Algebraic Methods in Combinatorics

Solutions 4

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: As usual, for a set $A \subseteq [n]$, let $\chi_A \in \{0,1\}^n$ denote its characteristic vector. Let $\mathcal{A} = \{A_1, \dots, A_m\}$ and $L = \{l_1, \dots, l_s\}$ with $|A_1| \leq |A_2| \leq \dots \leq |A_m|$. Now, for each $1 \leq i \leq m$, define the polynomial $f_i \in \mathbb{R}[x_1, \dots, x_n]$ as such:

$$f_i(\underline{x}) = \prod_{j : l_j < |A_i|} \left(\underline{x} \cdot \chi_{A_i} - l_j \right).$$

Given this polynomial, let its multilinear version be denoted as $\tilde{f}_i$, so that for all $\underline{x} \in \{0,1\}^n$ we have $\tilde{f}_i(\underline{x}) = f_i(\underline{x})$. Then, we have the following:

1a) For each i, $\tilde{f}_i(\chi_{A_i}) = f_i(\chi_{A_i}) = \prod_{j : l_j < |A_i|} (|A_i| - l_j) \neq 0$.

1b) For each $k < i$, $\tilde{f}_i(\chi_{A_k}) = f_i(\chi_{A_k}) = \prod_{j : l_j < |A_i|} (|A_i \cap A_k| - l_j) = 0$, since $|A_i \cap A_k| \in L$ by assumption and $|A_i \cap A_k| < |A_i|$ (since $|A_k| \leq |A_i|$).

We now define some other polynomials. Specifically, for each set $I \subseteq [n]$ of size at most $s - r$, define $h_I \in \mathbb{R}[x_1, \dots, x_n]$ as such:

$$h_I(\underline{x}) = \prod_{k \in K} (x_1 + x_2 + \dots x_n - k) \prod_{i \in I} x_i.$$

As before, also take their multilinear version and denote it as $\tilde{h}_I$. Then, we have the following:

2a) For each $1 \leq i \leq m$ and I, $\tilde{h}_I(\chi_{A_i}) = 0$ - since $|A_i| = \chi_{A_i}(1) + \dots + \chi_{A_i}(n) \in K$.

2b) For all I, $\tilde{h}_I(\chi_I) \neq 0$ - since for all $k \in K$, $k > s - r \geq |I| = \chi_I(1) + \dots + \chi_I(n)$.

2c) For all $J \neq I$ with $|J| \leq |I|$, $\tilde{h}_I(\chi_J) = 0$.

To finish, we only need to show that the collection of polynomials $\{\tilde{f}_i\} \cup \{\tilde{h}_I\}$ is linearly independent. Indeed, if that is the case, since they live in the space of multilinear polynomials there are at most $\sum_{0\leq i\leq s}\binom{n}{i}$ many of them, and so, since there are $\sum_{0\leq i\leq s-r}\binom{n}{i}$ polynomials $\tilde{h}_I$, we get $m = |\{\tilde{f}_i\}| \leq \sum_{s-r<i\leq s}\binom{n}{i}$.

Suppose then that the polynomials are not linearly independent, so that there exist not all zero γ's such that

$$\sum_i \gamma_i \tilde{f}_i + \sum_I \gamma_I \tilde{h}_I = 0$$

First we show that all γ_i are zero. Indeed, otherwise, let j be minimal such that $\gamma_j \neq 0$. Then, using 1a),1b) and 2b), we can see that

$$0 = \sum_i \gamma_i \tilde{f}_i(\chi_{A_j}) + \sum_I \gamma_I \tilde{h}_I(\chi_{A_j}) = \gamma_j \tilde{f}_j(\chi_{A_j}) + \sum_{i>j} \gamma_i \tilde{f}_i(\chi_{A_j}) = \gamma_j \tilde{f}_j(\chi_{A_j})$$

implies that γ_j is zero, which is a contradiction. Therefore, we have

$$\sum_I \gamma_I \tilde{h}_I = 0$$

Suppose that not all γ_I are zero and let J be minimal such that $\gamma_J \neq 0$. Then, by 2b) and 2c),

$$0 = \sum_I \gamma_I \tilde{h}_I(\chi_J) = \gamma_J \tilde{h}_J(\chi_J) + \sum_{I\neq J:|I|\geq|J|} \gamma_I \tilde{h}_I(\chi_J) = \gamma_J \tilde{h}_J(\chi_J)$$

implies that $\gamma_J = 0$, which is a contradiction.

Problem 2: We work over $\mathbb{F}_p$. Let u_i be the characteristic vector of A_i and v_i the characteristic vector of B_i. Define

$$f_i(x) = \prod_{\ell\in L}(\langle x, u_i\rangle - \ell).$$

Then:

- $f_i(v_i) \neq 0$ for every $1 \leq i \leq m$.
- $f_i(v_j) = 0$ for every $1 \leq i < j \leq m$.

Let $\bar{f}_i$ be the multilinear version of f_i. Then the same holds for $\bar{f}_i$, namely $\bar{f}_i(v_i) \neq 0$ and $\bar{f}_i(v_j) = 0$ for $i < j$. We claim that $\bar{f}_1, \ldots, \bar{f}_m$ are linearly independent. Suppose by contradiction that $\sum_{i=1}^m \alpha_i \bar{f}_i = 0$ and not all α_i are zero. Let j be maximal with $\alpha_j \neq 0$. Then

$$0 = \left(\sum_{i=1}^m \alpha_i \bar{f}_i\right)(v_j) = \sum_{i=1}^m \alpha_i \bar{f}_i(v_j) = \sum_{i=1}^j \alpha_i \bar{f}_i(v_j) = \alpha_j \bar{f}_j(v_j),$$

where the third equality is by the maximality of j, and the last equality is because $\bar{f}_i(v_j) = 0$ for $i < j$. It follows that $\alpha_j = 0$, a contradiction.

