Solutions for the AAC Competition Problems 2010

1. We will say that a matrix is *sensitive* if its rank changes upon any change of any of its entries. What are the possible ranks of sensitive $n \times n$ matrices

a) over the field of complex numbers?

b) over an arbitrary field?

Solution:
a) Let A be an $n \times n$ matrix over $\mathbb{C}$. Let c_{ij} be the (i,j)-cofactor of A. Then $\det A = c_{ij}a_{ij} + d_{ij}$ where $d_{ij} = \sum_{k \neq j} c_{ik}a_{ik}$. Note that neither c_{ij} nor d_{ij} depend on a_{ij}. If $\det A \neq 0$, then, upon changing a_{ij} to any value a'_{ij} if $c_{ij} = 0$ and to any value $a'_{ij} \neq -\frac{d_{ij}}{c_{ij}}$ if $c_{ij} \neq 0$, we obtain a matrix A' with $\det A' \neq 0$. This shows that $n \times n$ matrices of rank n are not sensitive.

For any $0 \leq r < n$, we will construct a sensitive $n \times n$ matrix A of rank r. If $r = 0$, then $A = 0$ is a sensitive matrix of rank r. So assume $r > 0$. Let $\mathbf{b}_1, \dots, \mathbf{b}_r$ be linearly independent vectors in $\mathbb{C}^n$ such that the entries of each $\mathbf{b}_j$ add to zero. Such vectors exist since $r \leq n-1$; for example, we can take $\mathbf{b}_1 = \begin{bmatrix} 1 & -1 & 0 & 0 & \dots & 0 \end{bmatrix}^T$, $\mathbf{b}_2 = \begin{bmatrix} 0 & 1 & -1 & 0 & \dots & 0 \end{bmatrix}^T$, etc. Let A be the $n \times n$ matrix whose first r columns are $\mathbf{b}_1, \dots, \mathbf{b}_r$ and the remaining columns are equal to $\sum_{j=1}^r \mathbf{b}_j$. Then $\text{rank} A = r$. Note also that each column of A is a linear combination of the other columns. If we change one entry in one column in any way, then the entries of the new column will no longer add to zero and, consequently, this column will not be a linear combination of the other columns. It follows that the resulting matrix A' has rank $r+1$. Therefore, A is sensitive.

b) The above construction of a sensitive $n \times n$ matrix of rank $r < n$ works over any field $\mathbb{K}$. Also, the above proof that all $n \times n$ matrices of rank n are not sensitive is valid over any field $\mathbb{K}$ except the field of two elements. If $\mathbb{K} = \{0,1\}$, then the proof still goes through unless $c_{ij} \neq 0$ for all i,j (then we may not be able to change a_{ij} in the desired way). But then $c_{ij} = 1$ for all i,j and, therefore, $A^{-1} = \frac{1}{\det A}[c_{ji}]$ has rank 1. This forces $n = 1$.

Answer: the possible ranks of sensitive $n \times n$ matrices over a field $\mathbb{K}$ are $0, 1, \dots, n-1$ except in the case $|\mathbb{K}| = 2$ and $n = 1$ (then the possible ranks are 0 and 1).

2. Let $A = [a_{ij}]$ be an $n \times n$ real symmetric matrix whose entries satisfy (i) $a_{ii} = 1$ and (ii) $\sum_{j=1}^n |a_{ij}| \leq 2$ for all i. Prove that $0 \leq \det A \leq 1$.

Solution: Since A is real and symmetric, its eigenvalues are real. Let λ be one of them and let $\mathbf{x}$ be a corresponding eigenvector. Then, for any i, we have

$$\sum_{j \neq i} a_{ij}x_j = (\lambda - a_{ii})x_i. \tag{1}$$

Choose i so that $|x_i|$ is maximal among all $|x_j|$, $j = 1, \dots, n$. Then

$$\left| \sum_{j \neq i} a_{ij} x_j \right| \leq |x_i| \sum_{j \neq i} |a_{ij}|. \tag{2}$$

Combining (1) and (2) and canceling $|x_i|$, we obtain Gershgorin's inequality:

$$|\lambda - a_{ii}| \leq \sum_{j \neq i} |a_{ij}|.$$

Since $a_{ii} = 1$ and $\sum_{j \neq i} |a_{ij}| \leq 1$, we have $|\lambda - 1| \leq 1$, i.e., $0 \leq \lambda \leq 2$.

