26.5.09

סיבוכיות - שיעור 11

ניזכר (שוב) בבעיות אופטימיזציה. הכוונה לבעיות בהן יש הרבה "פתרונות" חוקיים, ומטרתנו למצוא את המקסימלי/מינימלי ביחס לפרמטר כלשהו. למשל, קליק, 3SAT, ו- SC.

תרגמנו בעיות אלה לבעיות הכרעה (בדרך כלל ע"י הוספת פרמטר k לקלט שיהיה את הפרמטר שאנחנו רוצים למקסם). חשוב לשים לב שכאן אינן בעיות הכרעה בזמן. אז ראינו שבעיות ההכרעה שלהן הן NP-שלמות. נובע מכך שבעיות האופטימיזציה המתאימות הן NP-קשות (אך לא שלמות כי הן לא ב- NP). מכיוון שהן NP-קשות ויש לנו רק זמן פולי, פנינו לאלגוריתמי קירוב.

כשראינו שגם בעיות הקירוב הן לפעמים לא כל כך קלות, הגדרנו בעיות Gap על מנת להוכיח שבעיות הקירוב הן NP-קשות. ניזכר שבעיית Gap מחלקת את עולם הקלטים אצלנו לשלוש קבוצות - קלטים טובים, קלטים רעים, וקלטים שלא אכפת לנו מהם. ספציפית, $Gap\text{-}A[c,hc]$ מחלקת את הקלטים של A לפי פרמטר האופטימיזציה של A לאלו שמתחת ל- c (טובים), אלה שמעל hc (רעים) ואלו שבאמצע (Gap)*.

* הנחנו כאן שזו בעיית מינימום (כמו למשל VC). בבעיית מקסימום החלק העליון הוא ה"טוב", התחתון הוא ה"רע" והאמצע נשאר באמצע. כמו למשל הגדרה ב- Clique.

הראינו בשיעור שעבר שאם יש לנו אלגוריתם h-קירוב ל- A, אנחנו יכולים לפתור את בעיית $Gap\text{-}A[c,hc]$ לכל c. לכן, אם $Gap\text{-}A[c,hc]$ היא NP-קשה עבור c כלשהו, קשה לקרב את A ביחס h.

Gap-3SAT

קלט: 3CNF.

בעיית אופטימיזציה: זוהי בעיית מקסימום. הפרמטר אותו אנחנו רוצים למקסם הוא החלק היחסי של הפסוקיות שסיפקנו (לספק את כולם עדיף מלספק $\frac{1}{2}$, ולספק $\frac{1}{2}$ עדיף מלספק $\frac{1}{3}$)

__בעיית Gap:__ נסתכל על $Gap\text{-}3SAT[\frac{7}{8}+\varepsilon,1]$. כלומר קבענו את הסף העליון להיות 1 (כמו ב-3SAT הרגיל) ואת הסף התחתון להיות $\frac{7}{8}+\varepsilon$.

בעיה זו היא בעיה __קלה יותר__ מבעיית ההכרעה 3SAT. זאת מכיוון שלרוב הקלטים אנחנו דורשים בדיוק אותו דבר (לקבל כשיש השמה מספקת ולדחות כשאי אפשר לספק הרבה בכלל), אך בבעיה זו מותר לנו "לטעות" לפעמים. לכן כל אלגוריתם המכריע את 3SAT פותר את $Gap\text{-}3SAT[\frac{7}{8}+\varepsilon,1]$ אך לא להיפך.

באופן כללי, בעיית $Gap[\alpha,\beta]$ תמיד קלה יותר מבעיית Gap אשר המרווח שלה מוכל בקטע $[\alpha,\beta]$ (בהנחה שזה Gap של אותה בעיה כמובן), וניתן להסתכל על בעיית ההכרעה כבעיית Gap בהן $\beta=\alpha$.

כפי ש-3SAT היא הבסיס והמקור של כל הבעיות ה-NP-שלמות, כך אם Gap-3SAT יכולה לשרת כתחליף לה לבעיות __Gap__. נשאלת השאלה למה דווקא בחרנו סף התחתון כמו $\frac{7}{8}+\varepsilon$.

