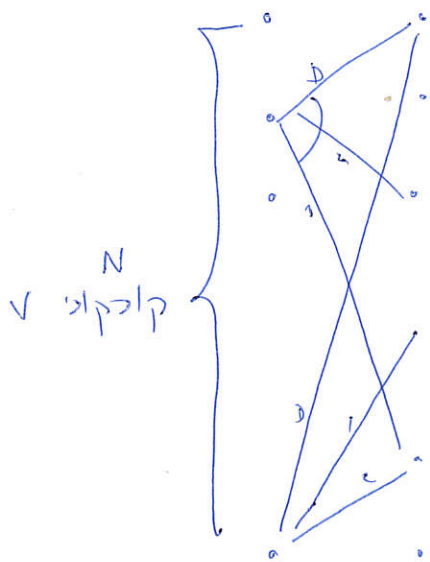


PRG for space-bounded comp

הקטנים ביותר שיש להם $1/n$ מקום

הקטנים ביותר שיש להם $1/n$ מקום, הם הקטנים ביותר שיש להם $1/n$ מקום

!מכאן: $[N, D, \lambda]$ $G=(V, E)$ ויש לו קטנים ביותר $1/n$ מקום



הקטנים ביותר שיש להם $1/n$ מקום

$((v, i), (v, i+1)) \Rightarrow (v, w) \in E$

$v \in V$ ויש לו קטנים ביותר $1/n$ מקום

$v[i] = w$

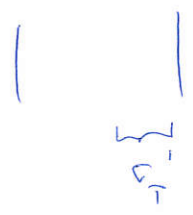
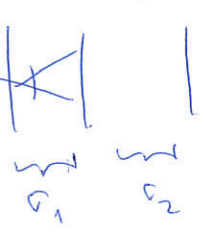
הקטנים ביותר שיש להם $1/n$ מקום

הקטנים ביותר שיש להם $1/n$ מקום, הם הקטנים ביותר שיש להם $1/n$ מקום

$\sigma_i \in [D]$ ויש לו קטנים ביותר $1/n$ מקום

$(v[\sigma_i], i+1)$ ויש לו קטנים ביותר $1/n$ מקום

הקדמה: המטרה היא להבין את המבנה של המרחב הווקטורי $\mathbb{R}^n$ ואת התאם בין המרחב הזה למרחב המטריצות $M_n(\mathbb{R})$.



$$(\sigma_1, \dots, \sigma_n) \in \mathbb{R}^n$$

המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 .

המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 . המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 .

המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 . המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 .

המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 . המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 .

המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 . המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 .

המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 . המרחב $\mathbb{R}^n$ הוא מרחב ווקטורי ממדים n . המרחב $M_n(\mathbb{R})$ הוא מרחב ווקטורי ממדים n^2 .

Branching program

Σ alphabet T tape, W width BP

$V \in W^x [T+1]$

configuration for time t

$l: (W^x [T+1]) \times \Sigma \rightarrow V$ local rule

$l((v, i), \sigma) = (v', i')$ write, move head

$i' = i + 1$ right

move head left

$[N, D]$ $D \in \Sigma^*$ $S \in V$, $G = (V, E)$ tape BP input

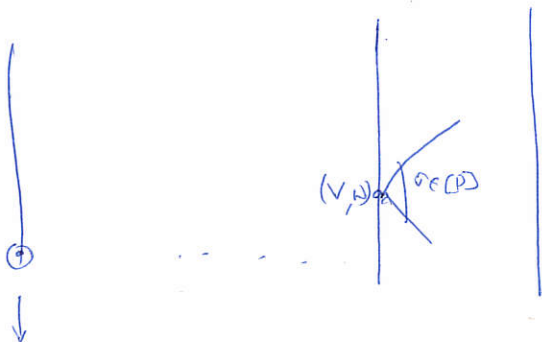
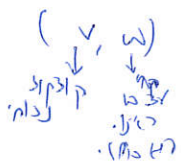
BP Σ^*

