

Lecture 7: Histograms & Continual observation

Textbook: Cynthia Dwork and Aaron Roth. The
Algorithmic Foundations of Differential Privacy

מרצה: אורי שטמר

ניזכר בבעיית חישוב היסטוגרמות:

קלט: דטהבייס $S = (x_1, \dots, x_n) \in D^n$ עבור דומיין כלשהו D .

משימה: לכל איבר דומיין $d \in D$ צריך לחשב הערכה למספר המופעים של d בדטהבייס S .
כלומר, לכל $d \in D$ אנחנו רוצים לחשב ספירה $|\{i : x_i = d\}|$. $\hat{c}(d) \approx \text{count}_S(d)$.
*** כמוכן שאנחנו רוצים לחשב זאת תוך כדי הבטחת פרטיות...**

הגדרה: נגדיר את השגיאה של אוסף של תשובות $\hat{c}(\cdot)$ בתור

$$\text{error}_S(\hat{c}) = \max_{d \in D} |\hat{c}(d) - \text{count}_S(d)|$$

אנחנו כבר מכירים כמה פתרון מסוים לבעיה הזאת:

בעצם הפונקציה שאנחנו מעוניינים לחשב כאן היא:

$$f(S) = (\text{count}_S(d_1), \text{count}_S(d_2), \dots, \text{count}_S(d_{|D|})) \in \mathbb{R}^{|D|}$$

וכפי שראינו בתחילת הקורס, הרגישות הגלובלית של הפונקציה הזאת היא 2 ולכן כדי להחזיר קירוב פרטי לזוקטור הזה מספיק לנו להוסיף לכל קואור' רעש $\text{Lap}(\frac{2}{\epsilon})$.

אנחנו דוגמים בסה"כ $|D|$ רעשים מתוך $\text{Lap}(\frac{2}{\epsilon})$. לפי התכונות של התפלגות לפלאס, בהסתברות לפחות $1 - \beta$, אף אחד מהרעשים האלה לא יהיה גדול מ $\frac{2}{\epsilon} \log(\frac{|D|}{\beta})$ בערך מוחלט, ולכן זה חוסם את השגיאה של האלגוריתם שלנו. זה מצויין כאשר הדומיין D הוא לא יותר מדי גדול. אבל פחות מצויין כאשר D ממש ענק.

פתרון נוסף:**Algorithm SbH**

קלט: דטהבייס $S \in D^n$

(1) לכל איבר דומיין $d \in D$ בצע:

(א) אם $\text{count}_S(d) = 0$ אזי קבע $\hat{c}(d) = 0$

(ב) אם $\text{count}_S(d) > 0$ אזי

i. חשב $\hat{c}(d) \leftarrow \text{count}_S(d) + \text{Lap}(\frac{2}{\epsilon})$

ii. אם $\hat{c}(d) < \frac{2}{\epsilon} \ln(\frac{2}{\delta}) + 1$ אזי קבע $\hat{c}(d) \leftarrow 0$

(2) החזר את ההערכות $\hat{c}(\cdot)$, נניח מעוגלות למספרים שלמים לשם פשטות.

כלומר, האלגוריתם הזה דומה לאלגוריתם שאנחנו כבר מכירים – זה שמוסיף רעש לפלאסי לכל הספירות – חוץ מזה שאנחנו לא מרעישים ספירות שהן אפס ואנחנו מאפסים את כל הספירות הרועשות "הקטנות".

ניתוח השגיאה:

אנחנו מחזירים תשובות מדויקות לכל הספירות שאמורות להיות אפס. מכיוון שהדטהבייס הוא בגודל n , אז ייתכנו לכל היותר n ספירות שונות מאפס. כלומר לאורך כל הריצה אנחנו דוגמים לכל היותר n רעשים מהתפלגות $\text{Lap}\left(\frac{2}{\varepsilon}\right)$. לפי התכונות של התפלגות לפלס, בהסתברות לפחות $1 - \beta$ מתקיים שכל הרעשים האלה (בערך מוחלט) הם לכל היותר $\frac{2}{\varepsilon} \log\left(\frac{n}{\beta}\right)$. בנוסף, אנחנו מאפסים את כל הספירות הרועשות הקטנות, מה שיכול להגדיל את השגיאה לכל היותר $1 + \frac{2}{\varepsilon} \ln\left(\frac{2}{\delta}\right)$. סה"כ השגיאה שלנו היא לכל היותר $O\left(\frac{1}{\varepsilon} \ln\frac{1}{\delta}\right)$.

