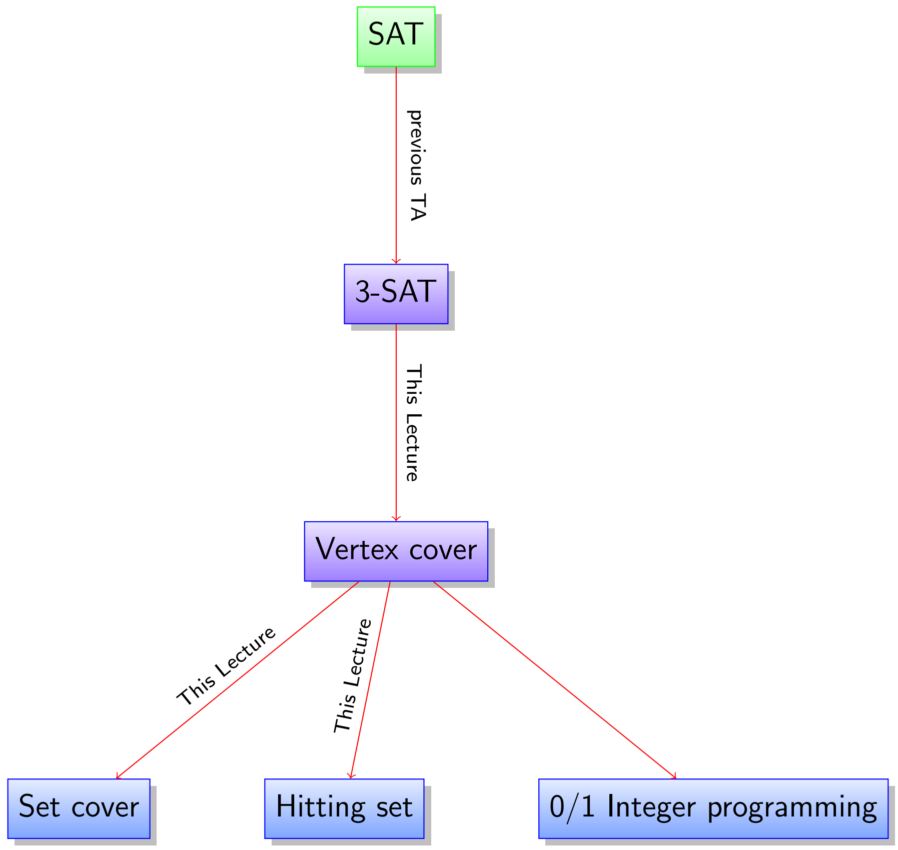
חישוביות—הרצאה 11

מבוא

היום נראה הרבה דוגמאות לרדוקציות.

תמונת העולם

ראינו בהרצאה הקודמת ש־Bounded־Halting $\in \mathcal{NP}$־Complete, בתרגול הקודם ראינו רדוקציה מ־SAT ל־$3SAT$.



$\mathbf{3SAT \leq_P VC}$

משפט: $3SAT \leq_P VC$ ממשפט זה נסיק ש־

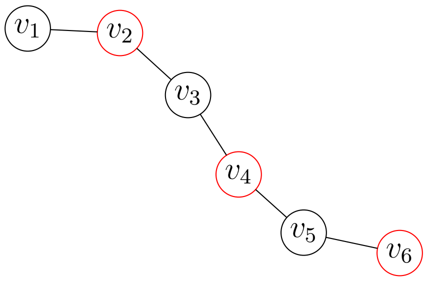
$$SAT \leq_P 3SAT \leq_P VC$$

היא $VC \in \mathcal{NP}$־Complete
כיסוי קודקודים בגרף אם G גרף לא מכוון REVOC-XETREV של G הוא תת קבוצה של קודקודים כך שכל קשת של G נוגעת באחד מהקודקודים הללו. בעיית כיסוי הצמתים שואלת האם גרף מכיל כיסוי צמתים בגודל ספציפי.

$$VC := \{< G, k > | G \text{ is an undirected graph that has a } k\text{-node vertex cover}\}$$

דוגמה

עבור G המתואר באיור, קיים כיסוי בצמתים בגודל 3 (הצמתים המסומנים באדום, כלומר $\{v_2, v_4, v_6\}$, אומנם הוא לא הכיסוי היחיד בגודל 3), ולכן מתקיים $< G, 3 > \in VC$.