(time t) $\rightarrow$ time $T+1$

$V^x([N+1])$ configuration

time t

time



$$l((v, w), \sigma) = \begin{cases} (v[\sigma], w) & \text{if } v[\sigma] \neq w \\ (v[\sigma], w+1) & \text{if } v[\sigma] = w \end{cases}$$

write
move
head

configuration
 $(S, 0, 0)$

$(v, N+1)$ = input symbol and head - acc
- acc

$N(N+1)$ $\approx$ N^2 N $1/5$

$T+1$ γ

$|E|=D - \Sigma$

Σ N Q_1, Q_2 γ acc $\rightarrow$ acc $1/5$

$(0, 10-01)$ $(1, \dots, 1)$ $\rightarrow$ acc $1/5$

acc rej 1

acc $\rightarrow$ acc $1/5$ M BP T Σ N $1/5$ acc $1/5$

Σ^T $1/5$ acc $1/5$

MCD $1/5$ acc $1/5$ BP $1/5$ acc $1/5$

Σ N BP $1/5$ acc $1/5$ BP $1/5$ acc $1/5$

$\sigma_1, \dots, \sigma_T \in \mathbb{P}$ $1/5$

acc $1/5$ BP $1/5$ acc $1/5$ BP $1/5$ acc $1/5$

(acc, rej) $1/5$ acc $1/5$ BP $1/5$ acc $1/5$

הערה

plc

20/10/20

5

ϵ -PRG

$\hookrightarrow$

$$G: \{0,1\}^L \rightarrow \Sigma^T$$

משפט 2.1

(3) $M \in \mathcal{P}(\mathcal{P}(\Sigma^T))$

$$[N, T, \epsilon] \rightarrow \text{BP}$$

BP

(3) $M \in \mathcal{P}(\mathcal{P}(\Sigma^T))$

let $M \in \mathcal{P}(\mathcal{P}(\Sigma^T))$

BP

BP

$\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$

$\hookrightarrow G$

משפט 2.2

$\mathcal{C}$ is a $\mathcal{C}$ -code

BP

$$G: \{0,1\}^L \rightarrow \Sigma^T$$

PRG

$\hookrightarrow$

משפט 2.3

$$L \rightarrow T$$

stretch

BP

$$L = O(\lg n) \rightarrow \text{poly}(n) = T$$

$\hookrightarrow$

$$\boxed{T = 2^{\Theta(L)}}$$

$$\left[\begin{array}{ccc} 2^n & \text{poly}(n) & \sum_{i=1}^n \epsilon_i \\ \downarrow & \downarrow & \downarrow \\ n/2 & \text{poly}(n) & O(n) \end{array} \right] \rightarrow \text{BP}$$

$\epsilon_i \in \epsilon$

$\text{poly}(Tn) = \dots$

$\text{poly}(Tn)$

$$\frac{? \text{pr} \quad \text{PRG} \quad \varepsilon' \quad \text{PRG} \quad \text{h/c} \quad \text{h/c}}{}$$

$$G: \{a, b\}^L \rightarrow \{a, b\}^T \quad \text{הפוך} \quad \text{הפוך} \quad \text{הפוך}$$

$$[W, T, \Sigma] \text{-BP} \quad \text{f} \quad \varepsilon \text{-PRG} \quad \text{h/c}$$

$$L = O\left(\lg\left(\frac{|W| \cdot |T| \cdot |\Sigma|}{\varepsilon}\right)\right) \quad \text{PRG}$$

$$Y_1, \dots, Y_L \quad \text{הפוך} \quad \text{הפוך} \quad \text{הפוך} \quad \text{הפוך}$$

$$Y_i \in \Sigma^T \quad \text{הפוך} \quad \text{הפוך} \quad \text{הפוך}$$

$$G: [L] \rightarrow \Sigma^T \quad \text{הפוך}$$

$$G(i) = y_i \quad \text{הפוך}$$

$$[W, T, \Sigma] \text{-M} \quad \text{M BP} \quad \text{h/c} \quad \text{הפוך}$$

$$\Pr_{\sigma} \left[\frac{1}{M} \sum_{i=1}^M G(i) \in \Sigma^T \right] \leq \frac{1}{2} \quad \text{הפוך}$$

