15. NP-שלמות של בעיות סיפוק נוסחאות בתחשיב הפסוקים

בפרק הקודם הגדרנו קבוצת שפות, השפות ה **NP**-שלמות, שסיבוכיות זיהוין קשורה באופן הדוק בשאלה "האם **P** = **NP**?". נחזור ונזכיר כי לשפה L שהינה **NP**-שלמה, מתקיים $L \in$ **P** אם ורק אם **P** = **NP** (ובהיפוך לוגי שקול, $L \notin$ **P** אם ורק אם **P** ≠ **NP**). בסיום הפרק הקודם, ראינו כי אמנם קיימות שפות כאלה ובפרט השפה BH הינה **NP**-שלמה. השפה BH, הינה שפה המוגדרת באופן ברור כ"קשורה" בבעיה הנובעת ממושג החישוב (הבעיה הינה, "האם למכונת טיורינג לא-דטרמיניסטית נתונה, יש חישוב העוצר תוך מספר נתון של צעדים?").

האם קיימות שפות **NP**-שלמות שאינן "קשורות באופן כה הדוק למושג החישוב"? שים לב כי השאלה הינה למעשה חסרת שחר, משום שלא ברור כלל כי ניתן לנסחה. למרות זאת, שאלה זו עולה בראשנו ואנו מעוניינים לענות עליה. העובדה ששאלה הינה חסרת שחר (כלומר, אינה ניתנת כלל לניסוח מדויק) אינה הופכת אותה למעניינת פחות (אלא בדרך כלל להיפך...).

בהמשך נראה שורה של בעיות **NP**-שלמות, שאינן נראות כה קשורות למושג החישוב. בפרק זה נראה את הראשונה בינהן. נציג בעיה העוסקת בסיפוק של נוסחאות בתחשיב הפסוקים. בהנתן פסוק כזה, אנו מתבקשים לקבוע האם קיימת לו הצבה מספקת (כלומר, האם קיימת הצבה של ערכי אמת למשתנים, כך שערך הפסוק הינו True). משמעות העובדה שבעיית סיפוק זו הינה **NP**-שלמה, היא שתחת ההנחה ש- **P** ≠ **NP**, לא קיים אלגוריתם יעיל (כלומר, מכונת טיורינג פולינומיאלית) המכריע האם לפסוק נתון ישנה הצבה מספקת. כפי שנראה, עובדה זו נשארת בעינה אפילו אם הפסוק נתון תמיד בצורה הנורמלית CNF.

ראשית נבצע חזרה קלה על חומר שאמור להיות מוכר מקורס בלוגיקה.

<u>הגדרה 15.1</u> (פסוק בצורה CNF):

* הסימנים $x_1, x_2, \cdots$ יקראו **משתנים**.
* יהי x_i משתנה, אז x_i וגם $\overline{x_i}$ הם **ליטראלים**.
* יהיו $l_1, \ldots, l_t$ ליטראלים, אז $l_1 \vee l_2 \vee \cdots \vee l_t$ (מסומן גם, $\bigvee_{i=1}^{t} l_i$) נקרא **פסוקית** (clause).
* תהינה $C_1, \ldots, C_m$ פסוקיות, אז $C_1 \wedge C_2 \wedge \cdots \wedge C_m$ (מסומן גם, $\bigwedge_{i=1}^{m} C_i$) נקרא **פסוק בצורה** CNF (Conjunctive Normal Form).

<u>הגדרה 15.2</u> (הצבת אמת וערך פסוק): תהי $X = \{x_1, x_2, \cdots\}$ קבוצת משתנים.

* הפונקציה, $\tau : X \to \{\mathrm{F},\mathrm{T}\}$, נקראת **הצבת ערכי אמת**. הפונקציה מציבה לכל משתנה את הערך T (יקרא אמת, בלעז True) או F (יקרא שקר, בלעז False).

* **הערך של הליטראל** x_i **תחת ההצבה** τ, זהה לערך שמציבה ההצבה τ למשתנה x_i (כלומר, זהה ל-$\tau(x_i)$) ואילו **הערך של הליטרל** $\overline{x_i}$ **תחת ההצבה** τ, הינו המשלים של הערך שמציבה ההצבה τ למשתנה x_i (כלומר, $\tau(\overline{x_i}) \in \{\mathrm{T},\mathrm{F}\} \setminus \{\tau(x_i)\}$).

* **הערך של הפסוקית** $C = l_1 \vee \cdots \vee l_t$ **תחת ההצבה** τ, הינו T אם ורק אם קיים i, כך שערך הליטראל l_i תחת ההצבה τ, הינו T (אם לא קיים i כזה, אז ערך הפסוקית הינו F).

* **הערך של הפסוק** $\bigwedge_{j=1}^{m} C_j$ תחת ההצבה τ, הינו T אם ורק אם לכל j, ערך הפסוקית C_j תחת ההצבה τ, הינו T (אחרת, ערך הפסוק הינו F).

<u>הגדרה 15.3</u> (הבעיה *SAT*): בהנתן פסוק ϕ בצורה *CNF*, האם קיימת לפסוק ϕ הצבה מספקת (כלומר, האם קיימת פונקציה, $\tau : X \to \{\mathrm{T},\mathrm{F}\}$, כך שהערך של ϕ תחת ההצבה τ, הינו T)?

