Catalog

Question 1

Answer:

The relationships between the four notions of differential privacy are as follows:

1. Pure Differential Privacy (ε-DP) implies Approximate Differential Privacy ((ε, δ)-DP), but not vice versa. Under ε-DP, the privacy loss random variable is almost surely bounded between $-\varepsilon$ and ε because the ratio of probabilities $\Pr[A(D) = o]/\Pr[A(D') = o]$ is bounded by e^{ε}. This strict bound means that for all outputs, the difference in probabilities is tightly controlled, satisfying (ε, δ)-DP with δ = 0. However, (ε, δ)-DP allows the privacy loss to exceed ε with probability up to δ, so it does not imply the strict bounds of ε-DP unless δ = 0.

2. Pure Differential Privacy (ε-DP) implies Zero-Concentrated Differential Privacy (ρ-zCDP), but not vice versa. In ε-DP, the bounded privacy loss random variable ensures sub-Gaussian tails with parameter $\rho \geq \varepsilon^2/2$. This sub-Gaussian behavior aligns with the definition of zCDP, where the privacy loss random variable has a certain concentration (controlled variance). Conversely, zCDP allows for unbounded privacy loss values with sub-Gaussian tails, so it does not enforce the strict bounds required by ε-DP.

3. Zero-Concentrated Differential Privacy (ρ-zCDP) implies Rényi Differential Privacy (α, ε′(α)-RDP), but not necessarily the other way around. zCDP ensures that the privacy loss random variable is sub-Gaussian, which implies that the Rényi divergence of order α between A(D) and A(D′) is at most ε′(α) = ρα. This directly satisfies the definition of RDP. However, RDP can allow for privacy loss random variables with heavier tails (sub-exponential), so it does not always imply the sub-Gaussian concentration required for zCDP unless additional conditions are met.

4. Rényi Differential Privacy (α, ε′(α)-RDP) implies Approximate Differential Privacy ((ε, δ)-DP), and vice versa under certain parameters. RDP bounds the Rényi divergence, which controls the moments of the privacy loss random variable. By applying concentration inequalities, one can derive (ε, δ)-DP guarantees from RDP parameters. Similarly, (ε, δ)-DP provides bounds on the cumulative distribution function of the privacy loss, which can be used to derive RDP parameters for certain α. The conversion between RDP and approximate DP depends on the specific values of α, ε, and δ.

5. Zero-Concentrated Differential Privacy (ρ-zCDP) implies Approximate Differential Privacy ((ε, δ)-DP), but not vice versa. The sub-Gaussian nature of the privacy loss random variable in zCDP allows us to bound the probability that the privacy loss exceeds any ε, leading to (ε, δ)-DP with δ depending on ρ and ε. Specifically, tail bounds for sub-Gaussian distributions show that the probability of large deviations decreases exponentially, satisfying the δ requirement. However, approximate DP allows for heavier-tailed distributions (sub-exponential), so it does not ensure the sub-Gaussian concentration needed for zCDP.

6. Pure Differential Privacy (ε-DP) implies Rényi Differential Privacy (α, ε′(α)-RDP), but not vice versa. Since ε-DP bounds the privacy loss random variable between $-\varepsilon$ and ε, all its moments are bounded, and the Rényi divergence of any order α is at most ε′(α) = αε²/2 (for $\alpha \geqslant 1$). This satisfies the RDP definition with specific ε′(α). Conversely, RDP does not impose the strict pointwise bounds on the privacy loss random variable required for ε-DP unless ε′(α) is zero for all α, which is trivial.

In conclusion, the implications between these notions form a hierarchy based on the restrictiveness of the privacy guarantees, primarily determined by the behavior of the privacy loss random variable:
Pure DP (most restrictive, bounded privacy loss) implies zCDP (sub-Gaussian privacy loss),
zCDP implies RDP (controls on the Rényi divergence, sub-exponential tails),
RDP implies Approximate DP (least restrictive, allows small probability δ of larger privacy loss).

Question 2

Answer:
(a) Since the privacy loss $L(o)$ is almost surely equal to ε_0, it means that for all outputs o, we have $\ln\left(\frac{\Pr[A(D)=o]}{\Pr[A(D')=o]}\right) = \varepsilon_0$. This implies $\Pr[A(D) = o] = e^{\varepsilon_0}\Pr[A(D') = o]$ for all o. Therefore, the mechanism satisfies Pure Differential Privacy (ε-DP) with $\varepsilon = \varepsilon_0$, because the ratio of probabilities is exactly bounded by e^{ε_0}.

