

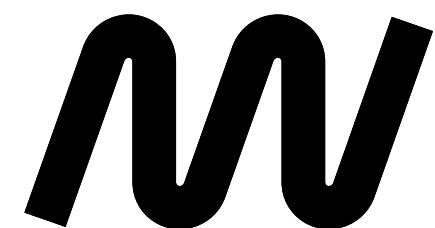


CAPTCHA
COMPLETELY AUTOMATED PUBLIC TURING TEST TO TELL COMPUTERS AND HUMANS APART
קאפצ'ה קابتשא

Bloomfield
Science Museum
Jerusalem

متحف العلوم
على اسم بلومفيلد
القدس

מוזיאון המדע
ע"ש בלומפילד
ירושלים



המחשב כמראה פילוסופית אל מול האדם

המחשב האלקטרוני הומצא לפני כמה עשרות שנים, ומאז חדר לכל תחומי חיינו בהיקף כה נרחב, עד ששכחנו לשאול את עצמנו מה משמעותו של המכשיר המופלא הזה, מה הבסיס המדעי שעליו הוא ניצב ומהי השפעת המחשב על החשיבה המדעית בהווה ובעתיד?

מי ששאל את עצמו את השאלות האלה היה אלן טיורינג (Mathison Turing Alan), המתמטיקאי האנגלי שחזה את המחשב כבר בשנת 1936 והבין כבר אז, לפני היות מחשבים בעולם, שהמחשב יהווה מראה שבאמצעותה נוכל לבחון את מהות המוח והתודעה שלנו. פריצת הדרך הפילוסופית הזו מציבה את מדעי המחשב בחזית המדע המודרני, ומאפשרת להם לטפל בבעיות מאתגרות ומרתקות.

שאלות מדהימות

תערוכת CAPTCHA בוחנת שאלות מרכזיות המצויות בבסיס מדעי המחשב, בכללן:

- מהם גבולות היכולת של המחשב, ומה הוא לעולם לא יוכל לחשב?
- האם המחשב יעבור אותנו בתבונתו, והאם יגיע אי פעם למודעות עצמית כמו של בני האדם?
- האם מחשב יכול להיות יצירתי?
- כיצד כל זה מעיד עלינו ועל מחשבתנו?

ישומים רבי עֶצְמָה

בד בבד עם העיסוק בשאלות העיוניות, ובהשראתן, עוסקים מדעני המחשב בפיתוח ישומים אשר להם השפעה אדירה על חיי כל אחד ואחת מאיתנו, למשל:

- שיטות הצפנה רבות עֶצְמָה שבלעדיהן לא היה אפשר לקיים את המסחר באינטרנט והבנקאות ברשת.
 - שיטות מחקר חדשות בכל תחומי הידע האנושי.
 - רשתות תקשורת חובקות עולם ששינו את פני החברה, הפוליטיקה והקשר שלנו עם הזולת.
 - מערכות רפואיות שמצילות חיי אדם מדי יום ביומו.
- מדינת ישראל היא מרכז חשוב במחקר ובפיתוח של כל אלה, והתערוכה מציגה את העושים במלאכה אצלנו.



האיש שחלם על מכונות חושבות

עקבותיו של אלן טיורינג שזורות כשתי וערב במסגרת התערוכה שלנו. פילוסוף וטכנולוג, מתמטיקאי ומפצח צפנים, הוגה ומיישם - פועלו של האיש שהניח בחייו הקצרים את יסודות מדעי המחשב, הטביע את חותמו בכל תחומי המדע שהקים. היה זה אדם מדהים שלא זכה בחייו לגמול ולהכרה הראויים לו. כעת, מאה שנה אחרי הולדתו, אתם יכולים להתוודע לאיש ולתרומתו לעולם של ימינו ולעולם המחר.



מה זה חישוב?

מהו מחשב?

מחשב הוא מכונה המעבדת נתונים שמוזנים לתוכה (קלט) ומפיקה תוצאות (פלט) על פי תכנית, כלומר על פי רצף פעולות נתון מראש. רוב המחשבים הם רב־תכליתיים - יכולים לבצע יותר מסוג אחד של עיבוד, משום שניתן להזין לתוכם תכניות שונות שמותאמות למשימות שונות. עם זה, יש מחשבים שמתוכננים לבצע רק משימה אחת. כל המחשבים היום הם אלקטרוניים וספרתיים (דיגיטליים), כלומר מבוססים על מעגלים משולבים חשמליים שמייצגים את הנתונים המעובדים כמספרים, ואת פקודות התכנה באופן דומה. עם זה, חשוב לזכור שאין הדבר הכרחי - בעבר נבנו מחשבים שפעלו בטכנולוגיות אחרות, למשל אלקטרו־מכניות, ובעתיד סביר שנראה מחשבים קוונטיים, ומי יכול לשער מה עוד?

אלגוריתם הוא מתכון המורה על סדרה של פעולות שביצוען יביא לפיתרון של בעיה נתונה. האלגוריתם מקבל קלט ומחזיר פלט. הבעיה אינה חייבת להיות בעיה מתמטית, ויכולה להיות קשורה לחיי היום־יום.



מה למשל?

בעיית הדרך הקצרה ביותר מהבית לבית הספר - לכל ילד יש בית ובית ספר (או גן ילדים). הקלט לבעיה הוא מפת הרחובות בעיר (ואורכיהם), וכן נקודת המוצא (הבית) ונקודת המטרה (בית הספר). אלגוריתם לפתרון הבעיה צריך לאפשר לכל ילד לחשב בצורה שיטתית את הדרך שבה עליו ללכת כדי להגיע ליעדו במסלול הקצר ביותר.

ומה עוד?

כֶּפֶל מספרים - כאן הקלט הוא שני מספרים שלמים (ארוכים ככל שנרצה). בכיתות היסוד אנחנו לומדים אלגוריתם לכפל המספרים. איננו מוגבלים באורכי המספרים, ומסוגלים תמיד לכפול ולהגיע לתוצאה הנכונה שהיא הפלט.

כדי להביא תועלת אלגוריתם צריך להיות יעיל - עליו להוביל אותנו אל התוצאה במהירות. אנשי מדעי המחשב מנסים כל העת לפתח אלגוריתמים יעילים ומהירים לפתרון בעיות, חלקן תאורטיות וחלקן מחיי היום־יום.

מקור המילה אלגוריתם הוא שמו של המתמטיקאי הפרסי בן המאה התשיעית, מוחמד אבן מוסא אל־ח'ואריזמי.

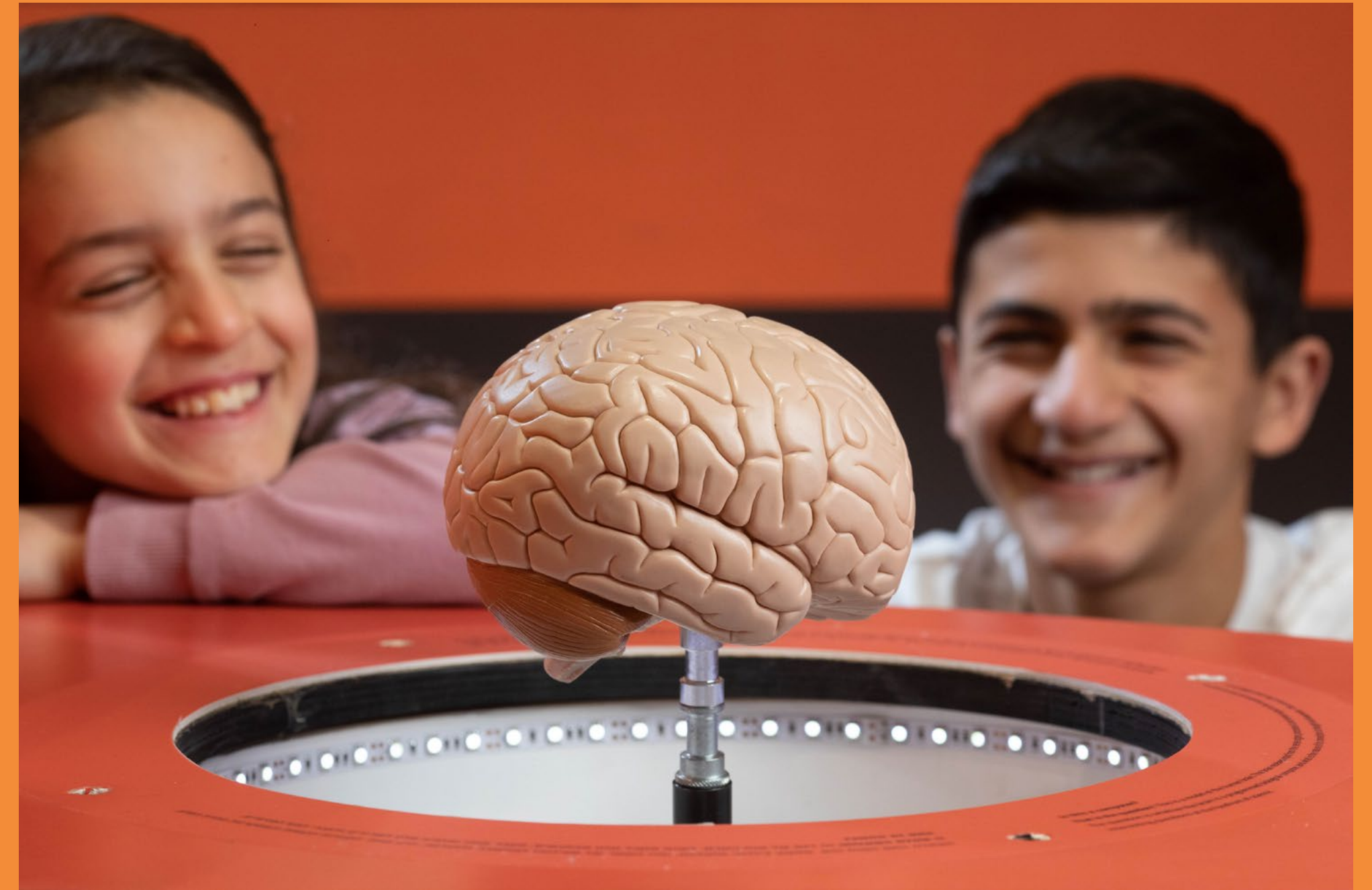
האם זה מחשב?