הגדרה 15.3 מציגה את *SAT* כבעיית הכרעה המתייחסת לקלטים העונים על אפיון מסוים (במקרה זה, פסוקים בצורה *CNF*). לעומת זאת, כל הפיתוח הפורמלי שלנו (לגבי המחלקות **P** ו-**NP**) נעשה במונחים של שפות. תרגום של בעית הכרעה לשפה הינו טריביאלי כאשר הקלט הינו מחרוזת כלשהי, אך לא ברור איך לטפל בבעיות הכרעה שהקלט שלהם עונה לאפיון מסוים. למעשה כבר נתקלנו בשאלה זו, בבעית העצירה למשל, ופתרנו אותה ע"י שהנחנו כפיקציה כי כל מחרוזת מתארת קלט העונה לאפיון (כלומר, במקרה של בעית העצירה, כל מחרוזת מתארת מכונה כלשהי). אנו נאמץ פתרון זה גם כאן וכן גם בהמשך. הדרך הפשוטה ביותר לעשות זאת, היא להניח (או לקבוע) קידוד סטנדרטי קבוע של קלטים העונים לאפיון הדרוש (במקרה שלנו, פסוק בצורה *CNF*) ולזהות מחרוזות שאינן קידוד של קלט כזה, כמקודדות קלט חוקי מסויים הנקבע באופן שרירותי. בדוגמא שלפנינו, אפשר להשתמש בקידוד הסטנדרטי הבא של נוסחאות בתחשיב הפסוקים. בשלב ראשון, נניח כי הנוסחאות יקודדו ע"י מחרוזות מעל הא"ב, $\Sigma = X \cup \overline{X} \cup \{\wedge,\vee,(,)\}$ (בשלב שני, נקודד את הא"ב האינסופי הזה ע"י מחרוזות בינאריות). ברור שלא כל מילה מעל הא"ב Σ הינה פסוק, וודאי לא בצורה *CNF*. לדוגמא: המילה $(\overline{x}_3) \wedge (x_1 \vee x_2)$ הינה פסוק בצורה *CNF*, המילה $(x_3 \wedge x_4) \vee x_5$ אינה פסוק בצורה *CNF* ואילו המילה $(\vee x_4) \wedge x_5 x_3$ איננה פסוק כלל. אנו נפרש מחרוזות מעל Σ שאינן מקודדות פסוקי *CNF*, כמקודדות את הפסוק הריק (זו בחירה שרירותית ובאותו אופן יכולנו לפרש מחרוזות אלו, כמקודדות את הפסוק $(x_1 \vee x_2)$). כמו כן, נסכים כי הפסוק הריק אינו ניתן לסיפוק (כלומר, אין השמת ערכי אמת הנותנת לו ערך T). שים לב כי הפרשנות הנ"ל היא פיקציה שתפקידה לאפשר לנו לדון בבעיות הכרעה דרך הטרמינולוגיה של שפות. חשוב לציין כי קל לזהות האם מחרוזת נתונה אינה קידוד נכון של פסוק בצורה *CNF* (ולכן מקודדת את הפסוק הריק) כך שהרחבת הבעיה *SAT* בצורה שהיא מוגדרת על כל מחרוזת, אינה הופכת אותה ל"קשה יותר".

15.1 משפט Cook

משפט 15.1 (Cook): השפה SAT הינה **NP**-שלמה.

טענה 15.1: $SAT \in \mathbf{NP}$.

הוכחה: נציג יחס דו-מקומי המאפיין את SAT. היחס, שיסומן R_{SAT}, מורכב מזוגות (ϕ,τ), כך שלפסוק ϕ יש ערך T תחת הצבת האמת τ. שים לב כי די להגדיר את ההצבה τ רק עבור המשתנים המופיעים בפסוק ϕ. לפיכך, אורך הייצוג של τ אינו עולה על אורך הייצוג של ϕ (כלומר, אורך העדות לינארי באורך הקלט). ודא כי היחס, R_{SAT}, ניתן לזיהוי בזמן פולינומיאלי (כלומר, בהנתן זוג, (ϕ,τ), קל לבדוק האם לפסוק ϕ יש ערך אמת T תחת ההצבה τ) וכי $\phi \in SAT$ אם ורק אם קיימת הצבה, τ, כך ש- $(\phi,\tau) \in R_{SAT}$.

טענה 15.2: לכל שפה $L \in \mathbf{NP}$, קיימת רדוקציה פולינומיאלית מהשפה L לשפה SAT.

הוכחה: תהא $L \in \mathbf{NP}$, תהא M_L, מכונת טיורינג פולינומיאלית ולא-דטרמיניסטית המקבלת את L, שקיומה מובטח מהיות $L \in \mathbf{NP}$, ויהא P_L פולינום החוסם את זמן ריצתה של M_L. נציג רדוקציה (ע"י העתקה) f_L, מהשפה L לשפה SAT. הרדוקציה ממפה קלטים עבור הבעיה L, אל קלטים לבעיה SAT (כלומר, פסוקים). במהלך כל ההוכחה נניח ללא הגבלת הכלליות, כי למכונה האי-דטרמיניסטית, M_L, דרגת אי-דטרמיניזם 2 והיא אינה נופלת לעולם מן הסרט (לכל שפה $L \in \mathbf{NP}$ יש מכונה כזאת). הרדוקציה (כלומר, הפונקציה f_L) צריכה לקיים שני תנאים:

(1) הפונקציה, f_L, ניתנת לחישוב בזמן פולינומיאלי.

(2) $x \in L$ אמם $f_L(x) \in SAT$.

להלן רעיון הבניה. נתבונן בחישוב אפשרי של M_L על קלט x. חישוב כזה, ארכו לכל היותר $P_L(|x|)$ צעדים ולפיכך סורק לכל היותר $P_L(|x|)$ משבצות של הסרט של M_L. נתבונן במטריצה בגודל $P_L(|x|) \times P_L(|x|)$, ששורותיה מתאימות לקונפיגורציות החישוב של M_L על הקלט x, ועמודותיה מתאימות לתאים על הסרט של המכונה M_L. ביתר פרוט, השורה ה i-ית במטריצה, מתאימה לקונפיגורציה ה i-ית של המכונה M_L (על הקלט x), העמודה ה j-ית מתאימה לתא ה j-י בסרט, והכניסה ה-(i,j) במטריצה, מתאימה לתוכן התא ה j-י בקונפיגורציה ה i-ית. הזכר כי הסתכלנו במטריצה דומה בפרק 11 (בסעיף על Tiling). שים לב כי (בניגוד לפרק 11 כאן) ישנם מספר חישובים אפשריים של המכונה הלא-דטרמיניסטית, M_L, על הקלט x, ולכל חישוב כזה מתאימה מטריצה אחת ויחידה. כל אחת מהמטריצות הנ"ל מקיימת מספר אילוצים, כגון שכל שתי שורות עוקבות שונות לכל היותר בכניסה אחת בלבד (העמודה המתיחסת למקום הראש). רעיון הרדוקציה, הוא להתאים לכל כניסה במטריצה משתנים אשר יתארו את תוכן הכניסה ולהכריח את המשתנים הללו להתאים למטריצה אפשרית של חישוב (של M_L על x) ע"י כתיבת פסוק שסיפוקו מחייב ערכי משתנים הממלאים את כל התנאים המתקיימים במטריצת החישוב. בנקודה זו

אינך אמור עדיין להבין את הבניה. כל מה שנכתב עד כה הוא אינטואיציה לא מחייבת שעשויה להועיל בהמשך.