(b) The privacy loss $L(o)$ lies within $[0, \varepsilon_1]$ for all outputs o, which means $\ln\left(\frac{\Pr[A(D)=o]}{\Pr[A(D')=o]}\right) \leq \varepsilon_1$ and $\Pr[A(D) = o] \leq e^{\varepsilon_1}\Pr[A(D') = o]$. Additionally, since $L(o) \geq 0$, $\Pr[A(D') = o] \leq \Pr[A(D) = o]$. Thus, the mechanism satisfies Pure Differential Privacy (ε-DP) with $\varepsilon = \varepsilon_1$, as the privacy loss is bounded within $[0, \varepsilon_1]$.

(c) The privacy loss $L(o)$ follows a normal distribution with mean 0 and variance σ^2, exhibiting sub-Gaussian tails. This implies that for all $\alpha > 1$, the Rényi divergence $D_\alpha(A(D) \parallel A(D')) \leq \frac{\alpha}{2\sigma^2}$. Hence, the mechanism satisfies Zero-Concentrated Differential Privacy (ρ-zCDP) with $\rho = \frac{1}{2\sigma^2}$, because the privacy loss random variable meets the sub-Gaussian concentration required by zCDP.

(d) Here, $L(o)$ follows a Laplace distribution with sub-exponential tails, which means the moment-generating function exists only within a finite interval. This allows us to bound the Rényi divergence $D_\alpha(A(D) \parallel A(D'))$ by $\varepsilon'(\alpha) = \frac{\alpha}{b}$ for $\alpha > 1$. Therefore, the mechanism satisfies Rényi Differential Privacy (α, ε′(α)-RDP), as it provides explicit bounds on the Rényi divergence based on the scale parameter b.

(e) The privacy loss $L(o)$ takes values $\pm\varepsilon_2$ with equal probability, so $|L(o)| = \varepsilon_2$ almost surely. This means that both $\Pr[A(D) = o] \leq e^{\varepsilon_2}\Pr[A(D') = o]$ and $\Pr[A(D') = o] \leq e^{\varepsilon_2}\Pr[A(D) = o]$ hold for all o. Consequently, the mechanism satisfies Pure Differential Privacy (ε-DP) with $\varepsilon = \varepsilon_2$, due to the absolute bound on the privacy loss.

In summary:
(a) represents (1) Pure Differential Privacy (ε-DP).
(b) represents (1) Pure Differential Privacy (ε-DP).
(c) represents (3) Zero-Concentrated Differential Privacy (ρ-zCDP).
(d) represents (4) Rényi Differential Privacy (α, ε′(α)-RDP).
(e) represents (1) Pure Differential Privacy (ε-DP).
Each privacy loss distribution corresponds to the strictest differential privacy notion it satisfies, and by the implications established, it also satisfies the less restrictive notions.

Question 5

Answer:
To show that the VC dimension of the class C of convex subsets in the unit square $[0,1]^2$ is ∞, need to demonstrate that for any positive integer n, there exists a set of n points in $[0,1]^2$ that can be shattered by C.
1. Selection of Points:
Let n be any positive integer.
Choose n distinct points $\{x_1, x_2, \ldots, x_n\}$ in $[0,1]^2$ such that no three points are colinear (they are in general position). Since $[0,1]^2$ is uncountably infinite, always select such points within the unit square.
2. Shattering the Points:
For any binary labeling of these n points (each point labeled either 0 or 1), to find a convex set $S \subseteq [0,1]^2$ such that:
All points labeled 1 are inside S.
All points labeled 0 are outside S.
3. Construction of the Convex Set:
If all points are labeled 1:
The convex hull of all the points $\{x_1, x_2, \ldots, x_n\}$ is a convex set containing all the points, satisfying the labeling.
If some points are labeled 0 and others 1:

Let P_1 be the set of points labeled 1.

Let P_0 be the set of points labeled 0.

Construct the convex hull Conv(P_1) of the positively labeled points P_1. This is the smallest convex set containing all points in P_1.

Since the points are in general position, for each negatively labeled point $x_i \in P_0$, there exists a hyperplane (in 2D, a straight line) that separates x_i from Conv(P_1).

For each $x_i \in P_0$, introduce a half-plane that excludes x_i but includes Conv(P_1).

Intersecting Convex Sets:

The intersection of convex sets is convex. Therefore, intersecting Conv(P_1) with the half-planes that exclude the negatively labeled points yields a convex set S that contains all positively labeled points and excludes all negatively labeled points.

Conclusion:

Since can construct such a convex set S for any binary labeling of the n points, the set of points $\{x_1, x_2, \dots, x_n\}$ is shattered by C.

As n was arbitrary, this process works for any positive integer n.

Therefore, the VC dimension of C is ∞.

Question 6

Answer:

An infinite VC dimension implies that the class C is not PAC learnable, because no finite sample size can guarantee uniform convergence between empirical risk and true risk for all distributions over $[0,1]^2$; thus, learning C with arbitrarily high accuracy and confidence is impossible in the PAC framework.