



נקראו לדגל. אנשי ימין ושמאל שקלטו את

הדגל בתתי הכהרה נעו, ללא מודעות, בצורה

ברורה אל המרכז הפוליטי

<< הפכה את הלאומיים יותר לשמאליים יותר, ואת הלאומיים פחות לימניים יותר. הנבדקים שלהם הוקרן הדגל נעו בצורה מובהקת למרכז. חשוב להדגיש כי בקבוצות שלא עברו חשיפה לדגל נותרו הבדלים גדולים בין נבדקים לאומיים יותר לבין כאלה שפחות. בין הקבוצות שנחשפו לדגל, ההבדלים למעשה נעלמו. במלים אחרות, הקרנת הדגל, שנקלט בלי מודעות הנבדק, גרמה לשתי הקבוצות השונות כליך אידיאולוגית להתאחד

”משפט פשוט אחד, המשפט הזה, כמעט ומשבית את כל היכולת המודעת שלכם. ומכאן קל להטיק שרוב־רובם של התהליכים המנטליים צריכים להתרחש הרחק מהישג ידה של המודעות”

סביב המרכז הפוליטי. הנבדקים אצורצו אל מדורת השבט וישבו מאוחדים סביבה. הניסוי השני בסדרה נערך מעט לפני ההתנתקות מעזה. מבנה הניסוי היה דומה, אולם השאלות נגעו הפעם למתנחלים. הנבדקים נשאלו שאלות כגון איך ירגישו ביום ההתנתקות (שמחה או עצב), עד כמה מתיישבי גוף קטיף מייצגים את הרעיון של הפרחת השממה ויישוב הארץ, ועד כמה מהווים המתנחלים סכנה לאופייה הדמוקרטי של מדינת ישראל.

התוצאות היו זהות. בקבוצות שלא עברו חשיפה לא־מודעת לדגל היו הבדלים גדולים בין הלאומיים יותר (שנטו להתעצב מההתנתקות ולחשוב שהמתנחלים הם חלוצים מודרנים), לבין הלאומיים פחות (שהעריכו כי יתעצבו פחות, ואולי אף ישמחו, וחשבו שהמתנחלים מסוכנים לישראל). הקבוצות שעברו חשיפה לדגל נעו זו

לקראת זו, עד שסטטיסטית כלל לא ניתן היה להבחין ביניהן.
כבניסוי הראשון, גם כאן: למרות שהנבדקים לא ראו את הדגל, הוא גרם להם להתמתן בעמדותיהם ולצעוד לקראת אחדות במרכז המפה הפוליטית.

הניסוי השלישיבסדרה,אולי המפתיעמכולם, נערך לפני הבחירות האחרונות. במהלכו שאלנו את הנבדקים לאיזו מפלגה הם חושבים שיצביעו. גם כאן התוצאות היו חד־משמעיות. בעוד שלא לא חשיפה לדגל היו הבדלים גדולים בדפוסי ההצבעה בין הלאומיים יותר (נוטים לימין) ללאומיים פחות (נוטים לשמאל), הקבוצות שנחשפו לדגל לא הראו את הבדלים הללו. במלים אחרות, היתה גם כאן תזוזה לעבר המרכז.

מעט לאחר הבחירות התקשרנו אל הנבדקים ושאלנו עבור איזו מפלגה הם הצביעו. הסתבר לנו שגם על הצבעת האמת (או יותר מדויק לומר, דיווחי הנבדקים על הצבעותיהם) היתה למניפולציה העדינה שלנו השפעה גדולה. נבדקים שנחשפו לדגל באופן סבלימינאלי הצביעו יותר למרכז מאשר נבדקים שלא נחשפו לדגל. תוצאות

אידיאולוגיים, המוטבעים עמוק באישיות ובתודעה שלנו, יכולים לבוא לידי ביטוי מבלי שהאדם יודע על כך. במידה רבה, הראנו שהתנהגות לאומית דומה לנהיגה: פעמים רבות אנו יכולים למצוא את עצמנו בסוף הנסיעה, בלי שאנחנו יודעים למה וכיצד הגענו לשם. במלים אחרות, נהגנו ללא מודעות. כך גם כאן. פעמים רבות אנחנו מתנהגים באופן התואם את האידיאולוגיה הלאומית, בלי שאנו יודעים שאנו עושים זאת, או מה הדבר שגרם לנו להתנהג כך. לאומיות בנאלית, הראנו, יכולה להיגרם מחוץ למודעות.

המסקנה השנייה היא שלמרות ההתחלה ההיסטורית העגומה במחקר על השפעות לא־מודעות על קבלת החלטות בחיים שמחוץ למעבדה, יש למחקר פוטנציאל רב. במסטרים דמוקרטיים, אקט הבחירה בבחירות כלליות הוא אחת ההחלטות הפוליטיות החשובות ביותר בחיי האזרח, ואם זו מושפעת על־ידי חשיפה של כמה עשרות־אלפיות שנייה, הרי שאין שום סיבה להניח שהחלטות מכריעות אחרות אינן מושפעות באופן דומה. נראה כי התהליכים הלא־מודעים מורכבים וחזקים בהרבה מכפי שנהגנו לחשוב.

האתגר של המעבדה שלי, ומעבדות דומות לה ברחבי בעולם, הוא להבין את התהליכים המנטליים העומדים בבסיס ההשפעות הלא־מודעות על התנהגותנו. מה קורה בתוך הראש לאחר חשיפה לא־מודעת לאינפורמציה? מה מופעל שם ב”מינד”, במערכת הקוגניטיבית, ומה מופעל במוח, וכיצד הוא משפיע על הכוונות ודרכן על ההתנהגות?

הערה לסיום: למיטב הבנתי ההשפעות מהסוג שתיעדנו כאן אינן היוצא מן הכלל. הן אינן מעין אירוע ביזארי ששייך לעולם הקוסמות: אחת, שתיים, שלוש ו.....הופ, הצבעתם ‘קדימה’ נהפוך הוא: כך כנראה מתנהלים חיינו: מהשפעה לא־מודעת אחת לאחרת, שחוברות עם הנטיות, ההרגלים ויכולות השליטה המנטליות שלנו, ובכך יוצרות את מה שאנחנו. בהינתן המגבלות הקשות על יכולתנו המודעת, פשוט קשה לדמיין אפשרות אחרת. ■

ran.hassin@huji.ac.il

פרויקט “המוח הכחול”

אודיטאה #01 | 73

על מחשבים שלא קיימים וחתולים שהם גם חיים וגם מתים

דורית אהרונוב

בעשרות מעבדות ברחבי העולם מנסים ברגעים אלה לבנות את המחשב הקוונטי, מערכת מיחשוב שאיש אינו יודע לצפות את עוצמתה ואת שימושיה האפשריים. פרופסור דורית אהרונוב מסמנת את אבני הדרך ואת המכשולים בדרך לבניית המחשב הראשון, שיתבסס על עקרונותיה מעוררי הפליאה של פיזיקת הקוונטים

■ בגבול הדק שבין מדע בדיוני, עולם המחשבים והפיזיקה הקוונטית, נולד לפני כ־15 שנה תחום מדעי חדש – מחשבים קוונטים. מחשבים אלו יתבססו על חוקיה המוזרים של תורת הקוונטים, לפיהם למשל יכול אלקטרון להיות בשני מקומות בו־זמנית. המדענים טרם הצליחו לבנות ולו מחשב קוונטי אחד, שכן איננו יודעים עדיין לשלוט בחוקי הפיזיקה הקוונטית במעבדה, ברמת הדיוק הנדרשת. עם זאת, מאות חוקרים ברחבי העולם שוקדים בימים אלו על בניית מחשב קוונטי ומנסים להבין את שימושיו האפשריים.

