Algebraic Methods in Combinatorics

Solutions of Assignment 13

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: We follow the proof of Theorem 3.6. Write $v := v(G)$. By definition, we know that $e(G) = vd(G)/2 > v(p-1)$. For each $e \in E(G)$ we define a variable $x_e \in \mathbb{F}_p$. Now, for each vertex $v \in V(G)$, we define the polynomial $p_v((x_e)_e) = \sum_{e:v\in e} x_e^{p-1}$. Since $\sum_{v\in V(G)} \deg p_v = v(p-1) < e(G)$, where the RHS is the number of variables, we may apply the Chevalley–Warning Theorem to conclude that the number of simultaneous solutions $(x_e)_{e\in E(G)}$ to all the p_v is divisible by p. There is a trivial solution given by $x_e = 0$ for all $e \in E(G)$, so there must exist another solution in which not all variables are 0.

Note that for any $x \in \mathbb{F}_p$, $x^{p-1} = 1$ in $\mathbb{F}_p$ if and only if $x \neq 0$. Thus, if $\sum_{e:v\in e} x_e^{p-1} = 0$, i.e. $p_v((x_e)_e) = 0$, and $|\{e : v \in e, x_e \neq 0| > 0$, then due to the fact that $d_G(v) \leq 2p-1$, it must hold that $|\{e : v \in e, x_e \neq 0| = p$. It follows that the subgraph having edge set $\{e \in E(G) : x_e \neq 0\}$ is 3-regular and nonempty. $\square$

Problem 2: Let us first give the proof following the hints. Denote $y_i = x_1 + x_2 + \cdots + x_i$ for all $i \in [n]$ with the convention that $y_0 = 0$. Note that $y_i \in \mathbb{Z}_n$ for all i. By the pigeonhole principle, among $y_0, y_1, \ldots, y_n$, there exist some $0 \leq i < j \leq n$ such that $y_i = y_j$. This implies that $x_{i+1} + \cdots + x_j = 0$. We can safely take $I := \{i+1, i+2, \ldots, j\}$.

The second proof is to apply the Erdős-Ginzburg-Ziv Theorem. Let us add $x_{n+1} = x_{n+2} = \ldots, x_{2n-1} = 0$. By the Erdős-Ginzburg-Ziv Theorem, there exists a set $J \subseteq [2n-1]$ of size $|J| = n$ such that $\sum_{i\in J} x_i = 0$. Taking $I = J \cap [n]$, we obtain the desired set. $\square$

Problem 3: We intend to use the Chevalley-Warning Theorem. For this purpose, we define polynomials $f_1, f_2, f_3 \in \mathbb{F}[x_1, x_2, \ldots, x_{3p-1}]$ as follows:

$$f_1(x_1, x_2, \ldots, x_{3p-1}) = \sum_{i=1}^{3p-1} x_i^{p-1},$$
$$f_2(x_1, x_2, \ldots, x_{3p-1}) = \sum_{i=1}^{3p-1} x_i^{p-1} a_i,$$
$$f_3(x_1, x_2, \ldots, x_{3p-1}) = \sum_{i=1}^{3p-1} x_i^{p-1} b_i.$$

We have $\sum_{i=1}^{3} \deg f_i = 3(p-1)$ and the number of variables is $3p-1$, so by the Chevalley-Warning Theorem, the number of common roots of f_1, f_2, f_3 is divisible by p. Since the all-zero vector is a common root of f_1, f_2, f_3 there exists some non-zero vector $x = (x_1, \ldots, x_{3p-1})$ for which $f_i(x) = 0, 1 \le i \le 3$. Consider the set $I = \{i \mid x_i \neq 0\}$ Recall that $y^{p-1} = 1$ for all $y \in \mathbb{F}_p \setminus \{0\}$, so for the set I, we have:

$$\sum_{i \in I} 1 = 0 \qquad \text{(because } f_1(x) = 0\text{)},$$
$$\sum_{i \in I} a_i = 0 \qquad \text{(because } f_2(x) = 0\text{)},$$
$$\sum_{i \in I} b_i = 0 \qquad \text{(because } f_3(x) = 0\text{)}.$$

