

מעבויג למחקר
ירבל פילמוס

על מה אני עובד

אני מוצא"ן בשלושה תחומים עיקריים:

- סיכויים מישורית
- אנטליזת פוריה ציסקראי
- קומבינאציות

יש הרבה קשרים בין תחומים אלה.

סיבוכיות חישובית

סיבוכיות חישובית היא תחום משלים
לאלגוריתמים. בעוד שאלגוריתמים מראים
מה ניתן לעשות, בסיבוכיות אנחנו מראים
מה לא ניתן לעשות.

בנוסף, מצדדנים באמצעים חישוביים אחרים:
מצדדים, הוכחה, תקשורת, ועוד.
בהקשר זה מצדדנים גם בגבולות חישוביות
וגם בשלישיות.

דוגמה: החתכות של קבוצות

אנ"ש מחזיקה תת-קבוצה $Z \subseteq A, \dots, \dots$

וי"צ'ני מן מחזיק תת-קבוצה $B \subseteq \{1, \dots, n\}$.

הם מצוננים לעלוג האם שגת הקבוצה

נחבבה, צ"י שליחה ביאים אינן לשני.

מטרת למצוד אג מספר הביאים שנשלחים.

שימושים: חסמים תחלתיים למצרכי מקוצרה

ולאלגוריתמים בעלי זכרון מוגבל (streaming).

הפרוטוקול הטריידינג

א"י: שולחת לבן את הקובץ שלה (מ גיל'ים).

בן מחזיר גיל'ים אחז: "כן" או "לא".

סה"כ: וזו גיל'ים.

בז' קורב הראה שהצדדים ח"ק"ים להחליף

(מ) גיל'ים, אפילו אם אנחנו מרשים להם

להשגשג באקראיוו וללא צד גס'כו' קבוצ.

פרוטוקול הדמזם

צגור טל אהז מ-ח האיקרימ האקרימ:

אי"ק וקן מ"קרימ מסר האזח [נס].

שול אוחץ על שרון צבר שסוכר מ-ו-ס.

כשמיצ האספר של אהז מהסקרימ,

אימ האיקר נצבר מהקבוצה שלו, הוא אוחץ על זמזם,

ומכסיקים (איקר זה אינו אחילוק).

אימ אף אהז על לחץ האקרימ, האיקר אחילוק!

פרוטוקול הדמזם

ברורמן ואח' הראו כיצד לממש את הפרוטוקול
באמצעות 0.4827 בי"ס, והראו שמספר זה
גורמטי! (עצ כי (מ)ס).

בצורה עם סלונט (יובל זמן) ואח', הראו
שכל פרוטוקול שהוא "כמעט" אורמטי.
חייב להיות בהנחה לפרוטוקול הזמזם.

אנליזת פוריה דיסקרטי

אנליזת פוריה שימושית מאוד במתמטיקה
בהנדסה, ואפילו במחשבים – למשל בצ'יפ קוץ
קול, גמורה, ו-ו'צאא.

התיאוריה של מצד הממשלה, פצמים רבוג אנו
ממצע'ים בפונקציות $\mathbb{R} \rightarrow \mathbb{C}$, f ,
למשל הפונקציה שמצד מסוים מחשבה.
כלי חשוב לחקור פונקציות כאלה הוא
אנליזת פוריה דיסקרטית.

אבל מה זה?

נקודת המוצא היא פילח פור"ק:

$$f(x_1, \dots, x_n) = \sum_{S \subseteq [n]} \hat{f}(S) \chi_S, \quad \chi_S = \prod_{i \in S} (-1)^{x_i}$$

אנל'טת פור'ק ז'סקר'ת ש'מול'ת בת'ק
נ'כר מת'מ' הת'אור'ת, $\epsilon n \delta$:

PAC learning, property testing,
hardness of approximation

הטלת מטבע משותפת

2 שחקנים מאוילים מטבע הוצן, וזה התוצאה
מבצעים בונקציה $f: \{0,1\}^2 \rightarrow \{0,1\}$ כך שחקנים
הסוף מטבע הוצן.

