סיבוכיות – תרגולים

תרגול 1 – 23.02.2010

הודעות:

- יהיה בוחן במשקל 15% מהציון הסופי.
- יהיו כנראה 7 תרגילי בית ללא ציון, הגשת 6 מהם חובה.
- אתר הקורס: http://www.cs.tau.ac.il/~idobene/Complexity10b

רדוקציות

הגדרה: בהינתן שתי שפות, L_1, L_2 , נאמר ש- L_1 **ניתנת לרדוקציה פולינומית** ל- L_2 מסוג קארפ, ונסמן זאת ב- $L_1 \le_p L_2$ אם קיימת פונקציה הניתנת לחישוב בזמן פולינומי f כך ש- $x \in L_1 \Leftrightarrow f(x) \in L_2$.

היום נראה $3\text{COL} \ge_p 3\text{NAE} \ge_p 4\text{NAE} \ge_p 3\text{SAT}$.

הגדרת הבעיות

פסוק kCNF הוא אוסף של k הסגרי "או", כל אחד מהם בן k ליטרלים.

דוגמה: הסגר 3CNF : $x_1 \vee x_2 \vee \bar{x}_3$.

3SAT : בהינתן פסוק 3CNF , האם קיימת השמה שמספקת את כל ההסגרים בו?

4NAE : בהינתן פסוק 4CNF , האם קיימת השמה בה בכל הסגר יש לפחות ליטרל אחד שמקבל T ולפחות ליטרל אחד שמקבל F ?

3NAE : כנ"ל עם פסוקי 3CNF .

3COL : בהינתן גרף פשוט, האם קיימת צביעה של הצמתים ב- 3 צבעים, כל שכל זוג צמתים שכנים מקבלים צבעים שונים?

רדוקציה I: $3\text{SAT} \le_p 4\text{NAE}$.

בהינתן פסוק φ מסוג 3CNF , נבנה פסוק φ' מסוג 4CNF . אם φ הוא על המשתנים $x_1,\ldots,x_n$, נוסיף ליטרל חדש z לעוד הסגר.

דוגמאות:

φ	φ'
$x_1 \vee x_2 \vee x_3$	$x_1 \vee x_2 \vee x_3 \vee z$
$\bar{x}_1 \vee x_4 \vee \bar{x}_7$	$\bar{x}_1 \vee x_4 \vee \bar{x}_7 \vee z$

הרדוקציה היא בבירור פולינומית.

אם ל- φ יש השמה מספקת, ניתן ל- z ערך F , ונקבל בכל הסגר ב- φ' משתנה אחד עם ערך T ואחד עם ערך F .

אם ל- φ' יש השמה NAE -מספקת: אם z קיבל ערך F , נשמיט אותו ונקבל השמה מספקת ל- φ . אחרת, נשים לב שגם ההשמה ההופכית, בה הופכים את ערכי כל המשתנים, היא גם השמה מספקת. בהשמה זו, z הוא F , ולכן חזרנו למקרה הקודם.

רדוקציה II: $4\text{NAE} \le_p 3\text{NAE}$.

$$\underbrace{x_1 \vee x_2 \vee x_3 \vee x_4}_{\psi} \rightarrow \begin{matrix} x_1 \vee x_2 \vee z_i \\ \underbrace{x_3 \vee x_4 \vee \bar{z}_i}_{\psi'} \end{matrix} .$$

כל הסגר 4CNF עובר לשני הסגרי 3CNF , בהם מופיע משתנה z_i ייחודי לאותו זוג הסגרים.

ברור כי ניתן לבצע את הרדוקציה בזמן פולינומי.

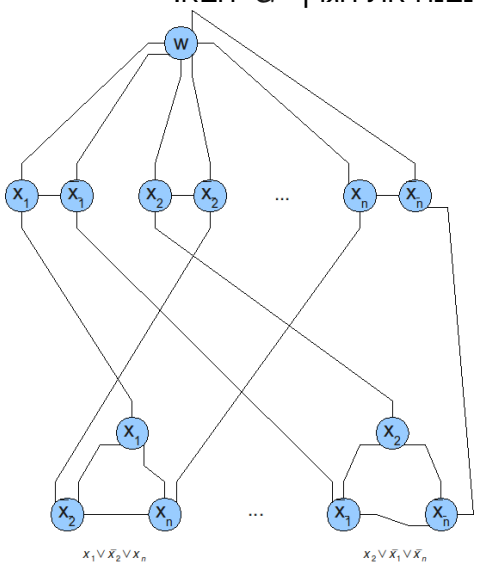
אם ל- ψ' יש השמה 3NAE -מספקת: עבור הסגר בודד כנ"ל, אם z_i הוא T אזי x_1 או x_2 הם F , ו- x_3 או x_4 הם F . אחרת, z_i הוא F , ואז x_1 או x_2 הם T ו- x_3 או x_4 הם F .

אם ל- ψ יש השמה מספקת: נפריד לארבעה מקרים:

1. אם $x_1 = x_2$ ו- $x_3 = x_4$: במקרה זה, $x_1 \ne x_3$. ניתן ל- z_i ערך הפוך מ- x_1 , וזה יספק את זוג ההסגרים.
2. אם $x_1 = x_2$ ו- $x_3 \ne x_4$: שוב, ניתן ל- z_i ערך הפוך מ- x_1 . ההסגר השני מסתפק בכל מקרה.
3. באופן דומה, אם $x_1 \ne x_2$ ו- $x_3 = x_4$.
4. אם $x_1 \ne x_2$ ו- $x_3 \ne x_4$: שני ההסגרים מסתפקים ללא תלות בהצבת z_i .

רדוקציה III: $3NAE \leq_p 3COL$.
בהינתן פסוק 3NAE φ על המשתנים $x_1,\ldots,x_n$ ו- m הסגרים:

נבנה את הגרף G הבא:



נקבל גרף עם $3m+2n+1$ צמתים, ולכן הבניה אורכת זמן פולינומי באורך הקלט.
אם ל- ψ יש השמה 3NAE מספקת: נגדיר את הצביעה הבאה ל- G : נצבע את w בירוק. לכל $1\leq i\leq n$, אם x_i הוא T , ניתן ל- x_1 בשכבה השנייה צבע כחול ול- $\bar{x}_i$ אדום, אחרת ל- x_i אדום ול- $\bar{x}_i$ כחול. בכל הסגר, ליטרל אחד קיבל T וליטרל שני קיבל F , ולכן בצביעה לכל משולש בשכבה השלישית שכן אחד כחול ושכן אחד אדום. ניתן להשלים זאת לצביעה של כלל המשולש.
$\Leftarrow$: נניח בה"כ ש- w צבוע ירוק. אם x_i צבוע בכחול בשכבה השנייה, ניתן לו ערך T , אחרת ניתן לו ערך F . נניח בשלילה שקיים הסגר בו כל הליטרלים קיבלו T (או F). אזי קיים משולש המתאים להסגר שכל שכניו צבועים כחול (אדום). לכן, המשולש עצמו צבוע באדום וירוק בלבד (כחול וירוק). אבל לא ניתן לצבוע משולש ב- 2 צבעים. סתירה! לכן, זוהי השמה NAE -מספקת.

תרגול 2 – 02.03.2010

סיבוכיות זיכרון

הגדרות:

סיבוכיות זיכרון תוגדר על מ"ט עם שלושה סרטים:

- סרט קלט לקריאה בלבד.
- סרט עבודה לקריאה וכתיבה, מוגבל בזיכרון.
- סרט פלט לכתיבה בלבד.

נאמר שמכונה **משתמשת בזיכרון** $\boldsymbol{f(n)}$ אם לקלט באורך n לא משתמשים ביותר מ-$f(n)$ מקום על סרט העבודה.

$\mathbf{SPACE}\left(\boldsymbol{f(n)}\right)$ - אוסף השפות להן קיימת מ"ט כנ"ל עם זיכרון $f(n)$.

אורקלים: בהינתן שפה $O\subseteq\Gamma^*$, $\boldsymbol{M^O}$ היא מ"ט עם סרט נוסף שניתן לכתוב עליו קלט x, וביחידת זמן אחת מוחזר האם $x\in O$ או לא.

בהינתן מחלקת סיבוכיות A, $\boldsymbol{A^O}$ הוא אוסף כל השפות שניתנות להכרעה על ידי M^O, כאשר $L(M)\in A$.

