

$$M: X^n \rightarrow T$$

~~XXXXXXXXXX~~

1. טל. סימולציה של אלגוריתם

אלגוריתם מיקום, אלגוריתם  $(\epsilon, \delta)$ -DP, הסווג,  $X, X'$ , הסווג בכניסה  
יחידה,  $S \subseteq T$ ,  $\delta$  מיקום  $\epsilon$ :

$$P_M [M(x) \in S] \leq e^\epsilon \cdot P_M [M(x') \in S] + \delta$$

ג. רעיון -  $f: X^n \rightarrow \mathbb{R}^d$  פונקציה הן הן פונקציה  $\epsilon$  והכנסה  
ההסתה  $f$  של קרובים. (global sensitivity)

$$GS_f = \max_{x, x' \in X^n} |f(x) - f(x')|$$

\* "גלובל" - סוג של תצורה יחיד

ג. מושג Laplace הוסף ל- $\epsilon$ -DP, צורה "ע" הוסף ל- $\epsilon$

$$\text{Lap} \left( \frac{GS_f}{\epsilon} \right)$$

מ  $f$  הוא הכול' שלו, ורעיון  $GS_f$ ,  $A$  הוא  $\epsilon$ -DP

$$A(x) = f(x) + \text{Lap} \left( \frac{GS_f}{\epsilon} \right)$$

הוכה שהמונח  $A(x)$  הוא  $(\epsilon, \delta)$ -DP

כדי לקבוע אם  $x, x'$  הם קרובים, הוסף ל- $\epsilon$  ההסתה

המונח  $A(x)$  הוא  $\epsilon$  מוק' של  $f(x)$   $z \in \mathbb{R}^d$  מוק' של  $f(x)$

$$A(x) = z : \epsilon$$

~~$P_x(z)$~~   
המונח  $A(x)$  הוא  $\epsilon$  מוק' של  $f(x)$   $z \in \mathbb{R}^d$  מוק' של  $f(x)$

$$f(x)_i + N_i = z_i$$
  
 $N_i \sim \text{Lap} \left( \frac{GS_f}{\epsilon} \right)$

$$\frac{P_x(z)}{P_y(z)} = \frac{\prod_{i=1}^d \frac{2\epsilon}{GS_f} \exp \left( -\frac{\epsilon \cdot |f(x)_i - z_i|}{GS_f} \right)}{\prod_{i=1}^d \frac{2\epsilon}{GS_f} \exp \left( -\frac{\epsilon \cdot |f(y)_i - z_i|}{GS_f} \right)}$$

דלתא



$$\frac{P_x(z)}{P_y(z)} = \prod_{i=1}^d \exp\left(\frac{\varepsilon \cdot (|f(y)_i - z_i| - |f(x)_i - z_i|)}{GSF}\right)$$

$$\leq \prod_{i=1}^d \exp\left(\frac{\varepsilon \cdot |f(y)_i - f(x)_i|}{GSF}\right)$$

$$= \exp\left(\varepsilon \cdot \frac{|f(y) - f(x)|}{GSF}\right)$$

עבור  $x, y$  נניח שההפרש בין  $f(x)$  ל- $f(y)$  הוא  $GSF$ ! כלומר  
 $|f(y) - f(x)| \leq GSF$

$$\leq \exp(\varepsilon) = e^\varepsilon$$

כלומר עבור  $z \in \mathbb{R}^d$  נניח  $x, y \in \mathbb{R}^d$  : נניח

$$\frac{P_x(z)}{P_y(z)} \leq e^\varepsilon$$

•  $\varepsilon$ -DD נניח  $\mu$



2. כל הנתון  $\sigma$  אינו  $x$  ברוב סיבתי :

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

insert(x):

$\forall 1 \leq i \leq k, S[h_i(x)] \leftarrow 1$

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

query(x):

return  $(S[h_1(x)] = 1) \&\& \dots \&\& (S[h_k(x)] = 1)$

False Negative (היה נכון ונחשב לא נכון) ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

False Positives (היה לא נכון ונחשב נכון) ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

$h_1(a) = 1, h_1(b) = 3, h_1(c) = 2$   
 $h_2(a) = 2, h_2(b) = 4, h_2(c) = 3$

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓

המפתח  $x$  הוא  $hash$  של  $x$  ונקרא "1" ✓



הוכחה,  $S$  היא קבוצת  $k$  איברים מ- $n$  איברים,  $(n)$

הוכחה  $S$  היא  $(n)$  איברים:

*הוכחה*

$$\binom{k}{m} \binom{k-1}{m-1} \dots \binom{1}{m-k+1} = k!$$

הוכחה על ידי אינדוקציה.