ניתוח פרטיות (קודם נראה סקיצה של הרעיון ואח"כ נפרמל):

נקבע זוג דטהבייסים שכנים S, S' כך ש- $S' = S \cup \{x'_i\}$. נזכור שהאלגוריתם מחזיר הערכה $\hat{c}(d)$ לכל איבר דומיין $d \in D$ ונשים לב שכאשר אנחנו מריצים את SbH על S ועל S' אז כל התשובות $\hat{c}(d)$ מתפלגות בדיוק אותו דבר, חוץ מהתשובה $\hat{c}(x'_i)$.

אנחנו יודעים ש $\text{count}_{S'}(x'_i) > 0$.

אם בנוסף גם מתקיים ש $\text{count}_S(x'_i) > 0$ אזי הערך של $\hat{c}(x'_i)$ מקיים פ"ד לפי התכונות של המ.לפלאס מכיוון שבשלב i אנחנו מוסיפים רעש לפלאסי מתאים. (שלב i בו i לאחר מכן, אם קורה בו משהו, זה כבר רק *postprocessing*).

אם לעומת זאת מתקיים ש $\text{count}_S(x'_i) = 0$ אזי אנחנו יודעים שבריצה על S נקבל ש $\hat{c}(x'_i) = 0$ (כלומר בהסתברות 1). בגלל ש S, S' הם שכנים, במקרה זה אנחנו יודעים ש $\text{count}_{S'}(x'_i) = 1$ ולכן ההסתברות שלא נאפס את הספירה הזאת בשלב i היא לכל היותר $\frac{\delta}{2}$ לפי התכונות של התפלגות לפלאס.

כלומר, בכל מקרה, החישוב של $\hat{c}(x'_i)$ מתפלג כמעט אותו דבר בין שתי הריצות (עד כדי ε, δ). מכיוון ששאר התשובות מתפלגות בדיוק אותו הדבר בשתי הריצות, סה"כ אנחנו מקבלים שהאלגוריתם משמר פ"ד כנדרש.

ניתוח הפרטיות (יותר פורמלי):

נקבע זוג דטהבייסים שכנים S, S' כך ש- $S' = S \cup \{x'_i\}$ ונקבע מאורע $F \subseteq \mathbb{N}^{|D|}$. נניח לשם פשטות כי $x'_i = 1$.

ננתח עכשיו את המקרה המעניין יותר שבו $\text{count}_S(1) = 0$ & $\text{count}_{S'}(1) = 1$

נפצל את הקבוצה F באופן הבא:

$$F_0 = \{f \in F : f_1 = 0\} \quad \& \quad F_1 = \{f \in F : f_1 > 0\}$$

אבחנה 1:

$$\Pr[\mathcal{A}(S') \in F_1] \leq \delta \quad \& \quad \Pr[\mathcal{A}(S) \in F_1] = 0$$

נחשב:

$$\Pr[\mathcal{A}(S') \in F] = \Pr[\mathcal{A}(S') \in F_1] + \Pr[\mathcal{A}(S') \in F_0] \leq \delta + \Pr[\mathcal{A}(S') \in F_0]$$

$$= \delta + \Pr[\hat{c}_{S'}(1) = 0] \cdot \Pr[\mathcal{A}(S') \in F_0 \mid \hat{c}_{S'}(1) = 0] = ((1))$$

נסמן $\widetilde{F}_0 = \{(c_2, c_3, \dots, c_{|D|}) : (0, c_2, c_3, \dots, c_{|D|}) \in F_0\}$ ונסמן ב $\mathcal{A}(S')_{[2,|D|]}$ את אוסף התשובות עבור איברים $2, 3, \dots, |D|$ שמתקבלות מהרצת $\mathcal{A}(S')$ אזי

$$\begin{aligned} ((1)) &= \delta + \underbrace{\Pr[\hat{c}_{S'}(1) = 0]}_{\leq 1 = \Pr[\hat{c}_S(1) = 0]} \cdot \underbrace{\Pr[\mathcal{A}(S')_{[2,|D|]} \in \widetilde{F}_0]}_{= \Pr[\mathcal{A}(S)_{[2,|D|]} \in \widetilde{F}_0]} \\ &\leq \delta + \Pr[\hat{c}_S(1) = 0] \cdot \Pr[\mathcal{A}(S)_{[2,|D|]} \in \widetilde{F}_0] \\ &= \delta + \Pr[\hat{c}_S(1) = 0] \cdot \Pr[\mathcal{A}(S) \in F_0 \mid \hat{c}_S(1) = 0] \\ &= \delta + \Pr[\mathcal{A}(S) \in F] \end{aligned}$$

ננתח עכשיו את המקרה השני שבו $\text{count}_{S'}(1) > 0$ & $\text{count}_S(1) > 0$.