Now, $\bar{f}_1, \dots, \bar{f}_m$ are linearly independent polynomials in the space of all multilinear n-variable polynomials of degree at most s. This space has dimension $\sum_{i=0}^{s} \binom{n}{i}$. The claim follows.

Problem 3(a): We partition $\mathcal{A}$ into sets $\mathcal{A}_1, \dots, \mathcal{A}_m$ with the following properties:

1. $|\mathcal{A}_i| \leq k-1$ for every $i = 1, \dots, m$.
2. $|\bigcap_{A \in \mathcal{A}_i} A| \notin L \pmod{p}$ for every $i = 1, \dots, m$.
3. For every $1 \leq i < j \leq m$ and $B \in \mathcal{A}_j$, it holds that $|B \cap (\bigcap_{A \in \mathcal{A}_i} A)| \in L \pmod{p}$.

To achieve this, take $\mathcal{A}_1$ to be a maximal subset of $\mathcal{A}$ of size at most k with $|\bigcap_{A \in \mathcal{A}_1} A| \notin L$ (mod p). Note that such subsets exist because every $\mathcal{A}_1$ with $|\mathcal{A}_1| = 1$ satisfies this, so $\mathcal{A}_1$ is well-defined. Also $|\mathcal{A}| \leq k-1$ by the assumption in the problem. For every $B \in \mathcal{A} \setminus \mathcal{A}_1$, it holds that $|B \cap (\bigcap_{A \in \mathcal{A}_i} A)| \in L \pmod{p}$ by the maximality of $\mathcal{A}_1$. Now repeat this for $\mathcal{A} \setminus \mathcal{A}_1$ to find $\mathcal{A}_2, \mathcal{A}_3, \dots$. Namely, for each $i \geq 1$, take $\mathcal{A}_i$ to be a maximal subset of $\mathcal{A} \setminus (\mathcal{A}_1 \cup \dots \cup \mathcal{A}_{i-1})$ of size at most k with $|\bigcap_{A \in \mathcal{A}_i} A| \notin L \pmod{p}$. This results in a partition $\mathcal{A}_1, \dots, \mathcal{A}_m$ with the desired properties.

For $i = 1, \dots, m$, let B_i be an arbitrary set in $\mathcal{A}_i$, and put $A_i := \bigcap_{A \in \mathcal{A}_i} A$. Then $A_i \cap B_i = A_i$, so $|A_i \cap B_i| \notin L \pmod{p}$. Also, for $1 \leq i < j \leq m$, we have $|A_i \cap B_j| = |B \cap (\bigcap_{A \in \mathcal{A}_i} A)| \in L$ (mod p). So by Problem 2, $m \leq \sum_{i=0}^{s} \binom{n}{i}$. On the other hand, $m \geq |\mathcal{A}|/(k-1)$ because $|\mathcal{A}_i| \leq k-1$ for every i. So $|\mathcal{A}| \leq (k-1)\sum_{i=0}^{s} \binom{n}{i}$, as required.

Problem 3(b): We assume that $s < p$ (otherwise $L = \{0, \dots, p-1\}$ and there is no set A with $|A| \notin L \pmod{p}$).

Partition $[n]$ into a $X_1, \dots, X_{k-1}, Y$ where $|X_i| = p$ and $|Y| = n - (k-1)p$. For $i = 1, \dots, k-1$, let $\mathcal{A}_i = \{X_i \cup A : A \subseteq Y, |A| = s\}$, and let $\mathcal{A} = \bigcup_{i=1}^{k-1} \mathcal{A}_i$. Then

$$|\mathcal{A}| = (k-1) \cdot \binom{n-(k-1)p}{s} = (k-1) \cdot \frac{(1-o(1))n^s}{s!}$$

(for fixed $s < p$ and k for n tending to infinity). Note that $\sum_{i=0}^{s} \binom{n}{i} = (1+o(1))\binom{n}{s} \leq (1+o(1))\frac{n^s}{s!}$ (again, assuming that s is fixed and n grows), so indeed $\mathcal{A}$ asymptotically achieves the bound from Problem 3(a).

Now take $L = \{0, \dots, s-1\}$. For every $A \in \mathcal{A}_i$ we have $|A| = s + p \equiv s \pmod{p}$, so $|A| \notin L \pmod{p}$. Now let $A_1, \dots, A_k \in \mathcal{A}$ be distinct. For $i = 1, \dots, k$, let $\ell_i \in \{1, \dots, k-1\}$ such that $A_i \in \mathcal{A}_{\ell_i}$, and write $A_i = X_{\ell_i} \cup B_i$ for $B_i \subseteq Y$, $|B_i| = s$. By pigeonhole, there are

$1 \leq i < j \leq k$ such that $\ell_i = \ell_j$. Then $B_i \neq B_j$ (because $A_i \neq A_j$), so $|B_i \cap B_j| < s$. Hence, $|B_1 \cap \cdots \cap B_k| < s$, which implies that $|A_1 \cap \cdots \cap A_k| \equiv |B_1 \cap \cdots \cap B_k| \in L \pmod{p}$.