ABA = 0.$$

Hence for any $m \geq 0$ we have

$$X^{m+1} = X^m(AB - BA) = AX^mB - X^mBA.$$

Take the trace of both sides:

$$\operatorname{tr} X^{m+1} = \operatorname{tr} A(X^mB) - \operatorname{tr}(X^mB)A = 0$$

(since for any matrices U and V, we have $\operatorname{tr} UV = \operatorname{tr} VU$). As $\operatorname{tr} X^{m+1}$ is the sum of the $m+1$-st powers of the eigenvalues of X, the values of $\operatorname{tr} X, \ldots, \operatorname{tr} X^n$ determine the eigenvalues of X uniquely, therefore all of these eigenvalues have to be 0. This implies that X is nilpotent.

Problem 4.
Let p be a prime number and $\mathbb{F}_p$ be the field of residues modulo p. Let W be the smallest set of polynomials with coefficients in $\mathbb{F}_p$ such that

- the polynomials $x + 1$ and $x^{p-2} + x^{p-3} + \cdots + x^2 + 2x + 1$ are in W, and
- for any polynomials $h_1(x)$ and $h_2(x)$ in W the polynomial $r(x)$, which is the remainder of $h_1(h_2(x))$ modulo $x^p - x$, is also in W.

How many polynomials are there in W?

Solution. Note that both of our polynomials are bijective functions on $\mathbb{F}_p$: $f_1(x) = x + 1$ is the cycle $0 \to 1 \to 2 \to \cdots \to (p-1) \to 0$ and $f_2(x) = x^{p-2} + x^{p-3} + \cdots + x^2 + 2x + 1$ is the transposition $0 \leftrightarrow 1$ (this follows from the formula $f_2(x) = \frac{x^{p-1}-1}{x-1} + x$ and Fermat's little theorem). So any composition formed from them is also a bijection, and reduction modulo $x^p - x$ does not change the evaluation in $\mathbb{F}_p$. Also note that the transposition and the cycle generate the symmetric group ($f_1^k \circ f_2 \circ f_1^{p-k}$ is the transposition $k \leftrightarrow (k+1)$, and transpositions of consecutive elements clearly generate S_p), so we get all $p!$ permutations of the elements of $\mathbb{F}_p$.

The set W only contains polynomials of degree at most $p-1$. This means that two distinct elements of W cannot represent the same permutation. So W must contain those polynomials of degree at most $p-1$ which permute the elements of $\mathbb{F}_p$. By minimality, W has exactly these $p!$ elements.

Problem 5.
Let $\mathbb{M}$ be the vector space of $m \times p$ real matrices. For a vector subspace $S \subseteq \mathbb{M}$, denote by $\delta(S)$ the dimension of the vector space generated by all columns of all matrices in S.

Say that a vector subspace $T \subseteq \mathbb{M}$ is a *covering matrix space* if

$$\bigcup_{A \in T,\, A \neq 0} \ker A = \mathbb{R}^p.$$

Such a T is *minimal* if it does not contain a proper vector subspace $S \subset T$ which is also a covering matrix space.

(a) (8 points) Let T be a minimal covering matrix space and let $n = \dim T$. Prove that

$$\delta(T) \leq \binom{n}{2}.$$

(b) (2 points) Prove that for every positive integer n we can find m and p, and a minimal covering matrix space T as above such that $\dim T = n$ and $\delta(T) = \dbinom{n}{2}$.

Solution 1. (a) We will prove the claim by constructing a suitable decomposition $T = Z_0 \oplus Z_1 \oplus \cdots$ and a corresponding decomposition of the space spanned by all columns of T as $W_0 \oplus W_1 \oplus \cdots$, such that $\dim W_0 \leqslant n-1$, $\dim W_1 \leqslant n-2$, etc., from which the bound follows.

We first claim that, in every covering matrix space S, we can find an $A \in S$ with $\operatorname{rk} A \leqslant \dim S - 1$. Indeed, let $S_0 \subseteq S$ be some minimal covering matrix space. Let $s = \dim S_0$ and fix some subspace $S' \subset S_0$ of dimension $s-1$. S' is not covering by minimality of S_0, so that we can find an $u \in \mathbb{R}^p$ with $u \notin \cup_{B \in S',\, B \neq 0} \operatorname{Ker} B$. Let $V = S'(u)$; by the rank-nullity theorem, $\dim V = s - 1$. On the other hand, as S_0 is covering, we have that $Au = 0$ for some $A \in S_0 \setminus S'$. We claim that $\operatorname{Im} A \subset V$ (and therefore $\operatorname{rk}(A) \leqslant s - 1$).

