Math 286X: Arithmetic Statistics

Spring 2020

Problem set #3

Problem 1. Let $A \subset \mathbb{R}^n$ be a bounded set whose boundary is Lipschitz. Let $k \geqslant 1$ and $y \in (\mathbb{Z}/k\mathbb{Z})^n$. Show that

$$\lim_{T\to\infty} \mathbb{P}(x \equiv y \mod k \mid x \in (T \cdot A) \cap \mathbb{Z}^n) = \frac{1}{k^n}.$$

Solution. Apply Widmer's theorem to the sets $T \cdot A$ and $\frac{1}{k} \cdot (T \cdot A - y)$. Use that $\operatorname{vol}(T \cdot A)/\operatorname{vol}(\frac{1}{k} \cdot (T \cdot A - y)) = k^{-n}$. If ∂A is (M, L)-Lipschitz, then $\partial(T \cdot A)$ is (M, TL)-Lipschitz and $\partial(\frac{1}{k} \cdot (T \cdot A - y))$ is $(M, \frac{T}{k} \cdot L)$-Lipschitz. $\square$

Problem 2. Find a compact subset $A \subset \mathbb{R}$ with positive volume, but so that

$$\liminf_{T\to\infty} \#((T \cdot A) \cap \mathbb{Z}) = 0.$$

Solution. Choose an enumeration $a_1, a_2, \ldots$ of the rational numbers in the interval $[0, 1]$. Let $A = [0, 1] \backslash \bigcup_{n \geqslant 1} B_{2^{-n-2}}(a_n)$, where $B_r(x)$ is the open ball of radius r centered at x. By the monotone convergence theorem, A is measurable and has volume at least $1 - \sum_{n=1}^{\infty} 2^{-n-1} = \frac{1}{2} > 0$. On the other hand, for any $T \in \mathbb{Z}$, we have $(T \cdot A) \cap \mathbb{Z} = \varnothing$ because we have removed all rational numbers from A. $\square$

Problem 3. Identify the space V_n of monic polynomials of degree n with $\mathbb{R}^n$ by sending $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ to $(a_{n-1}, \ldots, a_0)$. Consider the map $\varphi_n : \mathbb{R}^n \to V_n \cong \mathbb{R}^n$ sending $x = (x_1, \ldots, x_n)$ to $f(X) = \prod_i (X - x_i)$.

a) Show that the Jacobian determinant at $x \in \mathbb{R}^n$ is $(-1)^n \prod_{i<j}(x_i - x_j)$.

   Solution. We have $\partial_i \varphi_n(x) = -\prod_{j \neq i}(X - x_j)$. Now, subtract the first partial derivative ∂_1 from all other partial derivatives ∂_i with $i > 1$. We get $\partial_i \varphi_n(x) - \partial_1 \varphi_n(x) = (x_1 - x_i) \prod_{j \neq i,n}(X - x_j)$, which is a polynomial of degree $n - 2$. The X^{n-1}-coefficient in $\partial_1 \varphi_n(x)$ is -1. Hence, the Jacobian determinant of φ_n at x is $(-1)^n \prod_{1<i}(x_1 - x_i)$ times the Jacobian determinant of φ_{n-1} at $(x_2, \ldots, x_n)$. The claim follows by induction. $\square$

b) Show that the volume of the image $\varphi_3([-1,1]^3) \subset V_3 \cong \mathbb{R}^3$ is 16/45. (Use a computer if you like.)

Solution. Each (a_2, a_1, a_0) in the image has exactly one preimage $(x_1, x_2, x_3) \in [-1,1]^3$ with $x_1 \geqslant x_2 \geqslant x_3$. The Jacobian determinant at such a point has absolute value $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. Therefore,

$$\begin{aligned}
&\operatorname{vol}(\varphi_3([-1,1]^3)) \\
&= \int_{-1}^{1} \int_{-1}^{x_1} \int_{-1}^{x_2} (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \mathrm{d}x_3 \mathrm{d}x_2 \mathrm{d}x_1 \\
&= \frac{16}{45}.
\end{aligned}$$

□

Problem 4. Fix some $n \geqslant 2$. Order the algebraic integers $\alpha \in \overline{\mathbb{Z}}$ of degree n and trace 0 by length $|\alpha|$. Let $\operatorname{disc}(\alpha)$ be the discriminant of the ring $\mathbb{Z}[\alpha]$. We always have $|\operatorname{disc}(\alpha)| \ll_n |\alpha|^{n(n-1)}$. Show that

$$\lim_{\varepsilon \to 0} \mathbb{P}(|\operatorname{disc}(\alpha)| \geqslant \varepsilon |\alpha|^{n(n-1)} \mid \alpha \text{ as above}) = 1.$$

