KAIST
2021 MAS575 Combinatorics
Homework 4

Fanchen Bu
University: KAIST
Department: Electrical Engineering
Student ID: 20194185

May 11, 2021

Contents

HW 4.1

Let A and B be two nonempty subsets of $\mathbb{Z}_p$. Let

$$X = \{a + b : a \in A, b \in B, ab \neq 1\}.$$

Show that $|X| \geq \min\{|A| + |B| - 3, p\}$.

Proof. We may assume that $|A|+|B|-3 \leq p$, otherwise, i.e, $|A|+|B| \geq p+4$, then for any fixed $g \in \mathbb{Z}_p$, we have 4 distinct pairs (a_i, b_i) such that $a_i = g - b_i$, for $i \in [4]$. Then if we want $|X| < p$, there must exist some $g_0 \in \mathbb{Z}_p$ such that $a_i b_i = 1, a_i + b_i = g_0$, for all $i \in [4]$. Then we have $a_1 g_0 - a_1^2 = a_2 g_0 - a_2^2$, which gives $(a_1 - a_2)(g - a_1 - a_2) = 0$, and thus $a_2 = g - a_1 = b_1$. Similarly, we have $a_3 = b_1$, and thus $a_2 = a_3$, which is a contradiction with the fact that pairs (a_i, b_i) are all distinct. We may also assume that both $|A|$ and $|B|$ are at least 2 and $|A| + |B| \geq 5$, otherwise it is trivial.

Now suppose that $|X| \leq |A| + |B| - 4$. Let $f(x, y) \coloneqq (xy - 1) \prod_{c \in C}(x + y - c)$, where $X \subset C \subset \mathbb{Z}_p$ with $|C| = |A| + |B| - 4$. We have $\deg(f) = |C| + 2 = |A| + |B| - 2$ and the coefficient of $x^{|A|-1}y^{|B|-1}$ in f is $\binom{|C|}{|A|-2} \neq 0$, as $1 \leq |C| \leq p - 1$. By Combinatorial Nullstellensatz, there exist $a \in A$ and $b \in B$ such that $f(a, b) \neq 0$, i.e., $a + b \notin C$ and $ab \neq 1$, but then $a + b \in X$, contradicting with $X \subset C$, and thus completing the proof. $\square$

HW 4.2

A graph is k-regular if every vertex has degree k. Let p be a prime. Let G be a graph with no loops. Prove that if the average degree of G is greater than $2p-2$ and the maximum degree is at most $2p-1$, then G contains a p-regular subgraph.

Proof. Let $G = (V, E)$. For $x \in \mathbb{F}_p^E$, let

$$f(x) \coloneqq \prod_{v \in V} (1 - (\sum_{e \sim v} x_e)^{p-1}) - \prod_{e \in E} (1 - x_e),$$

where $e \sim v$ means the vertex v and edge e are incident and $x_e = x(e)$. By Fermat's little theorem, for $z \in \mathbb{F}_p$, $z^{p-1} \equiv 1 \pmod p$ iff $z \not\equiv 0 \pmod p$. Thus $\prod_{v \in V}(1 - (\sum_{e \sim v} x_e)^{p-1}) = 1$ if $\sum_{e \sim v} x_e \equiv 0 \pmod p, \forall v \in V$ and 0 otherwise. Clearly, $f(0) = 1 - 1 = 0$. Now we set $L_e = \{0, 1\} \subset \mathbb{F}_p$ for all $e \in E$, then for $x \in \mathbb{F}_p^E$ such that $x \not\equiv 0$ and $x_e \in L_e$ for all $e \in E$, $f(x) \neq 0$ iff $\sum_{e \sim v} x_e \equiv 0 \pmod p, \forall v \in V$, as $\prod_{e \in E}(1 - x_e) = 0$. Because the maximum degree is at most $2p - 1$, it means $\sum_{e \sim v} x_e \in \{0, p\}, \forall v \in V$. Then we take H be the subgraph of G consisting of $e \in E$ such that $x_e = 1$, then H is nonempty and p-regular. Now it remains to show that there exists $x_e \in L_e, \forall e \in E$ such that $f(x) \neq 0$. The coefficient of $\prod_{e \in E} x_e$ in f is $-(-1)^m \not\equiv 0 \pmod p$. On the other hand, the average degree of G is $2m/n > 2p - 2$, which gives that $m > (p-1)n$, thus $\deg(f) = m$, as in f the first term has degree $(p-1)n$ and the second one has degree m. Then by Combinatorial Nullstellensatz, there exists $x \in \mathbb{F}_p^E$ with $x_e \in L_e$ for all $e \in E$ such that $f(x) \not\equiv 0 \pmod p$, completing the proof. $\square$

HW 4.3

Suppose that there exist m affine hyperplanes covering each point in $\{0,1\}^n - \{0\}$ at least twice but not covering 0. What is the minimum m in terms of n?