מה הסיבה לעניין הרב במחשבים קוונטיים שעדיין לא קיימים? מתברר שישנן בעיות חישוב שמחשב קוונטי יוכל לפתור בכמה דקות, בעוד שמחשב רגיל יצטרך להקדיש להן יותר מזמן החיים של היקום כולו. יוצא מכך, שלמחשבים קוונטיים יהיו כנראה יכולות חישוב עצומות, עובדה שעשויה להוביל למהפכה חישובית נוספת. אנחנו עדיין רחוקים מאוד מלהבין אילו חישובים ניתן יהיה לבצע, ומה תהיינה ההשלכות הטכנולוגיות של בניית מחשב קוונטי, אך ברור שזו תהיה פריצת דרך טכנולוגית ומדעית כאחד. זאת ועוד: בניית מחשב קוונטי תהווה מבחן לעצם נכונותה של תורת הקוונטים בהיבטים שבהם מעולם לא נבחנה ואומתה. עוד בטרם נבנה המחשב הקוונטי הראשון, כבר שינה המחקר בתחום החישוב הקוונטי תפיסות יסוד בפיזיקה, במדעי המחשב, ואפילו בפילוסופיה של המדע.

על־מנת להבין איך מאפשרת תורת הקוונטים לחשב חישובים מהירים כל־כך, ומדוע ההשלכות של תחום החישוב הקוונטי כה מרחיקות לכת, עלינו להבין תחילה את העקרונות שעליהם מושתת החישוב הקוונטי.

תורת הקוונטים

בשנות ה־20 של המאה הקודמת פותחה (או נתגלתה, או אולי הומצאה, תלוי בהשקפתכם על המדע) תורת הפיזיקה הקוונטית. תורה זו שינתה לתמיד את עולם הפיזיקה ואת מה שאנחנו, המדענים, מוכנים לקבל כהסבר הגיוני על העולם הפיזיקלי. תורת הקוונטים מתבססת על רעיונות שנשמעים, אין דרך אחרת לומר זאת, קצת מטורפים: חלקיק יכול להיות בשני מקומות בו־זמנית. חתול יכול להיות גם חי וגם מת (תיאורטית). במובנים רבים מתנהג העולם כמו רולטה רוסית, בצורה אקראית לחלוטין ולכאורה ללא שום הסבר.

למרות מוזרותה, אוששה תורת הקוונטים במאה האחרונה באלפי ניסויים. כיום סבורים המדענים כי תורת הקוונטים היא התורה שמתארת במדויק את העולם הפיזיקלי. אין זה אומר שהפיזיקה הקלאסית אינה נכונה, כשמדובר בתופעות פיזיקליות בסדר־גודל של בני אנוש. אבל כשמדובר בסקאלות קטנות, הפיזיקה הקלאסית שאנו רגילים לה נעשית פחות וכחות

<< מדויקת, ופיזיקת הקוונטים, מתברר, מתארת בדיוק את מה שקורה.

יש כמובן בעיה "קטנטנה": תורת הקוונטים לא כליך "מסתדרת" לפיזיקאים עם תורת היחסות, שגם היא בפני עצמה מתארת מצוין את העולם הפיזיקלי - בסקאלות עצומות. מבחינה תיאורטית, המדענים לא מצליחים ליישב ביחד את שתי התיאוריות הגאוניות האלו. אבל כרגע, הבעיה המטרידה הזו לא רלוונטית לנו. אנחנו, כמו עולם המדע כולו, ניח לצורך המאמר שתורת הקוונטים היא התורה שמתארת את העולם הפיזיקלי בסקאלות יחסית קטנות.
בינתיים היא עושה זאת בהצלחה מרובה.

עיקרון הסופרפוזיציה: גם כאן וגם שם

העיקרון הראשון והחשוב ביותר בתורת הקוונטים הוא עיקרון ה"סופרפוזיציה". על-פי עיקרון מופלא זה, **אלקטרון ולמעשה כל חלקיק קוונטי, יכול להיות בכמה מקומות או בכמה מצבים בו־זמנית**. אם למערכת רגילה יש שני מצבים אפשריים (למשל "כאן" ו"שם", "דולק" ו"כבוי"), הרי שהמערכת הקוונטית יכולה להימצא בו־זמנית בשני המצבים. היא נמצאת במעין צירוף של שני מצבים אלו. ונא לא לבלבל: זה לא אומר שהיא בהסתברות מסוימת פה ובהסתברות מסוימת שם, ואנחנו פשוט לא יודעים. לא ולא. הכוונה היא שאכן, באותו הזמן, המערכת נמצאת במידה מסוימת במצב זה ובמידה מסוימת במצב אחר. הנורה היא בו־זמנית גם דולקת וגם כבויה. האלקטרון, אותו האלקטרון, עובר בו־זמנית דרך שני סדקים מרוחקים בקיר.

הפיזיקאים מתארים את צירוף האפשרויות הזה, הסופרפוזיציה, בעזרת פונקציה הנקראת פונקצית גל. ערך פונקציית הגל של האלקטרון במקום מסוים הינו מספר, המתאר את מידת היותו של האלקטרון במקום זה. מיקומו של האלקטרון מיוצג על-ידי פונקציית הגל כולה ואינו מרוכז בהכרח במקום אחד.

איך אפשר להבין אינטואיטיבית את עיקרון הסופרפוזיציה? ריצ'רד פיינמן (Richard Feynman), אחד מגדולי הפיזיקאים המודרניים, אמר: **"אני חושב שאני יכול לומר בבטחה שאף אחד אינו מבין את תורת הקוונטים"** (תרגום חופשי). אני משערת שהוא התכוון במיוחד לעיקרון הסופרפוזיציה. עיקרון זה נוגד את האינטואיציה הבסיסית שלנו. למי שגדל בעולם שלנו, עולם עם חוקים פיזיקליים ברורים, שבהם מערכת היא או "פה" או "שם", ואף פעם לא גם פה וגם שם, יהיה קשה מאוד להתרגל לעיקרון הסופרפוזיציה. אבל זו בדיוק הנקודה: לחוקים פיזיקליים אפשר רק להתרגל או לא להתרגל. אין להם בעצם הסבר "הגיוני". אחרת הם לא היו חוקים, אלא מסקנות לוגיות מחוקים אחרים. הרי גם כוח הגרביטציה שכולנו מקבלים כמובן מאליו אינו באמת "הגיוני". למה, בעצם, ששני גופים בעלי מסה ימשכו זה את זה? אנחנו פשוט התרגלנו לחוק הגרביטציה כי אנחנו רואים מדי יום ביומו עצמים נופלים.