משפט ההיררכיה

טענה: קיימת מ"ט אוניברסלית M עם התכונה הבאה: בהינתן קלט מ"ט M^* שרצה בזמן $f(n)$ וקלט x, M מסמלצת את ההרצה של M^* על x תוך שימוש בזיכרון $c\cdot f(|x|)$ (c קבוע).

משפט: לכל אורקל O ולכל שתי פונקציות נורמליות $f(n),g(n)$ כך ש-$f(n)=\omega(g(n))$ מתקיים $\mathrm{SPACE}(g(n))^O\subsetneq\mathrm{SPACE}(f(n))^O$.

נראה מקרה פרטי: $\mathrm{SPACE}(n^2)^O\subsetneq\mathrm{SPACE}(n^3)^O$.

נגדיר מ"ט D באופן הבא: על קלט x, תהי M_x מ"ט שקידודה x (עם אורקל O). D תריץ את M_x על x במשך $|x|^{2.9}$ זיכרון (כלומר, לא חוצים בסרטי העבודה את גבול הזיכרון הזה).

אם M_x עצרה על x במהלך השימוש בזיכרון זה, D תענה הפוך, כלומר $D(x)=1-M_x(x)$. אם M_x לא עצרה, D תחזיר 0.

מצד אחד, קל לראות כי $L(D)\in\mathrm{SPACE}(n^3)^O$.

נראה ש-$L(D)\notin\mathrm{SPACE}(n^2)^O$: נניח בשלילה שיש מ"ט M' שרצה בזיכרון αn^2 ומכריעה את $L(D)$. בה"כ, ניתן להניח של-M' קידוד ארוך כרצוננו. כאשר מריצים את M' על $\langle M'\rangle$: M' עוצרת תוך $\alpha|\langle M\rangle|^2\ll|\langle M\rangle|^{2.9}$ זיכרון. אבל אז, נקבל $D(\langle M'\rangle)\neq M'(\langle M'\rangle)$, ולכן $L(M')\neq L(D)$, כמבוקש.

מש"ל.

stConn

קלט: גרף מכוון $G=(V,E)$ על n צמתים, ושני צמתים s,t.

שאלה: האם קיים מסלול (מכוון) בין s ל-t?

נראה $\mathrm{stConn}\in\mathrm{SPACE}(\log^2 n)$.

האלגוריתם: נראה, בהינתן שני צמתים u,v אלגוריתם הבודק האם יש מסלול באורך לכל היותר d בין u ל-v:

1. אם $d=1$, בודקים אם יש קשת מ-u ל-v.
2. אם $d>1$, עוברים על כל הצמתים w בגרף, ולכל אחד מהם בודקים האם יש מסלול באורך $\left\lceil\frac{d}{2}\right\rceil$ בין u ל-w ויש מסלול באורך $\left\lceil\frac{d}{2}\right\rceil$ בין w ל-v.

כל איטרציה לוקחת $O(\log n)$ זיכרון. עומק הרקורסיה הוא לכל היותר $\log n$ (בכל שלב d קטן פי 2). בסך הכל, נדרש $O(\log^2 n)$ זיכרון.

תרגול 3 – 09.03.2010

<u>הודעה</u>: בודק תרגילים: יובל רוכמן. מספר התא יישלח באימייל.

<u>הגדרות</u>:

- $\mathbf{Ntime}\left(n^k\right)$ היא מחלקת כל השפות עבורן קיימת מ"ט לא דטרמיניסטית שמכריעה אותן בזמן $O\left(n^k\right)$.
- $\mathbf{NP}=\bigcup_{k\geq 1}\mathrm{NTime}\left(n^k\right)$.
- נגדיר בנוסף $\mathbf{EXP}=\bigcup_{k\geq 1}\mathrm{Time}\left(2^{n^k}\right)$ ו- $\mathbf{NEXP}=\bigcup_{k\geq 1}\mathrm{Ntime}\left(2^{n^k}\right)$.

הכרעה לעומת חיפוש

נניח שיש אורקל A שבהינתן גרף, מכריע האם הוא 4-צביע בזמן פולינומי. נרצה למצוא אלגוריתם פולינומי A^* שמוצא 4-צביעה לגרף שיש בו צביעה כזו.

בהינתן גרף G, יהי G' הגרף המתקבל מ-G על ידי הוספת קליק K_4. עוברים על כל הצמתים המקוריים (לא כולל ה-K_4 שהוספנו) אחד אחרי השני. בצומת v מתאים, נגדיר את הגרפים:

$$G_1=\left(V\left(G'\right),E\left(G'\right)\cup\left\{v_2,v_3,v_4\right\}\right)$$
$$G_2=\left(V\left(G'\right),E\left(G'\right)\cup\left\{v_1,v_3,v_4\right\}\right)$$
$$G_3=\left(V\left(G'\right),E\left(G'\right)\cup\left\{v_1,v_2,v_4\right\}\right)$$
$$G_4=\left(V\left(G'\right),E\left(G'\right)\cup\left\{v_1,v_2,v_3\right\}\right)$$

<u>האלגוריתם</u>:

- בהתחלה, בודקים בעזרת A ש-G הוא 4-צביע.
- מסדרים את הצמתים לפי סדר: $v_1,\ldots,v_n$.
- לאחר השלב ה-i, G^i עדיין 4-צביע.
- מריצים את האורקל A לבחירת צבע j ל-v_i כך שהגרף G^j הוא 4-צביע.
- בסיום, מקבלים 4-צביעה חוקית לכל צמתי G' (ו-G).

The padding argument

<u>טענה</u>: $\mathrm{EXP}\neq\mathrm{NEXP}\Rightarrow\mathrm{P}\neq\mathrm{NP}$.

די להראות שאם $\mathrm{P}=\mathrm{NP}$, אזי $\mathrm{EXP}=\mathrm{NEXP}$.

תהי $L\in\mathrm{NEXP}$. אזי קיימת מ"ט לא דטרמיניסטית M שמכריעה את L בזמן $2^{p(n)}$, עבור פולינום p. נגדיר שפה חדשה L' באופן הבא: $L'=\left\{x\$1^t\middle|x\in L,t=2^{p(|x|)}\right\}$. נטען ש-$L'\in\mathrm{NP}$.

נבנה במכונה פולינומית לא דטרמיניסטית שמכריעה את L'. על קלט y, מוודאים שהוא מהצורה $y=x\$1^t$, ובודקים שמספר ה-1-ים מקיים $t=2^{p(|x|)}$. בדיקה זו מתקיימת בזמן פולינומי ב-t (וב-$|y|$).

אם מספר ה-1-ים לא נכון, דוחים. אם הוא נכון, מריצים את M על x, ומקבלים או דוחים בהתאמה.

זמן הריצה הכולל: $\mathrm{poly}\left(|y|\right)+2^{p(x)}=\mathrm{poly}\left(|y|\right)$.

לכן, $L'\in\mathrm{NP}$, ולכן לפי ההנחה $L'\in\mathrm{P}$.

לכן, קיימת מכונה M' שמכריעה את L' בזמן פולינומי. כדי להראות ש-$L\in\mathrm{EXP}$, בהינתן קלט x, נרפד אותו לקלט y שהוא "מועמד חוקי" ל-L', $|y|=\Theta\left(2^{p(|x|)}\right)$. נריץ על y את M', ונקבל הכרעה של L בזמן $\mathrm{EXP}(|x|)=\mathrm{POLY}\left(|y|\right)$.

שפות דלילות ב-NP

תהי L שפה המקיימת: לכל $n\geq 496$ מתקיים $\left|L\cap\left\{0,1\right\}^n\right|=2n^4+9$. הוכיחו כי $L\in\mathrm{NP}\Rightarrow L\in\mathrm{coNP}$.

סקיצת ההוכחה: נראה ש-$\bar{L}\in\mathrm{NP}$. לכל $n\geq 496$, יש רשימה באורך $2n^4+9$ $w_1,\ldots,w_t$ שהן המילים היחידות באורך n הזה ב-L. ה"הוכחה" ש-$x\notin L$ תהיה רשימת כל המילים הללו, כאשר לכל w_i מצרפים את ההוכחה ש-$w_i\in L$. כדי לוודא ש-$x\notin L$, מוודאים שכל המילים $w_i\in L$ וש-x אינו שווה לאף אחת מהן.

