תורת החישוביות – תרגול מספר 12
אלגוריתמי קירוב

אלגוריתמי קירוב

רוב העיסוק שלנו בקורס היה בבעיות הכרעה, אך ניתן לדבר באופן כללי יותר על בעיות של חישוב פונקציות. למשל, בהינתן פסוק CNF – כמה השמות מקבלות יש לו? בהינתן גרף – מה גודל הכיסוי בצמתים המינימלי שלו? מה מספר הצביעה שלו? וכדומה. בבירור תשובות לשאלות אלו גם מאפשרות לנו לפתור את בעיות ההכרעה המתאימות ולכן חישוב הפונקציות הללו קשה לפחות כמו פתרון בעיות ההכרעה. מצד שני, כאשר התשובה היא מספרית (ולא רק "כן/לא") ניתן לקוות שאפשר יהיה **לקרב** אותה – להחזיר תשובה שאינה התשובה האופטימלית, אבל היא "לא רעה". כך למשל בהינתן גרף ניתן למצוא לו כיסוי בצמתים שגודלו אינו יותר מפי 2 מגודל הכיסוי בצמתים האופטימלי.

פורמלית, תהא $f:\Sigma^*\to\mathbb{N}$ פונקציה.

מכונה M לחישוב פונקציות היא קירוב d־חיבורי של f ‏($d>0$) אם לכל $x\in\Sigma^*$ מתקיים $|M(x)-f(x)|\le d$, כלומר $f(x)-d\le M(x)\le f(x)+d$.

מכונה M לחישוב פונקציות היא קירוב α־כפלי של f ‏($\alpha>1$) אם לכל $x\in\Sigma^*$ מתקיים $\frac{1}{\alpha}f(x)\le M(x)\le\alpha f(x)$.

הקירובים הללו הם "דו צדדיים" במובן זה ש־$M(x)$ יכול להיות גם קטן וגם גדול יותר מ־$f(x)$. ברוב המקרים דורשים שהקירוב יהיה "חד צדדי". כך למשל אם גרף הוא 3 צביע, זו טעות סבירה מצד M להגיד שהגרף הוא 4 או 5 צביע, אך לא סביר ש־M תגיד שהגרף הוא 2 צביע (שכן ניתן לצבוע את הגרף ב־4 או 5 צבעים, זה פשוט פחות טוב, ולעומת זאת הטענה שאפשר לצבוע את הגרף בשני צבעים היא שגויה).

לכן, אם $f(x)$ מייצג בעיית מינימיזציה לרוב דורשים כי יתקיים $f(x)\le M(x)$, ואם $f(x)$ מייצג בעיית מקסימיזציה דורשים $M(x)\le f(x)$.

לרוע המזל, מתברר כי במקרים רבים לא קיימים אפילו קירובים טובים בזמן פולינומי, מהטעם הפשוט שאפשר לנצל קירוב טוב כדי לפתור את בעיית ההכרעה המקורית בזמן פולינומי.

דוגמה חיבורית: מסלולים המילטוניים

נגדיר פונקציה: מספר המסלולים ההמילטוניים בגרף המכוון $G=f(G)$. אם $\mathrm{P}\ne\mathrm{NP}$ הפונקציה בוודאי אינה ניתנת לחישוב בזמן פולינומי שכן היינו יכולים לפתור בעזרתה את בעיית המסלול ההמילטוני: בהינתן G היינו מחשבים את $f(G)$ ומקבלים אם ורק אם $f(G)>0$.

נראה כי הפונקציה אינה ניתנת ל־3־קירוב חיבורי (ולמעשה, כי היא אינה ניתנת ל־d־קירוב חיבורי עבור כל d קבוע).

הרעיון הוא שבהינתן G, ניתן לבנות ממנו גרף חדש G' כך שאם ב־G לא היה מסלול המילטוני גם ב־G' אין, אך אם היה ב־G ולו מסלול המילטוני יחיד, אז ב־G' יהיו מסלולים המילטוניים רבים.