ומדוע בעצם, לא התרגלנו לחוק הסופרפוזיציה, שגם הוא חוק טבע בעולמנו? ההסבר הוא שחוק זה שולט בעולם בסקאלות קטנות במיוחד (אטומיות), ואינו מורגש בסקאלות שבהן פועלים בני אדם בדרך כלל. הרי

אנחנו לא רואים את החברים שלנו כפול (אם לא שתינו יותר מדי). על-פי תורת הקוונטים, פונקציית הגל של אדם, או של עצמים גדולים אחרים, גם היא "מרוחה", קצת פה וקצת שם, אבל במידה כליך מועטה, שלא ניתן להבחין בכך כלל. מכל בחינה שהיא, ניתן לומר שפונקציית הגל של עצמים גדולים כמונו מרוכזת לגמרי באופציה אחת מתוך שלל המקומות האפשריים. יש לתורת הקוונטים הסבר מדוע במערכות גדולות עיקרון הסופרפוזיציה פחות ופחות נראה לעין. אסביר זאת לקראת סוף המאמר.
כעת, הבה נבדוק מה ההשלכות של עיקרון הסופרפוזיציה בסקאלות קטנות, למשל בסקאלה של האלקטרון. אם האלקטרון נמצא בו־זמנית בכל המקומות, האם יש משמעות כלשהי לשאלה מהו מיקומו של האלקטרון? איך בכלל אפשר לקבל מידע על מיקום האלקטרון, אם זה אינו קבוע ומוחלט?

עיקרון המדידה: לא פה ולא שם

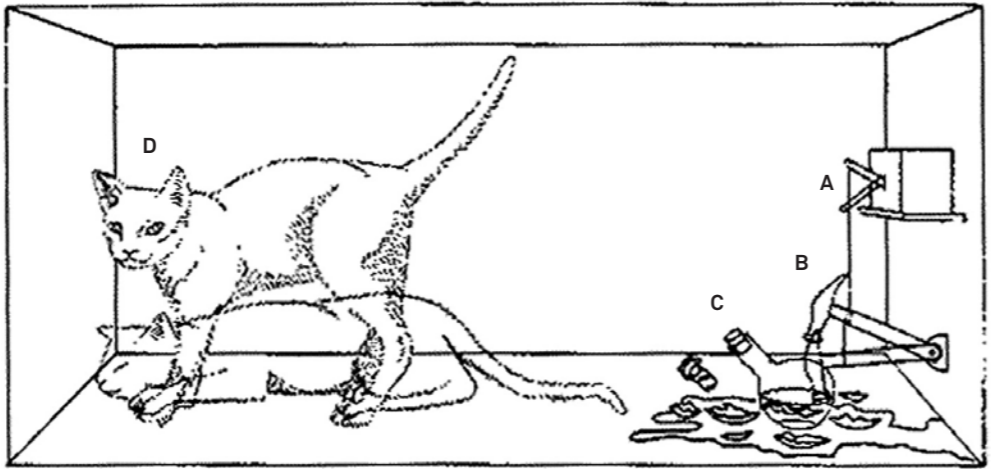
העיקרון השני החשוב של תורת הקוונטים הוא עיקרון המדידה, שקובע שתוצאת המדידה של מיקום אלקטרון שפונקציית הגל שלו "מרוחה", היא הסתברותית. לא ניתן לחזות את התוצאה גם אם יהיו בידינו כל הנתונים על מצבו של האלקטרון, כלומר נדע במדויק את פונקציית הגל שלו. אם למשל נבצע מדידה שתבדוק באיזה משני צידיו של חלקיק מסוים ממוקם האלקטרון, הרי שהוא יימצא בצד אחד בהסתברות מסוימת שתלויה בערכה של פונקציית הגל באזור זה, ובצד השני בהסתברות המשלימה. תוצאת המדידה היא הסתברותית - היא אינה ניתנת לחיזוי.

מעבר לכך, ניח שמדדנו ומצאנו את האלקטרון מימין. במקרה זה, על-פי עיקרון המדידה, קורסת פונקציית הגל של האלקטרון בבת־אחת

"העיקרון הראשון והחשוב ביותר בתורת הקוונטים הוא עיקרון ה"סופרפוזיציה". על פי עיקרון מופלא זה, אלקטרון ולמעשה כל חלקיק קוונטי, יכול להיות בכמה מקומות או בכמה מצבים בו זמנית. אם למערכת רגילה יש שני מצבים אפשריים ולמשל "כאן" ו"שם", "דולק" ו"כבוי", אז המערכת הקוונטית יכולה להימצא בו-זמנית בשני המצבים. היא נמצאת במעין צירוף של שני מצבים אלו"

(תוך כדי תהליך המדידה) לפונקציית גל שמרוכזת בצד ימין. **המדידה עצמה משנה את פונקציית הגל, ובעצם את מיקומו של החלקיק**. זוהי התנהגות שונה לחלוטין מכל המוכר לנו מעולם הפיזיקה הקלאסית: הצופה - מעצם העובדה שהוא צופה - משנה את מה שהוא צופה בו. לפי תורת הקוונטים, אין דרך להתבונן בעולם מבלי לשנות אותו.

כמו עיקרון הסופרפוזיציה, גם עיקרון המדידה נוגד את כל מה שאנחנו חווים בחיי היומיום. בואו נבחן הטלת מטבע על־מנת להבין זאת טוב יותר. בהטלת מטבע "הוגן", אנחנו אומרים שיש סיכוי "חצי־חצי" לעץ או פלי. אבל לו היינו יודעים את כל תנאי ההתחלה - זווית הזריקה המדויקת, משקלו



המדויק של המטבע, כיווני הרוח וכו' - היינו יכולים לחזות את התנועה שיעשה המטבע באוויר, ולכן גם לחזות במדויק על איזה צד ייפול. המחסור בנתונים הוא זה שמיתרגם לאי ודאות וגורם לנו לומר שהתוצאה היא הסתברותית. באופן עקרוני, תהליך זריקת המטבע ניתן לחיזוי מדויק לו היו בידינו כל הנתונים.

אלא שעל־פי תורת הקוונטים, מצב האלקטרון שונה לחלוטין. לא מדובר כאן במחסור בנתונים, אלא בכך שמיקומו המדויק של האלקטרון אינו קיים למעשה, לפני שהוא נמדד. אין, בעצם, מציאות מוחלטת. זה לא שהאלקטרון נמצא באמת באחד משני המקומות, ואנחנו לא יודעים מספיק על־מנת לקבוע איפה. לא, האלקטרון הוא גם כאן וגם שם בו־זמנית, ורק עם המדידה הוא קורס באופן הסתברותי לאחד משני המצבים.

