בס"ד

(24)

נושא 4 - מעגלים בוליאניים

א) הגדרה

מעגל בוליאני הוא מודל חישובי היכול לקבל קלטים באורך קבוע n* ויש לו פלט יחיד 1/0.

מייצגים מעגל בוליאני באמצעות גרף מכוון ללא מעגלים (גרף DAG) שבו יש שלושה סוגים של צמתים:

* מודל לא פורמלי להפקיד כך שהוא 'יוניפורמי' צריך מעגל לכל אורך.

(1) צמתים $x_1,x_2,\ldots,x_n$ המייצגים את הקלט. לצמתים אלו אין קשתות נכנסות אלא רק יוצאות. כל צומת מייצגת ביט 1/0.

(2) צומת המייצגת את הפלט. לצומת זו יש רק קשתות נכנסות ולא יוצאות.

(3) כל צומת אחרת, מייצגת אחד משלושת השערים הלוגיים {AND, OR, NOT}. לצומת NOT יש קשת כניסה אחת ולצמתי AND ו-OR יש שתי קשתות נכנסות. לכל אחד מהצמתים מסוג זה יכול להיות 1/2 קשתות יוצאות.

הערות חשובות:

- גודל מעגל בוליאני C יסומן ב-$|C|$, ומייצג את מספר השערים הלוגיים ב-C. גודל זה מייצג את סיבוכיות המעגל הבוליאני.
- הפלט של C על קלט x יסומן ב-$C(x)$.
- מעגל בוליאני שבו יש לכל שער לוגי קשת יוצאת אחת הוא למעשה נוסחה בוליאנית.

ב) משפחת מעגלים וזיהוי שפה

משפחת מעגלים היא סדרה של מעגלים בוליאנים $\{C_n\}_{n\in\mathbb{N}}$ כאשר לכל $n\in\mathbb{N}$ יש מעגל בוליאני מתאים המקבל קלטים באורך n.

הגדרת סיבוכיות משפחת מעגלים: תהא פונקציה $T:\mathbb{N}\to\mathbb{N}$. נאמר כי משפחת מעגלים היא מסדר גודל של $T(n)$ אם לכל מעגל בוליאני C_n השייך למשפחת המעגלים ומקבל קלטים באורך $n\in\mathbb{N}$ מתקיים $|C_n|\le T(n)$, כלומר גודל המעגל הבוליאני C_n קטן מ-$T(n)$. $T(n)$ חוסם מלמעלה גודל כל מעגל בוליאני המקבל קלטים מאורך n.

ג) המחלקה $SIZE(T(n))$

נאמר ששפה $L\in SIZE(T(n))$ אם קיימת משפחת מעגלים $\{C_n\}_{n\in\mathbb{N}}$ מסדר גודל $O(T(n))$ המכריעה את L, כלומר עבור $n\in\mathbb{N}$ מתקיים: לכל $x\in\{0,1\}^n$ $C_n(x)=1 \iff x\in L$.

3) המחלקה P/poly

זוהי מחלקה המכילה את אוסף כל השפות L שקיימת להן משפחת מעגלים המכריעה אותן בסדר גודל פולינומי. כלומר את ק"ם $P/poly = \bigcup_{i\in\mathbb{N}} SIZE(n^i)$

בעזרת המשפט הבא נראה מה הקשר בין המחלקה P/poly למחלקה P.

<u>משפט:</u> לכל מכונת טיורינג דטרמיניסטית M העובדת בזמן $T(n)$, יש משפחת מעגלים $\{C_n\}_{n\in\mathbb{N}}$ בגודל $O(T(n)^2)$ כך שלכל $x\in\{0,1\}^n$ מתקיים $C_n(x)=1 \Leftrightarrow M(x)=1$.

ראינו בהרצאה: פונקציה המחשבת ... מ-M ל-$\{C_n\}_{n\in\mathbb{N}}$ ניתן לחישוב ... עובדת. [illegible]

הוכחה: דומה מאוד לקוק לוין. תהי M דטרמיניסטית, אזי קיימת לה מ"ט oblivious $\tilde{M}$ המחשבת אותה השפה. בזמן $T_{\tilde{M}}(n)$, $L(M)=L(\tilde{M})$. נבנה משפחת מעגלים $\{C_n\}_{n\in\mathbb{N}}$ עבור $\tilde{M}$. עבור כל קלט $x\in\{0,1\}^n$ המעגל הבוליאני C_n יקבל את הקלט $x=x_1x_2\dots x_n$ וימלא את ריצת $\tilde{M}$ על x ע"י חישוב כל הקונפיגורציות שלה $z_1,\dots,z_{T(n)}$. כמו בהוכחת קוק לוין כל $z_i=(a_i,b_i,q_i)$ כאשר a_i הוא תו קלט נוכחי, b_i תו עבודה נוכחי ו-q_i מצב נוכחי.

