Mathematical Toolkit **Autumn 2018**

Homework 3

Due: November 30, 2018

Note: *You may discuss these problems in groups. However, you must write up your own solutions and mention the names of the people in your group. Also, please do mention any books, papers or other sources you refer to. It is recommended that you typeset your solutions in LaTeX.*

1. **Random Polynomials.** **[2+2+2+4]**

   For a prime number p, recall that the field $\mathbb{F}_p$ has the elements $\{0, 1, \ldots, p-1\}$, with addition and multiplication done modulo p. A degree-d polynomial in the variable x over the field $\mathbb{F}_p$ (for pime p) is defined as:

   $$P(x) \;=\; c_0 + c_1 \cdot x + \ldots + c_d \cdot x^d \,,$$

   where the coefficients $c_0, \ldots, c_d$, and the variable x all take values in $\mathbb{F}_p$ (and all addition and multiplication is done modulo p). A value $x \in \mathbb{F}_p$ is called a root of P if $P(x) = 0$. Consider picking a random polynomial P by selecting $c_0, \ldots, c_d$ independently and uniformly at random from $\mathbb{F}_p$, and define the random variable

   $$Z \;=\; \text{Number of roots of } P \,.$$

   (a) Define an appropriate probability space Ω so that each possible degree-d polynomial P corresponds to an outcome in Ω.

   (b) Let $a \in \mathbb{F}_p$. For a *fixed* $x \in \mathbb{F}_p$, compute the probability

   $$\mathbb{P}\left[P(x) = a\right] \,.$$

   Remember that the probability is over the choice of the polynomial P.

   (c) Let Z be as defined above. Calculate $\mathbb{E}\left[Z\right]$.

   (d) Calculate $\mathsf{Var}\left[Z\right]$.

2. **One sided Chebyshev?** **[8]**

   Recall that for a real-valued random variable Z with mean μ and variance σ^2, Chebyshev's inequality shows that

   $$\mathbb{P}\left[|Z - \mu| \geq c\right] \;\leq\; \frac{\sigma^2}{c^2} \,.$$

Note that the above bound does not say anything when $c \leq \sigma$. Prove the following one-sided variant of Chebyshev's inequality for any real-valued random variable with mean μ and variance σ^2:

$$\mathbb{P}\left[Z - \mu \geq c\right] \;\leq\; \frac{\sigma^2}{c^2 + \sigma^2}\,.$$

Note that this bound is meaningful even when $c \in [0, \sigma]$.
(**Hint**: First bound the probability that $\mathbb{P}\left[Z + t - \mu \geq c + t\right]$.)

3. **Dominating sets.** **[2+2+6]**

Given a graph $G = (V, E)$ and a set $U \subseteq V$, a set S is said to be a dominating set for U, if for each $i \in U$, S contains i or some neighbor of i.

For a graph G with n vertices, let U be a subset of vertices such that all vertices in U have degree at least d. Consider picking a random set S_1 by including each vertex in V independently with probability p.

(a) What is $\mathbb{E}\left[|S_1|\right]$?

(b) For a fixed vertex $i \in U$, what is the probability that neither i nor any of its neighbors are included in S_1?

(c) Use the above to show that there exists a dominating set for U of size at most $n \cdot \left(\frac{1+\ln(d+1)}{(d+1)}\right)$.

4. **Approximating continuous functions.** **[3+2+3+2+2]**

In this exercise, we will prove Weierstrass's approximation theorem, which says that every continous function on $[0, 1]$ can be approximated to any desired degree of accuracy, using a polynomial of high enought degree. Here we outline Bernstein's proof of the theorem using probabilistic methods.

Let $f : [0, 1] \to \mathbb{R}$ be a *uniformly continuous* function i.e., $\forall \varepsilon > 0$, there exists a $\delta > 0$ such that

$$\forall x, y \in [0, 1] \qquad |x - y| < \delta \;\Rightarrow\; |f(x) - f(y)| < \varepsilon\,.$$

We will show that for any desired $\varepsilon > 0$, we can find a polynomial p such that $\forall x \in [0, 1]$, $|f(x) - p(x)| \leq \varepsilon$. We will prove this by approximating the given input x by an average of n coin tosses, where each coin comes up heads (equals 1) with probability x. Formally, let

$$Z \;=\; X_1 + \cdots + X_n\,,$$

where each $X_i = 1$ independently with probability x and 0 otherwise.

(a) Calculate $\mathbb{E}\left[\frac{Z}{n}\right]$ and $\mathsf{Var}\left[\frac{Z}{n}\right]$.

(b) Show that for each $k \in \{0, \ldots, n\}$, $\mathbb{P}[Z = k]$ can be written as a polynomial in x of degree at most n.

