הוכחות אקראיות

מאת **פרופ' עודד גולדרייך**

המושג המסורתי של הוכחה, ובייחוד מערכות הוכחה מסוג NP, מוגדר ביחס לתהליך וידוא יעיל ודטרמיניסטי. בניגוד לכך, המוכנות לחרוג מהמסורת ולהשתמש בתהליכי וידוא יעילים אך אקראיים מאפשרת כמה יתרונות:

- מערכות הוכחה אינטראקטיביות, שמשתמשות בתהליך וידוא אקראי, הן בעלות כושר ביטוי רב מזה של המערכות המסורתיות (מסוג NP) ומאששות את היתרון של דו־שיח על תקשורת חד־כיוונית.
- מערכות כאלו עשויות לאפשר וידוא באפס מידע ולהפריך את הקשר ההכרחי כביכול שבין השתכנעות בנכונות של טענה לבין לימוד של דבר־מה נוסף בנוגע אליה.
- ניתן לתרגם ביעילות הוכחות מסוג NP לצורה בעלת יתירות אשר תומכת בשיערוך מקורב של אמיתות ההוכחה על בסיס קריאה של חלק זעיר ממנה.

בכל המערכות הללו המוודא משתמש באקראיות ומחליט על סמך מידע הסתברותי, אלא שהסתברות הטעות שלו חסומה באופן מפורש וניתנת להקטנה באמצעות הרצות חוזרות של המערכת.

על סוג הטענות שבהן נדון

אפתח בשתי הערות על אופיין של הטענות שיהיו במוקד הדיון. ראשית אדגיש שמדובר בטענות המתייחסות למידע הכלול בתוכנן בלבד ושאינן מתייחסות למציאות חיצונית כלשהי. אף שכל המידע הרלוונטי לאמיתותן נמצא בהן, ייתכן שקבלת מידע נוסף (שייקרא הוכחה) מקל את וידוא אמיתותן (verification). טענה אופיינית היא שלמערכת של משוואות יש פתרון בשלמים (אי־שליליים).

הסתכלו למשל במערכת המשוואות הזאת:

$$x+y+z = 2$$
$$x-y \geq 0$$
$$2y+z \leq 2$$
$$x \leq 1$$

מובן שתוכלו לאמת בקלות את הטענה שלמערכת זו יש פתרון בשלמים (אי־שליליים), אלא שנראה לי שתודו שמתן הוכחה – בדמות הצבה (כגון x=y=1 z=0) למשתנים – מקילה את וידוא הטענה. שימו לב שההוכחה אינה מופיעה במפורש בגוף הטענה, אבל היא כלולה בה במובלע. גם הטענה שלמערכת מן הסוג הזה אין פתרון בשלמים כוללת את כל המידע הנחוץ לצורך וידוא שלה, אלא שבמקרה זה הוכחה בדמות הצבה יחידה למשתנים אינה מספיקה.

אני מתכוון להשתמש בדוגמה זו (קרי: פתרון של מערכות משוואות הכוללות הרבה משוואות בהרבה נעלמים) בכל מהלך הדיון. מכך מתברר שהטענות שנדון בהן, שכל אחת מהן מתייחסת למערכת מסוימת שהיא חלק מהטענה, הן טענות ספציפיות חסרות חשיבות כללית, בניגוד לטענות כלליות (קרי: משפטים מתמטיים) כגון משפט פיתגורס או המשפט האחרון של פרמה.

הערה למתקדמים: אני מתעקש על פתרון בשלמים של משוואות משום שבמקרה זה אפילו שאלת הקיום של פתרון למערכת משוואות ליניארית היא בעיה NP־שלמה. מכאן שכל מה שייאמר על הבעיה הזאת (של פתרון בשלמים של מערכת משוואות) חל על כל הטענות במחלקת הסיבוכיות NP.

המושג המסורתי של הוכחה: מערכות מסוג NP

היצירתיות הכרוכה במציאת הוכחות והיוקרה המתלווה אליה משכיחות מאיתנו את העובדה שהתהליך הלא יצירתי של וידוא הוכחות הוא שנותן להוכחות את ערכן. מבחינה מושגית הוכחות הן משניות ביחס לתהליך הווידוא, ואילו מבחינה פורמלית מערכות הוכחה מוגדרות על סמך תהליך הווידוא שלהן.

