תורת הסיבוכיות - תרגול 6
חישוב הסתברותי: המחלקות ZPP ו־RL

המחלקה ZPP - "אלגוריתמי לאס וגאס"

שני אפיונים שקולים

ישנן שתי גישות עיקריות לחישובים הסתברותיים. ניתן להתיר לחישוב לטעות לעתים בתשובתו הסופית, אך לדרוש כי סיבוכיות האלגוריתם תהיה יעילה; וניתן לדרוש כי האלגוריתם יוציא תמיד את התשובה הסופית הנכונה, אך להתיר הסתברות כלשהי לכך שסיבוכיות האלגוריתם לא תהיה יעילה. הסוג הראשון של אלגוריתמים מכונה אלגוריתמי מונטה־קרלו, והסוג השני - אלגוריתמי לאס־וגאס.

הדוגמה הקלאסית לאלגוריתם לאס וגאס היא אלגוריתם Quicksort; לאלגוריתם זה זמן ריצה של $O\left(n^2\right)$ במקרה הגרוע (למרבה האירוניה, במימוש נאיבי של האלגוריתם, "המקרה הגרוע" יהיה זה שבו המערך כבר ממויין...), אך בגרסה ההסתברותית של האלגוריתם, תוחלת זמן הריצה היא $O\left(n\log n\right)$, וכמובן שהאלגוריתם מוציא תמיד את הפלט הנכון. מדד התוחלת יהיה גם זה שבו אנו נשתמש.

נאמר כי $L\in\mathrm{ZPP}$ אם קיימת מכונת טיורינג הסתברותית M עבור L שטועה בהסתברות 0 ותוחלת זמן הריצה שלה לכל קלט היא פולינומית.

ניתן לתת מייד אפיון אלטרנטיבי ל־ZPP שלפעמים קל יותר להיעזר בו: $L\in\mathrm{ZPP}$ אם קיימת מכונת טיורינג הסתברותית M שזמן ריצתה על כל קלט הוא פולינומי (באופן מוחלט, לא בתוחלת), כך של־M יש מצב סופי נוסף "לא יודע", ובנוסף לכך:

- M אינה טועה על אף קלט (דהיינו, אם $x\in L$ אז M אינה דוחה, ואם $x\notin L$ אז M אינה מקבלת).
- לכל קלט x, M עונה "לא יודע" על x בהסתברות לכל היותר $\frac{1}{3}$.

לצורך ההוכחה ניעזר במשפט בסיסי בתורת ההסתברות - אי שוויון מרקוב: אם X הוא משתנה מקרי חיובי ו־$k>0$ קבוע, אז מתקיים $\Pr\left(X\ge k\cdot\mathrm{E}\left[X\right]\right)\le\frac{1}{k}$. במילים: ההסתברות לכך ש־X יהיה גדול יותר מאשר פי k מהתוחלת שלו היא לא יותר מ־$\frac{1}{k}$.

הוכחת אי השוויון פשוטה. נגדיר משתנה מקרי I שהוא אינדיקטור למאורע $X\ge k\cdot\mathrm{E}\left[X\right]$ (דהיינו, מקבל 1 במקרה זה ו־0 אחרת). מכיוון שאם $X\ge k\cdot\mathrm{E}\left[X\right]$ אז $\frac{X}{k\cdot\mathrm{E}[X]}\ge1$ נקבל ש־$I\le\frac{X}{k\cdot\mathrm{E}[X]}$. על ידי לקיחת התוחלת של שני האגפים נקבל

$$\Pr\left(X\ge k\cdot\mathrm{E}\left[X\right]\right)\quad=\quad\mathrm{E}\left[I\right]\le\frac{\mathrm{E}\left[X\right]}{k\cdot\mathrm{E}\left[X\right]}=\frac{1}{k}$$

כמבוקש.

כעת נעבור להוכחת השקילות בין שני האפיונים של ZPP. בכיוון האחד, אם M מכונה בעלת אפשרות לתשובת "לא יודע", אז נבנה מכונה M' שעל קלט x מריצה את M על x שוב ושוב עד אשר M עונה תשובה שאינה "לא יודע". מכיוון שההסתברות של M לענות תשובה שאינה "לא יודע" בכל סיבוב היא $\frac{2}{3}$, אז בתוחלת לאחר $\frac{3}{2}$ סיבובים M' תעצור, ומכיוון ש־M פולינומית הרי שגם M' פולינומית בתוחלת.

