תורת החישוביות – תרגול מספר 8
אי־דטרמיניזם ו־NP

חסמי זמן ריצה

נאמר כי פונקציה $f:\mathbb{N}\to\mathbb{N}$ מהווה **חסם זמן ריצה** עבור מ"ט (דטרמיניסטית) M, אם לכל קלט w, מספר צעדי החישוב של M על w הוא $f(|w|)$ לכל היותר. נאמר שמ"ט היא **פולינומית** אם קיים לה חסם זמן ריצה שהוא פולינום. נסמן ב־P את מחלקת השפות שניתנות להכרעה בזמן פולינומי. נשים לב כי ההגדרה גוררת מייד ש־$P\subseteq\mathrm{R}$ (מדוע?).

מעגל אוילר

כידוע, אפשר לקודד גרף כמחרוזת בינארית סופית. בהמשך נשתמש בקידוד אחיד עבור גרפים בלי לציין במפורש מהו, ונראה שלמטרותינו שיטת הקידוד המדויקת אינה חשובה. נתמקד בינתיים בגרפים לא מכוונים.

נאמר שגרף הוא **אויילרי** אם הוא מכיל מעגל אויילר. כלומר, יש בו מעגל שעובר בכל **קשת** בדיוק פעם אחת. נסמן את שפת הגרפים האוילריים:

$$\mathrm{EC}=\{G\mid \text{בגרף } G \text{ יש מעגל אוילר}\}.$$

האם $\mathrm{EC}\in P$?

נזכיר כי קיים תנאי פשוט לבדיקה, שמאפשר לדעת אם גרף נתון מכיל מעגל אוילר: בגרף יש מעגל אוילר אם ורק אם כל דרגות הצמתים בו הן זוגיות. לפיכך, די לנו במעבר על כל הצמתים ובדיקה של מספר שכניהם. עוד נשים לב שבכל קידוד סביר של הגרף (למשל, מטריצת שכנויות, או רשימת קודקודים), ניתן לבצע את הנ"ל בזמן פולינומי. לעומת זאת, היכולת לבדוק את התנאי בזמן לינארי, או ריבועי, כבר תלויה בשיטת הקידוד המדויקת.

לפיכך, אכן מתקיים $\mathrm{EC}\in P$.

מעגל המילטון

נאמר שגרף הוא **המילטוני** אם הוא מכיל מעגל המילטון. כלומר, יש בו מעגל שעובר בכל **צומת** בדיוק פעם אחת. נסמן את שפת הגרפים ההמילטוניים:

$$\mathrm{HC}=\{G\mid \text{בגרף } G \text{ יש מעגל המילטון}\}.$$

האם $\mathrm{HC}\in P$?

נתחיל בטענה קלה יותר: $\mathrm{HC}\in\mathrm{R}$, מפני שאפשר לעבור על כל המעגלים האפשריים בגרף ולבדוק אם הם מתאימים. פורמאלית, נעבור על כל הסידורים של צמתי הגרף, $v_1,\ldots,v_n$, ולכל סידור כזה נבדוק אם לכל i מתקיים $(v_i,v_{i+1})\in E$, וכן כי $(v_n,v_1)\in E$. אם מצאנו סידור שעונה על התנאי, הרי שמצאנו מעגל המילטוני.

הואיל וקידוד הגרף מכיל את כל הצמתים והקשתות, נניח שגודל הקלט לפחות כמספר הצמתים בגרף, n. אמנם אפשר לקודד את מספר הצמתים ב־$\log n$ ביטים בלבד, הרי שלרוב נצטרך לקודד את הקשתות אחת אחת, ולכן זו הנחה סבירה.

לרוע המזל, בדיקה של כל $n!$ הסידורים תיקח זמן שאינו פולינומי בגודל הקלט (למשל, קל להווכח כי $n!>(n/2)^{n/2}>2^n$ מעיון ב־$n/2$ האברים הגדולים במכפלה המוגדרת על־ידי $n!$), ולכן, שיטה זו לא תצלח כדי להוכיח ש־$\mathrm{HC}\in P$. כפי שנראה בהמשך הקורס, פתרון בעיה זו שקול לבעיה הפתוחה החשובה ביותר שנראה בקורס כולו – האם $P=NP$?

אי־דטרמיניזם - תזכורת

מכונת טיורינג א"ד הינה מכונת טיורינג רגילה למעט כך שפונקציית המעברים שלה מוגדרת באופן הבא:

δ:Q\F×Γ $\rightarrow (Q \times \Gamma \times \{R, L, S\})^2$. זאת אומרת שבכל שלב נתון יש למכונה שתי אפשרויות כיצד להתקדם.