__טענה:__ לכל נוסחת 3CNF (עם בדיוק שלושה ליטרלים שונים בכל הסגר) קיימת השמה שמספקת לפחות $\frac{7}{8}$ מהסגרים.

__הוכחה:__ באמצעות השיטה ההסתברותית:

- כמה הסגרים מספקת השמה __בתוחלת__?
- נגדיר לכל הסגר C_i את Y_i להיות משתנה 0/1 השקול לאינדיקטור "האם C_i מסופק?"
- $E(Y_i)=\frac{7}{8}$
- $E(\sum Y_i) \overset{\text{ליניאריות התוחלת}}{=} \sum E(Y_i) = m\cdot\frac{7}{8} \quad (m=\#\text{clauses})$
- מכיוון __שבתוחלת__ הן $\frac{7}{8}m$ הסגרים מסופקים, בהכרח קיימת השמה כלשהי שמספקת $\frac{7}{8}m$ הסגרים!

לכן לדבר על Gap-3SAT$[\alpha,1]$ לכל $\alpha \le \frac{7}{8}$ זה לא מעניין בכלל, מכיוון שאלגוריתם שתמיד מקבל כל קלט יפתור בעיה זו. (וודאי שאתם מבינים למה).

משפט ה-PCP (Probabilistically Checkable Proofs)

המשפט: $\forall \varepsilon > 0$, Gap-3SAT$[\frac{7}{8}+\varepsilon, 1]$ is NP-hard

ההוכחה היא אחת הארוכות והמורכבות ביותר במדעי המחשב, ופותחה במשך מספר שנים ע"י חוקרים הכוללים בין השאר את האנשים שכתבו את הספר שאנחנו לומדים ממנו ואת המרצה שאנחנו מתמוגגים ממנו. ב-2001 קיבל מולי ספרא (כן, כן, אותו מולי ספרא שאנחנו רואים פעם בשבוע) את פרס גדל יחד עם 8 חוקרים נוספים על ~~[illegible]~~ עבודתם בנושא משפט ה-PCP והקשר שלו לקושי בקירוב.

למותר לציין שההוכחה בת המאות עמודים אינה מוכלת בחומר של הקורס. אבל, בכל זאת, נניח את נכונותו ונעסוק בכמה מהשלכותיה.

ניזכר בהגדרה של NP באמצעות מכונה מוודאת ועד. כעת נגדיר מחלקה אחרת אשר דומה לה אך חלשה יותר: למוודא מותר לקרוא רק מספר סופי ($O(1)$) ביטים מהעד. מותר לו, עם זאת, לבחור אילו ביטים הוא קורא באמצעות הטלת מטבע, ומותר לו לטעות בהסתברות מאוד קטנה (כלומר לא לשים לב לשגיאה בעדות לקלט לא תקין, אך לא להיפך).

בעיית Gap-3SAT$[\frac{7}{8}+\varepsilon,1]$ שייכת למחלקה זו, בעזרת האלגוריתם הבא (שמתואר כאן באופן כללי, לא מדויק ולא פורמלי):

בהינתן נוסחת 3CNF ועדות שהיא השמה למשתני הנוסחה, המכונה מגרילה מספר קבוע של השמות של משתנים ומספר קבוע של הסגרים. היא בודקת האם ניתן לספק את כל הסגרים שבחרה באמצעות השמה שעומדת בתנאים של ההשמות שקראה (כלומר, כל משתנה

החלק הזה, כמו של העמוד הבא, לא ממש קשור לשאר החומר. שווה לקרוא, אבל אל תגזימו אם זה לא ממש ברור לכם. אם אתם בלחץ של זמן, קפצו על העמוד הזה והבא

שהיא יודעת את סדרכו היא משתמשת בו, והיא רצה על כל האפשרויות
של כל המשתנים האחרים המופיעים בפסוקים) אם קיימת השמה מספקת
כזו היא מקבלת, אחרת דוחה.
אם העד הוא השמה מספקת, אז היא מקבלת בהסתברות 1.
אם הנוסחה היא נוסחה שבה השמה לכל היותר מספקת $\frac{7}{8}+\varepsilon$ מהפסוקים
שלה. אזי שלכל עד שניקח, הסיכוי לקבל יהיה קטן כפי שנרצה
(תלוי בכמה הפסוקים והשמות בודקים כמובן). לכן $[1, \frac{7}{8}+\varepsilon]$ Gap-3SAT
שייכת למחלקה זו.
מעובדה זו, יחד עם משפט ה-PCP נובע שכל הבעיות
ב-NP שייכות למחלקה הזו (כי בעיה NP-קשה שייכת למחלקה הזו),
ולכן NP מוכלת בה. מכיוון שמחלקה זו מוכלת ב-NP באופן
טריוויאלי מהגדרתה, נובע שזוהי בעצם הגדרה שקולה ל-NP.