ברור שכן! זה מחשב. המחשב מקבל קלט מהמקלדת, העכבר והרשת, מעבד אותו בשבב המיקרו־מעבד שבתוכו לפי התכנית שמוזנת מהדיסק הקשיח לזיכרון שלו, ומציג את הפלט על המסך.

מחשב בקרת ירי מכני ששימש במלחמת העולם השניה לכוון טורפדות בצוללות. המחשב מקבל כקלט את הכוונים, המרחקים והמהירויות של הצוללת והמטרה, מעבד אותם ע"י מערכת סבוכה של גלגלים ותמסורות שמיישמים תכנית לחישובים טריגונומטריים, ומכוון בפלט את הטורפדו כך שיגיע ליעדו.

מד אור של צלם מאמצע המאה ה־20, שהוא סוג של מחשב פשוט. המכשיר מקבל כקלט את עצמת האור שהוא מודד בתא הפוטו־וולטאי שמותקן בו ואת סוג הפילם שהצלם מזין לחוגות שעליו, מעבד אותם במעגל אלקטרו־מכני ומציג בפלט את כוון החשיפה המתאים לקבלת תמונה מיטבית.

מכשיר שמיעה דיגיטלי חדיש. המכשיר מבוסס על מחשב זעיר שמקבל כקלט את עצמת הקול הנקלט במיקרופון שבצידו האחד, מעבד אותו בשבב שתוכנת לתקן במדויק את ליקוי השמיעה של בעל המכשיר, ומשמיע כפלט את הצליל המתוקן באזניה שבצידו השני.



מחשב (ABS) מערכת למניעת נעילה בבלימה – ANTI-LOCK BRAKING SYSTEM) של מכונית. המחשב מקבל בקלט אותות מחיישנים בגלגלי הרכב, ואם הוא מבחין שהרכב מחליק הוא מוציא בפלט אותות שמפעילים את הבלמים לסירוגין להשגת בלימה מירבית בלי איבוד שליטה ברכב.

מכונת כביסה ה"מוח" שלה הוא מחשב. כמו בהרבה מכשירים ביתיים, יש בה מחשב קטן ששולט בפעולתה. המחשב מקבל קלט מחיישנים שונים על כמות וטמפרטורת המים, ומתוכנת על ידי תכנית הכביסה שנבחרה לייצר פלט שמנהל את הברזים והמנועים ששולטים במחזור הכביסה. במכונות חדישות חלק מהקלט הוא הכביסה עצמה - המכונה יכולה לשקול את הכביסה ולחשב את תוכנית הכביסה בעצמה!

מטחנת בשר אמנם יש למכונה קלט (בשר, לחם, בצל וכו') שהוא מעבד לפלט של בשר טחון; אולם אין לה תכנית כלשהי ולכן איננו מגדירים אותה כמחשב.

פלנימטר הפלנימטר הוא מחשב אנלוגי פשוט שהומצא במאה ה-19. מטרתו לחשב את השטח של צורה סגורה במישור, למשל שטח של אגם על מפה. הקלט שלו מוזן על ידי הולכת המחט שבקצה הזרוע על היקף הצורה, והמכשיר בנוי כך שבגלל המבנה שלו הוא מחשב את השטח (האינטגרל). הפלט מוצג על החוגות בבסיס המכשיר.

שאלת השאלות! האם מוח האדם הוא מחשב? המוח מקבל קלט מאברי החושים, מעבד אותו ומוציא פלט לשרירים ולאברי הגוף הפנימיים. השאלה האם המוח הוא מחשב ביולוגי מתוכנת, ומה מהות הקשר של פעילותו למחשבה ולתודעה, היא אחת הסוגיות הקשות והמסקרנות בחזית המדע.

הצגה בינארית: לספור על אצבע אחת

המכשיר שלפניכם ממחיש את השיטה הבינארית, שיטת הספירה לפי בסיס 2. בניגוד לשיטה העשרונית שבה משתמשים בספרות 0,1,2,3,...,9 בשיטה הבינארית משתמשים רק בשתי ספרות, 0 ו-1. המכשיר הזה מקבל מספר גולות בפתח העליון ומתרגם את המספר הזה למספר בינארי שמוצג בתחתית המכשיר כסדרת גולות: כל גולה מייצגת "1" ומקום שאין בו גולה מייצג "0".

השיטה הבינארית משמשת בכל המחשבים האלקטרוניים בימינו, כיוון שבמעגלים אלקטרוניים נוח להבחין בין "יש מתח" ו"אין מתח", מצבים שמייצגים "1" ו-"0". המעבד של המחשב מכיל מעגלים אלקטרוניים שמעבדים מספרים בינאריים כאלה - סדרות של "1" ו-"0" - שמחליפים את המספרים העשרוניים המוכרים לכולנו.





לחשב פרצוף

מצטלמים ובודקים כיצד תמונת הפנים משתנה.

מחשבים ספרתיים (דיגיטליים) מסוגלים לטפל באופן פנימי רק בנתונים מספריים, אבל אין זה אומר שהם טובים רק בחשבון. המחשב יכול לטפל בכל קלט אם ניתן להפכו לסדרה של מספרים. במוצג זה אות הוידאו מומר למספרים בהתאם לעצמת האור בכל נקודה בתמונה, מאפס (שחור) עד 9 (לבן). המספרים, שמוצגים במסך בצד ימין מייצגים את התמונה ומאפשרים למחשב להבין ולעבד אותה. שינוי הבהירות משנה את המספרים בהתאם.

המחשב הספרתי (דיגיטלי) מייצג באמצעות מספרים נתונים מסוגים רבים ושונים, למשל: **תמונות בשחור-לבן**: התמונה נדגמת בנקודות במרווחים שווים. כל נקודה מיוצגת כמספר שמשקף את "רמת האפור", או הבהירות, באותה נקודה. **תמונות צבעוניות**: התמונה נדגמת בנקודות במרווחים שווים. כל נקודה מיוצגת ע"י שלושה מספרים שמשקפים את הבהירות בשלושת צבעי היסוד (אדום, ירוק וכחול) באותה נקודה. **מוסיקה וצליל**: אות השמע נדגם עשרות אלפי פעמים כל שניה. כל דגימה מיוצגת ע"י מספר שמשקף את רמת המתח של האות (כלומר, את גובה צורת הגל שמייצגת את הצליל) ברגע הדגימה. **טקסט**: כל אות (או תו דפוס אחר) מיוצגת ע"י מספר בין 0 ל-255, על פי קוד המכונה ASCII.

מחשבים פיצה

מסובבים גלגלים ומרכיבים פיצה בהתאמה אישית.

אלגוריתם הוא דרך שיטתית לביצוע של משימה מסוימת צעד אחר צעד. המשימה הפעם: מכינים פיצה! המחשב פותר בעיות ע"י הפעלת אלגוריתמים מתאימים, שמתוכנתים לתוכו. כמו במתכון שבניתם לפיצה, האלגוריתמים במחשב בנויים מסדרת פעולות. וכמו בפיצה, אם לא נבחרו הפעולות המתאימות בסדר הנכון, לא תתקבל התוצאה הרצויה - לזה אנחנו קוראים 'באג'!

אלגוריתם הוא דרך שיטתית (כלומר כזו שצעדיה מוגדרים היטב) לביצוע של משימה מסוימת, שמטפלת בנתונים, במספר סופי של צעדים המתבצעים בזה אחר זה. חלק חשוב במדעי המחשב עוסק בפיתוח אלגוריתמים יעילים ככל האפשר לשם פתרון של בעיות מעשיות שונות, כגון מיון וחיפוש מידע במסדי נתונים, הצפנה ופענוח של מידע, ופתרון משוואות מתימטיות. האלגוריתמים מיושמים בתוכנות מחשב שפותרות את הבעיות האלה. מקור המלה אלגוריתם בהגיה הלטינית של שמו של המתמטיקאי הפרסי בן המאה התשיעית, מוחמד אבן מוסא אל-ח'ואריזמי.



איך מחשב פותר מבוך?

אלגוריתם המבצע חיפוש לרוחב (BREADTH-FIRST SEARCH - BFS) - מתנהג כמו גל במים - מתקדם בקצב אחיד לכל ה"כיוונים". הוא יוצא מהכניסה של המבוך וברגע הראשון מגלה את כל הפינות הסמוכות לכניסה, ברגע הבא את כל הפינות הבאות - הסמוכות לסמוכות, וכן הלאה: בכל רגע נתון הוא פונה לכל כיוון אפשרי ומגלה כל פינה חדשה שטרם נתגלתה. כך הוא עושה עד שהוא מגיע לפינות הרחוקות ביותר, ולמוצא המבוך. אחר־כך האלגוריתם שב לאחור ומסמן את המסלול הנבחר המחבר את הכניסה למוצא.

אלגוריתם המבצע חיפוש לעומק (DEPTH-FIRST SEARCH - DFS) מתנהג כאסיר נמלט אשר מבקש להתרחק מנקודת הכניסה למבוך ככל שרק אפשר - הוא רץ לתוך המבוך ומנסה להעמיק... עד שהוא נתקע בקיר. אחר־כך הוא חוזר לאחור, לפנייה הראשונה בה טרם ביקר - ושוב הוא רץ עד שנתקע בקיר, וכך הלאה - שוב ושוב הוא מנסה, וכל פעם חוזר לאחור לבדוק אפשרות שטרם נוסתה. זאת עד שיימצא את המסלול המוביל למוצא, ואז יחדל. אחר־כך האלגוריתם שב לאחור ומסמן את המסלול הנבחר המחבר את הכניסה למוצא.