נגדיר:

$$G_1 = \{c_1 : \exists (c_2, \dots, c_{|D|}) \text{ such that } (c_1, \dots, c_{|D|}) \in F\}$$

ולכל $g \in G_1$ נגדיר

$$G^g = \{(c_2, \dots, c_{|D|}) : (g, c_2, \dots, c_{|D|}) \in F\}$$

נחשב:

$$\begin{aligned} \Pr[\mathcal{A}(S') \in F] &= \sum_{g \in G_1} \Pr[\hat{c}_{S'}(1) = g] \cdot \Pr[\mathcal{A}(S') \in F \mid \hat{c}_{S'}(1) = g] \\ &= \sum_{g \in G_1} \Pr[\hat{c}_{S'}(1) = g] \cdot \Pr[\mathcal{A}(S')_{[2,|D|]} \in G^g] \\ &= \sum_{g \in G_1} \Pr[\hat{c}_{S'}(1) = g] \cdot \Pr[\mathcal{A}(S)_{[2,|D|]} \in G^g] \\ &\leq \sum_{g \in G_1} e^\epsilon \cdot \Pr[\hat{c}_S(1) = g] \cdot \Pr[\mathcal{A}(S)_{[2,|D|]} \in G^g] \\ &= e^\epsilon \cdot \Pr[\mathcal{A}(S) \in F] \end{aligned}$$

הערה 1: בניתוח הפרטיות הנ"ל דיברנו על שני דטהבייסיים שכנים כך ש S' מתקבל כתוצאה מהוספת איבר ל S . איך שהגדרנו פ"ד, אנחנו צריכים להתחשב על שינוי של איבר ולא רק על הסרה/הוספה של איבר. אפשר לתקן את אנליזת הפרטיות בקלות.

הערה 2: ההגדרה של פ"ד ביחס להסרה/הוספה של איבר היא לא סימטרית ולכן צריך לנתח שני כיוונים באנליזה (מה שלא עשינו בהוכחה האחרונה...)

שאלה: האלג' הנ"ל משמר (ϵ, δ) -פרטיות ולא $(\epsilon, 0)$ -פרטיות. האם זה הכרחי?

נראה תוצאת אי-אפשרות שאומרת שעבור $(\epsilon, 0)$ -פרטיות, שגיאה מסדר גודל של $\log|D|$ היא הכרחית.

משפט: לכל אלגוריתם $(\epsilon=1, \delta=0)$ -פרטי לבעיית ההיסטוגרמות יש שגיאה $\Omega(\log|D|)$.

הוכחה:

נניח בשלילה שיש אלגוריתם פרטי \mathcal{A} לבעיית ההיסטוגרמות כך שבהסתברות לפחות $2/3$ מתקיים שכל הספירות שהוא מחזיר מדויקות עד כדי טעות $\frac{\log|D|}{16}$ לכל היותר.

נבנה אוסף של קלטים עבור האלגוריתם:

- עבור כל $d \in D$ נסמון ב S_d את הדטהבייס שמכיל $\frac{\log|D|}{4}$ עותקים של האיבר d ובנוסף מכיל $(n - \frac{\log|D|}{4})$ עותקים של איזשהו איבר שרירותי $\perp \in D$. כלומר,

$$S_d = \left(\underbrace{d, d, \dots, d}_{\frac{\log|D|}{4} \text{ copies}}, \underbrace{\perp, \perp, \dots, \perp}_{n - \frac{\log|D|}{4} \text{ copies}} \right) \in D^n$$

כעת נשים לב כי לכל $d \in D$ מתקיים

$$\text{count}_{S_d}(d) = \frac{\log|D|}{4}$$

ולכל $e \in D \setminus \{d, \perp\}$ מתקיים

$$\text{count}_{S_d}(e) = 0$$

מכיוון שהנחנו שלא אלגוריתם שלנו יש שגיאה לכל היותר $\frac{\log|D|}{16}$ אנחנו יודעים שאם נריץ אותו על דטהבייס קלט S_d אז ההערכה $\hat{c}(d)$ חייבת להיות לפחות $\frac{3\log|D|}{16}$ ולכל $e \in D \setminus \{d, \perp\}$ ההערכה $\hat{c}(e)$ חייבת להיות לכל היותר $\frac{\log|D|}{16}$.

