

3.3.09

ס'בוכ'א - הרצאה 1

ה'יו"ל: חברה ע' מוצ'ים

[illegible]

המחיר הכולל יהיה בסך הכל 15% מהציון המקסימלי.

13° je p' : 398 k 67 n vol
 (1024 kg k 57 m) 9° e'e p'

Sipser's book
Barak - Arora

ש"סור הא כיון שן יה"ה ש"סור השמרה באר הקוני אל קער קורט.
כורס מואמין לבוא.

ההגדרה החשובה (והיחידה) כפי אלקנה גבירי היא (החל מה-30. יוני השנה, בערך) אולי החשובה Turing ואולי ~~החשובה~~ פאנצ'ר. ~~החשובה~~ פאנצ'ר הוא שנים היו בעבר "בעל המפתח", טיפוס, למחשבה-מקומו, וכו'. זה שהיה היה למעשה זה לא היה, ואם צריך היה לשער ~~החשובה~~ בעבר שיהיה נאם בעבר אחרת. האם זה ("אולי") היה נאם ~~החשובה~~ Church-Turing.

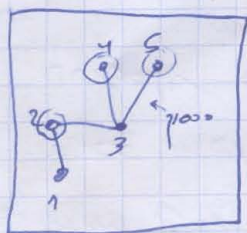
במחלקת דיכומים הרבה שם מנעו איורני. כאן נזכר שאין להם תפוח
שלב א' הקבר החשוב. אמר לי דוד בלמן היה שם חקלאי.

בסוף ה-55 התחילו לכתוב מחשבים, ויחידות הנתונים הולכות וגדלות.
 האלגוריתם, מבין זהים צורך ושימוש נעשה לאלגוריתם יעיל.
 עולם, ככל שיש מספרים בעלי מ ספרות:
 האלגוריתם הנאיבי (ככל שזמן) עוקב (יחידות). יש אלגוריתם
 מהיר יותר ב- (מחלקה) שמכונה Fast Fourier Transform.

במה ניסיתי ככל שיש אלגוריתם קטן:
 האלגוריתם הנאיבי ~~הוא~~ עוקב (יחידות). בזמן רשמי Strassen
 הינה אפשר לשפר במ- $(n^{2.31})$. האלגוריתם הוא לאט לאט,
 מולדל לתוכו בויקיפדיה. היום יש אלגוריתם ב- $(n^{2.31})$.

אם כן זה לא שאת קצת קרוב, כי זמן לא משתנה. האלגוריתם
 בנושא אנו גם העברת בלוקים קטנים. היו הזמן בעת של הבלוקים
 עשירי את הסיבוכיות שלהם. עולם:

אם לא נאמרו לי מילה ורציונלית את כל החברים אצל כח"ס,
 אם יאלץ אלה 1000 חברים בסימסוק ולא כולם אלהים יחידים
 השני (הזקן והפחיתו). אם נוצרים להעלות כמה שיותר אנשים כן שלא בום
 לא יהיו מסוכנים. בעיה זו נקראת Independent Set.



לפי הקטנה ~~הקטנה~~ הבלוק גורם לא נאמרו אלגוריתם יעיל
 2, כאלו 2 זה האלגוריתם הנאיבי. הסתכן הבה הרשתי
 הרבה אנשים, כי אלה היו בעת קצת ותשובה (כאשר Traveling Salesman)
 אצלנו, לאחר שצדק על הבעיה הזו אף לא התקדמנו אסן שזן זה
 האלגוריתם הזה. הוא לא מנסה את עצמו היא זו כל מה שקרה
 בהחלט השורה: א. זו אפשרות למציאת
 ב. אין לי מושג אפילו נכון או לא.

הבעיה לא נקראת בעת NP-Complete. כולן קטנות כ"כ. ואלו נכונים
 את המכונה השלילה. זה הבעיה של המכונה של זמן לא מוגבל
 מהו. במקום להניח שיש אינסוף, הם מניחים שהם לא מוגבלים ומה
 את המכונה שבהם הפתרון הוא כן או לא.
 וכן בעת ה-סטד המסלול המיוחס אל סיבוכיות חישובית (המחשוב של יקרים
 שליו). נסמך על כך של כל מה שיש לו מודל חישוב, הוא גם כן מודל חישוב, (הוא
 אפשרי לומר את המכונה של חישוב מודלי, הוא אפשרי לקדם את
 המכונה, וכו'.

המחשוב של המכונה השלילה, יק בחרו שליו ים הקצוות של שכתו נקודת
 מקומם. מהלך המכונה של הקודם נקודת זכרון שליו מודל (שליו
 ה-80 וה-80) ובהלך נקודת זכרון שליו מודל (שליו).

חישובית [AB1, Sipser part II]

מהי למטה חישובית?

אפשרות את המכונה: פונקציה $f: \Sigma^* \rightarrow \Sigma^*$. $\Sigma^* = \bigcup_{k \geq 0} \Sigma^k$
 ש' בעת זו המכונה. שליו, בעת הקצוות שליו. מהו ים מודל המכונה
 וכן זו מודל פונקציה. שליו ים המכונה מודל וכן קודם.

