פרויקט בנושאים מתקדמים 7:

קלט: (לשניהם) ו- שזה ה-witness (רק ה-prover). .

המטרה: לשכנע את ה-verifier ש-.

סיבוכיות: . מניחים ש- .

* סיבוכיות תקשורת:
* סיבוכיות שאילתות:
* סיבוכיות מוודא:
* סיבוכיות מוכיח:

שגיאת soundness: negl.

* הוכחה אינטראקטיבית לשפה בעזרת . (זה ).
* נשלח את הקידוד הטנזורי של . כלומר, נשתמש ב- כאשר ונשלח .

נשים לב כי לפי ההגדרה של , הוא כאשר .

ל- יש בעיקרון 3 אפשרויות: *פונקציית הזהות/ קוד / להכפיל עם מטריצה רנדומלית.*

* *אחרי שהמוודא מקבל הוא מריץ . איך? בוחרים שורה, עמודה וטור אקראיים (פשוט אחד בכל מימד) ובודקים ששלושתם מילות קוד.*
* *מריצים את (ככה מוכיחים ש- בשפה בעזרת ) – בשכבה האחרונה המוודא צריך לעשות שאילתות ל- כדי לוודא את המוכיח. אבל – המוודא עושה שאילות ל- של ולא ל- עצמו.*
* *עושים כדי להוכיח ש- כש- מסמן אינדקס מסוים ו- זה הערך שאנחנו מצפים שיהיה שם. (זה בעצם השאילתות של המוודא בשכבה האחרונה של ה-). איך הולך ה-?* ***(אסף?)***
* *איפשהו בפרוטוקול של ה- צריך להשתמש ב- של – איפה ואיך?*
* *איך עושים של (במקרה הדו-מימדי)? בהינתן נקודה שרוצים להבין מה הערך שלה, בודקים שהשורה היא מילת קוד, בוחרים נקודה אקראית ובודקים שהעמודה היא מילת קוד.*

*הערה: רון אמר שהבדיקה הזאת יותר חלשה מ- – זה רק בודק שהתו תקין ולא נותן לנו למצוא את התו התקין עצמו בהסתברות גבוהה – אבל זה מספיק לנו.*

*ואיך ממשים?*

* *מצאנו:* Sumcheck protocol for Multilinear polynomials and GKR Function

<https://github.com/tsunrise/sumcheck_multilinear>

* *מצאנו:* Reed Solomon

<https://github.com/tomerfiliba/reedsolomon>

*שלב #1: נגדיר ו-.*

*שלב #2: ליצור* class *של* TensorCode *שמקבל בבנאי קוד ויש לו את המתודות:*

* *– בהינתן מילה מחזיר את .*
* *– בהינתן מילת קוד מחזיר כך ש- או אם אין שכזה.*
* *– בהינתן מילת קוד מחזיר אם קיים כך ש- מספיק קרוב ל- ו- אחרת*

*(הגדרה יותר מדויקת ל"מספיק קרוב"? הוא בוחר שורה, עמודה וטור אקראי ובודק שהם מילות קוד תקינות)*

* *– בהינתן מילת קוד ואינדקס מחזיר אם הבדיקה שלו הצליחה  
  (הוא בודק את ההרחבה לבדיקה הדו-מימדית של ה-).*

*שלב #3: ממשים ששולח ל- את*

*שלב #4: ה- מריץ .*

*שלב #5: מריצים עד שלב אחד לפני האחרון.*

*שלב #6: מריצים את הפרוטוקול האינטראקטיבי של המטריצות (מה?).*

*הערה: נרצה לממש ו- משלנו שמשתמשים בקוד של ה- שמצאנו ואחרי זה מריצים את ה-.  
עולה השאלה – איך אנחנו רוצים לממש אותם?*