תרגול 4 – 16.03.2010

NL

$\mathrm{NL}=\mathrm{NSpace}\left(\log n\right)$.

משפט: stCon שלמה ב- NL .

משפט *Savitch*: $\mathrm{NL}\subseteq\mathrm{Space}\left(\log^2 n\right)$.

משפט אימרמן: $\mathrm{NL}=\mathrm{coNL}$.

2SAT

משפט: $\overline{\mathrm{2SAT}}$ היא NL -שלמה.

הוכחה:

שלב I: $\overline{\mathrm{2SAT}}\in\mathrm{NL}$.

בהינתן פסוק φ מסוג 2CNF על המשתנים $x_1,\ldots,x_n$, נגדיר את הגרף G הבא:

לכל הסגר מהצורה $\left(u\vee w\right)$, נחבר את $\bar{u}$ ל-w ואת $\bar{w}$ ל-u (בקשתות מכוונות).

הרעיון: אם יש מסלול מ-u ל-w , אזי אם u הוא T בכל השמה מספקת, גם w חייב להיות T .

טענה: ל-φ אין השמה מספקת אם ורק אם קיים i עבורו יש מסלול מכוון מ-x_i ל-$\bar{x}_i$, וגם יש מסלול מכוון מ-$\bar{x}_i$ ל-x_i .

תחילה, נניח את נכונות הטענה, ונראה כיצד נובע כי $\overline{\mathrm{2SAT}}\in\mathrm{NL}$.

בהינתן קלט φ , נבחר i , וננסה לנחש מסלול באורך לכל היותר $2n$ מ-x_i ל-$\bar{x}_i$ ומ-$\bar{x}_i$ ל-x_i . אם מצאנו זוג מסלולים כנ"ל, נקבל. אחרת, נדחה.

הערה: אין צורך לבנות באופן מפורש את הגרף כדי לבצע סיורים עליו. לכן, נדרש $O\left(\log n\right)$ זיכרון.

הוכחת הטענה:

אם יש מסלול מ-x_i ל-$\bar{x}_i$, ומ-$\bar{x}_i$ ל-x_i עבור i כלשהו, בכל השמה מספקת ל-φ :

אם x_i הוא T , אזי $\bar{x}_i$ הוא T .

אם $\bar{x}_i$ הוא T , אזי x_i הוא T .

לכן, אין השמה מספקת ל-φ .

אם לכל i אין מסלול מ-x_i ל-$\bar{x}_i$ או אין מסלול מ-$\bar{x}_i$ ל-x_i , נבנה את ההשמה בשלבים, בכל שלב נבחר משתנה x_i שלא קיבל ערך. נסמן ב-u את הצומת (או המשתנה) מבין $\left\{x_i,\bar{x}_i\right\}$ עבורו לא קיים מסלול מ-u ל-$\bar{u}$. ניתן ל-u ערך T .

נשים לב: אם ב-G יש מסלול מ-x ל-y , אזי יש גם מסלול מ-$\bar{y}$ ל-$\bar{x}$.

כל ליטרל שנגיש מ-u יקבל T , וההופכי של כל ליטרל שקיבל T יקבל F .

שתי סוגי סתירות עלולות להיווצר:

1. לא ייתכן שיש מסלול גם מ-u ל-w וגם מ-u ל-$\bar{w}$.
2. לא ייתכן שמשתנה יקבל ערכים סותרים בשלבים שונים.

שלב II: נרצה להוכיח ש- $\overline{\mathrm{2SAT}}$ היא NL -שלמה.

נראה $\mathrm{stCon}\leq_{\mathrm{L}}\overline{\mathrm{2SAT}}$:

בהינתן גרף מכוון ושני צמתים s,t , נגדיר פסוק ψ באופן הבא:

$$\psi=\left(s\vee s\right)\wedge\left(\bar{t}\vee\bar{t}\right)\wedge\left(\bigwedge_{\left(u,w\right)\in\vec{E}\left(G\right)}\left(\bar{u}\vee w\right)\right)$$

הרדוקציה בזיכרון לוגריתמי:

ניתן למצוא כל חלק בפלט הרדוקציה (למשל לבדוק האם הסדר ספציפי קיים) בזיכרון לוגריתמי.

נכונות:

אם יש השמה מספקת ל-ψ , s חייב להיות T , ו-t חייב להיות F . בנוסף, כל צומת שנגיש מ-s חייב להיות T , ולכן t לא נגיש מ-s , כלומר אין מסלול מכוון מ-s ל-t .

אם אין מסלול מ-s ל-t : ניתן ערך T לכל המשתנים הנגישים מ-s ו-F לכל האחרים. שני ההסגרים הראשונים כמובן מסתפקים, ולכל הסגר אחר מהצורה $\bar{u}\vee w$: אם הוא לא מסתפק, אזי $u=\mathrm{T}$ ו-$w=\mathrm{F}$, ולכן u נגיש מ-s ו-w לא. סתירה, כי היות ו-$\left(u,w\right)$ קשת, w נגיש מ-s דרך u .

מש"ל.

מסקנה (ממשפט אימרמן): 2SAT היא NL -שלמה.

בעיות נוספות

1. בהינתן גרף מכוון ושני צמתים s,t, האם קיימים בדיוק 3 מסלולים מכוונים שונים מ-s ל-t? הבעיה ב- NL .
2. בהינתן גרף על n צמתים, האם קיים בו מסלול מכוון פשוט באורך לפחות $\frac{n}{2}$?
3. בהינתן גרף, האם יש בו קליק בגודל 3007 ?

תרגול 5 – 23.03.2010

<u>סיבוכיות זיכרון</u>

הרכבת רדוקציות

אם f רדוקציה במקום לוגריתמי מ- A ל- B , ו- g רדוקציה במקום לוגריתמי מ- B ל- C :
כדי להרכיב רדוקציות, מחזיקים סרט וירטואלי עבור הפלט של f . אם מתבקשים לחשב את $g\circ f(x)$, מריצים את M_g על הסרט הווירטואלי, ובכל פעם שצריך ביט j מתוך $f(x)$, מריצים את M_f על מנת לחשב אותו.
לכן, צריכת הזיכרון = צריכת הזיכרון של f + צריכת הזיכרון של g + $O(\log n)$, ובסך הכל $O(\log n)$.

סיווג בעיות

1. בהינתן גרף מכוון G ושני צמתים s,t , האם קיימים בדיוק שני מסלולים שונים מ- s ל- t ?
<u>פתרון</u>: הבעיה ב- NL . לשם כך, די לוודא ש:
   1. ב- G יש לפחות שני מסלולים מ- s ל- t .
   2. ב- G יש פחות משלושה מסלולים מ- s ל- t .

   הבעיה הראשונה ב- NL : מנחשים מראש מקום בו המסלולים שונים, מנחשים שני מסלולים באורך לכל היותר n , בודקים שהם אכן מסלולים ושהם שונים במקום שניחשנו. אם כן, מקבלים.
   לגבי הבעיה השנייה: הבעיה המשלימה היא: "האם קיימים לפחות שלושה מסלולים שונים מ- s ל- t ?" בעיה זו היא ב- NL (כמו קודם), ולכן לפי משפט אימרמן, גם הבעיה השנייה ב- NL .
2. בהינתן גרף מכוון G , האם הקוטר שלו הוא לפחות $\frac{n}{2}$? ($\text{קוטר}_G=\max_{u,v} dist(u,v)$)

<u>פתרון</u>: הבעיה המשלימה: הקוטר הוא פחות מ- $\frac{n}{2}$, כלומר המרחק בין כל שני צמתים ב- G קטן מ- $\frac{n}{2}$. להכרעת בעיה זו, נעבור על כל זוגות הצמתים בגרף, ולכל זוג ננסה לנחש מסלול באורך קטן מ- $\frac{n}{2}$. אם מצאנו מסלולים כנ"ל לכל זוג, נקבל. אחרת, נדחה.

לכן, לפי משפט אימרמן, גם הבעיה המקורית היא ב- NL .

