את בעיית UG ראינו שנוכל לקרב בפקטור 2 ואפילו בפקטור קטן טיפה מ-2 אבל לא בהגדרה קבוע (תלוי בדרגת הגרף).

Gap-UG [ε,1-ε] - היא בעיה שלא סביר שהיא NP-קשה. מצד שני לא מכירים אלג' פולינומי הפותר אותה.

* בעיית פירוק לגורמים היא בעיה ב-NP אך לא סביר שהיא NP-קשה כיוון שהיא גם בעיה ב- coNP אז.

בבעיית Gap-UG האילוצים הם מסוג מיוחד כיוון שלא אילוץ מכל זוג יחודי אפשרי. למשל, אם צבענו קודקוד בצבע אחד אז הקודקוד השכן שלו יכול לקבל צבע יחיד.

נשים לב שזו בעיה קלה אם מסתכלים על סיפוק כל האילוצים. פשוט בוחרים קודקוד, צובעים אותו ושאר הגרף נצבע כתוצאה מהאילוצים אלא אם הגענו לסתירה, מספר הצבעים קבוע וצביעת הגרף מתבצעת בזמן פולינומי.

אם נסתכל על הבעיה שרוצה לספק 1-ε, הבעיה הופכת להיות קשה יותר. נראה שהבעיה הזו אינה NP-קשה אך מניחים שהיא לא ב-P.

Gap-MC [1-√ε, 1-ε] - רוצים למצוא חלוקה של קודקודי הגרף כך שמספר הקשתות החוצות בין הקבוצות הוא לפחות 1-ε או להחליט שאין אף חלוקה עבורה יותר מ-1-√ε מהקשתות חוצות בין הקבוצות. (נשים לב שזו בעצם בעיה פרטית של UG (כיוון שאפשר להסתכל על זה כצביעת גרף ב-2 צבעים ואז בצביעת קודקוד, צבע השכנים נקבע)

נשים לב שהבעיה gap-Max-Cut [1-1.01ε, 1-ε] היא בעיה NP-קשה.

נזכר בבעיית חשבון הבנק: רוצים להפקיד כסף ו"ידיד" מנגנון שיאפשר רק לנו להוציא מן הבנק כדי למשוך כסף. כדי לעשות זאת, נצמיד לחשבון "סוד". למשל נצרף גרף שהוא 3-צביע ורק אנחנו נדע איך לצבוע את הגרף. הבעיה היא שאנו רוצים לשכנע את הפקיד שאנו יודעים לצבוע את הגרף ב-3 צבעים מבלי לחשוף את הצביעה בפני הפקיד.

כדי לפתור את הבעיה נגדיר את הפרוטוקול הבא: "נפרוס" את הגרף על השולחן. אנחנו נבחר פרמוטציה של 3 הצבעים ונכניס למעטפות אטומות את הצביעה של כל קודקוד. הבנקאי יבחר קשת רנדומית ויבדוק רק אם 2 הקודקודים שמחוברים אליה צבועים בצבעים שונים. הסיכוי שמישהו יצליח "לעבוד" עלינו היא $\frac{1}{|E|}$. לכן אם נעשה זאת סו בפעמים למשל, הסיכוי שמישהו יצליח לעבוד עלינו מבלי שנתפוס אותו יהיה מספיק קטן.

BPP

פתרון בעיות באמצעות רנדומיות. למשל, את בעיית בדיקת ראשוניות ניתן לבדוק באמצעות רנדומיות ב-P (ולאחרונה התגלה שגם ללא רנדומיות (גם ב-P)).

ראינו את בעיית SAT שהיא בעיה פרטית של TQBF שבו כל הכמתים הם E. בעיית SAT היא NP-שלמה ובעיית TQBF נמצאת ב-PSPACE.

בעיית TQBF מצומצמת היא Σ_i-complete. אנו מגבילים את הנוסחה ככה שמספר ה"בלוקים" של כמתים מאותו סוג הוא לכל היותר i. (כלומר מספר ההחלפות בין E ל-∀ בנוסחה הוא i-1). (וכן מתחילים עם הכמת ∃).