Now let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of A. We already know that $\lambda_i \geq 0$ for all i, so we can apply the Arithmetic Mean/Geometric Mean Inequality:

$$(\lambda_1 \cdots \lambda_n)^{\frac{1}{n}} \leq \frac{1}{n}(\lambda_1 + \cdots + \lambda_n).$$

This can be rewritten as follows:

$$(\det A)^{\frac{1}{n}} \leq \frac{1}{n} \operatorname{tr} A.$$

Since $\operatorname{tr} A = n$, we get $\det A \leq 1$, as desired.

3. Let $R = \mathbb{Z}/m\mathbb{Z}$, the ring of residues modulo m ($m > 1$). If $a \in \mathbb{Z}$ is coprime to m, then the map $f_a(x) = ax$ is a bijection $R \to R$, so f_a can be regarded as a permutation of m symbols. Let $\sigma(m, a)$ be the sign of this permutation.

a) Show that if $m = 2^\alpha k$ where k is odd and $\alpha \geq 1$, then $\sigma(m, a) = \sigma(2^\alpha, a)$ for all a coprime to m.

b) Determine $\sigma(2^\alpha, a)$ as a function of α and a.

Solution:

Lemma 1. Let X be a finite set and let Z_i, $i = 1, \dots, m$, be a partition of X. Let π be a permutation of X that leaves each subset Z_i invariant. Let π_i be the restriction of π to Z_i and let ε_i be the sign of π_i. Then the sign of π is $\varepsilon_1 \cdots \varepsilon_m$.

Proof. The disjoint cycle decomposition of π is the combination of the disjoint cycle decompositions of π_i, $i = 1, \dots, m$. □

Lemma 2. Let X_1 and X_2 be finite sets and let $X = X_1 \times X_2$. Let π_i be a permutation of X_i, $i = 1, 2$, and let $\pi = \pi_1 \times \pi_2$, i.e., π is the permutation of X defined by $\pi((x_1, x_2)) = (\pi_1(x_1), \pi_2(x_2))$ for all $x_1 \in X_1$ and $x_2 \in X_2$. Let ε_i be the sign of π_i, $i = 1, 2$. Then the sign of π is $\varepsilon_1^{|X_2|} \varepsilon_2^{|X_1|}$.

Proof. Let $\pi' = \pi_1 \times id_{X_2}$ and $\pi'' = id_{X_1} \times \pi_2$. Then $\pi = \pi' \circ \pi''$. Now, X can be partitioned into the sets $Z_y := X_1 \times \{y\}$, where $y \in X_2$. Clearly, π' leaves each Z_y invariant; the restriction of π' acts on each Z_y in the same way as π_1 acts on X_1, namely, $\pi'((x_1, y)) = (\pi_1(x_1), y)$ for all $x_1 \in X_1$. By Lemma 1, the sign of π' is $\varepsilon_1^{|X_2|}$. Similarly, the sign of π'' is $\varepsilon_2^{|X_1|}$. The result follows. $\square$

a) Let R_1 be the ring of residues modulo 2^α and let R_2 be the ring of residues modulo k. By Chinese Remainder Theorem, the map $\iota : R \to R_1 \times R_2$ defined by $\iota(x) = (x \bmod 2^\alpha, x \bmod k)$ is an isomorphism of rings. Let $f_a^{(1)}(x_1) = ax_1$ for all $x_1 \in R_1$ and $f_a^{(2)}(x_2) = ax_2$ for all $x_2 \in R_2$. According to our notation, the sign of $f_a^{(1)}$ is $\varepsilon_1 = \sigma(2^\alpha, a)$ and the sign of $f_a^{(2)}$ is $\varepsilon_2 = \sigma(k, a)$. One immediately verifies that $\iota \circ f_a \circ \iota^{-1} = f_a^{(1)} \times f_a^{(2)}$, so the sign of f_a is the same as the sign of $f_a^{(1)} \times f_a^{(2)}$. By Lemma 2, the sign of the latter is $\varepsilon_1^{|R_2|}\varepsilon_2^{|R_1|}$. Since $|R_2| = k$ is odd and $|R_1| = 2^\alpha$ is even ($\alpha \geq 1$), we obtain $\varepsilon_1^{|R_2|}\varepsilon_2^{|R_1|} = \varepsilon_1$.

b) If $\alpha = 1$, then $f_a = id_R$, so $\sigma(2^\alpha, a) = 1$. So assume $\alpha \geq 2$. We partition R into $R_i := \{x \in R \mid x \equiv 2^i\ell \pmod{2^\alpha} \text{ for some odd } \ell\}$, $i = 0, 1, \ldots \alpha$. Since a is odd, the subsets R_i are invariant under f_a. (Note that R_0 is the group of invertible residues modulo 2^α.) Let $f_a^{(i)}$ be the restriction of f_a to R_i and let ε_i be the sign of $f_a^{(i)}$.