בכיוון השני, אם M מכונה בעלת תוחלת זמן ריצה $p\left(n\right)$, אז נבנה מכונה M' שעל קלט x מריצה את M על x למשך $3\cdot p\left(|x|\right)$ צעדים, ועונה "לא יודע" אם M לא עצרה בזמן זה; אחרת, היא עונה כמו M. מאי שוויון מרקוב עולה ש־M' עונה "לא יודע" בהסתברות $\frac{1}{3}$ לכל היותר, וביתר המקרים היא עונה נכון.

היחס לאלגוריתמי מונטה־קרלו

מהו כוחם של אלגוריתמי לאס־וגאס ביחס לאלגוריתמי מונטה־קרלו? ניתן לתאר אותו בפשטות על ידי המשפט הבא: $\mathrm{ZPP}=\mathrm{RP}\cap\mathrm{coRP}$.

כזכור, RP היא מחלקת הבעיות שיש להן אלגוריתם הסתברותי שצודק תמיד בתשובת "כן", אך עשוי לטעות בהסתברות קבועה כלשהי בתשובת "לא". coRP היא המחלקה המשלימה של בעיות שבהן האלגוריתם ההסתברותי צודק תמיד בתשובת "לא" אך עשוי לטעות בתשובת "כן". דוגמה קלאסית לאלגוריתם coRP היא אלגוריתם מילר־רבין לבדיקת ראשוניות (שצודק על כל ראשוני אך עשוי לטעות על פריקים).

נעבור להוכחת הטענה. בכיוון אחד, אם $L\in\mathrm{RP}\cap\mathrm{coRP}$ אז יש מכונות הסתברותיות פולינומיות M_1,M_2 שהן מכונות RP ו־coRP בהתאמה עבור L וטועות בהסתברות $\frac{1}{3}$. מכונת ZPP M עבור L, בהינתן קלט x, תריץ את M_1,M_2 על x; אם שתיהן ענו את אותה התשובה, עונה כמוהן, ואחרת עונה "לא יודע".

אם $x \in L$ אז M_1 תענה תמיד "כן" על x, ואילו M_2 תענה "כן" בהסתברות $\frac{2}{3}$ ו-"לא" בהסתברות $\frac{1}{3}$, ועל כן בהסתברות $\frac{1}{3}$ M תענה "לא יודע" ואחרת תענה נכון. ניתוח סימטרי עובד גם כאשר $x \notin L$, כך ש-M היא מכונת ZPP תקנית (על פי ההגדרה האלטרנטיבית שהצגנו).

בכיוון השני, נניח כי $L \in \mathrm{ZPP}$ עם מכונה M. נבנה מכונת RP M' עבור L: בהינתן x, M' תריץ את M על x. אם M ענתה תשובה אינפורמטיבית, תענה כמוה; אם M ענתה "לא יודע" אז M' תענה "כן".

בבירור אם $x \in L$ אז M' מחזירה תמיד תשובה נכונה; אם $x \notin L$ אז M' טועה אם M עונה "לא יודע", כלומר בהסתברות $\frac{1}{3}$.

באופן דומה מראים כי $\mathrm{ZPP} \subseteq \mathrm{coRP}$.

סיבוכיות זכרון הסתברותית ושרשראות מרקוב

נגדיר מחלקת סיבוכיות המתאימה לחישובים הסתברותיים עם טעות חד צדדית הדורשים סיבוכיות זכרון יעילה (לוגריתמית):

$L \in \mathrm{RL}$ אם קיימת מכונת טיורינג הסתברותית M שעובדת בזכרון לוגריתמי ובזמן פולינומי כך ש-

$$
\begin{aligned}
x \in L \quad &\Rightarrow \quad \Pr\left(M\left(x\right) = \mathrm{acc}\right) \geq \frac{2}{3} \\
x \notin L \quad &\Rightarrow \quad \Pr\left(M\left(x\right) = \mathrm{rej}\right) = 1
\end{aligned}
$$

שימו לב לדרישה על זמן הריצה הפולינומי! ניתן להוכיח כי ללא דרישה זו מקבלים מחלקה הזהה בכוחה ל-NL.

בבירור מתקיימים יחסי ההכלה $\mathrm{DL} \subseteq \mathrm{RL} \subseteq \mathrm{NL} \subseteq \mathrm{P}$.

מכיוון ש-RL סגורה לרדוקציות logspace ו-STCON היא NL-שלמה, נובע שאם $\mathrm{STCON} \in \mathrm{RL}$ אז NL=RL.

מה קורה כאשר מסתכלים בבעיה דומה ל-STCON, אך על גרף לא מכוון? מסתבר שבמקרה זה, ניתן להוכיח ללא קושי שהשפה ב-RL.

נגדיר: $\mathrm{USTCON} = \{(G,s,t) \mid$ G גרף לא מכוון שבו קיים מסלול מ-s אל $t\}$.

