20: Solving Satisfiability with the Lovász local lemma

בעיית **הספיקות** – מתי פסוק ניתן לסיפוק?

נזכיר: פסוק $k\text{-}CNF$ היא במבנה: $\underbrace{(x_1 \vee x_2 \vee x_5 \vee \dots)}_{k} \wedge \underbrace{(\overline{x_1} \vee x_2 \vee \overline{x_7} \vee \dots)}_{k} \wedge \dots$

למה: תהי φ נוסחת $k\text{-}CNF$ שבה **אין** משתנה שמופיע ביותר מ- $2^k/4k$ פסוקיות. אזי, φ ניתנת לסיפוק.

הוכחה: נסמן ב-m את מספר הפסוקיות ב-φ.

לכל משתנה ב-φ, נקבע ערך ב- $\{0,1\}$ באופן מקרי ואחיד ובת"ל.

לכל $i \in [m]$, נגדיר $\mathcal{E}_i$ את המאורע "פסוקית i לא מסופקת".

אנחנו בעצם רוצים להראות ש $\mathbb{P}\left[\bigcap_{i\in[m]} \bar{\mathcal{E}_i}\right] > 0$. וזה מתאים בדיוק ללמת המקומיות של לובאס.

נצטרך לבנות גרף תלויות שמתאים למאורעות, ולהראות ש-3 התנאים מתקיימים:

1. סימטריות: מתקיים $\mathbb{P}[\mathcal{E}_i] \le p$ לכל $i \in [n]$.
2. תלות מוגבלת: $\Delta\big(D(\mathcal{E}_1, \dots, \mathcal{E}_n)\big) \le d$ (הדרגה המקסימלית).
3. חסם על p, d: $4pd \le 1$.

בניית הגרף D

$$V = V(D) \coloneqq \{\mathcal{E}_i : i \in [m]\}, \qquad E = E(D) \coloneqq \left\{\left(\mathcal{E}_i, \mathcal{E}_j\right) : clauses\ i, j\ share\ common\ variables\right\}$$

הקודקודים הם המאורעות של "פסוקית לא מסופקת". בין שני קודקודים, תהיה צלע אם יש משתנה משותף בין הפסוקיות המתאימות.

מאורע $\mathcal{E}_i$ הוא בת"ל הדדית מכל המאורעות $\mathcal{E}_j$ אם לפסוקיות שלהם אין משתנים משותפים, כי אז ההשמה של כל פסוקית j לא תשפיע על ההשמה של i.

אז הגרף הוא אכן גרף תלויות, כי כל מאורע יהיה בת"ל במכל המאורעות שלא סמוכים אליו בגרף.

<u>נקבע את d</u>: לפי ההנחה, אין משתנה שמופיע **ביותר מ-** $2^k/4k$ פסוקיות.

אז המקרה הגרוע ביותר שיכול להיות זה אם יש פסוקית שבה יש k משתנים שונים, וכל אחד מהם מופיע ב- $2^k/4k$ פסוקיות:

$$\Delta(D) \le k \cdot \frac{2^k}{4k} = \frac{2^k}{4} = 2^{k-2} = d$$

<u>נקבע את p</u>: ההסתברות שפסוקית לא תהיה מסופקת, היא ההסתברות שכל אחד מהמשתנים שלה לא מסופקים:

$$\mathbb{P}[\mathcal{E}_i] \le 2^{-k}, \qquad \forall i \in [m]$$

<u>נבדוק האם החסם על p, d מתקיים</u>:

$$4pd \le 4 \cdot 2^{k-2} \cdot 2^{-k} = 2^2 \cdot 2^{-2} = 1$$

אזי לפי למת המקומיות של לובאס, מתקיים $\mathbb{P}\left[\bigcap_{i=1}^{n} \bar{\mathcal{E}_i}\right] > 0$. כלומר יש הסתברות חיובית ממש שכל הפסוקיות מסופקות. כנדרש.

אלגוריתם מקרי לספיקות – *A randomized Algorithm for Satisfiability*

הלמה של לובאס מבטיחה קיום של השמה מספקת. נרצה להשתמש בלמה כדי למצוא השמה כזו.

