# CSE660
# Differential Privacy

November 27, 2017

Marco Gaboardi

Room: 338-B

gaboardi@buffalo.edu

http://www.buffalo.edu/~gaboardi

# Differential privacy

**Definition**

Given $\varepsilon, \delta \geq 0$, a probabilistic query $Q: X^n \rightarrow R$ is $(\varepsilon,\delta)$-differentially private iff

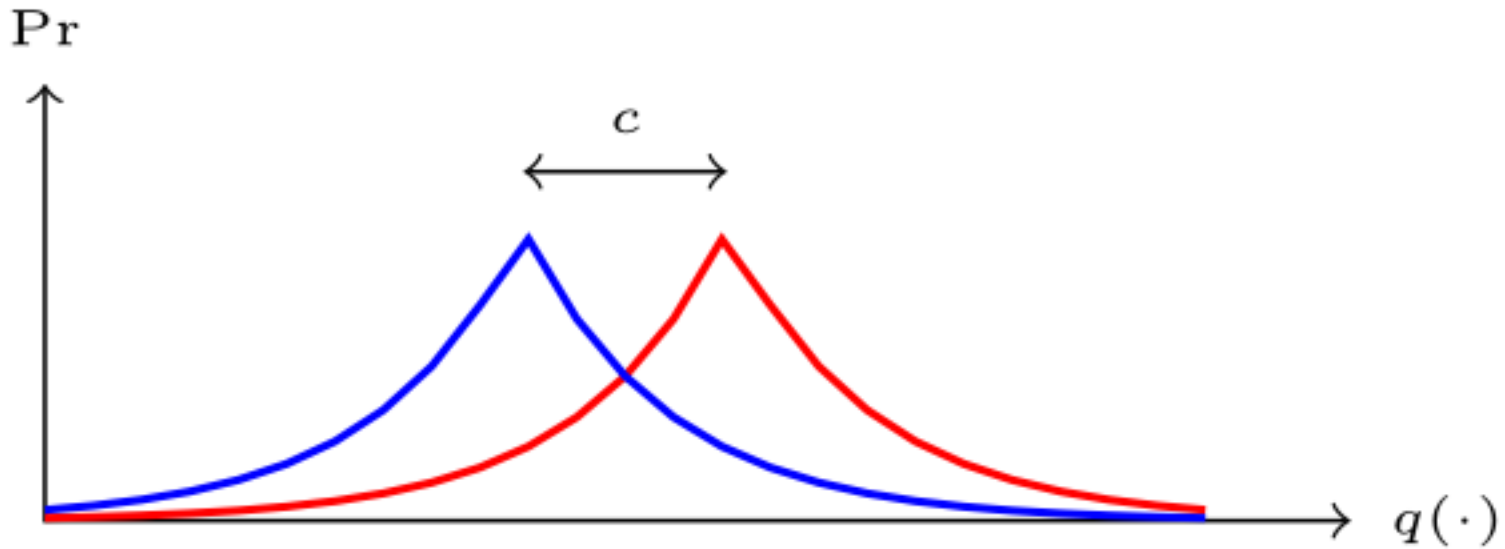
for all adjacent database $b_1, b_2$ and for every $S \subseteq R$:

$$\Pr[Q(b_1) \in S] \leq \exp(\varepsilon)\Pr[Q(b_2) \in S] + \delta$$

# Laplace Mechanism

**Algorithm 2** Pseudo-code for the Laplace Mechanism

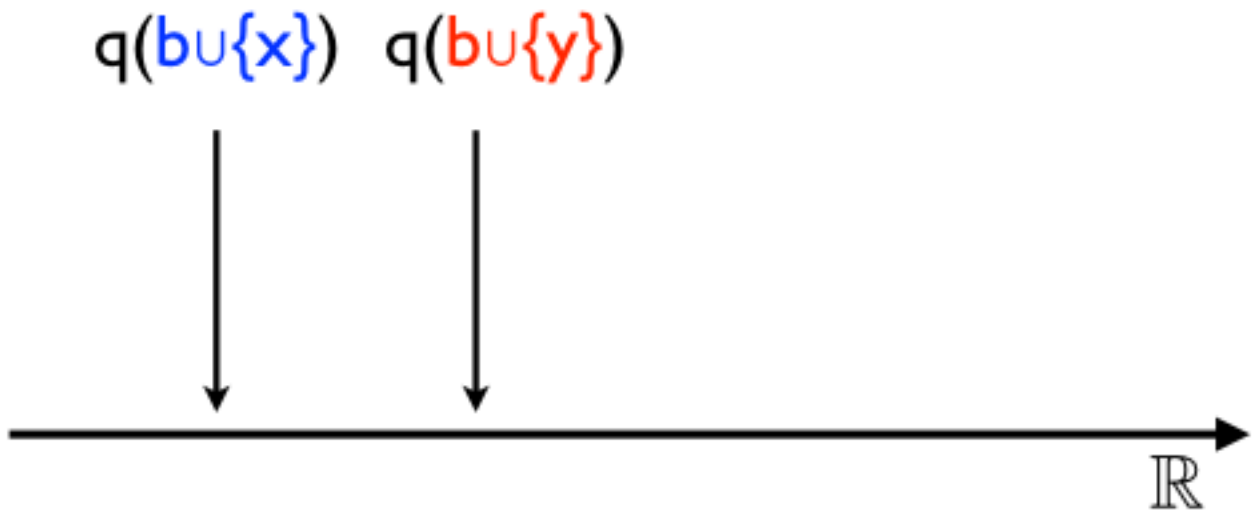
1: **function** LAPMECH($D, q, \epsilon$)
2: $\quad Y \xleftarrow{\$} \mathsf{Lap}(\frac{\Delta q}{\epsilon})(0)$
3: $\quad$ **return** $q(D) + Y$
4: **end function**



# Global Sensitivity

**Definition 1.8** (Global sensitivity)**.** The *global sensitivity* of a function $q : \mathcal{X}^n \to \mathbb{R}$ is:

$$\Delta q = \max \left\{ |q(D) - q(D')| \;\middle|\; D \sim_1 D' \in \mathcal{X}^n \right\}$$



# Local sensitivity

**Definition 1.8** (Global sensitivity)**.** The *global sensitivity* of a function $q : \mathcal{X}^n \to \mathbb{R}$ is:

$$\Delta q = \max \left\{ |q(D) - q(D')| \;\middle|\; D \sim_1 D' \in \mathcal{X}^n \right\}$$

**Definition 1.14** (Local sensitivity)**.** The *local sensitivity* of a function $q : \mathcal{X}^n \to \mathbb{R}$ at $D \in \mathcal{X}^n$ is:

$$\ell\Delta q(D) = \max \left\{ |q(D) - q(D')| \;\middle|\; D \sim_1 D',\ D' \in \mathcal{X}^n \right\}$$

# Calibrating noise to the local sensitivity



We may add noise proportional to the local sensitivity (LS).

Unfortunately, this does not guarantee privacy.

Suppose that for a given D we have LS(D)=0 but that we also have D~D' with LS(D')=$10^9$.

We will see that we can do anyway better than GS.

# Some methods

- Smooth Sensitivity
- Propose-Test-Release
- Releasing Stable Values

# Smooth Sensitivity

**Definition 2.2** (Smooth sensitivity). *For $\beta > 0$, the $\beta$-smooth sensitivity of $f$ is*

$$S^*_{f,\beta}(x) = \max_{y \in D^n} \left( LS_f(y) \cdot e^{-\beta d(x,y)} \right).$$

**Definition 2.1** (A Smooth Bound on $LS$). *For $\beta > 0$, a function $S : D^n \to \mathbb{R}^+$ is a $\beta$-smooth upper bound on the local sensitivity of $f$ if it satisfies the following requirements:*

$$\forall x \in D^n : \quad S(x) \geq LS_f(x) ; \tag{1}$$

$$\forall x, y \in D^n, d(x,y) = 1 : \quad S(x) \leq e^{\beta} \cdot S(y) . \tag{2}$$

