# הוכחת האליבי המוצק

## לתחום מחקרה של הפרופ' שפי גולדווסר – תורת הסיבוכיות והוכחות אפס מידע – השלכות על בטיחות השימוש בערוצי מידע, ומכאן על תחומים רבים בחיי היום־יום. למתמטיקה הגיעה די באקראי, היא מספרת, ולמרות מהלכה המהיר של הקריירה שלה בארצות הברית החליטה לשוב לארץ. כתבה ראשונה בסדרה שתציג דיוקנאות של חוקרים בולטים מהדור החדש בישראל

מאת יוסי מלמן

לא, זה לא קרה לפרופסור שפי גולדווסר באמבטיה, כמו לארכימדס. היא אף מתקשה לשחזר את הרגע שבו התברר לה כי היא שותפה לתגלית מדעית. לאביתו של דבר, היא אומרת, אל הגילוי בתחום הקרוי "הוכחת אפס מידע" הגיעה בתהליך מבושך של עבודת צוות. שותפיה לגילוי הם שניים. הפרופסור האיטלקי סילביו מיקאלי מהמכון הטכנולוגי במסצ'וסטס (אמ־איי־טי), שליד בוסטון, והקנדי צ'ארלס ראקוף מאוניברסיטת טורונטו.

שפי גולדווסר, בת שלושים ושש, היא פרופסור במחלקת מדעי המחשב ומתמטיקה שימושית במכון ויצמן ברחובות ובאמ־איי־טי התחום הרחב של מחקרה נקרא "סיבוכיות". "זהו ענף מתמטי שחוקר מהו כוחו של המחשב ומהן מגבלותיו", היא מסבירה. "יש מספר פעולות מינימלי שהמחשב חייב לבצע כדי לפתור בעיה כלשהי שהוצגה לו. מספר פעולות זה נקרא סיבוכיות הבעיה, והוא אינו תלוי בסוג המחשב שמשתמשים בו, בין שזה מחשב־על ובין שזה מחשב ביתי. שתי שאלות בסיסיות נשאלות במחקר כשמוצגת למחשב בעיה לפתרון: א. מהי סיבוכיות הבעיה; וב. כיצד לפתח אלגוריתם, או תוכנית מחשב שפותרת את הבעיה במספר הפעולות המינימלי האפשרי. אם מצאת תוכנית מחשב שדורשת מספר פעולות השווה לסיבוכיות הבעיה, כלומר, מספר הפעולות המינימלי הדרוש – מצאת תוכנית אופטימלית לבעיה. ואין פתרון מהיר ממנה".

כדי להסביר מהו אלגוריתם נדרשת גולדווסר לשמפו לשיער. "אלגוריתם הוא מעין סדרת הוראות מדויקות לביצוע, כדי לפתור את הבעיה. לעתים, בקורס בסיסי במדעי המחשב, מסבירים את מושג האלגוריתם בעזרת הדוגמה של שמפו לשערות. על כל מכל שמפו יש הנחיות כיצד לחפוף את השיער אתה לוקח מהחומר, חופף, שוטף, ומתבקש לחזור על הפעולה. זהו אלגוריתם לחפיפת שיער. במקרה זה – האלגוריתם מאוד בעייתי", היא מוסיפה בחיוך, "כי כהוראות לא נאמר מתי להפסיק אילו היה מחשב מבצע את הוראות החפיפה כלשונן, הוא היה נשאר באמבטיה לזמן ארוך".

מהשמפו עוברת הפרופ' גולדווסר לתיאורון ויאוכרת את משחקו הייחודי של השחקן הבריטי דרק ג'קובי, כדי להסביר תת־ענף של הסיבוכיות שבו מתמקדת עבודתה. זו הקריפטולוגיה, או תורת הצפנים. לפני שנים אחדות הועלה על במות לונדון וניו יורק, בכיכובו של ג'קובי, המחזה "שוברים את הצופן", שהוצג אחר כך בלבוש עברי גם בישראל. המחזה עסק בחייו הטכובכים של המתמטיקאי האנגלי אלן טורינג, שפיצח את ה"אניגמה", מכונת הצופן הגרמנית שבירת הצופן המדאי איפשרה למדריין הבריטי לקלוט ולפענח את התשדורות הגרמניות במלחמת העולם השנייה. כיום מפתחים מתמטיקאים בכל העולם צפנים משוכללים הרבה יותר, שבהם נעזרים לא רק לצורכי צבא ומודיעין אלא גם בעולם הבנקאות, התעשייה והתקשורת בכללותה.

"המתכנן הגרמני של מכונת הצופן", מדגישה גולדווסר, "הניח וידע שיהיה אפשר לשבור את הצופן שלו. זו היתה ונשארה שאלה של תחכום. זה שנים שוקדים המתמטיקאים על פיתוח צפנים שיהיה ניתן להוכיח ביחס אליהם כי פיצוחם יימשך, גם בהמשך המהיר, זמן רב כל כך, שמבחינה מעשית לא יהיה אפשר לשבור אותם. כלומר, סיבוכיות פיצוח הצופן תהיה גדולה יותר ממספר החלקיקים ביקום, למשל. אין ברשותנו זמן כזה, ולכן מבחינתנו צופן כזה הוא בלתי שביר".