הראינו שאם כל משתנה מופיע בלכל היותר $2^k/4k$ פסוקיות, אז φ ספיקה. נרשום עבור $\alpha < 1$ כלשהו:

$$\frac{2^k}{4k} = \frac{2^k}{2 \cdot 2 \cdot k} = \frac{2^{k-2}}{k} = 2^{\alpha k}$$

נרצה למצוא השמה ספציפית. בשביל זה נצטרך עוד הנחות לגבי α. יהיו שני שלבים:

20: Solving Satisfiability with the Lovász local lemma

<u>בשלב הראשון</u>, נייצר השמה חלקית אקראית, ונוכיח (עם הלמה של לובאס) שבהסתברות חיובית ההשמה החלקית ניתנת להרחבה להשמה מספקת.

<u>בשלב השני</u>, נראה שבהסתברות ששואפת ל-1, יש **גרף תלויות** שההשמה החלקית מפרקת אותו לרכיבי קשירות "קטנים".

ואז, נחשוב על כל רכיב קשירות בתור תת-נוסחה של φ.

ואם בכל מרכיב יש מעט מאד משתנים, נוכל למצוא השמה מספקת בזמן שהוא אקספוננציאלי בגודל המרכיב, אבל בגלל שהרכיבים קטנים הוא כמעט קבוע.

<u>התוצאה המרכזית שנגיע אליה:</u>

לכל k זוגי מספיק גדול וקבוע, קיים $\alpha := \alpha(k) > 0$ כך שמתקיים:

> תהי φ נוסחת $k\text{-}CNF$ עם m פסוקיות, כך שכל משתנה מופיע בלכל היותר $2^{\alpha k}$ פסוקיות.
>
> אזי בהסתברות 1, אפשר למצוא השמה מספקת ל-φ, כך שתוחלת זמן הריצה הוא פולינומי ב-m.

<u>הגדרות:</u>

- φ היא נוסחת $k\text{-}CNF$ עבור $k \geq 4$ זוגי.
- המשתנים הם $x_1, \dots, x_\ell$.
- הפסוקיות הן $C_1, \dots, C_m$.
- כל משתנה מופיע בלכל היותר $2^{\alpha k}$ פסוקיות.
- $0 < \alpha < 1$, נקבע אותו בהמשך.

<u>הנחות:</u>

- אין פסוקית שמכילה זוגות של ליטרלים משלימים כמו $x, \bar{x}$. (אם יש, אז אותה פסוקית בוודאות מסופקת, ונוכל פשוט להוריד את הפסוקית הזו).
- אין פסוקית עם ליטרלים שחוזרים על עצמם. (כי אם יש, אפשר פשוט לאחד אותם).

כלומר באופן כללי, בכל פסוקית מספר הליטרלים שווה למספר המשתנים.

ההנחות האלה נותנות לנו שבכל פסוקית יהיו בדיוק k משתנים לאורך ההוכחה. אפשר להכליל את ההוכחה כך שבכל פסוקית i יש k_i ליטרלים.

השמה חלקית אקראית (שלב א)

נגדיר: פסוקית C תיקרא **מסוכנת** אם יש לה <u>בדיוק</u> $k/2$ ליטרלים שקיבלו ערכים והיא עדיין לא מסופקת.

1. נעבור על המשתנים $x_1, \dots, x_n$. לכל x_i:
   a. אם קיימת פסוקית מסוכנת שמכילה את x_i, אז לא ניתן ל-x_i השמה ונעבור למשתנה הבא.
   b. אחרת, אז ניתן ל-x_i ערך 0 או 1 באופן מקרי ואחיד ובת"ל מכל השאר.

בכל איטרציה אנחנו קובעים השמה למשתנה אחד בלבד.

משתנה שלא קיבל ערך במהלך שלב א ייקרא משתנה **דחוי**.

נאמר שפסוקית **שרדה** את שלב א אם היא לא מסופקת ע"י ההשמה החלקית שהוגדרה במהלך שלב א.

פסוקית שורדת לא בהכרח חייבת להיות מסוכנת: אם יש לה מספיק משתנים משותפים עם פסוקית מסוכנת, אז יכול להיות שיש לה פחות מ- $k/2$ משתנים שקיבלו ערכים.

