Algebraic Methods in Combinatorics

Solutions 1

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: Note first that if q is just a prime number, then the same argument but over $\mathbb{F}_q$ as in the proof of Berlekamp's theorem for the Oddtown problem (Claim 1.4. in the notes) will work. However, this will not work if $q = p^t$ for some prime p and $t > 1$. The reason is that if we consider some $A \in \mathcal{A}$ and take its characteristic vector over $\mathbb{F}_q$, it could be that even though $|A|$ is not divisible by q, we have $\chi_A \cdot \chi_A = 0$, since this field has characteristic p, **not q**!

Nevertheless, the solution to this will be to apply the same argument over $\mathbb{Q}$. Indeed, let $v_1, \ldots, v_m$ denote the characteristic vectors of the elements of $\mathcal{A}$. Suppose, for a contradiction that $m > n$. Then, they are linearly dependent as vectors in the vector space $\mathbb{Q}^n$ (over $\mathbb{Q}$), and so, there exist $\gamma_1, \ldots, \gamma_m \in \mathbb{Q}$ (not all zero) such that

$$\gamma_1 v_1 + \ldots + \gamma_m v_m = \underline{\mathbf{0}}$$

By multiplying both sides of the above equation by some adequate integer (the least common multiple of the denominators of the γ's), we can assume that the γ's are coprime integers. Now, note that because of the above equation, for each i we have

$$0 = v_i \cdot (\gamma_1 v_1 + \ldots + \gamma_m v_m) = \sum_{j \neq i} \gamma_j (v_i \cdot v_j) + \gamma_i (v_i \cdot v_i) = \sum_{j \neq i} \gamma_j |A_i \cap A_j| + \gamma_i |A_i|.$$

Since each term $|A_i \cap A_j|$ is divisible by $q = p^t$ but $|A_i|$ is not, we must have that $p | \gamma_i$. Since this occurs for all i, this contradicts the fact that the γ's are coprime.

Problem 2:(b) We work over $\mathbb{F}_2^n$. Let V be the subspace given by the span of the characteristic vectors of elements of $\mathcal{A}$ and U be the vector space given by the span of the characteristic vectors of elements of $\mathcal{B}$. For all characteristic vectors χ_A, χ_B for elements $A \in \mathcal{A}$ and $B \in \mathcal{B}$, we have $\chi_A \cdot \chi_B = |A \cap B| = 0$. Therefore, $V \subseteq U^\perp$ and so, $\dim V + \dim U \leq n$ which then implies that $|\mathcal{A}||\mathcal{B}| \leq |V||U| = 2^{\dim V + \dim U} \leq 2^n$.

To see that 2^n is tight, do the following. For n even, let $\mathcal{A}, \mathcal{B}$ both be the family of sets which for each i, either contain all elements in $\{2i-1, 2i\}$ or none of them. For n odd, let $\mathcal{A}$ be the family of sets which do not contain n and for each $i \leq \frac{n-1}{2}$, either contain all elements in $\{2i-1, 2i\}$ or none; let $\mathcal{B}$ be the family of sets which for each $i \leq \frac{n-1}{2}$, either contain all elements in $\{2i-1, 2i\}$ or none.

Problem 2:(a) We will work in the vector space $\mathbb{F}_2^n$. The main observation here is the following. Let V be the subspace given by the span of the characteristic vectors of elements of $\mathcal{A}$. Then,

$$|\mathcal{A}| \leq 2^{\dim(V)-1}.$$

Indeed, let $v_1, \ldots, v_k$ be a basis of V consisting of characteristic vectors of elements of $\mathcal{A}$ - let $A_1, \ldots, A_k$ denote these sets. Trivially, $k = \dim(V)$ and $V = \{\sum_{i \in I} v_i : I \subseteq [k]\}$. Now, let $A \in \mathcal{A}$, v_A denote its characteristic vector and I be such that $\chi_A = \sum_{i \in I} v_i$. Then take an element $B \in \mathcal{B}$, v_B its characteristic vector, and note that by assumption, we have the following in $\mathbb{F}_2$:

$$1 = |A \cap B| = v_A \cdot v_B = \sum_{i \in I} v_i \cdot v_B = \sum_{i \in I} |A_i \cap B| = |I|.$$

Hence, I has odd size and so, $\mathcal{A} \subseteq \{\sum_{i \in I} v_i : I \subseteq [k], |I| = \text{odd}\}$ implying $|\mathcal{A}| \leq 2^{k-1} = 2^{\dim(V)-1}$.

To now solve our problem, fix $B_0 \in B$, and let U be the subspace spanned by the vectors $\{v_B - v_{B_0} : B \in \mathcal{B}\}$. Observe that for every $B \in \mathcal{B}$ and $A \in \mathcal{A}$, it holds that $(v_B - v_{B_0}) \cdot v_A = (v_B \cdot v_A) - (v_{B_0} \cdot v_A) = 1 - 1 = 0$. Hence, $U \subseteq V^\perp$. Therefore, $\dim(U) \leq n - \dim(V) = n - k$. Observe that $\{v_B : B \in \mathcal{B}\} \subseteq v_{B_0} + U$, and therefore $|\mathcal{B}| \leq |U| = 2^{n-k}$. It now follows that $|\mathcal{A}||\mathcal{B}| \leq 2^{k-1}2^{n-k} = 2^{n-1}$, as required.