אם הרעיון הזה מפריע לכם, אתם בחברה טובה. אלברט איינשטיין כתב בשנת 1926 למקס בורן (Max Born): **"תיאוריית מכניקת הקוונטים אומרת הרבה, אך אינה מקרבת אותנו בעצם אל סודו של ה'זקן'. אני, מכל מקום, משוכנע שהוא לא משחק בקוביות."** עד סוף ימיו (איינשטיין נפטר ב־1955) הוא האמין שתורת הקוונטים למרות הצלחותיה מספקת הסבר חלקי בלבד. איינשטיין סבר שאם הפיזיקאים יתאמצו מספיק, תימצא תיאוריה שמתארת את הטבע בעזרת משתנים שכרגע הם חבויים מעינינו - משתנים שלו היינו יודעים מה ערכם, היינו יכולים לנבא את תוצאות כל המדידות בוודאות, וללא צורך בהסתברות. תורת **משתנים חבויים** שכזו תשחזר את הביטחון האהוב של הפיזיקה הקלאסית במציאות שרירה וקיימת.

איינשטיין טעה. בשנות ה־60 תיאר הפיזיקאי ג'ון בל (John Bell) ניסוי שמאפשר להכריע בשאלה האם תיתכן תורה פיזיקלית המתבססת על משתנים חבויים, שתחליף את תורת הקוונטים. בניסוי מפורסם שערך הניסיונאי אלן אספק (Alain Aspect) בתחילת שנות ה־80, נבדקה הצעת הניסוי של בל. התוצאה היתה: אף תורת משתנים חבויים, תהא מתוחכמת ככל שתהא, אינה יכולה להסביר את תוצאות הניסויים הפיזיקליים שראה אספק במעבדתו (במסגרת תוכלו לראות תיאור של משחק שמתבסס על הניסוי של בל, ומסביר כיצד ניתן לשלול קיום תיאוריה של משתנים חבויים

איך יכול חתול להיות גם מת וגם חי? ב-1935 תיאר הפיזיקאי ארוין שרדינגר את הניסוי שבתמונה, בניסיון להדגיש את הפרדוקסליות בתורת הקוונטים. (כמובן, זהו ניסוי דמיוני, ואף אחד לא חושב לבצע אותו!). הפוטון לפי תורת הקוונטים נמצא בסופרפוזיציה של פוגע ולא פוגע במונה הגייגר; כתוצאה מכך, הפטיש מכה ולא מכה בו זמנית בבקבוק הרעל, והחתול, (ותיאורטית, אם הוא מבודד לגמרי מהסביבה, מה שבלתי אפשרי כמובן) הוא חי ומת בו-זמנית, כל עוד לא פותחים את הקופסא ובדוקים את מצבו, כלומר כל עוד לא מבצעים מדידה.

ומה הקשר בין תורת הקוונטים לחיינו?

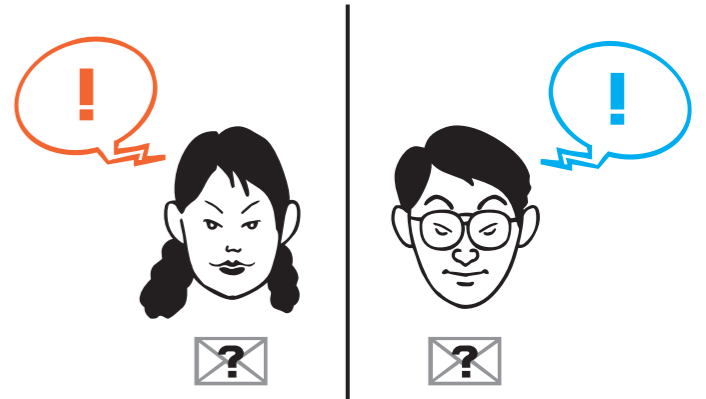
בעזרת ניסוי פיזיקלי). המסקנה היא שלא נוכל לוותר על אי־הוודאות ההסתברותית הקיימת בתורת הקוונטים. ככל הנראה, ניאלץ כולנו לוותר דווקא על הרעיון נוסך הביטחון, שעליו חלם איינשטיין, של מציאות מוחלטת ובת־חיזוי בטבע וביקום.

ומה הקשר בין תורת הקוונטים לחיינו?

השפעת תורת הקוונטים על הפילוסופיה של המדע היא כמובן עצומה. רעיונות כאלו - לא נשמעו כמותם! הם נוגעים בשאלות כמו מה היא מציאות, מה היא ידיעה, איך ניתן להתקרב אל המציאות עצמה (ואל סודו של ה"זקן"), מה היא השפעת המתבונן על העולם, ועוד.

ומה עם עולם הפיזיקה? העקרונות המוזרים של תורת הקוונטים מסבירים תופעות רבות ברמה המיקרוסקופית. למשל, אם זורקים כדור על קיר בכוח חזק, הוא תמיד יחזור, אבל כשמדובר באלקטרונים, הם יכולים לעבור גם דרך קירות עבים, ולצאת מן הצד השני! תופעה זו נקראת מינהור קוונטי (מינהור - ממנהרה). או דוגמה נוספת, שהיא למעשה התופעה ההפוכה: אם מגלגלים כדור על שולחן, כשהוא יגיע לקצה השולחן הוא ייפול, אבל כשמדובר באלקטרונים, לאלקטרון יש סיכוי טוב לקפוץ אחורה כאילו היה מחסום בקצה השולחן! תופעות אלו ורבות אחרות נצפו אינספור פעמים במעבדה, ותורת הקוונטים יכולה להסביר אותם ואף לנבא את התנהגותם.

האם תופעות קוונטיות נוכחות גם מחוץ למעבדה, בחיי היומיום שלנו? הרי כליך קשה לראות תופעות קוונטיות בסקאלות גדולות! מתברר שתופעות רבות סביבנו ניתנות להסבר אך ורק באמצעות תורת הקוונטים. למשל, העובדה המופלאה שהעולם אינו קורס לנקודה אחת בודדת. הרי זה מה שהיה אמור לקרות כתוצאה מכוח המשיכה בין האלקטרונים בעלי המטען השלילי והפרוטונים בעלי המטען החיובי. תורת הקוונטים מספקת לכך הסבר, שלא נפרטו כאן. גם את צבעי הקשת ניתן להסביר רק בעזרת



<p> </p>	אליס	0	1
בוב		0,0	0,1
		1,0	1,1

"המשחק של בל"