3. בהינתן G,s,t כנ"ל, האם יש מסלול באורך <u>בדיוק</u> 17 בין s ל- t ?
<u>פתרון</u>: ב- L : עוברים על כל סדרות הצמתים באורך 17 , ובודקים האם זהו מסלול מ- s ל- t .
4. בהינתן גרף <u>לא מכוון</u> G ושני צמתים s,t , האם קיים מסלול מ- s ל- t ?
<u>פתרון</u>: ב- L , לפי משפט *Reingold* משנת 2005.
5. בהינתן גרף G , האם יש בו חלוקה לשני קליקים?
<u>פתרון</u>: ב- G יש חלוקה לשני קליקים אם ורק אם ב- $\bar{G}$ יש חלוקה לשתי קבוצות בלתי תלויות אם ורק אם $\bar{G}$ הוא 2 -צביע אם ורק אם כל המעגלים ב- $\bar{G}$ זוגיים. לכן, הבעיה המשלימה: האם יש מעגל אי-זוגי ב- $\bar{G}$? בעיה זו ב- NL , ולכן לפי משפט אימרמן, גם הבעיה המקורית ב- NL .
6. בהינתן G , האם קיימות $A,B\subseteq V(G)$ כך ש- $|A\cap B|=1$ ו- $A\cup B=V(G)$ כך ש- A קליק ו- B קבוצה בלתי תלויה?
<u>פתרון</u>: ב- L . עוברים על כל הצמתים בגרף, ולכל צומת בודקים האם שכניו הם קליק, והאם קבוצת הלא-שכנים היא בלתי תלויה.
7. בהינתן גרף G , האם לכל שני מעגלים פשוטים C_1,C_2 ב- G מתקיים $|C_1|+|C_2|<n$?
<u>פתרון</u>: הבעיה coNP -שלמה.
הבעיה המשלימה: האם קיימים C_1,C_2 כך ש- $|C_1|+|C_2|\geq n$? יש רדוקציה מבעיית המעגל ההמילטוני.

תרגול 6 – 13.04.2010

<u>מחלקות סיבוכיות הסתברותיות</u>

<u>הגדרה</u>: עבור $p_1,p_2\in[0,1]$, נגדיר את $\mathbf{BPP}(p_1,p_2)$ כמחלקת השפות L עבורן קיימת מכונת טיורינג M דטרמיניסטית שרצה בזמן פולינומי, כך שלכל $x\in\{0,1\}^*$, אם $x\in L$ אזי $\Pr_r[M(x,r)=1]\geq p_2$, ואם $x\notin L$ אזי $\Pr_r[M(x,r)=1]\leq p_1$, כאשר r מציין סדרה של הטלות מטבע, $|r|=\text{Poly}(|x|)$.

<u>הערה</u>: נשים לב שההסתברות היא על פני המטבעות האקראיים r ולא על פני הקלטים.

<u>הערה</u>: ניתן להגדיר את הנ"ל בעזרת מכונת טיורינג הסתברותית שמטילה מטבעות אקראיים. מספרם יהיה פולינומי כי זמן הריצה פולינומי.

מחלקות סטנדרטיות

טעות דו-צדדית: $\text{BPP}=\text{BPP}\left(\frac{1}{3},\frac{2}{3}\right)$.

טעות חד-צדדית: $\text{RP}=\text{BPP}\left(0,\frac{1}{2}\right)$, $\text{coRP}=\text{BPP}\left(\frac{1}{2},1\right)$.

<u>נשים לב</u>: $\text{RP}\subseteq\text{NP}$.

תהא $L\in\text{RP}$, ותהא M מ"ט המתאימה לה. נחשוב על r כעל עד במכונת NP . אם $x\in L$, אזי קיים r שמוביל את המכונה לקבל (בעצם לפחות $\frac{1}{2}$ מהעדים האפשריים עושים זאת), ואם $x\notin L$, אזי לא קיים r כזה.

אפשר להראות: $\text{BPP}=\text{BPP}\left(\frac{1}{2}-n^{-10},\frac{1}{2}+n^{-10}\right)=\text{BPP}\left(2^{-n^{10}},1-2^{-n^{10}}\right)$.

<u>שאלה פתוחה</u>: האם $\text{SAT}\in\text{BPP}$?

<u>טענה</u>: אם $\text{SAT}\in\text{BPP}$ אזי $\text{NP}=\text{RP}$.

כזכור, $\text{RP}\subseteq\text{NP}$, ולכן די להראות ש- $\text{NP}\subseteq\text{RP}$. נראה ש- $\text{SAT}\in\text{RP}$.

מההנחה, $\text{SAT}\in\text{BPP}$, ולכן קיימת מ"ט פולינומית דטרמיניסטית M , שבהינתן נוסחה וסדרת מטבעות אקראיים r , מחזירה אם הנוסחה ספיקה בהסתברות שגיאה לכל היותר 2^{-n} (על פני r).

נבנה מ"ט M' , שבהינתן נוסחה ϕ מבצעת: לכל משתנה x_i נקבע ערך T , נציב אותו ב- ϕ ונריץ את M על הנוסחה המתקבלת, כדי לדעת אם הנוסחה שקיבלנו ספיקה. אם כן, נקבע את x_i להיות T , ואחרת F (בכל שלב ממשיכים עם הנוסחה שהתקבלה). כעת, נבדוק אם ההשמה שקיבלנו מספקת את ϕ . אם כן, נחזיר *כן*. אחרת, נחזיר *לא*.

אם $\phi\notin\text{SAT}$, אזי ההשמה בסוף האלגוריתם בהכרח לא תספק את ϕ , כדרוש.

אם $\phi\in\text{SAT}$, וכל הפעלות המכונה M החזירו תשובה נכונה, אזי האלגוריתם ימצא השמה מספקת ויחזיר *כן*. ההסתברות שלפחות אחת מבין n ההרצות של M החזירה תשובה לא נכונה היא לכל היותר $n\cdot 2^{-n}$, ו- $n\cdot 2^{-n}\leq\frac{1}{2}$, ובהסתברות לפחות $\frac{1}{2}$ תוחזר תשובה נכונה (הסתמכנו על זה ש- $\Pr[A\cup B]\leq\Pr[A]+\Pr[B]$).

זמן הריצה של M' הוא n פעמים זמן הריצה של M , ולכן פולינומי.

כמו כן, לכל $L\in\text{NP}$ ניתן להפעיל רדוקציה פולינומית ל- SAT , ואז להפעיל את האלגוריתם RP הנ"ל על התוצאה.

מש"ל.

האם $\text{SAT}\in\text{BPP}\left(\frac{1}{2}-n^{-10},\frac{1}{2}+n^{-10}\right)$? שאלה פתוחה, השקולה ל- $\text{SAT}\in\text{BPP}$.

האם $\text{SAT}\in\text{BPP}\left(\frac{1}{2}-2^{-n^{10}},\frac{1}{2}+2^{-n^{10}}\right)$? כן.

האלגוריתם:

בהסתברות $p=\frac{1}{2}-2^{-n^{10}}$, החזר *כן*.

בהסתברות $1-p=\frac{1}{2}+2^{-n^{10}}$, הגרל השמה לנוסחה. אם מספקת, החזר *כן*, ואחרת *לא*.

ניתוח:

אם $\phi\notin\text{SAT}$, נחזיר שהיא ספיקה בהסתברות $p\leq\frac{1}{2}-2^{-n^{10}}$.

אם $\phi\in SAT$, נחזיר שהיא ספיקה בהסתברות לפחות $\left(\frac{1}{2}-2^{-n^{10}}\right)+\left(\frac{1}{2}+2^{-n^{10}}\right)\cdot\frac{1}{2^n}$, וזה לפחות $\frac{1}{2}+2^{-n^{10}}$.

תרגול 7 – 27.04.2010

<u>רנדומיזציה/דה-רנדומיזציה</u>

לינאריות התוחלת

לכל $X_1,\ldots,X_n$ מ"מ, מתקיים $E[X_1]+\ldots+E[X_n]=E[X_1+\ldots+X_n]$.

1. יהי φ פסוק 3SAT עם m הסגרים, בכל הסגר 3 משתנים שונים (פסוק E3SAT). נוכיח כי קיימת השמה ל- φ המספקת לפחות $\frac{7}{8}m$ הסגרים.