האלגוריתמים המוצגים לפתרון מבוכים הם דוגמה לאלגוריתם על גרפים. גרף הוא מבנה מתמטי המאפשר להציג בעיות רבות ושונות מחיי היום־יום. הדוגמאות כוללות מפת כבישים, רשת מסילות ברזל, צינורות להולכת מים, מפות של מדינות ועוד. האלגוריתם הזה מאפשר לגלות ולהכיר את הגרפים ואת תכונותיהם, ובכלל זה לזהות מאין ניתן להגיע ולאן.



המחשב אינו כל-יכול

אף על פי שהמחשבים בימינו הם מהירים ורבי עֶצְמָה, הם אינם כל-יכולים. מדעני מחשב עוסקים רבות בשאלה מה המחשב יכול בעיקרון לחשב?

משימות בלתי אפשריות

יש משימות שמחשב, אפילו המהיר והחזק ביותר שנבנה אי פעם לא יוכל לבצע, משום שיידרש לו זמן כה ממושך שגם גיל היקום - מהמפץ הגדול עד שיכבו הכוכבים - לא יספיק לביצוע המשימה. ישנן גם משימות אחרות שהוכח כי לא ניתן לפתור בכלל.

באופן מפתיע, לנושא הזה יש השלכה מעשית רבת חשיבות: שיטות ההצפנה הנהוגות היום, שמאפשרות למשל את המסחר המקוון באינטרנט, מתבססות על בעיות שאינן ניתנות כיום לחישוב בזמן מעשי. אם מישהו ימציא אלגוריתם חדש ויעיל לבעיות אלה, יהיו לכך השלכות מרחיקות לכת!

ומה עם המוח שלנו?

קשה לדבר על גבולות יכולתו של המחשב בלי לתהות לגבי ההשלכות על גבולות החשיבה האנושית: האם המוח מסוגל לחשוב בכיוונים שחסומים בפני המחשב? האם גם החשיבה שלנו מוגבלת? מה דעתכם?

המחשב אינו כל-יכול
The computer is not o
ستطيع الحاسوب عمل كل شيء



מהרף עין עד גיל היקום, ויותר

שיטות ההצפנה הנהוגות היום, למשל במסחר המקוון באינטרנט, מתבססות על מגבלת הזמן. בעקרון ניתן לפצח אותן על ידי ניסוי וטעיה של כל צירופי הסיסמאות האפשריים, אולם הסיסמאות שמתמשים בהן ידרשו זמנים כה ארוכים שבאופן מעשי אין חשש שיפוצחו.

דוגמא למשימה שברמת הידע שלנו היום לא ניתנת לפתרון עקב מגבלת זמן היא בעיית הסוכן הנוסע. עניינה הוא סוכן מכירות אשר צריך לעבור בערים רבות המקושרות ביניהן באמצעות רשת כבישים. המטרה היא לחשב את המסלול הקצר ביותר אשר מבקר בכל אחת מהערים פעם אחת בדיוק. אפשרות אחת היא לעבור על כל המסלולים האפשריים, אבל כבר כאשר יש 80 ערים, מספר האפשרויות הוא עצום ורב (יותר ממספר החלקיקים ביקום), ולכן הפתרון הזה אינו ישים. מדעני המחשב הוכיחו שהבעיה הזאת כלולה במשפחת הבעיות המכונות בעיות NP - קשות. משמעות הדבר שללא פריצת דרך מחקרית משמעותית, לא נצליח לפותרה.



היזהרו מהמלכודת המעריכית!

ידועה האגדה על מלך פרס שרצה לתגמל את ממציא משחק השחמט. כשנשאל מה הוא מבקש, הצביע האיש אל לוח השחמט. הוא ביקש שישלמו לו במהלך 64 ימים באופן הבא. ביום הראשון יניחו גרגר תבואה אחד על המשבצת הראשונה של הלוח. ביום השני יניחו שני גרגרים על המשבצת השניה; ביום השלישי 4 גרגרים, וכך הלאה, בכל יום כפליים מהמספר שקיבל ביום הקודם. המלך נענה לו, בחשבו שהוא יוצא מהעסק בזול, עד שהתברר לו כי כל האורז בעולם לא יספיק לכך.

קל להוכיח שמספר הגרגרים הכולל על הלוח יהיה $2^{64}-1$, שזה 18,446,744,073,709,551,615.

מספר הגרגרים על המשבצת שמספרה N הוא 2^{N-1} , שתיים כפול בעצמו N-1 פעמים. פונקציה כזו נקראת אקספוננציאלית, או מעריכית, ותכונתה שערכה גדל מהר מאד עם עליית הערך N. משימה שדורשת ממחשב זמן שתלוי באופן מעריכי בגודל הנתונים נחשבת קשה לביצוע.

במדעי המחשב המודרניים מודדים סיבוכיות של משימה נתונה במונחים של הזמן הנדרש לביצועה (ביחס למספר הסיביות של הקלט). התלות של משך הביצוע בגודל הקלט עשויה להיות לינארית (וכללית יותר, פולינומית) או מעריכית. משמעותה של תלות לינארית (או פולינומית) היא שמשך הביצוע גדל ביחס ישר לגודל הקלט (או לחזקה קבועה שלו). במקרה זה אומרים שהמשימה מתבצעת בזמן לינארי (או פולינומי). משמעותה של תלות מעריכית היא שכל תוספת של סיבית



לקלט מכפילה את משך הביצוע בגודל קבוע, לדוגמה, פי 2. כמודגם במוצג זה, צמיחה מעריכית גדלה במהירות רבה. אלגוריתמים של זמן פולינומי הם, יעילים יותר מאלגוריתמים של זמן מעריכי, מפני שעבור קלטים גדולים הם מהירים בהרבה. כך למשל, אין אלגוריתם (ניסוח של תהליך) מְּוכר לפירוק מספר שלם לגורמיו הראשוניים בזמן פולינומי. שיטות הצפנה מסוימות מסתמכות על ההנחה (שלא הוכחה) שלא ניתן לבצע פירוק לגורמים בזמן פולינומי. דוגמא נוספת למשימה קשה לחישוב, משום שהזמן הדרוש לביצועה הוא פונקציה מעריכית, היא פתרון המשחק המוכר הקרוי "מגדלי האנוי".



ריצוף בלתי אפשרי

- לוח שחמט שלם ניתן בנקל לריצוף ע"י אריחים של שתי משבצות.
- בעיות ריצוף של המישור באריחים, נפוצות הן במשחקי חשיבה והן בתורת המתמטיקה. לא כל לוח סופי ניתן לריצוף, ולא תמיד קל לזהות איזה לוח ניתן לריצוף ואיזה לא.
- לוח השחמט החסר פינה אחת לא ניתן לריצוף ע"י אריחים של שתי משבצות - תמיד תשאר משבצת לא מכוסה. הנה ההוכחה: כל אריח מכסה שתי משבצות על הלוח, ולכן מספר המשבצות שהאריחים יכסו הוא תמיד זוגי. אולם בלוח חסר הפינה יש 63 משבצות, מספר אי-זוגי, ולכן לא ניתן לרצפו באריחים כאלה.
- לוח השחמט החסר שתי פינות נגדיות לא ניתן לריצוף ע"י אריחים של שתי משבצות - וקל להוכיח את זה. הנה ההוכחה: כל אריח מכסה שתי משבצות סמוכות על הלוח, אחת שחורה ואחת לבנה; לכן כל שטח שנצליח לרצף יכיל מספר שווה של משבצות משני הצבעים. לוח שחמט שלם מכיל מספר שווה של משבצות מכל צבע, ואכן ניתן לרצפו בקלות. אולם בלוח חסר הפינות הנגדיות חסרות שתי משבצות מאותו צבע, כלומר אין בו מספר שווה של משבצות שחורות ולבנות, ולכן לא ניתן לרצפו באריחים כאלה.
- האם אפשר לדעתכם לרצף את לוח עם משבצת אחת חסומה בעזרת אריחים בצורת "ריש", כאשר כל אריח מכסה 3 משבצות? ניתן גם ניתן! נעשה זאת כך: נחלק את הלוח לארבעה רבעים שממדי