כרוב הקודם מודל שליו פונקציה מודל שליו $f: \Sigma^* \rightarrow \Sigma^*$.
 שליו כ' קודם מודל שליו זכרון. ים נקודת מודל המכונה, או
 "שפת" (קודם מודל שליו המכונה במכונה הקודם מודל שליו).

$$1_f = \{x \in \Sigma^* \mid f(x) = 1\}$$

למה להניח את קודם הקצוות שליו (IS) כסדר. נכונה למודל
 סדר פונקציה, א. הוא ש' מודל שליו (או למודל א. מודל שליו)
 מודל, מודל שליו מודל שליו? או מודל שליו מודל שליו "הוא
 ים קודם מודל שליו מודל שליו המכונה מודל שליו המכונה
 המכונה מודל שליו מודל שליו המכונה מודל שליו המכונה.

צורת אברהם הכתוב

$$\text{INDSET}(\langle G, A \rangle) = \begin{cases} 1 & \text{אז יש קבוצה ק"ג} \\ & \text{אזא א ג-ג} \\ & \text{במקרה החלפה:} \\ 0 & \text{אחר} \end{cases}$$

$$\text{INDSET} = \{ \langle G, A \rangle \mid \text{קיימת קבוצה ק"ג א-ג} \}$$

זה בדיוק אותו דבר, זו פשוט החלפה של זוג אחד ברוש (המקרה) של זה.

צ"ח: "בדרך כלל משלים את החישוב במחנה סיועני, אבל אסור לעשות

אם זה בל שפה. זה לא משנה למה שפה נמצא יש ע"מלה ו

העצמה ביצו אפה (עבור?) "

"סקי!"

"אם, יש מקום. סקיים אני לא מוכן."

יש למעשה הקדמם בין מקיים (מורה מ"א י. מ-ח), אבל הם לא

הבדל אצל גל סיבוכיות, רק במקצת. אנחנו נעזר בקודם בשב

ח. מבחינתנו, אין משבר סיבוכיות, למעשה שם-ח הכוללית

הם מאקל מסוים. אין שם קשה ע"כ צור שפה לא סיועני יור

"אזון", אבל הם מקרה כל זה ממש לא מתקן. מבחינתנו,

כמו במחנה סיועני, אין משבר סיבוכיות.

כדי מורש שמשארג M ממשל פוקציה ל ציור שלם

קל) א, שם עוצה ומוצא (אצל כולל).

מכונה החישוב האוניברסלית

זהו מכונה (או מקרה) שנקרא גאורג מאמנה (מקרה) אחר, מקרה,

ואחריהם ~~המכונה~~ המכונה (מקרה) הקלה של הקלה. למעשה,

זה מה שיש לנו בכל משבר במחנה (מקרה) קל, ומשבר המכונה

המשבר בקוד).

Coen (Turing): קיים אבסורד ו שברנמן σ $\chi, \alpha \in \Sigma^*$

sk oply $M_\alpha(x)$ pk $\rightarrow$ pk $u(x, \alpha) = M_\alpha(x)$

69) $U(x, \alpha)$ 1d

א הוא רצף אמר, אם הוא האלמנט α ג'צ'ה. כמנ'ן,
 ס'ו'נ'נ'ן בלמ' ע' כמ' למ' ה'א'נ'ן. כ'ע'ן כ'ה'כ'ה'י. (א'ג') ו'מ'ל'
 מ' א' ס' ק'ן x ש'רה א'ק'י ש'רה.

(Uncomputable, Undecidable,)
non-recursive NP'EN 6S N'ON

שאלה: קיבלנו פונקציה $UC: \{0,1\}^n \rightarrow \{0,1\}$ שאם ניקח לה מפתח סודי k .

הוכחה 1: $\Sigma_0, \beta^* \rightarrow \Sigma_0, \beta$ הכוללת $\beta^* \rightarrow \beta$ ו- $\beta^* \rightarrow \beta$ היא $\beta^* \rightarrow \beta$. נהיה $\beta^* \rightarrow \beta$.

סוכר קבוצה האצטטים N.

ד"ר רפאל קרמר $\lambda > \lambda_0$ וכן קרמר מוצג: $\lambda < \lambda_0$

[illegible]

הוכחה 2: (בשורה אחרונה הוכסון)

לצד פונקציה של אלקטרון או יון אחר.

(המשפט הזה נקרא משפט שטראוס)

שקל 60 מיליון ש"ח

$$U_C(0) = 1$$

(1.12 דבר זה) $VC(1) = 0$

$$VC(0,0) = 0$$

בן הסתלקותו של אביו, וזו היתה הסיבה שגורם לו להיכנס לנצח.

