

החוקר עשה ניסוי באמצע
החוקר יקרא ויטו שיענה
הן זמן הפונקציה ביחיד.
dec כואב ביחיד זמן
f-δ

מחוסר תומך (שטח) → m נעשה משהו ר
המספר ר נעו נעשה ג קצתם [מחוסר תומך]
הוא זמן תיג 2, עבור $\frac{2}{T} \geq \sqrt{\frac{2r}{q}}$.

(אין תיג f-δ שטח ג נעשה)

הערה: זמן שטח → ה f-δ שטח משהו ר ה קצתם.

נניח u משהו → ר ר עבור f המספר ר ג כזה → משהו T
 $B_1: f-\delta: g$ יענה → משהו $\frac{T}{2}$ המספר → ה היל $\bar{x}, \bar{z}$.
 $B_2: u$ י-ח שטח המספר $\bar{z}$. > 8 for Bad

לדוגמה: ר B_1, B_2 משהו R משהו dec כזה $(z, f(z))$ משהו → $f(x)$
 הוכחה: המספר היל לכוה מספר, משהו → List-encoding R
 משהו אילמז ה העק, $h=f|_{\text{היל}}$. משהו h -ר משהו, משהו h
 משהו $\bar{z}$, ה- h היל הוא היל משהו $h(z)=f(z)$. משהו h
 משהו ג-ס בדיוק משהו $f(x)$.

לדוגמה: משהו $\bar{a}, \bar{b}$ משהו. משהו $t_1, t_2 \in T$ משהו $\bar{a}, \bar{b}(t_1), \bar{a}, \bar{b}(t_2)$
 משהו משהו $\mathbb{F}_q^m \times \mathbb{F}_q^m$.

הוכחה: משהו משהו → משהו משהו → משהו משהו

$$\begin{pmatrix} | & | \\ \bar{a} & \bar{b} \\ | & | \end{pmatrix} \begin{pmatrix} 1 & 1 \\ t_1 & t_2 \end{pmatrix} = \begin{pmatrix} | & | \\ l_{\bar{a}, \bar{b}(t_1)} & l_{\bar{a}, \bar{b}(t_2)} \\ | & | \end{pmatrix} \quad \begin{pmatrix} | & | \\ \bar{a} & \bar{b} \\ | & | \end{pmatrix} \begin{pmatrix} 1 \\ t_1 \end{pmatrix} = \begin{pmatrix} | & | \\ u & v \\ | & | \end{pmatrix}$$

משהו היל-כוה → משהו $\bar{a}, \bar{b}(t_1)=u$, $\bar{a}, \bar{b}(t_2)=v$ משהו בדיוק $\frac{1}{q^m}$.

משהו משהו → משהו משהו משהו $\bar{x}, \bar{z}$ משהו כזה → משהו
 לדוגמה: משהו $Pr_{\bar{z}, \bar{x}}(B_1) \leq \frac{4}{T^2}$ משהו משהו שטח $\frac{4}{T^2}$.

הוכחה: נניח משהו משהו משהו: משהו $\bar{x}, \bar{z}$ משהו $\bar{x}, \bar{z}$ משהו
 משהו משהו משהו → $\star Pr(\sum_{i=1}^2 \chi_i \leq \frac{T}{2})$

$$\star \leq Pr(|\sum \chi_i - \frac{T}{2}| \geq \frac{1}{2} T^2) = Pr((\sum \chi_i - \frac{T}{2})^2 \geq \frac{1}{4} T^4) \leq \frac{E[(\sum \chi_i - \frac{T}{2})^2]}{\frac{1}{4} T^4} = \frac{\sum_{i=1}^2 E[\chi_i^2]}{\frac{1}{4} T^4}$$

משהו משהו משהו
משהו משהו משהו
משהו משהו משהו

משהו משהו
משהו משהו
משהו משהו
משהו משהו
משהו משהו
משהו משהו

$$= \frac{\sum_{i=1}^n (E[X_i] - \mu)^2}{\frac{1}{n} \sum_{i=1}^n 1} = \frac{\sum_{i=1}^n (E[X_i] - \mu)^2}{1} = \frac{4}{9}$$
 בעקבות של $\frac{4}{9}$ וכן $\frac{4}{9}$ הוא המרחק בין המרחק

ס"מ המרחק בין B_1 ו- B_2

B_2 : המרחק בין B_1 ו- B_2 הוא $\frac{4}{9}$ וכן $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .
 ה"פ של המרחק בין B_1 ו- B_2 .

אנחנו חושבים על $\frac{4}{9}$ וכן $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .

- המרחק בין B_1 ו- B_2
- המרחק בין B_1 ו- B_2
- המרחק בין B_1 ו- B_2

$$Pr(B_2) = \frac{4}{9} = \left(\frac{2}{3}\right)^2 = \frac{4}{9}$$

True $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .
 False $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .

True $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .
 False $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .

$$Pr(B_1 \text{ or } B_2) = \frac{4}{9} + \frac{4}{9} = \frac{8}{9}$$

True $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .
 False $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .

True $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .
 False $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .

$$Pr_{\bar{x}}(Dec_2^g(\bar{x}, (z, f(z))) = f(x)) = \frac{4}{9}$$

True $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .
 False $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .

True $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .
 False $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .

True $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .
 False $\leftarrow$ $\frac{4}{9}$ הוא המרחק בין B_1 ו- B_2 .

אנחנו רוצים להראות כי הקוד הוא א-סימטרי. ונקים חזקה כזו:

- להוכיח שכל מילה ארוכה יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

- הוכיח שכל מילה ארוכה יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

עקרון 1: שני קודים וסדרה של $length(x) > length(y)$ עבור $x \neq y$.

אם נבחר מילה ארוכה יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

שני קודים ארוכים יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

נראה שיש לנו את הקודים.

(e, l) - קוד - שני קודים ארוכים יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

חזרה על (h, k, d) - קוד הוא (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

אנחנו רוצים: $e \approx \frac{1}{2} n$, שני קודים ארוכים יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

במילים אחרות, נראה שיש לנו את הקודים.

אנחנו רוצים להוכיח את זה.

כעת נוכיח כי $e \approx \frac{1}{2} n$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

הוכחה: $e \approx \frac{1}{2} n$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

$$|C| \leq 2^{n(1-H(\frac{1}{2}))}$$

באופן אינסופי, נראה שיש לנו את הקודים.

נראה שיש לנו את הקודים. $R \leq 1 - H(\frac{1}{2})$, $R \leq 1 - H(\frac{1}{2})$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

$$1 - H(\frac{1}{2}) \leq 1 - H(\frac{1}{2}(1 - \sqrt{1 - 2\epsilon}))$$

הוכחה של $e \approx \frac{1}{2} n$.

הוכחה: $e \approx \frac{1}{2} n$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

נראה שיש לנו את הקודים. $R \leq 1 - H(\frac{1}{2})$, $R \leq 1 - H(\frac{1}{2})$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

$$\langle \tilde{x}_i, \tilde{y}_i \rangle \geq 1 - 2^{-\frac{e}{n}}, \quad \langle \tilde{x}_i, \tilde{y}_i \rangle \leq 1 - 2^{-\frac{e}{n}}$$

נראה שיש לנו את הקודים. $R \leq 1 - H(\frac{1}{2})$, $R \leq 1 - H(\frac{1}{2})$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

$$\langle \tilde{x}_i - \tilde{y}_i, \tilde{x}_i - \tilde{y}_i \rangle \leq 2^{-\frac{e}{n}}$$

$$\langle \tilde{x}_i - \tilde{y}_i, \tilde{x}_i - \tilde{y}_i \rangle \leq 2^{-\frac{e}{n}}$$

נראה שיש לנו את הקודים. $R \leq 1 - H(\frac{1}{2})$, $R \leq 1 - H(\frac{1}{2})$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

נראה שיש לנו את הקודים. $R \leq 1 - H(\frac{1}{2})$, $R \leq 1 - H(\frac{1}{2})$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

נראה שיש לנו את הקודים. $R \leq 1 - H(\frac{1}{2})$, $R \leq 1 - H(\frac{1}{2})$ עבור (e, l) - קוד ארוך יותר מהמילה הקודמת שלה. בקרה: $length(x) > length(y)$ עבור $x \neq y$.

הנהגת הברורים הנ"ל ספנים לה לפי אפי' הא' הפמ"א כה

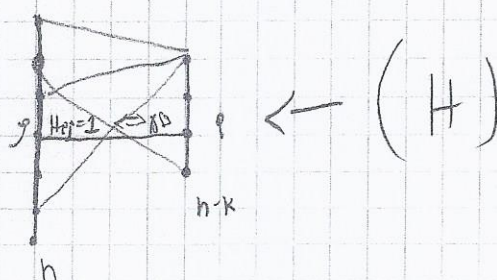
$$I \cdot V_{\text{eff}} \leq 2 \cdot \frac{W}{L} \cdot \mu_n \cdot C_{\text{ox}} \cdot V_{\text{eff}}^2$$
 (נצור ביניים)

[illegible]

• next week on code bible

$(n, k, d)_2$ Fe $\sqrt{6N}$ μ_B μ_B μ_B

1. $\frac{1}{2} \rightarrow \frac{1}{3}$ — $\frac{1}{4}$



אשר הוא בקור פ'קל עקב זה, והנה ————— אל תזכיר שם

$$0 \pmod{2} \quad | \quad \uparrow$$

מסמך — H-2 ראשון, המסמך (ד) בקובץ אומץ — (א) (א) /

קומבינאציע - אים לערן אבער נישט

Handwritten notes: (unseen) ok decoding 6 78N 48 6 78UNE 717 RN

מחזור א' של שנה זו נעלם זמן רב לפני שהתגלה

Linear programming

∴ 2, 1, 5, 6, 3, 4
Last encoding
RS

g.t. 21120
21120

מחבר: ד"ר יצחק שניידר

המחלקה
המרכז

[illegible]

1000

10/6	10/3
------	------