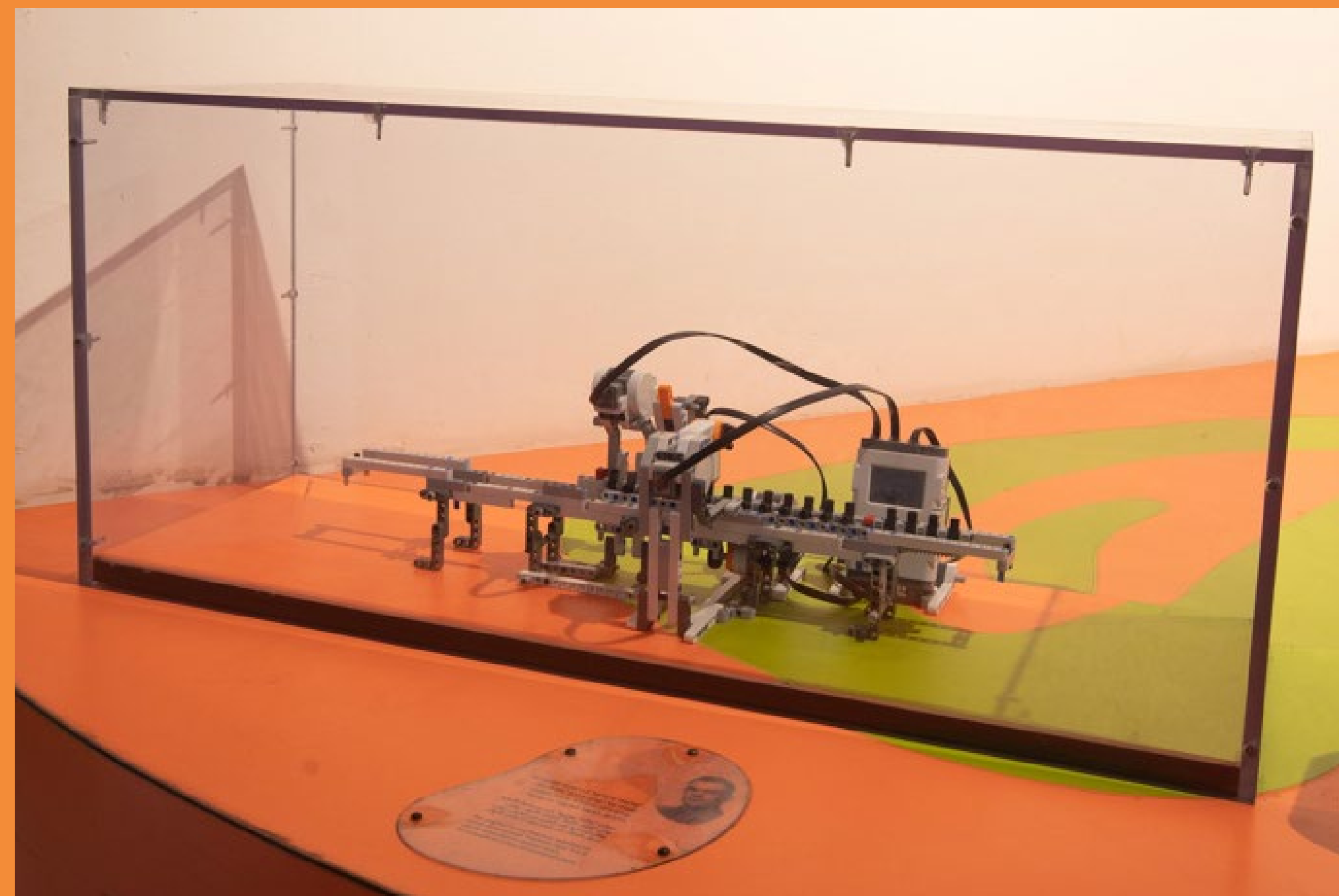
כל אחד מהם הוא 4×4 משבצות. באחד הרבעים חסרה משבצת אחת (המקורית - זו שכבר מכוסה). שלושה האחרים מושלמים ומייצרים "פינה". על הפינה הזאת נניח אריח אחד בצורת "ריש". מה קבלנו? בכל אחד מהרבעים יש משבצת אחת מכוסה. נטפל בכל אחד מהם בנפרד - נפריד כל אחד לארבעה רבעים (שממדי כל אחד מהם הוא 2×2 משבצות) ונקבל שלושה רבעים מושלמים, ואחד שחסרה בו משבצת אחת, שוב נלביש "ריש" אחד, ונגלה שאפשר לסיים.

- הצגנו כאן אלגוריתם (דרך שיטתית לביצוע משימה) לפתרון הבעיה. למעשה ניתן להוכיח בדרך דומה שניתן לכסות כל לוח רבועי שממדיו הם חזקה של 2, אשר משבצת אחת בתוכו כבר כוסתה. איך עושים זאת? מפרקים את הבעיה ל-4 בעיות "קטנות יותר". ומדוע זה עובד? כי המקרה הקטן ביותר (ריבוע 2×2 חסר משבצת אחת) פתיר בקלות. אלגוריתם מסוג זה נקרא אלגוריתם רקורסיבי. באלגוריתמים רקורסיביים אנחנו משתמשים כאשר ניתן לפרק את הבעיה הנתונה לבעיות קטנות יותר מאותה הצורה. במה הן קטנות יותר? בגודל הקלט (בדוגמה שלפנינו, גודל הלוח).
- האם ניתן לרצף את הלוח באריחים צבעוניים המכונים "אריחי ואנג"? מתימטיקאים הוכיחו שקיימות קבוצות סופיות שונות של אריחים כאלה - אריחי ואנג - שניתן לרצף איתן את המישור (האינסופי) כולו, אולם לא קיים אלגוריתם שיאפשר למחשב להכריע מראש האם כל קבוצה של אריחים יכולה לעשות זאת. ההוכחה לכך עושה שימוש ברעיון של מכונת טיורינג שהגה אלן טיורינג 30 שנים קודם לכן.

המכונה שטיורינג הגה

הרעיון שהגה אלן טיורינג ב-1936 היה של מכונה דמיונית שתוכל לבצע כל חישוב אפשרי; הוא הסתפק בפרסום הרעיון ולא ניסה לבנות את המכונה, ששימשה אותו רק כמודל תיאורטי. מאז נבנו דגמים רבים שממחישים את הרעיון של טיורינג בצורתו המקורית תוך שימוש במגוון חמרי גלם. במכונה הזו תוכלו להבחין בשני חלקים עיקריים: "סרט" אשר מיוצג ע"י המסילה שעליה רכיבי לגו שחורים שיכולים להיות מוטים בשני מצבים, כדי לייצג את התווים "0" ו-"1"; ו"ראש" הכולל עין חשמלית לבחינת מצב התווים וזרוע שיכולה לשנות את מצב רכיבי הלגו.

כל מחשב מודרני מבוסס על המודל החישובי שהגה טיורינג. הגאונות היא בכך שמודל כה פשוט יכול לממש את כל מה שאפשר לעשות עם מחשב מודרני, ומנגד - מה שאי אפשר לעשות עם מכונת טיורינג גם אי אפשר לעשות במחשבים המשוכללים ביותר שנבנו בעולם!



המחשב החושב

האם מכונות יכולות לחשוב?

ככל שהמחשבים ישתכללו ועצמתם תגדל, תתחדד השאלה: האם מחשב חזק דיו יוכל לחשוב? ומהי בכלל משמעות הדבר - לחשוב?

אלן טיורינג הבין את העניין כבר בשנת 1950. במאמרו "מכונות חישוב ותבונה" הוא ניתח בבהירות את הדרך לענות על השאלה "האם מכונות יכולות לחשוב?", ולשם כך הגדיר את "מבחן טיורינג". המבחן מציב מחשב ובן-אנוש מאחורי מסך, ומבקש מהם לשוחח עם בוחן אנושי באמצעות מסרי טקסט. אם הבוחן אינו מצליח להבחין מי האדם ומי המחשב, טיורינג קבע כי עלינו להסכים שהמחשב המסתתר חושב.



המבחן הקובע

מחשב שיעבור את מבחן טיורינג במלואו הוא עדיין בגדר חזון רחוק, אבל בינתיים, המחשבים מבצעים כבר היום מטלות שבעבר נחשבו לנחלתו של האדם בלבד: הם מזהים תמונות, משחקים בשחמט (ומנצחים אותנו!), כותבים מוסיקה - ועדיין, איננו סבורים שהמחשב חושב באמת. אלא שהמחשבים ימשיכו להגדיל את יכולותיהם בעוד אנו נשארים כשהיינו. וכאן נשאלת השאלה: האם יבוא יום והמחשבים יעברו את יכולת החשיבה של האדם? ומה יקרה אז?

שאלת השאלות

שאלה מטרידה יותר היא זו: האם מחשב שיעבור את מבחן טיורינג בהצלחה יהיה מודע לעצמו כשם שאנחנו מודעים לעצמנו? האם כשהמחשב יצהיר שהוא שמח, או עצוב, או שכואב לו, נאמין לו שהוא מרגיש כך באמת? לעת עתה השאלה עולה רק בסיפורי מדע בדיוני, כי עוד לא הצלחנו לבנות מחשב כזה במציאות. מה יקרה אם נצליח?

מחשב מלחין?

שתים מהיצירות המושמעות באזניות נכתבו בידי מלחינים בני אנוש. היצירה בזוג האזניות הנותר נכתבה בידי המחשב IAMUS שנבנה בידי מדענים באוניברסיטה של מלגה בספרד. IAMUS מתוכנת לצרף צלילים באופנים שנותנים חווית האזנה טובה, אולם איש לא אומר לו אילו צלילים לבחור; המחשב כתב את המנגינה באופן עצמאי, הדפיס חוברת תוים והעביר אותה לנגנים אנושיים שניגנו את היצירה.

IAMUS הוא המחשב המתקדם בעולם בשטח ההלחנה הממוחשבת, והוא נבנה במיוחד למטרה זו. השאלה, האם המחשב הזה אכן יצירתי או שהוא רק מכונה שמבצעת הוראות, פתוחה לדיון, והמחלוקת הערנית בעניין זה תעמיק ככל שיכולות המחשב ישתכללו.

על כל פנים, IAMUS כבר הוציא תקליטור ראשון מיצירותיו...

מה שבטוח - מאזינים רבים מתקשים להבחין בין המחשב למלחין האנושי, מה שאומר שבתחום המוגבל הזה של יצירת מוסיקה IAMUS עובר בהצלחה את מבחן טיורינג!



מחשב צייר?

חלק מהתמונות המוצגות צוירו בידי אדם, וחלק בידי מחשב בשם AARON שפיתח האמן האמריקאי הרולד כהן. AARON מתוכנת ליצור תמונות בסגנונות שונים כשהוא מנצל הן ידע שתוכנת לתוכו על עצמים שונים בעולם (למשל אנשים וצמחים) והן כללי יסוד של אמנות הציור (כמו העובדה שעצם קרוב אלינו מסתיר עצם רחוק יותר אבל לא להיפך).