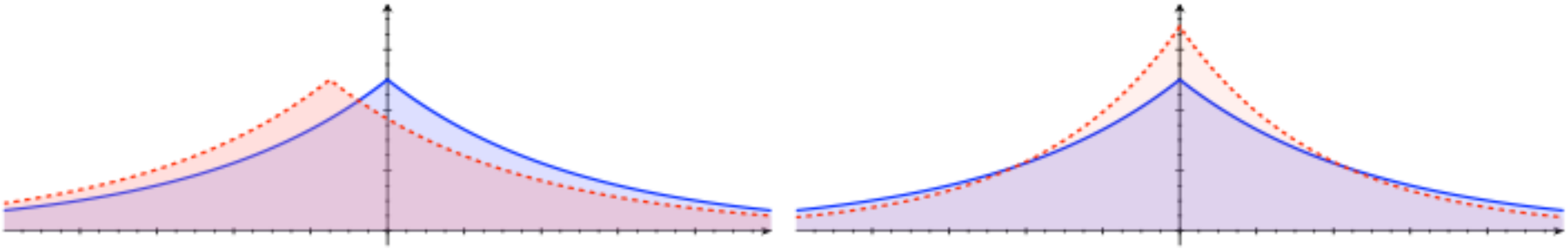
[Nissim, Raskhodnikova, Smith '06]

# Calibrating noise to the smooth sensitivity



**Lemma 2.6.** *Let $h$ be an $(\alpha, \beta)$-admissible noise probability density function, and let $Z$ be a fresh random variable sampled according to $h$. For a function $f : D^n \to \mathbb{R}^d$, let $S : D^n \to \mathbb{R}$ be a $\beta$-smooth upper bound on the local sensitivity of $f$. Then algorithm $\mathcal{A}(x) = f(x) + \frac{S(x)}{\alpha} \cdot Z$ is $(\epsilon, \delta)$-differentially private.*

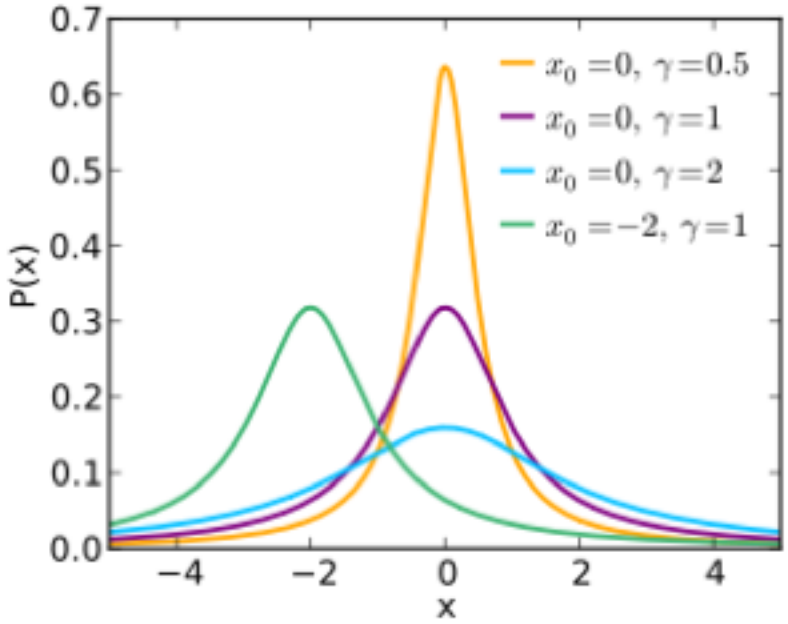
For two neighbor databases $x$ and $y$, the output distribution $\mathcal{A}(y)$ is a shifted and scaled version of $\mathcal{A}(x)$. The sliding and dilation properties ensure that $\Pr[\mathcal{A}(x) \in \mathcal{S}]$ and $\Pr[\mathcal{A}(y) \in \mathcal{S}]$ are close for all sets $\mathcal{S}$ of outputs.



[Nissim, Raskhodnikova, Smith '06]

# Admissible Noise

Adding noise $O(\mathrm{SS}_q^{\varepsilon}(x)/\varepsilon)$ (according to a Cauchy distribution) is sufficient for $\varepsilon$-differential privacy.




Laplace and Gauss give (ε,δ)-DP

Computing the Smooth Sensitivity can be intractable.