שני שחקנים, אליס ובוב, משחקים את המשחק הבא. כל אחד מהם יקבל ביט מקרי: 0 או 1, שהשני לא ידע מה הוא. מרגע קבלת הביטים אסור יהיה להם לדבר. כל אחד מהם צריך להגיד צבע, אדום או כחול. הכללים לפיהם הם מנצחים תלויים בביטים שהם קיבלו: אם שניהם קיבלו את הביט 1, הם מנצחים אם הצבעים שלהם זהים. אחרת, הם מנצחים אם הצבעים שלהם שונים. מטרתם כמובן לנצח בהסתברות הטובה ביותר! כל אחת מהאפשרויות בטבלה מתקבלת בהסתברות שווה, כלומר רבע. קל לבדוק שאם אליס תמיד תגיד אדום, ובוב תמיד כחול (כלי תלות בביט שכל אחד מהם קיבל), הם ינצחו בשלושה מתוך ארבעה מקרים, כלומר, בהסתברות 0.75. מסתבר שלא משנה כמה מתוחכמת תהיה האסטרטגיה שלהם, הם אינם יכולים לנצח בסיכוי גדול מזה. אבל אם אליס ובוב מכינים מראש מצב קוונטי של שני קיוביטים בסופרפוזיציה, וכל אחד מהם לוקח איתו קיוביט בודד, הם יכולים מבלי לדבר ביניהם להשתמש בקיוביטים שלהם בכמעין "תקשורת קוונטית" ולנצח בהסתברות גבוהה הרבה יותר! הניסוי של אספקט לשלילת האפשרות של תיאורית משתנים חבויים, ניתן למעשה להצגה כמשחק זה, כאשר מכשירי המדידה מייצגים את אליס ואת בוב. במעבדה התקבלו התאמות גבוהות משמעותיות מכל מה שניתן להסביר בעזרת אסטרטגיה קלאסית כלשהי, כלומר בעזרת תורת משתנים חבויים.

תורת הקוונטים, כמו גם את הבדלי הצבעים החדים בין חלקיה השונים של שלהבת הנר, ועוד כהנה וכהנה.

השפעת תורת הקוונטים על חיינו חורגת בהרבה מעבר להסברן של תופעות קיימות. תורת הקוונטים אחראית במידה רבה לשינויים הטכנולוגיים וההיסטוריים של המאה ה־20. השימוש הרה־האסון והמוכר ביותר שהאנושות בחרה לעשות בתורת הקוונטים הוא פיתוח פצצת האטום. אולם האנושות השתמשה מאז בתורת הקוונטים בדרכים רבות אחרות, פחות מוכרות, אך מאוד משמעותיות. גודלו של המחשב הראשון היה כשל חדר ומשקלו היה

13 טון, והוא שימש מדינות; מה שאיפשר את הפיכת המחשב לנגיש לכל (ואת השינוי הגדול בחיים המודרניים כתוצאה ממהפכת המיחשוב) היה המצאת הטרנזיסטור. התופעה העיקרית עליה מתבסס הטרנזיסטור היא מינהור קוונטי. עולם הטכנולוגיה והתקשורת המודרני נשען כמעט לחלוטין על תגליות שמתבססות על תופעות קוונטיות. מחשבים אישיים, טלוויזיות, טלפונים סלולריים ואינטרנט לא היו קיימים לולא המצאות המתבססות על תורת הקוונטים. גם פרויקט הגנום האנושי לא היה קיים, וכן רוב רובו של מדע הביולוגיה המודרנית, וכמובן גם אינסוף מכשירים רפואיים מתקדמים. בעצם לא ניתן לדמיין את העולם המודרני ללא תגליות המתבססות על תורת הקוונטים.

על אף כל הטכנולוגיות הרבות שהשתנו בעקבות תורת הקוונטים, דבר אחד לא השתנה, זו הדרך שבה מאוחסן ומעובד המידע בכל אחת מהטכנולוגיות הללו. עם כל השינויים והשכלולים שעברו המחשבים וכל מוצרי הלוואי שלהם, הרעיון שעומד בבסיס תהליך החישוב נשאר כשהיה. זה מה שישתנה לחלוטין במחשב הקוונטי.

<p> </p>	אליס	0	1
בוב		0,0	0,1
		1,0	1,1

כל תהליכי עיבוד האינפורמציה שאנו מכירים (כגון חיפוש מידע באינטרנט, חיזוי מזג האוויר בעזרת מחשב, קריאת כרטיס האשראי עליידי הכספומט ועוד) ניתנים לתיאור בעזרת רעיון מאוד פשוט: המידע מקודד באמצעות אפסים ואחדות, שנקראים **ביטים**. ייצוג האפסים והאחדות יכול להיות בעזרת נורות דולקות או כבויות (כפי שזה היה במחשבים ישנים) או בעזרת זרמים או מתחים שונים (כפי שזה במחשבים של היום), אבל מה שחשוב זה לא הייצוג הפיזיקלי, אלא המידע המקודד. מידע זה ניתן לעיבוד עליידי הפעלת פעולות פשוטות ("שערים לוגיים" כגון AND ו־NOT) מספר רב של פעמים בזו אחר זו, לפי סדר שמוכתב עליידי התוכנה, כלומר האלגוריתם.

אחת השאלות שמאוד מעניינות מדעני מחשב ומדענים בכלל היא: מהו זמן החישוב הנדרש על־מנת לבצע תהליך עיבוד מידע כלשהו. ניקח למשל את הבעיה הבאה: מזכירות האוניברסיטה העברית מתכננת את מערכת השעות לשנת הלימודים הבאה. יש כמובן אילוצים רבים: ישנם קורסים רבים שאסור שיהיו חופפים, יש אילוצים שמוכתבים ממספר האולמות וממספר התלמידים בחוגים השונים. האוניברסיטה רוצה להרכיב את מערכת השעות האופטימלית - זו שעונה על מספר מקסימלי של אילוצים. למרות שהבעיה אינה עוסקת במספרים, זוהי בעיה חישובית. ניתן כמובן לתכנת תוכנית מחשב שתבדוק את כל מערכות השעות האפשריות ותמצא את זו האופטימלית. האם זהו חישוב שמחשב יכול לבצע בזמן סביר? האם מדובר בשניות? בדקות? אולי בשעות?

על־מנת לבדוק זאת, נוכל למשל להריץ את תוכנית המחשב עם חלק קטן מהקורסים לשם ניסיון. ניח שהתוכנית מסיימת את החישוב תוך שתי שניות. האם נוכל להסיק מכך משהו לגבי זמן החישוב האמיתי? וניח שזמן החישוב האמיתי (כשכוללים את כל הקורסים) הוא שעה וחצי. האם נוכל להסיק מכך כמה זמן ייארך החישוב אם נרצה לשנות קצת את הנתונים,

למשל להוסיף קורס חדש? נראה שהתשובה על השאלה "כמה זמן ייארך חישוב מסוים" בכל אחד מהמקרים אינה נותנת מידע משמעותי, אלא אוסף מספרים שאינם נראים קשורים זה לזה.

אחד הצעדים החשובים ביותר במדעי המחשב, צעד שהפך את מדעי המחשב מאוסף של שאלות ותשובות לתיאוריה מדעית, נעשה בשנות ה־60 עליידי ג'ק אדמונדס (Jack Edmonds). אדמונדס הציע להחליף את השאלה "כמה זמן נמשך חישוב מסוים" בשאלה "כיצד משתנה או **מתנהג** מספר פעולות החישוב כאשר מגדלים את מספר הנתונים". כמו במקרים רבים במדע, עצם הצגת השאלה הנכונה היווה פריצת דרך - התיאוריה של מדעי המחשב כיום מבוססת כולה על שאלה זו. בדוגמה שהבאנו, ניתן לנסח את השאלה של אדמונדס באופן הבא: איך משתנה זמן חישוב מערכת השעות האופטימלית כאשר מוסיפים לתוכנית הלימודים קורס נוסף?