$$\delta = \frac{1}{|W|^{T \cdot |W| + 3}} \quad \text{הפוך}$$

$$\sigma \in \Sigma \quad \text{הפוך} \quad \text{הפוך}$$

$$P = P(\sigma) = \Pr_{Y \in \Sigma^T} [M(Y) = \sigma] \quad \text{הפוך}$$

$$P' = P'(\sigma) = \Pr_{i \in [L]} [M(y_i) = \sigma] \quad \text{הפוך}$$

$$M[y_i] = \sigma \quad \text{in } X_i \quad \mu_0$$

$$E(X_i) = \mu \quad \text{in } X_1, \dots, X_n \quad \mu$$

$$\Pr \left(\left| \frac{1}{n} \sum X_i - \mu \right| \geq \frac{\epsilon}{\sqrt{n}} \right) \leq e^{-\frac{n \epsilon^2}{2 \sigma^2}} \quad \text{for } \epsilon > 0$$

$$L = \mathcal{O} \left(\frac{\log \frac{1}{\delta}}{(\epsilon/w)^2} \right) \quad \text{for } \delta$$

$$\Pr \left(\left| \frac{1}{n} \sum_{i=1}^n \epsilon_i \right| \geq \frac{\epsilon}{\sqrt{n}} \right) \leq \frac{1}{\sqrt{n}} \cdot \delta$$

↓

$$\begin{aligned} & \text{for } \epsilon > 0 \\ & \Pr \left(\left| \frac{1}{n} \sum_{i=1}^n \epsilon_i \right| \geq \frac{\epsilon}{\sqrt{n}} \right) \leq \frac{1}{\sqrt{n}} \cdot \delta \\ & \text{for } \epsilon > 0 \end{aligned}$$

$$\Pr \left(\left| \frac{1}{n} \sum_{i=1}^n \epsilon_i \right| \geq \frac{\epsilon}{\sqrt{n}} \right) \leq \frac{1}{\sqrt{n}} \cdot \delta < 1 \quad \text{for } \epsilon > 0$$

$$\Pr \left(\left| \frac{1}{n} \sum_{i=1}^n \epsilon_i \right| \geq \frac{\epsilon}{\sqrt{n}} \right) \leq \frac{1}{\sqrt{n}} \cdot \delta < 1 \quad \text{for } \epsilon > 0$$

הוכחה בשיטת 2
 $BP \quad \delta \quad - \text{check} \quad \text{to} \quad PRG$

$\text{PRG } \{ \text{seed} \}$
 $\Sigma \rightarrow \{0,1\}^*$

$[U, ZT, \Sigma]$

BP

מכונה

M

היא

$\frac{H(\Sigma)}{c}$

ולכן מראה כי $X \in \Sigma^T$ מקבלת את התוצאות של M על מנת שהיא תהיה מקבילה ל- Σ

הוכחה כי $\Sigma = \{0,1\}^n \subset W$ היא תת-קבוצה של W , ולכן Σ היא תת-קבוצה של W

כעת נראה כי X היא תת-קבוצה של M וכל $x \in X$ היא תת-קבוצה של M

$\lg(|W|)$

$$(X \mid \Sigma_T = 0)$$

$\downarrow$
 Σ_T^*

$\rightarrow \frac{H(\Sigma)}{c}$

$$\lg(|W|) - \lg(|\Sigma|) = \lg\left(\frac{|W|}{|\Sigma|}\right)$$

(seed, PRG) $\rightarrow \text{PRG}$ $\rightarrow \text{PRG}$ $\rightarrow \text{PRG}$

הוכחה כי $E(X, y)$ היא תת-קבוצה של X

M היא תת-קבוצה של X

$$E: \left[\begin{matrix} \Sigma^T \\ \{0,1\}^n \end{matrix} \right] \times \{0,1\}^+ \rightarrow \left[\begin{matrix} \Sigma^T \\ \{0,1\}^{m_2} \end{matrix} \right]$$