אז למה כל זה מעניין אותנו? מכיוון שזה אומר לנו על הרבה
דברים שאנחנו יכולים לעשות עם בעיות NP. למשל, דמיינו את
התרחיש הבא: אתם רוצים לשמור כסף בבנק, אבל אתם לא רוצים
שיגנבו אותו. מכיוון שאתם לא מעוניינים לספק תעודת זהות, הבנק
צריך דרך כלשהי לדעת שזה אתם לפני שהוא מוציא לכם כסף.
אתם רוצים שיהיה לכם סוד כלשהו שרק אתם יודעים ויוכיח שזה באמת אתם.
מועמד מושלם לפתור בעיה זו היא בעיה קשה (NP) אשר לכם יש את
העדות שנותנת פתרון, ומוכיח שזה אתם. אך אם תתנו לפקיד הבנק
את העדות, פקיד הבנק יוכל להשתמש בעדות למחרת ולהוציא לכם
את כל הכסף. בזכות מה שקראנו עכשיו, אנחנו יודעים שאפשר
(וגם איך אפשר) לאפשר לפקיד הבנק לקרוא רק מספר קטן
של ביטים מההוכחה שלכם ולוודא את נכונותה עם הסתברות שגיאה
זניחה. הדבר הזה יותר מהיר וגם יותר בטוח. למעשה, אפשר
גם לספק הוכחות-חסרות-מידע, שלא נותנות לפקיד אף רמז לגבי
העד שלכם, גם אם גילוי סליו מיליון הפעמים. ייתכן שנדבר יותר
על הנושא בשיעור הבא.

נעבור לדון בבעית אופטימיזציה אחרת, כמו למשל Max-Clique.
עד איזה קבוע ניתן לקרב אותה? נסתכל על מקרה פרטי של הבעיה:

<u>הקלט:</u> גרף $G=(V,E)$ המורכב מ-m שלשות של קודקודים שכל
כל שלישיה מהווה Independent Set.

<u>בעית המקסימום:</u> למצוא את הקליקה הגדולה ביותר.

אם נוכיח קושי למקרה זה, הרי שזה עדיין יהיה תקף למקרה הכללי.
נעשה זאת.

נסתכל על $\text{Gap-Clique}[(\frac{7}{8}+\varepsilon)m, m]$, כלומר, נדרש לקבל כאשר יש קליקה
הכוללת נציג <u>מכל</u> שלישיה, לדחות כאשר יש לכל היותר $\frac{7}{8}+\varepsilon$ מזה,
ואחרת לא אכפת לנו.

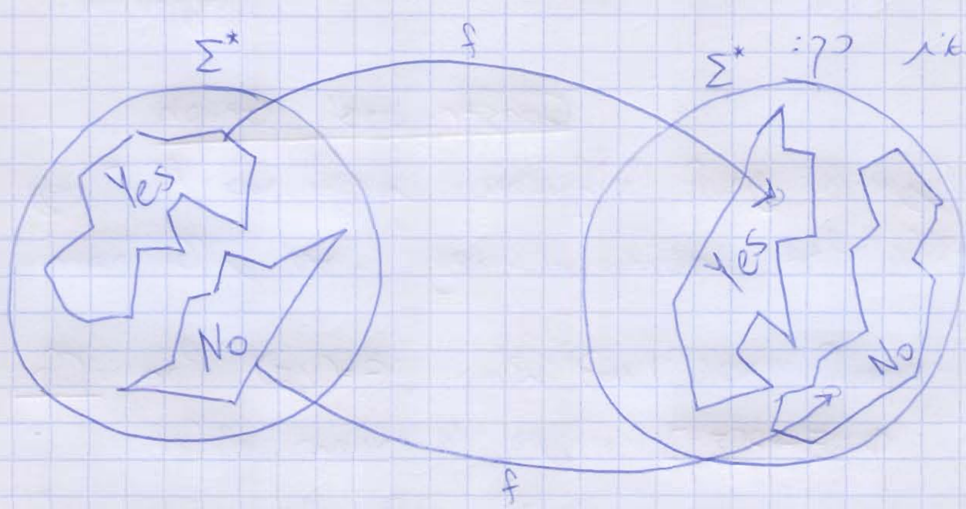
<u>טענה:</u> $\text{Gap-Clique}[(\frac{7}{8}+\varepsilon)m, m]$ היא NP-קשה.