נוח לחשוב על החישוב שמכונה כזאת מבצעת כ**עץ חישוב בינארי**, שבו השורש מייצג את הקונפיגורציה ההתחלתית של המכונה וכל מסלול מהשורש לעלה מייצג חישוב אפשרי של המכונה עד הגעה למצב למסיים. נשים לב שיכולים להיות מסלולים אין־סופיים (עץ החישוב הוא לאו דווקא סופי).

אנו נדבר על מ"ט א"ד בהקשר של קבלת שפות, ולכן צריך להגדיר מתי מכונה כזאת מקבלת קלט. נגדיר ש**מ"ט א"ד *מקבלת*** את הקלט w אם **קיים** מסלול חישוב שמסתיים במצב מקבל. נגדיר את השפה $L(M)$ של מ"ט א"ד M להיות אוסף הקלטים אותו היא מקבלת.

אי־דטרמיניזם ו־NP

ההקשר שבו המודל האי־דטרמיניסטי שונה באופן בולט מהמודל הדטרמיניסטי הוא דווקא העולם המוגבל חישובית.

נאמר שלמ"ט א"ד M יש חסם זמן ריצה $f(n)$ אם לכל קלט w מספר צעדי החישוב של M **בכל ריצה אפשרית** על w הוא $f(|w|)$ לכל היותר.

נאמר שמ"ט א"ד היא **פולינומית** אם קיים לה חסם זמן ריצה שהוא פולינום. נסמן (באופן זמני) ב־NP' את מחלקת השפות שניתנות לקבלה על־ידי מ"ט א"ד בזמן פולינומי.

נתחיל בלהראות שמכונות א"ד פולינומיות מסוגלות להכריע שפות שאיננו יודעים אם הן ב־P (תזכורת: P היא מחלקת השפות הניתנות להכרעה על ידי מ"ט דטר' פולי').

כאמור, HC היא שפה שאיננו יודעים אם היא ב־P, אך סבורים שהיא איננה ב־P. נוכיח כי $\text{HC} \in NP'$.

נראה מכונה א"ד פולינומית M המכריעה שפה זו: על קלט G, המכונה תנחש סידור (יחיד!) של n צמתים ותבדוק האם הניחוש יוצר מסלול המילטוני.

אם ב־G מעגל המילטוני אז הוא ניתן לתיאור כסידור של הצמתים, ובמסלול החישוב בו M תנחש סידור זה הבדיקה תעבור בהצלחה ו־G יתקבל. לכן **קיים** ל־M מסלול חישוב מקבל עבור G, ו־$G \in L(M)$.

אם ב־G אין מעגל המילטוני אז **שום מסלול חישוב** לא יוביל למצב מקבל ולכן $G \notin L(M)$.

נשאר לטעון שמכונה זו היא פולינומית. אורך המעגל שצריך לנחש הוא לינארי. צריך לבדוק האם הצמתים שניחשנו שונים זה מזה, ושבין כל שני צמתים עוקבים בסידור קיימת קשת. שתי הבדיקות הללו ניתנות לביצוע בזמן פולינומי, ולכן המכונה פולינומית, ו־$\text{HC} \in NP'$.

המחלקה NP

נזכיר את המחלקה NP, אותה ראינו בהרצאות.

נאמר כי $L \in NP$ אם קיים יחס R_L שהוא:

1. חסום פולינומית (כלומר קיים פולינום P שלכל $(x,y) \in R_L$ מתקיים $|y| < P(|x|)$).
2. ניתן להכרעה פולינומית (כלומר בהנתן זוג (x,y) אפשר להכריע בזמן פולינומי אם $(x,y) \in R_L$).
3. מקיים שלכל $x \in \Sigma^*$ מתקיים: $x \in L \iff \exists y : (x,y) \in R_L$.

תחת הגדרה זו, לא קשה להווכח כי $\text{HC} \in NP$ - נגדיר עבורה את היחס

$$R_{\text{HC}} = \{(G,C) \mid G \text{ הוא מסלול המילטוני בגרף } C\}.$$

אורך מעגל המילטוני הוא מספר הצמתים בגרף, לכן היחס חסום פולינומית. בדיקה שסדרה של הצמתים היא אכן סידור שלהם, ושיש קשת בין כל שני צמתים עוקבים ניתנות להעשות בזמן פולינומי, ולכן היחס ניתן להכרעה פולינומית. לבסוף, $G \in \text{HC}$ אם ורק אם קיים בו מעגל המילטוני C.

הוכחנו כי $\text{HC} \in NP$.