Remark: To see that $\dim(V^\perp) = n - \dim V$, consider the matrix M whose rows are the vectors $v_1, \ldots, v_k$ (which form a basis for V). Observe that $\underline{\mathbf{x}} \in V^\perp$ if and only if $M\underline{\mathbf{x}} = \underline{\mathbf{0}}$. Now, the dimension of the space of solutions of this linear system is $n - k$ (see Lemma 4.16 in the Linear Algebra recap at the end of the lecture notes - remember that $v_1, \ldots, v_k$ are linearly independent so $\text{rk}(M) = k$).

Problem 3(a),(b): Follows from what we did in Problem 2(b).

Problem 3(c): We will build on the ideas shown in Problem 2(b). Let us first divide $\mathcal{A}$ into $\mathcal{A}^{\text{odd}}$, the subfamily of the odd-sized sets, and $\mathcal{A}^{\text{even}}$, the subfamily of the even-sized sets. From what we already know, we can get a bound of $|\mathcal{A}| \leq n + 2^{\lfloor n/2 \rfloor}$. Indeed, from the Oddtown problem (Claim 1.4. in the notes), we know that $|\mathcal{A}^{\text{odd}}| \leq n$ (since this family satisfies the 'oddtown' rules). Also, from Problem 3(a), we have $|\mathcal{A}^{\text{even}}| \leq 2^{\lfloor n/2 \rfloor}$. But we can do better!

Again we work in the vector space $\mathbb{F}_2^n$. Let the characteristic vectors of the elements of $\mathcal{A}^{\text{odd}}$ be $v_1, \ldots, v_k$ and V be the subspace given by their span. Note that the same proof as in the Oddtown problem (Claim 1.4. in the notes), shows that these vectors are linearly independent! Now, let U be the subspace given by the span of the characteristic vectors of the elements of $\mathcal{A}^{\text{even}}$.

Claim. $U \cap V = \emptyset$.

Proof. Suppose otherwise, so that there exists a vector $w \in U \cap V$. Let $w = \gamma_1 v_1 + \ldots \gamma_k v_k$ and suppose w.l.o.g. that $\gamma_1 \neq 0$. Recall that $\mathcal{A}$ is such that every two distinct elements have even-sized intersection, that is, the dot product of their characteristic vectors is 0. Therefore, $w \cdot v_1 = \gamma_1 \neq 0$. On the other hand, $w \in U$ and so it can also be written as a linear combination of elements of $\mathcal{A}^{\text{even}}$. Since the dot product of v_1 (which is **not** in $\mathcal{A}^{\text{even}}$) with any of these elements is 0, we have also $w \cdot v_1 = 0$, which is a contradiction. □

To finish the proof, just note that again the characteristics of $\mathcal{A}$ imply that $U \cup V \subseteq U^\perp$ and so, $U + V \subseteq U^\perp$, giving dim $(U+V) \leq n - \text{dim } U$. Moreover, the claim above implies that dim $(U+V) = \text{dim } U + \text{dim } V = \text{dim } U + k$. So, $k + 2\text{dim } U \leq n$, and since, $k = |\mathcal{A}^{\text{odd}}|$ and $|\mathcal{A}^{\text{even}}| \leq 2^{\text{dim } U}$, we have the bound

$$|\mathcal{A}| \leq k + 2^{\frac{n-k}{2}}.$$

This is always at most $2^{\lfloor n/2 \rfloor} + 1$.

Slightly different proof: By the properties of $\mathcal{A}$, we have that $U \subseteq V^\perp$, which has dimension $n - \text{dim } V$. We can then consider working on the vector space $V^\perp$, take in it the bilinear form coming from the usual dot product in $\mathbb{F}_2^n$. We then, again by orthogonal complement considerations, still have $U \subseteq U^\perp$ and so, $2\text{dim } U \leq \text{dim } V^\perp \leq n - \text{dim } V$. Now, the rest goes as above.

Problem 4: Let $\mathcal{A} := \{A_1, \ldots, A_m\}$ and suppose, for sake of contradiction, that $m < n$. The key idea here is to apply Claim 1.8. from the notes. For this, define the dual sets $B_i := \{j : i \in A_j\} \subseteq [m]$ for each $i \in [n]$. Since $n > m$, we can apply Claim 1.8. to these sets to find disjoint and non-empty sets $I, J \subseteq [n]$ such that

$$\bigcup_{i \in I} B_i = \bigcup_{j \in J} B_j$$

What this means for our family $\mathcal{A}$ is that every set in it either is disjoint to $I \cup J$ or intersects both of them! It then already makes sense to want to colour the elements of $[n]$ so that I is red and J is blue - since then every set intersecting $I \cup J$ would have both a red element (from I) and a blue element (from J). Indeed, if $[n] = I \cup J$, then this would be a two-colouring such that no set in $\mathcal{A}$ is monochromatic - this would be a contradiction to the fact that $\mathcal{A}$ is not 2-colourable.

In general, let $K := [n] \setminus (I \cup J)$. Recall that we know that all sets in $\mathcal{A}$ either intersect both I and J or are contained in K. In fact, let us denote by $\mathcal{A}_K$ the subfamily of those contained in K. Now, take an element $i \in I$ (exists since this is non-empty) and by assumption, we know there exists $A \in \mathcal{A}$ such that $i \in A$ and moreover, $\mathcal{A} \setminus A$ is 2-colourable. In particular, since $A \notin \mathcal{A}_K$, we have that $\mathcal{A}_K \subseteq \mathcal{A} \setminus A$ is 2-colourable, meaning that there exists a red/blue-colouring of K such that no set in $\mathcal{A}$ which is contained in K is monochromatic. We now extend this to a colouring of $[n]$ by colouring I red and J blue, giving a colouring such that no set in $\mathcal{A}$ is monochromatic - this is a contradiction to the fact that $\mathcal{A}$ is not 2-colourable.