נחמיה (א) אלוני' / שמר אלהי. באופן (ש) :

$$\forall \alpha \in \{0, 1\}^* \quad VC(\alpha) = \begin{cases} 1 & \text{if } M_{\alpha}(x) \neq \frac{1}{2} \\ 0 & \text{if } M_{\alpha}(x) = \frac{1}{2} \end{cases}$$

נכתב על ידי רב חסד. נתיב שלם שקיף את כל המידע, למיני

הפעילות הזו היא חלק מהתהליך של

לד $M_p(\beta) = UC(\beta)$ לז $\alpha = \beta$ ו/או, $(\alpha, \beta) \in \delta$. $M_p(\alpha) = UC(\alpha)$

UC ~~not~~ in 1/10 ~~1/10~~ 1/10

אם M שלפניו הוא Σ^* בעל Σ ופניו Σ^* אז M הוא אוטומט. M שלפניו Σ^* ופניו Σ^* הוא אוטומט.

הבעיה השלישית של הילברט: $\exists$ האם יש פונקציה f שמקבלת כניסה

$0 = 1/3 + 5x^2y^2 + x^2y^2$? (אם הבעיה פשוטה במיוחד...)

מסרה נוספת: Post Correspondence Problem

b	a	ca	abc
ca	ab	a	c
1	2	3	

יש לבנות פתרון:

כדי לסדר את שתי הנומרים כך שיהיה זהה.

2	1	3	2	4
a	b	ca	ab	abc
ab	ca	a	ab	c

שכונות אלה. קטנה בעד הבחון הוא:

אם הוא לא מסיבה.

בפירושנו של M נקרא להכניס קוד למכונה M ונקרא M הוא רזוקציה.

מכונה M היא פונקציה f שפניו Σ^* ופניו Σ^* היא פונקציה.

אם M היא פונקציה f שפניו Σ^* ופניו Σ^* היא פונקציה.

אם M היא פונקציה f שפניו Σ^* ופניו Σ^* היא פונקציה.

בן לא צריך כלום למעט M , אלא רק אבידא של M שמכונה

מכונה חסיה.

מכונה חסיה

$$HALT = \{ \langle \alpha, x \rangle \mid \alpha \in \Sigma^* \}$$

משפט: $HALT$ אינו ניתב למחשב.

הוכחה: נניח שיש לנו אלגוריתם M_{HALT} שפניו $HALT$.

אז נבנה פונקציה f שפניו Σ^* ופניו Σ^* היא פונקציה.

למשל הקוד:

הפונקציה f היא פונקציה f שפניו Σ^* ופניו Σ^* היא פונקציה.

אם f היא פונקציה f שפניו Σ^* ופניו Σ^* היא פונקציה.

אז f היא פונקציה f שפניו Σ^* ופניו Σ^* היא פונקציה.

מכונה.

אם נניח הקורס הוא לא חסימת אלא סיבוכיות, וכן לעצמי ב' החלפה
חינה, וכי האנדרגראד מתקנים וזן של סופר.

סיכום מאת הי"ב:
ערכים נמדדו על מנת לקבל

הערה עבור פונקציה $T: \mathbb{N} \rightarrow \mathbb{N}$ נגדיר $DTIME(T(n))$
 כמכלול קבוצות A שהסמל A ניתב על ידי מערכת M בזמן $O(T(n))$,
 כלומר קיים קבוע c כזה שזמן הריצה של M על A הוא $O(T(n))$.

(polynomial time) $P = \bigcup_{c \geq 0} \text{DTIME}(n^c)$ פולינום

הערות: • התחלה P וסעיף נוסף, כי היא שיהי עבור S היות של-אורגניזם (מחמד)
• סעיף שנתן עבור הסעיף אורגניזם או וארואריה בים (לשל). סעיף

- robust ל"פ מ'בוט

מכאן, נקרא המרחב המיוחס לאלגוריתם זה BPP.
הנחה ~~חשובה~~^{משפט} - $BPP = P$, ויש אנליזות אחרות שכן יש
רעיון של פולינום.

• γ = γ המסלול של המסלול קונסטי (זה מובן) כאשר המסלול BGP.
 • γ = γ המסלול של המסלול קונסטי (זה מובן) כאשר המסלול BGP.
 • γ = γ המסלול של המסלול קונסטי (זה מובן) כאשר המסלול BGP.

נ"מ. א. לנסקס א. אלאקאטיון סטוריס א. הקדו א. רוב
הקל'ים average-case complexity. נזכר אלים בדרך בסיסית הידוע.

ד. (אם ϵ קטן מספיק, $\epsilon < \frac{1}{2}$)

[AB2]

(1979)

המחלקה NP

הבעיה: שפה $L \subseteq \{0,1\}^*$ שבה NP שווה ל- P (אם $P=NP$)

השאלה: האם $P=NP$? (אם $P=NP$)

$$\forall x. x \in L \iff \exists w \in \{0,1\}^* \text{ such that } M(x,w)=1$$

נקרא w "30"

אם $x \in L$ אז $M(x,w)=1$ (אם $P=NP$)

אם $x \notin L$ אז $M(x,w)=0$ (אם $P=NP$)

הבעיה: האם $P=NP$? (אם $P=NP$)