המושג של תהליך וידוא מניח – כמובן מאליו – את המושג של חישוב, ולמעשה גם את המושג של חישוב יעיל. ההנחה הסמויה הזאת הופכת למפורשת בהגדרה של הוכחות מסוג NP, שם מזוהה חישוב יעיל עם חישוב דטרמיניסטי שזמן הריצה שלו עולה במתינות כפונקצייה של אורך הקלט (השם NP אינו מוצלח, אבל הוא המקובל). מכאן שמערכות הוכחה מסוג NP הן מערכות המשתמשות בתהליכי וידוא יעילים המופעלים על הוכחות שאורכן גדל במתינות עם אורך הטענות המוכחות (כאשר בדרך כלל פונקציות הגדלות במתינות מזוהות עם פונקציות החסומות בפולינום).

הערת אגב: שאלת P-vs-NP

אני משער שהקוראים מניחים כמובן מאליו שלהוכחות יש ערך, וגם אני מאמין בכך. אלא שהאמונה הזאת מבוססת על ההנחה שקל יותר לוודא נכונות של הוכחה לטענה מאשר להעריך את אמיתות הטענה כאשר היא נתונה ללא הוכחה. אך האם אמונה זו נכונה?

התשובה היא שהדבר אינו ידוע. שאלה זו היא אחד מן הניסוחים של השאלה המרכזית ביותר במדעי המחשב אשר ידועה בשם "שאלת P-vs-NP". ההשערה המקובלת היא שהתשובה היא חיובית, זאת אומרת שקל לוודא נכונות של הוכחה לטענה יותר מאשר להעריך את אמיתות הטענה כאשר היא נתונה ללא הוכחה. תשובה שלילית לשאלה זו שומטת את הקרקע מתחת למושג ההוכחה, משום שבמקרה זה להוכחות אין ערך רב בווידוא הנכונות של טענות. ◄

עיון נוסף במושג של מערכות הוכחה

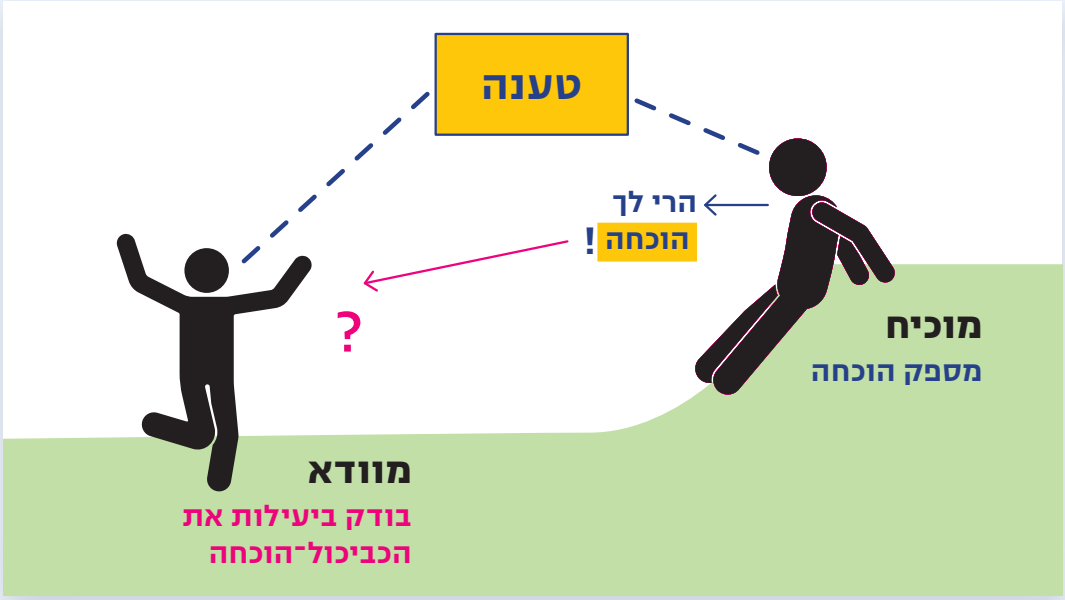
הדיון שלנו במערכות הוכחה התמקד בתהליך הווידוא. כעת אני מבקש להדגיש במפורש את התנאים הנדרשים מתהליך וידוא (קרי: שלמות ונאותות). תנאים אלו מתייחסים לטענות מסוג מסוים אשר מערכת ההוכחה חלה עליהם (כגון הטענה על קיום פתרון בשלמים למערכת משוואות):

- **תנאי השלמות** (completeness) דורש כי לכל טענה נכונה (מהסוג הרלוונטי) קיימת הוכחה אשר מתקבלת כתקפה באמצעות תהליך הווידוא.
- **תנאי הנאותות** (soundness) דורש שלטענות שקריות אין "הוכחה כביכול" אשר מתקבלת כתקפה באמצעות תהליך הווידוא.