בפרט, אם אוסף הערכות \hat{c} הוא "טוב" עבור קלט S_d כלשהו, אז הוא לא אוסף הערכות טוב לאף דטהבייס אחר S_e עבור $e \in D \setminus \{d, \perp\}$.

נזכור שהנחנו שאלגוריתם \mathcal{A} מצליח בהסתברות לפחות $2/3$ ושהוא מקיים $(\epsilon, 0)$ -פ"ד. לכן, לכל $d \neq e \in D$ אנחנו מקבלים

$$\frac{2}{3} \leq \Pr \left[\begin{array}{l} \mathcal{A}(S_d) \text{ מחזיר} \\ \text{תשובה טובה} \\ S_d \text{ עבור} \end{array} \right] \leq e^{2\epsilon \frac{\log|D|}{4}} \cdot \Pr \left[\begin{array}{l} \mathcal{A}(S_e) \text{ מחזיר} \\ \text{תשובה טובה} \\ S_d \text{ עבור} \end{array} \right] = \sqrt{|D|} \cdot \Pr \left[\begin{array}{l} \mathcal{A}(S_e) \text{ מחזיר} \\ \text{תשובה טובה} \\ S_d \text{ עבור} \end{array} \right]$$

ולכן

$$\frac{2}{3\sqrt{|D|}} \leq \Pr \left[\begin{array}{l} \mathcal{A}(S_e) \text{ מחזיר} \\ \text{תשובה טובה} \\ S_d \text{ עבור} \end{array} \right]$$

כלומר, כשאנחנו מריצים את \mathcal{A} על קלט S_e , אז בהסתברות לפחות $\frac{2}{3\sqrt{|D|}}$ הוא מחזיר תשובה שטובה בכלל לדטהבייס אחר S_d , וזה נכון לכל $e \neq d$.
 לכן,

$$\Pr \left[\begin{array}{l} \mathcal{A}(S_e) \text{ נכשל} \\ \text{ולא מחזיר תשובה} \\ S_e \text{ עבור } \end{array} \right] \geq \Pr \left[\bigcup_{d \in (D \setminus \{e, 1\})} \left\{ \begin{array}{l} \text{מחזיר } \mathcal{A}(S_e) \\ \text{תשובה טובה} \\ \text{עבור } S_d \end{array} \right\} \right] \stackrel{\substack{\text{מאורעות} \\ \text{זרים}}}{=} \sum_{d \in (D \setminus \{e, 1\})} \Pr \left[\begin{array}{l} \text{מחזיר } \mathcal{A}(S_e) \\ \text{תשובה טובה} \\ \text{עבור } S_d \end{array} \right] \geq \frac{(|D| - 2) \cdot 2}{3\sqrt{|D|}} > 1$$

סתירה.

Privacy under continual observation

עד היום בקורס דיברנו על המקרה בו הדטה היה סטטי, במובן הזה שהמטרה שלנו הייתה לנתח איזשהו דטהבייס (אולי מבוזר) שנקבע מראש. לפעמים השאלות שרצינו לענות עליהם נבחרו בצורה אדפטיבית, אבל הדטה תמיד היה קבוע מראש.

היום נשנה קצת את הסיפור וננסה להבין מה אנחנו יכולים להגיד כאשר הדטה משתנה לאורך זמן. נתרכז בבעיה הבאה:

נניח שאנחנו רוצים לתחזק מונה של מספר המתחסנים נגד קורונה בישראל ונניח שאנחנו רוצים שהמונה הזה יבטיח פרטיות דפרנציאלית.

הגדרה פורמלית של בעיית המונה:

- התנאים: בכל יום $1 \leq t \leq T$ אנחנו מקבלים קלט $x_t \in \mathbb{N} \cup \{0\}$ ולאחר מכן צריכים להחזיר פלט c_t
- דרישת נכונות: בכל יום $1 \leq t \leq T$ מתקיים $c_t \approx \sum_{i=1}^t x_i$
- דרישת פרטיות: איך נגדיר??