First we determine ε_0. Note that R_0 can be partitioned into two subsets according to the remainder mod 4, namely, $R_0^+ := \{x \in R \mid x \equiv 1 \pmod 4\}$ and $R_0^- := \{x \in R \mid x \equiv 3 \pmod 4\} = -R_0^+$. ($R_0^+$ is a subgroup in R_0 of index 2 and R_0^- is the coset of -1.) Suppose $a \equiv 1 \pmod 4$. Then R_0^+ and R_0^- are invariant under f_a. Since $f_a(-x) = -f_a(x)$, we see that f_a acts in essentially the same way on R_0^+ and on R_0^-. By Lemma 1, the sign of $f_a^{(0)}$ is $+1$. Now, if $a \equiv 3 \pmod 4$, then $-a \equiv 1 \pmod 4$. Since $f_a = f_{-1} \circ f_{-a}$, we see that the sign of $f_a^{(0)}$ is equal to the sign of $f_{-1}^{(0)}$, which is easy to determine. Indeed, f_{-1} swaps the elements x and $-x$ for $x \equiv 1, \ldots, 2^{\alpha-1}$, and fixes 0 and $2^{\alpha-1}$. Hence $f_{-1}^{(0)}$ is a product of $|R_0|/2 = 2^{\alpha-2}$ transpositions. Thus, the sign of $f_{-1}^{(0)}$ is $+1$ if $\alpha > 2$ and -1 if $\alpha = 2$. To summarize,

$$\varepsilon_0 = \begin{cases} (-1)^{\frac{a-1}{2}} & \text{if } \alpha = 2; \\ +1 & \text{if } \alpha > 2. \end{cases}$$

Now pick $i < \alpha - 1$. Then the mapping $\ell \mapsto 2^i\ell$ gives a bijection between odd residues modulo $2^{\alpha-i}$ and R_i. This bijection commutes with f_a. Hence

$$\varepsilon_i = \begin{cases} (-1)^{\frac{a-1}{2}} & \text{if } \alpha - i = 2; \\ +1 & \text{if } \alpha - i > 2. \end{cases}$$

Since f_a fixes 0 and $2^{\alpha-1}$, we have $\varepsilon_{\alpha-1} = \varepsilon_\alpha = +1$. By Lemma 1, we conclude that the sign of f_a is $\varepsilon_0\varepsilon_1 \cdots \varepsilon_\alpha = \varepsilon_{\alpha-2} = (-1)^{\frac{a-1}{2}}$.

Answer: for $m = 2^\alpha k$, with k odd, we have $\sigma(m, a) = \begin{cases} (-1)^{\frac{a-1}{2}} & \text{if } \alpha > 1; \\ +1 & \text{if } \alpha = 1. \end{cases}$

Remark. The above formula covers the case of even m. The result is radically different when m is odd: $\sigma(m, a)$ is then equal to $\left(\frac{a}{m}\right)$, the Jacobi symbol known from Number Theory. Exercise: prove this fact.

4. Show that if a field $\mathbb{K}$ is not algebraically closed, then the solution set in $\mathbb{K}^n$ of any system of equations

$$f_1(x_1, \ldots, x_n) = \ldots = f_m(x_1, \ldots, x_n) = 0,$$

where $f_1, \ldots, f_m$ are polynomials in n variables over $\mathbb{K}$, coincides with the solution set of one equation $F(x_1, \ldots, x_n) = 0$, for some polynomial F in n variables over $\mathbb{K}$. [For example, if $\mathbb{K} = \mathbb{R}$, then we can take $F = f_1^2 + \cdots + f_m^2$.]

Solution: First we show by induction on m that there exists a polynomial $H_m(y_1, \ldots, y_m)$ such that the only solution of the equation $H_m = 0$ is $(0, \ldots, 0)$. Consider $m = 2$. Since $\mathbb{K}$ is not algebraically closed, there exists a polynomial $h(x)$ of degree $d \geq 2$ that has no roots in $\mathbb{K}$. Set $H_2(y_1, y_2) = y_2^d h(\frac{y_1}{y_2})$. Then the only solution of the equation $H_2 = 0$ is $(0, 0)$, as desired. Assume that H_{m-1} has been constructed. Set $H_m(y_1, \ldots, y_m) = H_2(y_1, H_{m-1}(y_2, \ldots, y_m))$.

Now, the system of equations $f_1 = 0, \ldots, f_m = 0$ is equivalent to the single equation $F = 0$ where $F(x_1, \ldots, x_n) = H_m(f_1, \ldots, f_m)$.

