

דברים שאמרתי בטקס הענקת פרס ישראל

[תוספת ספונטנית: מראש, לא התכוונתי לומר שום דבר פוליטי, אבל הרגשתי מחויב לענות בקצרה לדבריו של מעניק הפרס, דוד פלבר, אשר נשא נאום שהינו – לדעתי – לא פחות פוליטי מן התגובה שלי, למרות שרוב הציבור עשוי לראות את נאומו של פלבר כלא פוליטי. נאומו של פלבר, היה מבוסס על ההיסטוגרפיה הציפונית, אשר (ככל היסטוגרפיה של תנועה לאומית) משלבת מיתוסים מכוננים עם עובדות היסטוריות. בפרט, ההיסטוגרפיה הזו לוקה בעיוורון למחיר ששילם עם אחר על "התקומה של עם ישראל בארצו". בתגובתי אמרתי "הייתי רוצה להוסיף משהו טיפה פוליטי. הסיפור הוא לא שלם בלי לציין את המחיר ששילם עם אחר על התקומה שלנו והמחויבות המוסרית שלנו לנסות כמיטב יכולתנו לנסות לפצות ולא להמשיך לדכא את העם האחר, אנחנו כמובן עושים את ההיפך."]]

אני עומד כאן כנציג של תחום המחקר הנקרא "תאוריה של מדעי המחשב" ונראה לי שאני נציג מובהק יותר שלו מאשר זוכים קודמים של פרס זה, משום שבניגוד להם לא הייתה לי כל תרומה ישירה מחוץ לתחום זה. מבחינה זו, הפרס הנוכחי הוא יום חג לתחום המחקר שלי, ודאי ככל שמדובר בישראל.

ההשפעות המהפכניות של טכנולוגית המחשבים על חיי הפרט והחברה בת-ימינו מפעימה ודומיננטית באופן שגורם לציבור הרחב לזהות את מדעי המחשב עם הטכנולוגיה הזו ולפספס את התוכן האינטלקטואלי של מדעי המחשב. ברצוני לדבר טיפה על תוכן זה.

אנחנו חוקרים את מושג "החישוב היעיל" כאשר **חישוב** הוא כל תהליך שינוי הכפוף לחוקים פשוטים (ז"א כמעט כל רכיב של תמונת העולם שלנו הוא חישוב מבחינתי), ו**יעילות** יכולה להתייחס לשורה של מדדים של שימוש במשאבים (בעיקר זמן ומקום).

דוגמה ראשונה: הכפלה של מספרים (בייצוג עשרוני). בבית הספר היסודי, למדנו שיטה ("אלגוריתם") לחישוב המכפלה של מספרים רבי-ספרות: מכפילים את המספר הראשון בספרה הימנית ביותר של המספר השני ורושמים את התוצאה, אח"כ מכפילים את המספר הראשון בספרה השנייה של המספר השני ורושמים את התוצאה בהזזה של ספרה אחת, וכך הלאה. כמה פעולות (של הכפלת ספרה בספרה) אנחנו מבצעים כאשר אנו מכפילים שני מספרים בני N ספרות? (תשובה: סדר גודל של N בריבוע.) **האם ניתן למצוא את המכפלה ע"י ביצוע הרבה פחות פעולות?** (תשובה: כן! כמעט בסדר גודל של N, שזה סדר הגודל הדרוש לחיבור מספרים כאלו!)

הדוגמה הנ"ל חושפת את הפער שבין שיטות ידועות (אלגוריתמים ידועים) לפתרון בעיות לבין השיטות היעילות ביותר האפשריות. המחקר נע בין מציאת שיטות יעילות יותר לבין הצגת עדויות לכך ששיטות יעילות יותר לביצוע המשימה אינן קיימות. למעשה, מטרתנו לאפיין את רמת היעילות שניתן להגיע אליה במשימות שונות. בנוסף לכך, מתגלות משימות ובעיות חישוביות חדשות שעולות מתוך הבנה של יישומים אפשריים ומתוך ההיגיון הפנימי של הבנת התחום. נושא זה יעלה בסוף הדוגמה הבאה.