האורך של כל z_i הוא $\ell=\log(|Q|)+2\log(|\Gamma|)$, כאשר Q הוא קבוצת המצבים ו-Γ קבוצת הא"ב של M.

ניתן לחשב כל z_i באמצעות ℓ פונקציות שכל פונקציה F_j עבור $1\le j\le \ell$ מחזירה את הביט ה-j ב-z_i. כדי לחשב את z_i צריך $(z_{i-1}, z_{prev(i)}, x_{inputpos(i)})$, כאשר z_{i-1} הוא קונפיגורציה קודמת, $z_{prev(i)}$ הוא קונפיגורציה האחרונה בה הראש קורא היה באותו תא בסרט העבודה כמו מצב נוכחי, ו-$x_{inputpos(i)}$ הוא הביט במיקום ה-i ב-X. a_i מחושב באמצעות $x_{inputpos(i)}$, b_i מחושב באמצעות $z_{prev(i)}$ ו-q_i מחושב באמצעות z_{i-1}. $F_j(z_{i-1},z_{prev(i)},x_{inputpos(i)})=z_i[j]$.

מהמשפט שלמדנו בקוק לוין לכל פונקציה בוליאנית כזו קיימת נוסחה בגודל קבוע המקבילה לה. כיוון שנוסחה בוליאנית היא צורה פרטית של מעגל בוליאני, C_n יהיה מורכב מ-ℓ פונקציות אלו עבור כל קונפיגורציה z_i.

ראינו בתחילת הקורס ... רשום ... בסרט העבודה ... מ"ט ... [illegible]

לסיום אם הפלט בקונפיגורציה $z_{T(n)}$ הוא 1 אזי C_n יפלוט 1 ואחרת 0.

גודל C_n - מורכב מ-$\ell\cdot T_{\tilde{M}}(n)$ נוסחאות בוליאניות שכל אחת מהן בגודל קבוע ולכן גודל המעגל הוא $O(T_{\tilde{M}}(n))$. אולם כיוון ש-$T_{\tilde{M}}(n)=O(T(n)^2)$ לפי משפט שלמדנו בנוסחת oblivious אזי גודל המעגל C_n ביחס ל-M הוא $O(T(n)^2)$ כנדרש. מ.ש.ל.

<u>משפט הקשר בין P/poly ל-P:</u> מתקיים $P\subseteq P/poly$.

הוכחה: תהא $L\in P$ אזי יש לה מ"ט M שמכריעה אותה בזמן פולינומי. לפי משפט קודם יש משפחת מעגלים גם כן שמכריעה את L בזמן פולינומי. ולכן $L\in P/poly$. P מוכלת ממש ב-P/poly כי P/poly מכילה גם בעיות עצירה.

ה) <u>השפות CKT-True ו- CKT-SAT</u>

נגדיר שתי שפות:

$CKT\text{-}True = \{\langle C_n, x\rangle \mid C_n(x)=1$ וגם C_n הוא מעגל בוליאני לקלט בגודל n ו- $x\in\{0,1\}^n\}$.

$CKT\text{-}SAT = \{\langle C_n, x\rangle \mid C_n(x)=1$ כך ש- $x\in\{0,1\}^n$ הוא מעגל בוליאני לקלט באורך n וקיים $C_n\}$.

משפטים:

(1) $CKT\text{-}True \in P\text{-}COMPLETE$, כאשר הגדרת שלמות ב-P על בסיס רדוקציות בזכרון לוגריתמי מוגבל.

הוכחה: CKT-True שייכת ל-P שכן ניתן להגדיר מ"ט M המקבלת מעגל בוליאני וקלט x ומריצה את x על C_n ועונה כמוהו בזמן פולינומי.

להוכחת שלמות ב-P, תהי $L\in P$ אזי קיימת לה מ"ט דטרמיניסטית M. נגדיר פונקציית רדוקציה f המקבלת $x\in\{0,1\}^n$ ומחזירה מעגל בוליאני לקלט באורך n, כמו משפט ראשון בסעיף הקודם. $f(x)=(C_n, x)$. f ניתנת לחישוב בזכרון לוגריתמי מוגבל ולכן הטענה מתקיימת.

