

הקדמה  
חשיבות  
היום החשוב  
מכונה אינטראקט  
בעיה לא חשיבות

סבוכות זמן

P  
NP

מנהלה

477 רב, במסגרת ובה מיליון ד-2 הקבוצה (המקרה וזמן זמן 2 הקבוצה), בשני ימים ויהי שיעור ביום. (בראש) ב. סביב. התחיל חובה ציון של התחיל יעצור 88% ציונים. יהיה מבחן ובחן באמצע הסמסטר, הבחן יהיה 15% מהציון הסיפורי (בכמה שאלות אחרי מסו) שאלה קבוצה של 477- שני  $13^{20}-16^{20}$ , שילי  $9^{20}-10^{20}$  עשרת הקידים ניתן להקדם דרך האתר של ס'77

ספרים: Sipser (נמו לאור וקראו באינטרנט), Arava-Barak (נמו לאור וקראו באינטרנט), מילוף זה באמצע Powerpoint של מילי ספרה.

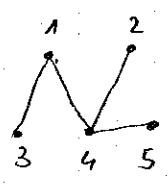
הקדמה

30s: עלו שלבי המילים החשובים (כאשר, לפני המילה) ההיננים שקולב זה לזה. זה מבין מצד של Church-Turing: כל מה שניתן לחשב בטבע, ניתן גם לחשב במחשב. תכונה בשנת C (או ב מיליון שנה).

50s: גיור השגיאות התחילה (צנים לחשב אך ניתן לחיוב בלוגיקה חבי טבע המילה (ברור \*))

• ככל שיש מספר בני מ ספרה  
- האלגוריתם הפשוט  $O(n^2)$   
- יש אלגוריתם  $O(n \log n)$  ממוטט - Fast Fourier Transform

• הכפול 2 מיליון מאח (לא מספר שלמה)  
- אלגוריתם (ש'בי)  $O(n^3)$   
- אפסר שטראסן  $O(n^{2.8})$  Strassen  
שפסל יותר טוב  $O(n^{2.37})$



• מבק מ מבנים רבים להבנתו. עמיתיה כמה שיותר מאוי שיהיו זוג המספרים (IS)

האלגוריתם הטוב ביותר לזכרון  $O(n)$

זו בעיה NP-שלמה וכמה יש לז אפסל בעיה מביאזיה, פ'זיקה, מבנו ...

70s: הכלני שהבעיה האוי קשורה למחשבת. בכ (נא) העבר שנקטו סבוכות חשיבות

חיסוב

משימה חסובה היא חיסוב פונקציה  $f: \{0,1\}^* \rightarrow \{0,1\}$  (מחלקת בינארית או ממצאית בינארית). כושר  $\Sigma^* = \cup_{n \geq 0} \{0,1\}^n$ .

\* (שם זה שהטוח יאל פוגע מנחמה יתר או שניה). להיגר יתר ממשלה (כינוי אחר עקף כשלנו). פ (כופ), לעתים לא ילפין אלפנו א התחום \*/

ערכו (תשנין) בחישוב פונקציות בולטניות. כושר,  $f: \{0,1\}^* \rightarrow \{0,1\}$ .

\*/ שפה רגש אלס של מחלקה, (נתן עתקניר לוג זה ע"י קליפה המחולקת שבהן f מחלקה 1 (כהקדמה בשפה)). \*/

בצורה שקולה, נתון עברו (ל (languages) שנתן תה קלטה של  $\{0,1\}^*$ ).

כושר,  $L_p = \{x \in \{0,1\}^* : f(x) = 1\}$ . לעולם קרא עצה כליה החלטה.

\*/ (מצור לעציות המסורה, אם היינו ווקעם לפגרי את הקליה "הלם קיימת קליפה בת" בלוק" א היינו ילויב אלוי לפגרי את הקליה בצמן בולונאי. (שלים ע"ג שלמקום את א ואל עתף ע"ב) כל הכנסתיות זה פיתוח לא טוב, כ אקולא:  $\{0,1\}^n \approx \binom{n}{k}$ . אך קיים פיתוח טוב אכך בצמן בולונאי בהיותן א \*/

אינדיקטור:  $INDSET = \{ \langle \sigma, a \rangle : \text{קיימת } \sigma \text{-קליפה של לפגרי א} \}$  /  $\{ \text{קודקודים שליו בינרים אל קול}$

עו בצורה שקולה (יתן ענסת כפונקציה בולטנת)  $f(\langle \sigma, a \rangle) = \begin{cases} 1 & \text{אם קיימת קליפה} \\ & \text{ב } \sigma \text{ של } \dots \\ 0 & \text{אחרת} \end{cases}$

מילא החישוב (שלם ממל משנה) יכיה (א) גורמתים לעתקים בטבר C (או Java, או שבר מכונית השילונם עם סרט ממו או יתר...). הרעה: אין מילל לזכרון.

