

נניח $NP = PCP(O(\log n), O(1))$.

משפט: יש $0 < \alpha < \beta \leq 1$ כך ש- $\text{Gap}_{[\alpha, \beta]} \text{max3SAT}$ היא NP-שלמה.

תהי $A \in NP$. אזי יש לה מערכת PCP, כך שעבור קלט $x \in \{0, 1\}^n$ יש מוכיח שמספק הוכחה $w \in \{0, 1\}^{m = \text{Poly}(n)}$.

נבנה פסוק 3SAT φ_x שהמשתנים שלו הם $w_1, \dots, w_m$. לכל $y \in \{0, 1\}^{O(\log n)}$ הטלת מטבעות אפשרית לבדוק של מערכת ה-PCP, הרדוקציה תעשה את הדבר הבא:

- תחשב איזה שאילתות בודק ה-PCP ישאל $i_1, \dots, i_q$.
 - הרדוקציה תבנה טבלת אמת: לכל השמה אפשרית $w_{i_1}, \dots, w_{i_q}$, הרדוקציה מחשבת האם $V(x, y, w_{i_1}, \dots, w_{i_q})$ מקבל או לא.
 - הרדוקציה ממירה את טבלת האמת לפסוק 3SAT $\varphi_{x,y}$.
- הפלט של רדוקציה: $\varphi_x = \bigwedge_{y \in \{0, 1\}^{O(\log n)}} \varphi_{x,y}$. פסוקית באורך k שתלוי רק ב- q .

נכונות הרדוקציה:

אם $x \notin A$, לכל w הוא מבטא איזשהו מוכיח כלשהו של מערכת PCP, ולכן $\Pr_y[V(x, y, w_{i_1}, \dots, w_{i_q}) = 1] \leq \alpha$, ולכן $\Pr_y[\text{מסתפק} \varphi_{x,y} \text{ על } w] \leq \alpha$. לכן, עבור חלק $1 - \alpha$ יש לפחות פסוקית אחת של $\varphi_{x,y}$ שלא מסתפקת, ולכן בסך הכל חלק $\beta = \frac{1 - \alpha}{k}$ מהפסוקיות לא מסתפקות.

אם $x \in A$, אזי יש מוכיח הוגן שנותן $w \in \{0, 1\}^m$ כך שלכל $y \in \{0, 1\}^{O(\log n)}$, $V(x, y, w_{i_1}, \dots, w_{i_q}) = 1$, ולכן ההשמה w מספקת כל $\varphi_{x,y}$, ולכן φ_x ספיק לגמרי. אפשר לקחת $\beta = 1$.

בעיה NP-קשה: אפשר לתת עדות לקליטים בשפה.	שפה: האם פסוק 3SAT ספיק לגמרי?
$PCP(O(\log n), O(1))$: אפשר לתת עדות לשייכות בשפה שאפשר לבדוק רק עם מעט שאילתות.	בעיית ההבטחה: בן - יש השמה שמספקת הרבה פסוקיות. לא - כל השמה מספקת מעט פסוקיות.

טענה: אם $\text{Gap}_{[\alpha, \beta]} \text{max3SAT}$ היא NP-קשה עבור $0 < \alpha < \beta \leq 1$, אזי $NP \subseteq PCP(O(\log n), O(1))$.

תהי $L \in NP$. יש לה רדוקציה φ ל- $\text{Gap}_{[\alpha, \beta]} \text{max3SAT}$. המטרה שלנו: לבנות מערכת PCP עבור A .

עבור קלט $x \in \{0, 1\}^n$ יש פסוק 3SAT $\varphi_x(z_1, \dots, z_n) = \bigwedge_{i=1}^m c_i$ כך שאם $x \in L$ אז יש השמה w שמספקת המון פסוקיות, ואם $x \notin L$, כל השמה w מספקת לכל היותר $\alpha \cdot m$ פסוקיות. נבנה את מערכת ה-PCP:

המוכיח מספק השמה למשתני φ_x .

הבודק מטיל $i \in \{1, \dots, n\}$. שואל מה הערכים של המשתנים שמופיעים בפסוקיות c_i . מקבל ערכים של משתנים. אם הפסוקית מסתפקת - מקבל. אחרת - דוחה.

נכונות:

אם $x \in L$, יש השמה w למשתני φ_x שמספקת המון פסוקיות, ולכן $\Pr_i[\text{מסתפק } c_i \text{ על } w] \geq \beta$.