<u>תיאור הרדוקציה</u> (משפה $L \in \mathbf{NP}$ אל השפה SAT): קלט הרדוקציה הינו x ואילו הפלט הוא $f_L(x)$ שיתואר להלן. נשתמש בסימונים M_L ו-P_L כמתואר לעי"ל וכן $m \triangleq P_L(|x|)$. הפסוק, $f_L(x)$, יכיל את המשתנים הבאים (בסוגריים תאור לא מחייב של "תפקיד" המשתנים בפסוק):

(1) לכל $1 \le i,j \le m$ ולכל $\sigma \in \Gamma$ (Γ הוא א"ב העבודה של M_L) יותאם משתנה $b_{i,j,\sigma}$ (קבוצת המשתנים, $\{b_{i,j,\sigma}\}_{\sigma \in \Gamma}$, תקודד את תוכן התא ה-$j$-י בקונפיגורציה ה-$i$-ית. קידוד העובדה שתוכן התא ה-(i,j) הוא האות σ, יעשה ע"י $b_{i,j,\sigma} = \mathrm{T}$ ולכל $\tau \neq \sigma$ יתקיים $b_{i,j,\tau} = \mathrm{F}$. זהו קידוד אונרי לא חסכוני, אך זה נוח לנו וחסכון בקבוע אינו מעניין אותנו).

(2) לכל $1 \le i \le m$ ולכל $q \in Q$ (Q היא קבוצת המשתנים של M_L) נתאים משתנה $s_{i,q}$ (קבוצת המשתנים, $\{s_{i,q}\}_{q \in Q}$, תקודד את מצב המכונה, M_L, בקונפיגורציה ה-i-ית. $s_{i,q} = \mathrm{T}$ אמם בקונפיגורציה ה-i-ית, מצב המכונה הינו q).

(3) לכל $1 \le i,j \le m$, נתאים משתנה $h_{i,j}$ (קבוצת המשתנים, $\{h_{i,j}\}_{j=1}^{m}$, תקודד את מיקום הראש של המכונה M_L, בקונפיגורציה ה-i-ית. $h_{i,j} = \mathrm{T}$ אמם בקונפיגורציה ה-i הראש נמצא בתא ה-j-י).

כעת, כאשר סיימנו את תיאור המשתנים שיופיעו בנוסחא $f_L(x)$, הגיע הזמן לתאר את הנוסחא עצמה. להלן תיאור "כללי" של הנוסחא. הנוסחא תורכב מארבע תתי-נוסחאות בצורה CNF שסימני "Λ" בינהן. תת-הנוסחא הראשונה "תכריח" את המשתנים עם אינדקס i, להתאים לקונפיגורציה (בפרט, לכל i,j בדיוק אחד מן ה-$b_{i,j,\sigma}$ יקבל ערך T, ולכל i, בדיוק אחד מן ה-$s_{i,q}$ ואחד מן ה-$h_{i,j}$ יקבל ערך T). תת-הנוסחא השניה "תכריח" את המשתנים עם אינדקס $i = 1$, להתאים לקונפיגורציה ההתחלתית של M_L על קלט x (בפרט, תוכן $|x|$ התאים הראשונים יהיה x, תוכן שאר התאים יהיה b והראש יהיה במצב q_0 בתא השמאלי ביותר). תת-הנוסחא השלישית "תדרוש" כי משתנה המצב עם סיום החישוב, יהיה במצב סופי מקבל (דבר שיבטיח כי סיפוק תת-הנוסחא, גורר קיום חישוב מקבל של M_L). תת-הנוסחא הרביעית "תכריח" את המשתנים בעלי אינדקסים עוקבים, להתאים לקונפיגורציות עוקבות של המכונה M_L על קלט x (ללא חלק זה, הנאמר בסוגריים לגבי תת-הנוסחא השלישית, אינו תקף).

<u>נוסחא I:</u> תת-הנוסחא הראשונה, Φ_1, תורכב מתתי-הנוסחאות הבאות:

- לכל $1 \le i,j \le m$, נכתוב פסוק,

$$\phi_{i,j}^{(1)} = \left(\bigvee_{\sigma \in \Gamma} b_{i,j,\sigma}\right) \wedge \left[\bigwedge_{\substack{\sigma,\tau \in \Gamma \\ \sigma \neq \tau}} \left(\overline{b}_{i,j,\sigma} \vee \overline{b}_{i,j,\tau}\right)\right]$$

החלק השמאלי של הפסוק (כלומר, $\bigvee_{\sigma \in \Gamma} b_{i,j,\sigma}$), דורש כי <u>לפחות</u> אחד מן המשתנים, $b_{i,j,\sigma}$ יהיה בעל ערך T ואילו החלק הימני דורש כי <u>לכל היותר</u> אחד מן המשתנים הללו יהיה בעל ערך T (ודא כי אם קיימים $\sigma \neq \tau$ כך ש- $b_{i,j,\sigma} = b_{i,j,\tau} = \mathrm{T}$, אז החלק הימני של $\phi_{i,j}^{(1)}$ אינו מסופק). $\phi_{i,j}^{(1)}$ בכללותה, "דואגת" לכך שהמשתנים

$\{b_{i,j,\sigma}\}_{\sigma\in\Gamma}$, "יקודדו" אות אחת ויחידה.

- לכל $1\le i\le m$ נכתוב פסוק,

$$\phi_i^{(2)} = \left(\bigvee_{q\in Q} s_{i,q}\right) \wedge \left[\bigwedge_{\substack{p,q\in Q\\ p\neq q}} \left(\overline{s}_{i,p} \vee \overline{s}_{i,q}\right)\right]$$

$\phi_i^{(2)}$ "דואגת" לכך שהמשתנים $\{s_{i,q}\}_{q\in Q}$, "יקודדו" מצב אחד ויחיד (השווה עם $\phi_{i,j}^{(1)}$).