(c) Consider the expression

$$p(x) \;=\; \sum_{k=0}^{n} \mathbb{P}[Z = k] \cdot f\left(\frac{k}{n}\right) \;=\; \mathbb{E}\left[f\left(\frac{Z}{n}\right)\right].$$

By the previous part, this is a polynomial in the variable x of degree at most n (the values of f at different points in the expression do not depend on x). Let $\delta > 0$ be such that $\forall x, y \in [0,1]$, $|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon/2$. Define the event

$$E_x \;\equiv\; \left\{\left|\frac{Z}{n} - x\right| \geq \delta\right\},$$

and let $M = \sup_{x \in [0,1]} |f(x)|$. Show that for any $x \in [0,1]$

$$|f(x) - p(x)| \;\leq\; \frac{\varepsilon}{2} \cdot \mathbb{P}[E_x^c] \;+\; 2M \cdot \mathbb{P}[E_x].$$

(d) Use Chebyshev's inequality to bound $\mathbb{P}[E_x]$ in terms of x, n and δ.

(e) Using the above bound, find the least n such that for all $x \in [0,1]$, $\mathbb{P}[E_x] \leq \frac{\varepsilon}{4M}$.

Note that the above gives a polynomial p of degree at most n such that $\forall x \in [0,1]$, we have $|f(x) - p(x)| < \varepsilon$.

5. **Random 3-SAT.** **[3 + 3 + 4]**

A 3-SAT formula φ in n variables $\{x_1, \ldots, x_n\}$ is written as

$$\varphi \;\equiv\; C_1 \wedge \cdots \wedge C_m,$$

where each C_i is a clause of the form $C_i = (l_{i_1} \vee l_{i_2} \vee l_{i_3})$ and each l_{i_j} is in turn x_{i_j} or its negation $\overline{x}_{i_j}$. In this problem, we will choose the formula at random. In fact, we will fix the *structure* of the formula and only decide at random wether or not to negate a variable in a literal.

Let n be the number of variables and let $m > n\log(n)$ be the number of clauses we will choose. Let $S_1, \ldots, S_m \subseteq [n]$ be distinct sets (fixed in advance) such that $|S_i| = 3$ for each $i \in [m]$. For $S_i = \{i_1, i_2, i_3\}$, we generate the i^{th} clause in the formula as follows

- For each $j \in \{1,2,3\}$, independently take $l_{i_j} = x_{i_j}$ with probability $1/2$ and $l_{i_j} = \overline{x}_{i_j}$ with probability $1/2$.
- Take the clause $C_i = (l_{i_1} \vee l_{i_2} \vee l_{i_3})$.

Different clauses are generated independently of each other. Let φ be the (random) 3-SAT formula generated according to this process.

(a) Let $A \in \{0,1\}^n$ be a fixed assignment to the variables i.e., $A(x_j) \in \{0,1\}$ for each $j \in [n]$. Let $\varphi(A)$ denoted the number of clauses in φ satisfied by the assignment A. Calculate $\mathbb{E}[\varphi(A)]$. Show that this is a fixed number K depending only on m (but not on n and A).

(b) Let $\varepsilon > 0$ and an assignment $A \in \{0,1\}^n$ be given. Let K be as above. Show that

$$\mathbb{P}[|\varphi(A) - K| \geq \varepsilon \cdot m] \to 0 \quad \text{as} \quad n \to \infty\,.$$

(c) Show that

$$\mathbb{P}[\exists A \in \{0,1\}^n.\ |\varphi(A) - K| \geq \varepsilon \cdot m] \to 0 \quad \text{as} \quad n \to \infty\,.$$

All probabilities and expectations in the above problem are over the choice of the random formula φ.

6. **Random incoherent matrices.** **[2+ 4 + 4]**

Recall that in the class we proved that if a matrix $A \in \mathbb{R}^{k \times n}$ satisfies that

$$\left\|A^{(i)}\right\| = 1 \quad \forall i \in [n] \qquad \text{and} \qquad \left|\left\langle A^{(i)}, A^{(j)} \right\rangle\right| \leq \eta \quad \forall i \neq j,\ i,j \in [n]\,,$$

then A satisfies the restricted isometry property with parameters $(s, (s-1)\cdot\eta)$. In this problem we will construct such matrices randomly. Let $A \in \mathbb{R}^{k \times n}$ be a random matrix where each entry A_{ij} is chosen independently as

$$A_{ij} \;=\; \begin{cases} 1/\sqrt{k} & \text{with probability } 1/2 \\ -1/\sqrt{k} & \text{with probability } 1/2 \end{cases}$$

(a) Show that for each column $A^{(i)}$, we have $\left\|A^{(i)}\right\| = 1$.

(b) For two columns $A^{(i)}$ and $A^{(j)}$ with $i \neq j$, show that

$$\mathbb{P}\left[\left|\left\langle A^{(i)}, A^{(j)} \right\rangle\right| \geq \eta\right] \;\leq\; 2 \cdot \exp\left(-\eta^2 k/6\right)$$

(c) Show that for $k \geq 18 \cdot \ln(n)/\eta^2$, we have that the random matrix A satisfies the restricted isometry property with parameters $(s, (s-1)\cdot\eta)$, with probability at least $1 - O(1/n)$.