והבודק יקבל בהסתברות לפחות β .

אם $x \notin L$, לכל השמה w , ההשמה מספקת לכל היותר $\alpha \cdot m$ פסוקיות. לכן, כל מוכיח למערכת ה-PCP מגדיר השמה w , ולכן $\Pr[V \text{ יקבל}] \leq \alpha$.

מספר השאילתות - 3. המערכת פולינומית. מספר המטבעות - $\log m$, כאשר m הוא מספר הפסוקיות ב- φ_x . φ_x הוא הפלט של הרדוקציה מ- L ל- Gap-max3SAT . φ_x פולינומית, ובפרט $m = \text{Poly}(|x|)$, $\log m = O(\log |x|)$.

לכן, $L \in PCP_{[\alpha, \beta]}(\log m, 3)$.

רוצים להתחיל עם בעיית $\text{Gap}_{[\alpha, \beta]} \max 3\text{SAT}$ NP-קשה, ולהסיק ממנה שבעיות Gap אחרות הן NP-קשות.
לא רוצים לעשות את כל העבודה מחדש. רוצים להפעיל רדוקציות.

הגדרה: רדוקציה שמעבירה Gap ל- Gap נקראת **רדוקציה משמרת פער**.

ראינו: $3\text{SAT} \leq \text{Clique} \leq \text{IS} \leq \text{VC}$.

תזכורת: $3\text{SAT} \leq \text{Clique}$.

האם הרדוקציה משמרת פער?

אם התחלנו עם $\varphi \in \text{Yes}$, אזי יש השמה שמספקת $\beta \cdot m$ פסוקיות, ויש קליקה בגודל $\beta \cdot m$.

אם התחלנו עם $\varphi \in \text{NO}$, אזי כל השמה מספקת לכל היותר $\alpha \cdot m$ פסוקיות, ולכן הקליקה המתקבלת גודלה לכל היותר $\alpha \cdot m$.

תזכורת: $\text{Clique} \leq \text{IS}$.

הרדוקציה:

קלט: $G = (V, E)$.

פלט: $\bar{G} = (V, \bar{E})$.

טענה: יש ב- G קליקה בגודל $k \Leftrightarrow$ יש ב- $\bar{G}$ קבוצה ב"ת בגודל k .
האם הרדוקציה משמרת פער? כן!

נניח שהיינו יודעים כי $\text{Gap}_{[\sqrt{n}, 10\sqrt{n}]} \max \text{IS}$ (פער פי 10) היא NP-קשה.

הרדוקציה תיתן ש- $\text{Gap}_{[n-\sqrt{n}, n-10\sqrt{n}]} \min \text{VC}$ NP-קשה.

אבל $n - 10\sqrt{n}$ מאוד קרוב ל- $n - \sqrt{n}$. נעלים לנו הפער הכפלי.

בפועל ראינו: $\text{Gap}_{[\alpha \cdot m, \beta \cdot m]} \max \text{IS}$ היא NP-שלמה. לכן, $\text{Gap}_{[(1-\alpha) \cdot m, (1-\beta) \cdot m]} \min \text{VC}$ היא NP-שלמה.

נשאר לנו פער כפלי, אולי קטן יותר.

ל- VC באמת יש אלגוריתם קירוב עם פקטור 2.

הבעיה 3SAT3:

קלט: פסוק 3SAT $\varphi(x_1, \dots, x_n) = \bigwedge_{i=1}^m c_i$, שכל משתנה x_i מופיע לכל היותר 3 פעמים.

פלט: ספיק או לא.

טענה: $3\text{SAT} \leq 3\text{SAT3}$.

הרדוקציה (על קלט פסוק 3SAT $\varphi(x_1, \dots, x_n) = \bigwedge_{i=1}^m c_i$):

לכל משתנה x_i שמופיע k_i פעמים, נכניס k_i משתנים שנקרא להם x_{ij} .

מחליף את המופע ה- j של x_i במשתנה x_{ij} , ונוסיף פסוקית $x_{ij_1} \rightarrow \dots \rightarrow x_{ij_{k_i}} \rightarrow x_{ij_1}$, תוך

שימוש בשקילות $a \rightarrow b \equiv \neg a \vee b$.

הפסוק החדש הוא פסוק 3SAT3 φ' .

כמה פסוקיות יש בו? $m + \sum_{i=1}^m k_i = m + 3m = 4m$.