הגדרה שקולה ל־NP באמצעות אי־דטרמיניזם

ראינו כי $\mathrm{HC} \in NP$ וכן כי $\mathrm{HC} \in NP'$. נראה כעת כי זהו אינו צירוף מקרים: נוכיח כי $NP = NP'$.

נתחיל בלהראות שלכל שפה ב־NP יש מ"ט א"ד פולינומית.

אם $L \in NP$ אז קיים יחס R_L שהוא חסום פולינומית, ניתן להכרעה פולינומית ומקיים שלכל x:
$x \in L \iff \exists y : (x, y) \in R_L$. תהי M_R מכונה פולינומית דטר' המכריעה את היחס R_L, ויהי $P : \mathbb{N} \to \mathbb{N}$ הפולינום החוסם את היחס – פולינום שקיומו מובטח מכך שהיחס חסום פולינומית.

נגדיר את M להיות מ"ט א"ד שעל קלט x:

1. מנחשת מחרוזת אקראית y באורך של עד $P(|x|)$ ביטים.
2. מריצה את M_R על (x,y) ועונה כמוה.

אם $x \in L$ אז קיים y באורך של עד $P(|x|)$ כך ש $(x, y) \in R_L$, ולכן קיים מסלול חישוב שבו M מנחשת y זה. במסלול חישוב זה M_R תקבל את (x,y) ולכן M תקבל את x ו־$x \in L(M)$.

אם $x \notin L$ אז לכל y באורך של עד $P(|x|)$ מתקיים $(x, y) \notin R_L$, ולכן בכל מסלול חישוב M תנחש y, ו־M_R תדחה את (x, y). לכן, בכל מסלול חישוב M תדחה את x ו־$x \notin L(M)$.

M מקבלת כקלט x ומנחשת מחרוזת באורך פולינומי y, ולאחר מכן היא מסמלצת את M_R לזמן שהוא פולינומי ב־$|(x, y)|$ – הקלט ל־M_R. אבל $|(x, y)|$ פולינומי ב־x (אורכו לכל היותר $|x| + P(|x|) + c$), הרכבת פולינומים נותנת פולינום, ולכן הסימולציה של ריצת M_R על (x, y) עורכת זמן פולינומי ב־$|x|$ ו־M כולה רצה זמן פולינומי ב־$|x|$.

נעבור לכיוון השני בהוכחה. נתונה לנו שפה L הניתנת להכרעה על־ידי מ"ט א"ד פולינומית. כלומר, קיימת מ"ט א"ד פולינומית M עם $L = L(M)$ שזמן ריצתה חסום בפולינום P, ונרצה להראות יחס המקיים את כל הדרישות עבור $L(M)$.

כזכור, אפשר לקודד מסלול חישוב של מ"ט א"ד כמחרוזת. נגדיר את היחס R_L להיות כל הזוגות (x, y) כך ש־M מגיעה למצב מקבל כשהיא רצה על x עם מסלול חישוב y, ו־$|y| \leq P(|x|)$.

הדרישה על אורך y מבטיחה שהיחס חסום פולינומית. הוא ניתן להכרעה פולינומית באמצעות המכונה הבאה.

M' על קלט (x, y):

1. אם $|y| > P(|x|)$, דוחה.
2. מריצה את M על x עם מסלול החישוב y.
3. אם M קיבלה, מקבלת, ואחרת דוחה.

נשים לב ש־M' רצה זמן פולינומי, ולכן R_L ניתן להכרעה פולינומית.

אם $x \in L(M)$ אז קיים מסלול חישוב מקבל, y, באורך של עד $P(|x|)$ ולכן $(x, y) \in R_L$.

אם $x \notin L(M)$ אז לכל מסלול חישוב y באורך $P(|x|)$ לכל היותר, M תדחה את x. לכן לכל y מתקיים $(x, y) \notin R_L$.

ולכן $x \in L \iff \exists y : (x, y) \in R_L$.

הוכחנו $L \in NP$.

דוגמה: COMPOSITE

נזכיר כי בעבר הגדרנו את שפת המספרים הפריקים:

$$\text{COMPOSITE} = \{n \in \mathbb{N} \mid \text{פריק } n\}.$$

נשים לב כי גודל הקידוד של n הוא $\log n$, ולכן נתעניין כאן במכונות טיורינג שרצות בזמן פולינומי ב־$\log n$.

נראה כעת כי $\text{COMPOSITE} \in NP$, בשתי דרכים.

- נגדיר יחס $R_{\text{COMPOSITE}} = \{(n,d) \in \mathbb{N} \times \mathbb{N} \mid 1 < d < n \text{ ו־} n \text{ מחלק את } d\}$.

