1 Differential Privacy

1.1 Setting: Collecting and Providing Statistical Data

- Problem: Gender, age, weight, ethnicity, and marital status (for example) may be sufficient for identification among 1000 patients. Illustrative example: “AOL search data scandal”

1.2 An Utopian Goal

- Ideally: Cannot learn anything about an individual that could not be learned without access to statistical database. Similar to semantic security: Nothing can be learned about a plaintext from the ciphertext that could not be learned without seeing the ciphertext.
- Impossible in this generality (while semantic security is possible). Example: Statistical information on average income. Auxiliary information: 20% higher than average. Note: Additional information gives solution regardless of person is in database.

1.3 The Differential-Privacy Approach

- Other approach to privacy: (Non-)Participating in a statistical database does not substantially affect the outcome of any analysis.
- Model: A database \(d\) is a string \(d_1, \ldots, d_n\) of length \(n\) over some set \(D\). Each \(d_i\) is called a row in \(d\). Two databases are neighbors if they coincide in \((n-1)\) rows. A query is a function \(f : D^n \to \mathcal{R}\). For now, assume \(\mathcal{R} \subset \mathbb{R}\) bounded. A privacy mechanism \(K_f\) adds noise to the true answer \(f(d)\) to produce the response \(K_f(d) = f(d) + \Delta\), where \(\Delta\) is a random variable.

- Definition: \(K_f\) gives \(\varepsilon\)-differential privacy if for all neighboring \(d, d' \in D^n\) and all \(S \subseteq \mathcal{R}\),

\[
\Pr[K_f(d) \in S] \leq \exp(\varepsilon) \cdot \Pr[K_f(d') \in S].
\]

- Definition: The sensitivity of a query \(f : D^n \to \mathcal{R}\) is \(\Delta f := \max_{\text{neighbors } d,d'} |f(d) - f(d')|\).

- Typical privacy mechanism: Let \(K_f = f(d) + \Delta\), where \(\Delta \sim \text{Lap}(0, b)\) (Laplacian distribution with mean 0 and variance \(2b^2\)) and \(b = \Delta f / \varepsilon\), i.e., with density

\[
x \mapsto \frac{1}{2b} \exp \left( -\frac{|x|}{b} \right)
\]

and cumulative distribution function \(\Pr[\Delta \leq x] = \frac{1}{2} \left[ 1 + \text{sgn}(x) \left( 1 + \exp \left( -\frac{|x|}{b} \right) \right) \right]\).

- This gives \(\varepsilon\)-differential privacy:

\[
\Pr[K_f(d) \in S] = \int_S \frac{\varepsilon}{2\Delta f} \exp \left( -\frac{|f(d) - r|}{\Delta f} \right) d\lambda(r)
\]

\[
\leq \int_S \frac{\varepsilon}{2\Delta f} \exp \left( -\frac{\Delta f}{\Delta f} \right) d\lambda(r)
\]

\[
\left[ -\Delta f - |f(d) - r| \leq -|f(d') - f(d) - f(d) - r| - |f(d) - r| \leq -|f(d') - r| \right]
\]

\[
= \exp(\varepsilon) \cdot \Pr[K_f(d') \in S]
\]

- Querying multiple values: If \(f : D^n \to \mathcal{R}^k\), let \(\Delta f = \max_{\text{neighbors } d,d'} \|f(d) - f(d')\|_1\).
1.4 Count Queries Are Powerful \cite{2}

- Special case: \( D = \{0, 1\} \), consider only subset-sum (count) queries \( f_Q : D^n \rightarrow [n] \), where \( Q \subseteq [n] \) and \( f_Q(d) := \sum_{i \in Q} d_i \).
- **Theorem:** Answering \( O(n \log^2 n) \) randomly chosen queries with error \( E = o(\sqrt{n}) \) allows an adversary to reconstruct most of the rows (all if \( n \to \infty \)) with the following algorithm:
  
  i) **[Query phase]** For \( j = 1, \ldots, t \), choose \( Q_j \subseteq [n] \) uniformly at random. Set \( a_Q := K f(d) \) where \( f = f_{Q_j} \).
  
  ii) **[Weeding phase]** Solve linear program with unknowns \( c_1, \ldots, c_n \):

  \[
  a_{Q_j} - E \leq \sum_{i \in Q_j} c_i \leq a_{Q_j} + E \quad \forall j \in [t] \\
  0 \leq c_i \leq 1 \quad \forall i \in [n]
  \]

  iii) **[Rounding Phase]** Let \( c'_i = 1 \) if \( x_i > \frac{1}{2} \) and \( c'_i = 0 \) otherwise.