<p> </p>	אליס	0	1
בוב		0,0	0,1
		1,0	1,1

יש בעיות שעבורן כל נתון נוסף מגדיל את זמן החישוב בפעולה אחת או במספר קבוע של פעולות, ולעומתן יש בעיות שעבורן כל נתון נוסף מכפיל את זמן החישוב פי מספר קבוע, למשל פי שתיים. עבור מי שאינו בקי בחישובים ובמספרים, ההבדל בין שתי ההתנהגויות נראה זניח ולא מעניין, זהה אכן כך כשמדובר במספר קטן של נתונים. אבל כשמדובר בכמה עשרות נתונים או יותר, ההבדל הוא עצום. התנהגות מהסוג השני, לפיה כל נתון נוסף מכפיל את זמן החישוב פי שתיים, נקראת "גידול אקספוננציאלי". זהו גידול הדומה למהירות ההתרבות של חיידקים: מספר קטן יחסית (כמה עשרות) של שלבים של גידול אקספוננציאלי מוביל למספרים אסטרונומיים.

"מחשבים קוונטים הם המודל החישובי היחיד הידוע לנו, שנראה כאילו אינו מציית לתיזה המודרנית של צ'רץ' וטירינג. חישוב קוונטי הוא כנראה מודל שונה איכותית מכל מודל חישוב אחר שאנו מכירים. נראה כאילו מחשבים קוונטיים יכולים לחשב ביעילות לא רק בעיות "קלות" למחשבים רגילים, אלא גם בעיות שחשבנו אותן כ"קשות" לחישוב"

בעיות שזמן חישובן גדל במספר קבוע עם כל נתון נוסף נחשבות במדעי המחשב לבעיות שניתנות לפיתרון בזמן סביר, ומתייחסים אליהן כבעיות "קלות". בעיות מהסוג השני, שכל נתון מכפיל עבורן את זמן החישוב, הן בעיות "קשות" שזמן חישובן אקספוננציאלי. אולי תופתעו, אבל בעיית תכנון מערכת השעות היא מהסוג השני, זמן חישובה הוא אקספוננציאלי. בתוכנית לימודים ובה רק מאה קורסים נגיע למספר אסטרונומי של פעולות חישוב נדרשות: שתיים בחזקת 100. זהו מספר גדול בהרבה ממספר החלקיקים המוערך ביקום כולו! אם נזין את הבעיה למחשב, נחכה לא שעות ואפילו לא ימים: יהיה עלינו לחכות זמן ארוך יותר ממשך חייו של היקום.

כעת אנו מגיעים לאחת מאבני היסוד החשובות ביותר בתיאוריה של מדעי המחשב: התיזה המודרנית של צ'רץ' וטירינג. תיזה זו דנה בסיווג של בעיות חישוב לבעיות קלות ולבעיות קשות. על־פי התיזה, סיווג זה אינו תלוי בדגם המחשב שבו משתמשים לפיתרון הבעיה. למשל, בעיית מציאת מערכת השעות האופטימלית תהיה קשה בכל המחשבים; בעיות אחרות תהיינה קלות בכולם. על־פי התיזה, אין הבדל עקרוני, מהותי, אם מנסים לפתור בעיה בעזרת חשבונייט חרוזים, מחשב ביתי, או המחשב של נאס"א (למרות שכמובן מעשית יש הבדלים). הרעיון הוא שאם בעיה היא קשה, אזי גם אם נצליח לפתח מחשב מהיר בהרבה עם מעבד משוכלל בהרבה - נוכל רק להגדיל במעט את מספר הנתונים שנצליח לפתור עבורם את הבעיה, אך מהר מאוד יגיע גם המחשב החדש לקצה גבול יכולתו. גם אם נתאמץ מאוד לשפר את המעבדים והצי"פים מהם מורכב המחשב, בעיות קשות עדיין תהיינה קשות.

<p> </p>	אליס	0	1
בוב		0,0	0,1
		1,0	1,1

בשנת 1994 גילה פיטר שור (Peter Shor) - אז חוקר ב־IBM - תגלית מרעישה: מתברר שבעיית פירוק מספר שלם לגורמיו הראשוניים, בעיה שמתמטיקאים חשבו לבעיה קשה במשך מאות שנים, ניתנת לפתרון יעיל בעזרת מחשב קוונטי! העולם המדעי, על כל רבדיו, רעש.

מדוע אלגוריתם הפותר בעיה מתמטית שנראית תמימה לגמרי הוא חשוב כל־כך? מה כל־כך מעניין בפירוק של מספר לגורמים? הסיבה לעניין הרב בתגלית של שור קשורה לשיטת הצפנת המידע הנקראת RSA, הנפוצה בכל העולם. בטיחותה של שיטה זו מבוססת לחלוטין על ההנחה שפירוק מספרים לגורמים הוא בעיה קשה. והנה, מהאלגוריתם של שור נובע: לו היה בידינו מחשב קוונטי, היה ניתן לפתור את בעיית הפירוק לגורמים ביעילות, ומכאן, לפצח ולפענח את כל ההצפנות המבוססות עליה. זוהי מחשבה שערורייתית: לו היו קיימים מחשבים קוונטיים, ניתן היה לקרוא סודות מדינה, תקשורת בין בנקים ללקוחותיהם ועוד. ברור לכן מדוע תגליתו של שור עוררה עניין רב בבניית מחשב קוונטי בקרב הממשל האמריקני וגורמים נוספים.

התובנה הראשונה בעקבות האלגוריתם של שור היא:

שיטות ההצפנה הנפוצות אינן בטוחות בפני מחשבים

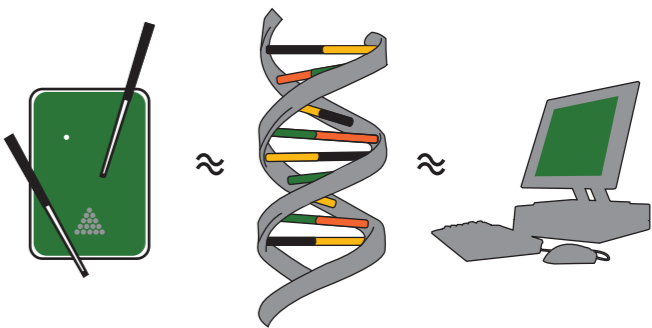
קוונטיים. האם ניתן לבנות מחשב קוונטי ולקרוא בעזרתו

את כל הסודות שנכתבו בעשרות השנים האחרונות? והאם

יש בעולם הצפנה בטוחה לגמרי?