בהינתן G, נבחר צומת שרירותי $v\in V$ ונחליף אותו ברכיב שכולל ארבעה צמתים: v_{in},v_{out},v_1,v_2, והקשתות הבאות: $v_{in}\to v_1,v_{in}\to v_2,v_1\to v_2,v_2\to v_1,v_1\to v_{out},v_2\to v_{out}$.

כמו כן כל קשת שנכנסה ל־v נכניס כעת ל־v_{in} וכל קשת שיצאה מ־v נוציא כעת מ־v_{out}.

קל לראות כי כעת **הכפלנו** את מספר המסלולים ההמילטוניים בגרף: כל מסלול קיים נכנס ל־v_{in}, ואז יש לו בחירה האם ללכת ראשית כל ל־v_1 ואז ל־v_2 ומשם ל־v_{out}, או קודם ל־v_2 ואז ל־v_1 ואז ל־v_{out} (הוא חייב לעשות אחד משני מסלולים אלו או שאחד מהצמתים v_1,v_2 לא יכללו כלל במסלול שאמור להיות המילטוני).

על הבניה הזו ניתן לחזור מספר פעמים שרירותי כרצוננו. אחרי 3 חזרות, מספר המסלולים ההמילטוניים בגרף יוכפל פי 8 (ובפרט יישאר 0 אם הוא היה 0 לפני כן). G' יהיה הגרף שמתקבל מ־G על ידי 3 חזרות שכאלו, אז מתקיים $f(G')=8f(G)$.

כעת, אם g היא קירוב 3־חיבורי ל־f, אז בהינתן G ניתן להכריע ביעילות באמצעות חישוב g את השפה ־DHC בהינתן גרף G, נבנה את G', נחשב את $g(G')$ ונקבל אמ"מ $g(G')>3$.

למעשה ניתן כעת לחשב **במדויק** את $f\left(G\right)$ בעזרת קירוב 3־חיבורי. תהא M המכונה שמבצעת את הקירוב. אז מתקיים:

$$\left[\frac{M\left(G'\right)}{8}\right] = \left[\frac{f\left(G'\right)\pm3}{8}\right]=\left[\frac{8f\left(G\right)\pm3}{8}\right]=\left[f\left(G\right)\pm\frac{3}{8}\right]=f\left(G\right)$$

כאשר $f\left(G'\right)\pm3$ כאן פירושו "לכל היותר במרחק ±3 מ־$f\left(G'\right)$".

החלוקה ב־8 גרמה לשגיאה להתקזז ולהיות קטנה יותר מחצי, ולכן על ידי לקיחת הערך השלם הקרוב ביותר אנחנו מגיעים לערך המדויק של $f\left(G\right)$.

דוגמה כפלית: בעיית הסוכן הנוסע

בבעיית הסוכן הנוסע, נתון גרף מלא K_n על n צמתים, ופונקציית משקל $w:E\to\mathbb{R}^{+}$, והמטרה היא למצוא מעגל המילטוני עם משקל מינימלי (שימו לב שבגרף זה אין בעיה למצוא מעגל המילטוני כלשהו, שכן הגרף הוא גרף מלא, ולכן כל פרמוטציה על הצמתים נותנת מעגל המילטוני חוקי בגרף). נגדיר את הפונקציה הבאה: $f\left(K_n,w\right)=\min\{w\left(C\right)\mid$ מעגל המילטוני $C\}$, כלומר בהינתן מופע של הסוכן הנוסע, f מחזירה את משקל המעגל ההמילטוני המינימליביחס לפונקציית המשקל w. נראה שבהנחה ש־$\mathrm{P}\neq\mathrm{NP}$ לא קיים קירוב α־כפלי ל־f לכל $0<\alpha$ קבוע.

נניח בשלילה שקיים α־קירוב, ונראה שבאמצעות הקירוב ניתן להכריע את השפה HC.