PRG

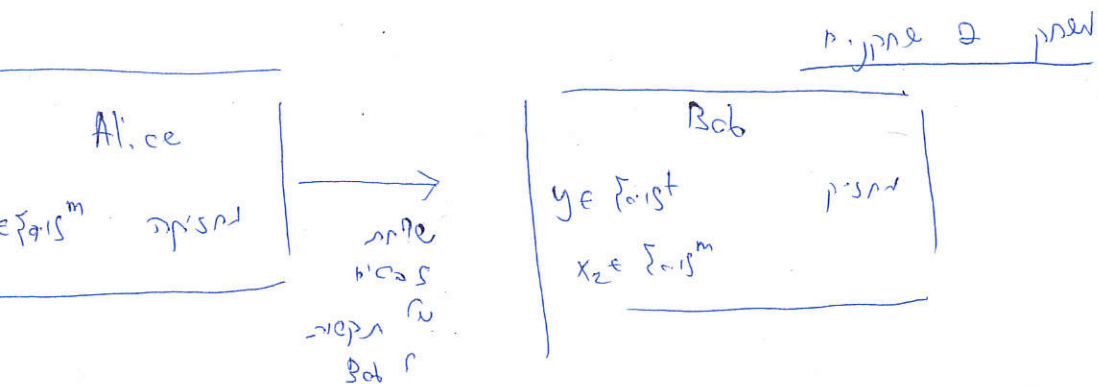
(k, ϵ) strong ext

$s = \lg |W|$

$k = m_2 s - \lg \frac{1}{\epsilon}$

$\epsilon > 0$

$$\sigma(x, y) = (x, E(x, y)) \quad \sigma: \{0,1\}^{m_1+m_2} \rightarrow \{0,1\}^{m_1+m_2}$$



ההצגה 2, בה x הוא מידע אודות x ו- y הוא מידע אודות x ו- x_2 הוא מידע אודות x ו- x_2 הוא מידע אודות x

ההצגה 2, בה x הוא מידע אודות x ו- y הוא מידע אודות x ו- x_2 הוא מידע אודות x ו- x_2 הוא מידע אודות x

$$x \in \{0,1\}^m \Rightarrow \begin{cases} x_1, x_2 \in_R \{0,1\}^m \\ y \in_R \{0,1\}^t \end{cases} \quad (1)$$

$$\begin{cases} x_1 \in_R \{0,1\}^m \\ x_2, y \in_R \{0,1\}^t \end{cases} \quad (2)$$

$x_2 = E(x_1, y)$

ההצגה 2, בה x הוא מידע אודות x ו- y הוא מידע אודות x ו- x_2 הוא מידע אודות x ו- x_2 הוא מידע אודות x

shared randomness r $\Rightarrow$ $y = r \oplus x$

A, B $\Rightarrow$ $x_2 = E(x_1, y)$

$$H_{\infty}(X_1 | W=w) < k$$

pk on weh

e 32)

232)
17/10

$$p_{x_1} [w] \leq \epsilon$$

12/1

$$p(X_1 = x_0 | U = u_0) \geq 2^{-k}$$

on to

12/1)

12/1)

$$2^{-m} > p(X_1 = x_0) \geq p(U = u_0) \cdot p(X_1 = x_0 | U = u_0)$$

5k

$$\geq p(U = u_0) \cdot 2^{-k}$$

$$p(U = u_0) \leq 2^{-(m-k)}$$

12/1

$$p_{w \in W} [w] \leq |U| \cdot 2^{-(m-k)}$$

12/1

$$= 2^{-(m-k-s)}$$

$$\leq \epsilon$$

$$k = m - s - \lg \frac{1}{\epsilon}$$

A, B and $n \times n$

G

של

~~המשפט~~

$$X_1 \in \mathbb{R}^T$$

המשפט

המשפט

B and $A \in \mathbb{R}^{n \times n}$ and $\sigma_0 \in W = \{ \sigma \in \mathbb{R}^n \mid \sigma \geq 0 \}$