טענה: $\mathrm{USTCON} \in \mathrm{RL}$ (למעשה, תוצאה חדשה יחסית של Reingold מראה כי $\mathrm{USTCON} \in \mathrm{DL}$ אך לא נראה זאת כאן).

הפתרון קל לתיאור - פשוט נטייל בגרף באופן אקראי החל מ-s, בתקווה להיתקל "בטעות" ב-t. טיול שכזה, שבו בכל צעד נבחרת קשת באקראי מכל הקשתות המחוברות אל הצומת, נקרא הילוך מקרי. אם אחרי פרק זמן מסויים לא נגיע ל-t, ניכנע ונפלוט "לא", בעוד שאם נגיע ל-t כמובן שנפלוט "כן". הקושי הוא בניתוח הסתברות ההצלחה כפונקציה של אורך הטיול בגרף. היעד הוא הסתברות הצלחה **קבועה** (שאינה תלויה בגודל הגרף), וסיבוכיות זמן ריצה **פולינומית** בגודל הגרף (סיבוכיות הזכרון הלוגריתמית נובעת מאליה מכיוון שאנו זוכרים בכל שלב רק את הצומת הנוכחי ואת מונה הצעדים שלנו, שערכו הוא תמיד פולינומי).

מדוע פתרון זה לא יעבוד גם עבור גרף מכוון? אינטואיטיבית, מכיוון שהילוך מקרי בגרף מכוון עשוי "להתקלקל" בקלות באופן שיקשה על תיקון. למשל, נתבונן בשרוך בעל n צמתים שמוביל מ-s אל t, כך שמכל צומת בגרף יש קשת מכוונת אל s. ההסתברות להגיע מ-s אל t בהילוך מקרי מבלי לחזור שוב אל s היא $\frac{1}{2^n}$, כך שתוחלת מספר הצעדים הדרושים להגעה אל t היא $\Omega\left(2^n\right)$. בהילוך מקרי בגרף לא מכוון אין בעיה כזו, כי גם אם עושים צעד לכיוון הלא נכון, יש סיכוי סביר "לתקן" זאת בסיבוב הבא על ידי חזרה כלעומת שבאנו.

הטענה ההסתברותית שמוכיחה את נכונות האלגוריתם היא זו: אם קיים מסלול מ-s אל t בגרף הלא מכוון, אז תוחלת מספר הצעדים עד להגעה מ-s אל t היא לכל היותר $2\left|E\right|\left|V\right|$. אם כן, מספיק שהאלגוריתם ירוץ במשך $6\left|E\right|\left|V\right|$ צעדים (מספר שהוא כמובן פולינומי בגודל הקלט) ואז על פי אי שוויון מרקוב נקבל הסתברות $\frac{2}{3}$ להצלחה (ההסתברות שמספר הצעדים שיידרש להגעה מ-s אל t יהיה גדול מ-$6\left|E\right|\left|V\right|$ היא לכל היותר $\frac{1}{3}$).

לצורך הוכחת הטענה, נשתמש בתוצאות מהענף של תורת ההסתברות שחוקר תהליכים דוגמת הילוכים מקריים בגרף - שרשראות מרקוב. שרשרת מרקוב (בזמן בדיד) היא גרף מכוון (לא בהכרח סופי, אך בעל מספר בן מניה של צמתים) כך שלכל קשת מותאמת הסתברות חיובית, ולכל צומת, סכום ההסתברויות על כל הקשתות היוצאות מצומת זו הוא 1. אפשר לחשוב על שרשרת מרקוב כעל תהליך אקראי כלשהו המורכב מ"מצבים" כך שבכל יחידת זמן בדידה עוברים מהמצב הנוכחי למצב הבא, כשהמצב הבא נקבע אקראית, אך רק על פי המידע על המצב הנוכחי - כלומר, השרשרת היא **חסרת זכרון** (זוהי התכונה המאפיינת של תהליכים מרקוביים).

ניתן לתאר שרשרת מרקוב באמצעות מטריצה P כך ש-P_{ij} היא הסתברות המעבר מ-i אל j. סכום כל שורה במטריצה הוא 1 - מטריצה שכזו מכונה מטריצה סטוכסטית. אם v הוא וקטור שמציין את ההסתברות שלנו להיות במצבי השרשרת ברגע מסויים, אז $v \cdot P$ הוא הוקטור שמציין את ההסתברות שלנו להיות במצבי השרשרת ברגע שלאחר מכן (אחרי שבוצע הצעד הבא בשרשרת). וקטור מנורמל π המקיים $\pi = \pi \cdot P$ נקרא **וקטור סטציונרי** (זהו "וקטור עצמי משמאל" של המטריצה המתאים לערך העצמי 1). וקטור כזה מתאר את ההתנהגות האופיינית של השרשרת בטווח הארוך (למשל, אם למצב מס' 1 הסתברות $\frac{1}{3}$ בתוך π, פירוש הדבר הוא שאנו מצפים שבטווח הארוך, התהליך המתואר על ידי P יבלה שליש מזמנו במצב 1).