\*/ נשמך אם שברוק אין רפואה שברט C יס נמצה כל לזכרון. לו לא ממצה של המל C ח"כ אלפנו נכר עו שבר C שיויה מילכלת לזכרון \*/

מכונה החישוב האוניברסלית

נתן עינינו תוכנית בטבר C בלברט מחוזית של  $\{0,1\}$  (סמן כי  $M_a$  את החיפוטא שנתנו ש  $\alpha$  מיינדט.

מערב קים אלפגרימ  $U$  שבהיותן C  $U(x, \alpha) = M_a(x)$  :  $x \in \{0,1\}^*$ ,  $\alpha \in \{0,1\}^*$  (מבחינה סימולטאנית)  $U$  משרת את  $M_a$  כל קים x. (Turing)

הערה: אם  $M_a(x)$  זר ע  $U(x, \alpha)$  (תקל).

כאיין הוכחה  $U$  איור (ל התוכנית  $\alpha$  שיהי שירה ומסמלם אמת.

הערה: Turing בטרם הרע שנתן עתוף ביונת כל ממשל.

בעיות לא חשבוניות (uncomputable, undecidable, non-recursive)

בעיה (Turing) - קיומה פונקציה  $UC: \{0,1\}^* \rightarrow \{0,1\}$  שכל נתיב בשיעור  $\beta$  לא מוגדרת.

הוכחה שניתן אחרת שלילית משפט פונקציה  $f$  אם  $\beta \in \{0,1\}^*$  האלמנטים כשמופיעים לא קרא  $x$  ביצר התולטו נתיב  $f(x)$  ככל  $f(x)$ .

הוכחה 1: קביעת הפונקציה  $\{0,1\}^* \rightarrow \{0,1\}$  היא משימה  $\mathcal{N}$  אם קביעת האלמנטים היא משימה  $\mathcal{N}_0$  הכוללת את קבוצת  $\mathcal{N}_0 < \mathcal{N}$  ולכן יש פונקציה  $\beta$  לא מוגדרת.

הוכחה 2: (שגיאת הטכניק (הכסוף (שגוי הטכניק) שבלעדית מוכיח את המשפט קטוע) / וההוכחה היא אגרת פונקציה ש"צפוי" את כל האלמנטים הקיימים \*

	$M_0$	$M_1$	$M_2$	$M_3$	$M_4$	$M_5$	$M_6$	$M_7$	$M_8$	$M_9$	$M_{10}$	...
0	0	1	1									
1	0	2	0									
00	00	1	1									
01	2	0	0									
10												
11												

אם נסתכל על הטבלה, וזה נקרא את הפונקציה שלנו  $\beta$  (היא כסוף).

$UC(0) = 1$   
 $UC(1) = 0$  (שגיאת הטכניק)  
 $UC(00) = 0$   
 ...

$$\forall \alpha \in \{0,1\}^*. UC(\alpha) = \begin{cases} 0 & \text{אם } M_\alpha(\alpha) \text{ מוגדרת} \\ 1 & \text{אחרת} \end{cases}$$

נניח  $M_\beta$  לקוח אלמנטים  $M_\beta$  שיוצג  $\beta$  הקוד  $\beta$  התחילת את  $UC$  כלומר לא קרא  $\alpha \in \{0,1\}^*$   $M_\alpha(\alpha)$  מוגדרת ומשימה את  $UC(\alpha)$  ככל  $\alpha$ . כפי, אבל  $\alpha = \beta$  קרא  $M_\beta(\beta)$  מוגדרת ומשימה  $UC(\beta)$  ככל  $\beta$  כי מוכיח להפך את  $UC$ .