אם  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים,  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים,  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים.

אם  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים,  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים.

$$\binom{k}{m}^k$$

הוכחה על ידי אינדוקציה.

אם  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים,  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים.

$$\binom{k}{m}^k$$

הוכחה על ידי אינדוקציה.

אם  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים,  $S$  היא קבוצת  $k$  איברים,  $(n)$  איברים.

הוכחה על ידי אינדוקציה.

הוכחה על ידי אינדוקציה.

$$\left(1 - \frac{1}{m}\right)^{k \cdot m} = \left(1 - \frac{1}{m}\right)^k$$

הוכחה על ידי אינדוקציה.

$$\left(1 - \left(1 - \frac{1}{m}\right)^k\right)^k$$

הוכחה על ידי אינדוקציה.

הוכחה על ידי אינדוקציה.

הוכחה על ידי אינדוקציה.

הוכחה על ידי אינדוקציה.

$$\frac{1}{\binom{m}{k}}$$

הוכחה על ידי אינדוקציה.



$(v_1, 0), (v_2, 1), (v_3, 2), (v_4, 4), (v_5, 6), (v_6, 7), (v_7, 8)$

$ADS_2(v_1) = \{(v_1, 0), (v_2, 1), (v_4, 4), (v_6, 7)\}$

~~$ADS_2(v_1) = \{(v_1, 0.74), (v_2, 0.53), (v_4, 0.37), (v_6, 0.23)\}$~~

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )  
הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )  
כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ .

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )  
 $\sum_{i \in ADS(v)} \hat{I}_{i,v} = 0$

$p_{i,v} = k^{+k} \{h(j) \mid j \in ADS(v), d(j,v) < d(i,v)\}$ ,  $\hat{I}_{i,v} = \frac{1}{p_{i,v}}$

$\hat{p}_{i,v} = \min\{1, p_{i,v}\}$

Inverse Prob. של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )

$p_e = k^{+k} \{h(j) \mid d(j,v) < d(i,v)\} = k^{+k} \{h(j) \mid j \in ADS(v), d(j,v) < d(i,v)\}$

הסתברות  $v_i$  של  $v_i$  (כאשר  $v_i$  הוא המרחק בין  $v_i$  ל- $v_1$ )  
 $E[\hat{I}_{i,v}] = \frac{1}{p_i} \cdot p_i + (1-p_i) \cdot 0 = 1$



$$\hat{I}_{v_1, v_1} = \frac{1}{1} = 1$$

$$\hat{I}_{v_1, v_2} = \frac{1}{1} = 1$$

$$\hat{I}_{v_1, v_3} = 0$$

$$\hat{I}_{v_1, v_u} = \frac{1}{0.7u}$$

$$\frac{.3}{.3} = 1$$

$$\hat{I}_{v_1, v_1} + \hat{I}_{v_1, v_2} + \hat{I}_{v_1, v_3} + \hat{I}_{v_1, v_u} = 2 + \frac{1}{0.7u}$$

$\Rightarrow$  אולי אפשר  $\alpha(d_{ij})$  או אולי  $\alpha(d_{ij})$

$$\alpha(d_{ij}) = \begin{cases} 1 & d_{ij} \leq 4 \\ 0 & \text{אחרת} \end{cases}$$

אולי אפשר  $\alpha(d_{ij})$  או אולי  $\alpha(d_{ij})$

$$\sum_{d_{ij} \leq 4} = \hat{I}_{v_1, v_1} \cdot \alpha(d_{v_1, v_1}) + \hat{I}_{v_1, v_2} \cdot \alpha(d_{v_1, v_2}) + \hat{I}_{v_1, v_u} \cdot \alpha(d_{v_1, v_u})$$

$$+ \hat{I}_{v_1, v_3} \cdot \alpha(d_{v_1, v_3})$$

$$= 1 \cdot 1 + 1 \cdot 1 + 1 \cdot \frac{1}{0.7u} + 0 \cdot \frac{1}{0.53}$$