[Nissim, Raskhodnikova, Smith '06]

# Propose Test Release

**Propose-test-release** Given $q : \mathcal{X}^n \to \mathbb{R}$, $\epsilon, \delta, \beta \geq 0$

1. Propose a target bound $\beta$ on local sensitivity.
2. Let $\hat{d} = d(x, \{x' : \mathrm{LS}_q(x') > \beta\}) + \mathrm{Lap}(1/\varepsilon)$, where $d$ denotes Hamming distance.
3. If $\hat{d} \leq \ln(1/\delta)/\varepsilon$, output $\perp$.
4. If $\hat{d} > \ln(1/\delta)/\varepsilon$, output $q(x) + \mathrm{Lap}(\beta/\varepsilon)$.

# Stability-based algorithms

**Releasing stable values** Given $q : \mathcal{X}^n \to \mathbb{R}$, $\epsilon, \delta \geq 0$

1. Let $\hat{d} = d(x, \{x' : q(x') \neq q(x)\}) + \mathrm{Lap}(1/\varepsilon)$, where $d$ denotes Hamming distance.
2. If $\hat{d} \leq 1 + \ln(1/\delta)/\varepsilon$, output $\perp$.
3. Otherwise output $q(x)$.

**Proposition 3.3** (releasing stable values)**.** *For every query $q : \mathcal{X}^n \to \mathcal{Y}$ and $\varepsilon, \delta > 0$, the above algorithm is $(\varepsilon, \delta)$-differentially private.*

# Stability-based algorithms

Consider, for example, the *mode* function $q : \mathcal{X}^n \to \mathcal{X}$, where $q(x)$ is defined to be the most frequently occurring data item in $x$ (breaking ties arbitrarily). Then $d(x, \{x' : q(x') \neq q(x)\})$ equals half of the gap in the number of occurrences between the mode and the second-most frequently occurring item (rounded up). So we have:

**Proposition 3.4** (stability-based mode)**.** *For every data universe $\mathcal{X}$, $n \in \mathbb{N}$, $\varepsilon, \delta \geq 0$, there is an $(\varepsilon, \delta)$-differentially private algorithm $\mathcal{M} : \mathcal{X}^n \to \mathcal{X}$ such that for every dataset $x \in \mathcal{X}^n$ where the difference between the number of occurrences of the mode and the 2nd most frequently occurring item is larger than $4\lceil \ln(1/\delta)/\varepsilon \rceil$, $\mathcal{M}(x)$ outputs the mode of $x$ with probability at least $1 - \delta$.*

# Stability-based Histogram

1. For every point $y \in \mathcal{X}$:
   (a) If $q_y(x) = 0$, then set $a_y = 0$.
   (b) If $q_y(x) > 0$, then:
      i. Set $a_y \leftarrow q_y(x) + \mathrm{Lap}(2/\varepsilon n)$.
      ii. If $a_y < 2\ln(2/\delta)/\varepsilon n + 1/n$, then set $a_y \leftarrow 0$.
2. Output $(a_y)_{y \in \mathcal{X}}$.

# Stability-based Histogram

**Utility:** The algorithm gives exact answers for queries $q_y$ where $q_y(x) = 0$. There are at most $n$ queries $q_y$ with $q_y(x) > 0$ (namely, ones where $y \in \{x_1, \ldots, x_n\}$). By the tails of the Laplace distribution and a union bound, with high probability all of the noisy answers $q_y(x)+\text{Lap}(2/\varepsilon n)$ computed in Step 1(b)i have error at most $O((\log n)/\varepsilon n) \leq O(\log(1/\delta)/\varepsilon n)$. Truncating the small values to zero in Step 1(b)ii introduces an additional error of up to $2\ln(1/\delta)/\varepsilon n + 1/n = O(\log(1/\delta)/\varepsilon n)$.

