Splošna definicija diferencirane zasebnosti

Metod Jazbec

Mentor: prof. dr. Aljoša Peperko

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Diplomski seminar, 2018

Kazalo vsebine I

Uvod - opis teme

- Doba podatkov. Kako podatke primerno zaščititi?
- Veliko neprimernih metod, potreba po strogi matematični definiciji zasebnosti.
- Diferencirana zasebnost, lepa teorija a neuporabna v praksi?
- Objavljanje in rudarjenje podatkov.

Uvod - opis teme

- ’American Health Care Records’ primer.

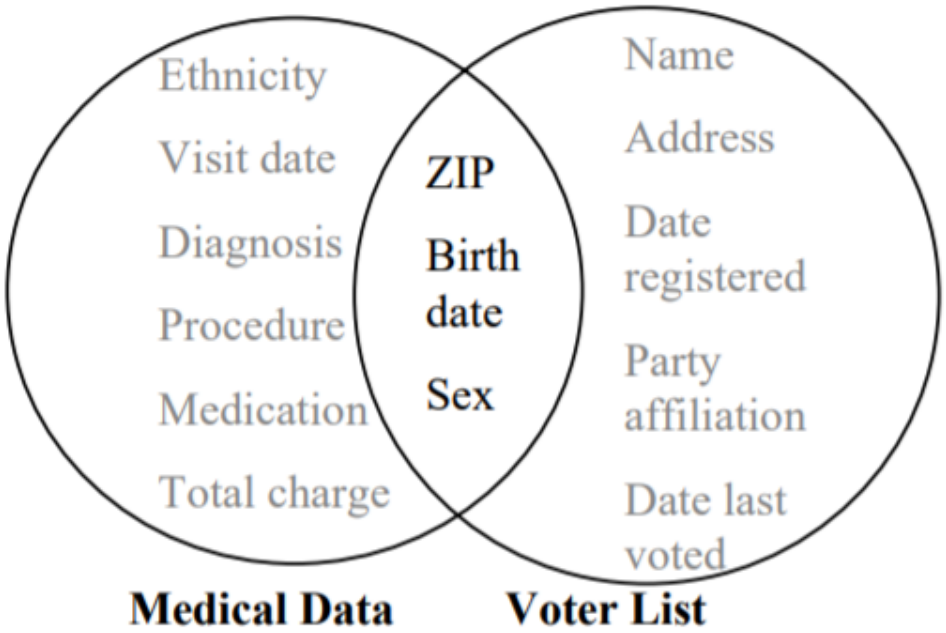

Figure 1: Metoda anonimizacije in napad s pomožno podatkovno bazo.

Uvod - opis teme

Pacient	Diabetes
Anja	1
Bojan	1
Cene	0
Darja	0
Edi	1

Table 1: Podatkovna baza z imeni pacientov in podatki o diabetesu.

- Apple primer (’data mining’).
- **Tema diplomskega dela:** splošen model zasebnosti, ki omogoča enotno obravnavo različnih vrst podatkov.

Monotoni razredi

Definicija (Monoton razred)

Monoton razred $\mathcal{M}$ je družina podmnožic Ω (torej $\mathcal{M} \subset \mathcal{P}(\mathcal{M})$) z naslednjima lastnostima:

- $\{A_i\}_{i=1,\ldots\infty} \in \mathcal{M}, A_i \subseteq A_{i+1} \Rightarrow \bigcup_{i=1,\ldots\infty} A_i \in \mathcal{M}$ (zaprtost za monotono naraščajoče števne unije),
- $\{A_i\}_{i=1,\ldots\infty} \in \mathcal{M}, A_i \supseteq A_{i+1} \Rightarrow \bigcap_{i=1,\ldots\infty} A_i \in \mathcal{M}$ (zaprtost za monotono padajoče števne preseke).

- Vsaka σ-algebra je monoton razred.

Monotoni razred

- Karakterizacija $\sigma(\mathcal{S})$ kot najmanjši monoton razred, ki vsebuje algebro $\mathcal{S}$.

Izrek (O monotonih razredih)

Naj bo $\mathcal{S}$ algebra in $\mathcal{M}$ monoton razred na množici Ω. Naj velja še $\mathcal{S} \subseteq \mathcal{M}$. Potem sledi $\sigma(\mathcal{S}) \subseteq \mathcal{M}$.

Osnovno o metričnih prostorih

Definicija (Kompaktnost metričnih prostorov)

Metrični prostor (D, ρ) je *kompakten*, če ima vsako zaporedje v D konvergetno podzaporedje z limito prav tako v D (povedano drugače, vsako zaporedje v D ima vsaj eno stekališče vsebovano v D).