  - Note first: LP has solution because \( d \) is feasible solution
  - For \( x \in [0, 1]^n \), denote by \( \overline{x} \) rounding each coordinate to the nearest multiple of \( \frac{1}{n} \).
  - We say \( x \) is \( \epsilon \)-far away from \( d \) if \( |x_i - d_i| \geq \frac{1}{3} \) for more than an \( \epsilon \)-share of all rows \( i \).
  - If an \( x \) satisfies the LP, we have for any query \( Q_j \) selected by the algorithm

  \[
  \left| \sum_{i \in Q_j} (\bar{x}_i - d_i) \right| \leq \left| \sum_{i \in Q_j} (\bar{x}_i - x_i) \right| + \left| \sum_{i \in Q_j} x_i - a_{Q_j} \right| + \left| a_{Q_j} - \sum_{i \in Q_j} d_i \right| \leq \frac{|Q_j|}{n} + E + E \leq 1 + 2E.
  \]

  Conversely, we say a query \( Q \subseteq [n] \) disqualifies \( \overline{x} \) if \( \sum_{i \in Q} (\bar{x}_i - d_i) > 1 + 2E \).

- **Disqualifying Lemma** (without proof here, based on Azuma’s inequality): Suppose \( x, d \in [0, 1]^n \), \( E = o(\sqrt{n}) \). If \( x \) is \( \epsilon \)-far away from \( d \) then there is \( \delta > 0 \) so that

  \[
  \Pr_{Q_j} \left[ \sum_{i \in Q_j} (x_i - d_i) > 2E + 1 \right] = \delta.
  \]

  - For any \( \bar{x} \) that is far away from \( d \), lemma says that \( \bar{x} \) is disqualified by one of the queries picked by the algorithm with probability \( 1 - (1 - \delta)^t \). With the union bound,

  \[
  \Pr_{Q_1, \ldots, Q_t} \left[ \forall \bar{x} : \exists j : Q_j \text{ disqualifies } \bar{x} \right] > 1 - (n + 1)^n(1 - \delta)^t > 1 - o(1/n^k)
  \]

  for any \( k \in \mathbb{N} \), when choosing, say, \( t = n \log^2 n \).

  - Now, \( \bar{c} \) was not disqualified by any \( Q_j \), so \( \bar{c} \) is not far away from \( d \). Hence, also \( c' \) and \( d \) differ in at most an \( \epsilon \)-share of the rows.
1.5 Tightness

- This is tight in the following sense: If an attacker must assume that the database is random (uniform distribution), then there is a mechanism with perturbation $E = \sqrt{n} \cdot (\log n)^{1+\varepsilon}$ that does reveal almost nothing by answering polynomially many queries:

- Input: Query $Q \subseteq [n]$
  
  i) Compute $a_Q := \sum_{i \in Q} d_i$
  
  ii) Return $|Q|^2$ if $|a_Q - \frac{|Q|}{2}| < E$ and return $a_Q$ otherwise

- Of course, this mechanism is useless. Remedy: Allow only sublinear number of queries [2, 5]

1.6 Non-Numerical Queries [7]

- Definition: Given a database $d \in D^n$, let $q : D^n \times \mathcal{R} \to \mathbb{R}$ be a measurable scoring (weighting) function. Then define the exponential privacy mechanism $K_f$ by

  $$\Pr[K_f(d) \in S] := \frac{\int_{S} \exp(\varepsilon q(d, r)) d\lambda(r)}{\int_{\mathcal{R}} \exp(\varepsilon q(d, r)) d\lambda(r)}.$$  

  (We require that $q$ is such that the integral is bounded.)

- Define $\Delta q := \max_{r \in \mathcal{R}, \text{neighbors } d, d'} |q(d, r) - q(d', r)|$.

- Lemma: As defined above, $K_f$ gives $(2\varepsilon \Delta q)$-differential privacy.

- For neighboring $d, d'$ the change in both numerator and denominator of (1.1) can be at most $\exp(\varepsilon \Delta q)$ each, i.e., at most $\exp(2\varepsilon \Delta q)$ in total.