1. היחס חסום פולינומית, כי $d < n$, ולכן קידוד d אינו גדול מקידוד n ($\log d \leq \log n$).
2. היחס ניתן להכרעה פולינומית, כי אנחנו יודעים לחלק מספרים טבעיים ביעילות ולבדוק אם יש שארית.
3. $n \in \text{COMPOSITE} \iff$ קיים $1 < d < n$ המחלק את n ללא שארית $\iff \exists d : (n,d) \in R_{\text{COMPOSITE}}$.

- נגדיר מ"ט א"ד: M תנחש מספר טבעי d, $1 < d < n$, ואם d מחלק את n תקבל, ואחרת תדחה.
  - המכונה פולינומית, כי ניתן לנחש d ולבדוק חלוקה בזמן פולינומי.
  - אם $n \in \text{COMPOSITE}$ אז יש d המחלק אותו, ולכן קיימת ריצה של M בה היא מנחשת את d ומקבלת.
  - אם $n \notin \text{COMPOSITE}$ אז אין לו מחלק d בתחום, ולכן אין ל־M מסלול מקבל.

הערות לסיום

$\textbf{PRIMES} \in P$

שפת המספרים הראשוניים, PRIMES, היא המשלימה ל־COMPOSITE.

אפשר להראות כי מתקיים גם $\text{PRIMES} \in NP$, בכלים של תורת החבורות[1]. עם זאת, נשים לב כי הטענות $\text{PRIMES} \in NP$, $\text{COMPOSITE} = \overline{\text{PRIMES}} \in NP$ לבדן אינן גוררות כי $\text{PRIMES} \in P$ (שכנעו עצמכם בכך!).

למעשה, מתקיים $\text{PRIMES} \in P$, אך הדבר לא קל להוכחה, וטענה זו הוכחה רק בשנת 2002 (!). הואיל ו־P סגורה למשלים (מדוע?) גם השפה המשלימה, COMPOSITE, שייכת ל־P.

היחס FACTOR

נעיין ביחס

$$\text{FACTOR} = \{(n,p) \in \mathbb{N} \times \mathbb{N} \mid 1 < p < n \text{ ו־} n \text{ מחלק את } p\}.$$

היחס ניתן ל**זיהוי יעיל**, באמצעים שהזכרנו כבר – חלוקה עם שארית.

האם הוא ניתן ל**חיפוש יעיל**? כלומר, בהנתן n, האם אפשר למצוא בזמן פולינומי p המחלק אותו או לדעת כי אין כזה? נשים לב כי לו היינו יודעים לפתור את בעיית החיפוש הזו, היינו יודעים גם להכריע את PRIMES (וכפועל יוצא מכך, את COMPOSITE).

לעומת זאת, אנחנו לא יודעים על גרירה הפוכה – כיום ידוע ש־$\text{PRIMES} \in P$, אולם השאלה האם היחס FACTOR ניתן לחיפוש יעיל נותרה פתוחה.

[1] ההוכחה חורגת מתחומו של קורס זה, אולם נביא אותה כאן בקווים כלליים, למעוניינים.
n אי־זוגי הוא ראשוני או חזקה של ראשוני אם"ם החבורה $(\mathbb{Z}n/\mathbb{Z})^*$ היא ציקלית, כלומר יש לה יוצר. לכאורה, היחס המתאים הוא (n,g) כאשר g יוצר של $(\mathbb{Z}n/\mathbb{Z})^*$.
בדיקה ש־n אי־זוגי קלה לביצוע. בדיקה שאינו חזקה של מספר טבעי פשוטה גם היא: נוציא שורש מסדר $2, 3, \ldots, \log n$ ל־n, ונוודא שאף אחד מהשורשים אינו שלם.
אולם, לא ברור כיצד ניתן לוודא יחס זה בזמן פולינומי – איך מודאים ש־g יוצר? כדי לוודא זאת, יש לבדוק ראשית ש־$g^{n-1} \equiv 1$, ובנוסף כי $g^{(n-1)/p_i} \not\equiv 1$ לכל p_i ראשוני שמחלק את $n-1$. לכן, היחס האמיתי צריך להכיל גם את המחלקים של $n-1$, והוכחות שהם ראשוניים; הוכחות אלו יכילו מחלקים ראשוניים קטנים יותר, וחוזר חלילה. לכן, היחס יכיל זוגות מהצורה (n,a) כאשר a מחזורת שמקודדת את g, את הראשוניים p_i שמחלקים את $n-1$, לכל p_i כזה a_i דומה שמוכיח שהוא ראשוני, ובתוך כל a_i ראשוניים קטנים יותר והוכחות ראשוניות עבורם. אפשר להראות שאורך a באמת פולינומי, כי p_i קטנים ביחס ל־n ומספרם קטן.