(2) $CKT\text{-}SAT \in NP\text{-}COMPLETE$.

ו) <u>משפחות מעגלים אוניפורמיות</u>

משפחת מעגלים $\{C_n\}_{n\in\mathbb{N}}$ תקרא P-אוניפורמית אם קיימת מ"ט דטרמיניסטית ופולינומית אשר בהינתן קלט 1^n מוצרת את המעגל C_n. כלומר, לפי אורך הקלט מייצרת את המעגל ממשפחת המעגלים המטפל בקלטים באורך זה.

<u>המחלקה $\mathcal{L}$:</u> נסמן ב- $\mathcal{L}$ את אוסף כל השפות L שיש להן משפחת מעגלים P-אוניפורמית שמכריעה אותן.

<u>משפט:</u> $P = \mathcal{L} \subseteq P/poly$.

הוכחה: $\mathcal{L} \subseteq P/poly$ טריוויאלי. נוכיח $P=\mathcal{L}$. כיוון 1- תהי $L\in\mathcal{L}$ אזי יש ל-L משפחת מעגלים $\{C_n\}_{n\in\mathbb{N}}$ P-אוניפורמית המכריעה אותה. כיוון שהיא P-אוניפורמית יש מ"ט M דטרמיניסטית ופולינומית המייצרת את C_n לכל קלט באורך n. נבנה מ"ט M_L שתכריע את L. M_L על קלט $x\in\{0,1\}^*$ תריץ את M על הקלט $1^{|x|}$ ותייצר את $C_{|x|}$. M_L תריץ את $C_{|x|}$ על x ותענה כמוה. כיוון ש-M פולינומית ו- $C_{|x|}$ גם כן בגודל פולינומי אזי M_L פולינומית ולכן $L\in P$.

כיוון 2- תהי $L\in P$ בסעיף ג' הראינו הוכחה כיצד ניתן לבנות משפחת מעגלים בזמן פולינומי המכריעה את L

ג) יכולת חישוב של מעגל בוליאני

משפט: לכל n גדול מספיק קיימת פונקציה $f:\{0,1\}^n \to \{0,1\}$ שאינה ניתנת לחישוב/ הכרעה ע"י מעגל בוליאני בגודל $\frac{2^n}{100n}$.

הוכחה: נוכיח באמצעות שיקולי ספירה. כל פונקציה בוליאנית ניתן לתאר באמצעות מחרוזת באורך 2^n שכן יש 2^n קלטים אפשריים ולכל קלט יש שני פלטים אפשריים. לכן נוכל לזהות את הפונקציה הבוליאנית בתור מחרוזת באורך 2^n כך שבמקום ה-i יש את הפלט של הקלט ה-i.

לכן סה"כ מספר הפונקציות הבוליאניות הוא 2^{2^n}.

כעת נחשב מהו אורך המחרוזת הדרוש לקידוד מעגל בוליאני באורך $S\in\mathbb{N}$. לשם כך יש לקודד את S השערים הלוגיים. כל שער לוגי דורך לציין אילו 1 או 2 שערים מחוברים אליו, דרוש $2\log(S)$ ביטים, ועוד 2 ביטים לציין סוג השער ($\text{AND}, \text{OR}, \text{NOT}$). סה"כ $S\cdot(2\log(S)+2) \le 45\log(S)$.

עבור $S=\frac{2^n}{100n}$ נקבל שמספר המעגלים באורך זה: $2^{9\cdot\frac{2^n}{100n}\log\left(\frac{2^n}{100n}\right)} = 2^{9\cdot\frac{2^n}{100n}\cdot(n-\log(100n))} < 2^{\frac{9}{10}\cdot 2^n}$.

שהוא קטן ממש ממספר הפונקציות הבוליאניות באורך זה, ולכן הטענה מתקיימת.

יהיה כנראה
צריך עוד ביט׳ים
חסום ב-$9S\log(S)$.

ח) מקביליות

תכונה חשובה לתוכנה היא שניתן לחשב אותה באופן מקבילי, כלומר שכמה מעבדים או מחשבים יוכלו לחשב אותה באותו הזמן במקביל. כך יתאפשר רק עבור חישובים שאינם דורשים אחד את השני. במעגל בוליאני נשים לב שכל השערים באותה רמה אפשר לחשב באופן מקבילי ואינם תלויים אחד את השני. לכן תכונה חשובה של מעגלים בוליאניים כזה לא רק גודל מספר השערים במעגל אלא גם העומק של השערים. נגדיר שתי מחלקות שמתחשבות בזה:

מחלקות NC ו-AC