1.7 Privacy as a Solution Concept for Mechanism Design [7]

- A player’s strategy is said to be $\varepsilon$-dominant if no other strategy ever provides this player with more than $\varepsilon$ additional utility.

- Lemma: A mechanism satisfying $\varepsilon$-differential privacy makes truth-telling an $(\exp(\varepsilon) - 1)$-dominant strategy for any player with a utility function that maps $\mathcal{R}$ to $[0, 1]$.

- Notation: Let $\mu_{K_f, d}$ be the probability distribution of $K_f(d)$, i.e., $\mu_{K_f, d}(S) = \Pr[K_f(d) \in S]$. When unambiguous, we omit indices.

- Even stronger: Regardless of the utility function $u : \mathcal{R} \to \mathbb{R}_{\geq 0}$, no player can cause a relative change of more than $\exp(\varepsilon)$ in its utility because $E[u(K_f(d))] = \int_{\mathcal{R}} u(r) d\mu_d(r) \leq \exp(\varepsilon) \cdot \int_{\mathcal{R}} u(r) d\mu_{d'}(r) = \exp(\varepsilon) \cdot E[u(K_f(d'))]$. 

1.7.1 Unlimited Supply Auctions

- Consider auctioneer with endless supply of arbitrarily divisible good. The outcome (response) is a price $p \in \mathcal{R} := [0, 1]$. Each bidder $i$ will reveal a non-increasing demand curve $b_i : \mathcal{R} \to \mathbb{R}_{>0}$, mapping prices to desired units. Requirement: $pb_i(p) \leq 1$
• For bid vector (database) $b$ and price $p$, we sell $\sum_i b_i(p)$ items, yielding revenue $q(b,p) = p\sum_i b_i(p)$. Let $OPT$ denote the maximum revenue.

**Theorem:** The exponential mechanism gives $2\varepsilon$-differential privacy and has expected revenue at least $OPT - \frac{3}{\varepsilon} \ln(e + \varepsilon^2 OPTm)$, where $m$ is the number of items sold in $OPT$.

• Privacy follows from above lemma, as a bidder can change $q(b,p)$ by at most $pb_i(p) \leq 1$

• Let $S_t := \{ r \in R \mid q(d,r) > OPT - t \}$. Note:

$$\mu(S_{2t}) \leq \frac{\mu(S_t)}{\lambda(S_t)} \leq \frac{\int_{S_t} \exp(\varepsilon q(d,r)) \, d\lambda(r)}{\int_{S_t} \exp(\varepsilon q(d,r)) \, d\lambda(r)} \leq \frac{\exp(-\varepsilon t) \cdot \lambda(S_{2t})}{\lambda(S_t)} \leq \exp(-\varepsilon t) \cdot \lambda(S_t) \leq 1$$

• Suppose $t \geq \frac{1}{\varepsilon} \ln \left( \frac{OPT}{\lambda(S_t)} \right)$. Then

$$E[q(d,K_f(d))] \geq \left( 1 - \frac{\exp(-\varepsilon t)}{\lambda(S_t)} \right) \cdot (OPT - 2t) \geq \left( 1 - \frac{t}{OPT} \right) \cdot (OPT - 2t) \geq OPT - 3t$$

• Assume, w.l.o.g., that $OPT > t$ (otherwise trivial). Set $t = \frac{1}{\varepsilon} \ln(e + \varepsilon^2 OPTm)$. Since $t \geq \frac{1}{\varepsilon}$, we have $t \geq \frac{1}{\varepsilon} \ln \left( \frac{OPTm}{t} \right)$. Hence, by previous item, it remains to show that $\frac{t}{m} \leq \lambda(S_t)$.

• Note that for all prices $\geq OPT - \frac{t}{m}$ less than the optimal price, the same $m$ items would continue to be sold (demand non-increasing as price increase), and for all these $m$ items the loss is at most $\frac{t}{m}$. Hence, the total profit would still be at least $OPT - t$. Hence, the measure of all prices giving revenue at least $OPT - t$ (i.e., $\lambda(S_t)$) is at least as large as the measure of all prices $\geq OPT - \frac{t}{m}$ (that is, $\lambda([OPT - \frac{t}{m}, OPT]) = \frac{t}{m}$).

References