<u>מסקנה (לאחר שנוכיח):</u> קשה לקרב את Max-Clique ביחס של $\frac{7}{8}+\varepsilon$.

איך נוכיח שבעית Gap היא NP-קשה? זה נראה נוח לעשות רדוקציה
מ- $\text{Gap-3SAT}[\frac{7}{8}+\varepsilon, 1]$, אך עושים רדוקציה בין בעיות Gap?

<u>רדוקציות משמרות Gap</u>

רדוקציית Karp משמרת Gap, מבעית Gap אחת לשניה, היא
רדוקציה שמעבירה קלטים טובים לקלטים טובים, קלטים רעים לקלטים
רעים, ועם קלטי ה-Gap היא עושה מה שבא לה. למעשה,
היא נראית כך:



נשתמש ברדוקציה משמרת Gap כדי להראות ש- $SAT \le_p Clique$.
למעשה, בפועל נתבונן על הרדוקציה המקורית שהשתמשנו בה כדי להוכיח ש- Clique היא NP-קשה ונוכיח שהיא משמרת Gap בין Gap-3SAT ל- Gap-Clique על אותו Gap (כלומר אותם $[\alpha,\beta]$)

~~[illegible]~~ בהינתן נוסחת 3CNF, ניצור קודקוד אחד עבור כל ליטרל (משתנה שמופיע מספר פעמים יופיע בגרף כמספר קודקודים). הקשתות בגרף יהיו כל הקשתות $(V\times V)$ <u>למעט</u> בין קודקודים "באותו הסגר" (כלומר ~~[illegible]~~ באותה שלישיה) ובין כל ליטרל לשלילתו (לעצמו, לכל משלימיו)

φ

$(\alpha \vee \beta \vee \gamma)$

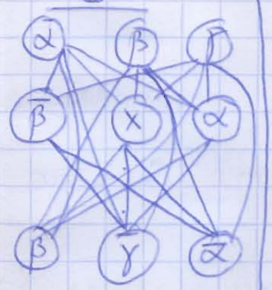
$(\bar\beta \vee x \vee \alpha)$

$\vdots$

$(\beta \vee \bar\gamma \vee \bar\alpha)$

$\Longrightarrow \quad \xrightarrow{f}$

G



כעת, מהוכחת ~~[illegible]~~ נכונות צריך להוכיח שלמות ונאותות.
הוכחת שלמות זהה לחלוטין להוכחה ברדוקציה בין בעיות ההכרעה.
אם לגבי נאותות רק לעשות צעד. בהינתן קליקה בגודל l ב-G, נתן להגדיר השמה (ע"י השמת T לכל ליטרל בקליקה והמשך כרצוננו) אשר מספקת לפחות $\frac{l}{m}$ מהפסוקים. לכן גם Gap-Clique$[\frac{7}{8}+\varepsilon,1]$ היא NP-קשה.

<u>Constraints' Graph</u>

ננסה להבין כמה מבעיות האופטימיזציה שלמדנו על מנת למצוא בעיה רחבה וכללית יותר. נעשה זאת באמצעות גרף אילוצים: (CSG)

<u>הגדרה:</u> גרף $G=(V,E)$, קבוצת "צבעים" אפשריים לקודקודים Σ, ואילוצים המתוארים ע"י פונקציה $\phi: E \to P[\Sigma^2]$

כלומר, יש לנו קבוצת צבעים לצבוע את הקודקודים בגרף, וכל קשת מציבה תנאי לגבי הקודקודים שלה. כל קשת היא למעשה אילוץ על הקודקודים בגרף.

נרצה להגדיר בעית מקסימום. ניתן לעשות זאת בשתי דרכים שונות, עם שני פרמטרי אופטימיזציה שונים: הקודקודים והקשתות.

לפי קודקודים - CSG_V

פתרון חוקי יהיה צביעה חלקית של הקודקודים $A:V\to\Sigma\cup\{\perp\}$, כאשר $\perp$ מסמן קודקוד לא צבוע, אשר מקיימת שכל קשת המחברת בין קודקודים צבועים מקיים את האילוצים שלה. פורמלית צביעה חוקית מוכרחה לקיים:

$$(u,v)\in E \;\&\; A(u),A(v)\in\Sigma \Rightarrow (A(u),A(v))\in\Phi(u,v)$$

מטרתנו היא למקסם את מספר הקודקודים שצבענו, כלומר לצבוע כמה שיותר קודקודים ועדיין לעמוד באילוצים.