- לכל $1\le i\le m$ נכתוב פסוק,

$$\phi_i^{(3)} = \left(\bigvee_{j=1}^{m} h_{i,j}\right) \wedge \left[\bigwedge_{\substack{1\le j,k\le m\\ j\neq k}} \left(\overline{h}_{i,j} \vee \overline{h}_{i,k}\right)\right]$$

$\phi_i^{(3)}$ דואג לכך שקבוצת המשתנים $\{h_{i,j}\}_{j=1}^{m}$, "תקודד" את מיקום הראש של המכונה, M_L, על גבי הסרט.

נכתוב,

$$\Phi_1(|x|) = \left(\bigwedge_{1\le i,j\le m} \phi_{i,j}^{(1)}\right) \wedge \left(\bigwedge_{1\le i\le m} \phi_i^{(2)}\right) \wedge \left(\bigwedge_{1\le i\le m} \phi_i^{(3)}\right)$$

$\Phi_1(|x|)$ בכללותו, מבטיח כי המשתנים "מקודדים" קונפיגורציות (כלשהן) של המכונה M_L. ודא את נכונות הטענות הבאות.

(1) $\Phi_1(|x|)$ הינו פסוק בצורה CNF.

(2) אורך המחרוזת $\Phi_1(|x|)$ הינו $O(m^3)$ (במה תלוי הקבוע המובלע בסימון O?).

(3) הנוסחא, $\Phi_1(|x|)$, תלויה רק במכונה M_L, בפולינום P_L ובאורך הקלט x, אך לא בקלט עצמו.

(4) קיימת מכונת טיורינג פולינומיאלית, אשר על קלט x, מחשבת את $\Phi_1(|x|)$ המתאים (רמז: המכונה "מכילה" את M_L ואת P_L ומחשבת תחילה את $m = P_L(|x|)$).

<u>נוסחא II:</u> תת-הנוסחא השניה, Φ_2, "תבטיח" כי קבוצת המשתנים,

$$\{b_{1,j,\sigma}\} \bigcup \{s_{1,q}\} \bigcup \{h_{1,j}\}$$

תקודד את הקונפיגורציה ההתחלתית של המכונה M_L על קלט x. יהי $x = \sigma_1 \cdots \sigma_n$ (כאשר $\sigma_j \in \Sigma$, היא אות א"ב קלט). נכתוב,

$$\Phi_2(x) = h_{1,1} \wedge s_{1,q_0} \wedge \left(\bigwedge_{1\le j\le n} b_{1,j,\sigma_j}\right) \wedge \left(\bigwedge_{n<j\le m} b_{1,j,\not b}\right)$$

$h_{1,1}$, מבטיח כי בקונפיגורציה ההתחלתית הראש נמצא בתא הראשון. s_{1,q_0}, מבטיח כי M_L נמצאת במצב ההתחלתי. החלק השלישי של $\Phi_2(x)$, מבטיח כי תוכן $|x| = n$ התאים הראשונים זהה ל-x. החלק הרביעי של $\Phi_2(x)$, מבטיח כי תוכן שאר התאים הינו $\not b$). ודא כי קיימת מכונת טיורינג פולינומיאלית, אשר על קלט x מחשבת את $\Phi_2(x)$. שים לב כי $\Phi_2(x)$, הינה תת-הנוסחא היחידה של הפסוק $f_L(x)$, אשר תלויה במחרוזת הקלט x עצמה

ולא רק בארכה.

<u>נוסחא III:</u> תת-הנוסחא השלישית, Φ_3, "תבטיח" כי המכונה M_L, נמצאת בסיום החישוב בקונפיגורציה מקבלת. יהי q_{ACC}, המצב המקבל של המכונה M_L. נכתוב,

$$\Phi_3(|x|) = \bigvee_{1 \le i \le m} s_{i,q_{ACC}}.$$

ודא כי קיימת מכונת טיורינג פולינומיאלית, אשר על קלט x מחשבת את $\Phi_3(|x|)$.

<u>נוסחא IV:</u> תת-הנוסחא הרביעית, Φ_4, "תבטיח" כי "שורות משתנים עוקבות" אכן מתאימות לקונפיגורציות עוקבות של המכונה M_L. $\Phi_4(|x|)$, תורכב מ-m^2 תתי-נוסחאות, $\phi^{(4)}_{i,j}$ $(1 \le j \le m)$. תת-הנוסחא, $\phi^{(4)}_{i,j}$, תבטיח "התאמה" בין השורה ה-i-ית לשורה ה $i+1$-ית לגבי התאים $j-1, j$ ו-$j+1$. נכתוב,

$$\phi^{(4)}_{i,j} = (\overline{h}_{i,j} \to \phi^{(5)}_{i,j}) \wedge (h_{i,j} \to \phi^{(6)}_{i,j}).$$

כלומר, אם $\overline{h}_{i,j} = \mathrm{T}$ (הראש איננו בתא ה-j) אז חייבת להתקיים הנוסחא, $\phi^{(5)}_{i,j}$ (אשר תקודד אי-שינוי בתוכן התא ה-j) ואילו אם $h_{i,j} = \mathrm{T}$ (הראש הינו בתא ה-j) אז חייבת להתקיים הנוסחא $\phi^{(6)}_{i,j}$ (אשר תקודד שינוי אפשרי של תוכן התא ה-j, תזוזה של הראש ושינוי המצב, בהתאם לפונקצית המעברים של המכונה M_L). שים לב כי הנוסחא, $\phi^{(4)}_{i,j}$ מכילה קשר שאינו בקבוצה $\{\wedge,\vee\}$, ובפרט $\phi^{(4)}_{i,j}$ אינה בצורה CNF (בענין זה נטפל בהמשך). הנוסחא, $\phi^{(5)}_{i,j}$, קלה לתיאור.

$$\phi^{(5)}_{i,j} = \bigwedge_{\sigma \in \Gamma} (b_{i,j,\sigma} = b_{i+1,j,\sigma})$$