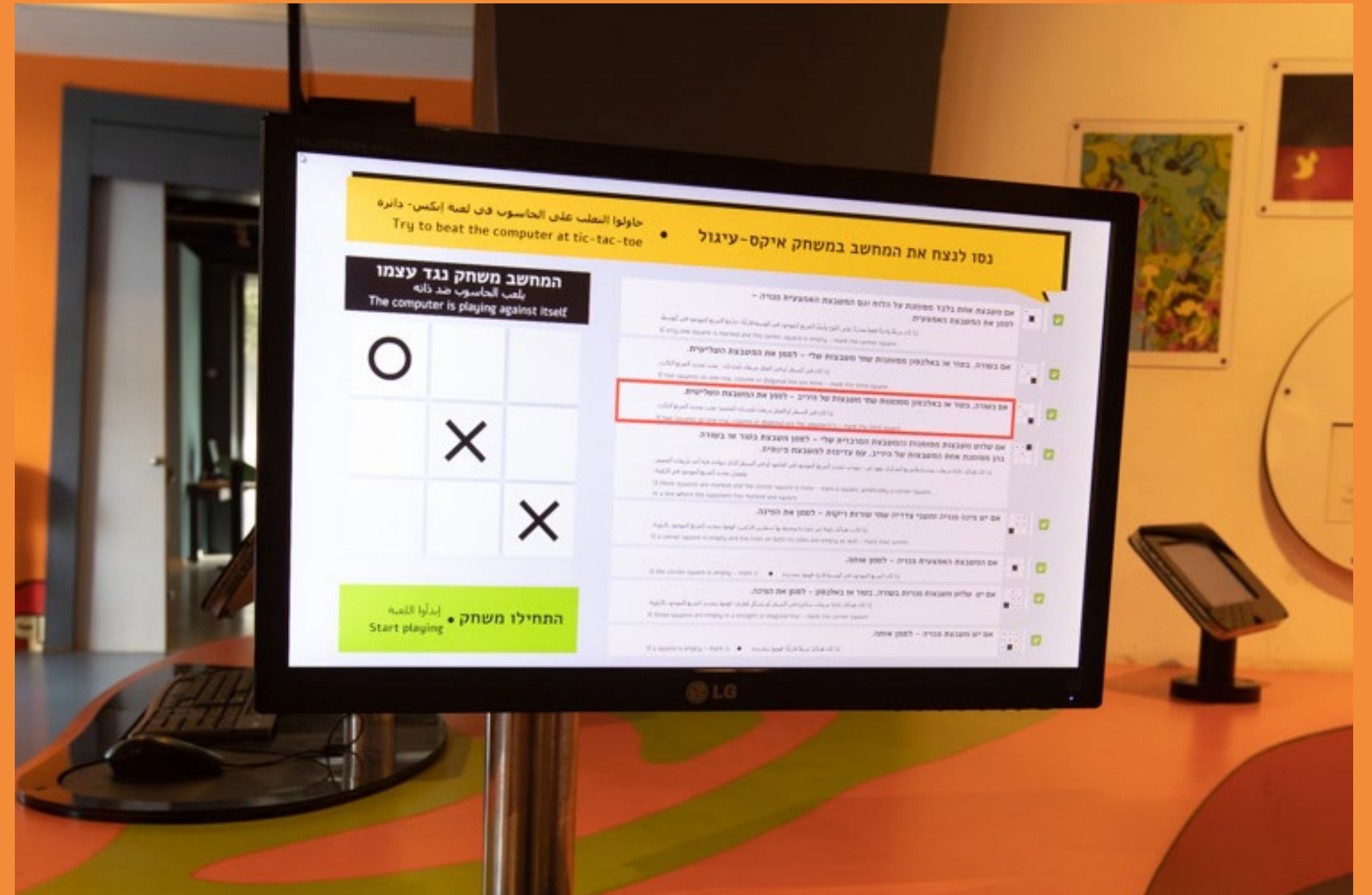
הרולד כהן פיתח את AARON במשך יותר משלושים שנה, כשהוא משכלל אותו כל העת. השאלה, האם המחשב הזה אכן יצירתי או שהוא רק מכונה שמבצעת הוראות, פתוחה לדיון, והמחלוקת הערנית בעניין זה תעמיק ככל שיכולות המחשב ישתכללו.

על כל פנים יצירותיו של AARON הוצגו בתערוכות ובמוזיאונים ברחבי העולם ואף נמכרו לאספנים. מה שבטוח - צופים רבים מתקשים להבחין בין המחשב לצייר האנושי, מה שאומר שבתחום המוגבל הזה של יצירת תמונות AARON עובר בהצלחה את מבחן טיורינג!



שחקו מול המחשב!

המשחק 'איקס עיגול' הוא משחק פשוט שקל לשחקנים מיומנים לא להפסיד בו (כלומר לאכוף תיקו) אם הם מיישמים אסטרטגיה נכונה. המחשב שלפניכם תוכנת ליישם אסטרטגיה כזו ואף מציג לפניכם את השיקולים שהוא שוקל לבחירת המהלכים שלו.

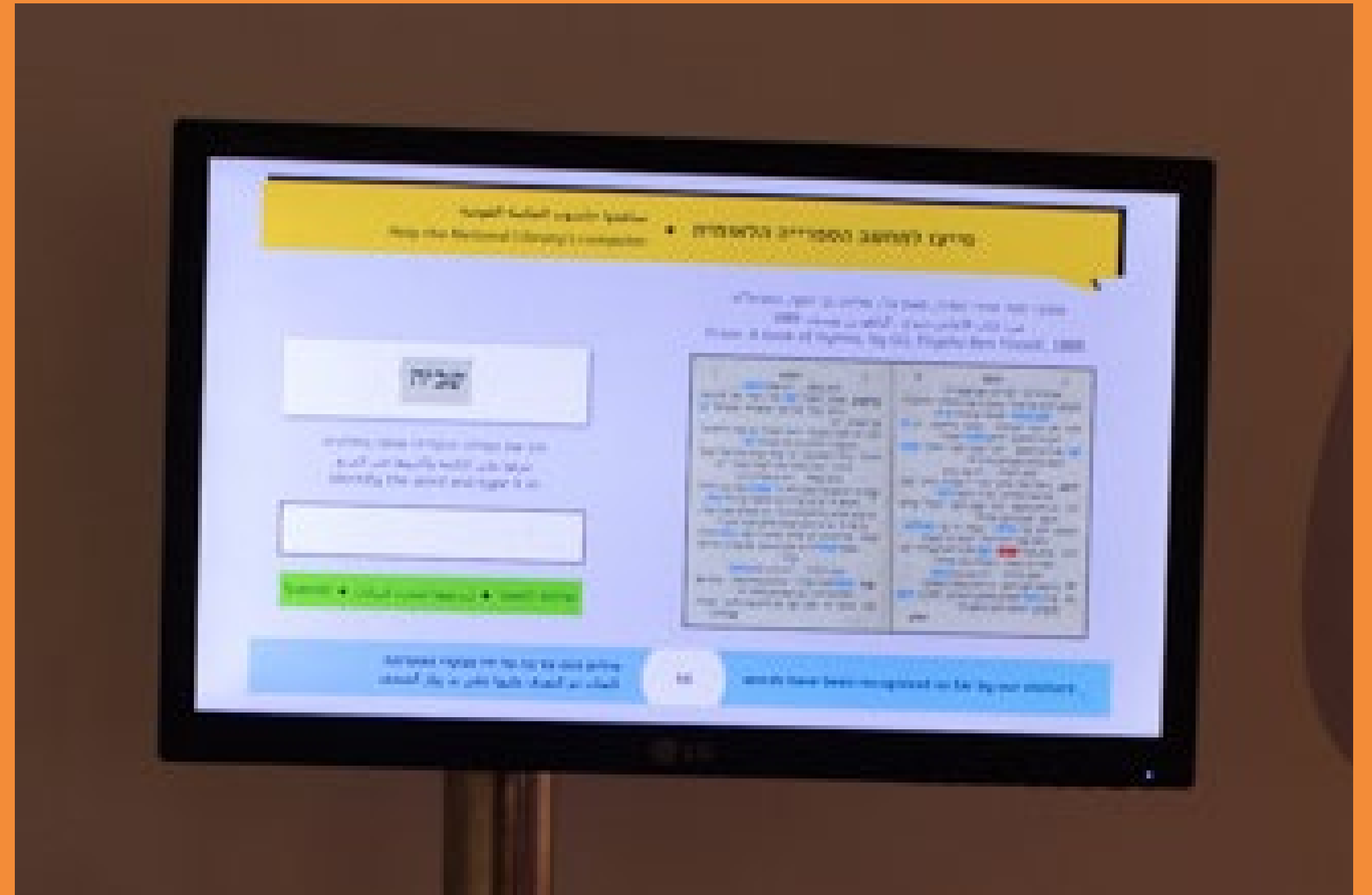


הכירו את אלייזה!

אלייזה היא תכנית שיחה (צ'אטבוט) שמחקה פסיכולוג. למרות שהיא מגיבה על דבריכם באופן שנראה הגיוני, בפועל היא רחוקה מלהיות חכמה: התכנית מזהה מילות מפתח בדבריכם ומשתמשת בהן בחזרה בתבניות מוגדרות מראש. למשל, אם המשתמש אומר "אני עצוב" התכנית יכולה להגיב "למה אתה אומר שאתה עצוב?" ובכל זאת, נוצרת שיחה משעשעת שכמעט יכולה להטעות אתכם לחשוב שיש מולכם מישהו שמבין אתכם!

אלייזה (באנגלית ELIZA) היא תוכנית מחשב שנכתבה בשנת 1966 על ידי מדען המחשב ג'וזף וייצנבאום, במטרה ליצור פרודיה על הפסיכותרפיה בשיטת קרל רוג'רס. למרות שניתן בקלות לסבך אותה כך שתגיב לא לעניין, באופן מפתיע היו לא מעט אנשים שהגיבו אל 'אלייזה' כאילו היתה מטפל אמיתי! אלייזה מציגה דוגמה ל"מבחן טיורינג", שבו על המשתמש להחליט אם מתקשר איתו אדם או מחשב. אלן טיורינג שיער ב-1950 שבסוף המאה ה-20, כבר יהיו מחשבים שיוכלו להטעות אותנו לחשוב שהם בני אדם בשיחה כללית. בכך הוא טעה: כמו שאתם רואים מהשיחה עם אלייזה, אפילו בתחום מוגבל כמו שיחה עם פסיכולוג עדיין המחשב רחוק מלגלות את ההבנה והגמישות הדרושה. אולי בעוד 50 שנה...?