הוכחה  $Halt = \{x, \alpha : M_\alpha \text{ קרא } x\}$

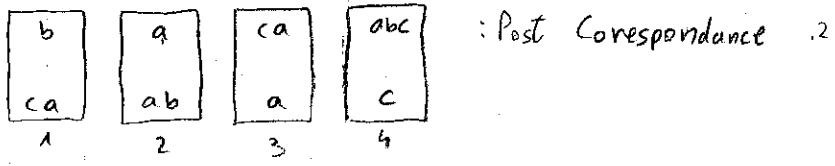
משפט:  $Halt$  אינה ניתנת לחישוב.

הוכחה נניח  $M_{Halt}$  שיש אלמנטים  $M_{Halt}$  הפותר את  $Halt$  (כאן  $\alpha$  קרא  $M_\alpha$  אלמנטים  $M_\alpha$  שפותר את  $UC$ , כפי,  $UC$  האלמנטים הקודם, בהינתן קרא  $\alpha$ ,  $M_\alpha$  מפעיל את  $M_{Halt}(\alpha)$  אם התוצאה היא "לא מוגדרת", נכריז ונקיט ככל "א", אחרת (כפי) כפי  $u$  את  $M_\alpha(\alpha)$  ונקיט את התפקוד  $M_\alpha$  שיהיה החיבור.

הוכחה טענת ההוכחה שהתחננו בה היא טכניק הרדוקציה: הטני שלביה  $B$  קשה אפוא כמו  $A$  כי זה שהתחננו שפתרון  $B$  יתן גם פתרון  $A$ .

הוכחה (ניסוח) יש ביד הוכחה בליט שכל נתיב לחישוב:

1. המילה המסיימת של המילה. נתונה משימה  $X^3 + Y^2 + 5X^2Y + 9 = 0$  ולקיים  $X, Y$  המי ויש פתרון במספרים שלמים.



היא איננה מספר המילה  $X$  כי ישנה מספר  $X$  שיהיה  $X$  שיהיה  $X$  (כאן במקרה אחר).

סביביות זמן ריצה (1965)

(נסר) למה לא מחלקה של שפת, אומר, של פונקציות בולטיות.

הצורה: סביר פונקציה  $\mathbb{N} \rightarrow \mathbb{N}$ :  $D \rightarrow T$  (גודל אר  $D$  TIME( $T$ )) בהיכר אלו השלם שניתן לבנות אותו בעזרת אלגוריתם של בזמן  $O(D)$  עבור קבוע  $c$  כלשהו.

הצורה:  $P = UDTIME(n^c)$   
 $c \geq 1$

• הצורה:  $P$  מוצגת בצורה יציבה (robust): קל לראות מחלקה בין אם (נסר) לא תוכנית בשפת C, Java, או מכונה טיולית.

• (נסר) לא  $P$  עלה במחלקה הכלילית שנמצאת אפואו כזמן וזמן. זה מוזק מחלקה זו בק שאלה נרצה לחסור שלביות אינו  $P$ .

• אפשר גם להתייחס לאלגוריתמים זהשתיים כאלקואיט. זהו זה מוכיח שהצורה המחלקה BPP, שאלה פתירה חלופה היא  $P = BPP$ ?

• אם משתמשים בפירוק קיוצ'ט מחקם מחלקה שקרית BQP.

• ניתן להסתכל גם על פתרונות מקורבים או פתרונות למה הקלם.

NP (מחלקה) [Arora Barak 2] (1971)

ההצורה NP היא מחלקה השלם שניתן לייצר שליבת אלה בזמן פולינומילי.

הצורה: שפה  $L \subseteq \{0,1\}^*$  היא  $P$  - NP אם קיים פונקציה  $\mathbb{N} \rightarrow \mathbb{N}$  ואלגוריתם  $M$  של  $\{0,1\}^*$  כך של  $x \in \{0,1\}^*$ , מחקם:

$$x \in L \iff \exists w \in \{0,1\}^{p(|x|)} \text{ s.t. } M(x, w) = 1$$

\* אם היינו משני את ההצורה  $M$  ו-  $A$  ס, היינו  $N$  היה משנה את  $\rightarrow$  ההצורה (בדיון היינו נשאל)  $\rightarrow$   $NP$ . אם היינו משנה את  $E$  ו-  $A$ , היינו שמים  $\rightarrow$   $co-NP$ .