Remark 3.1. *Similar with the case when the affine hyperplanes cover the points at least once, we may first consider* $(\{x \in \mathbb{R}^n : x_i = 1\})_{i\in[n]}$, *these* n *affine hyperplanes cover each point in* $\{0,1\}^n - \{0\}$ *with at least two coordinates being* 1. *It remains to cover those with exactly a single coordinate being* 1, *adding* $\{x \in \mathbb{R}^n : \sum_{i\in[n]} x_i = 1\}$ *suffices. This intuitive construction gives us a case when* $m = n + 1$.

Claim 3.1. *The minimum* m *is* $m(n) = n + 1$.

Proof. First, we state the lemma proved and used in the lecture.

Lemma 3.1. *Let* p *be a polynomial in* $\mathbb{R}[x_1, ..., x_n]$ *with* $p(0) \neq 0$ *and* $p(x_1, ..., x_n) = 0, \forall (x_1, ..., x_n) \in \{0,1\}^n - \{0\}$, *then* $\deg(p) \geq n$.

Proof. Suppose not, i.e., $\deg(p) < n$. In particular, p does not contain the term $\prod_{i\in[n]} x_i$. Define $f(x_1, ..., x_n) := p(x_1, ..., x_n) - c\prod_{i\in[n]}(x_i - 1)$, where we choose $c \neq 0$ such that $f(0) = 0$. Observe that $\deg(f) = n$ and the coefficient of $\prod_{i\in[n]} x_i$ in f is $-c \neq 0$. Then by Combinatorial Nullstellensatz, there exists $x \in \{0,1\}^n$ such that $f(x) \neq 0$, but it is easy to check that $f(0) = 0$ and $f(x) = 0 - 0 = 0, \forall x \in \{0,1\}^n - \{0\}$. By contradiction we complete the proof. □

The idea in the remark provides us an example with $m = n+1$, thus the minimum $m(n) \leq n+1$. Let $(H_i)_{i\in[m]}$ be the affine hyperplanes covering each point in $\{0,1\}^n - \{0\}$ at least twice but not covering 0, where $H_i = \{x \in \mathbb{R}^n : a_i x = b_i\}$. Define

$$p(x_1, ..., x_n) := \prod_{i\in[m-1]} (a_i x - b_i),$$

observe that $\deg(p) = m - 1$ and if $x \in H_i$ and $x \in H_j$ for some $i \neq j \in [m]$, then $p(x) = 0$ as at least one of i and j is in $[m-1]$. Thus, $p(x) = 0, \forall x \in \{0,1\}^n - \{0\}$. Besides, $p(0) = 0$ as none of these affine hyperplanes covers 0. By Lemma 3.1, we have $m - 1 \geq n$, thus $m(n) \geq n + 1$. Therefore, $m(n) = n + 1$, completing the proof. □

HW 4.4

Let p be a prime and $\mathbb{F}_p = \mathrm{GF}(p)$ be the filed of size p. Let $f_1, ..., f_m$ be polynomials in $\mathbb{F}_p[x_1, ..., x_n]$ with no constant terms. Let $Q_1, ..., Q_m$ be subsets of $\mathbb{F}_p$ such that $0 \in Q_i$ for all i. If $\sum_{i=1}^m \deg(f_i)|\mathbb{F}_p \setminus Q_i| < n$, then there exists a vector $x \in \{0,1\}^n$ such that $f_i(x) \in Q_i$ for all i and $x \neq 0$.

