Algebraic Methods in Combinatorics

Solutions to Assignment 2

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: Let A be a Nikodym set in $\mathbb{F}_p^n$ and suppose that $|A| < \binom{p-2+n}{n}$. Since by Lemma 1.15, the number of monomials of degree at most $p-2$ is $\binom{p-2+n}{n}$, by a lemma we saw in class there is a non-zero polynomial f of degree at most $p-2$ such that $f(a) = 0$ for all $a \in A$ (this is the same as the argument in the beginning of the proof of Theorem 1.13 in the notes).

By the property satisfied by A, we have that for each $x \in \mathbb{F}_p^n$, there is a $u \in \mathbb{F}_p^n \setminus \{\vec{0}\}$ such that $f(x+tu) = 0$ for all $t \neq 0$. Note that viewing $p(t) := f(x+tu)$ as a univariate polynomial of t, it then has degree at most $p-2$ and at least $p-1$ roots. Therefore, it must be the zero polynomial. Now, note that the constant term of the polynomial $p(t)$ is $f(x)$ and therefore, $f(x) = 0$. But then, this must be true for all x and thus, since f has degree at most $p-2$, it must be the zero polynomial, which is a contradiction.

Problem 2(a): Let us denote the set S by $S := \{p^{(1)}, p^{(2)}, \ldots, p^{(m)}\} \subset \mathbb{R}^n$. We want to show that $m \leq \binom{n+s+1}{s}$. Let also $\delta_1, \ldots, \delta_s$ denote the s possible distances between distinct points in S. For each $1 \leq j \leq m$, define the polynomial

$$f_j(\mathbf{x}) = \prod_{1 \leq i \leq s} \left(|\mathbf{x} - p^{(j)}|^2 - \delta_i^2\right).$$

Just as in Section 1.6 of the notes, it is easy to check that these polynomials are linearly independent since $f_j(p^{(i)}) = 0$ for all $i \neq j$ and $f_j(p^{(j)}) \neq 0$ for all j. Now we need only to show that these polynomials are contained in a subspace of dimension at most $\binom{n+s+1}{s}$. Indeed, note that each polynomial f_j can be written as

$$f_j(\mathbf{x}) = \prod_{1 \leq i \leq s} (|\mathbf{x} - p^{(j)}|^2 - \delta_i^2) = \prod_{1 \leq i \leq s} \left(|\mathbf{x}|^2 - 2\sum_{k=1}^{n} x_k p_k^{(j)} + |p^{(j)}|^2 - \delta_i^2\right).$$

Therefore, letting $y := |x|^2$ (a polynomial of $x_1, \ldots, x_n$), f_j can be viewed as a polynomial in $\mathbb{R}[y, x_1, \ldots, x_n]$ with degree at most s. By Lemma 1.15 in the notes, this space has at most

$\binom{n+s+1}{n+1} = \binom{n+s+1}{s}$ monomials of degree at most s, which also form then a basis for the subspace containing the polynomials f_j, as desired.

Problem 2(b): Take S to be all points in $\{0,1\}^{n+1}$ with exactly s non-zero coordinates. Clearly, the possible distances are $\sqrt{2s}, \sqrt{2(s-1)}, \ldots, \sqrt{2}$. Furthermore, the set belongs to the space of points with $x_1 + \ldots + x_{n+1} = s$ and so can be isometrically mapped to $\mathbb{R}^n$.

Problem 3(a): For each of the sets $A \in \mathcal{A}$ let v_A be its characteristic vector, and let s_1 and s_2 be the two possible sizes. For each such A, define the polynomial $f_A : R^n \to R$ as follows:

$$f_A(x) = \Big(|A| + x_1 + \ldots + x_n - 2\langle x, v_A\rangle - s_1\Big)\Big(|A| + x_1 + \ldots + x_n - 2\langle x, v_A\rangle - s_2\Big).$$

Notice that if x is the characteristic vector of a set B, then $|A| + x_1 + \ldots + x_n - 2\langle x, v_A\rangle$ is precisely equal to $|A\Delta B|$. Hence, for $B \in \mathcal{A}$ one can see that $f_A(v_B)$ is equal to $s_1 s_2 \neq 0$ when $B = A$, and is equal to 0, otherwise. Hence, as seen in the lecture notes, the defined polynomials are linearly independent.

Now define polynomials $\bar{f}_A(x)$ obtained from $f_A(x)$ by replacing each occurrence of x_i^2 by x_i, for all $i \in [n]$. By doing this, we do not change the evaluation of these polynomials in v_B, for each $B \in \mathcal{A}$, hence the new collection of polynomials is again linearly independent. The evaluation does not change since v_B is a 0/1 vector, and $x_i = x_i^2$ for $x_i \in \{0, 1\}$.

Now, it is easy to see that this collection of polynomials can be generated by the following set of monomials:

$$1, x_1, \ldots, x_n, \text{ and } x_i x_j \text{ for } 1 \leq i < j \leq n.$$

There is $1 + \frac{n(n+1)}{2}$ of those generating monomials, hence they span a space of at most this dimension, and due to the independence of the $\bar{f}_A$'s there is at most $1 + \frac{n(n+1)}{2}$ of them, so we have our desired bound on $\mathcal{A}$.

Problem 3(b): Take $\mathcal{A}$ to be the family consisting of all sets of two elements, together with the empty set. $\mathcal{A}$ has the desired number of sets, and the possible symmetric differences are in the set $2, 4$, which completes the proof.