ישנה סיבה נוספת וחשובה לא פחות להתעניין בתגלית המרעישה: האלגוריתם של שור מצביע על כך שמחשבים קוונטים הם המודל החישובי היחיד הידוע לנו, שנראה כאילו אינו מציית לתיזה המודרנית של צ'רץ' וטירינג. חישוב קוונטי הוא כנראה מודל שונה איכותית מכל מודל חישוב אחר שאנו מכירים. נראה כאילו מחשבים קוונטיים יכולים לחשב ביעילות לא רק בעיות "קלות" למחשבים רגילים, אלא גם בעיות מסוימות שאנו חושבים כ"קשות" לחישוב.

זוהי התבונה השנייה בעקבות האלגוריתם של שור:
התיזה המודרנית של צ'רץ' וטיורינג נראית לנו היום מוטלת בספק רב. מחשב קוונטי יוכל לפתור את בעיית הפירוק לגורמים, הנחשבת לבעיה קשה עבור מחשבים רגילים. אלו בעיות קשות נוספות ניתנת לפיתרון ביעילות אם נצליח לבנות מחשב קוונטי?



על פי התיזה המודרנית של צ'רץ' וטיורינג:
 כל מדולי החישוב בתמונה שקולים מבחינת השאלה אילו בעיות חישוב הן קלות עבורן ואילו הן בעיות קשות, כאלו שזמן החישוב שלהן גדל אקספוננציאלית.

מביטים רגילים לביטים קוונטיים

במחשב קוונטי, יוחלפו הביטים הרגילים ב"ביטים קוונטיים" ונקרא להם קיוביטים. קיוביט יכול להיות כל מערכת פיזיקלית (אלקטרון, פוטון ועוד) שיכולה להיות בשני מצבים, 0 או 1, כמו ביט רגיל. אבל בהבדל מביטים רגילים, קיוביט יכול להימצא גם בסופרפוזיציה של 0 ו1.

ומה קורה כשהיו לנו הרבה קיוביטים ביחד? לשני קיוביטים יש ארבע שרשרות ביטים אפשריות (00, 01, 10, 11), לשלושה חלקיקים יש שמונה (000, 001, 010, 101, 110, 111). כל חלקיק נוסף מכפיל את מספר האפשרויות פי שניים, ולכן למאה חלקיקים יש שתיים בחזקת מאה שרשרות ביטים אפשריות! פגשנו כבר את הגודל העצום הזה.... זהו גידול אקספוננציאלי במספר האפשרויות. לפי עיקרון הסופרפוזיציה, מערכת קוונטית נמצאת בצירוף של כל השרשרות האפשריות. מערכת של מאה חלקיקים הינה מערכת פיזיקלית קטנה מאוד יחסית - אבל מספר האפשרויות שהיא נמצאת בהן בוז'מנית גדול ממספר החלקיקים המוערך ביקום כולו! פונקציית הגל של מערכת זו מפוזרת על פני מספר כמעט אינסופי של אפשרויות.

קשה מאוד להבין קונספטואלית איך יתכן שלמערכת קטנה של מאה חלקיקים יש תיאור כה מסובך ומורכב. היכן שומר הטבע את כל המידע הזה? כיצד הוא מעדכן אותו כשהמערכת משתנה עם הזמן? זהו פלא שהוא

מעל להבנתנו. אולם כיום זהו התיאור היחיד שאנחנו מכירים למערכות קוונטיות. גידול אקספוננציאלי זה במספר האפשרויות שמערכת קוונטית יכולה להימצא בהן בוז'מנית הוא האחראי לכוח החישוב העצום של מחשבים קוונטיים.

אלגוריתמים קוונטיים

כדי לתאר מהו אלגוריתם קוונטי עלינו להבהיר לא רק מה הן הסופרפוזיציות המתארות את מצב הקיוביטים, אלא גם מה הן פעולות החישוב האלמנטריות שבהן אנו יכולים להשתמש: השערים הלוגיים הקוונטיים. מבלי להיכנס להסבר מפורט, השערים הקוונטיים שמשמשים בהם באלגוריתמים קוונטיים דומים מאוד לשערי AND ו-NOT. אלא שבמחשב קוונטי נצטרך להשתמש בשער נוסף, שיעביר קיוביט ממצב 0 או 1 למצב של סופרפוזיציה. כך נוכל ליצור סופרפוזיציות מורכבות כרצוננו. המימוש הפיזיקלי המדויק של השערים הקוונטיים (לדוגמה, על-ידי הפעלת קרן לייזר, או הפעלת שדה מגנטי למשך זמן מסוים) אינו משנה לענייננו.

החישוב הקוונטי מתחיל בכך שכל הקיוביטים הם במצב 0 או 1. כעת מפעילים על הקיוביטים את רצף השערים הקוונטיים, על-פי האלגוריתם הקוונטי. לדוגמה, אם יש לנו מחשב בן שישה קיוביטים שמאותחלים כולם ל-0, המצב ההתחלתי של המערכת הוא 000000. אם השער הראשון באלגוריתם פועל על הקיוביט השמאלי והופך אותו לסופרפוזיציה של 0 ו1, אזי לאחר הפעלת השער יימצא המחשב כולו בסופרפוזיציה של שני מצבים: 000000 ו100000. עם הפעלת עוד ועוד שערים, הולכות ומשתתפות בסופרפוזיציה יותר ויותר שרשרות אפשריות של שישה ביטים. בסופו של דבר, כאשר סיימנו לבצע את סדרת הפעולות על-פי האלגוריתם, מתבצעת מדידה. בכך קורס המצב לאחת משרשרות הביטים האפשריות, ושרשרת זו היא תוצאת החישוב.

חישוב קוונטי - היתרונות

מחשב קוונטי יכול להימצא בסופרפוזיציה של מספר עצום (אקספוננציאלי) של שרשרות ביטים אפשריות. ניתן לחשוב על תהליך החישוב הקוונטי כאילו הוא מעין סופרפוזיציה של מספר עצום של חישובים אפשריים - מחשב עם מקביליות אקספוננציאלית. זה נשמע נהדר, אבל זה לא כל-כך פשוט. זוכרים את עיקרון המדידה? בסופו של החישוב, עלינו למדוד את המערכת, ואז המצב קורס לאחד מתוך המספר העצום של החישובים האפשריים, וכל המקביליות האקספוננציאלית שעליה היתה תקוותנו נעלמה כלא היתה.

כאן בא לעזרתנו אפקט קוונטי ידוע, שעליו טרם דיברנו: אפקט ההתאבכות. כל מי שאוהב מים יודע מהי התאבכות גלים! זוהי התופעה שבה מבטלים הגלים אלה את אלה (התאבכות הורסת), או להיפך - מצטרפים אלה לאלה ליצירת גל גדול (התאבכות בונה). לא לחינם נקראת

הסופרפוזיציה גם "פונקציית גל". ניתן להתייחס לחישובים השונים בסופרפוזיציה כגלים. חישובים אלו יכולים לבטל את אלה או להתווסף אלה לאלה (בדיוק כמו גלים), כאשר מפעילים עליהם שערים קוונטיים מתאימים. האלגוריתם הקוונטי מתוכנן כך שהתשובות שאינן נכונות יבטלו אלו את אלו בעזרת התאבכות הורסת, והסופרפוזיציה הסופית תתאחד לכדי התשובה הנכונה. זה בדיוק מה שפיטר שור עשה באלגוריתם שלו לפירוק מספר לגורמיו.