לפי קשתות - CSG_E

בהגדרה זו פתרון חוקי הוא כל צביעה מלאה של הקודקודים $A:V\to\Sigma$. מטרתנו היא פשוט למקסם את מספר הקשתות שאילוציהן מקיימים, כלומר את מספר הקשתות $(u,v)\in E$ המקיימות $(A(u),A(v))\in\Phi(u,v)$.

שתי אפשרויות אלה אינן שקולות (כלומר, ערך הפרמטר אותו אנחנו ממקסמים לא תמיד יהיה אותו דבר, וגם לא תמיד הצביעה האופטימלית תהיה אותה צביעה לפי שני הגדלים), אך שתיהן מאוד שימושיות.

גרף אילוצים הוא הכללה די ברורה של k-צביעה של גרף. נגדיר Σ להיות $\{1,\dots,k\}$, ואת האילוצים של כל הקשתות להיות שאסור ששני הצבעים זהים. אך היא בעיה כללית מאוד, ובעיות רבות שאנו מכירים הן מקרים פרטיים שלה, לדוגמה: Clique, IS, 3SAT, VC, MaxCut וכו'. אתם מוזמנים לנסות למצוא כיצד לייצג בעיות אלה באמצעות גרף אילוצים (אך נראה זאת בהמשך ולכן זה לא הכרחי).

טענה: $Gap\text{-}CSG_V[\frac{7}{8}+\varepsilon,1]$ היא NP-קשה.

~~הוכחה~~

הוכחה: נראה רדוקציה מ- $Gap\text{-}3SAT[\frac{7}{8}+\varepsilon,1]$. בהינתן נוסחת CNF
φ נבנה גרף ~~[illegible]~~ בו כל הסגר הוא
קודקוד. קבוצת הצבעים שלנו תהיה $\Sigma=\{1,2,3\}$, וכל צבע
מייצג איזה ליטרל בתוך הפסוק "אחראי" על סיפוקו. אם צבענו
בצבע 1, אז הליטרל הראשון הוא בהכרח T. נגדיר קשת
בין שני קודקודים (הסגרים) אם יש בהם ליטרל ומשלימו, ונאסור על
צביעה שטוענת ששניהם אמת. למשל, בין שני הסגרים
(α,β,γ) ו- $(\bar{x},y,\bar{z})$ נאסור על הצביעה ~~[illegible]~~
שנותנת לראשון את ה~~[illegible]~~ צבע 1 ולשני את הצבע 3, אך
נתיר את שאר הצביעות. כעת, מספר הקודקודים שניתן לצבוע
מבלי לסתור על האילוצים הוא בדיוק מספר הפסוקים שניתן
לספק.

* kCSG זה CSG עם ~~[illegible]~~ k צבעים.

משפט: $Gap\text{-}kCSG_V[\delta,1] \leq_L Gap\text{-}k^L CSG_V[\delta^L,1]$ *

כלומר אם ~~[illegible]~~ להבדיל בין גרפים עם k צבעים שניתן
לצבוע את כל ~~[illegible]~~ קודקודים לבין כאלו שאפשר רק ~~[illegible]~~ לצבוע δ מהן זה קשה,
אז ~~[illegible]~~ גם קשה להבדיל בין גרפים עם k^L צבעים שניתן ~~[illegible]~~ לצבוע לבין כאלו
שאפשר ~~[illegible]~~ לצבוע רק δ^L ~~[illegible]~~ מהם.

הוכחה:

בהינתן גרף אילוצים עם k צבעים, נגדיר את G' להיות הגרף
בעל k^L צבעים הבא:

~~[illegible]~~ $V' = V^L$ (כל קודקוד חדש מייצג L-יה של קודקודים מקוריים)

~~[illegible]~~ $\Sigma' = \Sigma^L$ (כל צבע הוא למעשה צביעה של ה-L קודקודים)

E',Φ' יאסרו על G כזוג L-יות שיש להן קודקודים משותפים והם נותנים
לאותו קודקוד (מקורי) צבעים שונים, או שאחת מהן נותנת לקודקוד
צבע שעובר על אילוץ כלשהו בגרף המקורי.

כעת נראה שהרדוקציה באמת משמרת gap.

