אוניברסיטת בן-גוריון בנגב
הפקולטה למדעי הטבע - המחלקה למדעי המחשב
סמסטר א׳ תשע״א

סילבוס קורס

שם הקורס: מושגי יסוד בפרטיות ולמידה חישובית.

שם קורס באנגלית: Elements of privacy and computational learning.

מס׳ קורס: 202-1-5711

סוג קורס: בחירה

נק״ז: 2

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

דרישות קדם: הקורס מיועד לתלמידי שנה ג׳ במדעי המחשב, ותלמידי שנה ד׳ בהנדסת תכנה.

דרישת קדם: ממוצע 75 ומעלה. ההרשמה בתיאום עם אחד המרצים.

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.

<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.

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

<u>דרישות הקורס:</u>

תרגילי בית.

הערה : הרצאות הקורס חופפות את אלו של "נושאים <u>מתקדמים</u> בפרטיות ולמידה חישובית"

(4 שעות שבועיות). התלמידים ידרשו להגיש את תרגילי הבית שינתנו ב- "נושאים

<u>מתקדמים</u>", אולם יהיו פטורים ממספר קטן של הרצאות ומביצוע הפרויקט.

מרכיבי ציון הקורס:

100% : הגשת תרגילים.

ספרות הקורס:

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