נכונות:

אם φ ספיק, יש השמה ל- $x_1, \dots, x_n$ שמספקת את φ . נבחר ל- x_{ij} את הערך של x_i , והשמה זו תספק את כל הפסוקיות.

אם φ' ספיק, אז בהכרח כל x_{ij} מקבלים את אותו ערך w_i , ובהכרח w מספקת את φ ולכן φ ספיק.

מה הרדוקציה מראה לגבי פער?

φ'	φ	
$\geq (3+\beta)m$	$\geq \beta m$	Yes
יש $(3+\alpha)m$. יכול להיות שיש השמה שתספק $4m-1$.	$\leq \alpha m$	No

למשל, ייתכן ש- x_1 או $\neg x_1$ מופיע בכל פסוקית, ואז ל- x_{ij} אפשר לבחור ערך 0 או 1 בצורה שכל הפסוקיות המקוריות יסתפקו.

לא למבחן

עובדה: יש סדרה של גרפים לא מכוונים G_n , כך ש- G_n מדרגה קבועה D ($D=10$) על n קודקודים, ומתקיים $G_n=(V,E)$, $|V|=n$, ולכל $A \subseteq V$, $|E(A,\bar{A})| \geq \min(|A|, |\bar{A}|)$.

בחזרה לרדוקציה:

$$\text{מקבלת } \varphi(x_1, \dots, x_n) = \bigwedge_{i=1}^m c_i$$

- לכל i , שמופיע n_i פעמים, ניצור n_i משתנים חדשים x_{ij} . נחליף את המופע ה- j של x_i ב- x_{ij} .
- נוסיף פסוקיות עוקבות: לכל $i=1, \dots, n_i$, ניקח גרף על n_i קודקודים כמו בעובדה. הגרף דרגתו קבועה D , ויש לו את התכונה שלכל $A \subseteq V$, $|E(A, \bar{A})| \geq \min(|A|, |\bar{A}|)$, ולכל קשת בגרף x_{ij_1}, x_{ij_2} , נוסיף $x_{ij_1} \rightarrow x_{ij_2}$, $x_{ij_2} \rightarrow x_{ij_1}$.
- כל משתנה מופיע $2D+1$ פעמים. קיבלנו רדוקציה ל- $\text{Gap}_{\lfloor \cdot \rfloor} \max 3\text{SAT}(2D+1)$.
- מספר הפסוקיות ב- φ' : $m + \sum_{i=1}^n k_i \cdot 2D = m + 2D \cdot 3m = (6D+1) \cdot m$. ישנן m משתנים.

נכונות:

φ'	φ	
$\geq (6D+\beta)m$ (כל הפסוקיות העקביות, βm מהמקוריות)	$\geq \beta m$	Yes
$\leq (6D+\alpha)m$	$\leq \alpha m$	No

המשך החומר למבחן

נזכר איפה התחלנו:

A - בעיית אופטימיזציה:

על קלט x , יש קבוצה של פתרונות מותרים S_x , לכל אחד יש $c(s)$. בעיית האופטימיזציה מחפשת פתרון מותר עם ערך אופטימלי. c - קירוב של בעיית מקסימום ($c \geq 1$):

על קלט x , מוצא ערך O כך ש- $\frac{\text{OPT}_x}{c} \leq O \leq \text{OPT}_x$, כאשר OPT_x הוא הערך האופטימלי.

בהתחלה ראינו אלגוריתמי קירוב (למשל 2-קירוב ל-VC).

הגדרה: נאמר שבעיית קירוב היא **NP-קשה** אם קיום אלגוריתם פולינומי שפותר את בעיית הקירוב גורר $P=NP$.

הערה: משפט *Cook*: $c=1$ - קירוב הוא NP-קשה. עכשיו נוכיח: $c>1$ - קירוב הוא NP-קשה. ראינו: $c=2$ - קירוב ב-P.