- Ni najbolj splošna definicija kompaktnosti.
- $a, b \in D^n$, $\rho_H(a, b) :=$ # mest, na katerih se vektorja razlikujeta (Hammingova razdalja/metrika)
- D kompakten, $diam(D) := \max_{d,d' \in D} \rho(d, d')$

Splošni podatkovni model

(U, ρ) poljuben metrični prostor in $D \subseteq U$. Posamezni vnosi v opazovani podatkovni bazi so elementi množice D. Celotno bazo prikažemo z vektorjem $\mathbf{d} = (d_1, ..., d_n) \in D^n$, kjer $d_i \in D$ predstavlja i-ti vnos oz. vrstico.

- Množico U opremimo z Borelovo σ -algebro, označimo jo z $\mathcal{A}_U$.

Primeri različnih vrst podatkov

- **Kategorični podatki:** množica hobijev, $\mathcal{H} = \{nogomet, kitara, ...\}$, $D = 2^{\mathcal{H}}$, diskretna metrika
- **Numerični podatki:** RGB slike dimenzije $n \times m$, $D = \mathbb{R}^{n \times m \times 3}$, $\rho(A, B) = \sum_{i,j,k} |a_{i,j,k} - b_{i,j,k}|$, $\mathcal{A}_D = \{A_1 \times A_2 \times A_3 | A_1 \in \mathcal{B}(\mathbb{R}^n), A_2 \in \mathcal{B}(\mathbb{R}^m), A_3 \in \mathcal{B}(\mathbb{R}^3)\}$

Primeri različnih vrst podatkov

- **'Mešani' podatki:** zdravstevni podatki, $D = \{1, 2, ..., st.pacientov\} \times \{1, ..., 120\} \times \{M, Z\} \times \{Ljubljana, ...\} \times \{0, 1\}^n$, ρ in σ-algebra podobno kot zgoraj (one-hot encoding)
- **Funkcijski podatki:** merjenje porabe elektrike, $D = l_\infty$ ali $D = L_2([0, T])$, Banachovi prostori

Sosednje podatkovne baze

Pravimo da sta dve podatkovni bazi, **d**$= (a_1, ..., a_n)$ in **d'** $= (b_1, ..., b_n)$, *sosednji*, če se razlikujeta v natanko enem vnosu. Torej:

- obstaja $j \in \{1, ...n\}$, da velja $a_j \neq b_j$,
- za vsak $i \in \{1, ..., n\} \setminus j$ velja $a_i = b_i$.

Sosednji bazi označimo z **d** $\sim$ **d**´.

Poizvedba

- Poizvedba (query) je način pridobitve željenih informacij iz podatkovne baze (SQL ...).
- Metrični prostor vseh možnih odgovor (angl. set of all possible responses) na posamezno poizvedbo $(E_Q, \rho_Q, \mathcal{A}_Q)$
- Poizvedba merljiva funkcija $Q : U^n \to E_Q$, torej $Q^{-1}(A) \in \mathcal{A}_{U^n}$ za vsako $A \in \mathcal{A}_Q$.

Odzivni mehanizem

- Prehod iz determinističnih na probabilistične odgovore.
- $(\Omega, \mathcal{F}, \mathbb{P})$ verjetnostni prostor, $\mathbf{d} \in D^n$ opazovana podatkovna baza
- $\mathcal{Q}(n)$ množica (možnih oz. dovoljenih) poizvedb.

Odzivni mehanizem (za izbran nabor poizvedb $\mathcal{Q}(n)$) je definiran kot družina slučajnih spremenljivk

$$\{X_{Q,\mathbf{d}} : \Omega \to E_Q | Q \in \mathcal{Q}(n), \mathbf{d} \in D^n\}. \tag{1}$$

Perturbacija podatkovne baze

Potrebujemo družino merljivih preslikav (slučajnih vektorjev) $\{Y_{\mathbf{d}} : \Omega \to U^n | \mathbf{d} \in D^n\}$ Če taka družina obstaja, potem ima odzivni mehanizem obliko kompozituma.

$$X_{Q,\mathbf{d}} = Q \circ Y_{\mathbf{d}} \tag{2}$$

V praksi se ponavadi to izvede prek t. i. dodajanja šuma, torej $X_{\mathbf{d}} = \mathbf{d} + N$, kjer je N slučajni vektor z vrednostmi v U^n.

Perturbacija odgovorov na poizvedbo

Podana je poizvedba $Q : U^n \to E_Q$. V primeru da obstaja družina merljivih preslikav $\{Z_q : \Omega \to E_Q | q \in E_Q\}$, je odzivni mehanizem definiran kot

$$X_{Q,\mathbf{d}} = Z_{Q(\mathbf{d})} \tag{3}$$

Definicija diferencirane zasebnosti

Definicija (Diferencirana zasebnost za posamezno poizvedbo)

Naj bo $\epsilon > 0$ in $0 \leq \delta \leq 1$. Odzivni mehanizem je (ϵ, δ)-diferencirano zaseben za poizvedbo Q, če za vse $\mathbf{d} \sim \mathbf{d'} \in D^n$ in za vse $A \in \mathcal{A}_Q$ velja

$$\mathbb{P}(X_{Q,\mathbf{d}} \in A) \leq e^{\epsilon}\mathbb{P}(X_{Q,\mathbf{d'}} \in A) + \delta \tag{4}$$

- Simetričnost definicije!
- Zahtevnost testiranja.