לפסוקית שורדת תמיד יהיו לכל היותר $k/2$ משתנים שקיבלו ערך (נקבעו). למה?

ראשית, נשים לב שפסוקית מסופקת לא תחזור להיות לא-מסופקת. כי יש "או" בין המשתנים של הפסוקית.

אם פסוקית מוגדרת שורדת, היא בהכרח לא מסופקת.

ואם יש לה יותר מ- $k/2$ משתנים שנקבעו, זה אומר שבשלב מסויים היו לה בדיוק $k/2$ משתנים שנקבעו, והיא הייתה לא מסופקת.

אז באותו רגע היא הייתה מסוכנת. וברגע שפסוקית נהיית מסוכנת, בהגדרה אף משתנה אצלה לא יקבל ערך.

אז לא יכול להיות שיש לה יותר מ- $k/2$ משתנים שקיבלו ערך.

וגם נשים לב, שאם יש פסוקית שכל המשתנים שלה אף פעם לא היו משותפים עם פסוקית מסוכנת, אז כל המשתנים שלה יקבלו ערכים.

כלומר, כל פסוקית שורדת היא או מסוכנת בעצמה, או שיש לה משתנה דחוי שמשותף עם פסוקית מסוכנת.

כלומר היה שלב שבו היו לה בדיוק $k/2$ ליטרלים שקיבלו ערכים והיא עדיין לא מסופקת. אז היא הייתה מוגדרת מסוכנת.

בסה"כ, לכל פסוקית שורדת יש לפחות $k/2$ משתנים דחויים.

20: Solving Satisfiability with the Lovász local lemma

השלמה להשמה מספקת (המשך שלב א)

טענה: לכל k זוגי מספיק גדול וקבוע, קיים $\alpha > 0$ כך שקיימת השמה למשתנים הדחויים שמספקת את כל הפסוקיות השורדות.

הוכחה: נשתמש בלמת המקומיות כמו שעשינו בהתחלה, עם כמה שינויים:

<u>מקור האקראיות</u>: לא נשתמש בהשמה האקראית מחלק א. אלא, נקבע לכל משתנה דחוי ערך 0 או 1 באופן מקרי ואחיד ובת"ל מכל השאר.

עבור פסוקית שורדת C, נגדיר: $\mathcal{E}_C$ את המאורע "C לא סופקה על ידי ההשמה האקראית השנייה".

<u>גרף תלויות</u>: הקודקודים יהיו כל ה-$\mathcal{E}_C$. שני קודקודים $\mathcal{E}_C$ ו- $\mathcal{E}_{C'}$ יהיו סמוכים אם יש ל- C, C' משתנה דחוי משותף.

ההוכחה ש-D הוא אכן גרף תלויות זהה למה שעשינו בפעם הראשונה.

ההסתברות ש-C לא מסופקת: $\mathbb{P}[\mathcal{E}_C] \le 2^{-k/2}$. כי צריך שכל אחד מהמשתנים הדחויים לא יסופק.

הדרגה המקסימלית: $\Delta(D) \le k \cdot 2^{\alpha k}$. כי יש עד k משתנים דחויים בפסוקית שורדת, וכל אחד מהם נמצא בלכל היותר $2^{\alpha k}$ פסוקיות שורדות אחרות.

החסם על d, p (ההסתברות ל- $\mathcal{E}_C$ והחסם על הדרגה המקסימלית):

$$4dp = 4 \cdot \Delta(D) \cdot 2^{-k/2} \le 4 \cdot k \cdot 2^{\alpha k} \cdot 2^{-k/2} = k \cdot 2^{\alpha k + 2 - k/2} = 2^{\alpha k + 2 + \log_2 k - k/2} \le 1$$

כאשר המעבר האחרון מתקיים עבור k מספיק גדול ו-α מספיק קטן (כי אז ה- $(-k/2)$ יותר משמעותי משאר החלקים, והחזקה שלילית).

עכשיו, למת המקומיות אומרת שיש הסתברות חיובית ממש שכל פסוקית שורדת תסופק.

מרכיבי הקשירות של גרף התלויות (שלב ב)

כל רכיב קשירות של D מגדיר תת-נוסחה של φ (אוסף של חלק מהפסוקיות). ובין רכיבי קשירות, אין משתנים דחויים משותפים.