תנאי השלמות והנאותות הם בסיס המושג של מערכת הוכחה: השלמות דורשת שטענות נכונות יהיו ניתנות להוכחה, ואילו הנאותות דורשת שטענות שקריות לא יהיו ניתנות להוכחה. בדוגמה של טענות המתייחסות לקיום פתרון למערכת משוואות, פתרון של המערכת הוא בבחינת הוכחה לטענה, ותהליך הווידוא מתמצה בהצבת הערכים למשתנים ובבדיקה שערכים אלו מקיימים את כל אחת מן המשוואות.

נראה לי מועיל, בעיקר לצורך ההמשך, להציג מערכות הוכחה כמשחקים בין שני שחקנים: מוודא שמפעיל את תהליך הווידוא, ומוכיח שהוא מקור ההוכחות הפוטנציאליות. במילים אחרות, תהליך הווידוא מואנש על ידי המוודא (verifier), ומקור ההוכחות הפוטנציאליות הוא במוכיח (prover), שאינו מופיע במפורש בהגדרת המערכת (קרי: מערכת ההוכחה).

אם נשתמש בהאנשה זו, נוכל לראות במערכת הוכחה מסוג NP תקשורת חד־כיוונית מהמוכיח למוודא: המוכיח כותב הוכחה (לכאורה) ושולח אותה למוודא, וזה קורא אותה לשם וידוא נכונותה (ראו איור 1). אכן, המושגים "כותב" ו"קורא" מתאימים לראייה המסורתית של הוכחות ככתובות על ספר (או מאמר) וכנקראות על ידי החפצים בדעת.



איור 1. הוכחות מסורתיות: תקשורת חד־כיוונית

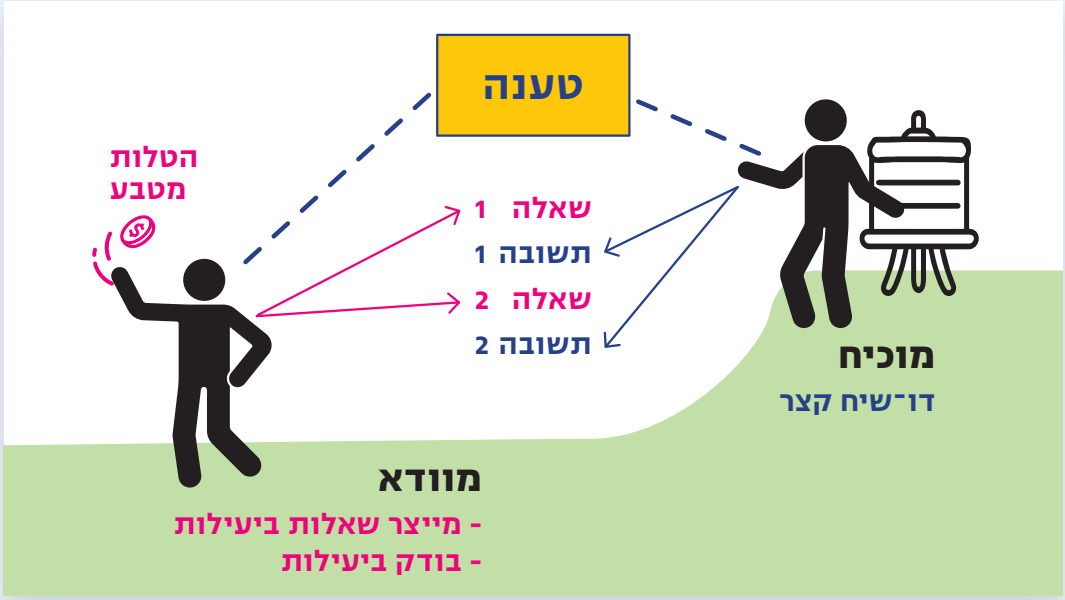
אם נמשיך בתהליך ההאנשה נוכל להציג כך גם את מושגי השלמות והנאותות: תנאי השלמות אומר שמוכיח מתאים (שייתכן שהוא בעל ידע רב מזה של המוודא) יכול לגרום למוודא להשתכנע בכל טענה נכונה, ותנאי הנאותות אומר שאין דרך לגרום למוודא להשתכנע בטענות שקריות.

