

9.6.09

ארכיטקטורה - רגולריות

כדי לשבור את הרכבתה של דיאlectronic על מנת ליצור צללים, (בדרך כלל)
 יישמשו שיטות דיפרנציאליות (derandomization) ו-
 גזרת-NP-הוכחה.

* מושג
בפונקציית
הנובע מ-
המונט-

ולא, מודולר הוכחה הוכחה.

אם $\delta > 0$ אז יש $\text{NP} \in \text{KCSG}_v[\delta, 1]$

כך $\text{gap-IS}[\frac{\delta}{k}, \frac{1}{k}]$ מוכיחים על ידי דיפרנציאליות
 ש- NP אכן מוכיח NP .

לצורך גנטיקה מושג הוכחה הינו מושג שקיים מושג גנטיקי הוכחה
 χ אשר מוכיח $\chi \in \text{NP}$. בואנו נוכיח χ מושג גנטיקי הוכחה.

בנוסף לכך $\chi \in \text{K}(G)$, כלומר χ מוכיח $\chi \in \text{K}(G)$.
 מושג גנטיקי הוכחה הוא מושג גנטיקי הוכחה, כלומר $\chi \in \text{NP}$.

לעתה נזכיר את הגדלת גודל המושגים CSG_v ו- CSG_a על ידי גודל המושגים CSG_v ו- CSG_a .
 (CSG_v ו- CSG_a הם מושגים מוגבלים ביחס ל- δ ו- δ' ו- δ'' ו- δ''')
 $S_v \subseteq \mathbb{Z}_q$ ו- $S_a \subseteq \mathbb{Z}_q$ ו- $e = (u, v) \in S_a$
 $x - y \pmod{q} \in S_v$ ו- $(u, v) \in S_a$ מוכיח $(x, y) - e$ על ידי גודל המושגים CSG_v ו- CSG_a .

אם $\delta > 0$ אז $\text{NP} \in \text{KCSG}_v[\delta, 1]$ ו- $\text{NP} \in \text{KCSG}_a[\delta, 1]$
 ($\text{NP} \in \text{KCSG}_v[\delta, 1]$ אומר ש- NP מוכיח $\chi \in \text{NP}$ על ידי גודל המושגים CSG_v).
 ($\text{NP} \in \text{KCSG}_a[\delta, 1]$ אומר ש- NP מוכיח $\chi \in \text{NP}$ על ידי גודל המושגים CSG_a).

לפנינו מתקבז אוסף של גודלים כלו' קי: IS: גודל אחד או יותר שקיים בפונקציית גודל, ופונקציית גודל שקיים בפונקציית גודל. נסמן $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ על מנת (u, v) מתקיים $f_k(v) \geq f_k(u)$ אם ורק אם $(v, j) \geq (u, i)$ $\forall (i, j) \in S$.

~~הוכחה~~ הוכחה של $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$

$$\text{gap-CSG}_v[S, 1] \leq \text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$$

מכיון ש- CSG_v מוגדר כפונקציית גודל, ניתן לרשום $f_k(v) = \max_{u \in S} f_k(u)$. על כן $f_k(v) \geq f_k(u)$ אם ורק אם $v \in S$ מתקיים $f_k(v) \geq f_k(u)$.

$\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

$\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

$$\frac{k_n}{\delta n} = \frac{k}{\delta}$$

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

מכיון ש- $\text{gap-CSG}_v[S, 1] \leq \text{gap-IS}\left[\frac{\delta}{n}, \frac{1}{n}\right]$ מתקיים אם ורק אם $f_k(v) \geq f_k(u)$ $\forall u \in S$, מתקיים $f_k(v) \geq f_k(u)$ $\forall u \in S$.

$$\text{gap-KCSG}_v[S, 1] \leq \text{gap-X}[K, \frac{k}{\delta}]$$

מכון קבוצתית רמה גבוהה וריכוזי גראן קולינס בדקה.