<u>הוכחה</u>: נגריל השמה מקרית, כל משתנה יקבל T או F בהסתברות $\frac{1}{2}$ באופן ב"ת. נסמן לכל $1\le i\le m$ ב- X_i את המשתנה האינדיקטור למאורע שההסגר ה- i מסופק, כלומר: $X_i=\begin{cases}1 & \text{ההסגר ה}-i\text{ מסופק}\\ 0 & \text{אחרת}\end{cases}$.

לכל הסגר ספציפי, ההסתברות שהוא לא מסופק היא $\frac{1}{8}$. לכל, $E[X_i]=\frac{7}{8}$. נסמן ב- X את מספר ההסגרים המסופקים. אזי $E[X]=E\left[\sum_{i=1}^{m}X_i\right]=\sum_{i=1}^{m}E[X_i]=\frac{7}{8}m$.

בכל הגרלה קיימת בחירה של המשתנים כך ש- X הוא לפחות כמו התוחלת שלו. לכן, קיימת השמה שבה יש לפחות $\frac{7}{8}m$ הסגרים מסופקים.

2. יהי G גרף לא מכוון עם m קשתות. חתך ב- G הוא חלוקה של הצמתים לשתי קבוצות. גודל החתך הוא מספר הקשתות שמחברות צומת מצד א' של החתך לצומת מצד ב' של החתך.

נטען: מתקיים תמיד: $\text{MAX-CUT}(G)\ge\frac{m}{2}$.

<u>הערה</u>: בעיית MAX-CUT היא NP -קשה.

<u>הוכחה</u>: בהינתן G, נגריל כל צומת להיות בצד א' או בצד ב' בהסתברות $\frac{1}{2}$ באופן ב"ת. לכל קשת e, יהי X_e המ"מ האינדיקטור למאורע ש- e בחתך. אזי $E[X_e]=\frac{1}{2}$, ולכן $E\left[\sum_{e\in E(G)}X_e\right]=\sum_{e\in E(G)}E[X_e]=\frac{m}{2}$. לכן, קיים חתך שגודלו לפחות כמו התוחלת.

דה רנדומיזציה

<u>שיטה א'</u>: **שיטת התוחלת המותנה**

<u>טענה</u>: בהינתן גרף G על צמתים $x_1,\ldots,x_n$, נניח שקבענו עבור חלק מהצמתים באיזה צד של החתך הם נמצאים. ניתן לחשב בזמן פולינומי את תוחלת גודל החתך שיתקבל אם נגריל את שאר הצמתים באופן ב"ת.

<u>הוכחה</u>:

עוברים על כל הקשתות וסוכמים לתוחלת את תוחלת המשתנה האינדיקטור עבור כל קשת. לכל קשת שלוש אפשרויות:

1. שני הצמתים הסמוכים לה כבר נקבעו: במקרה זה, הקשת תורמת בוודאות 1 או 0 לגודל החתך.
2. שני הצמתים הסמוכים לה לא נקבעו: כמו קודם, קשת זו תורמת $\frac{1}{2}$ לתוחלת.
3. בדיוק צד אחד נקבע: ההסתברות שהקשת תהיה בחתך היא $\frac{1}{2}$. לכן, קשת זו תתרום גם כן $\frac{1}{2}$.

תיאור האלגוריתם:

לכל $1 \le i \le n$:

נחשב בעזרת האלגוריתם הנ"ל את תוחלת גודל החתך אם x_i יהיה בצד א', ואת תוחלת גודל החתך אם x_i יהיה בצד ב'.

נבחר ל-x_i צד שלא מוריד את גודל התוחלת המקורית.

אזי: $$E\left[\begin{array}{c}\text{גודל החתך}\\ \text{בשלב כלשהו}\\ \text{לפני שקובעים}\\ \text{ל-}x_i\end{array}\right]=\frac{E\left[\begin{array}{c}\text{גודל החתך}\\ \text{אם } x_i \text{ בצד א}\end{array}\right]+E\left[\begin{array}{c}\text{גודל החתך}\\ \text{אם } x_i \text{ בצד ב}\end{array}\right]}{2}$$

בסיום הריצה, נקבל חתך (קבענו לכל הצמתים צד) שגודלו לפחות $\frac{m}{2}$.

<u>שיטה ב'</u>: **מרחבי מדגם קטנים**

<u>הגדרה</u>: עבור מ"מ $X_1,\ldots,X_n$, נאמר שהם ***k*-ב"ת** (*k-wise-independent*), אם כל קבוצה של k מתוכם ב"ת.

<u>דוגמה</u>: שימוש ל-MAX-CUT :

בהוכחה שקיים חתך שגודלו $\frac{m}{2}$, לא היינו צריכים באמת אי-תלות מלאה בין כל הקשתות. מספיק לדרוש שבחירת הצדדים לצמתים תהיה 2-ב"ת, ואז ההסתברות של כל קשת להיות בחתך היא $\frac{1}{2}$, ומשם באותו אופן, מקבלים שתוחלת גודל החתך היא $\frac{m}{2}$.

למה קיימים מרחבים k-ב"ת?

קיימת התפלגות על $X_1,\ldots,X_n$, $X_i \in \{0,1\}$, שהיא k-ב"ת, וגודלה $O\left(n^{\left\lfloor \frac{k}{2} \right\rfloor}\right)$.

נתאר בנייה עבור $k=2$:

בניה:

יהיו $Y_1,\ldots,Y_{\log n}$ מ"מ שמקבלים 0 או 1 בהסתברות $\frac{1}{2}$ באופן ב"ת.

לכל $\emptyset \ne S \subseteq \{Y_1,\ldots,Y_{\log n}\}$, נגדיר $X_S=\left(\sum_{Y\in S} Y\right) \bmod 2$.

נכונות: המ"מ הם ב"ת בזוגות.

עבור שתי קבוצות $S \ne T$, מתקיים:

$$\Pr[X_S=X_T]=\Pr[X_S+X_T=0 \pmod 2]=\Pr\left[\sum_{Y\in S\Delta T} Y=0 \pmod 2\right]=\frac{1}{2}$$

בשיעורי הבית נוכיח: $\text{MAX-CUT}(G) \ge \frac{m}{2}+\Omega\left(\sqrt{m}\right)$.

תרגול 8 – 04.05.2010

משפחות *Hashing* ב"ת בזוגות ומשפט *Valiant-Vazirani*

תזכורת:

קבוצה של מ"מ $X_1,\ldots,X_n$ שמקבלים ערכים מעל $\{1,\ldots,p\}$ נקראים ***k*-ב"ת** אם כל k מהם ב"ת.

ניתן לבנות באופן מפורש התפלגות של n משתנים k-ב"ת בגודל $O\left(n^{\left\lfloor\frac{k}{2}\right\rfloor}\right)$.

הבנייה עבור $k=2$: כדי לבנות $n-1$ מ"מ מעל $\{0,1\}$ שהם ב"ת בזוגות, ניתן להשתמש בכל הפולינומים הלינאריים הלא-טריביאליים מעל $\mathbb{Z}_2^{\log n}$. לוקחים מ"מ $Y_1,\ldots,Y_{\log n}$, ואז מגדירים לפיהם את $X_1,\ldots,X_n$. למשל, אם $X_1=Y_1+Y_3+Y_7$, $X_2=Y_1+Y_4+Y_{16}$, אזי $X_1=X_2$ אם ורק אם $Y_1+Y_4+Y_{16}=Y_1+Y_3+Y_7$, ומהבנייה והתכונות של $\mathbb{Z}_2$ נקבל את הרצוי.

משפחות גיבוב ב"ת בזוגות

משפט: יהיו $m,n\in\mathbb{N}$, $m<n$. אזי קיימת משפחה H_m^n של פונקציות מ-$\{0,1\}^n$ ל-$\{0,1\}^m$ המקיימת את הדרישות הבאות:

1. לכל $x,y\in\{0,1\}^n$ $x\neq y$, ולכל $a,b\in\{0,1\}^m$, $\Pr_{h\in_U H_m^n}\left[h(x)=a\wedge h(y)=b\right]=2^{-2m}$.
2. הקידוד של כל $h\in H_m^n$ הוא באורך $\mathrm{Poly}(n)$ ביטים.
3. בהינתן קידוד של $h\in H_m^n$ ונקודה $x\in\{0,1\}^n$, ניתן לחשב את $h(x)$ בזמן פולינומי באופן דטרמיניסטי.

משפחה כזאת נקראת **משפחת גיבוב ב"ת בזוגות**.