קלטים טובים: אם היתה בגרף המקורי (הקלט) צביעה חוקית, (של כל הקודקודים)
אז קל למצוא צביעה שלמה חוקית לגרף החדש: באמת ניתן לכל
אחד קודקוד את הצביעה שלו בגרף המקורי.

קלטים רעים: אנחנו רוצים להראות שאם בגרף המקורי ניתן לצבוע לכל
היותר δ צבעים, אז בגרף החדש ניתן לצבוע לכל היותר δ'. נראה
את הקונטרה-פוזיטיב: אם ניתן בחדש לצבוע יותר מ-δ' אז בהכרח
ניתן במקורי לצבוע δ מהקודקודים באופן חוקי.
אם צבענו יותר מ-δ' קודקודים, בהכרח הקודקודים האלה
(שהם לא יותר סדרות באורך L של קודקודים מקוריים) מכילים יותר מ-δ
קודקודים (יש רק δ' סדרות שנוצרות מ-δ קודקודים לכן בהכרח קיימת
הקודקודים הצבועים אינה מוכלת בה).
לכן ניתן לצבוע בגרף המקורי יותר מ-δ קודקודים, כאשר פשוט
ניתן לכל קודקוד מקורי את הצבע שלו לפי הגרף החדש. הצביעה
תהיה קונסיסטנטית (לא נצבע אותו קודקוד ביותר מצבע אחד) ומקיים
את כל האילוצים לפי בניית הגרף החדש.

לכן $Gap\text{-}kCSG_V[\delta,1] \le_L Gap\text{-}k'CSG_V[\delta',1]$.

טענה: $gap\text{-}kCSG_V[\delta,1] \le_L gap\text{-}IS[\delta/k,1,k]$
הוכחה: בהינתן גרף אילוצים G, ניקח כל קודקוד ונשכפל
אותו כמספר הצבעים ($V'=V\times\Sigma$). כעת ניתן לתאר כל
קודקוד כזוג סדור (u,i). נחבר בקשת את כל "גרסאות
הצבעים" השונות של כל קודקוד. $(i\neq j \Rightarrow ((u,i),(u,j))\in E')$
ונחבר בקשת כל שני קודקודים בצבעים שאינם תואמים את אילוצי
הגרף $((i,j)\notin\Phi(u,v) \Rightarrow ((u,i),(v,j))\in E')$.
כעת צביעה שלמה מתאימה ל-IS בגודל $\frac{1}{k}$ (נבחר "צבע"
אחד לכל קודקוד, לפי הצביעה השלמה של הגרף), ואם אין צביעה
של יותר מ-δ קודקודים, לא נמצא IS בגודל יותר מ-$\frac{\delta}{k}$.

אז מה עשינו פה היום? נזכר בשלושת הטענות האחרונות שהוכחנו.

1) $Gap\text{-}3CSG_v[\frac{7}{8}+\varepsilon, 1]$ is NP-hard

2) $Gap\text{-}kCSG_v[\delta, 1] \le_L Gap\text{-}k^l CSG_v[\delta^l, 1]$

3) $Gap\text{-}kCSG_v[\delta, 1] \le_L Gap\text{-}IS[\delta/k, 1/k]$

נבחר במשפט הראשון. לאחר מכן, נזכה במשפט השני $k=3$, $\delta=\frac{7}{8}+\varepsilon$, ונקבל ש- $Gap\text{-}3^l CSG_v[(\frac{7}{8}+\varepsilon)^l, 1]$ היא NP-קשה.
נשתמש במשפט השלישי ונקבל ש- $Gap\text{-}IS[\frac{(\frac{7}{8}+\varepsilon)^l}{3^l}, \frac{1}{3^l}]$ היא NP-קשה.

מהבנת הקשר שבין בעית Gap לבעית קירוב, נסיק שקשה לקרב את IS מסדר $\frac{1/3^l}{(\frac{7}{8}+\varepsilon)^l/3^l}=\frac{1}{(\frac{7}{8}+\varepsilon)^l}$. מכיוון ש- l יכול להיות גדול כפי שנרצה, $\frac{1}{(\frac{7}{8}+\varepsilon)^l}$ יכול להיות גדול כפי שנרצה, ומכך נקבל את המסקנה:

לא ניתן לקרב את IS (או Clique) עבור אף סדר קבוע בזמן פולינומיאלי (אלא אם P=NP)