הבציה: m מהשחקנים משתפים בקונויה,
שמירה להאר או התוצאה.

איזה בונקציה f כבאי' לחתור בני' להקאים
שוק מספר גזאל של שחקנים יוכל להאר
אך התוצאה?

פונקציית הרוב

בחירה מרבית היא פונקציה הרואה
שמינה בנת (הח) המאיים.

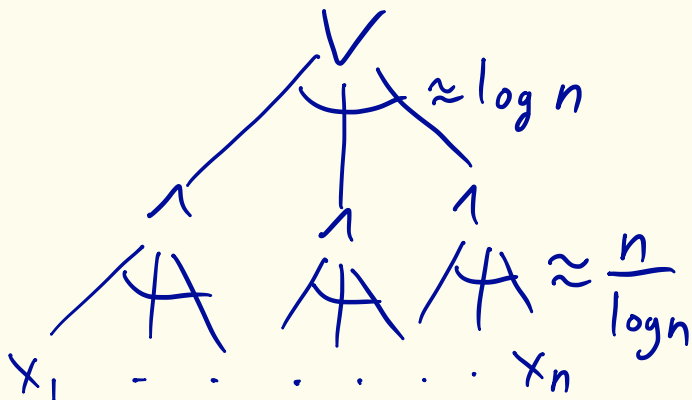
אם הח מסתמים מצביעים ב-

אז היא צאה הסופית תהיה ב גסיכו' $\frac{1}{2} > p$

עבור p קבוצ שליו' ק-ח.

האם פונקציה זו אופטימלית?

פונקציית השבטים



כז' עהאוו אר הת וצאה ע-ו, נצחלים

כ- $\frac{n}{\log n}$ שתקנים. אקום כז' עהאוו ע-ס.

מסב'קים $\log n$!

הפונקציה האופטימלית

איילטאי (Ajtai) וליטאל גיארן פונקציה קה

נדרשים $\frac{n}{\log^2 n}$ שחקנים כדי להאג סג

הטובאה (לכיוון כלשהו).

פונקציה קפרי קאה

מזד שני, טובאה 'סודית' בתחום (L, K)

מראה ל- $\frac{n}{\log n}$ שחקנים **תמיד** יכולים להאג

את הטובאה. מה האמת?

צ'שחק סב השאלות

קומבינאטיקה היא ג'חוס רחב. אזצ'ים אאגו
באמצעות צ'בונז' משוגפת עם י'קל צ'גן (שהוצ'כר
ל'צ'ע) ו'ש' מוכן, שמצ'ורף ל'פקולט'ה השכנה הקרוז'.

ל'ש' קוש'ג' עם מספר בין 1 ל'נ.

צ'נ' צ'ר'יק ל'מצוא אאגו באמצעות

שאלות כן/ל'א. מ'ט'ר'גו ל'מצ'ר אג' מס' השאלות.

ל'כמה שאלות י'צ'יקק ח'מקרה הצ'רוצ' ה'י'ג'ר'ג'?

שאלות קצרות

האסטרטגיה האופטימלית של זן עלולה?

לכלול שאלות מאז מסוג כוונת.

נרצה להבדיל את זן N - N שאלות

כואל-ביאליג (שאינן גלויג K - K).

צבור איטי N זן יכול צד"ן

למשל אסטרטגיה אופטימלית?

שיעור קצרות

רש"מ ה: $1.25 \approx N$ גמ' 3 מספיק.

היקב 1.25 הבוק עבד א'נסוף ערכי ח.

א'מא וצצ'מ אר סדר האונס המצויק עכ"ח,

א'ק י'ש ע'מא השערה מקוססת.

בעצ'ה נוספת היא ש- 1.25 השאלות האבוא

א'מא נ'גמא באופן מפורס - א'מא רק מוכיחים

קיום של אופ' כ'ה, באמצעות השלטה ההסגרית.

תורת ההסתברות