Algebraic Methods in Combinatorics

Solutions 3

The aim of the homework problems is to help you understand the theory better by actively using it to solve exercises. ***Do not read the solutions*** *before you believe you have solved the problems: it ruins your best way of preparing for the exam. The purpose of this write-up is merely to provide some guideline on how solutions should look like, and to help clean up hazy arguments. For hints, feel free to consult your teaching assistant.*

Problem 1:

(a) Let $A \in \mathcal{A}$ and let $B_1, \dots, B_k \in \mathcal{A}$ be the neighbours of A in G. Then $|A \cap B_i|$ for every i is odd by the definition G. Also, $|(A \cap B_i) \cap (A \cap B_j)| = |A \cap B_i \cap B_j|$ is even for every $i \neq j$. It follows that $A \cap B_1, \dots, A \cap B_k$ is an oddtown, so $k \leq n$.

(b) Construct the independent set greedily by adding an arbitrary vertex to the independent set, deleting all its neighbours, and repeating as long as there are vertices left. Each time we add one vertex to the independent set and delete at most d vertices, so at the end, the independent set has size at least $\frac{m}{d+1}$. This argument can also be described using induction.

(c) Let $A_1, \dots, A_k$ be an independent set in G. Then $|A_i \cap A_j|$ is even for every $i \neq j$ by the definition of G. Also, $|A_i|$ is odd for every i by assumption. Hence, $A_1, \dots, A_k$ is an oddtown, so $k \leq n$. Now, put $m = |\mathcal{A}|$ and let k be the largest size of an independent set in G. Then $k \leq n$ and $k \geq \frac{m}{n+1}$, giving $m \leq n(n+1)$.

Problem 2:

(a) Let A be the $m \times n$ matrix whose rows are $v_1, \dots, v_m$. Then $AA^T = M$, because $M_{i,j} = \sum_{k=1}^{n} (v_i)_k (v_j)_k = \langle v_i, v_j \rangle$. Therefore, $\text{rank} M \leq \text{rank} A \leq n$. Here we use that $\text{rank}(AB) \leq \text{rank}(A), \text{rank}(B)$, and that if A is $m \times n$ then $\text{rank}(A) \leq m, n$.

We have $\|v_i - v_j\|^2 = \|v_i\|^2 + \|v_j\|^2 - 2\langle v_i, v_j \rangle$. Let B be the $m \times m$ matrix whose ith row is $(\|v_i\|^2, \dots, \|v_i\|^2)$. So in B^T, the ith column is $(\|v_i\|^2, \dots, \|v_i\|^2)^T$. Then $D = B + B^T - 2M$. Observe that all columns of B are the same, they all equal $(\|v_1\|^2, \dots, \|v_m\|^2)^T$. Hence, $\text{rank}(B) \leq 1$, and therefore $\text{rank}(B^T) = \text{rank}(B) \leq 1$. So $\text{rank}(D) \leq \text{rank}(B) + \text{rank}(B^T) + \text{rank}(M) \leq n + 2$. Here we use that rank is subadditive, i.e. $\text{rank}(A + B) \leq \text{rank}(A) + \text{rank}(B)$.

(b) It will be convenient to write $S = \{v_0, \dots, v_m\}$. Our goal is to show that $m \le n$. Take $u_i = v_i - v_0$ for $1 \le i \le m$. Then $\|u_i\| = \|v_i - v_0\| = 1$ for every $1 \le i \le m$, and $\|u_i - u_j\| = \|(v_i - v_0) - (v_j - v_0)\| = \|v_i - v_j\| = 1$ for $1 \le i < j \le m$. Therefore,

$$\langle u_i, u_j \rangle = \frac{1}{2}\left(\|u_i\|^2 + \|u_j\|^2 - \|u_i - u_j\|^2\right),$$

so $\langle u_i, u_i \rangle = 1$ and $\langle u_i, u_j \rangle = \frac{1}{2}$ for $i \ne j$. This means that the Gram matrix M of $u_1, \dots, u_m$ has 1 on the diagonal and $\frac{1}{2}$ everywhere off the diagonal. We proved in class that the determinant of this matrix is non-zero; in general, we showed that if a matrix has $a_1, \dots, a_m$ on the diagonal and λ everywhere off the diagonal, with $\lambda > 0$ and $a_1, \dots, a_m > \lambda$, then the determinant is positive. Hence, $\operatorname{rank}(M) = m$. On the other hand, we proved in Item (a) that $\operatorname{rank}(M) \le n$, so $m \le n$.