המשפט $\epsilon \geq 0$ and σ_0

$$H(X_1 | \sigma_0) \geq k$$

המשפט

$$\left| \Psi_0 \left(X_2 \mid \sigma = \sigma_0 \right) - \Psi_X \left(X_2 \mid \sigma = \sigma_0 \right) \right| \leq \epsilon \quad | \sigma = 1 |$$

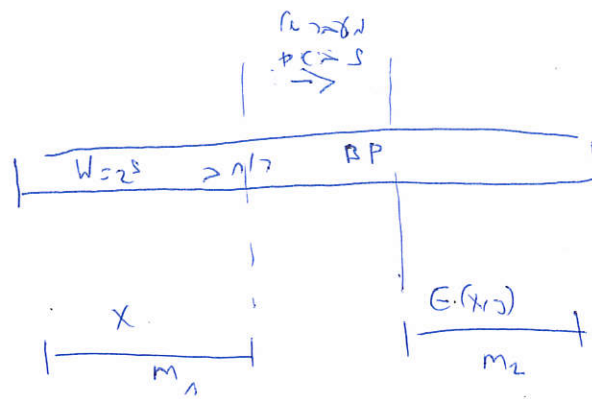
$E(X_1, Y)$

$\epsilon < 1$ and $\sigma_0 \in W$ and B and G

Generated Uniform

and $\epsilon \geq 0$ and $\sigma_0 \in W$ and B and G

$$\text{BP} \quad \int_N \approx 1/c \quad \approx \quad \int' / c$$

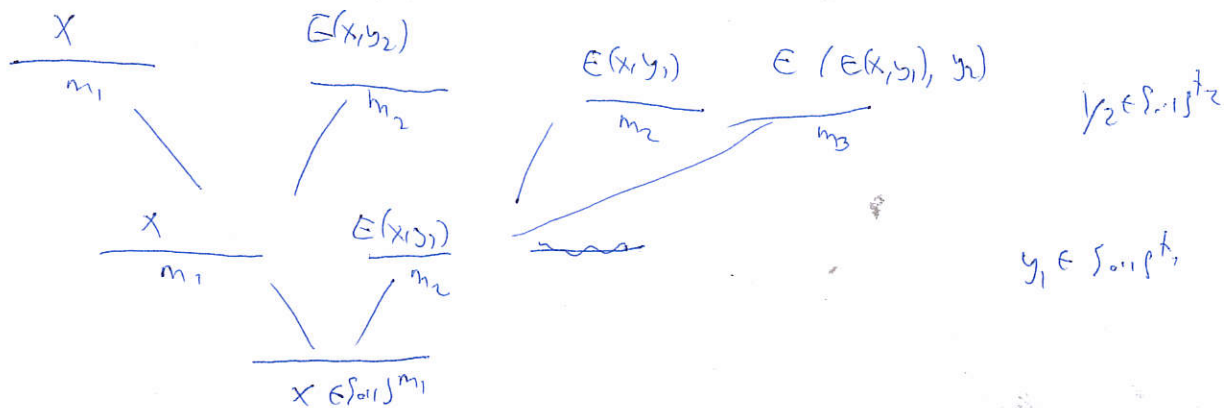


$$y_i \in \{0,1\}^t$$

$$X \in \{0,1\}^{m_1}$$

$$E: \{0,1\}^{m_1} \times \{0,1\}^{t_1} \rightarrow \{0,1\}^{m_2}$$

4 סוגים של נכנס



$$E_1: S_{0.15}^{m_1} \times S_{0.15}^{t_1} \rightarrow S_{0.15}^{m_2}$$

$$E_2: S_{0.15}^{m_2} \times S_{0.15}^{t_2} \rightarrow S_{0.15}^{m_3}$$

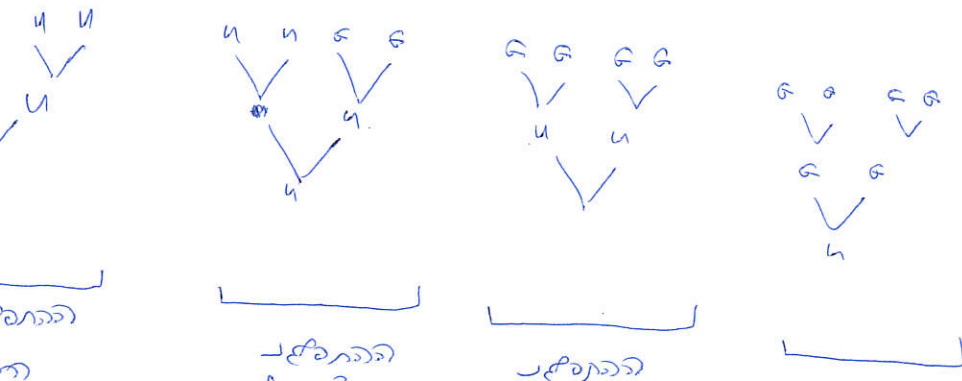
$$(k_1 = m_1 - \log \frac{1}{\epsilon}, \epsilon) \text{ st. ext}$$

$$(k_2 = m_2 - \log \frac{1}{\epsilon}, \epsilon) \text{ st. ext}$$

Hybrid

ROC

ROC



$$[W, m_1 + 2m_2 + m_3, \varepsilon]$$

M