מעבר להוכחות מסוג NP

תכונה מרכזית של מערכות הוכחה מסוג NP היא שהן מבוססות על תהליכי וידוא דטרמיניסטיים (זאת אומרת תהליכי חישוב שבהם כל צעד נקבע באופן חד־ערכי על סמך המצב הנוכחי). אף שציינתי את העובדה הזאת, אני מניח שהקוראים לא הקדישו לכך תשומת לב רבה, משום שהם ראו בה מובנת מאליה. בניגוד לכך, מאמר זה יתמקד במערכות הוכחה אשר מבוססות על תהליכי וידוא אקראיים אשר כרוכים בהסתברות של שגיאה. עניין זה מעורר התנגדות טבעית, משום שנראה שהסתברות שגיאה מנוגדת למושג ההוכחה, אלא שאני מבקש לכפור בתחושה זו. אני מבקש להדגיש שהסתברות השגיאה תהא חסומה במפורש, ושאפשר יהיה להקטין אותה כרצוננו באמצעות מספר מתאים של הפעלות חוזרות של מערכת ההוכחה. מובן שלא היינו מסתבכים בעימות עם תחושות מקובלות לולא הייתה בכך תועלת רבה. כמו כן אדגיש כי כמו במערכת מסוג NP, בכל מערכות ההוכחה ההסתברותיות תהליך הווידוא הוא יעיל.

הוכחות אינטראקטיביות (ואקראיות)

ראייה במערכת הוכחה משחק בין מוודא לבין מוכיח פוטנציאלי מעלה באופן טבעי את האפשרות לקיום תקשורת דו־כיוונית בין השחקנים, בניגוד לתקשורת החד־כיוונית שעליה מיוסדת מערכת הוכחה מסוג NP. תקשורת דו־כיוונית כזאת היא אכן דו־שיח (או אינטראקצייה) בין המוכיח למוודא, ולפיכך ייקראו מערכות הוכחה כאלו בשם הוכחות אינטראקטיביות (interactive proofs) או הוכחות מסוג IP (ראו איור 2).



איור 2. הוכחות אינטראקטיביות: תקשורת דו־כיוונית

המילה "אקראיות" אינה מופיעה בשם "הוכחות אינטראקטיביות", אבל לא קשה לראות שאקראיות חיונית ליתרון של הוכחות מסוג IP לעומת הוכחות מסוג NP. לו היה המוודא במערכת האינטראקטיבית דטרמיניסטי, היה המוכיח יכול לדעת מראש את כל הודעותיו. במקרה כזה הוא יכול היה פשוט לשלוח הודעה יחידה (אכן הוכחה מסוג NP) אשר כוללת את כל השיח בין שני השחקנים המקוריים. הלקח הכללי הוא שאין טעם לנהל שיח עם שחקן שניתן לחזות בקלות את כל הודעותיו. שיח הוא בעל ערך עבורנו רק אם הודעותיו של הצד השני אינן ידועות מראש, אם משום שהן אקראיות ואם משום שלרשות הצד השני משאבי חישוב רבים יותר.

בשלב זה ראוי שנפנה להגדרה המפורשת של **מערכות הוכחה מסוג IP**, אשר מבוססת על פרשנות מחודשת של תנאי השלמות והנאותות, פרשנות אשר מתייחסת למושג של עדות מסתברת (קרי: מושגי השלמות והנאותות יהיו הסתברותיים):

- **תנאי השלמות** דורש כי עבור כל טענה נכונה (מהסוג הרלוונטי) יש למוכיח דרך (קרי: "אסטרטגיה") לגרום למוודא לקבל את הטענה כתקפה בהסתברות 1.

  יש טעם גם בתנאי שלמות מוחלש יותר אשר דורש שהסתברות הקבלה תהא לפחות 2/3. למעשה ניתן להמיר מערכות מהסוג המוחלש למערכות מהסוג החזק הנ"ל.

- **תנאי הנאותות** דורש כי כל ניסיון לשטות במוודא ולגרום לו לקבל טענה שקרית ייכשל בהסתברות לפחות ½.

  אומנם נפילה בפח בהסתברות ½ היא דבר שקשה להסכין עימו, אלא שניתן להוריד כרצוננו את ההסתברות שניפול בפח בהפעלות חוזרות של המערכת.

כמו במקרה של הוכחות מסוג NP, השלמות דורשת שטענות נכונות יהיו ניתנות להוכחה, ולפי הנאותות טענות שקריות אינן ניתנות להוכחה (למעט בהסתברות זניחה).

דוגמה: איזומורפיזם בין מערכות של משוואות

נגדיר שתי מערכות של משוואות כאיזומורפיות אם ניתן לעבור מאחת לאחרת באמצעות שינוי של שמות המשתנים ושינוי של סדר המשוואות. הוכחה מסוג NP של איזומורפיזם בין משוואות יכולה להיות מורכבת מתיאור של החלפת שמות המשתנים ותיאור הפרמוטציה של סדר המשוואות.