לעומת זאת לא קיים כיסוי צמתים בגודל 2, ולכן $< G, 2 > \notin VC$ (בכל מסלול, כל צומת מכסה לכל היותר 2 קשתות אומנם בגרף יש 5 קשתות).

אבחנה: לכל G עם $|V| = n$, קיים כיסוי בצמתים בגודל n.

הוכחה: V מכסה את שני הקצוות, אפילו של כל אחת מהקשתות.

אבחנה 2: לכל G קיים VC בגודל $n - 1$.

הוכחה: נבחר $U = V$, וכך נכסה את שני הקצוות של כל קשת. כעת נוריד מ־U קודקוד v כלשהו, וכך לכל קשת ירד לכל היותר קצה אחד, ולפחות אחד ישאר מכוסה.

אבחנה: לכל $V \geq 3$, קיים גרף שעבורו $n - 2$ קדקודים לא מספיקים לכיסוי.

הוכחה: ב־K_n לא קיים כיסוי בגודל $n - 2$ כי לכל U כזה, $\{v_1 v_2\}$ כאשר $v_1, v_2 \notin U$ היא קשת שאינה מכוסה ע"י U.

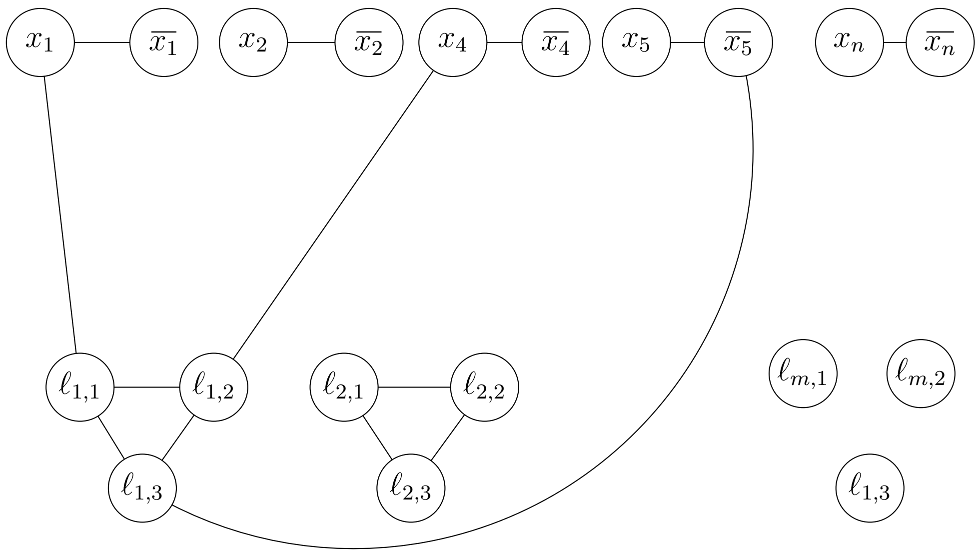
הוכחת משפט 11.1: נבנה פונקצית רדוקציה פולינומית מ־$3SAT$ ל־VC. בהוכחת הנכונות, נרצה להראות שכל השמה מספקת ל־ϕ משרה VC מתאים ב־$f(\phi)$, ולהיפך, כלומר כל VC מתאים ב־$f(\phi)$, משרה השמה מספקת השמה מספקת ל־ϕ