משפט *Valiant-Vazirani*: נניח שקיים אלגוריתם דטרמיניסטי פולינומי A, שעל קלט פסוק CNF φ, במידה ול-φ יש *השמה מספקת יחידה*, הוא מוצא השמה זאת (אין שום הנחה לגבי פסוקים עם 0 או לפחות 2 השמות מספקות). אזי $\mathrm{NP}=\mathrm{RP}$.

הוכחה:

טענה הסתברותית: תהי H_k^n משפחת גיבוב ב"ת בזוגות מ-$\{0,1\}^n$ ל-$\{0,1\}^k$ כמו קודם. תהי $S\subseteq\{0,1\}^n$ כך ש-$2^{k-2}\leq|S|\leq 2^{k-1}$. אזי $\Pr_{h\in_U H_k^n}\left[\left|\{x\in S\,|\,h(x)=0^k\}\right|=1\right]\geq\frac{1}{8}$.

הוכחה:

יהי N המ"מ שמייצג את מספר האיברים מ-S שממופים ל-0^k. אזי $E[N]=2^{-k}\cdot|S|\in\left[\frac{1}{4},\frac{1}{2}\right]$. ההסתברות ש-$N\geq 2$ היא לכל היותר $\binom{|S|}{2}\cdot\underbrace{2^{-2k}}_{\text{אי תלות בזוגות}}$.

ההסתברות ש-$N\geq 1$, לפי עקרון ההכלה וההפרדה היא לפחות:

$$\sum_{x\in S}\Pr\left[h(x)=0^k\right]-\sum_{x<x'\in S}\Pr\left[h(x)=0^k\wedge h(x')=0^k\right]=$$

$$=2^{-k}\cdot|S|-\underbrace{\binom{|S|}{2}\cdot 2^{-2k}}_{\text{אי תלות בזוגות}}\geq 2^{-k}\cdot|S|-2^{-2k}\cdot|S|^2=2^{-k}\cdot|S|\cdot\left(1-2^{-k}\cdot|S|\right)\geq\frac{1}{8}$$

נראה אלגוריתם שבהסתברות לפחות $\frac{1}{8n}$, בהינתן פסוק CNF φ, נכריע האם φ ספיק או לא (כמובן, בהינתן האלגוריתם A). האלגוריתם יקבל פסוק ספיק בהסתברות $\frac{1}{8n}$, ידחה פסוק לא ספיק בהסתברות 1.

האלגוריתם: (בהינתן פסוק φ על n משתנים)

ננחש באופן אקראי $2\leq k\leq n+1$ (מעכשיו, נניח שיש ל-φ בין 2^{k-2} ל-2^{k-1} השמות מספקות).

נבנה פסוק ψ באופן הבא: $\psi(x)=\varphi(x)\wedge h(x)=0^k$. ניתן לתאר דרישה זו היות ו-h ניתנת לחישוב יעיל, כאשר h נבחרת באופן אקראי מתוך H_k^n.

נכונות:

נבחן 2 מקרים:

אם ל- φ אין השמה מספקת, אז היות ו- $\psi=\varphi\wedge(\text{משהו})$, אז גם ל- ψ אין השמה מספקת.

אם ל- φ יש בין 2^{k-1} ל- 2^{k-2} השמות מספקות, אז בהסתברות $\frac{1}{n}$ נבחר באלגוריתם את הטווח הנכון. נסמן ב- S את קבוצת ההשמות הטובות ל- φ . אזי מהטענה, בהסתברות לפחות $\frac{1}{8}$ יהיה בדיוק $x\in S$ יחיד עבורו h מקרי שנבחר מקיים $h(x)=0$. לכן, בהסתברות לפחות $\frac{1}{8n}$ בחרנו טווח נכון, וגם בחרנו h שמקיימת שיש איבר יחיד שמקיים $h(x)=0$. לכן, הרצת האלגוריתם A תמצא את ההשמה, ולפיכך נכריע את SAT .

תרגול 9 – 11.05.2010

<u>אלגוריתמי קירוב ובעיית ה- TSP</u>

בהינתן בעיית מקסימיזציה, אלגוריתם A הוא c-קירוב אם לכל קלט x מתקיים $A(x)\geq\frac{\mathrm{OPT}(x)}{c}$.

בהינתן בעיית מינימיזציה, אלגוריתם A הוא c-קירוב אם לכל קלט x מתקיים $A(x)\leq c\cdot\mathrm{OPT}(x)$.

בעיית הסוכן הנוסע – TSP

בהינתן גרף K_n ופונקציית משקל $w:E(K_n)\to\mathbb{R}^+$, מצא מעגל המילטוני ממשקל מינימלי.

בעיית ההכרעה המתאימה היא NP-קשה.

<u>טענה</u>: נניח שקיים אלגוריתם c-קירוב לבעיית TSP עבור c קבוע כלשהו. אזי P=NP.

ההוכחה בתרגיל הבית.

בעיית TSP עם אי-שוויון המשולש

כמו TSP רגיל, עם ההגבלה שלכל x,y,z צמתים, $w(x,z)\leq w(x,y)+w(y,z)$.

באופן כללי, לכל מסלול $x_1,\ldots,x_n$ מתקיים $w(x_1,x_n)\leq\sum_{i=1}^{n-1}w(x_i,x_{i+1})$.

אלגוריתם 2-קירוב לבעיית TSP עם אי-שוויון המשולש (בהינתן גרף K_n ופונקציית משקל w):

1. נמצא עץ פורש מינימלי בגרף T.
2. נכפיל כל קשת בעץ לקבלת מולטי-גרף T'.

   אזי T' קשיר, ודרגת כל צומת זוגית, ולכן ב-T' יש מעגל אוילריאני.
3. נמצא את מעגל אוילר זה (בעזרת DFS).
4. נלך לאורך המעגל האוילריאני, נקפוץ מעל צמתים בהם כבר ביקרנו (פרט לשלב האחרון בו סוגרים את המעגל).

<u>נכונות</u>:

קפיצות לא מעלות את המחיר (בגלל אי-שוויון המשולש). בפרט, מחיר מעגל ההמילטון שנקבל הוא לכל היותר משקל T'. כמו כן, $w(T')=2\cdot w(T)$.

כל מעגל המילטוני (בפרט OPT) מכיל מסלול המילטוני (מסלול המילטוני הוא בפרט עץ פורש), ולפיכך משקלו לפחות כמשקל עפ"מ, כלומר משקל T.

קיבלנו: $\left(\begin{array}{c}\text{משקל הסיור}\\ \text{שקיבלנו}\end{array}\right)\cdot\frac{1}{2}\geq\text{משקל }T\geq\begin{array}{c}\text{משקל מעגל}\\ \text{המילטון מינימלי}\end{array}$, כלומר משקל הסיור שמתקבל חסום על ידי $2\cdot\mathrm{OPT}$, כלומר זהו 2-קירוב.

אלגוריתם 3/2-קירוב לבעיית TSP עם אי-שוויון המשולש

<u>הרעיון</u>: לבנות מעגל אוילר זול יותר, ובכך לקבל קירוב טוב יותר.

הגדרה: **שידוך** (זיווג) בגרף הוא אוסף קשתות שאין להן צומת משותף. **שידוך מושלם** הוא שידוך שמכסה את כל הצמתים בגרף.

בגרף עם מספר זוגי של צמתים קיים תמיד שידוך מושלם, ויש אלגוריתם שמוצא שידוך מושלם ממשקל מינימלי בזמן פולינומי.

<u>האלגוריתם</u>:

1. נמצא עץ פורש מינימלי T.
2. תהי O קבוצת הצמתים מדרגה אי-זוגית.
3. נמצא שידוך מושלם מינימלי M ב-O.
4. מקבלים ש-$T\cup M$ הוא גרף בו לכל צומת יש דרגה זוגית. נמצא בו מעגל אוילר, ונמשיך באותו אופן כמו קודם.

<u>נכונות</u>:

נשים לב שבכל גרף (ובפרט ב-T), סכום הדרגות של כלל הצמתים הוא פעמיים מספר הקשתות. לכן, מספר הצמתים מדרגה אי-זוגית הוא זוגי, כלומר $|O|$ זוגי.