The first line implies that $|I|$ is divisible by p. Since we assumed x is a non-trivial solution, we have $|I| > 0$ and since $|I| \le 3p-1$, it follows that $|I| = p$ or $|I| = 2p$. In the former case we are done, whereas in the latter, we can take $I' = [3p] \setminus I$, for which we have $\sum_{i \in I'} v_i = \sum_{i \in [3p]} v_i - \sum_{i \in I} v_i = 0 - 0 = 0$. $\square$

Problem 4: We follow the proof of Lemma 3.28. If $|A| + |B| \ge p + 3$ then for any $x \in \mathbb{F}_p$, we have

$$|(x - A) \cap B| = |x - A| + |B| - |(x - A) \cup B| \ge |A| + |B| - p \ge 3$$

so there exist distinct $a_1, a_2, a_3 \in A$ and (distinct) $b_1, b_2, b_3 \in B$ such that $x - a_i = b_i$ for $i \in [3]$. Note that the number of solutions $a \in \mathbb{F}_p$ such that $a(x - a) = 1$ is at most 2 (using that $\mathbb{F}_p$ is a finite field). Thus, $a_i b_i = 1$ holds for at most two $i \in [3]$. In other words, there exist $i \in [3]$ such that $a_i b_i \neq 1$. Since $a_i + b_i = x$, it holds that $x \in X$. As this holds for all $x \in \mathbb{F}_p$, we know that $|X| = p$ when $|A| + |B| \ge p + 3$.

Otherwise, we have $|A| + |B| \le p + 2$. Suppose for sake of contradiction that $|X| \le |A| + |B| - 4$. Then we may choose $X' \supset X$ such that $|X'| = |A| + |B| - 4$. Now define the polynomial $f(x,y) = (xy-1)\prod_{c\in X'}(x+y-c)$ over $\mathbb{F}_p$ and observe that $f=0$ on $A\times B$ and $\deg f = |X'|+2 = (|A|-1)+(|B|-1)$. Moreover, observe that the coefficient of the term $x^{|A|-1}y^{|B|-1}$ in f is exactly $\binom{|A|+|B|-4}{|A|-2} \pmod p$. Now note that

$$\binom{|A|+|B|-4}{|A|-2} = \frac{(|A|+|B|-4)!}{(|A|-2)!(|B|-2)!} \neq 0 \pmod p,$$

since the numerator of the above expression is a product of positive integers of size at most $|A|+|B|-4 < p$. Thus we may apply Corollary 3.23 to reach a contradiction.

Problem 5(a): This is a very standard exercise in Linear Algebra. Here, we give a proof using Hilbert's Nullstellensatz. Let us consider $\det M$ as a polynomial in $\mathbb{C}[x_1,\ldots,x_n]$. Note that whenever $x_i = x_j$ for any $i\neq j$, M contains two identical rows, so $\det M = 0$. In other words, for fixed $i\neq j$, $\det M$ vanishes over all zeros of the polynomial $x_i - x_j$. By Hilbert's Nullstellensatz, there exists some positive integer k such that $(x_i-x_j)\mid \det(M)^k$. Because $x_i - x_j$ is a linear polynomial, and hence irreducible, it follows that $(x_i-x_j)\mid\det(M)$. Therefore, we can write $\det(M) = \prod_{i>j}(x_i-x_j)\cdot Q(x_1,\ldots,x_n)$ since $\prod_{i>j}(x_i-x_j)$ is the minimal polynomial divisible by all polynomials $x_i-x_j, i\neq j$. Now we need to show that $Q(x_1,\ldots,x_n)=1$. Note that $\deg(\det(M)) = \binom{n}{2} = \deg(\prod_{i>j}(x_i-x_j))$ so $\deg Q = 0$, implying that $Q=c$ for some $c\in\mathbb{C}$. Finally, the coefficient of $x_1^0x_2^1\ldots x_n^{n-1}$ equals 1 in $\det(M)$ and 1 in $\prod_{i>j}(x_i > x_j)$, so $c=1$. $\square$