Proof. Define $g \in \mathbb{F}_p[x_1, ..., x_n]$ as

$$g(x_1, ..., x_n) \coloneqq \prod_{i\in[m]} \prod_{q\in\mathbb{F}_p\setminus Q_i} (q - f_i(x)) - c \prod_{k\in[n]} (x_k - 1),$$

where we choose $c \neq 0$ such that $p(0) = 0$. This is possible as each f_i contains no constant terms and each Q_i contains 0, thus $f_i(0) = 0, \forall i \in [m]$ and we have

$$\prod_{i\in[m]} \prod_{q\in\mathbb{F}_p\setminus Q_i} (q - f_i(0)) = \prod_{i\in[m]} \prod_{q\in\mathbb{F}_p\setminus Q_i} q \not\equiv 0 \pmod p.$$

Observe that $\deg(f) = n$ as $\deg(\prod_{i\in[m]} \prod_{q\in\mathbb{F}_p\setminus Q_i}(q - f_i(x))) = \sum_{i=1}^m \deg(f_i)|\mathbb{F}_p \setminus Q_i| < n$, and the coefficient of $\prod_{k\in[n]} x_k$ in f is $-c \neq 0$ as $\prod_{i\in[m]} \prod_{q\in\mathbb{F}_p\setminus Q_i}(q - f_i(x))$ does not contain $\prod_{k\in[n]} x_k$ that exceeds its degree. Then by Combinatorial Nullstellensatz, there exists $x \in \{0,1\}^n$ such that $f(x) \neq 0$. But $f(0) = 0$ and for $0 \neq x \in \{0,1\}^n$, $g(x) = \prod_{i\in[m]} \prod_{q\in\mathbb{F}_p\setminus Q_i}(q - f_i(x)) \neq 0$ iff $f_i(x) \in Q_i, \forall i \in [m]$, completing the proof. $\square$

HW 4.5

In a party, n couples are invited. They decided to sit around a table with $2n+1$ chairs such that the i-th couple are seated from each other by distance d_i (separated by $d_i - 1$ chairs). Prove that if $2n+1$ is a prime and $d_i \leq n$ for all $i \in [n]$, then this is possible.

Proof. First, we state the theorem proved and used in the lecture.

Theorem 5.1 (Dyson's Conjecture). *The constant term in the expansion of $\prod_{1\leq i\neq j\leq n}(1-\frac{x_i}{x_j})^{a_i}$ is $A!/\prod_{i\in[n]} a_i!$, where $A = \sum_{i\in[n]} a_i$. Equivalently, the coefficient of $\prod_{i\in[n]} x_i^{A-a_i}$ in $\prod_{1\leq i<j\leq n}(-1)^{a_j}(x_j - x_i)^{a_i+a_j}$ is $A!/\prod_{i\in[n]} a_i!$.*

Now, we assume that $p = 2n+1$ is an odd prime and label the $p = 2n+1$ chairs with $[p]$ clockwise starting from any fixed chair. And we define $f \in \mathbb{F}_p[x_1, ..., x_n]$ as

$$f(x_1, ..., x_n) \coloneqq \prod_{k\in[n]}(x_k + d_k) \prod_{1\leq i<j\leq n}(x_i - x_j)(x_i + d_i - x_j)(x_i - x_j - d_j)(x_i + d_i - x_j - d_j).$$

Observe that $\deg(f) = n + 4\binom{n}{2} = (p-2)n$. The coefficient of $\prod_{i\in[n]} x_i^{p-2}$ in f is equal to the coefficient of $\prod_{i\in[n]} x_i^{p-2}$ in $\prod_{k\in[m]} x_k \prod_{i<j}(x_i - x_j)^4$. And that is equal to the coefficient of $\prod_{i\in[n]} x_i^{p-3} = \prod_{i\in[n]} x_i^{2n-2}$ in $\prod_{i<j}(x_i - x_j)^4$, which is, by the statement in the second type of Theorem 5.1 with $a_i = 2$ for all i, $(2n)!/2^n \not\equiv 0 \pmod p$ as $2n < p$. Then by Combinatorial Nullstellensatz, there exists $x_i \in [p-1]$ for all i such that $f(x_1, ..., x_n) \not\equiv 0 \pmod p$. By take $y_k \equiv x_k + d_k \pmod p$ such that $y_k \in [p]$ for each $k \in [n]$, we have $y_k \equiv x_k + d_k \not\equiv 0 \pmod p$ for each $k \in [n]$; $x_i \neq x_j$ for all $i \neq j$, which means x_i's are all distinct; $x_j \not\equiv x_i + d_i \equiv y_i \pmod p$ for all $i \neq j$; and $y_i \equiv x_i + d_i \not\equiv x_j + d_j \equiv y_j \pmod p$ for all $i \neq j$, which means y_i's are all distinct. Thus, for the k-th couple, $k \in [n]$, it is possible to let one of them be seated at chair x_k and the other y_k with all desired conditions satisfied, completing the proof. $\square$