

**שם הקורס:** מערכות הוכחה מתקדמות

**מספר הקורס:** 236601

**מרצה:** ד"ר רון רוטבלום

**דרישות קדם:** תורת החישוביות 236343

**תיאור הקורס:**

מערכות הוכחה הינן בליבה של התאוריה של מדעי המחשב. למשל שאלת  $P$  vs  $NP$  עוסקת בשאלה האם כל מערכת הוכחה  $NP$  ניתן לסמלץ בזמן פולינומיאלי.

בקורס זה נעסוק במערכות הוכחה מתקדמות כמו:

1. הוכחות אינראקטיביות, שהן הכללה של מערכת הוכחה  $NP$  שבה מאפשרים למוודא אינטראקציה עם המוכיח (תוך שימוש באקראיות).
2. הוכחות אפס מידע, שבהן המוודא לא לומד דבר פרט לנכונות התוצאה.
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: 2-3 תרגילי בית ועבודה מסכמת. עבודה המסכמת תתבסס על קריאת מאמר(ים) בתחום, סיכום התוצאות, סקר ספרות והרחבת התוצאות או הצגת פישוט שלהן. הנחיות מפורטות תינתנה בהמשך לנרשמים לקורס.