Problem 5(b) If $n=p$, then $A=B=\mathbb{F}_p$. In this case, we can simply take $a_i = b_i = i-1$ for $i=1,\ldots,n$. As $p\geq 3$, all (a_i+b_i) are distinct, as desired.

From now on, we assume that $n\leq p-1$. Denote an arbitrary ordering of A by $a_1,a_2,\ldots,a_n$. Consider the following polynomial defined over $\mathbb{F}_p$,

$$f(x_1,\ldots,x_n) := \prod_{i>j}(x_i-x_j)\prod_{i>j}(x_i+a_i-x_j-a_j).$$

Notice that any $x_1,\ldots,x_n\in B$ with $f(x_1,\ldots,x_n)\neq 0$ is an ordering of B where all (a_i+x_i) are distinct (we may take $b_i = x_i$ for all i). Since $\deg f = n(n-1)$ and $|B| = n > n-1$, by Combinatorial Nullstellensatz (Corollary 3.23), it suffices to show that the coefficient of $x_1^{n-1}\ldots x_n^{n-1}$ is nonzero. To this end, notice that the coefficient of $x_1^{n-1}\ldots x_n^{n-1}$ in f is the same as the coefficient of $x_1^{n-1}\ldots x_n^{n-1}$ in $h(x_1,\ldots,x_n) := \prod_{i>j}(x_i-x_j)\prod_{i>j}(x_i-x_j)$. By 5(a), $h(x_1,\ldots,x_n) = \det(M)^2$. Now, recall the Leibniz formula for determinants that

$$\det(M) = \sum_{\pi\in S_n}\operatorname{sign}(\pi)\prod_{i=1}^n M_{i,\pi(i)} = \sum_{\pi\in S_n}\operatorname{sign}(\pi)\prod_{i=1}^n x_i^{\pi(i)-1},$$

where S_n is the symmetric group of order n, and $\operatorname{sign}(\cdot)\in\{1,-1\}$ is the sign functions of permutations. Thus,

$$h(x_1, \ldots, x_n) = \det(M)^2 = \sum_{\pi, \tau \in S_n} \operatorname{sign}(\pi) \operatorname{sign}(\tau) \prod_{i=1}^{n} x_i^{\pi(i)-1+\tau(i)-1}.$$

In order to get monomial $\prod_{i=1}^n x_i^{n-1}$, it must hold that $\pi(i) + \tau(i) = n + 1$ for all $i \in [n]$. Now, recall that $\operatorname{sign}(\pi) = (-1)^{N(\pi)}$, where $N(\pi)$ is the number of inversions of π, i.e. $|\{(i,j) : 1 \leq i < j \leq n : \pi(i) > \pi(j)\}|$ (for example, one can check Wikipedia). It is easy to see that $N(\pi) + N(\tau) = \binom{n}{2}$ if $\pi(i) + \tau(i) = n + 1$ for all $i \in [n]$, which means $\operatorname{sign}(\pi) \operatorname{sign}(\tau) = (-1)^{\binom{n}{2}}$ for this π and τ. Also, note that for every $\pi \in S_n$, there is a unique $\tau \in S_n$ satisfying $\pi(i) + \tau(i) = n + 1$ for all $i \in [n]$. Therefore, the coefficient of $\prod_{i=1}^n x_i^{n-1}$ in h (and also in f) is $n!(-1)^{\binom{n}{2}} \neq 0$ in $\mathbb{F}_p$. Here, we used that $n < p$ and p is a prime. This finishes the whole proof.

$\square$