For suppose that $Av \notin V$ for some $v \in \mathbb{R}^p$. For every $\alpha \in \mathbb{R}$, consider the map $f_\alpha : S_0 \to \mathbb{R}^m$ defined by $f_\alpha : (\tau + \beta A) \mapsto \tau(u + \alpha v) + \beta A v$, $\tau \in S'$, $\beta \in \mathbb{R}$. Note that f_0 is of rank $s = \dim S_0$ by our assumption, so that some $s \times s$ minor of the matrix of f_0 is non-zero. The corresponding minor of f_α is thus a nonzero polynomial of α, so that it follows that $\operatorname{rk} f_\alpha = s$ for all but finitely many α. For such an $\alpha \neq 0$, we have that $\operatorname{Ker} f_\alpha = \{0\}$ and thus

$$0 \neq \tau(u + \alpha v) + \beta A v = (\tau + \alpha^{-1}\beta A)(u + \alpha v)$$

for all $\tau \in S'$, $\beta \in \mathbb{R}$ not both zero, so that $B(u + \alpha v) \neq 0$ for all nonzero $B \in S_0$, a contradiction.

Let now T be a minimal covering matrix space, and write $\dim T = n$. We have shown that we can find an $A \in T$ such that $W_0 = \operatorname{Im} A$ satisfies $w_0 = \dim W_0 \leqslant n - 1$. Denote $Z_0 = \{B \in T \,:\, \operatorname{Im} B \subset W_0\}$; we know that $t_0 = \dim Z_0 \geqslant 1$. If $T = Z_0$, then $\delta(T) \leqslant n - 1$ and we are done. Else, write $T = Z_0 \oplus T_1$, also write $\mathbb{R}^m = W_0 \oplus V_1$ and let $\pi_1 : \mathbb{R}^m \to \mathbb{R}^m$ be the projection onto the V_1-component. We claim that

$$T_1^\sharp = \{\pi_1 \tau_1 \,:\, \tau_1 \in T_1\}$$

is also a covering matrix space. Note here that $\pi_1^\sharp : T_1 \to T_1^\sharp$, $\tau_1 \mapsto (\pi_1 \tau_1)$ is an isomorphism. In particular we note that $\delta(T) = w_0 + \delta(T_1^\sharp)$.

Suppose that $T_1^\sharp$ is not a covering matrix space, so we can find a $v_1 \in \mathbb{R}^p$ with $v_1 \notin \cup_{\tau_1 \in T_1, \tau_1 \neq 0} \operatorname{Ker}(\pi_1 \tau_1)$. On the other hand, by minimality of T we can find a $u_1 \in \mathbb{R}^p$ with $u_1 \notin \cup_{\tau_0 \in Z_0,\, \tau_0 \neq 0} \operatorname{Ker} \tau_0$. The maps $g_\alpha : Z_0 \to V$,

$\tau_0 \mapsto \tau_0(u_1 + \alpha v_1)$ and $h_\beta : T_1 \to V_1$, $\tau_1 \mapsto \pi_1(\tau_1(v_1 + \beta u_1))$ have $\operatorname{rk} g_0 = t_0$ and $\operatorname{rk} h_0 = n - t_0$ and thus both $\operatorname{rk} g_\alpha = t_0$ and $\operatorname{rk} h_{\alpha^{-1}} = n - t_0$ for all but finitely many $\alpha \neq 0$ by the same argument as above. Pick such an α and suppose that

$$(\tau_0 + \tau_1)(u_1 + \alpha v_1) = 0$$

for some $\tau_0 \in Z_0$, $\tau_1 \in T_1$. Applying π_1 to both sides we see that we can only have $\tau_1 = 0$, and then $\tau_0 = 0$ as well, a contradiction given that T is a covering matrix space.

In fact, the exact same proof shows that, in general, if T is a minimal covering matrix space, $\mathbb{R}^m = V_0 \oplus V_1$, $T_0 = \{\tau \in T \ : \ \operatorname{Im} \tau \subset V_0\}$, $T = T_0 \oplus T_1$, $\pi_1 : \mathbb{R}^m \to \mathbb{R}^m$ is the projection onto the V_1-component, and $T_1^\sharp = \{\pi_1 \tau_1 \ : \ \tau_1 \in T_1\}$, then $T_1^\sharp$ is a covering matrix space.

We can now repeat the process. We choose a $\pi_1 A_1 \in T_1^\sharp$ such that $W_1 = (\pi_1 A_1)(\mathbb{R}^p)$ has $w_1 = \dim W_1 \leqslant n - t_0 - 1 \leqslant n - 2$. We write $Z_1 = \{\tau_1 \in T_1 \ : \ \operatorname{Im}(\pi_1 \tau_1) \subset W_1\}$, $T_1 = Z_1 \oplus T_2$ (and so $T = (Z_0 \oplus Z_1) \oplus T_2$), $t_1 = \dim Z_1 \geqslant 1$, $V_1 = W_1 \oplus V_2$ (and so $\mathbb{R}^m = (W_0 \oplus W_1) \oplus V_2$), $\pi_2 : \mathbb{R}^m \to \mathbb{R}^m$ is the projection onto the V_2-component, and $T_2^\sharp = \{\pi_2 \tau_2 \ : \ \tau_2 \in T_2\}$, so that $T_2^\sharp$ is also a covering matrix space, etc.