כל מעגל המילטוני על מספר זוגי של צמתים ניתן לפירוק לשני זיווגים מושלמים. לכן, $\text{משקל זיווג מושלם מינימלי ב}-O\geq\text{משקל מעגל המילטוני מינימלי ב}-O\cdot\frac{1}{2}$.

נשים לב שמשקל מעגל המילטון מינימלי ב-O הוא לכל היותר משקל מעגל המילטון מינימלי בגרף המקורי, היות וכל מעגל בגרף המקורי ניתן להפוך למעגל ב-O על ידי קפיצות (ושימוש באי-שוויון המשולש).

נקבל: $\underbrace{w(T \cup M)}_{\substack{\text{מחיר המעגל} \\ \text{באלגוריתם}}} \leq w(T) + w(M) \leq w(\text{OPT}) + \frac{1}{2} \cdot w(\text{OPT}) = \frac{3}{2} \cdot w(\text{OPT})$.

במילים אחרות, קיבלנו $\frac{3}{2}$-קירוב.

תרגול 10 – 25.05.2010

בעיות GAP וקושי הקירוב

בעיות פער (GAP)

בהינתן בעיית מקסימיזציה/מינימיזציה A, יש להכריע עבור קלט x האם $\mathrm{OPT}_A(x)\geq\beta$ או $\mathrm{OPT}_A(x)\leq\alpha$ (ניתן להניח שמתקיים $\alpha<\mathrm{OPT}_A(x)<\beta$, כי אם $\alpha=\beta$, זו בעיית הכרעה רגילה).

<u>טענה</u>: תהי A בעיית מינימיזציה עבורה $\mathrm{Gap}-A[\alpha,\beta]$ היא NP-קשה. אזי NP-קשה לקרב את A בפקטור $\frac{\beta}{\alpha}-\varepsilon$ לכל $\varepsilon>0$.

נניח בשלילה שקיים אלגוריתם S שמהווה $\frac{\beta}{\alpha}-\varepsilon$-קירוב ל-$A$. נכריע את $\mathrm{Gap}-A[\alpha,\beta]$ באופן הבא:

בהינתן קלט x, נריץ את S על x ונבדוק את ערך הפתרון שמתקבל.
אם ערך הפתרון קטן מ-β, נאמר ש-$\mathrm{OPT}_A(x)\leq\alpha$, ואחרת נאמר ש-$\mathrm{OPT}_A(x)\geq\beta$.

נכונות:

אם $\mathrm{OPT}_A(x)\leq\alpha$, אזי S יחזיר פתרון שערכו לכל היותר $\left(\frac{\beta}{\alpha}-\varepsilon\right)\cdot\alpha<\beta$.

אם $\mathrm{OPT}_A(x)\geq\beta$, כל אלגוריתם יחזיר פתרון שערכו לפחות β.
לכן, נקבל הכרעה ל-$\mathrm{Gap}-A[\alpha,\beta]$, בסתירה.

משפט ה-PCP (גרסת קושי-קירוב): לכל $\varepsilon>0$ הבעייה $\mathrm{Gap}-\underbrace{\mathrm{E3SAT}}_{\substack{\text{בכל הסגר}\\ \text{3 משתנים שונים}}}\left[\frac{7}{8}+\varepsilon,1\right]$ היא NP-קשה.

בעיית MAX-2SAT

נראה רדוקציה מבעיית $\mathrm{Gap\text{-}E3SAT}\left[\frac{7}{8}+\varepsilon,1\right]$ לבעיית $\mathrm{Gap\text{-}2SAT}[\alpha,\beta]$ עבור ערכי α,β כלשהם.

בהינתן פסוק 3CNF φ עם m הסגרים, נבנה פסוק 2CNF φ' עם $10m$ הסגרים.

$$\underset{\varphi}{x\vee y\vee z}\quad\underset{\varphi'}{(x)(y)(z)(w)(\bar{x}\vee\bar{y})(\bar{y}\vee\bar{z})(\bar{w}\vee x)(\bar{w}\vee y)(\bar{w}\vee z)}$$

- w הוא משתנה שונה בין כל זוג עשיריות.
- התפקידים של x,y,z סימטריים.

נכונות:

נניח שיש השמה שבה אף אחד מהליטרלים x,y,z אינו מסתפק. עבור בחירת $w=\mathrm{F}$, מסתפקים 6 הסגרים ב-φ', ולא יותר.
נניח שבדיוק אחד מתוך x,y,z מסתפקים. עבור בחירת $w=\mathrm{F}$, מסתפקים 7 הסגרים ב-φ' ולא יותר.
נניח ששניים מתוך x,y,z מסתפקים. לכל בחירה של w, בדיוק 7 מסתפקים.
אם כל הליטרלים של x,t,z מסתפקים, עבור בחירת $w=\mathrm{T}$, 7 הסגרים מסתפקים ולא יותר.
אם ב-φ כל m ההסגרים מסתפקים, קיימת השמה ל-φ' בה $7m$ מההסגרים מסתפקים.

אם ב-φ, לכל השמה לכל היותר $\left(\frac{7}{8}+\varepsilon\right)\cdot m$ הסגרים מסתפקים, בכל השמה של φ' מסתפקים לכל היותר $\left(\frac{7}{8}+\varepsilon\right)\cdot m\cdot 7+\left(\frac{1}{8}-\varepsilon\right)\cdot m\cdot 6=\frac{55}{8}m+\varepsilon\cdot m$ הסגרים.

לכן, הבעיה $\mathrm{Gap\text{-}2SAT}\left[\frac{55}{80}+\varepsilon',\frac{7}{10}\right]$ היא NP-קשה. לכן, לפי הטענה הקודמת, קשה לקרב את MAX-2SAT בפקטור $\frac{7}{10}\cdot\frac{80}{55}-\varepsilon=\frac{56}{55}-\varepsilon$ לכל $\varepsilon>0$.

תרגול 11 – 01.06.2010

CSG , VC -ו- IS

פתרון שאלה 2 מתרגיל 5

הבעיה: תן אלגוריתם עם קירוב טוב מ- 2 ל- VC לגרפים r -רגולריים, כאשר r קבוע.

מספר הקשתות בגרף r -רגולרי עם n צמתים הוא $\frac{r\cdot n}{2}$.

כל צומת בכיסוי מכסה r קשתות, לכן גודל הכיסוי המינימלי הוא לפחות $\frac{n}{2}$.

נמצא צביעה לגרף עם $r+1$ צבעים כך שכל שני צמתים סמוכים מקבלים צבעים שונים.

ניקח את r מחלקות הצבע הקטנות ביותר – הן מהוות כיסוי לגרף שגודלו לכל היותר $\frac{r}{r+1}\cdot n$.

קיבלנו קירוב $\frac{2r}{r+1}$, כמבוקש.

המטרה: להוכיח שלא ניתן לקרב את IS בכל פקטור קבוע.
לשם כך, נגדיר בעיה חדשה, CSG .

הגדרה: **הבעיה $k-$CSG** :
קלט:
גרף G על n צמתים עם קשת בין כל זוג צמתים.
כמו כן, נתונה קבוצת צבעים Σ , $|\Sigma|=k$.
לכל זוג צמתים $u,v\in V(G)$, מוגדר אוסף אילוצים מתוך $\Sigma\times\Sigma$.
אוסף האילוצים מוגדר על ידי פונקציה $f:E(G)\to P(\Sigma\times\Sigma)$.
המטרה:
למצוא צביעה $\varphi:V(G)\to\Sigma\cup\{\perp\}$, $\perp\notin\Sigma$ כך שכמה שיותר צבעים יקבלו צבע מ- Σ ולכל $u,v\in V(G)$ אזי מתקיים $\varphi(u),\varphi(v)\in\Sigma$ אם $\langle\varphi(u),\varphi(v)\rangle\in f(u,v)$.

Gap-kCSG$[a,b]$ - בעיית ההכרעה לשאלה: "האם בגרף כנ"ל עם $|\Sigma|=k$ ניתן לצבוע b -חלק מהצמתים, או כל צביעה חוקית צובעת לכל היותר a -חלק מהצמתים?".