תת-הנוסחא, $\phi^{(5)}_{i,j}$, "מחייבת" שתוכן התא ה-j אינו משתנה במעבר זה. לצורך תיאור הנוסחא $\phi^{(6)}_{i,j}$, נציג תחילה מספר סימונים. זכור כי ללא הגבלת הכלליות, לכל (q,σ) מתקיים, $|\delta(q,\sigma)| \le 2$ (דרגת אי-דטרמיניזם 2). ראשית, עבור כל זוג, (q,σ) עבורו הפונקציה δ אינה מוגדרת נסמן $\delta(q,\sigma) = (q,\sigma,S)$. כעת, נסמן ע"י $\delta_1(q,\sigma)$, את האפשרות הראשונה ב-$\delta(q,\sigma)$ וע"י $\delta_2(q,\sigma)$ את האפשרות השניה (באם אינה קיימת, נניח $\delta_2(q,\sigma) = \delta_1(q,\sigma)$). כלומר, $\delta_1(q,\sigma), \delta_2(q,\sigma) \in Q \times \Gamma \times \{-1,0,+1\}$ (שים לב כי קודדנו תנועה שמאלה, דריכה במקום ותנועה ימינה, ע"י $-1,0,+1$ בהתאמה) וכן מתקיים, $\delta(q,\sigma) = \{\delta_1(q,\sigma), \delta_2(q,\sigma)\}$. כעת, לכל $k \in \{1,2\}$, נסמן את אברי השלישיה, $\delta_k(q,\sigma)$, ע"י $p_k(q,\sigma), \tau_k(q,\sigma), t_k(q,\sigma)$ בהתאמה. כלומר, לכל $1 \le k \le 2$, נסמן:

$$\delta_k(q,\sigma) = (p_k(q,\sigma), \tau_k(q,\sigma), t_k(q,\sigma)).$$

כעת נכתוב,

$$\phi^{(6)}_{i,j} = \bigwedge_{\substack{q \in Q-F \\ \sigma \in \Gamma}} \left\{ (b_{i,j,\sigma} \wedge s_{i,q}) \to \left[(b_{i+1,j,\tau_1(q,\sigma)} \wedge s_{i+1,p_1(q,\sigma)} \wedge h_{i+1,j+t_1(q,\sigma)}) \right.\right.$$

$$\left.\left. \vee\ (b_{i+1,j,\tau_2(q,\sigma)} \wedge s_{i+1,p_2(q,\sigma)} \wedge h_{i+1,j+t_2(q,\sigma)}) \right] \right\}$$

הנוסחא, $\phi_{i,j}^{(6)}$, מתארת את השינוי הנגרם בשורה ה $i+1$-ית, כאשר הראש נמצא בתא ה j-י, בשורה ה i-ית. שינוי זה תלוי בתוכן התא ה j-י ובמצב הראש בשורה ה i-ית. הנוסחא מחייבת, כי אם הזוג (תוכן תא, מצב) הינו (q,σ), אז בשורה ה $i+1$-ית, נעבור לתוכן תא, מצב ותזוזה, המתאימים בהתאמה ל- $\delta_1(q,\sigma)$ או ל- $\delta_2(q,\sigma)$. בכך סיימנו את כתיבת $\phi_{i,j}^{(4)}$. שים לב, כי הנוסחא $\phi_{i,j}^{(4)}$, איננה בצורה CNF. מצד שני, מספר המשתנים בנוסחא $\phi_{i,j}^{(4)}$, אינו תלוי באורך הקלט, x, אלא רק בקבועים של המכונה M_L (שים לב, כי ב-$\phi_{i,j}^{(4)}$, מופיעים לכל היותר $2|\Gamma|+2|Q|+3$ משתנים). לכן, קיימת נוסחא שקולה ל-$\phi_{i,j}^{(4)}$, שהיא בצורה CNF. נוסחא כזאת, אינה גדולה יותר מאשר 2^v, כאשר v הינו מספר המשתנים בנוסחא $\phi_{i,j}^{(4)}$. כלומר, קיימת נוסחא קבועה, $\phi_{i,j}^{(4')}$, בגודל קבוע (כלומר, גודלה אינו פונקציה של x, אלא תלוי ב- M_L בלבד), בצורה CNF, אשר שקולה לנוסחא $\phi_{i,j}^{(4)}$.

כעת נכתוב,

$$\Phi_4(|x|) = \bigwedge_{1\le i,j\le m} \phi_{i,j}^{(4')}$$

ולסיום נכתוב,

$$f_L(x) = \Phi_1(|x|) \wedge \Phi_2(x) \wedge \Phi_3(|x|) \wedge \Phi_4(|x|)$$

שים לב, כי $f_L(x)$ הינה נוסחא בצורה CNF וכי קיים אלגוריתם פולינומיאלי, המחשב את הפונקציה f_L.

כל ההסברים המילולים המתארים את חלקי הנוסחא $f_L(x)$, אינם מחיבים ואינם מהווים הוכחה לתקפות הרדוקציה (כלומר, לטענה "$x\in L$ אמם $f_L(x)\in SAT$"). הסברים אלו, מהוים רק מוטיבציה שמטרתה להקל על הבנת הבניה. בשלב זה, צריך להיות ברור מהי הפונקציה f_L (כלומר, איזה פסוק מתאימה f_L למחרוזת הקלט x) וכן צריך להיות ברור כי הפונקציה, f_L, ניתנת לחישוב בזמן פולינומיאלי. שוב נדגיש, כי הקלט הינו x, ולכן הכוונה ב"זמן פולינומיאלי" היא למספר צעדים חסום ע"י פולינום ב-x. השפה L, המכונה M_L והפולינום P_L, קבועים כאן ולפיכך כל גודל התלוי רק בהם הינו קבוע. בפרט, גודל קבוצת המצבים של M_L הינו קבוע, פונקצית המעברים של M_L הינה קבועה וכו'. מכונה המחשבת את f_L, יכולה להכיל את הקבועים הללו בתוכה.

נסכם שוב את מצבנו. תארנו פונקציה, f_L והשתכנענו בנכונות הטענה הבאה:

<u>טענת הפולינומיאליות:</u> הפונקציה f_L, ניתנת לחישוב בזמן פולינומיאלי.

נותר להוכיח:

<u>טענת תקפות:</u> לכל x מתקיים, $x\in L$ אם ורק אם $f_L(x)\in SAT$.

