Privacidade Diferencial - Mecanismos

Prof. Javam Machado

LSBD/DC/UFC

Novembro/2019

Mecanismos

- Laplace
- Gaussiano
- Exponencial

Mecanismos dirigem a quantidade de ruído adicionado à resposta de uma consulta para garantir a privacidade
Mecanismos de Laplace e Gaussiano são ambos utilizados em consultas sobre valores numéricos
O mecanismo Exponencial é utilizado para consultas sobre valores categóricos

Laplace - Revisão

- Função de densidade probabilística (define o ruído)

$$Lap(x) = \frac{1}{2b}\exp\left(-\frac{|x|}{b}\right)$$

- Mecanismo de Laplace

$$M(x, f, \varepsilon) = f(x) + Lap(\Delta f/\varepsilon, 0)$$

  - $b > 0$ é o parâmetro de escala ou diversidade
  - Δf é a sensibilidade da função f
  - ε é o budget de privacidade

Privacidade Diferencial – Teorema da composição

Composição Sequencial

- Temos um *dataset* D e desejamos saber:
  - O valor médio de idades;
  - A quantidade de pessoas no dado;
  - ...
- Todas as perguntas passam por um mecanismo $\mathcal{M}$ que garante ε-PD;
- Nossas respostas estarão garantindo o ε-PD?

Composição Sequencial

- Temos um *dataset* D e desejamos saber:
  - O valor médio de idades;
  - A quantidade de pessoas no dado;
  - ...
- Todas as perguntas passam por um mecanismo $\mathcal{M}$ que garante ε-PD;
- Nossas respostas estarão garantindo o ε-PD?

Não!

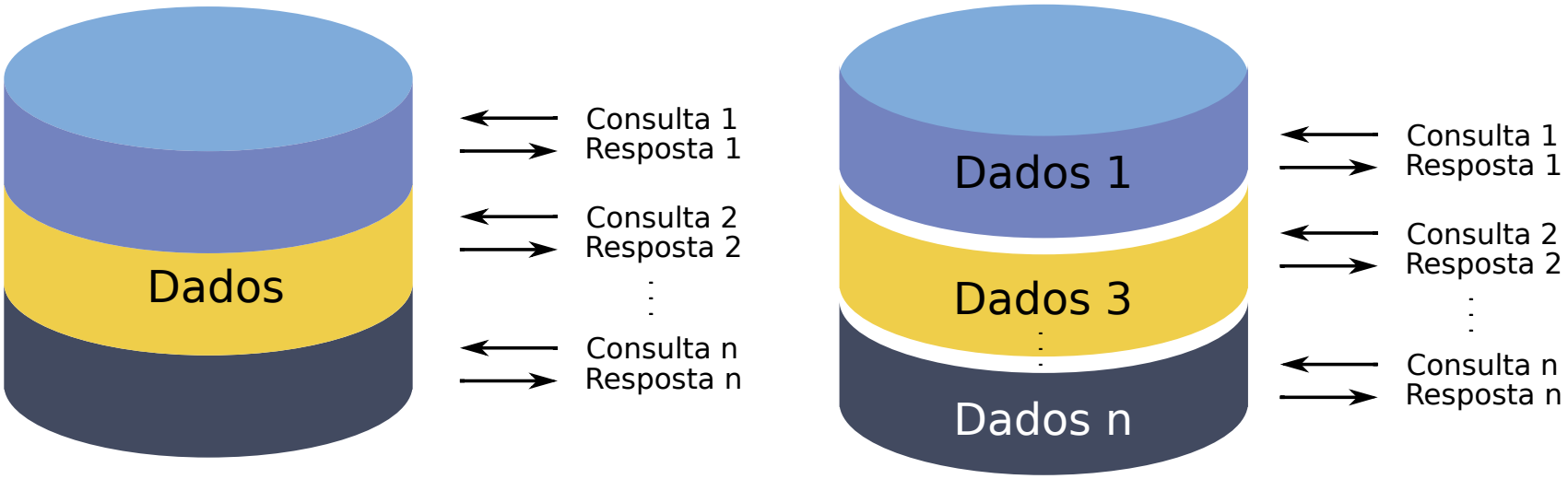
Composição Sequencial

- Acontece que se fizermos k perguntas, utilizando ε-PD, $Q = \{q_1, \ldots, q_k\}$:
  - Temos que a resposta final será $k\varepsilon$-PD, ou
  - Em caso de *budgets* diferentes: $\sum_{i=1}^{k} \varepsilon_i$-PD;

Composição Paralela

- Agora temos $Q = \{q_1, \ldots, q_k\}$ consultas utilizando ε-PD;
- Cada consulta $q_j \in Q$ tem um *budgets* atrelado ε_j;
- Cada consulta é aplicada nos conjuntos de dados disjuntos;
- Dataset D fragmentado em conjuntos disjuntos D_i;
- O resultado é $\max(\varepsilon_1, \ldots, \varepsilon_k)$-PD.

Composição



Sequencial

Paralela

- Sequencial: $\sum_{i=1}^{k} \varepsilon_i$-differential privacy;
- Paralela: $\max(\varepsilon_1, \ldots, \varepsilon_k)$-differential privacy.

Pós-processamento

- $\mathcal{M}_1$ é um algoritmo que satisfaz o ε-PD;
- Então $\mathcal{M}_2(\mathcal{M}_1(D))$ também satisfaz o ε-PD.

Mecanismo Exponencial

Mecanismo Exponencial

- Sabemos responder as consultas numéricas através do mecanismo de Laplace;
- Mas se quisermos consultas não numéricas:
  - i.e. “Qual a cor de cabelo mais comum na sala de aula?”
- Com o Mecanismo exponencial podemos responder a maioria das consultas numéricas ou não.

Mecanismo Exponencial

- Valor de entrada x;
- Conjunto de todas as saídas possíveis: $\mathcal{O}$;
- Função de qualidade (score) q, que mapeia uma entrada e saída a um score;
  - $q(x, o)$ é maior quanto melhor a saída o for para entrada x;
  - $o \in \mathcal{O}$;
  - Sensibilidade $\Delta q = S(q) = \max_{x,x',o} |q(x, o) - q(x', o)|$.

Mecanismo Exponencial

- Consulta: "Qual a cor de cabelo mais comum na sala de aula?";
- Possíveis saídas: $\mathcal{O} = \{\text{castanho}, \text{loiro}, \text{ruivo}\}$;
- Dataset: $D = \{$ (Joao, Cas.), (Maria, Rui.), (Pedro, Cas.) $\}$;
- O valor de $q(\text{Joao}, \text{Castanho})$ tem que ser maior que $q(\text{Joao}, \text{Ruivo})$ e $q(\text{Joao}, \text{Loiro})$.

Mecanismo Exponencial

- $Pr[\mathcal{M}_{exp}(x) = o] \propto \exp\left(\frac{\varepsilon q(x,o)}{2\Delta q}\right)$
- Valor exato da probabilidade:
  - $Pr[\mathcal{M}_{exp}(x) = o] = \frac{\exp\left(\frac{\varepsilon q(x,o)}{2\Delta q}\right)}{\sum_{o' \in \mathcal{O}} \exp\left(\frac{\varepsilon q(x,o')}{2\Delta q}\right)}$;
  - Processo feito através da normalização dos valores.

Mecanismo Exponencial

- Mecanismo utilizado para responder consultas não numéricas;
- É modelada como uma generalização de todos os mecanismos da PD;
- Eficiência é um problema.