**תורת החישוביות – הרצאה 13 (ואחרונה)**

**תרחיש: מערכת הוכחה חישובית עבור שפה**

*קלט: , טענה:*

– מוכיח

כותב הוכחה ושולח למוודא

אין עליו אילוצי זמן או יעילות – בעל כוח חישוב בלתי מוגבל

- מוודא

מסתכל על ואז מקבל או דוחה

נרצה שהמוודא יהיה יעיל – כלומר ירוץ בזמן פולי׳ (גם אורך ההוכחה ש- יכול לקבל חסום פולי׳)

שלמות: אם יש הוכחה ״משכנעת״

נאותות: אם שום הוכחה לא משכנעת

הבחנה: השפות שיש עבורן מערכת הוכחה כנ״ל (כלומר זוהי דרך אלטרנטיבית להגדרת )

הוכחה:

- לכל , יהי היחס המתאים. על קלט ישלח כך ש- ו- יוודא (יקבל/ידחה בהתאמה)

- תהי עם מערכת הוכחה כנ״ל ונראה כי ע״י יחס מתאים:

**מערכת הוכחה אינטראקטיבית עבור**

הרחבה 1: נאפשר אינטראקציה בין (במודל הקודם נבדוק הוכחה ״כתובה בספר״ ובמודל הנוכחי נאפשר ״שיח״ על ההוכחה)

הרחבה 2: הסתברותי יעיל (במודל הקודם היה יעיל דטרמיניסטית, ובמודל הנוכחי שלמות ונאותות לא מושלמות)

טריוויאלי: (מקרה פרטי של הוכחות מהמודל הקודם)

משפט (ללא הוכחה):

**דוגמה:**

הגדרה: 2 גרפים יקראו איזומורפיים ונסמן (זהו יחס שקילות) אם קיימת פונק׳  *חח״ע ועל המקיימת:*

*הגדרה: השפה :*

בשנים האחרונות גילו כי ניתן להכריע את השפה בסיבוכיות

הגדרה: השפה *:*

**מערכת הוכחה עבור**

אנלוגיה: לתת לחבר לטעום יינות ולבדוק האם הוא יודע להבחין ביניהם

: בוחר באקראי ופרמוטציה מקרית

מחשב

שולח את ל-

: מוצא כך ש- ושולח ל-

: מקבל אם ורק אם

הוכחה (לא פורמלית):

הסתברותי יעיל ( לא בהכרח יעיל)

שלמות: אם ורק לו ולכן ש- מחשב ואז יקבל

נאותות: אם איזומורפי לשניהם הסיכוי ש- (ואז יקבל) הוא .

ע״י חזרה על התהליך פעמים ניתן להוריד את השגיאה ל-.

**הוכחות באפס מידע**

הוכחה באפס-מידע עבור :

: בוחר באקראי פרמוטציה ושולח את

: בוחר באקראי ושולח ל-

: שולח פרמוטציה המראה

: בודק ש- כזו ומקבל אם ורק ם מתקיים

מתקיים (לא פורמלי):

יעיל

שלמות: אם אז איזומורפי לשניהם ו- תמיד מקבל

נאותות: אם אז איזומורפי לכל היותר לאחד מהם ולכן בסיכוי ידחה

אפס מידע: במהלך הפרוטוקול רואה ערבוב מקרי של , ואת זה הוא יכול לייצר בעצמו

**דוגמה: מטבעות קריפטוגרפים /**

ניהול המטבע

ייצור המטבעות / כרייה

חידה חישובית /

מטבע נוצר כשמוצאים המקיים

בחירת :

קלה (לא מדי)

חישוב הפונקציה קשה מאוד

טענה: אם לא קיימת כזו

בעיית החיפוש חישוב

**התמודדות עם בעיות חישוב ״קשות״**

1. הרחבת מרחב הפלט של הבעיה

* קירובים (כפליים, חיבוריים, קומבינציות של השניים)

2. צמצום מרחב הקלט של הבעיה (הקושי נובע בד״כ מהמקרה הרע)

* בעיות הבטחה: הקלט מתוך

דוגמה: : בגרף דו-צדדי פולי׳, בגרף מישורי בסיבוכיות

* סיבוכיות פרמטרית:

דוגמה: : בזמן פולי׳

3. גישות הסתברותיות

* סיבוכיות ממוצעת (פילוג על הקלט) – אלג׳ לאס ווגאס ואלג׳ מונטה-קרלו
* אלג׳ הסתברותיים (אלג׳ לכל קלט. הסתברות על ריצות האלג׳)

4. אלג׳ לא פולינומים משופרים

* דוגמה: טריוויאלי - . ידוע אלג׳ שרץ בסיבוכיות

5. היוריסטיקות

* למידת מכונה: כאשר לא טריוויאלית החישוב קשה