<u>שם הקורס</u>: מערכות הוכחה מתקדמות
<u>מספר הקורס</u>: 236607
<u>מרצה</u>: רון רוטבלום

<u>דרישות קדם:</u> תורת החישוביות 236343

<u>תיאור הקורס</u>:

האם ניתן לוודא נכונות של חישוב מבלי לבצע אותו מחדש? האם ניתן לוודא הוכחה ע״י קריאה של מספר קטנטן של ביטים מתוכה? האם אפשר להוכיח נכונות מבלי לחשוף מעבר לכך שהטענה נכונה?

בקורס זה נעסוק במערכות הוכחה מתקדמות פרוטוקולים מתקדמים וניתן תשובה חיובית לשאלות הללו. בפרט נדון ב:

1. הוכחות אינטראקטיביות, שהן הכללה של מערכת הוכחה NP שבה מאפשרים למוודא אינטראקציה עם המוכיח (תוך שימוש באקראיות). נראה את הכח הרב שיש להוכחות כאלה.

2. הוכחות אפס מידע, שבהן המוודא לא לומד דבר פרט לנכונות הטענה.

3. הוכחות PCP, שבהן מספיק למוודא לקרוא ביטים בודדים מההוכחה כדי להשתכנע בנכונותה.

4. מערכות הוכחה בעלות יעילות כפולה, שיכולות לשמש למיקור חוץ של חישובים והינן בחזית המחקר העכשווי בתחום.

דרישות הקורס: כ-3/4 תרגילי בית ומבחן **קל**.