Zadostne testne množice

Izrek 1

Naj bosta podana odzivni mehanizem (1) in poizvedba $(E_Q, \mathcal{A}_Q, Q)$. Naj bo $S \subset \mathcal{A}_Q$ algebra in naj velja $\sigma(\mathcal{S}) = \mathcal{A}_Q$. Če (4) velja za vse $A \in \mathcal{S}$, potem velja za vse $A \in \mathcal{A}_Q$.

Identična poizvedba

- Javna objava celotne podatkovne baze.
- $I_n : D^n \to D^n$, $I_n(\mathbf{d})=\mathbf{d}$

Izrek 2

Naj bo odzivni mehanizem s perturbacijo podatkovne baze (ϵ, δ)-diferencirano zaseben glede na identično poizvedbo $(U^n, \mathcal{A}_{U^n}, I_n)$. Potem sledi, da je tak mehanizem (ϵ, δ)-diferencirano zaseben glede na katerokoli poizvedbo $(E_Q, \mathcal{A}_Q, Q)$.

- Pomen tega tega, da v izreku ne postavimo nobenih omejitev na množico možnih odgovorov E_Q.

Perturbacija podatkovne baze po komponentah

Predpostavimo, da obstaja družina slučajnih spremenljivk (merljivih preslikav) oblike $\{Y_d : \Omega \to U | d \in D\}$. Potem za $\mathbf{d} = (d_1, ..., d_n)$ definiramo odzivni mehanizem $Y_{\mathbf{d}}$ kot

$$Y_{\mathbf{d}}(\omega) = (Y_{d_1}(\omega), ..., Y_{d_n}(\omega)), \tag{5}$$

kjer so Y_{d_i} med sabo neodvisne.

Poenostavitev na 1D baze

Izrek 3

Naj bo podana družina 1-dimenzionalnih diferencirano zasebnih mehanizmov $\{Y_d : \Omega \to U | d \in D\}$. Velja torej

$$\mathbb{P}(Y_d \in A) \leq e^{\epsilon}\mathbb{P}(Y_d \in A) + \delta$$

za vse $d, d' \in D, A \in \mathcal{A}_D$. Če definiramo n-dimenzionalni odzivni mehanizem kot (5), potem sledi, da je tudi ta diferencirano zaseben:

$$\mathbb{P}(Y_{\mathbf{d}} \in A) \leq e^{\epsilon}\mathbb{P}(Y_{\mathbf{d'}} \in A) + \delta$$

za vse $\mathbf{d} \sim \mathbf{d'} \in D^n, A \in D^n$.

- Uporaba na diskretnem metričnem prostoru.

- $D \subset \mathbb{R}$, kompakten.
- $L : \Omega \to \mathbb{R}$ Laplacovo porazdeljena slučajna spremenljivka s parametroma $(0, b), b > 0$. Verjetnostna gostota ima potem obliko $f(x) = \frac{1}{2b} e^{-\frac{|x|}{b}}$.
- Za vsak $d \in D$ potem definirajmo 1-dimenzionalni mehanizem kot $Y_d(\omega) = d + L(\omega)$.
- Parameter b izberimo tako da

$$b \geq \frac{diam(D)}{\epsilon - \log(1 - \delta)}.$$

Potem sledi, da je vsak n-dimenzionalen mehanizem oblike (5) (ϵ, δ) diferencirano zaseben za vsako n-dimenzionalno podatkovno bazo D^n in vsako poizvedbo.

Natančnost odzivnih mehanizmov

- $\rho(X_d, d)$ nenegativna slučajna spremenljivka.
- $\gamma := max_{d \in D} \mathbb{E}[\rho(X_d, d)]$. maksimalna pričakovana napaka danega mehanizma X_d.

Lema

Naj bo podana družina 1-dimenzionalnih diferencirano zasebnih mehanizmov $\{Y_d : \Omega \to U | d \in D\}$ (glej definicijo 1) in naj velja $0 \leq \delta < 1$. Potem sledi $\gamma > 0$.

Natančnost odzivnih mehanizmov

Izrek 4

Naj bo podana družina 1-dimenzionalnih diferencirano zasebnih mehanizmov $\{Y_d : \Omega \to U | d \in D\}$. Potem velja

$$\gamma \geq (1 - \delta)(\frac{diam(D)}{2(1 + e^{\epsilon})})$$

- (Ponovimo) **Neenakost Markova:** Naj bo X nenegativna slučajna spremenljivka in $a > 0$. Potem velja $\mathbb{P}(X \geq a) \leq \frac{\mathbb{E}(x)}{a}$.

Viri in literatura I

Naoise Holohan, Douglas J. Leith, Oliver Mason
Differential privacy in metric spaces: Numerical, categorical and functional data under the one roof
Information Sciences, Volume 305, 256-268, 2015.