האדם לעזרת המחשב

הספרייה הלאומית לקחה על עצמה משימה כבירה של הנגשת אוצרות התרבות והרוח בשפה העברית דרך האינטרנט. לשם כך היא סורקת רבבות ספרים וכתבי עת ומעבירה אותם בתכנת מחשב שמבצעת זיהוי תווים אופטי (OCR - OPTICAL CHARACTER RECOGNITION). לרוע המזל המחשב מתקשה לזהות נכונה מלים שאינן ברורות בסריקה, למשל עקב ניקוד ואיכות הגופנים, בפרט בחומרי מקור עתיקים.

כדי לפתור את הבעיה המחשב מסמן מלים שלא זיהה, ואתם מתבקשים לעזור לו בפיענוחן. התכנה משתמשת בקריאה של מספר בני אדם כדי להחליט בביטחון מה המילה הנכונה.

יתרון האדם על המחשב בראיה מופשטת מנוצל ב־CAPTCHA, מבחן שמטרתו למנוע מתוכנות אוטומטיות להיכנס לאתרים ברשת האינטרנט. המבחן מתבסס על הרעיון שהציע אלן טיורינג על מנת לבדוק האם למכונה יש בינה מלאכותית. ב־CAPTCHA התהליך הפוך, המחשב הוא שמחליט אם המשתמש עמו הוא "משוחח" הוא אדם או מחשב, בעזרת רצף אותיות מעוותות. בני אדם מפענחים את התמונה שהם רואים בקלות יחסית, מחשבים פשוט לא מצליחים לעשות זאת.

ה־reCAPTCHA הוא ניצול למטרה זו של מילה מתוך ספר שתוכנות זיהוי טקסטים לא הצליחו לפענח. אם נתקלתם בתיבת CAPTCHA של שתי מלים, אחת מוודאת שאתם בני אנוש והשניה היא המילה שאתם מסייעים לזהות.

* המוצג פותח בשיתוף הספרייה הלאומית.

הצפנה

ההצפנה מסייעת לנו לשמור על סודיות ועל פרטיות. בחיי היום-יום משתמשים בה לצרכי תקשורת (בין בני אדם, בין מכשירי טלפון ובכלל בין מחשבים); בשמירה על פרטי כרטיס אשראי ועל מידע אישי אחר; ויש אפילו מנעולים המתבססים על הצפנה. חברות, צבאות ומדינות משתמשים בהצפנה כדי להגן על מידע מסווג מסוגים שונים.



תורת הסוד

פעם התבססה ההצפנה על חידות וסודות. שני המשוחחים היו נפגשים ומסכימים על סוד משותף, והיו משתמשים בו כדי שהאחד יוכל להצפין מידע והשני יוכל לפענחו.

דוגמאות פשוטות כוללות את צופן אתב"ש שבמסגרתו הנביא ירמיהו החליף בין האותיות אל"ף ו"ת", בי"ת ו"ש", וכן הלאה, וכך כתב "ששכ" כאשר רצה לומר "בבל" או "לב קמי" במקום "כשדים". גם דוד ויהונתן החליטו מראש על ביטוי שבו ישתמש יהונתן ברשות הרבים ורק דוד ידע להבינו.

במשך השנים פותחו צפנים מחוכמים יותר, החל ב"צופן קיסר" (שקל לפצחו) וכלה ב"אניגמה" ששימשה את הגרמנים במלחמת העולם השנייה ופוצחה במאמץ רב על ידי אלן טיורינג ועמיתיו בבריטניה.

לצורך שימוש בצופן כזה היה על הצדדים להיפגש מראש ולהסכים על הסוד.

הצפנה, מתמטיקה ובעיות קשות

ב־40 השנים האחרונות הגישה השתנתה: שיטות הצפנה מודרניות אינן מחייבות כלל מפגש מקדים בין הצדדים. כיום אפשר לבצע רכישות דרך האינטרנט בצורה בטוחה, תוך שימוש בהצפנה פומבית. הערוצים יכולים להיות גלויים – כל העולם יכול לצותת לרשת האינטרנט (אף עושה זאת), אך רק הנמען מסוגל לפענח את ההודעה שנשלחה אליו! שיטות ההצפנה האלה מתבססות על בעיות מתמטיות מורכבות, שהקושי החישובי שלהן מונע פיענוח של המסרים בזמן מעשי ללא מידע נוסף שמצוי רק בידי הנמען. עם מדעני המחשב שתרמו תרומה מרכזית לפיתוחן של שיטות ההצפנה המודרניות נמנים פרופ' עדי שמיר ממכון ויצמן למדע ופרופ' מיכאל רבין מהאוניברסיטה העברית בירושלים.

גלגלי הצפנה

גלגלי הצפנה הם דרך נוחה להצפין בשיטות בהן כל אות מוחלפת באות קבועה אחרת. אלו צפנים סימטריים, כלומר תהליך הפענוח הפוך בדיוק לתהליך ההצפנה ומשתמש באותו כלל. כלל זה, המכונה מפתח, צריך להיות ידוע לשני הצדדים (השולח והנמען). הגלגלים שלפניכם מייצגים שלושה צפנים פשוטים: **גלגל 1: צופן קיסר** (יושם ע"י שליט רומא יוליוס קיסר לפני כאלפיים שנה). בצופן זה כל אות מוחלפת באות שנמצאת מספר קבוע של מקומות אחריה באלף בית. המפתח הוא המספר הזה, כלומר בכמה מקומות סובבתם את הגלגל הפנימי ביחס לחיצוני. למשל אם ההפרש הוא 3 אז א' מוחלפת ב'ד', ב' מוחלפת ב'ה', וכן הלאה.

גלגל 2: צופן אתב"ש. בצופן זה א' מוחלפת ב'ת', ב' מוחלפת ב'ש', וכן הלאה משני קצות האלף בית. צופן אתב"ש מופיע בתנ"ך: הנביא ירמיהו התנבא: "וּמְלַךְ שֶׁשָׁךְ יִשְׁתֶּה אַחֲרֵיהֶם" (ירמיהו כ"ה כ"ו), ובמקום אחר: "הֲנִי מַעִיר עַל בְּבֹל וְאֵל יִשְׁבִי לֵב קָמִי רוּחַ מְשֻׁחִית" (ירמיהו נ"א א'). בצופן אתב"ש ששך היא בבל, ואילו לֵב קָמִי הוא כשדים. **גלגל 3: צופן החלפה אקראי**. בצופן זה האותיות מוחלפות לפי התאמה אקראית שמיוצגת בגלגל. בימינו כבר לא נעשה שימוש בצפנים פשוטים אלה, כיוון שהם קלים מאוד לפיצוח - כמו שתוכלו לראות במוצג "תדיר ושאינו תדיר". במקומם פיתחו מדעני מחשב שיטות חזקות בהרבה.



הצפנה מיוון העתיקה

המכשיר המכונה סקיטאלי (SCYTALE) הוא דרך אחת ליישם צופן הזזה - צופן בו כל אות משנה את מיקומה לפי חוקיות מסוימת. השיטה מחייבת שימוש במוט בקוטר נתון, שחייב להיות בידי שני הצדדים (השולח והנמען). הסקיטאלי היה בשימוש כבר במאה השביעית לפסה"נ, וידוע ששימש את הצבא הספרטאני להעברת הודעות בעת מלחמה. יתרונו לשימוש כזה הוא במהירות ההצפנה והפיענוח ובחסינות משגיאות, אולם הוא קל יחסית לפיצוח ולכן אינו מתאים לשימושים אחרים.



קל להרכיב, קשה לפרוק

פירוק לגורמים של מספר שלם היא הצגתו כמכפלה של מספרים קטנים יותר - הנקראים הגורמים שלו. המטרה היא להציג את המספר כמכפלה של מספרים ראשוניים - כאלה שלא ניתן לפרק למכפלה של שני שלמים הקטנים מהם. לדוגמא: אנחנו מציגים את 6 כמכפלה של 2 ו-3. משפט מתמטי עתיק קובע שכל שלם (גדול מ-2) ניתן להצגה כמכפלה של ראשוניים וההצגה הזאת היא יחידה, אבל עד היום לא קיים אלגוריתם יעיל לחישוב ההצגה הזאת. מנגד, אם מוצעת הצגה, קל לוודא את נכונותה באמצעות כפל. את האלגוריתם לכפל מספרים לומד כל ילד בבית הספר ואכן קל לכפול שני מספרים, אפילו אם הם גדולים מאוד. מנגד, הפעולה ההפוכה - פרוק מספר למכפלה של ראשוניים - היא פעולה קשה מאוד ולא ידוע כיום אלגוריתם יעיל לביצועה.