We conclude that

$$\begin{aligned}\delta(T) &= w_0 + \delta(T_1) = w_0 + w_1 + \delta(T_2) = \cdots \\ &\leqslant (n-1) + (n-2) + \cdots \leqslant \binom{n}{2}.\end{aligned}$$

(b) We consider $\binom{n}{2} \times n$ matrices whose rows are indexed by $\binom{n}{2}$ pairs (i,j) of integers $1 \leqslant i < j \leqslant n$. For every $u = (u_1, u_2, \ldots, u_n) \in \mathbb{R}^n$, consider the matrix $A(u)$ whose entries $A(u)_{(i,j),k}$ with $1 \leqslant i < j \leqslant n$ and $1 \leqslant k \leqslant n$ are given by

$$(A(u))_{(i,j),k} = \begin{cases} u_i, \ k = j, \\ -u_j, \ k = i, \\ 0, \ \text{otherwise.} \end{cases}$$

It is immediate that $\operatorname{Ker} A(u) = \mathbb{R} \cdot u$ for every $u \neq 0$, so that $S = \{A(u) \ : \ u \in \mathbb{R}^n\}$ is a covering matrix space, and in fact a minimal one.

On the other hand, for any $1 \leqslant i < j \leqslant n$, we have that $A(e_i)_{(i,j),j}$ is the $(i,j)^{\text{th}}$ vector in the standard basis of $\mathbb{R}^{\binom{n}{2}}$, where e_i denotes the i^{th} vector in the standard basis of $\mathbb{R}^n$. This means that $\delta(S) = \binom{n}{2}$, as required.

Solution 2. (for part a)

Let us denote $X = \mathbb{R}^p$, $Y = \mathbb{R}^m$. For each $x \in X$, denote by $\mu_x : T \to Y$ the evaluation map $\tau \mapsto \tau(x)$. As T is a covering matrix space, $\ker \mu_x > 0$ for every $x \in X$. Let $U = \{x \in X : \dim \ker \mu_x = 1\}$.

Let T_1 be the span of the family of subspaces $\{\ker \mu_x \ : \ x \in U\}$. We claim that $T_1 = T$. For suppose the contrary, and let $T' \subset T$ be a subspace of T of dimension $n - 1$ such that $T_1 \subseteq T'$. This implies that T' is a covering matrix space. Indeed, for $x \in U$, $(\ker \mu_x) \cap T' = \ker \mu_x \neq 0$, while for $x \notin U$ we have $\dim \mu_x \geq 2$, so that $(\ker \mu_x) \cap T' \neq 0$ by computing dimensions. However, this is a contradiction as T is minimal.

Now we may choose $x_1, x_2, \ldots, x_n \in U$ and $\tau_1, \tau_2, \ldots, \tau_n \in T$ in such a way that $\ker \mu_{x_i} = \mathbb{R}\tau_i$ and τ_i form a basis of T. Let us complete $x_1, \ldots, x_n$ to a sequence $x_1, \ldots, x_d$ which spans X. Put $y_{ij} = \tau_i(x_j)$. It is clear that y_{ij} span the vector space generated by the columns of all matrices in T. We claim that the subset $\{y_{ij} : i > j\}$ is enough to span this space, which clearly implies that $\delta(T) \leqslant \binom{n}{2}$.

We have $y_{ii} = 0$. So it is enough to show that every y_{ij} with $i < j$ can be expressed as a linear combination of y_{ki}, $k = 1, \ldots, n$. This follows from the following lemma:

Lemma. For every $x_0 \in U$, $0 \neq \tau_0 \in \ker \mu_{x_0}$ and $x \in X$, there exists a $\tau \in T$ such that $\tau_0(x) = \tau(x_0)$.

Proof. The operator μ_{x_0} has rank $n - 1$, which implies that for small ε the operator $\mu_{x_0 + \varepsilon x}$ also has rank $n - 1$. Therefore one can produce a rational function $\tau(\varepsilon)$ with values in T such that $m_{x_0 + \varepsilon x}(\tau(\varepsilon)) = 0$. Taking the derivative at $\varepsilon = 0$ gives $\mu_{x_0}(\tau_0) + \mu_x(\tau'(0)) = 0$. Therefore $\tau = -\tau'(0)$ satisfies the desired property.

Remark. Lemma in solution 2 is the same as the claim $\operatorname{Im} A \subset V$ at the beginning of solution 1, but the proof given here is different. It can be shown that all minimal covering spaces T with $\dim T = \binom{n}{2}$ are essentially the ones described in our example.