5. We will say that a finite nonzero associative commutative ring (possibly without identity element) is *magical* if the product of all its nonzero elements is not equal to 0 or -1 (if the identity element exists). Find all magical rings.

Solution: Let R be a magical ring. Then R is not a field. Indeed, the product of all nonzero elements in a finite field is -1, because each factor except 1 and -1 cancels out with its inverse. Hence R contains a zero divisor x. Since the product of all nonzero elements is not zero, the only element $r \neq 0$ with the property $xr = 0$ is x itself. Consider the mapping $f : R \to R$ defined by $f(r) = xr$. This is an endomorphism of the additive group of R. The kernel of f is the set $\{0, x\}$ and the image is contained in the kernel. If the image is $\{0\}$, then $R = \{0, x\}$, the multiplication of R is zero and the addition is defined by $x + x = 0$. So assume that the image of f is $\{0, x\}$, i.e., it coincides with the kernel. Then R consists of four elements, say, $R = \{0, x, a, b\}$. Since a, b are not in the kernel of f, we have $ax = x = bx$. It follows that $abx = x$, so ab is not in the kernel of f and hence $ab = a$ or $ab = b$. These cases are symmetric, so assume without loss of generality that $ab = a$.

The additive group of R is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. In the first case, there is a unique subgroup of order two, $\{0, x\}$. Hence $a = -b$. It follows that the mapping $\mathbb{Z}_4 \to R$ defined by $0 \mapsto 0$, $1 \mapsto b$, $2 \mapsto x$, $3 \mapsto a$ is an isomorphism of rings. In the second case, $b = a + x$ and hence $b^2 = (a + x)b = a + x = b$. Therefore, b is the identity element of R. Writing 1 for b, we obtain $R = \{0, 1, x, x + 1\}$, with multiplication defined by $x^2 = 0$. This ring is isomorphic to the ring of matrices $\left\{ \begin{bmatrix} \lambda & \mu \\ 0 & \lambda \end{bmatrix} \mid \lambda, \mu \in \mathbb{Z}_2 \right\}$ and to the group ring of the cyclic group of order 2 with coefficients in $\mathbb{Z}_2$.

Answer: Up to isomorphism, there are exactly three magical rings:

- the additive group $\mathbb{Z}_2$ with zero multiplication,
- $\mathbb{Z}_4$,
- the group ring $\mathbb{Z}_2 G$ where G is the cyclic group of order 2.

6. Let G be a group and let e be its identity element. We will say that an element $a \in G$ is *engaged* if a commutes with exactly three elements: e, a and some element b (distinct from e and a). If this is the case, we will also say that a is engaged to b.

a) Prove that the relation *engaged to* is symmetric: if a is engaged to b, then b is engaged to a.

b) Prove that if G is a finite group, then one of the following three possibilities takes place: (i) there are no engaged elements, (ii) exactly one third of the elements are engaged, (iii) exactly two thirds of the elements are engaged.

c) Give examples of groups that realize each possibility in part (b).

Solution:
a) Suppose a is engaged to b. Then a commutes with ab, and hence ab is one of the three elements: e, a or b. Since $a \neq e$ and $b \neq e$, we have $ab = e$, i.e., $b = a^{-1}$. The centralizer of a is the same as the centralizer of a^{-1}, so b commutes with exactly three elements: e, b and a, which means that b is engaged to a. (Note also that the order of a is equal to 3. Indeed, it cannot be more than 3, because a commutes with all powers of a, and it cannot be less than 3, because $a \neq e$ and $a \neq b$.)

b) Assume that G is a finite group and a is an engaged element of G. Since the centralizer of a consists of three elements, the conjugacy class of a has order $\frac{1}{3}|G|$. One shows immediately that if a is engaged to b, then xax^{-1} is engaged to xbx^{-1}. Hence all elements in the conjugacy class of a are engaged. If there is an engaged element a' that is not conjugate to a, then the conjugacy class of a' is disjoint from the conjugacy class of a and has order $\frac{1}{3}|G|$. Finally, there cannot be an engaged element outside the conjugacy classes of a and a', because otherwise all elements of G would be engaged, which is impossible (since e is not engaged).

c) Any group whose order is not divisible by 3 cannot have any engaged elements by part b), or because any engaged element has order 3. The symmetric group S_3 has exactly two engaged elements (the 3-cycles), i.e., $\frac{1}{3}|S_3|$. The cyclic group C_3 has exactly two engaged elements, i.e., $\frac{2}{3}|C_3|$.