**"במערכת הוכחה הסתברותית ואינטראקטיווית הוכחות נבדקות בתהליך של שאלות ותשובות – בין מוכיח הטענה לבודק נכונותה. הבודק שואל שאלות שנבחרות באקראי, ואם המוכיח מסוגל לספק לכולן תשובות, הבודק יסכים כי הטענה תקפה. הדבר דומה לחקירת משטרה שבה מנסה החוקר למצוא פגמים באליבי של החשוד בפשע"**

**האם אכן השיגו המתמטיקאים את מבוקשם?**

"היום פיתחו צפנים שאפשר להוכיח ביחס אליהם, כי סיבוכיית שבירת הצופן היא כסיבוכיות הניסיון לפרק מספרים. המאמצים למצוא פתרון יעיל לבעיית הפירוק ימיהם כימי האנושות כך שאם יצליח מישהו לשבור צופן כזה, הוא גם יפתור בעיה מתכונית חשובה מאין כמוה ויגלה תגלית במתמטיקה ברמת תורת היחסות של איינשטיין. בניית צפנים כאלה, שלא ניתן ללמוד מהם אפילו מידע חלקי, היתה נושא הדוקטורט שלי".

גולדווסר נולדה ב־1958 בארצות הברית. אביה עשה שם בשליחות ממעם קופת חולים. בגיל חמש שבה לארץ ולמדה בבית ספר גורדון ובתיכון ד' בצפון תל אביב. "למדתי במגמה ריאלית", אף כי אהבתי גם ספרות", היא מספרת. "אני מניחה שגם מהבית דחפו אותי ללכת למגמה ריאלית. בדיעבד זו היתה בחירה נכונה. אבל לדעתי, יש מקום פגום במערכת החינוך, ולפיו מגמה ריאלית נחשבה ליותר יוקרתית ממגמות אחרות. במרוצת הזמן הלימודים במגמה התחילו גם למשוך אותי, אם כי לא הייתי מתארת אז את המתמטיקה כאש הבוערת בעצמותי".

לאחר לימודיה, שאותם סיימה בגיל צעיר מהרגיל, נסעה ללמוד מתמטיקה באוניברסיטת קרנגי מלון שבפיטסבורג, בארצות הברית. היא הצטרפה לאחיה, שלמד שם מינהל עסקים. לאחר קבלת התואר הראשון עברה לאוניברסיטת קליפורניה שבברקלי לימודי דוקטורט. "רציתי להחליף מקום ואווירה", היא אומרת על הסיבות להחלטתה לעבור לחוף המערבי של ארצות הברית, "אך בלי ספק גם השפיעה עלי העובדה שהיו בברקלי אנשים טובים במדעי המחשב".

בתוך שלוש שנים וחצי השלימה את עבודת הדוקטורט, קיבלה את התואר, והתקבלה ב־1983 לעבודה במחלקת מדעי המחשב באמ־איי־טי במרצת השנים הגיעה שם לדרגת פרופסור מן המניין והוציאה לעצמה שם בזכות מחקר על הוכחת הסתברויות מסוגים שונים ובמיוחד "הוכחת אפס בידע אינטראקטיווית".

"יש במתמטיקה מושג קלאסי של הוכחה", מבהירה הפרופ' גולדווסר. "הוכחה לטענה מתמטית ניתנת להיכתב בספר מתמטיקה ולהיבדק מאלף עד תיו על ידי כל קורא. המחקר שלנו מתמודד עם מושג חדש של הוכחה הסתברותית. במערכת הוכחה הסתברותית ואינטראקטיווית, למשל, הוכחות אינן נכתבות אלא נבדקות בתהליך של שאלות ותשובות – בין מוכיח הטענה לבודק נכונותה. הבודק שואל שאלות שנבחרות באקראי, ואם המוכיח מסוגל לספק לכולן תשובות, הבודק יסכים כי הטענה תקפה. למה הדבר דומה? לחקירת משטרה שבה מנסה החוקר למצוא פגמים באליבי של החשוד בפשע. אם החשוד תי מפשע, הוא יכול לענות לכל שאלה אפשרית. ואם הוא אשם, קרוב לוודאי שבעזרת שאלות אקראיות יגלה החוקר את תוכר ההתאמה שבתשובותיו. האנלוגיה המתמטית היא שהחשוד הוא המוכיח, והחוקר הוא הבודק את הטענה שהחשוד תי מפשע. להבדיל מהחוכחה הקלאסית, במערכת הסתברותית יש תביד אפשרות או הסתברות לטעות. אך הסתברות זו היא כה קטנה, שלמעשה כעורות אנוש בחוכחות קלאסיות יכולות לקרות לעתים קרובות יותר. היתרון הוא שמערכות הוכחה הסתברותיות יכולות להיות יעילות הרבה יותר

תצלום רב פיינר

שפי גולדוזמר. "באר"ב העבודה היא המרכז. בישראל יש חשיבות לעוד דברים, כמו המשפחה"

מהוכחות קלאסיות, ובמפתיע, אפשר לשכנע את הבודק בגבונות המענה בלי להוסיף מידע על פרטי ההוכחה. מכאן גם נובע השם 'הוכחת אפס מידע'".