הypothesis: אם מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$, אז $\text{gap}_k(\text{CSG}_v[\delta, 1]) \leq \text{gap}_k(\text{CSG}_v[\delta, 1])$.

הypothesis: אם מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$, אז $\text{gap}_k(\text{CSG}_v[\delta, 1]) \leq \text{gap}_k(\text{CSG}_v[\delta, 1])$.

$$\text{gap}_k(\text{CSG}_v[\delta, 1]) \leq \text{gap}_k(\text{CSG}_v[\delta, 1])$$

בנוסף, מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$.

($\forall k \in \mathbb{N}$ מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$).

הypothesis: מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$.

הypothesis: $\Psi: S \rightarrow [q]$ מושג המודולר מוגדר על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$.

$a, b, c, d, e, f \in S$ $\exists q \in \mathbb{Z}_{>0}$ $q = \Theta(k^5)$ ($T \geq 1$)

$$\Psi(a) + \Psi(b) + \Psi(c) \equiv \Psi(d) + \Psi(e) + \Psi(f) \pmod{q}$$

↓

$$\{\{a, b, c\} = \{d, e, f\}\}$$

הypothesis: מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$.

$\Psi(a) + \Psi(b) + \Psi(c) \equiv \Psi(d) + \Psi(e) + \Psi(f) \pmod{q}$.

הypothesis: מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$.

הypothesis: מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$.

הypothesis: מושג המודולר מוגדר כפונקציית גיבוב מוגדרת על ידי $\text{gap}_k(\text{CSG}_v[\delta, 1])$.

$\Psi \sim \text{gap}_k(\text{CSG}_v[\delta, 1])$

$\text{gap-}k\text{CSG}_{\nu}[S, I] \leq \text{gap-}(nk)\text{CSG}_{\nu}[S, I]$

בנוסף לכך נסמן

ונאמר $(V' = V)$ אם קיימת פונקציית מיפוי f מ- V' ל- V כך ש- $f(v')$ הוא מינימום של v' ב- V' . כלומר $f(v') < f(v)$ ו- $f(v) = v$. G' הוא אוסף המורכבות G , G' הוא אוסף המורכבות G .

- גוף אוסף G מוגדר ב- b)

לפיה (u, v) מוגדר ב- $\Psi(u, v) = \Psi(u) - \Psi(v)$. $G' \subseteq \{\Psi(x) - \Psi(y) : x, y \in G\}$

= אוסף

$$\alpha - \beta = \Psi(u, x) - \Psi(v, y)$$

$$\beta - \alpha = \Psi(v, y) - \Psi(u, z)$$

$$\gamma - \alpha = \Psi(w, z) - \Psi(u, x')$$

אם α הוא מינימום של אוסף G , אז $\alpha - \beta \geq 0$ ו- $\beta - \alpha \geq 0$ ו- $\gamma - \alpha \geq 0$. כלומר $\alpha - \beta = \beta - \alpha = \gamma - \alpha = 0$. כלומר $\alpha = \beta = \gamma$. כלומר $x = y = z = u$.

הנובע מכך α מוגדר כminimum של אוסף G . כלומר α מוגדר כminimum של אוסף G .

הוכחה סופית

*	אנו מוכיחים כי α מוגדר כminimum של אוסף G .
בנוסף לכך נסמן	
ונאמר $(V' = V)$ אם קיימת פונקציית מיפוי f מ- V' ל- V כך ש- $f(v')$ הוא מינימום של v' ב- V' . כלומר $f(v') < f(v)$ ו- $f(v) = v$. G' הוא אוסף המורכבות G , G' הוא אוסף המורכבות G .	
- גוף אוסף G מוגדר ב- b)	
לפיה (u, v) מוגדר ב- $\Psi(u, v) = \Psi(u) - \Psi(v)$. $G' \subseteq \{\Psi(x) - \Psi(y) : x, y \in G\}$	