דו"ח התקדמות סדנה באימות פורמלי - פרויקט Verifier

מנחים: פרופ' שרון שוהם בוכבינדר, מר נטע אלעד

חברי הצוות: רועי קליגר וגיא חדד

תאריך: 15/07/2024

סקירה כללית של הפרויקט

הפרויקט שלנו נועד לפתח כלי אימות פורמלי בפייתון עבור שלשות Hoare עם שפת while (כפי שראינו בכיתה, זו שפה פשוטה אשר תומכת בפקודות הבסיסיות skip, assign, if, seq, while). הכלי שלנו מפרש את שורות התוכנית כשלשות Hoare, מתרגם אותם לנוסחאות לוגיות מסדר ראשון, ופותר אותם באמצעות ה-z3-solver.

תהליך העבודה עד כה

פתחנו repo ב-github:
https://github.com/RoyKliger/verifier_workshop_project.git.

בקובץ commands.py בנינו מחלקות נפרדות לכל סוג פקודה (skip, assign, if, seq, while) ולכל מחלקה כתבנו פונקציה verify אשר מחזירה את ה-verification conditions המתאימים, על פי הטבלה שראינו בשיעורים הראשונים.

בקובץ verifier.py, כתבנו את הפונקציה solve אשר בהינתן תוכנית (סדרת פעולות), תנאי התחלה, תנאי סוף, והערות נוספות של המשתמש בין שורות התוכנית, מחזירה האם הקוד עונה על התנאים הללו.
הפונקציה עוברת על התוכנית השלמה ומתרגמת אותה באופן רקורסיבי לנוסחאות לוגיות מסדר ראשון עם התנאים המתאימים, ומחזירה האם התוכנית, יחד עם ה-precondition, ה-postcondition וה-annotations הנתונים על ידי המשתמש, תקפה.

מחשבות להמשך

הרחבת סט הפקודות הנתמכות כגון לולאות for, מערכים ופונקציות;

בניית parser לפירוש התוכנית ולשמירת הפקודות שבה;

חיסכון בכמות ההערות שהמשתמש צריך לספק, ואף שינוי בשיטת תרגום התוכנית לנוסחאות. אנחנו מתלבטים בין שימוש ב-wlp לבין השיטה השלישית שראינו עם שימוש בשכפול משתנים;

בניית ממשק ידידותי למשתמש, כדי שיהיה נוח להקליד את התוכנית כמו גם את ההערות ישירות לתוך הממשק;

התמודדות עם קלטים גדולים ואופטימיזציה.