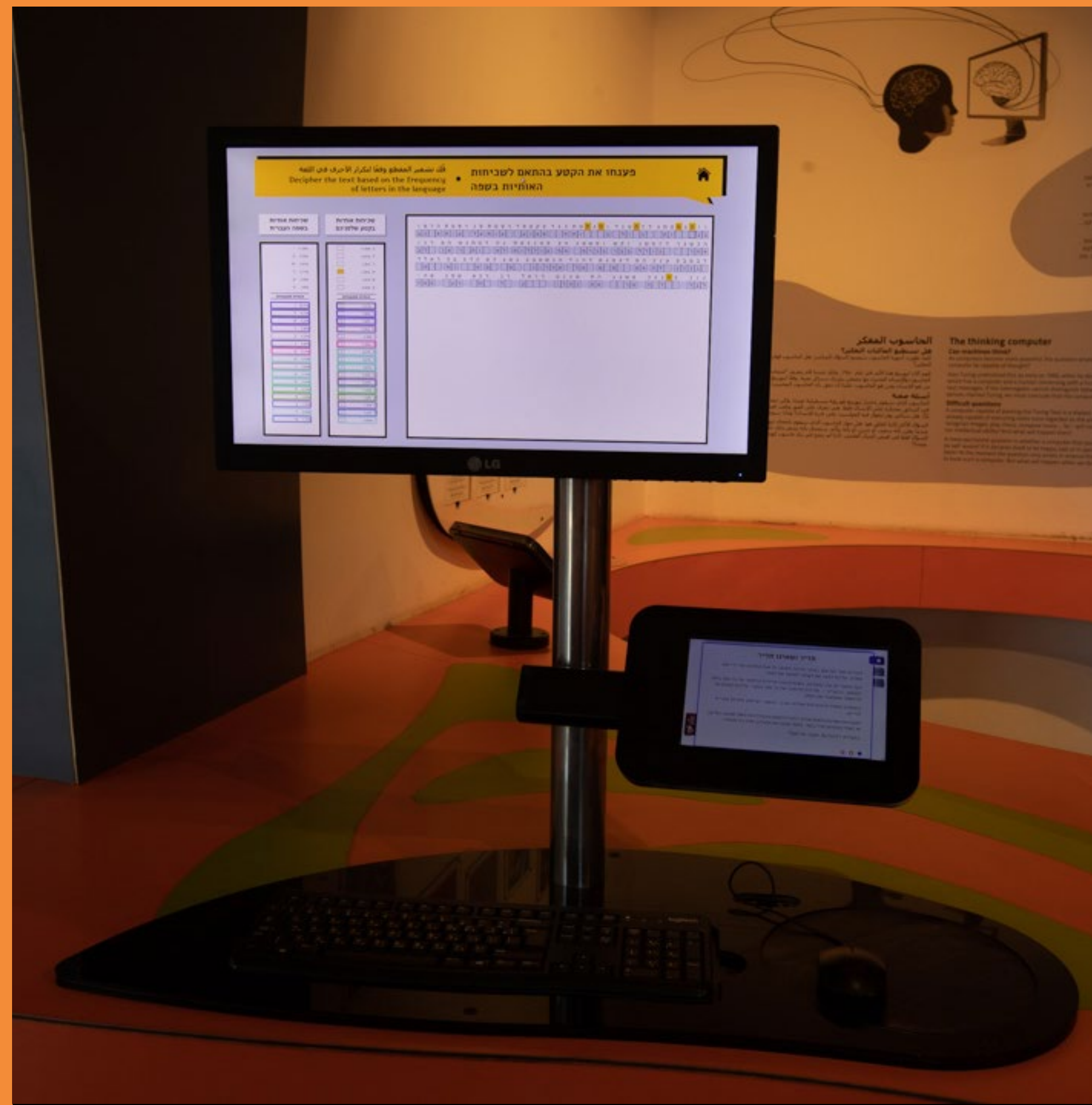
על בסיס הקושי של בעיית הפרוק נבנו אלגוריתמים שונים להצפנה. בעוד שבעולם העתיק התבססו על סודות מוסכמים בין המצפין למפענח כדי להעביר מידע מוצפן, הרי שבעולם המודרני משתמשים בבעיות מתמטיות קשות כדי לעשות זאת, ללא סודות מוסכמים בין הצדדים. שיטת RSA, למשל, המשמשת בתקשורת דרך האינטרנט, מבוססת על כך שניתן לפרסם מספר גדול שפרוקו אינו ידוע לציבור הרחב, אך ידיעת הפרוק תביא לפענוח הודעות שהוצפנו באמצעותו. וכך, הנמען יכול לחשב מספר גדול ולפרסמו ברבים בידיעה שרק הוא יודע את הפרוק, ולכן רק לו יהיה קל לפענח הודעות שתשלחנה אליו. לשיטה הזאת קוראים "הצפנה במפתח פומבי".



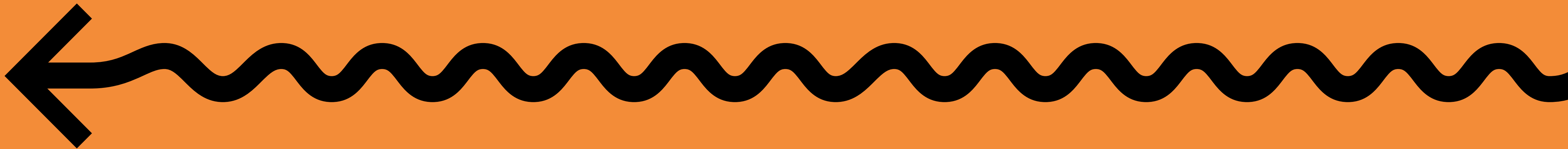
תדיר ושאינו תדיר

צופן החלפה מייצג 'מסיבת מסכות' שבה משתתפות אותיות השפה. אבל כמו שבמסיבת מסכות האיש הגבוה ביותר נשאר הגבוה ביותר גם אם עטה מסכה, כך ברור שהאות הנפוצה ביותר בשפה תישאר הנפוצה ביותר גם אם נקרא לה בשם אחרת. וכך, אם המסר המוצפן מספיק ארוך, ניתן לזהות את האותיות המקוריות לפי תדירויותיהן.

לכל אות בשפה יש תדירות אופיינית. ברור שהאות 'י' בעברית מופיעה בכל ספר "נורמלי" יותר פעמים מהאות ז'. תוך שימוש בטבלת תדירויות ניתן לחשוף את האותיות המסתרות - זו שמופיעה מספר מרבי של פעמים היא ודאי 'י', זו שלאחריה ו', וכו'.



הרחבה והעשרה



כיצד מדעי המחשב משנים את עולמנו?

מדעי המחשב בוחנים שאלות עיוניות מרתקות, אך למדענים העוסקים בתחום ולפועלם יש השפעה מעשית ביותר על העולם ועל חיי היום-יום שלנו. כיום קשה להיזכר בעולם שבו חיינו לפני שנים מעטות - בלי אינטרנט, בלי טלפונים חכמים, ללא רשתות חברתיות, נטול ויקיפדיה ובלי הטכנולוגיה הממוחשבת שהובילה למהפך בתחומי הרפואה; הבטיחות; הלימוד; המלחמה והשלום. מדעי המחשב אכן שינו את עולמנו, וממשיכים לשנותו באופן תדיר.

מדינת ישראל נמצאת כיום בקו הראשון של המחקר העולמי בתחום מדעי המחשב. מדענים ישראליים תרמו תרומה מרכזית להתפתחות התחום, כך למשל פרופ' עדי שמיר ממכון ויצמן שהיה בין ממציאי שיטת ההצפנה RSA, שלה תפקיד מרכזי בענפי הסחר האלקטרוני והבנקאות המקוונת המניעים את כלכלת העולם.

מדענים בישראל אף משתתפים בפרויקטים בינלאומיים שבהם משתמשים ביכולתו של המחשב כדי לחקור ולפענח את מסתרי פעולת המוח - נושא בעל השלכות מרחיקות לכת בתחומי מדעי המחשב, הביולוגיה, הרפואה והפילוסופיה.

מדעני המחשב במדינת ישראל בולטים בתרומתם למדעי המחשב בעולם כולו. בין הבולטים שבמדענים אלה ניתן למצוא את האנשים הבאים:

שם	מיכאל רבין
מוסד	האוניברסיטה העברית
תחומי מחקר	תורת החישוביות, אלגוריתמים הסתברותיים, חישוב מבוזר ומקבילי, הצפנה
פרסים	פרס אמ"ת (2004), פרס ישראל (1995), פרס טיורינג (1976)
שם	עדי שמיר
מוסד	מכון ויצמן
תחומי מחקר	הצפנה, סיבוכיות חישובית
פרסים	פרס ישראל (2008), פרס טיורינג (2002), פרס ארדש (1983)
שם	אמיר פנואלי (1941-2009)
מוסד	מכון ויצמן
תחומי מחקר	אפיון ואימות תוכנה
פרסים	פרס ישראל (2000), פרס טיורינג (1996)
שם	יהודה פרל
מוסד	אוניברסיטת קליפורניה, לוס אנג'לס
תחומי מחקר	בינה מלאכותית
פרסים	פרס טיורינג (2011)
שם	שפי גולדווסר
מוסד	מכון ויצמן
תחומי מחקר	הצפנה
פרסים	פרס גדל (2001, 1993)
שם	נוגה אלון
מוסד	אוניברסיטת תל אביב
תחומי מחקר	קומבינטוריקה, תורת הגרפים, השיטה ההסתברותית, דה־רנדומיזציה
פרסים	פרס אמ"ת (2011), פרס ישראל (2008), פרס גדל (2005), פרס ארדש (1989)
שם	אבי ויגדרזון
מוסד	המכון ללימודים מתקדמים, פרינסטון
תחומי מחקר	סיבוכיות חישובית
פרסים	פרס גדל (2009), פרס נבנלינה (1994)
שם	דוד הראל
מוסד	מכון ויצמן
תחומי מחקר	לוגיקה דינמית, חישוביות, הנדסת תכנה
פרסים	פרס אמ"ת (2010), פרס ישראל (2004)

שם	שרית קראוס
מוסד	אוניברסיטת בר-אילן
תחומי מחקר	מערכות מרובות סוכנים
פרסים	פרס אמ"ת (2010)
שם	מיכה שריר
מוסד	אוניברסיטת תל אביב
תחומי מחקר	גאומטריה חישובית, רובוטיקה
פרסים	פרס אמ"ת (2007)
שם	אירית דינור
מוסד	מכון ויצמן
תחומי מחקר	קומבינטוריקה, הוכחות
פרסים	פרס ארדש (2012)

פרס טיורינג ניתן על ידי ACM, האגודה למכונות מחשוב, בגין הישג יוצא דופן בתחום מדעי המחשב. הפרס שקול מבחינת יוקרתו לפרס נובל, שאינו ניתן בתחומי המתמטיקה ומדעי המחשב.