טענה: יש $c > 1$ כך ש- c קירוב של VC היא בעיה NP-קשה.
 בסדרת הרדוקציות, הגענו לבעיה $\text{Gap}_{[a,b]} \text{minVC}$, כאשר:
 Yes - יש בגרף כיסוי קודקודי בגודל הקטן מ- b .
 No - כל כיסוי קודקודי בגרף הוא בגודל הגדול מ- a .
 ראינו: יש $0 < \alpha < \beta < 1$ כך ש- $\text{Gap}_{[\beta n, \alpha n]} \text{VC}$ היא NP-קשה ($n = |V|$).
 נניח שיש לנו אלגוריתם c -קירוב ל-VC, שרץ בזמן פולינומי.
 נראה איך לפתור את $\text{Gap}_{[\beta n, \alpha n]} \text{VC}$ ב-P, ומשם ינבע $P = \text{NP}$.
 בהינתן מופע של $\text{Gap}_{[\beta n, \alpha n]} \text{VC}$, המופע הוא גרף $G = (V, E)$, ואנחנו רוצים לברר אם $G \in \text{Yes}$,
 ואז יש כיסוי קודקודי שגודלו לכל היותר αn , או $G \in \text{No}$, ואז כל כיסוי קודקודי גודלו לפחות βn .
 נפעיל את אלגוריתם הקירוב שיחזיר מספר O .
מקרה 1: $G \in \text{Yes}$.
 $\text{OPT} \leq O \leq c \cdot \text{OPT}$ ו- $\text{OPT} \leq \alpha n$, לכן, $O \leq c \alpha n$.
מקרה 2: $G \in \text{No}$.
 $\beta n \leq \text{OPT} \leq O$, לכן, $O \geq \beta n$.
תיאור האלגוריתם על קלט G , שיודעים $G \in \text{Yes}$ או $G \in \text{No}$:
 נפעיל את אלגוריתם הקירוב על G , ונקבל תשובה O .
 אם $O < c \alpha n$, נענה כן.
 אם $O > \beta n$, נענה לא.
 האלגוריתם מוגדר היטב כל עוד $c \alpha n < \beta n \Leftrightarrow c < \frac{\beta}{\alpha}$.

ראינו: $\text{Gap}_{[a,b]} \text{minA}$ NP-קשה $\Leftarrow$ קשה לקרב את A עד כדי פקטור $\frac{a}{b}$.
 באותו אופן, $\text{Gap}_{[a,b]} \text{MaxA}$ NP-קשה $\Leftarrow$ קשה לקרב את A עד כדי פקטור $\frac{b}{a}$.
 בעיית Gap NP-קשה $\Leftarrow$ קושי של קירוב.
 ראינו כי בעיית Gap של VC היא NP-קשה $\Leftarrow$ קושי לקרב את VC.

מה לגבי הכיוון ההפוך?
 האם קושי של קירוב גורר בעיית Gap NP-קשה?
 ראינו כי $\text{max2SAT} \in \text{Gap}_{[\frac{0.61}{\alpha}n, \frac{0.62}{\beta}n]}$ היא NP-קשה. לכן, קשה לקרב את max2SAT עד איזה
 קבוע $c = \frac{\beta}{\alpha} > 1$.

מצד שני, $\text{max2SAT} \in \text{Gap}_{[\alpha, 1]}$ לכל $\alpha < 1$, ובפרט $\alpha = \frac{1}{c}$, נפתר על ידי 2SAT:

$\varphi \in \text{Yes} \Leftarrow$ ספיק לגמרי.

$\varphi \in \text{No} \Leftarrow$ לא ספיק.

וגם $2\text{SAT} \in P$, כי 2SAT היא NL-שלמה.

לכן, להגיד שקשה לקרב בעיה עד פקטור של c , לא נותן את האינפורמציה איפה הפער הזה נמצא.
 לעומת זאת, לומר שבעיית $\text{Gap}_{[a,b]} \text{maxA}$ היא NP-קשה אומר שקשה לקרב עד פקטור c , ובנוסף אומר
 איפה הקושי הזה נמצא.

בעיית 2SAT היא דוגמה לזה ש- $\text{Gap}_{[0.61, c \cdot 0.61]}$ היא NP-קשה, ו- $\text{Gap}_{[\frac{1}{c}, 1]}$ ב-P.

נזכר כי $IS \leq VC$. הרדוקציה הייתה נכונה רק בגלל שידענו איפה ה- Gap של IS היה. הרדוקציה הייתה
 מועילה רק כי ידענו שיש קושי קירוב לפקטור כפלי, וידענו איפה הוא נמצא.
 אם רק היינו יודעים שיש קירוב, זה היה יכול להיות $[\sqrt{n}, 10\sqrt{n}]$, זה לא היה מועיל לנו כי
 ב- $[n - \sqrt{n}, n - 10\sqrt{n}]$ אין פקטור כפלי.