בניגוד לכך, לא ידועה לנו הוכחה מסוג NP לטענה ששתי מערכות של משוואות אינן איזומורפיות. כאן באות לעזרה הוכחות אינטראקטיביות. במערכת הוכחה מסוג IP המוצעת להלן המוודא בוחר אחת משתי מערכות המשוואות באקראי ויוצר עותק איזומורפי אקראי שלה (באמצעות החלפה אקראית של שמות משתנים וסידור אקראי של המשוואות). המוודא שולח את מערכת המשוואות שהתקבלה למוכיח ומבקש ממנו לציין את מקורה (קרי: אם היא איזומורפית למערכת המשוואות הראשונה או לשנייה). תנאי הנאותות מתקיים, משום שאם המערכות איזומורפיות, אין דרך לדעת את מקורה של מערכת המשוואות שנשלחה למוכיח, ולא ניתן לשטות במוודא בהסתברות העולה על 1/2. מנגד, תנאי השלמות מתקיים, משום שאם המערכות אינן איזומורפיות, גם עותקים איזומורפיים שלהם יהיו לא איזומורפיים.

תוצאה כללית

נחזור לשאלה הטבעית יותר של קיום פתרון (בשלמים) למערכת של משוואות. כזכור, לטענה שקיים פתרון כזה יש הוכחה פשוטה מסוג NP, אבל מה בדבר הטענה על אי־קיום פתרון כזה? גם

כאן באות לעזרה הוכחות אינטראקטיביות, אלא שבמקרה זה לא אוכל להציג כאן את ההוכחה (מסוג IP), משום שהיא מסובכת מדי. אבל אני מבקש לומר במפורש את התוצאה המתקבלת: **קיימות הוכחות אינטראקטיביות לטענה שלמערכת משוואות נתונה אין פתרון בשלמים.**

באופן כללי יותר, **לכל סוג של טענות שיש להן מערכת הוכחה מסוג NP, יש מערכת הוכחה מסוג IP לטענות ההפוכות** (מובן שלכל טענה ספציפית והיפוכה, רק אחת ממערכות ההוכחה מצליחה לשכנע את המוודא המתאים). אינטואיטיבית, הוכחות מסוג NP מספיקות לשם שכנוע בקיום של דבר־מה, ואילו לשם שכנוע באי־קיומו של אותו דבר אפשר להשתמש בהוכחות מסוג IP (אולם ככלל, הוכחות מסוג NP לא יצלחו למטרה זו).

שתי הערות

בהוכחה האינטראקטיבית לטענה ששתי מערכות אינן איזומורפיות נעשה שימוש מהותי בעובדה שהבחירה האקראית של המוודא נשמרת בסוד, ורק התוצר שלה נמסר למוכיח. מסתבר שלאותו סוג טענות יש הוכחה אינטראקטיבית שמשתמשת רק באקראיות שאינה נשמרת בסוד. באופן כללי, כל מערכת הוכחה אינטראקטיבית ניתנת להמרה למערכת שמשתמשת רק באקראיות גלויה. במילים אחרות, בהקשר של קיום מערכות הוכחה מסוג IP אין יתרון לשאלות מתוחכמות (אשר מסתירות את האקראיות) על שאלות אקראיות.