כעת נשתמש, ללא הוכחה, במשפט בסיסי בתורה של שרשראות מרקוב:

משפט: לכל שרשרת מרקוב המתוארת על ידי גרף **סופי** ו**קשיר היטב** קיים וקטור סטציונרי יחיד π. בנוסף, לכל מצב i, $\frac{1}{\pi_i}$ היא תוחלת מספר הצעדים שנדרשים לשרשרת להגיע ממצב i חזרה אל המצב i.

הדרישה לסופיות וקשירות-היטב הופכות את השרשרת ל"נחמדה" במובן זה שמכל צומת יש הסתברות חיובית להגיע לכל צומת אחר (מהקשירות-היטב) ויותר מכך, תוחלת הזמן שנדרשת לנו לחזור לכל צומת, מרגע שעזבנו אותו, היא סופית (זה נובע מסופיות הגרף; קיימים גרפים קשירים-היטב אינסופיים שבהם תכונה זו, שהיא התכונה המהותית שנדרשת בהוכחת המשפט, אינה מתקיימת).

אם P היא מטריצה סטוכסטית מגודל $n \times n$ כך שגם סכום כל **עמודה** הוא 1 (P היא "סטוכסטית כפולה") אז ברור כי הוקטור $v = \left(\frac{1}{n}, \ldots, \frac{1}{n}\right)$ הוא וקטור סטציונרי של P, ולכן מהמשפט נובע שתוחלת מספר הצעדים שנדרשים לחזרה ממצב לעצמו בשרשרת ש־P מייצגת הוא n.

כעת, בהינתן גרף לא מכוון G נבנה ממנו שרשרת מרקוב באופן הבא: ראשית נהפוך את G לגרף מכוון על ידי החלפת כל קשת של G בזוג קשתות לשני הכיוונים. כעת נבנה שרשרת שמצביה הם **קשתות** הגרף החדש (כלומר, יש בה $2|E|$ מצבים), כך שהסתברות המעבר מהמצב (u,v) למצב (v,w) היא $\frac{1}{d(v)}$. זוהי ההסתברות לכך שאם בהילוך המקרי שלנו על G הגענו ל־v מהצומת u, אז לאחר מכן נמשיך אל הצומת w. אם הגרף המקורי G קשיר וסופי, אז השרשרת שהתקבלה היא קשירה־היטב וסופית. בנוסף, המטריצה שמייצגת את השרשרת היא סטוכסטית־כפולה, שכן אם "נקפיא" את (v,w) אז יש בדיוק $d(v)$ שורות (u,v) שונות מאפס בעמודה של (v,w) (שמתאימות בדיוק לצמתים שהם שכנים של v). מכאן שההסתברות הסטציונרית של השרשרת היא $\pi = \left(\frac{1}{2|E|}, \ldots, \frac{1}{2|E|}\right)$ ובפרט תוחלת הזמן שנדרשת לחזרה אל מצב מעצמו היא $2|E|$. בחזרה לגרף G, פירוש הדבר הוא שעבור כל זוג צמתים u,v המחוברים בקשת, תוחלת הזמן של הגעה מ־u אל v מאז הפעם האחרונה שבה ההילוך הגיע מ־u אל v, היא $2|E|$. מכיוון שההילוך בגרף הוא חסר זכרון, זה אומר למעשה שהילוך שמגיע לצומת v יספיק להגיע ל־u וללכת ממנו אל v בתוחלת זמן של $2|E|$ צעדים.

אם נסמן ב־h_{uv} את תוחלת הזמן הנדרשת להגעה מצומת u אל צומת v בגרף, הרי שהוכחנו שעבור שני צמתים המחוברים בקשת, מתקיים $h_{uv} + h_{vu} \le 2|E|$. בפרט $h_{uv} \le 2|E|$ לכל שני צמתים המחוברים בקשת.

כעת אם u,v מופרדים על ידי מסלול באורך k: $u \to w_1 \to w_2 \to \ldots w_{k-1} \to v$, אז $h_{uv} \le h_{uw_1} + h_{w_1 w_2} + \ldots + h_{w_{k-1} v} \le 2k|E|$. מכיוון שהמרחק בין שני צמתים בגרף קשיר הוא לכל היותר $|V|$, נקבל את החסם $h_{st} \le 2|V||E|$ שעליו התבססנו באלגוריתם.