נזכר במשמעות של ההגדרה של פ"ד במקרה הרגיל, כלומר במקרה של אלגוריתם \mathcal{A} המתנה דטהבייס S :
 אמרנו שאלגוריתם \mathcal{A} כזה מקיים פרטיות דפרנציאלית אם לכל שני דטהבייסים שכנים S, S' השונים בשורה אחת, מתקיים שהתפלגות הפלטים של $\mathcal{A}(S)$ ושל $\mathcal{A}(S')$ הן דומות. המשמעות של זה היא שאפילו אם יריב מכיר את כל השורות ב S , חוץ מאת השורה שלי, ואז אותו יריב רואה את הפלט של האלגוריתם, אז עדיין היריב הזה "לא יכול ללמוד כמעט שום דבר" על השורה שלי, כי מנקודת המבט שלו, לא משנה מה היה רשום בשורה שלי – הפלט של האלגוריתם עדיין היה מתפלג כמעט אותו דבר.

אז עכשיו אנחנו רוצים להתאים את ההגדרה של פ"ד לסיפור שלנו כאשר אין לנו את כל הדטה מראש.

- עדיין אנחנו רוצים להניח שהיריב רואה את תוצאת החישוב. במקרה שלנו ז"א שהיריב רואה את c_1, c_2, \dots, c_T , כלומר רואה את המונה שאנחנו מתחזקים לאורך כל תהליך החישוב.
- עדיין אנחנו רוצים להניח שהיריב מכיר את הדטה של כולם חוץ משלי. מה זה אומר? אני יכול להשפיע על הקלט x_t באחד הימים ובאותו יום אני יכול לשנות את x_t בבדיוק אחד (אם אני מתחסן או לא). מעבר לזה, היריב מכיר את כל שאר הספירות.

הגדרת פרטיות עבור הסיפור שלנו:

- שתי סדרות קלט $\vec{x} = (x_1, \dots, x_T)$ ו- $\vec{x}' = (x'_1, \dots, x'_T)$ יקראו שכנות אם קיים $t \in [T]$ עבורו $|x_t - x'_t| \leq 1$ ובנוסף לכל $i \neq t$ מתקיים $x_i = x'_i$.
- אלגוריתם \mathcal{A} לבעיית המונה מקיים (ϵ, δ) -פרטיות אם לכל קביעה של שתי סדרות קלט שכנות \vec{x}, \vec{x}' ולכל מאורע $F \subseteq \mathbb{R}^T$ מתקיים
$$\Pr[\mathcal{A}(\vec{x}) \in F] \leq e^\epsilon \cdot \Pr[\mathcal{A}(\vec{x}') \in F] + \delta$$

נסיגות נאיביים לאלגוריתמים פרטיים לבעיית המונה:

$$(1) \quad \text{בכל יום } t \text{ נחשב } \hat{x}_t \leftarrow x_t + \text{Lap}\left(\frac{1}{\epsilon}\right) \text{ ונפרסם את } \hat{x}_t \text{ ונפרסם את } c_t \leftarrow c_{t-1} + \hat{x}_t.$$

כלומר, בכל יום אנחנו מרעישים את הספירה היומית ומוסיפים את הערך הרועש הזה למונה שאנחנו מתחזקים. העניין כאן הוא שלאורך הזמן הרעשים מצטברים לנו. בסה"כ יהיה לנו סכום של T רעשים שיצטבר למשהו מסדר גודל של $\frac{\sqrt{T}}{\epsilon}$.

$$(2) \quad \text{בכל יום } t \text{ נחשב ונפרסם את } c_t \leftarrow (\sum_{i=1}^t x_i) + \text{Lap}(b) \text{ עבור } b \approx \sqrt{T}$$

כלומר, בכל יום אנחנו מחשבים מחדש הערכה רועשת למונה שלנו. הבעייה כאן היא שקלטים שניתנים בתחילת החישוב משפיעים על כל המשך החישוב. למשל, הקלט x_1 משפיע על T סכומים רועשים כאלה. לכן, מקומפוזיציה, כדי שהאלגוריתם כולו ישמר פ"ד נצטרך להוסיף רעשים מסדר גודל $\frac{\sqrt{T}}{\epsilon}$.

כלומר, בשני הרעיונות הנאיביים האלה, השגיאה שלנו נראית כמו $\frac{\sqrt{T}}{\epsilon}$.