4.6.09 ②

סיבוכיות - שיעור 13

Σ_1 היא ב-NP ו-Π_1 היא ב-coNP.

<u>מכונת טיורינג הסתברותית</u> - מחלקת סרט נוסף: הסרט הרנדומי.

שפה $L \in BPP$ אם קיימת מ"ט הסתברותית M אם לכל x, ההסתברות שהמכונה תחזיר ש-'$x \in L$' היא לפחות 2/3. $Pr_r[M(x,r)='x \in L'] > 2/3$.
(כהנחה ש $x \in L$ באמת).

נסתכל מחלקה אחרת:

$x \in L \Rightarrow Pr_r[M(x,r) > \frac{1}{2}]$

$x \notin L \Rightarrow Pr_r[M(x,r) \leq \frac{1}{2}]$

כאן הכל הוא מאוד חד ולכן המחלקה הזו יותר חזקה. זו שקולה למחלקה הקרויה PP והיא מכילה את NP. (כדי להראות ש NP במחלקה זו, נגריל מטבע בסיכוי חצי, אם יצא 1 נחזיר T. אחרת, נריץ את המכונה ונחזיר את תשובתה. הסתברנו את הבעיה מההפרש בין 0 לגדול מ-$\frac{1}{2}$ לגדול מ-$\frac{1}{2}$).

נניח ויש לנו מכונה ב-BPP, אנחנו רוצים שהיא תחזיר תשובה נכונה באחוז בודדים טוב יותר, לשם כך נריץ את המכונה מספר t של פעמים ונחזיר את התשובה שהתקבלה ברוב הפעמים.

רוצים לחשב מה הסיכוי שנקבל תשובה נכונה/שגויה, הסיכוי הוא שנטעה ב-1/3 מההרצות של המכונה. אך מה הסיכוי שהמכונה תטעה ביותר מחצי מהפעמים (ולכן נחזיר תשובה שגויה)? (נשתמש בא"י צ'רנוף Chernoff כדי לחשב זאת.

בהינתן שפה $L \in BPP$, ניתן לייצר מכונה M' שהיא מ"ט הסתברותית כך ש-M' תחזיר תשובה שגויה בהסתברות $\frac{1}{3P(n)}$ (כש $P(n)$ הוא מספר הביטים הרנדומיים שהמכונה משתמשת בהם בתלות ב-n. P הוא פולינום)

אנחנו <u>לא</u> יודעים האם $BPP \subseteq NP$. עם זאת, אנו יכולים להוכיח כי $BPP \subseteq \Sigma_2$. נשים לב שזה אומר שאם נוכיח ש $P \neq BPP$ נקבל כי $P \neq NP$.

<u>הוכחה:</u>

L שייכת ל-BPP, לכן קיימת מכונה הסתברותית M. נשתמש במכונה זו כדי לייצר נוסחה: $x \in L \Leftrightarrow \exists s_1, \ldots, s_m \in \{0,1\}^m . \forall r \in \{0,1\}^m . \bigvee_{i=1}^{m} M(x, r \oplus s_i)$

במקרה 1, $x \in L$, אנחנו רוצים שתמיד יוחזר T. באופן התחלתי r מחזיר T עבור 2/3 מההגרלות (של r). אני משתמש ב-s_i כדי "להזיז" את כיסוי המקרים בהם יוחזר T. נעשה זאת מספיק פעמים (ע"י m מחרוזות s_i) וע"י כך נדאג שעבור $x \in L$, לכל r יהיה אחד ה-s_i שעבורו $r \oplus s_i$ יגרום ל-M לקבל. צריך גם לדאוג שהרזולוציה מתאימה לא נקבל קלטים רק ש $x \notin L$.

בהינתן $x \notin L$, "כיסוי" המחרוזות r שעבורם יוחזר T (בשגיאה) הוא $\frac{1}{3m}$ מהמחרוזות האפשריות (כי הסיכוי הוא $\frac{1}{3m}$). שכפול הכיסוי באמצעות s_i מתבצע m פעמים. לכן, באמצעות Union Bound נקבל כי נחזיר תשובה שגויה במקרה זה, לכל היותר עבור $m \cdot \frac{1}{3m} = \frac{1}{3}$ מתוך r. לכן עבור כל בחירת S, תמיד יהיה r רע ולכן יוחזר F עבור כל בחירה.