Solution. We separately consider each possible signature (r_1, r_2). Let $A = \{x \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^0 \mid |x| \leqslant 1\}$, let $I = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid x_i = x_j \text{ for some } i \neq j\}$ and let $B_\varepsilon = \{x \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^0 \mid \det(M(x))^2 \geqslant \varepsilon |x|^{n(n-1)}\}$, where $M(x)$ is the $n \times n$-matrix whose columns are the vectors $1, x, \ldots, x^{n-1} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$. Note that $\det(M(\lambda x))^2 = \lambda^{n(n-1)} \det(M(x))^2$, so $\lambda B_\varepsilon = B_\varepsilon$ for any $\lambda \in \mathbb{R}^\times$. Furthermore, $\det(M(x)) = 0$ if and only if $x \in I$. Consider the map

$$\varphi : (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^0 \to \left\{ \begin{array}{c} \text{monic } f(X) \in \mathbb{R}[X] \text{ of degree } n \\ \text{with } X^{n-1}\text{-coefficient } 0 \end{array} \right\} \cong \mathbb{R}^{n-1}$$

sending x to $\prod_i (X - x_i)$. Then,

$$\begin{aligned}
&\#\{\alpha \in \overline{\mathbb{Z}} \text{ of signature } (r_1, r_2) \text{ and trace 0 and length } |\alpha| \leqslant S\} \\
&= n \cdot \#\{\text{irreducible } f(X) \in \varphi(S \cdot A) \cap \mathbb{Z}[X]\} \\
&= n \cdot \#\{\varphi(S \cdot A) \cap \mathbb{Z}[X]\} + o(S^{(n-1)(n+2)/2})
\end{aligned}$$

and

$$\begin{aligned}
&\# \left\{ \begin{array}{c} \alpha \in \overline{\mathbb{Z}} \text{ of signature } (r_1, r_2) \text{ and trace 0} \\ \text{and length } |\alpha| \leqslant S \text{ and } |\operatorname{disc}(\alpha)| \leqslant \varepsilon |\alpha|^{n(n-1)} \end{array} \right\} \\
&= n \cdot \#\{\text{irreducible } f(X) \in \varphi(S \cdot (A \cap B_\varepsilon)) \cap \mathbb{Z}[X]\} \\
&= n \cdot \#\{\varphi(S \cdot (A \cap B_\varepsilon)) \cap \mathbb{Z}[X]\} + o(S^{(n-1)(n+2)/2}).
\end{aligned}$$

The boundaries of A and $A \cap B_\varepsilon$ are Lipschitz (the boundary of B_ε is contained in the set of x such that $\det(M(x))^2 = \varepsilon |x|^{n(n-1)}$, which is contained in the union of $r_1 + r_2$ zero sets of nonzero polynomials). The set $A \cap I$ is also Lipschitz. As we've seen in class, this implies that the boundaries of $\varphi(A)$ and $\varphi(A \cap B_\varepsilon)$ are Lipschitz. By a corollary to Widmer's theorem, it follows that

$$\mathbb{P}(|\operatorname{disc}(\alpha)| \geqslant \varepsilon |\alpha|^{n(n-1)} \mid \alpha \text{ as above}) = \frac{\operatorname{vol}(A \cap B_\varepsilon)}{\operatorname{vol}(A)}.$$

We have $B_\varepsilon \subseteq B_{\varepsilon'}$ for $\varepsilon > \varepsilon'$ and $\bigcup_{\varepsilon>0}(A \cap B_\varepsilon) = A \backslash I$. Hence, $\lim_{\varepsilon \to 0} \operatorname{vol}(A \cap B_\varepsilon) = \operatorname{vol}(A \backslash I) = \operatorname{vol}(I)$. □

Problem 5. Fix some $n \geqslant 2$. Order the algebraic integers $\alpha \in \overline{\mathbb{Z}}$ of degree n and trace 0 by length $|\alpha|$. Let $\lambda_1(\alpha) \leqslant \cdots \leqslant \lambda_n(\alpha)$ be the successive minima of the lattice $\mathbb{Z}[\alpha] \subset \mathbb{R}^n$ (with respect to the Euclidean norm on $\mathbb{R}^n$, say). We know that $\lambda_1(\alpha) \asymp_n 1$. Since $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent, it is also clear that $\lambda_i(\alpha) \ll_n |\alpha|^i$ for $i = 1, \ldots, n-1$. Show that

$$\lim_{\varepsilon \to 0} \mathbb{P}_{\inf}(\lambda_i(\alpha) \geqslant \varepsilon |\alpha|^i \text{ for } i = 1, \ldots, n-1 \mid \alpha \text{ as above}) = 1.$$

(In particular, assuming ε is small enough, for a positive proportion of α, we have $\lambda_i(\alpha) \geqslant \varepsilon |\alpha|^i$ for $i = 1, \ldots, n-1$. — "The lattice $\mathbb{Z}[\alpha]$ is almost never balanced.")

