# HW 9 - Polynomial Method in Combinatorics (Due Tue 04/23)

**1**. [Testing for Database consistency] Two friends **Dallin** and **Evan** separately maintain copies of a large database of information. Every week they must compare their databases for consistency. Since transmission is expensive, they would like to find if there is any inconsistency between their databases by sending very little amount of information. Let their full databases be represented as the following $\{0,1\}$-vectors:

$$\text{Dallin} : (a_0, a_1, \cdots, a_{n-1}) \quad ; \quad \text{Evan} : (b_0, b_1, \cdots, b_{n-1})$$

Design a randomized strategy that detects an inconsistency with high probability $\left(\text{say} \geq 1 - \frac{1}{n}\right)$ while transmitting only $O(\log n)$ bits.

*Proof.* Let $A$ be a degree-$n$ polynomial such that the coefficient on the degree-$n$ term of $A$ is $a_n$. Similarly, let $B$ be a degree-$n$ polynomial such that the coefficient on the degree-$n$ term of $B$ is $b_n$. For random testing, we let $S$ be a set of $m$ random elements from $\mathbb{R}$ such that $m \geq n^2$. We proceed by the folowing algorithm:

1. Dallin and Evan agree upon an $r \in S$ and transmit this value to each other.
2. Dallin evaluates $A(r) \mod (\log n)$ and transmits this value to Evan. Taking the output $\mod (\log n)$ ensures that the output is no more than $\log n$ bits while still being able to detect inconsistencies.
3. Evan similarly evaluates $B(r) \mod (\log n)$ and transmits this value to Dallin.
4. Evan and Dallin define a polynomial $P(x) = A(x) - B(x)$ and evaluate at $x = r$.

If $P(r) \neq 0$, then the databases are inconsistent. Otherwise, by the Schwartz-Zippel lemma, the databases are consistent with a probability $\leq \frac{n}{|S|}$ and are thus inconsistent with a probability $\geq 1 - \frac{n}{m}$. □

**2**. [Multivariate Factor Theorem + (Finite Field) Kakeya's Needle Conjecture; **Extra-Credit**]

$(i)$ Let $n \in \mathbb{N}$, $\mathbb{F}$ be a field and $S \subseteq \mathbb{F}$ such that $|S| < \binom{n+d}{d}$, then

$$\boxed{\exists \text{ (non-zero) } f \in \mathbb{F}[x_1, \cdots, x_n] \text{ of } deg(f) \leq d \ : \ f(S) = 0}$$

(*Hint*: First find the dimension of the vector space of all polynomials of degree at most $d$ in $n$ variables. *Remark*: This gives us a non-constructive proof for the existence of such an $f$.)

$(ii)$ Let $f \in \mathbb{F}_q[x_1, \cdots, x_n]$ be a non-zero polynomial of $deg(f) = d$, then show that

$$\boxed{\# \text{ roots of } f \leq dq^{n-1}}$$

(*Hint*: Use induction on $n$. Imitate the proof of Schwartz-Zippel Lemma.)

$(iii)$ In 1917, **Soichi Kakeya** asked the question: What is the smallest set in the plane (room) in which someone (Samurai) can rotate a unit needle (sword) around completely ?

Define a *Kakeya Set* $S$ as follows:

$$\text{Given any direction } \overrightarrow{v} \in \mathbb{F}^n, \ \exists \overrightarrow{u} \in \mathbb{F}^n \ : \ \overrightarrow{u} + t\overrightarrow{v} \in S, \ \forall t \in \mathbb{F}$$

The **Kakeya Needle Conjecture** then states that:

$$\boxed{\text{Any Kakeya set } S \subset \mathbb{R}^n \text{ has Hausdorff (fractal) dimension } n}$$

The conjecture is open for $n \geq 3$, but the following Finite Field analog of it has been proved:

$$\boxed{\text{Any Kakeya set } S \subset \mathbb{F}_q^n \text{ has } |S| > c\,|\mathbb{F}_q|^n \ \ (c \text{ depends only on the dimension } n)}$$

$(a)$ Let $f \in \mathbb{F}_q[x_1, \cdots, x_n]$, $deg(f) \leq q-1$. If $S \subset \mathbb{F}_q^n$ is Kakeya and $f(S) = 0$, then show that $f \equiv O$

$(b)$ Let $S \subset \mathbb{F}^n$ be a Kakeya set, then

$$|S| \geq \binom{q+n-1}{n} > \frac{q^n}{n!} = \frac{1}{n!}\,|\mathbb{F}_q|^n$$

(*Hint*: For $(a)$ use $(ii)$ and for $(b)$ use $(i)$. This result is by **Zeev Dvir** (2009))

**3**. [Low local-degree polynomials and Combinatorial Nullstellensatz; **Extra-Credit**]

Schwartz-Zippel Lemma says: For any (non-zero) $f \in \mathbb{F}[x_1, \cdots, x_n]$ of degree $d$ and a set $S \subset \mathbb{F}$ with $|S| > d$,

$$\boxed{\#\text{ roots of } f \text{ in } S^n \leq d|S|^{n-1}} \Leftrightarrow \boxed{P\big(\exists \text{ root of } f \text{ in } S^n\big) \leq \frac{d}{|S|}} \Leftrightarrow \boxed{P\big(\exists \text{ a non-root of } f \text{ in } S^n\big) \geq 1 - \frac{d}{|S|}}$$

Equivalently, one can say

$$\boxed{|S| > d \ \Rightarrow \ f \text{ has a non-root in } S^n}$$

In many applications (like in that of "Testing for perfect matching" problem) the *total degree* $d$ of the polynomial can be much larger than the *local-degree* of $f$ (The *local degree*, say $\delta$, of $f$ is the maximum exponent over each of its variables. So $d$ can be as large as $n\delta$). Schwartz-Zippel would be a trivial statement whenever $|S| \leq n$, that is, we have to sample over large $S$ for Schwarz-Zippel to make it work. Can we make it work for small $\delta$ ?

($i$) Consider a non-zero $f \in \mathbb{F}[x_1, \cdots, x_n]$. Let $\delta$ be the local degree of $f$, show (using induction on $n$) that

$$\boxed{|S| > \delta \ \Rightarrow \ f \text{ has a non-root in } S^n}$$

($ii$) [not-for-credit] One can in fact show a 'granulated' version of ($i$). Let $\delta_i$ be the degree of $f$ in $x_i$, then

$$\boxed{|S_i| > \delta_i, \forall i \ \Rightarrow \ f \text{ has a non-root in } S_1 \times S_2 \times \cdots \times S_n}$$

We could do a bit better than this too, as follows:

($iii$) [**Noga Alon's Combinatorial Nullstellensatz**, not-for-credit]

Let $f \in \mathbb{F}[x_1, \cdots, x_n]$ be of degree $d$. Let $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ be a monomial of degree $d$ in $f$ (that is, $\sum t_i = d$) with non-zero coefficient, then

$$\boxed{|S_i| > t_i, \forall i \ \Rightarrow f \text{ has a non-root in } S_1 \times S_2 \times \cdots \times S_n}$$

($iv$) [Covering $Q_n \setminus \{\overrightarrow{0}\}$ by Hyperplanes (revisited) - **Alon + Füredi** (1993)]

Suppose the hyperplanes $H_1, \cdots, H_m$ in $\mathbb{R}^n$ cover $Q_n \setminus \{\overrightarrow{0}\}$. Show that

$$m \geq n$$

(*Hint*: Assume $m < n$. Consider the polynomial as shown in class and then use ($iii$) to get a contradiction.)