<u>סקיצה של הוכחה:</u> נניח תחילה, כי $x \in L$. קיים חישוב של M_L, אשר מקבל את x, תוך $P_L(|x|)$ צעדים לכל היותר. נסתכל בקונפיגורציות של חישוב זה, שיסומנו $\alpha_1,\alpha_2,\ldots,\alpha_t$ בהתאמה, כאשר $t \le m = P_L(|x|)$. נראה כעת, כי ישנה השמת אמת למשתנים של $f_L(x)$, כך שערך הנוסחא $f_L(x)$, הינו T. ההצבה תקבע על פי הקונפיגורציות של החישוב המקבל. יהי S_i, מצב המכונה בקונפיגורציה α_i, H_i מיקום הראש בקונפיגורציה α_i ו- $B_{i,j}$, תוכן התא ה j בקונפיגורציה α_i. כל מה שנחוץ, הוא לקבוע את ערכי המשתנים, $\{b_{i,j,\sigma}\}_\sigma,\{h_{i,j}\}_j,\{s_{i,q}\}_q$ בהתאם לערכים הנ"ל. כלומר, $s_{i,q}=\mathrm{T}$ אם $S_i=q$, וכן $h_{i,j}=\mathrm{T}$ אם $H_i=j$, ולבסוף $b_{i,j,\sigma}=\mathrm{T}$ אם $B_{i,j}=\sigma$ (לשאר המשתנים יושם ערך F). קל לודא כי ההצבה הזאת מספקת את הנוסחא $f_L(x)$. יש לעבור על הבניה ולודא כי כל אחת מהנוסחאות מסופקת ובפרט הנוסחאות של $\phi_{i,j}^{(1)}$, $\phi_{i,j}^{(2)}$, $\phi_{i,j}^{(3)}$, Φ_2, Φ_3 ולבסוף כל אחת מהנוסחאות $\phi_{i,j}^{(4)}$. ע"י כך הוכחנו כי מתוך $x \in L$ נובע $f_L(x) \in SAT$.

כעת נראה את הכיוון ההפוך. נניח כי $f_L(x) \in SAT$. יש להשתמש בכל תתי-הנוסחאות של Φ_1 על מנת לראות כי המשתנים של השורות מתאימים לקונפיגורציות. מתוך Φ_2, ניתן להסיק כי משתני השורה הראשונה מתאימים לקונפיגורציה ההתחלתית על קלט x. מתוך Φ_4, ניתן להסיק כי שורות עוקבות מתאימות לקונפיגורציות עוקבות ומתוך Φ_3, נסיק כי אחת מהשורות מתאימה לקונפיגורציה מקבלת. מכאן, שיש חישוב של M_L, אשר מקבל את x ומכך נובע $x \in L$ (הפרטים בהוכחת כיוון זה, מאד מייגעים ולפיכך בחרנו להשמיטם).

בכך תמה הוכחת טענת התקיפות. נובע כי לכל שפה $L \in \mathbf{NP}$, הפונקציה f_L היא אמנם רדוקציה מהשפה L אל השפה SAT ולכן טענה 15.2 (היות SAT שלמה ב-**NP**) נובעת. □

15.2 על אופן הוכחת טענת NP-שלמות לגבי שפה נתונה

נסכם את אשר נעשה בסעיף הקודם. רצינו להוכיח כי שפה מסוימת (SAT) הינה **NP**-שלמה. לשם כך היה עלינו להוכיח, כי השפה ב-**NP** (ראה טענה 15.1) וכן כי כל שפה ב-**NP**, ניתנת לרדוקציה אליה (טענה 15.2). ההוכחה הראשונה היתה קלה למדי (וכך יהיה בדרך כלל). בהוכחת הטענה השניה ביצענו את השלבים הבאים:

(1) הראינו לגבי כל שפה $L \in \mathbf{NP}$, רדוקציה פולינומיאלית מ- L לשפה שאנו עוסקים בה, שתסומן L_0 (במקרה זה $L_0 = SAT$). כלומר, תארנו העתקה של קלטים עבור הבעיה L, אל קלטים עבור הבעיה L_0.

(2) הוכחנו כי ההעתקה שהצגנו בסעיף (1), שסומנה f_L, אמנם ניתנת לחישוב בזמן פולינומיאלי.

(3) הראינו כי ההעתקה, f_L, אמנם תקפה. כלומר, הראינו כי לכל מחרוזת x, מתקיים, $x \in L$ אמם $f_L(x) \in L_0$. על מנת להראות זאת, צריך היה להראות כי הגרירה היא אמנם דו-כיוונית. הכיוון, "$x \in L$ גורר $f_L(x) \in L_0$", הוא בדרך כלל בעיתי פחות וזאת מסיבות "פסיכולוגיות". אנו בונים את ההעתקה f_L, בחושבנו על הבעיה L ומתוך כוונה שקלט $x \in L$ יועתק אמנם ל- $f_L(x) \in L_0$. מסיבות פסיכולוגיות וללא

כל הצדקה, אנו בדרך כלל נזהרים פחות לוודא שקלט $x \notin L$ יועתק ל- $f_L(x) \notin L_0$. או במילים אחרות, ש- $f_L(x) \in L_0$ גורר אמנם $x \in L$. לסיכום, זכור לוודא את שני הכיוונים בגרירה והיה "חשדן" במיוחד כלפי הכיוון השני (שים לב כי בתאור הבניה, הודגשו כל הזמן האלמנטים שיעזרו לכיוון הבעיתי).

הרדוקציה שהראנו במקרה של SAT נקראת **גנרית**. הסיבה לשם זה, היא שהרדוקציה היא למעשה סכימה כללית אשר מאפשרת להתאים רדוקציה מכל שפה $L \in$ **NP** אל השפה L_0 (במקרה הנ"ל SAT). אך איך אפשר אחרת (הרי זאת ההגדרה)?

ובכן ישנה אפשרות אחרת: אם כבר הוכח כי הבעיה L_0 (למשל SAT) הינה **NP**-שלמה, נוכל להראות כי בעיה $L_1 \in$ **NP** הינה **NP**-שלמה, ע"י רדוקציה פולינומיאלית מ-L_0 אל L_1. הטיעון התומך בטענה כזאת הוא כדלקמן:

תהא $L_1 \in$ **NP**.