לתגלית יש לא רק חשיבות מדעית, אלא גם השפעה על אורחות חיינו. לכשל, הוכחות אפס מידע מאפשרות למשתמש להיכנס למחשב שלו בלא שאחרים, שאינם מוסמכים לכך, יוכלו לעשות זאת, גם אם קיימת האונה חשאית ובלתי חוקית לתקשורת שבין המשתמש למחשבו. הפתרון הכוכר של סיסמה (password) אינו מאפשר זאת. המחקרים הללו גם מאפשרים שימוש בטוח ומוגן יותר בערוצי המידע המכתשבים ובדואר אלקטרוני. התיאוריה מאפשרת זיהוי מה שמכונה "חתימה דיגיטלית". נחשב ב' יכול להיות סמוך ובטוח כי המידע, או המסמך, או הקובץ, שנשלח אליו, מקורו אכן במי חשב א' בדייוק כפי שפקיד בנק מזהה את חתימת הלקוח על ההמחאה כעזרת רוגמת חתימה המצויה בתיקיו

למערכת הבנקאות האמריקאית הוכנס זה לא כבר השימוש בחתימות דיגיטליות, ושימוש רומה לשם וידוי מגויים עושות רשתות סלולריות בכבלים המוכרות סרטים או תוכניות בתשלום ועל פי הזמנה. עתיד ורוד יותר צפוי לתחום זה כאשר בני אדם יבצעו בעזרת המחשב כמעט את כל הסידורים של־הם: קניות במרכול, תשלום מסים, העברות בנקאיות ועוד להוכחה ההתברותית יש גם השלכות על בריקת בזק בנוגע לנכונותן של תוכניות מחשב.

אל למרות הפיתויים הכספיים הטמונים בכל חקרה, שלא לדבר על מעמד מקצועי ויוקרה מדעית, החליטה גודלוזסר לפני שנתיים לשוב לישראל. "אולי זה לא נשמע די ציוני", היא מחייכת, "אבל התחתנתי עם מישהו שרוצה לגור בישראל בעלי הוא דוקטור למדעי המחשב באוניברסיטת תל אביב". אבל היא מודה ש"כבר שנים השתעשעתי ברעיון לחזור לארץ. מאז 1987 הגעתי לכאן לעשות את שנות השבתון שלי. נמשכתי לחזור לשפה, להוויה החברתית".

## "מכון ויצמן העניק לי תנאים מצוינים לעריכת המחקר. ההבדל העיקרי הוא שאם־איי־טי הוא מרכז עולמי של מחקר ואינטראקציה מדעית. מבחינה זו, הריחוק של ישראל פוגם"

**והחזרה הביתה עונה על הציפיות?**

"מבחינה אקדמית רק הזמן יקבע זאת. יש בישראל קהילה אקדמית טובה. מכון ויצמן העניק לי תנאים מצוינים לעריכת המחקר ואווירה תומכת. בשבוע הבא, לדוגמה, יתקיים במכון כנס בינלאומי שאליו יבואו ויקרים ממדינות רבות. ההבדל העיקרי הוא שאם־איי־טי הוא מרכז עולמי של מחקר ואינטראקציה מדעית. מבחינה זו, הריחוק של ישראל פוגם. אם כי הטכנולוגיה והתקשורת המודרנית – אני מתברת לחו"ל בקשר רואר אלקטרוני – מקצרים את המרחק בין המרכז לפריפריה".

**את מבחינה בעוד הבדלים בין הקהילות האקדמיות של שתי המדינות?**

"בארצות הברית יש דינמיקת עבודה אחרת: מקום העבודה הוא מרכז הקיום. בישראל יש חשיבות לעוד דברים, כמו המשפחה, התעסקת מקום מרכזי בחיים. ועוד הבדל, שאינו מפתיע. המחקר במדעי המחשב בישראל הוא מאוד תיאורטי ופחות יישומי. ייתכן שהסיבה לכך היא, שאין בארץ די משאבים למחקר יישומי. פרופסור בארצות הברית מתפרנס בכבוד מעבודתו באקדמיה, והפיתוי לעבוד בעבודה נוספת בתעשייה קטן. בישראל, לעומת זאת, רבים נאלצים לעסוק בייעוץ כדי להשלים את המשכורת, ולכן ישראלים רבים שלומדים בחו"ל אינם חוזרים. אבל בסך הכל האווירה טובה. עד כה אני אופטימית".