מכיוון שיש m פסוקיות, יש לכל היותר m רכיבים כאלה.

אם נצליח להראות שכל אחד מהרכיבים האלה בגודל $O(\log m)$, אז יש לכל היותר $O(k \log m)$ משתנים בפסוקיות של הרכיבים האלה.

ואז, בגלל שאנחנו יודעים ש-φ ספיקה, אז חיפוש *brute-force* על כל $2^{O(k \log m)} = m^{O(k)}$ ההשמות האפשריות ייתן השמה מספקת.

אז אם k קבוע, האלגוריתם הוא פולינומי.

המטרה שלנו היא להוכיח שכל זה קורה בהסתברות ששואפת ל-1. (נאמר שזה קורה <u>כמעט בוודאות</u>. *a.a.s. – asymptotically almost surly*)

למה: לכל k כמו שאמרנו קיים $\alpha \coloneqq \alpha(k) > 0$ ו- $C \coloneqq C(k, \alpha) > 0$ כך שכמעט בוודאות כל הרכיבים של D בגודל לכל היותר $C \cdot \ln m$.

הוכחה: כדי להוכיח, נשתמש בגרף D' שהוא דומה לגרף תלויות, רק שהקודקודים שלו הם לא מאורעות, אז אין מקריות.

$V(D')$ הם הפסוקיות של φ. 2 קודקודים יהיו סמוכים אם בין הפסוקיות יש משתנים משותפים.

כל הקודקודים של D (פסוקיות שלא מסופקות אחרי ההשמה השנייה) מיוצגים גם ב-D'.

ואם יש צלע בין שני קודקודים ב-D (כי יש להם משתנה דחוי משותף), אז יש גם צלע ב-D' כי יש משתנה משותף. כלומר $D \subseteq D'$, אז $\Delta(D) \le \Delta(D')$.

וגם, $\Delta(D') \le k \cdot 2^{\alpha k}$ (כי יש k משתנים בכל פסוקית, וכל אחד נמצא בלכל היותר $2^{\alpha k}$ פסוקיות אחרות). נסמן $\Delta \coloneqq \Delta(\mathrm{D}') \le k \cdot 2^{\alpha k}$.

4-Trees

כדי לנתח את הרכיבים של D', נשתמש בגרף עזר מסוג "עץ-4".

נגדיר:

R תת-גרף קשיר של D' (יכול להיות רכיב קשירות).

אז, עץ-4 של R הוא עץ מושרש (כלומר שיש לו קודקוד מסוים שמוגדר בתור שורש) S, שמקיים:

1. $V(S) \subseteq V(R)$
2. כל שני צמתים ב-S הם במרחק לפחות 4 צלעות ב- D'.
3. שני קודקודים הם סמוכים ב-S אם ב-D' המרחק שלהם הוא בדיוק 4.
4. כל קודקוד של R הוא או ב-S או במרחק לכל היותר 3 מ-$V(S)$ ב-R. כלומר ב-R, אפשר להגיע מכל קודקוד לקודקוד ששייך גם ל-S ב-3 צעדים.

נשים לב – S לא חייב להיות בעצמו תת-גרף של R.

20: Solving Satisfiability with the Lovász local lemma

ננסח 2 טענות, נשתמש בהן, ואז נוכיח בסוף.

טענה א: יהי S עץ-4 של תת-גרף קשיר של D'. אזי, $V(S) \subseteq V(D)$ (כלומר כל הפסוקיות של S שרדו ב-D) בהסתברות לכל היותר:

$$\mathbb{P} \leq \left((\Delta+1)\cdot 2^{-k/2}\right)^{v(S)} = \left(\left(k\cdot 2^{\alpha k}+1\right)\cdot 2^{-k/2}\right)^{v(S)} \approx$$

אם כל הפסוקיות של S שרדו, נאמר ש-S שרד.