מאז התגלית של שור, נמצאו מספר בעיות חישוב קשות נוספות שניתן להאיץ את פיתרון באופן דרמטי בעזרת חישוב קוונטי. אולם עבור רוב בעיות החישוב עדיין לא ידוע יתרון משמעותי לשימוש במחשב הקוונטי על פני מחשב רגיל. אם נודה על האמת, אנחנו ממש לא מבינים עדיין מה הם גבולות כוח החישוב של מערכות קוונטיות. ככל הנראה, אנחנו רואים כיום רק את קצה הקרחון של האפשרויות שתהיינה פתוחות בפנינו.

תיקון שגיאות קוונטי

מדוע, 14 שנה אחרי התגלית של שור, אין עדיין מחשבים קוונטיים על שולחנו? הסיבה העיקרית היא זו שדנו בה בתחילת המאמר - מערכות גדולות אינן מתנהגות בדרך כלל בצורה קוונטית. מחשבים קוונטיים, אם וכאשר ייבנו, יצטרכו להוות דוגמה נגדית לתופעה זו. מה בעצם הבעיה במערכות קוונטיות גדולות? הרי חוקי תורת הקוונטים לא מפסיקים לפעול מעבר לגודל מסוים...

ההסבר נעוץ בתופעה הבאה. אי אפשר לבודד לחלוטין מערכת פיזיקלית מסביבתה. כל מערכת פיזיקלית תיאלץ לפעול תוך כדי אינטראקציות בינה לבין הסביבה. את האינטראקציות האלו נוכל לדמות למדידות שהסביבה מפעילה על המערכת, מדידות הגורמות לקריסת הסופרפוזיציה. מספיק שרק חלקיק אחד במערכת יימדד על-ידי הסביבה - וכל הסופרפוזיציה עלולה לקרוס. כשמדובר במערכת קטנה, קל יחסית לבודד אותה מהסביבה, אולם ככל שהמערכת יותר גדולה, הסיכוי שאף חלקיק לא יימדד הולך ושואף לאפס והסופרפוזיציה קורסת יותר ויותר תכופות.

ההסבר הזה מבהיר מדוע הפיזיקאים חשבו תחילה שלא ניתן יהיה לבנות מחשבים קוונטיים המורכבים ממספר רב של קיוביטים. למרבה ההפתעה נוכחו הפיזיקאים שניתן בעזרת פעולות תיאורטיים השאולים ממדעי המחשב ומתורת הקודים לקודד את המצב הקוונטי כך שגם אם יקרוס, ניתן יהיה לתקן אותו. כיום אנו יודעים שגם אם המערכת לא מבודדת לחלוטין מהסביבה, עדיין ניתן יהיה לבצע חישובים קוונטיים ארוכים כרצוננו, כל עוד נוכל להפחית את מידת האינטראקציה עם הסביבה אל מתחת לסף מסוים. זו הסיבה שהפיזיקאים אופטימיים יחסית לגבי האפשרות שמחשב קוונטי אכן ניתן למימוש: כרגע, נראה שזוהי אינה בעיה עקרונית אלא "רק" בעיה טכנולוגית.

בינתיים המחשב הקוונטי הגדול ביותר שניסוינים הצליחו לממש הוא בן עשרה קיוביטים ומסוגל לפרק את המספר 15 לגורמים. "גם מסע בן אלף מילין מתחיל בצעד קטן", אמר לאו טסה.

עולם בלי סודות?

מה יעלה בגורל שיטות ההצפנה בעקבות האלגוריתם של שור? האם מחשב קוונטי יהפוך את העולם למקום שאין בו סודות ואין בו פרטיות? התשובה, למרבה האירוניה, היא שקיימת שיטת הצפנה בטוחה לחלוטין אפילו בפני מחשבים קוונטיים: הצפנה קוונטית.

הרעיון כאן הוא גאוני בפשטותו. עיקרון המדידה מבטיח שלא ניתן לבצע מדידות בסתר: מדידה קוונטית תמיד משאירה עקבות, שכן היא משנה את מצב המערכת הנמדדת. שני משתתפים המעוניינים בתקשורת סודית, יתקשרו ביניהם בעזרת מישלוח פוטונים בסופרפוזיציות קוונטיות שונות זה לזה. הם יוכלו להפיל בפח מאזין בלתי רצוי ולגלות אותו, על ידי כך שיבחרו חלק מן הפוטונים באקראי, וישוו את מצבם לפני ואחרי המישלוח, על מנת לוודא שאף אחד לא ניסה למדוד אותם בדרך. המאזין הפוטנציאלי לא ידע מראש אלו פוטונים ייבדקו, וכך לא יוכל להתחמק מגילוי.

הצפנה קוונטית מהווה תחליף משופר להצפנה קלאסית, שכן היא בטוחה באופן מוחלט. יתרה מכך: היא אינה דורשת יצירת סופרפוזיציות מסובכות, אלא רק סופרפוזיציות של כל חלקיק בפני עצמו, ולכן היא יחסית פשוטה למימוש. למעשה, מערכות הצפנה קוונטית מוצעות כבר היום למכירה. אינני יודעת לשם מה משתמשים בהן. אף אחד לא מספר יותר מדי על שיטות ההצפנה שלו.

והעתיד?

האם אי פעם נראה מחשבים קוונטיים בפעולה? אין סיבה שלא. יש עשרות מעבדות שמונסות לבנות מחשב כזה, ולא נראה שיש סיבה פיזיקלית או אחרת שהן ייכשלו בסופו של דבר. אני מאמינה שהדברים שאנחנו יודעים כיום שניתן לעשות בעזרת חישוב קוונטי, הם כאין וכאפס לעומת מה שנגלה אם באמת יהיו מחשבים קוונטיים פועלים. כך קרה בכל מהפכה טכנולוגית: את השימושים האמיתיים קשה מאוד לצפות מראש.

אישית אני חושבת שיהיה הרבה יותר מעניין אם נגלה שלא ניתן לבנות מחשב קוונטי. כרגע אנחנו לא רואים שום סיבה פיזיקלית לכך, אבל בהחלט לא ניתן לשלול את האפשרות. יתכן שבשלב כלשהו, עם הגדלת המערכות במעבדה למאות ואפילו אלפי קיוביטים, יתגלה מכשול בלתי צפוי. יתכן שהמערכות החדשות יתנהגו בצורה שונה ממה שאנו חוזים. יתכן שתורת הקוונטים שוב תפתיע.

בעיני, תהיה זו התרומה היפה ביותר של תחום החישוב הקוונטי לעולם: אולי בכך שניכשל, נגלה את היסודות לפיזיקה חדשה. ■■■

dorit.aharonov@gmail.com