(c) For points $x, y, z \in S$, if $\|x - y\| = d_1$ and $\|y - x\| = d_1$, then by the triangle inequality, $\|x - z\| \le \|x - y\| + \|y - z\| \le 2d_1$. As $d_2 > 2d_1$, we cannot have $\|x - z\| = d_2$, so $\|x - z\| = d_1$. This means that there is a partition $[m] = S_1 \cup \dots \cup S_k$ such that for distinct $x, y \in S_i$, $\|x - y\| = d_1$ (for every $i = 1, \dots, k$), and for $x \in S_i, y \in S_j$, $\|x - y\| = d_2$ (for every $1 \le i < j \le k$). Therefore, the (squared) distance matrix D has the form

$$D = \left(\begin{array}{c|c|c}
\begin{matrix} 0 & & d_1^2 & \\ & 0 & & \\ & & 0 & \\ d_1^2 & & & 0 \end{matrix} & d_2^2 & d_2^2 \\ \hline
d_2^2 & \begin{matrix} 0 & & d_1^2 & \\ & 0 & & \\ & & 0 & \\ d_1^2 & & & 0 \end{matrix} & d_2^2 \\ \hline
d_2^2 & d_2^2 & \begin{matrix} 0 & & d_1^2 & \\ & 0 & & \\ & & 0 & \\ d_1^2 & & & 0 \end{matrix}
\end{array}\right)$$

Let J be the all-1 matrix. Then $d_2^2 J - D$ equals

$$d_2^2 J - D = \left(\begin{array}{c|c|c} \begin{matrix} d_2^2 & & & d_2^2 - d_1^2 \\ & d_2^2 & & \\ & & d_2^2 & \\ d_2^2 - d_1^2 & & & d_2^2 \end{matrix} & 0 & 0 \\ \hline 0 & \begin{matrix} d_2^2 & & & d_2^2 - d_1^2 \\ & d_2^2 & & \\ & & d_2^2 & \\ d_2^2 - d_1^2 & & & d_2^2 \end{matrix} & 0 \\ \hline 0 & 0 & \begin{matrix} d_2^2 & & & d_2^2 - d_1^2 \\ & d_2^2 & & \\ & & d_2^2 & \\ d_2^2 - d_1^2 & & & d_2^2 \end{matrix} \end{array}\right)$$

Since $d_2^2 > d_2^2 - d_1^2 \geq 0$, the determinant of $\begin{pmatrix} d_2^2 & & & d_2^2 - d_1^2 \\ & d_2^2 & & \\ & & d_2^2 & \\ d_2^2 - d_1^2 & & & d_2^2 \end{pmatrix}$ is non-zero. Therefore, $C := d_2^2 J - D$ is invertible, and so $\operatorname{rank}(C) = m$. Recall from Item (a) that $D = B + B^T - 2M$, where B is the matrix whose ith row is $(\|v_i\|^2, \ldots, \|v_i\|^2)$. Hence, $C = d_2^2 J - B - B^T + 2M$. Note that the ith row of $d_2^2 J - B^T$ is $(d_2^2 - \|v_1\|^2, \ldots, d_2^2 - \|v_m\|^2)$. So all rows of $d_2^2 J - B^T$ are the same. Therefore, $\operatorname{rank}(d_2^2 J - B^T) = 1$. It follows that

$$\operatorname{rank}(C) \leq \operatorname{rank}(B) + \operatorname{rank}(d_2^2 J - B^T) + \operatorname{rank}(M) \leq n + 2,$$

using that $\operatorname{rank}(M) \leq n$. As $\operatorname{rank}(C) = m$, we get $m \leq n + 2$.

Problem 3: For any $a = (a_1, \ldots a_n) \in A$, we define a polynomial $p_a \in \mathbb{F}_3[X_1, \ldots, X_n]$ as follows:

$$p_a(x_1, \ldots, x_n) = \prod_{i=1}^{n} (1 + x_i - a_i).$$

First we show that these $|A|$ polynomials are linearly independent. Note that $p_a(a) = 1$ and, by the given property of A, $p_a(b) = 0$ for any $b \in A, b \neq a$. Now suppose that $\sum_{a \in A} \alpha_a p_a = 0$. Plugging in any $b \in A$, we get $(\sum_{a \in A} \alpha_a p_a)(b) = \alpha_b$, so $\alpha_b = 0$ for all $b \in A$ and we conclude that our polynomials are linearly independent.

Observe that the polynomials $p_a, a \in A$ are multilinear, that is, they are spanned by the set of monomials $\{\prod_{i \in S} x_i \mid S \subseteq [n]\}$. The dimension of this span is equal to the number of subsets of $[n]$, which equals 2^n. Finally, as our polynomials are independent it follows that $|A| \leq 2^n$, finishing the proof.