נשים לב ש $\Delta = k\cdot 2^{\alpha k}$. וה-1 לא משמעותי במיוחד (אם כל שאר הדברים גדולים מספיק). אז זה בערך:

$$\approx \left(2^{\alpha k+\log_2 k - k/2}\right)^{v(S)}$$

ודומה למה שהראינו מקודם, אם k מספיק גדול אז החזקה תהיה שלילית. אז יש לנו מספר קטן מ-1 בבסיס החזקה, שזה טוב בשביל חסם על ההסתברות. כאשר $v(S)$ יגדל, נוכל לומר שכמעט בוודאות עץ בגודל כזה לא שורד.

טענה ב: יהי R תת-גרף קשיר של D', ויהי S עץ-4 של R בגודל מקסימום. אזי, $v(S) \geq v(R)/\Delta^3$.

כלומר אם ב-R יש הרבה קודקודים, אז ב-S יש הרבה קודקודים.

ולפי טענה א, אם ב-S יש הרבה קודקודים, אז ההסתברות שהפסוקיות שלו שרדו מאוד נמוכה.

כזכור, אנחנו רוצים להוכיח:

לכל k כמו שאמרנו קיים $\alpha := \alpha(k) > 0$ ו- $C := C(k,\alpha) > 0$ כך שכמעט בוודאות כל הרכיבים של D בגודל לכל היותר $C\cdot \ln m$.

נשתמש בטענה א כדי להוכיח שכמעט בוודאות, D' לא מכיל עץ-4 בעל לפחות $C\ln m/\Delta^3$ קודקודים ששרד ב-D.

השרידות הזו היא מה שמביא את האקראיות.

מטענה ב נקבל שאם תת-גרף קשיר R של D' בגודל לפחות $C\ln m$ כלשהו שרד ב-D, אז יש לו עץ-4 בגודל לפחות $C\ln m/\Delta^3$ ששורד ב-D.

אבל לפי טענה א, עצים בגודל כזה כמעט בוודאות לא שורדים ב-D.

אז כמעט בוודאות, אין תת-גרף קשיר של D' כזה ששרד ב-D. אז כל מרכיבי הקשירות של D הם בגודל לכל היותר $C\cdot \ln m$ (כמעט בוודאות).

הוכחת טענה א

תהי C פסוקית של φ. נשאל מה ההסתברות שהיא שורדת ב-D.

כזכור, פסוקית שורדת היא או מסוכנת בעצמה או חולקת לפחות משתנה דחוי אחד עם פסוקית מסוכנת.

אם היא חולקת לפחות משתנה דחוי אחד עם פסוקית מסוכנת, אז בגרף D', היא סמוכה לפסוקית מסוכנת. אז ההסתברות ש-C שורדת:

$$\mathbb{P}[C\ survives] \leq \underbrace{\mathbb{P}[C\ is\ dangerous]}_{\leq 2^{-k/2}} + \underbrace{\mathbb{P}[\geq 1\ of\ its\ neighbors\ in\ D'\ is\ dangerous]}_{\leq \Delta\cdot 2^{-k/2}} \leq (\Delta+1)\cdot 2^{-k/2}$$

פסוקיות במרחק 2 (או יותר) ב-D' לא חולקות משתנים. אז המאורעות שפסוקיות כאלה הן מסוכנות, הם בלתי תלויים הדדית.

יהי $u \in V(S)$. כל קודקוד ב-R שיכולים לגרום ל-u לשרוד נמצאים במרחק 1 מ-u (ב-R).

ולכן הם במרחק לפחות 2 מכל הקודקודים האחרים של $V(S)$ (כי כל שני צמתים ב-S הם במרחק לפחות 4 ב-R).

כלומר, מאורעות השרידות של $V(S)$ כולם בת"ל הדדית. אז ההסתברות שכולם שרדו:

$$\mathbb{P}[V(S) \subseteq V(D)] \leq \left((\Delta+1)\cdot 2^{-k/2}\right)^{v(S)}$$

כנדרש לטענה א.

הוכחת טענה ב

ניזכר בטענה: כל עץ-4 של תת-גרף קשיר R הוא בגודל לפחות $v(R)/\Delta^3$.

נב"ש שגודל העץ-4 המקסימום ב-R (נקרא לו S) קטן ממש מ- $v(R)/\Delta^3$.

בהגדרה, כל קודקוד ב- $V(R)$ הוא במרחק לכל היותר 3 מ- $V(S)$.