BP

e'

n'J

$$D_3 \quad \vee \quad D_0$$

$$\vdash \neg \neg \neg N \quad 3\varepsilon \quad e$$

$$|M(D_0) - M(D_3)| \geq 3\varepsilon$$

$$0.5\varepsilon \leq 2$$

$$e' \quad j'$$

$$|M(D_{i+1}) - M(D_i)| \geq \frac{\varepsilon}{2^i}$$

$$e' > 0$$

$$|M(D_1) - M(D_0)| \geq \frac{\varepsilon}{2}$$

$$1 \text{ step}$$

Principle A, B present in the

principle of the

principle

$$\begin{array}{l} A \text{ is } X_1 \\ B \text{ is } X_2 \end{array}$$

$$\begin{array}{|c|c|c|} \hline u_1 & u_2 & x_1 \\ \hline \end{array}$$

principle

A

principle of the

principle

$$u_1, u_2, x_1 \text{ is } M \text{ is the principle}$$

(Principle 5) principle of the

$$\begin{array}{|c|c|} \hline \frac{1}{2} & x_1 \\ \hline \end{array}$$

$$\begin{array}{|c|} \hline x_2 \\ \hline \end{array}$$

principle of the

principle of the

principle of the

principle of the

2. קרי


$$x_1, x_2 \text{ } \mu = 0, \hat{\sigma}^2$$
$$Y_2 \in \mathbb{R}^{9 \times 5^T} \quad \rightarrow \quad \omega = 20 \quad B \quad \rightarrow \quad \gamma = 135$$