נסמן:

$$\phi(x_1, \ldots, x_n) = \bigwedge_{i=1}^{m} C_i$$

נסמן $C_i = \ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3}$

לדוגמה: $\phi(x_1, ..., x_5) = (x_1 \vee x_4 \vee \overline{x_5}) \wedge (x_3 \vee x_3 \vee x_2) \wedge (\overline{x_2} \vee \overline{x_1} \vee \overline{x_4})$ כאן $C_1 = \underbrace{x_1}_{\ell_{1,1}} \vee \underbrace{x_4}_{\ell_{1,2}} \vee \underbrace{\overline{x_5}}_{\ell_{1,2}}$, כמו כן $\ell_{3,3} = \overline{x_4}$. f תפלוט את הזוג (G, k) כאשר: לכל $i \in [n]$ נשים $e = x_i \overline{x_i}$, ולכל פסוקית ניצור K_3 עם הליטרלים שלה, כאשר לכל ליטרל יש קשת בין כל ליטרל פסוקית לליטרל השתנה אותו הוא מייצג, לדוגמה:



כאשר בדוגמה, זאת ציירנו את C_1 לפי הדוגמה לעיל. ונשים לב ש־m מייצג את מספר הפסוקיות ואילו n מייצג את מספר המשתנים.

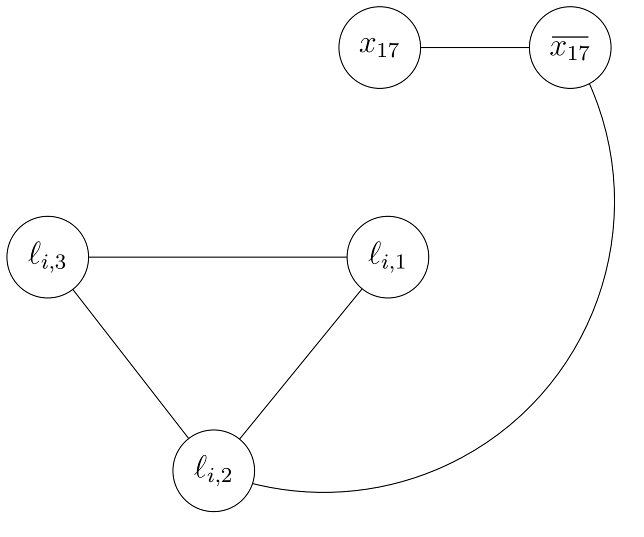
נבחר $k = n + 2m$ נוכיח נכונותת של f. פולינומיות: קל, לכל משתנה ולכל פסוקית מכניסים רכיב בעל מבנה פשוט, חיבור הקשתות בין הרכיבים, ישנן $O(m)$ קשתות, שקל לחשב אותן מתוך $\phi \Longleftarrow$ סה"כ זמן פולינומי בגודל הקלט, כאשר גודל הקלט הוא למשל $O(m \cdot \log n)$ בייצוג "המתבקש" של $\phi = (n, \underbrace{(\ell_1, \ell_2, \ell_3)}_{\text{EVERY LITERAL TAKES } O(\log n) \text{ BITS}}, ...)$, כיוון שיש m פסוקיות יש $3m$ ליטרלים, סה"כ נקבל $O(m \log n)$.

הערה: שימו לב שמניחים ייצוג סביר ולא יצוג עם יותר מידי יתירות, כי אז השפה עלולה להפוך לקלה מידי (ראו מטלה 4).

תקפות: נראה שני כיוונים:

$\Longleftarrow$) נניח $\phi \in 3SAT$, ונראה ש־$f(\phi) \in VC$. תהי $w = w_1, w_2, w_3, ..., w_n$ השמה המספקת את ϕ, נבנה VC מתאים עבור $f(\phi)$, על סמך w. הכיסוי בצמתים שלנו U יוגדר כך: בכל רכיב משתנה, נבחר ל־U את הליטרל המסתפק ע"י w ורק אותו. למשל, אם $w_5 = F$ אז נבחר ל־U את $\overline{x_5}$. לכל רכיב פסוקית המתאים לפסוקית C_i יהי $\ell_{i,j}$ ליטרל המסתפק ע"י w. אם יש יותר מאחד אז נבחר את זה עם ה־j המינימלי. (קיים כזה כי w השמה מספקת ואם כל הליטרלים ב־C_i היו F עבור w, אז $\phi = \bigwedge C_i$ היה גם F). ל־U נצרף את שני הקודקודים שאינם מסומנים ב־$\ell_{i,j}$ מתוך הרכיב C_i. אכן קבלנו U שגודלו $n + 2m$: בחרנו קודקוד מכל רכיב משתנה ו־2 קודקודים מכל רכיב פסוקית, נותר להראות ש־U אכן כיסוי בצמתים.

