אוניברסיטת בן-גוריון בנגב
הפקולטה למדעי הטבע - המחלקה למדעי המחשב
סמסטר א' תשע"א

סילבוס קורס

שם הקורס: נושאים מתקדמים בפרטיות ולמידה חישובית.

שם קורס באנגלית: Advanced topics in privacy and computational learning.

מס' קורס: 202-2-5751

סוג קורס: בחירה

נק"ז: 4

מרצי הקורס: דר' קובי נסים, דר' אריה קנטורוביץ.

דרישות קדם : זהו קורס מתקדם המיועד לתלמידי שנה ג' במדעי המחשב, תלמידי שנה ד'

בהנדסת תכנה ולמוסמכים.

דרישת קדם לתלמידי תואר ראשון: ממוצע 75 ומעלה.

מטרת ונושא הקורס:

לתחומי המחקר בפרטיות ובלמידה חישובית מוטיבציות שונות מאד, ובמבט ראשון נראה שאין קשר ביניהם. למרות זאת, המחקר של השנים האחרונות חשף נקודות מפגש מרובות בין השניים ובהן קונספטים ושיטות שהוצגו באחד התחומים משמשים בתחום השני. אנו נציג את ההתפתחויות המחקריות הללו.

The topics of privacy and of computational learning have very different motivations, and seem unrelated at first sight. Yet, recent research has uncovered many interaction points between the two, where concepts and tools introduced in one area turn to be useful in the other. We will present these new advances.

נושאי ההרצאות

רשימת נושאים טנטטיבית:

למידה:
- למידת PAC, התער של אוקם, סיבוכיות הדגימה ומימד VC.
- אלגוריתמי למידה למשימות ספציפיות: PARITY ועוד.
- למידה נאותה ולא נאותה (proper ו-improper).
- למידה במודל השאילתות הסטטיסטיות (SQ).

- אי אפשרות למידה של PARITY במודל SQ.
- Boosting : קלאסי, חלק.
- למידה של פונקציות סוב-מודולריות.
- Fat Shattering Dimension.

<u>פרטיות:</u>
- מתקפות על פרטיות. אי-פרטיות בוטה.
- פרטיות דיפרנציאלית ותכונותיה.
- בניה של אנליזות המקיימות פרטיות דיפרנציאלית.
- למידה פרטית.
- סניטיזציה של מידע.
- הסיבוכיות של למידה דיפרנציאלית.

A tentative topic list:

<u>Learning:</u>
- PAC learning, Occam's razor, sample complexity and the VC dimension
- Learning algorithms for specific tasks: PARITY, ...
- Proper vs. improper learning.
- Learning with statistical queries (SQ).
- Impossibility of learning PARITY with SQ.
- Boosting: classic, smooth
- Learning sub-modular functions.
- Fat Shattering Dimension.

<u>Privacy:</u>
- Attacks on privacy, blatant non-privacy.
- Differential Privacy and its properties.
- Constructing differentially private analyses.
- Private learning.
- Data Sanitization.
- The complexity of Differential Privacy.

<u>דרישות הקורס:</u>

הגשת תרגילים ופרויקט

<u>מרכיבי ציון הקורס:</u>

הגשת תרגילים : 50% פרויקט : 50%

ספרות הקורס:

Introduction to Computational Learning Theory, Kearns and Vazirani, MIT press, 1997