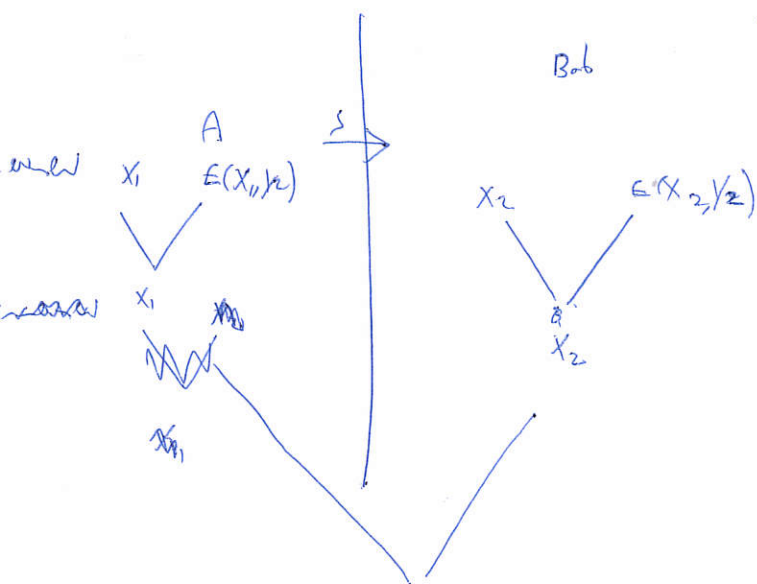
$\frac{P_B}{P_A} = \frac{B}{A}$

Strong - ext

$P_1 \quad P_2 \quad P_3 \quad P_4$

$$M(p_2, D_0)$$

לקח 3



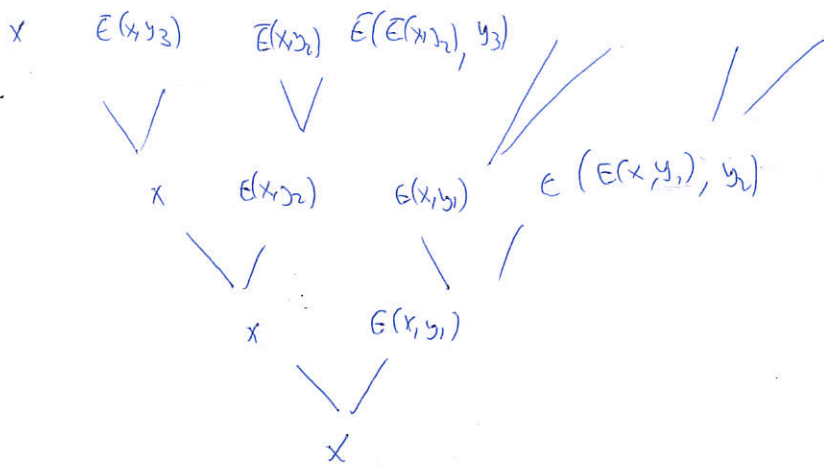
$\frac{1}{2} - \text{מרחק} - \text{מקור}$
 $\text{מרחק} - \text{מקור}$
 $\text{מרחק} - \text{מקור}$
 $A, B \text{ ו } D$

1. $\beta_1 = 1$ ϵ $\beta_2 = 1$ $\beta_3 = 1$

$$P(A \cup B) \leq P(A) + P(B)$$

⑤

! P22 7/10/15



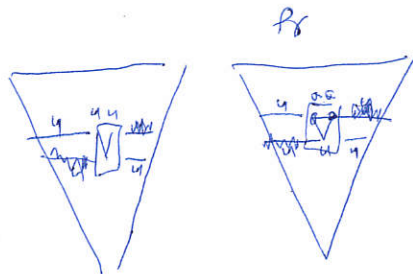
2 prior P_0

$P_0 \quad 2^L = L \quad 2'$

$W=2^L$ $> P_0$ BP $(L-1)E$ PRG 10/10

hybrid PRG 10/10

note: not

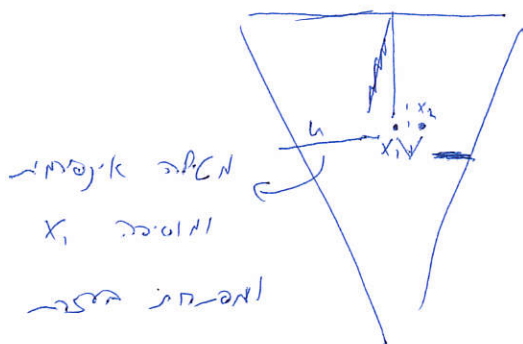


CRV value at 2 - null, not null

for B is A is a point in the plane

the unit disk

A is x_1, y
B is y_2



A
B
x_2 is the
the point in the

the point in the
the point in the
the point in the



y_1, y_2, y_3 is the

$x_1 = y$, the point in the disk - $y_1 = y$
the point in the disk

$y_2 = x_2$ the

the point in the disk - $y_3 = y_2$

x_1, x_2, y the

$x_2 = E(x_2, y)$, $x_1 = x_2, y$

$(0, 1) \geq E$

the point in the disk - $y_1 = y$

the point in the disk - $y_2 = y_1$

! b' > 6, 7, 2, 5

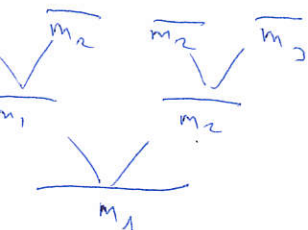
$$[W=2^s, T=2^t, \Sigma=\{0,1\}]$$

BP $-1N \rightarrow 0 + 3/7$

$\overline{m_1}$

$\Sigma_{0,1} s^t$

(k_1, ϵ)



m

$\Sigma_{0,1} s^t$

(k_2, ϵ)