- כל רכיב משתנה מכוסה, כי לכל x_i בחרנו את x_i או את $\overline{x_i}$ לפי w.
- כל רכיב פסוקית מכוסה, כי לכל רכיב כזה בחרנו בדיוק שני קודקודים. לא משנה איזה שניים בוחרים, המשולש יכוסה.
- נותר להראות שכל הקשתות בין הרכיבים מכוסות. נתבונן בקשתות שיוצאות מרכיב פסוקית C_i כלשהו. קיים $\ell_{i,2}$ שמסתפק ע"י w בה"כ נניח שכאן זה $\ell_{i,2} = \overline{x_{17}}$. כיסינו את כל הקשתות שיוצאות מ־C_i (כי מבניית U $\overline{x_1}7$ נבחר ל־U ולכן הוא מכסה את הקשת $\{\ell_{i,2}\overline{x_{17}}\}$, בנוסף מבניית U שני הקודקודים האחרים ברכיב הפסוקית נבחרו, ולכן גם במקרה שיוצאים מהם קשתות, הם מכוסות). ו־C_i היה רכיב פסוקית שרירותי $\Leftarrow$ כיסינו את כל הקשתות היוצאות מכל הרכיבים.



$\Longrightarrow$) נניח ש־$f(\phi) \in VC$ ונוכיח ש־$\phi \in 3SAT$ אם $\underbrace{f(\phi)}_{=(G,k)} \in VC$, אז קיים ל־$G$ VC נסמנו U שגודלו $k = n + 2m$, כאשר n, m הם כפי שנובע ממבנה הגרף. נשים לב ש־U חייב לבחור בדיוק קודקוד אחד מכל "רכיב משתנה" ובדיוק שני קודקודים מכל "רכיב פסוקית". (כדי לכסות את הרכיב משתנה ה־i חייבים לבחור את אחד הקצוות של הרכיב, אחרת הוא לא יכוסה. באופן דומה בשביל לכסות משולש חייבים לבחור שני קודקודים ממנו לפחות. קיבלנו $|U| \geq n + 2m$, מצד שני אסור לנו להוסיף יותר מזה בשום רכיב, אחרת נבחר ממש יותר מ־k, ואז U לא יהיה VC מתאים (עד לכך ש־$(G,k) \in VC$)). כעת נבנה השמה מספקת

עבור w נקבע $\phi(x_1,x_2,...,x_n)$ אם $w_i = T$ אם $x_i \in U$ ו־$w_i = F$ (אחרת בהכרח $\overline{x_i} \in U$ מהמסקנה לעיל, בפרט w מוגדרת היטב). נשאר להראות ש־w מספקת את ϕ ולכן ניתן יהי להסיק ש־$\phi \in 3-SAT$. נניח בשלילה שההשמה w לא מספקת את ϕ כלומר $\phi(w) = \bigwedge_i C_i(w) = F$ לכן קיים i כך ש־ $C_i(w) = F$ כיוון ש־$C_i = \ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3}$ נסיק ש־$\ell_{i,j}(w) = F$ לכל $1 \le j \le 3$ נראה קשת היוצאת מ־C_i שאינה מכוסה ע"י U, וזו תהיה סתירה לבחירת U. בה"כ $\ell_{i,1}, \ell_{i,2}$ נבחרו ל־U, ו־$\ell_{i,3} = \overline{x_{14}}$, כיוון שבפרט $\ell_{i,j}(w) = F$, מבניית w, גם $\overline{x_{14}}$ לא נבחר ל־U. כלומר $(\ell_{i,3}, \overline{x_{14}})$ נשארה לא מכוסה ע"י U סתירה. מסקנה: $\phi(w) = T$ כנדרש.
מש"ל □

נראה עוד מספר רדוקציות יותר פשוטות:

Hitting Set

הגדרה 11.2:

$$HS := \left\{ (n,k,C_1,C_2,...,C_m) \middle| \begin{array}{c} k \le n \in \mathbb{N}^+,\ 1 \le i \le m:\ C_i \subseteq [n] \\ \text{and there exists } U \subseteq [n] \text{ such that:} \\ 1.\ |U| = k \\ 2.\ \forall_i\ C_i\ \cap\ U \neq \emptyset \end{array} \right\}$$

טענה: $HS \in \mathcal{NP}$־Complete

הוכחה: נראה $VC \le_P HS$ כיוון ש־$VC \in \mathcal{NP}$־Complete(משרשרת רדוקציות קודמות־אם מאמינים למשפט $(Cook-Levin)$, נסיק שגם $HP \in \mathcal{NP}$־Complete. רעיון הרדוקציה: נשים לב שהבעיה HS היא הכללה טבעית של VC, כאשר V מקביל ל־$[n]$, k מקביל ל־k, ו־E מקביל ל־$C_1,C_2,...,C_m$ (במקרה של VC כל הקבוצות בגודל 2 בדיוק). פורמלית: $f(G,k)$ פולטת $(n=|V|,k,e_1,e_2,...,e_m)$ כאשר $E = \{e_1,e_2,...,e_m\}$

נכונות:

- **פולינומיות:** סיבוכיות חישוב f היא בערך לינארית (פחות או יותר מעתיקים את הקלט, צריך גם לחשב $|V|$, מתוך V, שזה גם יעיל, סה"כ פולינומי בגודל הקלט).
- **תקפות:** מספיק להראות כיצד לעבור מכיסוי בצמתים עבור $(G,k) \in VC$ ל־U מתאים (Hitting Set) ולהפך מ־U עבור $f(G,k) \in HS$ ל־VC מתאים עבור G. לדוגמה, עבור VC־U של G שגודלו k, U עצמו הוא HS עבור $f(G,k)$ בגודל k. בכיוון השני, עבור HS ל־$f(G,k)$, U, המפורש כתת קבוצה של V הוא VC של (G,k) שגודלו k.

Set Cover

הגדרה:

$$SC := \left\{ (n,k,C_1,C_2,...,C_m) \middle| \begin{array}{c} k \le n \in \mathbb{N}^+,\ 1 \le i \le m,\ C_i \subseteq [n] \\ \bigcup_{i=1}^m C_i = [n]\ \text{ and there exists an } U \subseteq [n] \\ \text{such that } 1.\ |U| \le k \qquad 2.\ \bigcup_{i \in U} C_i = [n] \end{array} \right\}$$

טענה: $SC \in \mathcal{NP}$־Complete.

הוכחה: נראה ש־$SC \le_S C$.

רעיון הבניה: נראה שאיכשהו, $[n]$ יתאים ל־E וכל קודקוד יתאים לקבוצה של E־ים. פורמלית f תוגדר באופן הבא:

$$f(G(V,E),k) = \left(|E|, k, C_1, ..., C_{|V|}\right)$$

כאשר $\forall_v\ C_v = \{e \in E | v \text{ incident to } v\}$. עניין טכני קטן, נחליף כל קשת בסמפר מתאים בתחום $[|E|]$ בצורה שרירותית.

Subset—Sum

$$\text{SS} := \left\{ (k,x_1,\ldots,x_t) \middle| x_1,\ldots,x_t,k \in \mathbb{N} \text{ s.t. there exists a subset } I \subseteq [t] \text{ for which } \sum_{i \in I} x_i = k \right\}$$

משפט: $\text{SS} \in \mathcal{NP}$־Complete. **הוכחה:**

1. $SS \in \mathcal{NP}$: נתאר מ"ט א"ד פולינומיתת עבור השפה SS, באופן הבא: $M(x)$ תנחש תת קבוצה $I \subseteq [t]$ ותבדוק האם הסכום $\sum_{i\in I} x_i = k$. אם כן תקבל, אחרת תדחה.
קל לראות ש־M פולינומית, כמו כן קיים מסלול מקבל אם $x \in \mathrm{SS}$.