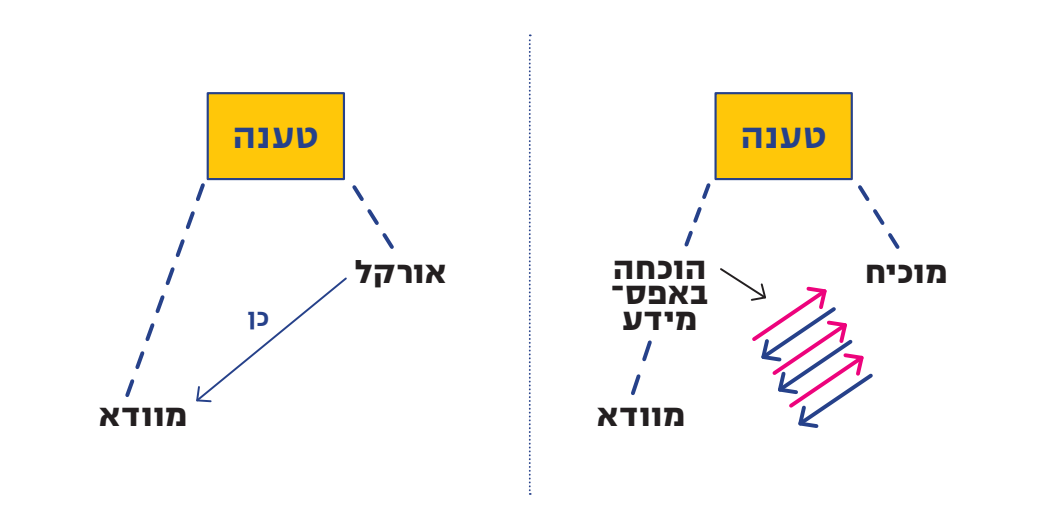
הדיון שלנו בהוכחות מסוג IP התמקד ביעילותו של המוודא ולא עסק כלל בסיבוכיות האסטרטגיה של המוכיח. דיון מעודן יותר עוסק בסיבוכיות של שתי המשימות ומתמקד במקרה שבו הסיבוכיות של אסטרטגיית המוכיח אינה עולה בהרבה על סיבוכיות הערכת האמת של הטענה (ללא הוכחה נלווית), ואילו סיבוכיות המוודא נופלת מסיבוכיות ההערכה (ללא הוכחה נלווית). מערכות הוכחה כאלו, שהן בעלות חשיבות מעשית רבה, נקראות דו־יעילות (doubly efficient).

הוכחות באפס־מידע

תחושה בסיסית שלנו בנוגע להוכחות היא שהן מלמדות אותנו על הטענה יותר מאשר על עצם היותה של הטענה נכונה. אכן, הוכחות נקראות ונלמדות בדרך כלל כדי להעמיק את הבנת הטענה ואת ההקשר הרחב שלה. בניגוד לכך, הוכחות באפס־מידע (zero-knowledge) מתוכננות מתוך כוונה שלא למסור דבר מלבד עצם נכונות הטענה. זו תכונה מבלבלת ולא טבעית בעליל, והיא אינה יכולה להתקיים בהוכחות מסוג NP. לכן היא מנוסחת, ולעיתים אף מושגת, בהוכחות מסוג IP.

הבה נתבונן בהוכחה מסוג IP שבה השתמשנו להוכחת אי־קיום איזומורפיזם בין שתי מערכות של משוואות. בהוכחה זו המוודא אינו לומד דבר מהמוכיח, משום שהוא רק בודק שתשובת המוכיח מתאימה לבחירה הראשונית שלו (של המוודא) אשר ידועה למוודא. הטעם היחיד בבדיקה זו הוא השתכנעות בנכונות הטענה שהמערכות הנתונות (של משוואות) אינן איזומורפיות.

בשלב זה ראוי לתהות איך ניתן להגדיר את האמירה "ההוכחה אינה מגלה דבר מלבד עצם נכונות הטענה" אשר השתמשנו בה לתיאור המושג של "הוכחה באפס־מידע". התשובה היא שההגדרה של הוכחה באפס־מידע של טענה מפרשת את האמירה הזאת כדרישה כי כל דבר אשר ניתן לחשב ביעילות לאחר קבלת הוכחה באפס־מידע, ניתן לחישוב יעיל גם על סמך הטענה המוכחת עצמה (בהנחה שהיא נכונה). במילים אחרות, ההגדרה מכוונת לשני עולמות שונים: העולם הממשי שבו מתנהל תהליך ◄



איור 3. הוכחות באפס־מידע: העולם הממשי נגד העולם הדמיוני

ההוכחה האינטראקטיבית ועולם דמיוני שבו ישות מהימנה אומרת לנו שהטענה נכונה (ראו איור 3). הגדרת אפס־מידע אומרת שכל חישוב שניתן לבצע בעולם הממשי ניתן לביצוע, בערך באותו מאמץ, גם בעולם הדמיוני.

אכן, הטעם היחיד בקבלת הוכחה באפס־מידע הוא ההשתכנעות עצמה בנכונות הטענה המוכחת, ויש בכך טעם רק כאשר אין לנו אמון גמור בישות הטוענת לנכונות הטענה. היעדר אמון בין ישויות שונות הוא המצב המייסד של תחום הקריפטוגרפיה, ואכן להוכחות באפס־מידע יש שימושים רבים בתחום זה. בעיקר הן מאפשרות לישות להוכיח שהיא נוהגת כהלכה, לפי סודותיה, מבלי לגלות דבר על סודותיה.