דוגמאות:

- בעיית k -צביעת הגרפים.
$|\Sigma|=k$, לכל שני צמתים לא שכנים, אוסף האילוצים המותר הוא $\Sigma\times\Sigma$, ולכל שני צמתים סמוכים, אוסף האילוצים המותר הוא $\{\langle i,j\rangle | i\neq j\}$.
- IS - אפשר עם צבע יחיד.
- 3SAT :
כל צומת ייצג הסגר.
$\Sigma=\{1,2,3\}$.
לכל שני הסגרים שלא מכילים משתנה משותף, קבוצת האילוצים המותרת היא $\Sigma\times\Sigma$.
האילוצים בין כל שני הסגרים המכילים משתנים משותפים יהיו כאלה שימנעו סתירה.
הסגר יצבע בצבע i אם הליטרל ה-i מספק אותו.

מסקנה: Gap-kCSG$\left[\frac{7}{8}+\varepsilon,1\right]$ היא NP -קשה (כי Gap-3SAT מקרה פרטי שלה).

טענות:

1. Gap-kCSG$[\alpha,\beta]\leq$Gap-IS$\left[\frac{\alpha}{k},\frac{\beta}{k}\right]$.

נבנה רדוקציה באופן הבא:
גרף מלא G עם n צמתים ואילוצים מתוך א"ב בגודל k יעברו לגרף G' עם $k\cdot n$ צמתים:
1. כל צומת ב-G יעבור לקלסטר צמתים $v_1,\ldots,v_k$ כאשר $v_1,\ldots,v_k$ מהווים קליק.

2. לכל שני צמתים $u,v\in V(G)$ כך ש- $(i,j)\notin f(u,v)$, נחבר קשת בין u_i ל- v_j.

נכונות:

אם ב- G קיימת צביעה $\varphi:V(G)\to\Sigma\cup\{\perp\}$, כך ש- β-חלק מהצמתים מקבלים צבע מ- Σ, לכל $v\in V(G')$ שקיבל צבע מ- Σ, נבחר את $v_1\in V(G')$ להיות ב- IS. בחרנו צומת אחד לכל היותר מכל קלסטר ללא הפרת איסורים, ולכן גודל ה- IS הוא $\frac{\beta\cdot n}{n\cdot k}=\frac{\beta}{k}$.

אם ב- G' יש IS בגודל $\alpha\cdot n$, אלה הם $\alpha\cdot n$ צמתים מקלסטרים שונים. נגדיר צביעה ל- G באופן הבא: לכל צומת v, אם אחד מהצמתים בקלסטר שלו, v_i נבחר ל- IS, נצבע את v ב- i. אחרת, נצבע את v ב- $\perp$. ניתן לראות שצביעה זו צובעת α-חלק מהצמתים.

2. לכל $\ell\geq 1$ טבעי, $\text{Gap-}k\,\text{CSG}[\alpha,\beta]\leq_{\text{P}}\text{Gap-}k^{\ell}\,\text{CSG}[\alpha^{\ell},\beta^{\ell}]$.

$$\text{Gap-E3SAT}\left[\frac{7}{8}+\varepsilon,1\right]\leq\text{Gap-3CSG}\left[\frac{7}{8}+\varepsilon,1\right]\overset{(2)}{\leq}\text{Gap-3}^{\ell}\text{CSG}\left[\left(\frac{7}{8}+\varepsilon\right)^{\ell},1\right]\overset{(1)}{\leq}\text{Gap-IS}\left[\left(\frac{\frac{7}{8}+\varepsilon}{3}\right)^{\ell},\left(\frac{1}{3}\right)^{\ell}\right]$$

לכן, קשה לקרב את IS בפקטור טוב מ- $\frac{1}{\left(\frac{7}{8}+\varepsilon\right)^{\ell}}$ לכל $\varepsilon>0$. לכן, לא ניתן לקרב את IS בכל פקטור קבוע.

ההיררכיה הפולינומית

NP$=\Sigma_1$ - מחלקת כל השפות L עבורן $x\in L\Leftrightarrow\exists \underbrace{w}_{\substack{\text{באורך}\\ \text{פולינומי}}}.\ \underbrace{M(x,w)}_{\substack{\text{מכונת טיורינג}\\ \text{דטרמיניסטית פולינומית}}}=1$.

coNP$=\Pi_1$ - מחלקת כל השפות L עבורן $x\in L\Leftrightarrow\forall \underbrace{w}_{\substack{\text{באורך}\\ \text{פולינומי}}}.\ \underbrace{M(x,w)}_{\substack{\text{מכונת טיורינג}\\ \text{דטרמיניסטית פולינומית}}}=1$.

Σ_2 - מחלקת כל השפות L עבורן $x\in L\Leftrightarrow\exists w_1.\forall w_2.M(x,w_1,w_2)=1$.

Π_2 - כנ"ל, אבל $x\in L\Leftrightarrow\forall w_1.\exists w_2.M(x,w_1,w_2)=1$.

באותו אופן, מגדירים את Σ_i ו- Π_i.

דוגמאות:

1. $\text{Max-Clique}\in\Sigma_2$: $\text{Max-Clique}=\left\{\langle G,k\rangle\middle|\begin{array}{c}\text{גודל הקליק המקסימלי}\\ \text{ב}-G\text{ הוא בדיוק }k\end{array}\right\}$.

   הסבר: $\exists \underbrace{S_1}_{\substack{\text{קליק}\\ \text{בגודל }k}}.\ \forall S_2.\ \underbrace{M(x,S_1,S_2)}_{\substack{S_1-\text{בודקת ש}\\ \text{בגודל }k\text{ ו}-S_2\text{ אינו קליק}\\ \text{בגודל }k+1}}=1$.

2. $\text{Min-DNF}\in\Pi_2$: $\text{Min-DNF}=\left\{\varphi\text{ נוסחת DNF}\middle|\begin{array}{c}\text{אין נוסחה }\varphi'\\ \text{שקולה קטנה יותר}\end{array}\right\}$.

   הסבר: $\forall \underbrace{\varphi'}_{\text{פסוק}}.\exists \underbrace{x}_{\text{השמה}}.\ \underbrace{M(\varphi,\varphi',x)}_{\substack{M\text{ תבדוק ש}-\varphi'\text{ קטנה יותר מ}-\varphi,\\ \text{ואם כן תבדוק שאכן }x\text{ שונה בין }\varphi\text{ ל}-\varphi'}}=1$.

   הערה: כנראה ששפה זו היא Π_2 -שלמה.

טענות:

- $\Sigma_i\subseteq\Pi_{i+1}$.
- $\Pi_i\subseteq\Sigma_{i+1}$.
- $\text{BPP}\subseteq\Sigma_2\cap\Pi_2$.

הגדרה: $\text{PH}=\bigcup_i\Sigma_i$.

PCP

הגדרה: $\mathbf{PCP}(r,q)$ - אוסף השפות L עבורן קיימת מערכת הוכחה כך ש:

- אם $x\in L$, המוודא (הסתברותי) מקבל בהסתברות 1.
- אם $x\notin L$, המוודא (הסתברותי) מקבל בהסתברות לכל היותר $\frac{1}{2}$.

המוודא לא מטיל יותר מ- $O(r)$ מטבעות, ולא מבצע יותר מ- $O(q)$ שאילתות להוכחה.
אורך ההוכחה חסום על ידי $O(q)\cdot 2^{O(r)}$.

המטרה: להוכיח כי $\text{NP}\subseteq\text{PCP}(\text{Poly}(n),1)$.

רעיון: **QuadEq** (בעיה NP -קשה).
איך נבנה פרוטוקול הוכחה?
נקרה להשמה מספקת u (באורך n).
מחשב את $u\otimes u$ - מטריצה או וקטור בגודל n^2 שמכילה את כל הזוגות $u_i\cdot u_j$.
נכתוב את קידוד $Hadamard$ ל- u ו- $u\otimes u$.

עבור וקטור a באורך k, ניתן להגדיר פונקציה לינארית $f(x_1,\ldots,x_k)=\sum_{i=1}^{k}a_ix_i$.

הקידוד – הצבת כל הערכים האפשריים בתוך הפונקציה f (פעם אחת u מהווה את המקדמים, ובפעם השנייה $u\otimes u$).
הבודקים – בודקים בעזרת "מבחן לינאריות" שאכן הצבנו את הקידוד של u ו-$u\otimes u$.
בודקים שהווקטור האחד הוא אכן טנזור של הווקטור השני.
לוקחים סכום מקרי של המשוואות הנתונות, ובודקים בקידוד של $u\otimes u$ האם באמת הפתרון חוקי.