2. $\mathrm{SS} \in \mathcal{NP}$־Complete: נראה רדוקציה פולינומית מ־VC ל־SS, דהיינו $\mathrm{VC} \le_p \mathrm{SS}$.
רעיון הבניה: כל קודקוד בגרף ייוצג ע"י קבוצת הקשתות שהוא מכסה, וכל קשת תיוצג כך שיהיה ניתן להוסיף אותה לכיסוי או לא. נגדיר

$$f(G,k) = \left(\underbrace{a_1, \ldots, a_m}_{\substack{\text{variable for} \\ \text{each edge}}}, \underbrace{b_1, \ldots, b_n}_{\substack{\text{variable for} \\ \text{each vertex}}}, k' \right).$$

כאשר:

$$a_i = 10^{i-1} \qquad b_i = 10^m + \sum_{e_i :\, v \in e_i} a_i \qquad k' = k \cdot 10^m + \sum_{i=1}^{m} 2 \cdot a_i$$

נשים לב כי:

$$\begin{aligned} a_1 &= \overbrace{0 \ldots 0}^{m-1} 1 \\ a_2 &= 0 \ldots 10 \\ &\ldots \\ a_n &= 1 \overbrace{0 \ldots 0}^{m-1} \end{aligned}$$

וכי

$$b_i = 1 \overbrace{001 \ldots 010 \ldots 11}^{m}.$$

אבחנה: נסמן ב־s את תוצאת הסכום שמתקבל, אזי כל סיבית ב־$s \ni \{0,1,2,3\}$. כיוון שכל איבר יכול להיסכם פעם אחת לכל היותר, ו־b_i מכיל בסיבית ה־j את הסיפרה 1 הקשת ה־i מכסה את הקודקוד ה־j ואחרת 0. סה"כ כל קשת נוגעת בשני קודקודים ולכן סכמנו את הסיבית המתאימה לכל היותר פעמיים, בעוד התוספת שיכלנו לבחור את ה־a המתאים נגיע מקסימום לשלוש פעמים. האבחנה היא שאם יש לנו VC אזי נבחר בדיוק את ה־k קודקודים של ה־VC, ולאחר מכן נשלים ל־2 בעזרת ה־a־ים המתאימים. היות והמקדם של הספרה ה־$m+1$ הוא k אזי תמיד נוכל לבחור k קודקודים מתאימים (כי ה־a־ים לא יכולים להוסיף לספרה ה־$m+1$). וע"פ הבניה נוכל תמיד לסדר ככה שיצא לנו 2 בכל הספרות שמתארות צלעות. (בגדול אנחנו משלימים ל־2, בגלל שקשת מכוסה לכל היותר ע"י 2 קודקודים, וזה אפשרי רק אם היה לנו מההתחלה VC). אנא וודא שאתה מבין את הערה האחרונה.

3. **נכונות הרדוקציה:**

- $f \in \mathrm{Poly}$ ־ קל לראות ש־f רצה בזמן פולינומי באורך הקלט.
- **תקפות:** ראשית נבחין ש־VC שווה ל־

$$\mathrm{VC} \equiv \{(G,k) | \exists_{VC} \; s.t. |VC| = k\}.$$

זה נכון, כי אם היה כיסוי קודקודים מאורך קטן יותר מ־k אם נוסיף קודקודים לא נהרוס את ה־VC ולכן קיים כיסוי קודקודים גם בגודל k. נמשיך בהוכחת התקפות:
$(\Rightarrow)$ נניח כי $(G,k) \in \mathrm{VC}$ ונראה כי $f(G,k) \in \mathrm{SS}$. נבצע את הבחירה הבאה:

$$I = \{b_i | v_i \in \mathrm{VC}\} \cup C.$$

כאשר C היא קבוצת כל ה־a_i כך שביחד הם יצרו את התבנית הבאה: $k\overbrace{2\ldots2}^{m}$. כפי שהסברנו באבחנה זה תמיד אפשרי.
$\Leftarrow$) הכיסוי $\{v_i : b_i \text{ selected}\}$. כלומר אנחנו לוקחים את הקודקודים המיוצגים ע"י ה־b_i שנבחרו. אכן זהו כיסוי ע"פ האבחנה. $\square$