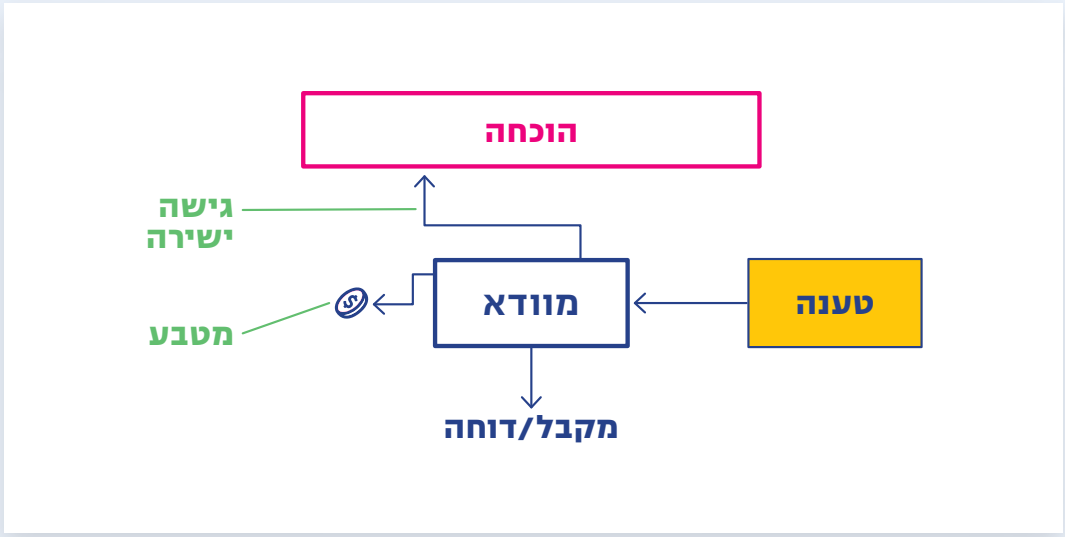
אם נחזור לדוגמה של טענות על קיום פתרון בשלמים של מערכת משוואות, הרי שהוכחה באפס־מידע של טענה כזאת משכנעת בקיום פתרון מבלי למסור מידע אף לא על אחד מהפתרונות. העובדה המדהימה היא שהוכחות אפס־מידע כאלו קיימות, בהנחה שקיימות פונקציות שהן קלות לחישוב אך קשות להיפוך (one-way functions), שזו הנחה הכרחית לקיום הקריפטוגרפיה המודרנית, ובייחוד לקיום מערכות הצפנה בטוחות וחתימות דיגיטליות שאינן ניתנות לזיוף.

באופן כללי יותר, **כל טענה אשר יש לה הוכחה מסוג NP ניתנת להוכחה באפס־מידע**. יתר על כן, אסטרטגיית המוכיח בהוכחת האפס־מידע הזאת ניתנת למימוש ביעילות בהינתן הוכחה מסוג NP לאותה טענה. (נזכיר כי גם לכל הוכחה מסוג IP יש הוכחה באפס־מידע.)

הוכחות הניתנות לבדיקה הסתברותית

נחזור כעת להוכחות מסוג NP ונשים מאחורינו את ההוכחות מסוג IP, אבל נשמור על האפשרות להשתמש באקראיות לשם וידוא של הוכחות.

תחושה בסיסית שלנו בנוגע להוכחות מסורתיות – ובייחוד מסוג NP – היא שיש לקרוא אותן במלואן. הבוחרים לדלג על חלק מן ההוכחה מסתכנים



איור 4. מערכות PCP: למוודא יש גישה ישירה לביטים שבהוכחה.

בקבלת טענה שקרית, אלא אם הם יודעים ממקור אחר את החלק שעליו דילגו. בניגוד לכך, הוכחות הניתנות לבדיקה הסתברותית, שייקראו הוכחות מסוג PCP (**P**robabilistically **C**heckable **P**roofs), מאפשרות להעריך את נכונותן באמצעות קריאה של חלקים קטנטנים בהן (ראו איור 4). כפי שיודגם מייד, על הוכחות אלו להכיל הרבה יתירות (redundancy), ואת החלקים הנבחנים בהן יש לבחור באקראי.