יהי $v \in V(D')$ כלשהו. נסמן את n_3 את מספר הקודקודים ב-D' במרחק לכל היותר 3 מ-v:

$$n_3 \leq \Delta + \Delta(\Delta-1) + \Delta(\Delta-1)(\Delta-2) = \Delta + \Delta^2 - \Delta + \Delta^3 - \Delta^2 - 2\Delta^2 + 2\Delta \leq \Delta^3 - 1$$

- ה-Δ זה בגלל החסם על מספר השכנים.
- ה-$\Delta(\Delta-1)$ זה חסם על מספר הקודקודים במרחק 2 (Δ שכנים של v, ולכל אחד לכל היותר $\Delta - 1$ שכנים כי הם לא שכנים של v).
- ובאופן דומה עבור קודקודים במרחק 3.

אז בגלל שכל הקודקודים ב-R הם במרחק לכל היותר 3 מקודקודי S, נקבל:

$$v(R) \leq v(S) \cdot n_3 <$$

ולפי ההנחה בשלילה, כל עץ-4 קטן ממש מ-$v(R)/\Delta^3$, אז:

$$< \frac{v(R)}{\Delta^3} \cdot (\Delta^3 - 1) < v(R)$$

סתירה.

גודל המרכיבים של D

ניזכר: רצינו להשתמש בטענה א כדי לומר שכמעט בוודאות אין ב-D' עץ-4 בגודל $C \log m/\Delta^3$ ששרד ב-D.

נגדיר $r \coloneqq C \ln m$.

נגדיר $\mathcal{E}$ את המאורע שעץ-4 בגודל לפחות $C \ln m/\Delta^3$ שרד ב-D. מה ההסתברות לזה? לפי חסם איחוד:

$$\mathbb{P}[\mathcal{E}] \leq (\#of\ 4\text{-}trees\ in\ D'\ of\ size\ r/\Delta^3\ ) \cdot (max\ prob.\ that\ a\ 4\text{-}tree\ survives)$$

מספר העצים ב-D' בגודל r/Δ^3 הוא לכל היותר:

$$m \cdot \Delta^{4r/\Delta^2}$$

<u>נוכיח</u>: נספור את מספר הדרכים לבנות עץ-4 בגודל r/Δ^3. בעצם בהינתן מבנה של עץ, נבחר איזה קודקוד לשים בכל צומת.

בהינתן תבנית, נספור את מספר הדרכים לבנות את העץ בצורה <u>סדורה</u> – כאשר יש משמעות לסדר בין הילדים.

במקום לספור עצים, נספור את מספר מעגלי האויילר על הקודקודים של העץ.

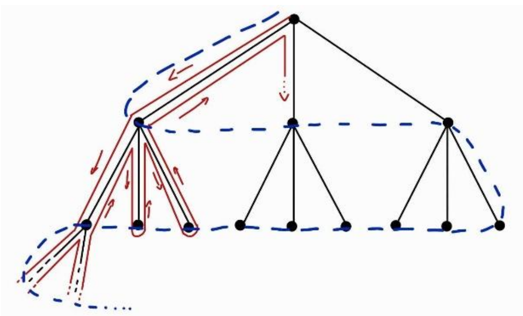
נספור מעגלים שמתחילים בשורש של העץ והולכים לפי הסדר שקבענו (נגיד *preorder*).

זה יהיה חסם עליון על מספר הדרכים.

יש m דרכים לבחור את השורש (כל הקודקודים ב-D', הפסוקיות מ-φ).

כל צלע בעץ מסמלת מסלול באורך 4. אז כדי לבחור את הקודקוד הבא, יש לכל היותר Δ^4 אפשרויות.

נשים לב שאנחנו סופרים כל פעם שחוזרים לצומת, למרות שבבנייה הצומת כבר קבועה:



תהליך הבנייה זה הקו הרצוף, לפי החיצים. המסלול אויילר זה הקו המקווקו, שזה פחות מהמסלול של הבנייה.