(1) ידוע כי L_0 הינה **NP**-שלמה. כלומר, לכל $L \in$ **NP**, השפה L ניתנת לרדוקציה פולינומיאלית אל L_0.

(2) ננית כי ישנה רדוקציה מ-L_0 אל L_1.

מ-(1) ו-(2) נובע כי ישנה רדוקציה מכל שפה ב-**NP** אל L_1. מה שעומד מאחורי הטיעון, הוא שרדוקציות פולינומיאליות הינן טרנזיטיביות.

<u>תרגיל 15.1:</u> הראה כי אם השפה L_1 ניתנת לרדוקציה פולינומיאלית לשפה L_2 והשפה L_2 ניתנת לרדוקציה פולינומיאלית לשפה L_3, אז השפה L_1 ניתנת לרדוקציה פולינומיאלית לשפה L_3.

<u>סקיצת פתרון:</u> תהא f הרדוקציה מ-L_1 אל L_2 (כלומר, f חשיבה פולינומיאלית ומתקיים $x \in L_1$ אמם $f(x) \in L_2$) ותהא g הרדוקציה מ-L_2 אל L_3, אז הרכבת הפונקציות $h \triangleq g \circ f$ (כלומר הפונקציה $h(x) \triangleq g(f(x))$) הינה רדוקציה פולינומיאלית מ-L_1 אל L_3 (ודא כי h חשיבה פולינומיאלית וכי מתקיים, $x \in L_1$ אמם $h(x) \in L_3$).

<u>סימון:</u> אם שפה L_1 ניתנת לרדוקציה פולינומיאלית לשפה L_2, אז נסמן $L_1 \propto_p L_2$.

בעזרת הסימון נחזור על הדיון שקדם לתרגיל 15.1.

<u>תרגיל 15.2:</u> תהי L_0 שפה **NP**-שלמה. תהי L_1 שפה ב-**NP** כך ש- $L_0 \propto_p L_1$, אז גם L_1 הינה **NP**-שלמה.

<u>סקיצת פתרון:</u> נתון כי $L_1 \in$ **NP**, לכן על מנת להראות כי L_1 הינה **NP**-שלמה, נותר להראות כי לכל $L \in$ **NP** מתקיים $L \propto_p L_1$. מכיוון ש-L_0 הינה **NP**-שלמה, נובע כי לאותה שפה L מתקיים $L \propto_p L_0$. בשימוש בנתון $L_0 \propto_p L_1$ ובתרגיל 15.1, נקבל אמנם $L \propto_p L_1$.

אנו נשתמש במסקנות תרגיל 15.2 בכל הוכחות **NP**-שלמות שיבואו בעתיד. בהנתן שפה L_1, נראה תחילה כי $L_1 \in$ **NP**, אחר כך נבחר שפה L_0, שידועה לנו כ **NP**-שלמה (בינתיים המבחר שלנו אינו גדול...) ונראה כי $L_0 \propto_p L_1$ ובכך נסיים. נדגיש שוב, כי על מנת להוכיח $L_0 \propto_p L_1$, יש להראות מיפוי של קלטים עבור הבעיה L_0, אל קלטים עבור הבעיה L_1. המיפוי, שיסומן f, צריך לקיים:

(1) המיפוי f ניתן לחישוב בזמן פולינומיאלי.

(2) $x \in L_0$ אמם $f(x) \in L_1$.

<u>אזהרה חוזרת:</u> שים לב כי על מנת להראות ששפה $L_1 \in$ **NP** הינה **NP**-שלמה, כאשר ידוע כי השפה L_0 הינה **NP**-שלמה, יש להראות רדוקציה של L_0 אל L_1 $(L_0 \propto_p L_1)$ ולא את ההיפך $(L_1 \propto_p L_0)$. ההיפך, אגב, נכון ממילא מכיוון ש-L_0 הינה **NP**-שלמה.

15.3 NP-שלמות של 3SAT

הבעיה $3SAT$ הינה "צמצום" של SAT במובן הבא:

<u>הגדרה 15.4</u> (הבעיה $3SAT$): בהנתן פסוק ϕ בצורה $3CNF$ (כלומר, פסוק בצורה CNF המורכב מפסוקיות שכל אחת מהן מכילה <u>לכל היותר</u> שלושה ליטראלים) האם קיימת לפסוק ϕ הצבה מספקת (כלומר האם קיימת פונקציה, $\tau : X \to \{\mathrm{T},\mathrm{F}\}$, כך שהערך של ϕ תחת ההצבה τ, הינו T)?

שים לב, כי אנו נפרש כל מחרוזת קלט, כפסוק CNF שכל אחת מפסוקיותיו מכילה שלושה ליטראלים לכל היותר. מובן כי הקידוד בו נשתמש, שונה מן הקידוד שהשתמשנו בו בסעיף 15.2.

<u>הערה למתקדמים:</u> הבעיה $3SAT$ הינה צמצום של SAT, במובן שכל קלט לבעיה $3SAT$ הוא בפרט קלט של הבעיה SAT (כלומר, ניתן לקידוד כקלט לבעיה SAT). ההפך אינו בהכרח נכון, אך כפי שנראה בהמשך, לכל קלט לבעיה SAT קיים קלט "שקול" לבעיה $3SAT$. יתר על כן, ניתן יהיה למצוא ביעילות קלט שקול זה. כלומר, אנו נראה רדוקציה פולינומיאלית מהשפה SAT אל השפה $3SAT$.

<u>משפט 15.2:</u> השפה $3SAT$ הינה **NP**-שלמה.