אם נחזור לדוגמה ששימשה אותנו עד כה – קיום פתרון בשלמים למערכת משוואות – הרי שהוכחה מסוג NP שמתארת פתרון כזה אינה ניתנת לבדיקה הסתברותית, משום שקיימות מערכות של משוואות שבהן סתירה בנוגע לערך של משתנה יחיד היא שאחראית להיעדר פתרון בשלמים למערכת. בכך אני רואה עדות להכרח שהוכחה מסוג PCP תכיל יתירות. באשר לאקראיות, יש לשים לב שמוודא דטרמיניסטי שבודק מספר קטנטן של מקומות בהוכחה מסוג PCP מגדיר למעשה הוכחה מסוג NP שהיא קצרה באופן לא סביר (קרי: אורך ההוכחה החדשה קטן מהאורך המינימלי הנחוץ להוכחה מסוג NP על פי ההשערות המקובלות בנוגע למחלקת הסיבוכיות NP).

לצערי, הרעיונות שבבסיס הבנייה של מערכות הוכחה מסוג PCP אינם ניתנים לתיאור במסגרת מאמר זה. לפיכך אסתפק בציטוט של תוצאה מרכזית בתחום שאומרת כי **כל הוכחה מסוג NP ניתנת לתרגום יעיל להוכחה מסוג PCP**. במערכת ה־PCP המתקבלת המוודא קורא רק שלושה ביטים אקראיים בהוכחה ודוחה בהסתברות של לפחות 0.49 כל "הוכחה שקרית" לכל טענה שקרית, ואילו בהסתברות 1 הוא מקבל הוכחה (מתורגמת כנ"ל) לטענה נכונה. הקבוע 0.49 מייצג מספר קבוע כלשהו הקטן מ־1/2, וגודל זה הוא אופטימלי עבור PCP שבו נקראים רק שלושה ביטים, ושלושה ביטים הם המינימום שיש לקרוא בהוכחת PCP.

לסיום אציין כי לבניית הוכחות מסוג PCP הייתה השפעה דרמטית על חקירתן של בעיות קירוב. הקשר בין הנושאים הללו מיוסד על היותה של הערכת ההסתברות שמערכת PCP מסוימת ◄

איור 5. באדיבות הראל לוז

מקבלת טענה נתונה – בעיית קירוב, וניתן לתרגם אותה להרבה בעיות קירוב טבעיות. אציין גם כי הוכחות מסוג PCP קשורות לתחום המחקר הידוע בשם "בדיקת תכונות" (property testing).

ההקשר הרחב

מערכות הוכחה אקראיות הן מקרה מובהק של הקשרים שבין חישוב לאקראיות. במקרה זה, כמו בקריפטוגרפיה ובחישוב מבוזר, יש יתרון חישובי ביכולתו של צד אחד לנקוט פעולות שאינן ניתנות לחיזוי על ידי הצד השני. הקשר שבין חישוב לאקראיות נמצא ביסוד התורה של פסאודו־אקראיות שם מוגדרים אובייקטים כ"אקראיים למעשה" אם לא ניתן להבחין ביעילות בינם לבין אובייקטים אקראיים ממש. ■

מקורות

חרגתי במודע מ"הקוד האקדמי" אשר מחייב אזכור של שמות החוקרים אשר תרמו לגוף הידע שהצגתי במאמר זה. אזכורים כאלו נראים לי חסרי טעם בסקירה המיועדת לקהל הרחב. יתר על כן, אזכור שמות ספורים מרחיב את הפער בין "ידועים" לבין "חוקרים מהשורה", פער אשר סותר את העובדה שהמדע הוא פרויקט קהילתי.

המקורות להלן (פרי עטי) מיועדים ל"תלמידי חכמים" (קרי: סטודנטים בלימודי הסמכה ומוסמכים במדעי המחשב ומתמטיקה). המקורות [3–5] מכסים בהרחבה את עיקר החומר שהוצג במאמר, ואילו המקורות [1, 2, 6, 7] מכסים נושאים שהוזכרו בקצרה.

1) Oded Goldreich. Foundation of Cryptography: Volume 1 – Basic Tools. Cambridge University Press, 2001.
2) Oded Goldreich. Foundation of Cryptography: Volume 2 – Basic Applications. Cambridge University Press, 2004.
3) Oded Goldreich. Probabilistic Proof Systems – A Primer. In Foundations and Trends in Theoretical Computer Science, Volume 3, Issue 1, 2007.
4) Oded Goldreich. Computational Complexity: A Conceptual Perspective. Cambridge University Press, 2008.
5) Oded Goldreich. P, NP, and NP-Completeness: The Basics of Complexity Theory. Cambridge University Press, 2010.
6) Oded Goldreich. Introduction to Property Testing. Cambridge University Press, 2017.
7) Oded Goldreich. On Doubly-Efficient Interactive Proof Systems. In Foundations and Trends in Theoretical Computer Science, Volume 13, Issue 3, 2018.