האם אפשר לעשות משהו יותר טוב? אנחנו נראה עכשיו אלגוריתם עם שגיאה $\frac{\text{polylog}(T)}{\epsilon}$

הרעיון:

נשים לב: גם בניסיון (1) וגם בניסיון (2) היו לנו בסה"כ T ספירות רועשות. בניסיון (1) כל משתמש השפיע רק על ספירה אחת, אבל כדי לחשב הערכה למונה נאצלנו לסכום $O(T)$ הערכות רועשות ולכן השגיאות הצטברו. בניסיון (2) הערכה לסכום תמיד מתקבלת מחישוב רועש אחד, אבל הבעייה היא שמשמש בודד יכול להשפיע על $O(T)$ חישובים ולכן נאלצנו להגדיל מאוד את כמות הרעש.

האם נוכל לעשות איזושהי "פשרה" בין שני הניסיונות האלה?

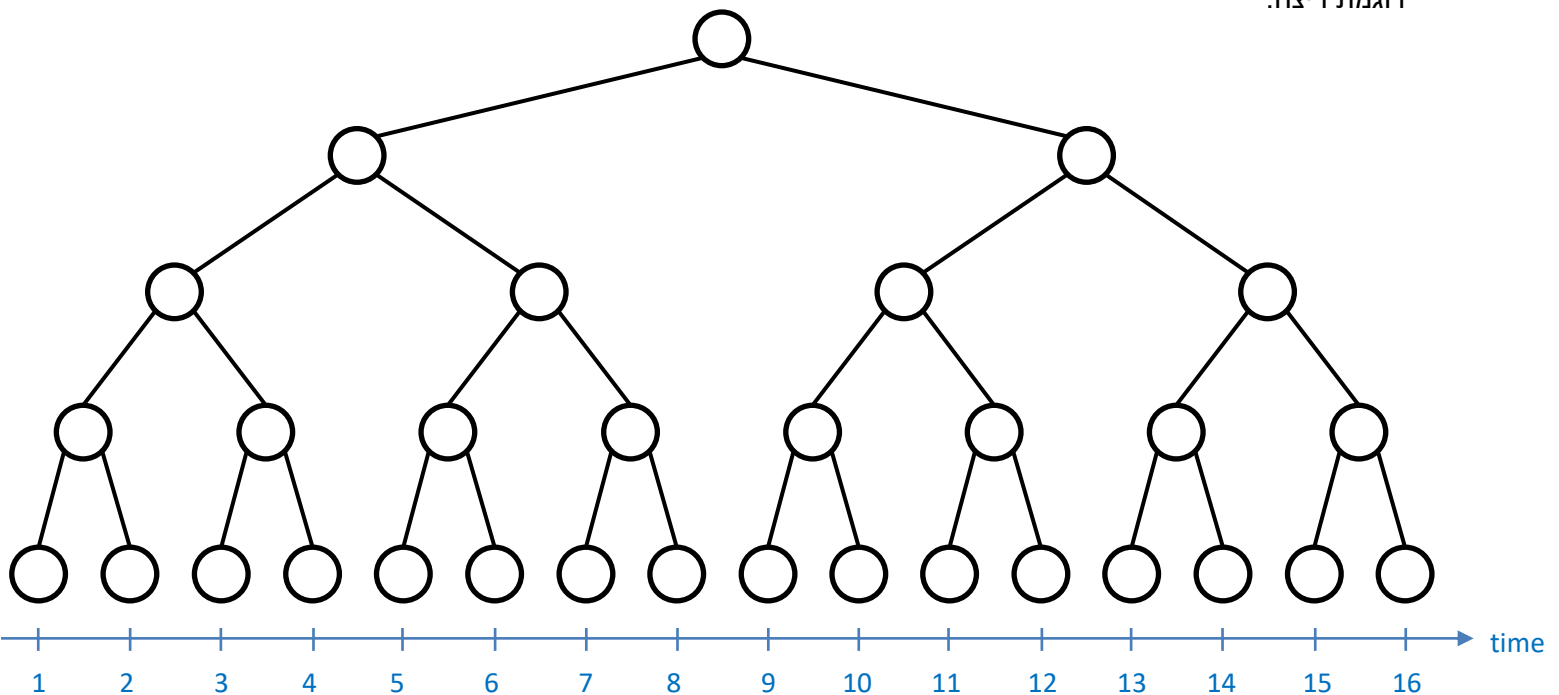
אנחנו נראה עכשיו אלגוריתם שבו יהיו לנו בסה"כ $2T$ ספירות רועשות, עם התכונות הבאות:

- כל משתמש משפיע רק על $O(\log T)$ מתוך הספירות האלה, ולכן יספיק לנו להוסיף רעש מסדר גודל $O\left(\frac{\log T}{\epsilon}\right)$ לכל ספירה.
- בכל שלב נוכל לחשב הערכה למונה ע"י סכימה של $O(\log T)$ ספירות רועשות, ולכן השגיאה לא תצטבר יותר מדי.