<u>הוכחה:</u> ברור כי $3SAT \in$ **NP** (באותו אופן בו הראינו כי $SAT \in$ **NP**). על מנת להראות את השלמות, די להראות כי $SAT \propto_p 3SAT$. להלן תיאור הרדוקציה. בהנתן פסוק, ϕ, בצורה CNF (קלט אפשרי לבעיה SAT) נעבור על

פסוקיותיו זו אחר זו ונחליף כל פסוקית בעלת יותר משלושה ליטראלים, בסדרת פסוקיות כדלקמן (פסוקיות בעלות שלושה ליטראלים ופחות, תועתקנה כפי שהן לפסוק הקלט ל-$3SAT$). את הפסוקית ה j-ית, $C_j = \bigvee_{i=1}^{t_j} l_{j,i}$, המכילה $t_j > 3$ ליטראלים, נחליף ב-t_j הפסוקיות הבאות:

$$C_j^{(1)} = l_{j,1} \vee y_j^{(1)}$$
$$C_j^{(2)} = \overline{y}_j^{(1)} \vee l_{j,2} \vee y_j^{(2)}$$
.
.
.
$$C_j^{(t_j-1)} = \overline{y}_j^{(t_j-2)} \vee l_{j,t_j-1} \vee y_j^{(t_j-1)}$$
$$C_j^{(t_j)} = \overline{y}_j^{(t_j-1)} \vee l_{j,t_j}$$

כאשר המשתנים, $\{y_j^{(i)}\}$, הם משתנים חדשים (שאינם מופיעים בפסוק ϕ). שים לב, כי המשתנה $y_j^{(i)}$, מופיע רק בפסוקיות המחליפות את הפסוקית ה j-ית (של הפסוק ϕ).

נסכם. הרדוקציה מעתיקה את הפסוק $\phi = \bigwedge_{j=1}^{m} C_j$, לפסוק $\phi' = \bigwedge_{j=1}^{m} \bigwedge_{i=1}^{t_j} C_j^{(i)}$, כאשר הפסוקיות $C_j^{(i)}$ הן כפי שהוגדרו לעי"ל. ודא כי ההעתקה אמנם ניתנת לחישוב בזמן פולינומיאלי, וכי הפסוק המתקבל בהעתקה הוא תמיד בצורה $3CNF$. לבסוף נראה כי הרדוקציה תקפה. נזכיר שוב כי על מנת להראות כי הרדוקציה תקפה, יש להראות כי $\phi \in SAT$ אמם $\phi' \in 3SAT$. התנאי המהותי שיש לודא, הוא שהנוסחא, ϕ, ניתנת לסיפוק אמם הנוסחא, ϕ', ניתנת לסיפוק.

נביא כעת סקיצה של ההוכחה:

<u>כיוון I:</u> נניח כי ϕ ניתנת לסיפוק. תהא τ הצבת אמת המספקת את ϕ. לכל פסוקית של ϕ, קיים ליטראל שערכו T. נניח כי בפסוקית, $C_j = \bigvee_{i=1}^{t} l_{j,i}$, הליטראל, $l_{j,k}$, מקבל ערך אמת T. נתבונן בפסוקיות המתאימה ל-C_j בנוסחא ϕ'.

$$C_j^{(1)} = l_{j,1} \vee y_j^{(1)}$$
.
.
.
$$C_j^{(k)} = \overline{y}_j^{(k-1)} \vee l_{j,k} \vee y_j^{(k)}$$
.

.

.

$$C_j^{(t_j-1)} = \overline{y}_j^{(t_j-2)} \vee l_{j,t_j-1} \vee y_j^{(t_j-1)}$$

$$C_j^{(t_j)} = \overline{y}_j^{(t_j-1)} \vee l_{j,t_j}$$

עבור כל $i<k$ נקבע למשתנים, $y_j^{(i)}$, ערך T, ועבור כל $i \geq k$ נקבע למשתנים $y_j^{(i)}$ ערך F. שים לב, כי הפסוקיות $C_j^{(i)}$, עבור $i<k$, מסופקות ע"י $y_j^{(i)}$, הפסוקיות $C_j^{(i)}$, עבור $i>k$, מסופקות ע"י $\overline{y}_j^{(i-1)}$ ואילו הפסוקית $C_j^{(k)}$, מסופקת ע"י $l_{j,k}$. שים לב כי הצבת משתני העזר (ה y-ים) של הפסוקית הנ"ל, לא משפיעה על פסוקיות אחרות. קיבלנו כי כל פסוקיות ϕ' מסופקות תחת הצבה זאת ולכן ϕ' ניתנת לסיפוק.

<u>ביוון II:</u> נניח כי ϕ' ניתנת לסיפוק, אז כל הפסוקיות ה"מתאימות" לפסוקית C_j (ב- ϕ) ניתנות לסיפוק. נראה כי לא יתכן שלכל הליטראלים המופיעים בפסוקית C_j, הושם ערך F. נניח בדרך השלילה, כי לכל הליטראלים, $\{l_{j,i}\}_{i=1}^{t_j}$, יש ערך F. נעבור על הפסוקיות, $C_j^{(i)}$, מ- $i=1$ אל $i=t_j$. מתוך, $C_j^{(1)} = l_{j,1} \vee y_j^{(1)}$, מחויב כי הערך של $y_j^{(1)}$, הוא T (כי $l_{j,1}$ ערכו F). מתוך, $C_j^{(2)} = \overline{y}_j^{(1)} \vee l_{j,2} \vee y_j^{(2)}$, מחויב כי הערך של $y_j^{(2)}$ הוא T, וכך הלאה עבור כל k כך ש- $t_j > k$. בהגיענו אל הפסוקית, $C_j^{(t_j)} = \overline{y}_{j_{(t_j-1)}} \vee l_{j,t_j}$, נקלע לסתירה, כי כבר מחויב שהערך של $\overline{y}_j^{(t_j-1)}$ הוא F (כי הערך של $y_j^{(t_j-1)}$ הוא T) ואילו הנחנו, כי הערך של l_{j,t_j}, הינו גם כן F. מכאן נובע, כי לכל פסוקית מקורית, C_j, קיים ליטראל שערכו T. כלומר, קיבלנו כי הנוסחא, ϕ, ניתנת לסיפוק.

<u>תרגיל 15.3:</u> תהי $gSAT$, קבוצת הפסוקים (לאו דוקא בצורה CNF) שקיימת להם הצבת אמת מספקת. הוכח כי $gSAT$ הינה **NP**-שלמה.

<u>תרגיל 15.4:</u> נגדיר מחדש את $3SAT$, באופן שהקלט שלה יהיה פסוקיות שכל אחת מהן מכילה <u>בדיוק</u> שלושה ליטראלים. הראה כי גם $3SAT$ המוגדרת כך, הינה **NP**-שלמה.