# Histogram

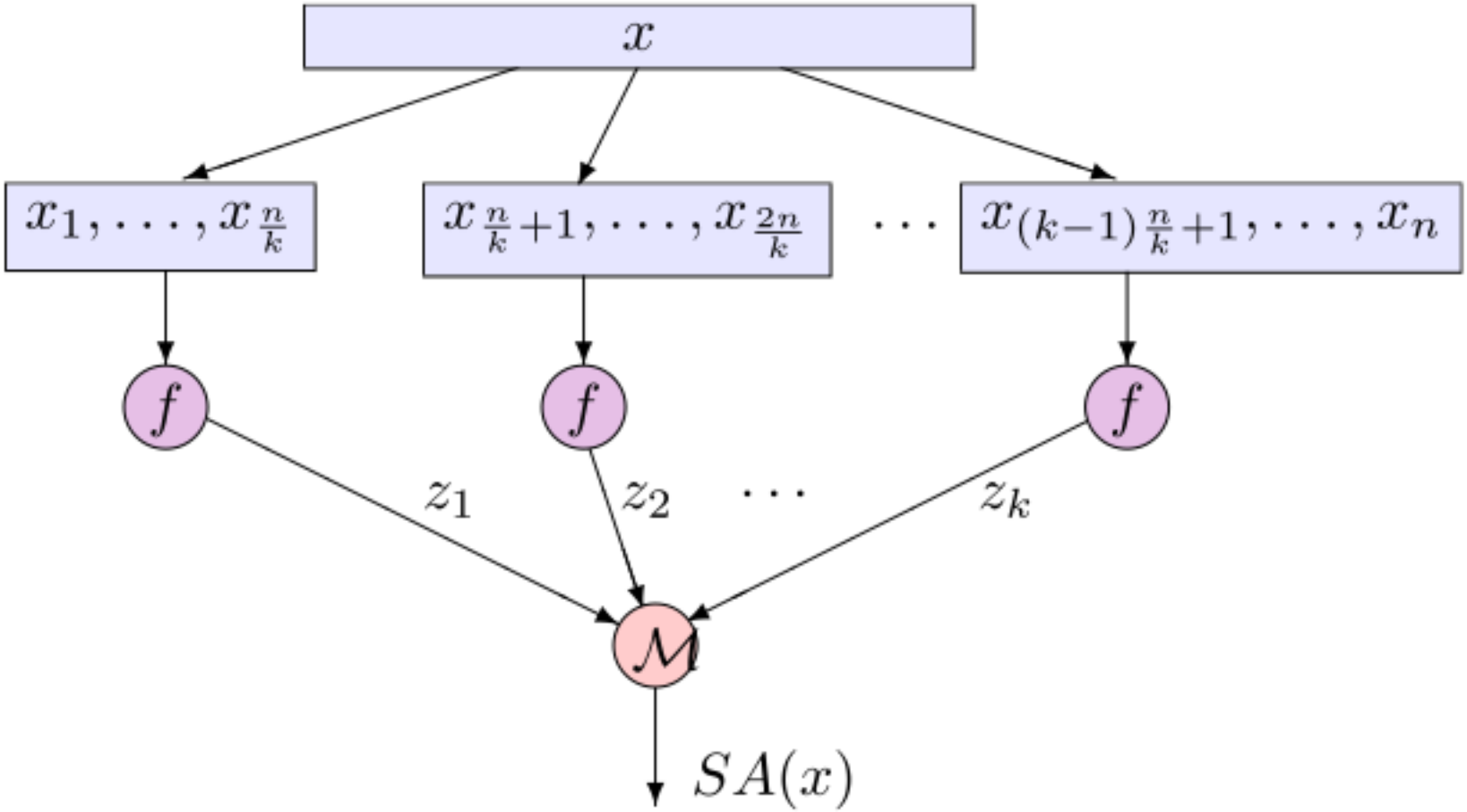
**Accuracy with the standard histogram DP algorithm:**

$$|q_h(D) - r_h| \leq O\left(\frac{log(|\mathcal{X}|)}{n}\right)$$

**Accuracy with the stable histogram DP algorithm:**

$$|q_h(D) - r_h| \leq O\left(\frac{log(1/\delta)}{n}\right)$$

# Sample and aggregate



# Privacy Amplification by subsampling



**Lemma 1.28** (Privacy amplification by subsampling)**.** Let $\mathcal{M} : \mathcal{X}^m \to \mathcal{R}$ be an $\epsilon$-differentially private mechanism for every $m \geq 1$. Let $\mathcal{S} : \mathcal{X}^n \to \mathcal{X}^{\gamma n}$ be a subsampling (without replacement) mechanism returning a i.i.d. subsample of the data points of size $\gamma n$, for $\gamma < 1$. Then, the mechanism $\mathcal{M}' = \mathcal{M} \circ \mathcal{S} : \mathcal{X}^n \to \mathcal{R}$ is $2\gamma(e^{\epsilon} - e^{-\epsilon})$-differentially private.