בהינתן גרף G נבנה מופע של בעיית הסוכן הנוסע באופן הבא - מספר הצמתים יהיה כמספר הצמתים ב־G, ולכל קשת $\{u,v\}$ בגרף המלא ניתן משקל 0 אם היא קיימת ב־G ו־1 אחרת. נשים לב שבמופע הזה מתקיים שבגרף G יש מעגל המילטוני אמ"מ $f\left(K_n,w_G\right)=0$. כעת נשים לב שכל קירוב α־כפלי ל־f חייב להחזיר 0 אם ערך f הוא 0 ומספר >0 אם ערך f גדול מ־0, ולכן בהינתן הקירוב ניתן להכריע את הבעיה ביעילות.

הקלות והקושי של קירוב 3SAT

נתון פסוק 3SAT φ ונניח לצורך פשטות שבכל פסוקית שלו כל הליטרלים הם של משתנים שונים זה מזה (אין פסוקית דוגמת $(x_1\vee x_1\vee\overline{x_1})$). בעיית הקירוב שלנו תהיה למצוא את המספר המקסימלי של פסוקיות שניתן לספק בו זמנית בפסוק.

האבחנה המפתיעה היא שבפסוק כזה ניתן לספק תמיד לפחות $\frac{7}{8}$ מהפסוקיות בו זמנית. ההוכחה היא דוגמה פשוטה למה שמכונה "השיטה ההסתברותית".

נגדיר מרחב הסתברות שבו כל השמה למשתני φ נבחרת בהסתברות אחידה.

לכל פסוקית C_k של φ נגדיר משתנה מקרי X_k, שמקבל 1 אם הפסוקית מסתפקת תחת ההשמה שנבחרה באקראי, ו־0 אם לא (משתנה כזה מכונה אינדיקטור). קל לראות על פי הגדרה ש־$\mathrm{E}\left[X_k\right]$, התוחלת של המשתנה, שווה להסתברות שהוא מקבל 1, וקל לראות שהסתברות זו היא $\frac{7}{8}$, שכן C_k מכילה בדיוק שלושה ליטרלים של משתנים שונים זה מזה ולכן בדיוק אחת מ־8 ההשמות האפשריות לשלושת המשתנים הללו **אינה** מספקת את C_k.

כמו כן נשים לב שמספר הפסוקיות הכולל של φ שהסתפקו בהשמה אקראית מתואר על ידי המשתנה המקרי $X=\sum_k X_k$. מלינאריות התוחלת נקבל $\mathrm{E}\left[X\right]=\mathrm{E}\left[\sum_k X_k\right]=\sum_k\mathrm{E}\left[X_k\right]=\frac{7}{8}t$, כאשר t הוא מספר הפסוקיות הכולל של φ.

מכאן שמספר הפסוקיות **הממוצע** שמסתפק בהשמה מקרית ל־φ הוא $\frac{7}{8}$ מהפסוקיות. בפרט, חייבת להיות השמה מקרית אחת לפחות שמספקת **לפחות** $\frac{7}{8}$ מהפסוקיות (אחרת הממוצע היה נמוך יותר). בפרט, זה מוכיח את קיומה של השמה שמספקת $\frac{7}{8}$ מהפסוקיות לפחות.

אם כן, קיים אלגוריתם $\frac{8}{7}$־קירוב כפלי לבעיה שהצגנו: פשוט אומרים "$\frac{7}{8}t$". מכיוון ש־$\frac{7}{8}t\le f\left(\varphi\right)\le t$ אז מצד אחד הקירוב מקיים $M\left(\varphi\right)=\frac{7}{8}t\le f\left(\varphi\right)$, ומצד שני $\frac{1}{8/7}f\left(\varphi\right)\le\frac{7}{8}t=M\left(\varphi\right)$.

עם זאת, קיימת הוכחה לכך שלכל $\varepsilon>0$, קטן ככל שיהיה, לא קיים אלגוריתם $\frac{8}{7}-\varepsilon$־קירוב לבעיה. כלומר, הקירוב הטריוויאלי הוא גם האופטימלי. הוכחה לכך שלא קיים הקירוב הנ"ל מסתמכת על תוצאה חזקה ומודרנית בסיבוכיות הנקראת "משפט ה־PCP" אשר לא נוכל להציג כאן.