1. **Normal Symmetry.** Consider a random vector $R = \frac{1}{\sqrt{D}}(r_1, r_2, \ldots, r_D)$, where each entry $r_i \sim N(0, 1)$ independently. Show the following facts about R:

   (a) Show that R is "spherically symmetric", i.e., given any two vectors $\mathbf{x}, \mathbf{y}$ with $\|\mathbf{x}\| = \|\mathbf{y}\|$, the probability density function of R at $\mathbf{x}$ is equal to that at $\mathbf{y}$. Hence, infer that $R/\|R\|$ is a uniformly random point on the surface of a unit D-dimensional sphere.

   (b) Prove that if $Y_1 \sim N(\mu_1, \sigma_1^2)$ and $Y_1 \sim N(\mu_1, \sigma_1^2)$ are independent, then
   $$Y_1 + Y_2 \sim N(\mu_1 + \mu_2, \sigma_1^2 + \sigma_2^2).$$

   (c) Show that $\|R\| \notin (1 \pm \varepsilon)$ with probability $\exp(-O(\varepsilon^2 D))$.

2. **(k-Universal.)** Recall the definition of *k-wise-independent* (also known as k-universal) from Lecture #13.

   (a) For a given matrix $A \in \{0, 1\}^{m\times u}$, define $h_A : \{0, 1\}^u \to \{0, 1\}^m$ by $h_A(x) = Ax$; all calculations are done modulo 2. Consider the hash family $H = \{h_A \mid A \in \{0, 1\}^{m\times u}\}$ be the set of all 2^{mu} functions obtained this way. Show that this hash family is not 2-universal.

   (b) For a given matrix $A \in \{0, 1\}^{m\times u}$ and $b \in \{0, 1\}^m$, define $h_{A,b} : \{0, 1\}^u \to \{0, 1\}^m$ by $h_A(x) = Ax + b$; all calculations are done modulo 2. Consider the hash family $H = \{h_{A,b} \mid A \in \{0, 1\}^{m\times u}, b \in \{0, 1\}^m\}$ be the set of all $2^{m(u+1)}$ functions obtained this way. Show that this hash family is 2-universal.

   (c) Construct matrix $A \in \{0, 1\}^{m\times u}$ as follows. Fill the first row $A_{1,\star}$ and the first column $A_{\star,1}$ with independently random bits. For any other entry i, j for $i > 1$ and $j > 1$, define $A_{i,j} = A_{i-1,j-1}$. So all entries in each "northwest-southeast" diagonal in A are the same. Also pick a random m-bit vector $b \in \{0, 1\}^m$. For $x \in U = \{0, 1\}^u$, define $h_{A,b}(x) := Ax + b$ modulo 2 as usual. Show this hash family H with $2^{(u+m-1)+m}$ hash functions is 2-universal.

   (d) Given elements $\alpha_0, \alpha_1, \ldots, \alpha_{k-1} \in \mathbb{F}$, define $f(x) = \sum_{i=0}^{k-1} \alpha_i x^i$, where the calculations are done in the field $\mathbb{F}$. Show that if $k \le p$, the hash family H of all such functions from $\mathbb{F} \to \mathbb{F}$ is k-universal.

3. **(Graph Domination.)** Given a graph $G = (V, E)$, a set $D \subseteq V$ is dominating if for every vertex v, either $v \in D$ or some neighbor of v is in D. Suppose the minimum degree of any vertex in G is δ.

   (a) Pick a random set D, where each vertex v is added to D independently with probability $\min\{1, \frac{c \log n}{1+\delta}\}$. Show that D is a dominating set with probability at least $1 - 1/n^{c-1}$.

   (b) Can you find a dominating set of expected size $\frac{n(1+\ln(1+\delta))}{1+\delta}$. (Hint: pick a smaller random set of vertices, and then add some more vertices as needed.)

4. **Hoeffding vs. Bernstein.** There are many different "Chernoff-style" concentration inequalities that are useful in different situations. E.g., consider the following Hoeffding's and Bernstein's inequalities.

Hoeffding Let $X_1, \ldots, X_n$ be independent r.v.s supported on $[a_i, b_i]$ and let $S := \sum_{i=1}^n X_i$. Then $\mathbf{Pr}[|S - \mathbf{E}[S]| \geq \lambda] \leq 2\exp\left(\frac{-2\lambda^2}{\sum_i (b_i - a_i)^2}\right)$.

Bernstein Let $X_1, \ldots, X_n$ be independent r.v.s supported on $[a_i, b_i]$ where $b_i - a_i \leq M$ and let $S := \sum_{i=1}^n X_i$. Then $\mathbf{Pr}[|S - \mathbf{E}[S]| \geq \lambda] \leq 2\exp\left(\frac{-\lambda^2/2}{\mathbf{Var}[S] + \frac{1}{3}M\lambda}\right)$.

(a) Find a setting with independent random variables supported on $[0, 1]$ where Hoeffding's inequality gives an asymptotically tighter bound than Bernstein's inequality. (Hint: Bernstein's inequality has unavoidable subexponential behavior for large λ.)

(b) Find a similar setting where Bernstein's inequality gives asymptotically better bound than Hoeffding's inequality. (Hint: consider the case when λ is small.)