אז מספר מסלולי אוילר האפשריים הוא לכל היותר:

$$m \cdot (\Delta^4)^{\Delta \cdot r/\Delta^3} = m \cdot \Delta^{4r/\Delta^2}$$

כי מכל אחד מה- r/Δ^3 מקומות, יוצאים לכל היותר Δ צלעות. ולכל צלע יש לכל היותר Δ^4 אפשרויות.

אזי, ההסברות של $\mathcal{E}$:

$$\mathbb{P}[\mathcal{E}] \le (\#of\ 4\text{-}trees\ in\ D'\ of\ size\ r/\Delta^3\ ) \cdot (max\ prob.\ that\ a\ 4\text{-}tree\ survives) \le m \cdot \Delta^{4r/\Delta^2} \cdot \left((\Delta+1)\cdot 2^{-k/2}\right)^{r/\Delta^3}$$

$$= \exp\left(\ln m + \ln\left(\Delta^{4r/\Delta^2}\right) + \ln\left(\left((\Delta+1)\cdot 2^{-k/2}\right)^{r/\Delta^3}\right)\right)$$

$$= \exp\left(\ln m + \frac{4r}{\Delta^2}\ln\Delta + \ln\left((\Delta+1)^{r/\Delta^3}\cdot\left(2^{-k/2}\right)^{r/\Delta^3}\right)\right)$$

$$= \exp\left(\ln m + \frac{4r}{\Delta^2}\ln\Delta + \ln\left((\Delta+1)^{r/\Delta^3}\cdot 2^{-kr/2\Delta^3}\right)\right) = \exp\left(\ln m + \frac{4r}{\Delta^2}\ln\Delta + \frac{r}{\Delta^3}\ln(\Delta+1) - \frac{kr}{2\Delta^3}\ln 2\right) =$$

ניזכר שהצבנו: $\Delta \le k\cdot 2^{\alpha k}$.

וניזכר ש $r \coloneqq C\ln m$

$$\le \exp\left(\ln m + \frac{4r}{\Delta^2}\ln\left(k\cdot 2^{\alpha k}\right) + \frac{r}{\Delta^3}\ln\left(k\cdot 2^{\alpha k}+1\right) - \frac{kr}{2\Delta^3}\ln 2\right) \le \exp\left(\ln m + \frac{4r\ln(2k)\,\alpha k}{\Delta^2} + \frac{r\ln(2k+1)\,\alpha k}{\Delta^3} - \frac{kr}{2\Delta^3}\right) \le$$

$$\le \exp\left(\ln m + \frac{4r\ln(2k)\,\alpha k}{\Delta^2} + \frac{r\ln(4k)\,\alpha k}{\Delta^3} - \frac{k\cdot C\ln m}{2\Delta^3}\right)$$

אם α תהיה מספיק קטנה, וניקח C מספיק גדול, אז הביטוי השלילי בסוף יהיה חזק יותר מכל השאר, ונקבל שכל זה שואף לאפס, או $o(1)$.

כנדרש.

לסיכום

טענה:

לכל k זוגי מספיק גדול וקבוע, קיים $\alpha \coloneqq \alpha(k)$ כך שמתקיים:

תהי φ נוסחת *k-CNF* עם m פסוקיות, כך שכל משתנה מופיע בלכל היותר $2^{\alpha k}$ פסוקיות.

אזי בהסתברות 1, אפשר למצוא השמה מספקת ל-φ בזמן שבתוחלת הוא פולינומי ב-m.

ההוכחה:

השלב הראשון נותן פירוק של φ לפסוקיות קטנות בגודל $O(\ln m)$. (בהסתברות ששואפת ל-1). זה נובע מטענות א ו-ב.

כלומר בהסתברות לפחות $1 - o(1)$ אנחנו מצליחים לפרק את גרף התלויות לחלקים מספיק קטנים.

ההתפלגות של הניסיונות לפירוק זו התפלגות $Geom\left(1-o(1)\right)$.

אז בתוחלת, תוך $O(1)$ ניסיונות של שלב א נקבל פירוק תקין.

והראינו שכל פירוק שנקבל, אפשר להרחיב להשמה מספקת.

אז נוכל ע"י *brute force* לבדוק את כל ה- $2^{O(k\log m)} = m^{O(k)}$ השמות האפשריות, שעבור k קבוע זה זמן פולינומי ב-m.

מש"ל. ■