האלגוריתם:

1. נגדיר עץ בינארי מעל ציר הזמן, כאשר העלים של העץ מתאימים לימים $\{1, 2, 3, 4, \dots, T\}$ (אנחנו מניחים כאן ש- T הוא חזקה של 2)
2. בכל קודקוד בעץ, כולל בעלים, נשים רעש ב"ת שנדגום מ $\text{Lap}\left(\frac{\log T}{\epsilon}\right)$
3. ביום t , כאשר אנחנו מקבלים קלט $x_t \in \mathbb{N} \cup \{0\}$, נוסיף את x_t לכל אחד מהקודקודים בעץ שנמצאים במסלול מהעלה של t ועד לשורש
4. כאשר תת עץ מסויים "מתמלא" נפרסם את תוכן הקודקוד שנמצא בשורש תת העץ הזה. (תת העץ המושרש בקודקוד u מתמלא בזמן t שהוא האינדקס הגדול ביותר של עלה ששייך לתת העץ המושרש בקודקוד u)

דוגמת ריצה:



ניתוח פרטיות (סקיצה):

ראשית נשים לב שברגע שתת עץ מסויים מתמלא, אז השורש של תת העץ הזה לא מתעדכן יותר לאורך הריצה. מכיוון שאנחנו מפרסמים ערכים בקודקודים רק לאחר שתת העץ שלהם התמלא, אנחנו חושפים את הערך המורעש שנמצא בכל קודקוד בדייק פעם אחת לאורך הריצה. (כלומר, לא יתכן מצב שבו נפרסם ערך מורעש לקודקוד מסויים ולאחר מכן נפרסם עוד ערך לאותו קודקוד)

לכן, כל קודקוד מורעש כזה הוא כמו הפעלה אחת של המ.לפלאס.

שינויי של המידע של אדם אחד משפיע רק על קלט x_t ברגע t אחד בריצה (והשינויי ב x_t הוא ב- ± 1 בלבד). שינויי זה משפיע על $\log T$ הקודקודים במסלול מהעלה t ועד לשורש העץ. לכן, לפי קומפוזיציה, רעש מסדר גודל $\frac{\log T}{\epsilon}$ בכל קודקוד מספיק כדי להבטיח שהאלגוריתם משמר $(\epsilon, 0)$ -פ"ד.

ניתוח השגיאה (סקיצה; לא הדוק)

טענת עזר: נניח שאין רעש בקודקודים, כלומר נניח שהקודקודים מכילים ספירות מדוייקות. אזי, בכל רגע t ניתן לחשב את סכום המונה (המדוייק) עד לזמן t ע"י סכימה של לכל היותר $\log T$ קודקודים.

רעיון ההוכחה של טענת העזר: מספיק לי לקחת (לכל היותר) קודקוד אחד מכל רמה בעץ. אני אף פעם לא צריך שניים כי אז הייתי יכול לקחת קודקוד מרמה גבוהה יותר במקומם.

לכן, בכל נקודת זמן t , כדי לחשב הערכה למונה הנוכחי מספיק לי לסכום $\log T$ קודקודים רועשים. לפי טענת העזר, נקבל מזה את הערך המדוייק בתוספת סכום של $\log T$ רעשים לפלאסיים, כל אחד מסדר גודל $\frac{\log T}{\epsilon}$.

סך הכל קבל שגיאה מסדר גודל $\frac{\text{polylog } T}{\epsilon}$.

אוקיי. אז קיבלנו שגיאה $\text{polylog } T$ בתחזוק המונה שלנו. זה טוב??

מה ידוע על הבעייה הזאת? (נראה עכשיו)

• עבור $(\epsilon, 0)$ -פ"ד ידוע שהשגיאה צריכה להיות לפחות $\log T$

מה לא ידוע על הבעייה הזאת? (שאלות פתוחות)

- האם שגיאה כזאת הכרחית גם תחת (ϵ, δ) -פ"ד?
- באלגוריתם הנ"ל השגנו $\text{polylog } T$ והחסם התחתון הוא $\log T$. האם אפשר להשיג ממש $\log T$? (ידוע שאפשר להשיג את זה רק תחת הנחות מסויימות על הקלט, אבל לא באופן כללי)

משפט: לכל אלגוריתם $(\epsilon=1, \delta=0)$ -פרטי לבעיית המונה יש שגיאה $\Omega(\log T)$.