$\Sigma_{0,1} s^t$

(k_1, ϵ)

$$s - \lg \frac{1}{\epsilon}$$

Δ

$$\Delta = O(\lg m_1 + 2 \lg \frac{1}{\epsilon})$$

$$s - \lg \frac{1}{\epsilon}$$

$i \Delta$

$$m_{i+1} = s - \lg \frac{1}{\epsilon}$$

$$\text{BP}, m_{i+1} = m_i = O(s + \lg m_1 + \lg \frac{1}{\epsilon})$$

$$\boxed{m_{i+1} = m_i = O(s + \lg \frac{1}{\epsilon})}$$

$$m_1 = O(\epsilon \cdot (s + \lg \frac{1}{\epsilon}))$$

! 2, 7, 2, 5

BP

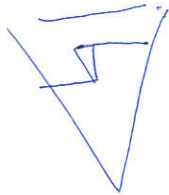
BP

BP $\Rightarrow$ $2^t \cdot \epsilon$

BP/CI

$$m_r > 0 \quad 97 >$$

Hybrid 100% BP NO : 2000 - 2000



ப'யிதோ ப'யி யே ஸி

$$r \propto \frac{1}{\epsilon} \propto \frac{1}{T} \quad \text{b/c} \quad \text{D} \propto r/c$$
[illegible]

$$L = m_1 + y_1 + \dots + y_n$$

Streck 5)

$$= \underbrace{O(\lg^L n)}_{\downarrow} + O(r \cdot \lg\left(\frac{m_i \cdot T}{\varepsilon}\right))$$

$$O(\lg T \cdot (s + \lg T + \lg \frac{1}{\epsilon})) \quad \lg T \cdot (\lg T + \lg \frac{1}{\epsilon} + \lg(\underbrace{m}_{s}))$$

$$= 0 \quad (I_{gT} + I_{gT} + I_{gT})$$

? explicit plan

P- explicit -

$$[x] \quad [y_1] \quad \dots \quad [y_k]$$

e. $\chi^2 \approx$

(b) 122 kg to 1.5 kg)

pass $O(\log m)$

HP

$b \approx 1.0$

$$m = O(g^2 n) \quad \text{b/c}$$

and (so) we need

$$\mathcal{P} = \{c, 1\}^l \Rightarrow \{c, 1\}^n$$

PRG

$$\left[W = 2^S, \underbrace{\overline{m} = n}_{T = \text{poly}(n)}, \Sigma = \{c, 1\} \right]$$

BP

2c)

$$y_t = \{c, 1\}^{t_n}$$

$$\frac{x}{m_1} \quad \frac{E(x, y_1)}{m_2} \quad \frac{E(E(x, y_1), y_2)}{m_2}$$

$$\frac{x}{m_1} \quad \frac{E(x, y_1)}{m_2}$$

$$\frac{x}{m_1} \in \{c, 1\}^m$$

$$\frac{\log T}{n}$$

$$y_i \in \{c, 1\}^{t_i}$$

$$L = m_1 + y_1 + \dots + y_r$$

$$\frac{1}{n^2}$$

$$O(\log T \cdot (s + \log T + \frac{1}{\epsilon}))$$

$$O((\log n)^2)$$

$$E_i: \{c, 1\}^{m_i} \times \{c, 1\}^{y_i} \Rightarrow \{c, 1\}^{m_{i+1}}$$

$$(k_i, \underline{e}) \cdot \text{ext}$$

UTS r -xvaw 2.5 e'
 125 322 $n^{0(15n)}$ 22/11
 $n^{0(15n)}$ 22/11

$$: \frac{(15-1) \text{ 22/11}}{125}$$