

התחלה של פתרון

$$(\mathbb{Z}_N \times \mathbb{Z}_N, +)$$

and show a 'discrete log'

התחלה של פתרון 2

$$D_n$$

shortest vector problem in a lattice

$$S_n$$

$$\chi_2$$

התחלה של פתרון HSP

Pell

התחלה של פתרון

$$x^2 - dy^2 = 1$$

(Pell)

Pell's equation
 הוכחה של פתרון
 קיים תמיד פתרון
 Branner
 100
 של פתרון

התחלה של פתרון

$$x^2 - 5y^2 = 1$$

(9, 4)

12

$20(\sqrt{x} \log x)$

דערם פארן - מאל - Pell גב דיק הא' ו' היטעם - $Z[\sqrt{6}]$

→ BG - BG 2020 Qv HSP

מדינת ישראל, משרד המשפטים, תביעה פלילית
מס' תפ"ד 123456789

$$|G\rangle \triangleq \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |0\rangle$$

I am still
 very happy to

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle$$

לפיכך מוכן לנו להניח את ההקשר
המשמעותי, המכונה "הקשר"
הוא $\mathbb{Z}[X] + H \cong \mathbb{Z}[X]$ כלומר $\mathbb{Z}[X]$

$$\text{coset state} \rightsquigarrow |x+H\rangle = \frac{1}{\sqrt{|G|}\sqrt{|H|}} \sum_{h \in H} |x+h\rangle$$

1. $\Gamma_{\text{FT}} G$ 8N (1) QFT 142 1. $\Gamma_{\text{FT}} G$ 8N (1) QFT 142

$$\frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{h \in H} |x_{x+h}\rangle = \frac{1}{\sqrt{|H||G|}} \sum_{h \in H} \sum_{y \in G} x_{x+h}(y) |y\rangle$$

על פי $\chi_s(t) = \chi_t(s)$ נקבל

$$= \frac{1}{\sqrt{|H||G|}} \sum_{y \in G} \left[\chi_y(x) \underbrace{\sum_{h \in H} \chi_y(h)}_{*} \right] |y\rangle =$$

χ_G הוא קרקסי G וכן χ_H הוא קרקסי H .
 קרקסי H הוא χ_H .
 $\chi_H = 0$ $\Rightarrow \chi_G = 0$

$$\zeta = \frac{\sqrt{|H|}}{\sqrt{|G|}} \sum_{\substack{y \in G: \\ x_y|_H \equiv 1}} x_y(x) |y\rangle$$

χ_y קרקס נקט קדמים הישרים
 (y - יצא) שיהיה C מילוי H בואס אכז
 וקדמיות של C בואס, מובח רף -

$$H \subseteq \text{Ker } \chi_Y \stackrel{\Delta}{=} \{g \in G : \chi_Y(g) = 1\}$$

Ker Ky ה'א ב' חזרה א G (אבא ר'א)
 אבא ר'א חזרה אבא ר'א חזרה אבא ר'א
 15

המשפט 2.1.1. $\chi_1, \dots, \chi_t$ פונקציות קרן, $H = \bigcap_{i=1}^t \text{Ker } \chi_i$ היא תת-קבוצה נורמלית של G .
 הפונקציה χ_{t+1} היא פונקציה קרן על G/H .

$$H = \bigcap_{i=1}^t \text{Ker } \chi_i$$

נניח $K \leq H$ ונבדוק את K' .

$$K = \bigcap_{i=1}^l \text{Ker } \chi_i$$

$$K' = \bigcap_{i=1}^{l+1} \text{Ker } \chi_i$$

כל $K' \leq K$ וכל $K \leq K'$ אז $K = K'$.

$$= K \cap \text{Ker } \chi_{l+1}$$

אם $K' \neq K$ אז $K' \leq K$ או $K \leq K'$.
 נניח $K' \leq K$. אז $K' \leq K \cap \text{Ker } \chi_{l+1} = K'$.
 כלומר $K' \leq K'$ וזה נכון. אבל אם $K \leq K'$ אז $K \leq K' \cap \text{Ker } \chi_{l+1} = K'$.
 כלומר $K \leq K'$ וזה נכון. אבל אם $K' \leq K$ אז $K' \leq K \cap \text{Ker } \chi_{l+1} = K'$.
 כלומר $K' \leq K'$ וזה נכון.

נניח $K' \neq K$

$$P_r[K' \neq K] = P_r[K \leq \text{Ker } \chi_{l+1}]$$

$$: \chi_{l+1}|_H = 1$$

$$= \frac{|H|}{|G|} \cdot \# \{ \chi_y \in \hat{G} \mid K \leq \text{Ker } \chi_{l+1} \}$$

כל $K \leq \text{Ker } \chi_{l+1}$ אם ורק אם $\chi_{l+1}(k) = 1$ לכל $k \in K$.
 כלומר $K \leq \text{Ker } \chi_{l+1}$ אם ורק אם $\chi_{l+1}|_K = 1$.

$$= \frac{|H|}{|G|} \leq \frac{1}{2}$$

$$O(\log |G| + \log \frac{1}{\varepsilon})$$

14 = range μ_{max} , $\Sigma \text{ } \dot{v}_i \cap B_0$, 18

הנני גורם רצף חזק בעם ממשל ארץ ישראל. יש לנו רצף
 של מנהלים מקצועיים בשרות המבחן של הארץ וקווי החזק
 של עובדים עם קהילות אלו עם החזק.

[illegible]

$r'(k) \quad H = (V_H, E_H) \quad \vee \quad G = (V_G, E_G) \quad - \text{ענף}$

$$\pi: V_G \rightarrow V_H$$

... $\rightarrow k \rightarrow \text{wert}$ ($|V_G| = |V_H| = n$ bei 1)

$$\{y, v\} \in E_G \iff \{g\pi(u), g\pi(v)\} \in E_H, \text{ w/B } | \cdot \rangle$$

אם קיים איזומורפיזם בין G ל- H אז $G \cong H$ (אם G ו- H איזומורפיים)

Graph Isomorphism (GI)

הבעיה של גיוס - GI היא האם $G \cong H$.

באופן כללי, GI היא בעיה NP -שלמה: זהו כי $GI \in NP$ ו- $GI \in co-NP$, וכן אם $GI \in NP$ אז $GI \in co-NP$.
ההיכר הוא בעיה קשה מאוד.

אחד מ- GI (ישנה חזקתה פולינומית) היא Graph Automorphism, כלומר האם יש אוטומורפיזם של G שמתחיל ב- G .

$$Aut G = \{ \pi \in S_n : G = \pi G \}$$

↑
הערה: S_n (או S_n)

כלומר.

$$f_G: S_n \rightarrow \{ \text{גרפים} \}$$

$$\pi \mapsto \pi G$$

הערה: f_G

הפונקציה f_G היא איזומורפיזם בין S_n ל- $Aut G$.

$$f_G(\pi) = f_G(\sigma) \iff \pi G = \sigma G$$

$$\iff \pi \sigma^{-1} G = G \iff \pi \sigma^{-1} \in Aut G$$

כלומר, $GI \leq GA$ (אם GI אז GA).