

מרצים: דר' ויזל יקיר ודר' יצחקי שחר

דרישות קדם:

לוגיקה ומבוא לאימות תוכנה או ניסיון בתחום (באישור המרצים).

סילבוס:

בקורס זה נלמד איך להוכיח נכונות של תכניות באמצעות אלגוריתמים לאימות פורמלי. הקורס יכלול פן תיאורטי ומעשי. בפן התיאורטי נלמד על אלגוריתמי ספיקות ללוגיקה פסוקית ולוגיקה מסדר ראשון (SAT and SMT), על תרגום של תוכניות ומודלי חומר ללוגיקה ועל אלגוריתמי הוכחה מבוססי SAT ו-SMT שפועלים על הייצוג הלוגי של התוכנית ומוכיחים או מפריכים את נכונותה. בחלק המעשי נשתמש בכלים לאימות פורמלי על מנת ליישם את הנושאים התיאורטיים שילמדו במהלך הסמסטר. נציין כי ביצוע הפרויקט יחל כבר בשבועות הראשונים כאשר תהיינה תת-משימות אותן נבצע במהלך הסמסטר כחלק מן הפרויקט. כחלק ממטרות הלמידה, הסטודנטים יחלקו את התוכנה למודולים, יכתבו מפרט לכל מודול, יבצעו אימות פורמלי של כל מודול אל מול המפרט שלו, ולבסוף יודאו ששילוב המפרטים מספק את דרישות הנכונות של המערכת. נושאים שיכוסו במסגרת הקורס:

1. אלגוריתמי SAT ו-SMT, מערכת הוכחה מסוג רזולוציה וכללי היסק.
2. בדיקת מודל חסומה ואינדוקציה.
3. אימות תוכנה: מעבר מקוד ללוגיקה על ידי שימוש ב-Constrained Horn Clauses.
4. אלגוריתמי הוכחה מבוססי SAT/SMT (על ידי שימוש באינטרפולציה והכללה אינדוקטיבית).
5. ניתוח בשיטת Abstract Interpretation
6. ניתוח מצביעים ו-Shape Analysis
7. אימות מודולרי

דרישות הקורס:

- תרגיל בית תיאורטי
- פרויקט
- אין בחינה סופית