Solution. If $\operatorname{disc}(\alpha) \geqslant \varepsilon |\alpha|^{n(n-1)}$, then $\operatorname{disc}(\alpha)^{1/2} \asymp_n \lambda_1(\alpha) \cdots \lambda_n(\alpha)$ and $\lambda_i(\alpha) \ll_n |\alpha|^i$ together imply that $\lambda_i(\alpha) \gg_n \varepsilon |\alpha|^i$, so the result follows from the previous exercise. □

Problem 6 (completely unnecessary for us)**.** a) Show that if a monic polynomial $f(X) = X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{R}[X]$ has a root $x \in \mathbb{C}$ with $|x| = 1$, then

$$1 + a_2 + a_1 + a_0 = 0$$

or

$$-1 + a_2 - a_1 + a_0 = 0$$

or

$$a_2a_0 - a_0^2 - a_1 + 1 = 0.$$

Solution. The first two equations are equivalent to $f(1) = 0$ and $f(-1) = 0$, respectively. Otherwise, $f(X)$ must have two complex conjugate roots $x, \overline{x}$ on the unit circle. This implies that $f(X)$ must be divisible by $(X-x)(X-\overline{x}) = X^2-(x+\overline{x})X+x\overline{x} = X^2-2\Re(x)X+1$, so by a polynomial of the form X^2+tX+1. Let

$$f(X) = (X^2+tX+1)(X+b_0).$$

Hence, $f(X) = X^3+(b_0+t)X^2+(tb_0+1)X+b_0$, so indeed

$$a_2a_0 - a_0^2 - a_1 + 1 = (b_0+t)b_0 - b_0^2 - (tb_0+1) + 1 = 0. \qquad \square$$

b) (if you know algebraic geometry or resultants) Show that for any $n \geqslant 1$, there is a nonzero polynomial $C(A_{n-1}, \dots, A_0) \in \mathbb{Z}[A_{n-1}, \dots, A_0]$ such that for any monic polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$, which has a root $x \in \mathbb{C}$ with $|x| = 1$, we have $C(a_{n-1}, \dots, a_0) = 0$. (And how would you compute such a polynomial C?)

Solution. As in part a), we have $f(1) = 0$, or $f(-1) = 0$, or $f(X)$ is divisible by a polynomial of the form X^2+tX+1. It suffices to construct a nonzero polynomial $D(A_{n-1}, \dots, A_0)$ such that $D(a_{n-1}, \dots, a_0) = 0$ whenever $f(X)$ is divisible by a polynomial of the form X^2+tX+1. (Take $C = D \cdot (1+A_{n-1}+\cdots+A_0)((-1)^n + A_{n-1}(-1)^{n-1}+\cdots+A_0)$.) Consider the morphism $\mathbb{A}^1 \times \mathbb{A}^{n-2} \to \mathbb{A}^n$ sending $(t, (b_{n-3}, \dots, b_0))$ to $(a_{n-1}, \dots, a_0)$, where $(X^2+tX+1)(X^{n-2}+b_{n-3}X^{n-3}+\cdots+b_0) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Its image is constructible and has (at most) dimension $1+n-2 \leqslant n-1$, so it must be contained in a proper subvariety of $\mathbb{A}^n$. Therefore, there is a nonzero polynomial $D(A_{n-1}, \dots, A_0)$ which vanishes on the entire image. $\square$

Problem 7. An isomorphism of graphs $G = (V, E)$ and $G' = (V', E')$ is a bijection $f : V \to V'$ between the sets of vertices such that $(x, y) \in E$ if and only if $(f(x), f(y)) \in E'$. Consider the set of undirected graphs G with n vertices (without loops, i.e., without edges of the form (x, x)), up to isomorphism. Show that

$$\sum_G \frac{1}{\#\operatorname{Aut}(G)} = \frac{2^{n(n-1)/2}}{n!}.$$

Solution. Let $V = \{1, \dots, n\}$ and let $F = \binom{V}{2}$ be the set of two-element subsets of V (the set of potential edges). Let $X = 2^F$ be the set of subsets E of F (the set of possible edge sets). Let the symmetric group S_n act in the natural way on F, and therefore on X. Graphs up to isomorphism correspond to S_n-orbits in X. The stabilizer of $E \in X$ is the automorphism group of $G = (V, E)$. Hence, the orbit–stabilizer theorem implies that

$$\sum_G \frac{1}{\#\operatorname{Aut}(G)} = \frac{\#X}{\#S_n} = \frac{2^{n(n-1)/2}}{n!}.$$

$\square$