קשה למצוא $s_1 \ldots s_m$ שיקיימו את התכונה שאנו רוצים, אבל, אנו יכולים להראות שהסיכוי שהם יקיימו את התכונה אם נגריל אותם הוא גדול מ-0. ולכן בפרט קיימים כאלו.

בהינתן $x \in L$, נבחר רנדומית $s_1, \ldots, s_m$. נראה שהסיכוי שקיים r שעבורו יחזור F הוא קטן מ-0 (היה מספיק אם היינו מראים שהוא בפרט קטן מ-1 כי אז המשלים גדול מ-0 ולכן קיימת בחירה $s_1, \ldots, s_m$ שמקיימת את התכונה). נחסום את הסיכוי מלמעלה ע"י סכימת הסיכוי של החזרת F עבור כל r אפשרי. r הוא שלב לתחום קבוע וכעת s הוא סטרינג רנדומי. לכן, מספר האפשרויות חסום ע"י $2^m \cdot \prod_1^m p(M(x,s)=0)$ וזה חסום ע"י $2^m \cdot (\frac{1}{3m})^m$ וזה מספר הקטן ממש מ-1. (שקף 12)

8.6.09 (3)

סבוכיות - שיעור 13

כאשר $x \notin L$ נשתמש ב-Union Bound ונראה שקיים לפחות r אחד שאינו מקיים את התנאי ולכן ונחזיר F (שקף 13).

נזכר שהבעיה st-Conn היא NL-שלמה. אם הגרף אינו מכוון, אזי הבעיה פרטית ולכן היא NL אך לא בהכרח שהיא NL שלמה. עד כה, כדי לבחור את המסלול היינו "מנחשים" את הקודקוד הבא (באמצעות המכונה הלא דטרמיניסטית). כעת, במקום לנחש, נגריל את אחד מהקודקודים.

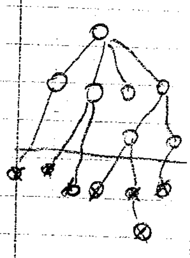
לשיטת ההגרלות קוראים random-walk. בשיטה זו, קודם מוסיפים קשת מכל קודקוד לעצמו. לאחר מכן, מתחילים מ-s. לכל קודקוד עם דרגה d_i, יש סיכוי $\frac{1}{d_i}$ לבחור כל קשת. "נטייל" בגרף, אם הגענו ל-t נקבל.

ההסתברות שנהיה בכל קודקוד בגרף קשיר היא $\lim_{t\to\infty} P_t(i) = \frac{d_i}{2|E|}$.
כלומר, ההסתברות תלויה בדרגת הקודקוד.

אנו נוכיח טענה מעט חלשה יותר ולפיה אם הגענו ל-t רק עם $P_t(i) = \frac{d_i}{2|E|}$ עבור כל i, אז לכל צעד מתקיים $P_{t+1}(i) = \frac{d_i}{2|E|}$.

קשת עצמית נחשבת פעמים בדרגה

<u>הוכחה</u>: באינדוקציה במצגת.



אנו נשתמש בטענה זו כדי לחסום את מספר הצעדים שיש ללכת כדי להגיע שמ-s נגיע אל t. אנו נסיק כי אם התחלנו מ-i אנו נבקר בו שוב לאחר $\frac{2|E|}{d_i}$ (כלומר 1 חלקי ההסתברות להיות בו).

בכל שלב יש לנו סיכוי ללכת בכיוון הנכון $\frac{1}{d_i}$. לכן לאחר d_i נסיונות אנו מצפים ללכת לקודקוד הבא הנכון. אם במקרים שלא בחרנו נכון נקח לנו $\frac{2|E|}{d_i}$ צעדים כדי לחזור לקודקוד i. לכן לאחר $2|E|$ צעדים אנו צפויים לעבור לקודקוד i+1 במסלול מ-s אל t. לכן, כדי למצוא את כל המסלול, עלינו לבצע $d(s,t)\cdot 2|E|$ ואת זה ניתן לחסום ע"י $|V|\cdot 2|E|$ צעדים.