דוגמה שנייה: בהינתן תהליך חישוב יעיל (למשל חישוב מכפלה של שני מספרים), האם ניתן למצוא תהליך יעיל אשר "הופך" אותו (ז"א: הולך מתוצרי התהליך הראשון לנתונים ההתחלתיים, למשל מן המכפלה לזוג מספרים (שווי-אורך) אשר מכפלתם היא אותה מכפלה)? יש מקרים בהם התשובה חיובית (למשל חיבור של שני מספרים רבי-ספרות), אך נראה שיש מקרים בהם התשובה שלילית (לדוגמה: הכפלה של מספרים כאלו). הדוגמאות השליליות נקראות **פונקציות חד-כיווניות** ויש להם שימושים רבים בקריפטוגרפיה ("תורת ההצפנה [לסודיות]").

הקריפטוגרפיה מזוהה עם בניה של שיטות לתקשורת סודית, תוך שימוש במערכות של הצפנה ופענוח של הודעות כאשר הפענוח מבוסס על מידע סודי הנקרא **מפתח**. אלא שהקריפטוגרפיה עוסקת גם בבניה של שיטות להתחייבות וחתימה דיגיטאלית על מסמכים, וגם שם המתחייב/חותם משתמש במידע סודי הנקרא מפתח. הצפנה סודית וחתימה דיגיטאלית הם שני יישומים מרכזיים שבהם עוסקת הקריפטוגרפיה, אבל היא לא מתמצה ביישומים אלו.

באופן כללי, ניתן לזהות את הקריפטוגרפיה כתחום שעוסק בבניה של מערכות יעילות לחישוב רב-משתתפים אשר קשה לחלק מן המשתתפים להסיט אותן מהפעולה הרצויה. במקרה של הצפנה מדובר במשלוח של הודעה בין שותפי-סוד כך שאדם שלישי אשר רואה את התקשורת אינו מבין את תוכנה (כאשר הבנת התוכן על ידי אדם שאינו שותף-סוד מוגדרת כהסטה של המערכת מפעולתה הרצויה). במקרה של חתימות מדובר בכך שרק המתחייב יכול ייצר התחייבויות הנושאות את חתימתו. במקרה הכללי מדובר בחישוב רב-משתתפים בטוח של כל משימה שניתן לבצע כאשר כל המשתתפים הגונים לחלוטין.

אחת מעבודותי מראה כי כל משימה רבת-משתתפים אשר ניתנת לביצוע כאשר כל הצדדים הגונים, ניתנת לביצוע גם כאשר רק רובם הגונים. במילים אחרות, עבודה זו מראה שניתן לממש ישות דמונית שהגונה לחלוטין ברשת תקשורת בה רק רוב המשתתפים הגונים ואילו השאר מנסים לחבל בפעילות בכל דרך אפשרית.

[השאר לא נאמר כדי לא לבחון את סבלנות הנוכחים...]

כמובן שלעבודה זו, כמו לעבודות אחרות בתחום הקריפטוגרפיה יש יישומים רבים. דברים אלו תקפים גם לגבי עבודות בתתי-תחומים אחרים של התיאוריה של מדעי המחשב. בדרך כלל, היישום המעשי של עבודות תאורטיות דורש התאמות רבות, ולעתים ראוי לומר שהוא רק מקבל השראה מהרעיונות שבבסיס העבודה התיאורטית.

אני רואה את תרומותי העיקריות לחינוך בשני מישורים. מישור אחד הוא בהבהרה וארגון של הידע המדעי הקיים. המאמרים המדעיים נכתבים לרוב באופן הפונה למעשה רק למומחים בתחום, אשר יודעים את הרקע לעבודה ואיך המאמר הנוכחי משתלב בה. סגנון זה מקשה מאוד על כניסה של חוקרים חדשים לתחום, והדרך להקל עליהם היא בכתיבה של סקירות וספרי לימוד, אשר מועילים גם למומחים בתחום משום שהם כוללים אינטגרציה וניסוח מחודש אשר קשה לבצע אותם במאמרים רגילים. מישור שני הוא של דו-שיח ישיר עם סטודנטים אשר מתייחס לאי-ההבנות השונות שלהם, שיכולות להיות טכניות ונקודתיות או קונספטואליות וכלליות. בנוסף, אני מקדיש תשומת לב לקושי הנפשי הכרוך בתסכולים הרבים העולים בעת ביצוע לימוד ומחקר. לדעתי, דיבור גלוי על הקשיים הללו וחיפוש הדדי של דרכי התמודדות הוא דבר חשוב ביותר.