(זה יהיה דומה מאוד לתוצאת אי-האפשרות הקודמת שראינו...)

הוכחה:

נניח בשלילה שיש אלגוריתם פרטי \mathcal{A} לבעיית המונה כך בהסתברות לפחות $2/3$ מתקיים שכל ההערכות שהוא מחזיר מדוייקות עד כדי שגיאה $k = \frac{\log T}{16}$ לכל היותר.

נבנה אוסף H של סדרות קלט אפשריות (יהיו בסה"כ T סדרות קלט אפשריות באוסף הזה) - עבור $i = 1, 2, \dots, T$, הסדרה ה- i ית היא:

$$\vec{x}^{(i)} = \left(0, 0, \dots, 0, \underbrace{\frac{\log T}{4}}_{\text{במקום ה- } i}, 0, \dots, 0 \right)$$

מכיוון שהנחנו שלא אלגוריתם שלנו יש שגיאה לכל היותר $\frac{\log T}{16}$ אנחנו יודעים שאם נריץ אותו על סדרת הקלט $\vec{x}^{(i)}$ אז לפני רגע i התשובה של האלגוריתם חייבת להיות לכל היותר $\frac{\log T}{16}$ ואחרי זמן i התשובה חייבת להיות לפחות

$$\frac{3 \log T}{16}$$

בפרט, אם סדרת תשובות היא "טובה" עבור סדרת קלט $\vec{x}^{(i)}$ כלשהו, אז היא לא סדרת תשובות טובה לאף סדרה אחרת $\vec{x}^{(j)}$ עבור $j \neq i$.

אבל הנחנו שאלגוריתם \mathcal{A} מקיים $(\epsilon, 0)$ -פ"ד ושכלל סדרת קלטים הוא מחזיר תשובה "טובה" בהסתברות לפחות $2/3$.

לכן, לכל $j \neq i$ מתקיים:

$$\frac{2}{3} \leq \Pr \left[\begin{array}{l} \mathcal{A}(\vec{x}^{(i)}) \text{ מחזיר} \\ \text{תשובה טובה} \\ \text{עבור } \vec{x}^{(i)} \end{array} \right] \leq e^{2\epsilon \frac{\log T}{4}} \cdot \Pr \left[\begin{array}{l} \mathcal{A}(\vec{x}^{(j)}) \text{ מחזיר} \\ \text{תשובה טובה} \\ \text{עבור } \vec{x}^{(i)} \end{array} \right] = \sqrt{T} \cdot \Pr \left[\begin{array}{l} \mathcal{A}(\vec{x}^{(j)}) \text{ מחזיר} \\ \text{תשובה טובה} \\ \text{עבור } \vec{x}^{(i)} \end{array} \right]$$

ולכן

$$\frac{2}{3\sqrt{T}} \leq \Pr \left[\begin{array}{l} \mathcal{A}(\vec{x}^{(j)}) \text{ מחזיר} \\ \text{תשובה טובה} \\ \text{עבור } \vec{x}^{(i)} \end{array} \right]$$

כלומר, כשאנחנו מריצים את \mathcal{A} על קלט $\vec{x}^{(j)}$, אז בהסתברות $\frac{2}{3\sqrt{T}}$ הוא מחזיר תשובה שטובה בכלל לסדרה אחרת של קלטים (הסדרה $\vec{x}^{(i)}$), וזה נכון לכל $j \neq i$.

לכן,

$$\Pr \left[\begin{array}{l} \mathcal{A}(\vec{x}^{(j)}) \text{ נכשל} \\ \text{ולא מחזיר תשובה} \\ \text{טובה עבור } \vec{x}^{(j)} \end{array} \right] \geq \Pr \left[\bigcup_{i \neq j} \left\{ \begin{array}{l} \mathcal{A}(\vec{x}^{(j)}) \text{ מחזיר} \\ \text{תשובה טובה} \\ \text{עבור } \vec{x}^{(i)} \end{array} \right\} \right] \stackrel{\substack{\text{מאורעות} \\ \text{זרים}}}{=} \sum_{i \neq j} \Pr \left[\begin{array}{l} \mathcal{A}(\vec{x}^{(j)}) \text{ מחזיר} \\ \text{תשובה טובה} \\ \text{עבור } \vec{x}^{(i)} \end{array} \right] \geq (T-1) \cdot \frac{2}{3\sqrt{T}} > 1$$

סתירה.