פרס נבנלינה (NEVANLINNA) מוענק על ידי הקונגרס הבינלאומי של המתמטיקאים עבור תרומה יוצאת דופן לאספקטים המתמטיים של מדעי המידע.

פרס גדל (GÖDEL) מוענק על ידי ההתאחדות האירופית לתאוריה של מדעי המחשב ו־ACM, עבור מאמר בולט באיכותו בתחום מדעי המחשב.

פרס ארדש (ERDŐS) מוענק על ידי האיגוד הישראלי למתמטיקה למתמטיקאי ישראלי העוסק במתמטיקה עיונית, במתמטיקה שימושית או במדעי המחשב.

פרס ישראל הוא הפרס החשוב והיוקרתי ביותר הניתן במדינת ישראל. הוא מוענק לאזרחי המדינה שגילו הצטיינות מיוחדת, מצוינות ופריצת דרך בתחומם או שתרמו תרומה מיוחדת לחברה בישראל.

פרס אמ"ת (אמנות-מדע-תרבות) מוענק על ידי קרן אמ"נ לקידום המדע, התרבות והאמנות בישראל, בחסות ראש ממשלת ישראל, על הצטיינות והישגים בעלי השפעה מרחיקת לכת ותרומה מיוחדת לחברה.



חוקרים אחרת

לחדירת המחשב האלקטרוני למחקר האקדמי בשנות החמישים היתה השפעה מיידית על המדע. אם בתחילה ניתן היה לחשוב שזו תהיה מוגבלת לביצוע מהיר יותר של חישובים מספריים שהיו דורשים זמן רב בעבודה ידנית, הרי שבהמשך הופיעו יישומים שקודם לא היה ניתן כלל להעלותם על הדעת.

תחום חשוב במיחשוב המדעי הוא הסימולציה של התנהגות והתפתחות מערכות בטבע. הדמיות כאלה יכולות לבחון התפתחות של תגובות כימיות, של מזג האוויר, של התהוות כוכבים וגלקסיות, של פעולת המוח ואיברים אחרים בגופנו, וגם של התנהגות אורגניזמים בתנאים שונים.

בעקבות עליית עצמתם ומהירותם של המחשבים ניתן היום לפתח סימולציות שמציגות את המערכת המתפתחת במגוון צורות גרפיות.

תחום חדש יחסית בו המחשבים מאפשרים מחקרים מהפכניים הוא תחום ה־BIG DATA, שמטפל בכמות גדולה מאד של נתונים (בנפח שמעל מאות טרה־בייט), שיכולים להתקבל בקצבים מהירים מאד וממקורות רבים ושונים. ניתוח נתונים בהיקפים כאלה לא היה אפשרי עד לאחרונה, והוא מאפשר הפקת תובנות שלא היו בתחום השגתנו עד כה.

למשל, האפשרות לבצע חיפוש במיליוני דפי טקסט, ספרים אלקטרוניים, דברי דואר אלקטרוני, מסמכים ארגוניים או מסרונים טוויטר מאפשר להסיק מסקנות מרחיקות לכת בתחומים רבים ושונים; ניתוח תבניות ומגמות בסחר במניות בבורסה מוביל לשיטות חדשות בניהול השקעות; ומיפוי מידע גנטי בהיקפים גדולים מאפשר מחקרים שמובילים להבנת המקורות והריפוי של מחלות.

מרפאים אחרת

הרובוט המיניאטורי מיועד לסייע למנתחים לבצע פעולות שונות במהלך ניתוחי מוח. מטרת השימוש ברובוט היא להקטין את הסיכון לפגיעה באזורי מוח חיוניים במהלך ניתוח המוח, ולהגדיל את דיוק הפעולה תוך פולשנות מזערית.

הרובוט מתוכנן לסייע בנטילת ביופסיה כחלק מאבחון גידולי מוח, ובגירוי מוחי עמוק שמהותו השתלת משדרים בתוך המוח אשר שולחים אותות חשמליים לאזורים ספציפיים בעומק המוח. שיטה זו מקובלת כיום לטיפול בהפרעות תנועה מסוג פרקינסון וכטיפול בחולי דיכאון קשים.

המערכת הרובוטית כוללת תוכנה אשר מאפשרת למנתח לתכנן את הניתוח מבעוד מועד על גבי הדמיית תלת מימד של מוחו של המנותח. התכנון מאפשר לזהות מכשולים כגון אזורים בהם לא רוצים לפגוע, ולתכנן מסלול בטוח ומדויק לנקודה הרצויה בעומק המוח.

השיטה המקובלת כיום בניתוחי מוח היא שימוש במערכות ניווט, שמסייעות למנתח להגיע לאזור היעד בצורה מדויקת. מערכות אלו רק מראות למנתח כיצד הוא מתקדם, בעוד הרובוט מאפשר למנתח להגיע למיקום שהוא תכנן מבעוד מועד, בצורה מדויקת ואמינה.

התוכנה במערכת הרובוטית מתייחסת לרכיבים נוספים באזור המנותח, ובכך משפרת את ביצוע הניתוח.

* הדגם מוצג באדיבות חברת מזור רובוטיקה

אלן טיורינג

האיש שהגה את המחשב לפני כולם

אלן טיורינג תרם במידה כה רבה למדעי המחשב עד כי לא ניתן לדמיין תחום זה כיום בלי היסודות שטיורינג העמיד - ואת כל זאת הוא עשה לפני שהיו מחשבים בעולם כלל! בחייו הקצרים הגה טיורינג את עצם הרעיון של מחשב בר־תיכנות ואת עמודי התווך העיוניים שלו, והניח את היסודות לתחומים מרכזיים המצויים בבסיס מדעי המחשב עד ימינו.

מדען גאון, ולא רק בתאוריה

בד בבד עם היותו מתמטיקאי טיורינג היה גם איש מעשה, ובשנת 1946 הוא פיתח את אחד המחשבים היישומיים הראשונים, שהיה אז המחשב המהיר בעולם. סקרנותו אף הובילה אותו לחקור נושאים בחזית המתמטיקה, התְּמָרָה, התְּכָנָה, הכימיה והביולוגיה.



הגיבור הנעלם של הניצחון על גרמניה הנאצית

עם פרוץ מלחמת העולם השנייה השתמש הצבא הגרמני במכונת הצפנה משוכללת בשם "אניגמה" שנחשבה בלתי ניתנת לפיצוח. האנגלים העניקו עדיפות עליונה לשבירת הצופן הזה, ואלן טיורינג היה זה שהשיג את פריצת הדרך המתמטית שאפשרה לפצח את צופן ה"אניגמה". היכולת לצותת לכל השדרים של האויב שיחקה תפקיד מרכזי בניצחון בעלות הברית, אולם תרומתו של טיורינג נשמרה בסוד עוד שנים רבות אחרי מותו.

האם המחשב יכול לחשוב?

כבר בהיותו בן 24 טיורינג הבין את ההקבלה בין המחשב ובין המוח האנושי, והיה הראשון ששאל "האם מכונות יכולות לחשוב?". בכך הפך לחוקר החלוץ של תחום הבינה המלאכותית, וניסח את 'מבחן טיורינג' המפורסם שמטרתו להבחין אם מחשב נתון חושב או לא. כפועל יוצא הוא חייב אותנו לשקול את הדומה והשונה בין מוחנו ובין המחשב, ותרם תרומה משמעותית לתחום הפילוסופיה של הנפש.

סוף טרגי

טיורינג היה הומוסקסואל, בתקופה חסרת סובלנות שבה החוק הבריטי ראה בכך פשע פלילי חמור. משהתגלה הדבר לשלטונות הוא הועמד לדין, הורשע והוכרח לעבור טיפול תרופתי קשה שדחף אותו לשים קץ לחייו והוא בן 42 בלבד. אל העוול שנגרם לאחד מגדולי המדענים בדורו מצטרפת תחושת החמצה קשה - מי יודע מה היה טיורינג ממשיך לחדש לו הניחו לו לחיות?

ה"אניגמה"

הצופן הגורלי

מכונת ההצפנה "אניגמה" שימשה את הצבא הגרמני להצפנת כל השדרים האלחוטיים שלו במלחמת העולם השנייה. הגרמנים האמינו שההצפנה חזקה במידה שאיש לא יוכל לה – טעות שהובילה אותם לשאננות מסוכנת. שבירת הצופן הזה בידי אלן טיורינג ועמיתיו שיחקה תפקיד מרכזי בהשגת הניצחון על גרמניה הנאצית.

159 ביליוני-ביליוני מפתחות

ה"אניגמה" מאפשרת להפוך שְׁדָר גלוי לסדרה של אותיות חסרות משמעות, ולהיפך. ההצפנה מבוססת על ערבוב של האותיות באמצעות גלגלי הצפנה. על מנת לפענח את השדר יש להעביר אותו ב"אניגמה" כשהגלגלים מסודרים באותו מצב, הקרוי "מפתח", כמו במכונה שהצפינה אותו. כמובן שהמפתח של כל שדר שקלטו האנגלים לא היה ידוע להם. ניסיון אקראי של מפתחות לא היה מועיל לאנגלים, כיוון שב"אניגמה" היו 159 ביליוני-ביליונים של מצבים אפשריים...

הגאון וה"בומבה"

על מנת לטפל ב"אניגמה" פיתחו טיורינג וצוותו מכונה בשם "בומבה" (שהתבססה על פיתוח קודם של מפצחי צפנים בפולין), אשר יכלה לבחון במהירות רבה מצבים שונים של גלגלי ההצפנה. משימה זו לא הייתה ברת ביצוע נוכח ריבוי המצבים האפשריים, אלמלא טיורינג הצליח לזהות, באמצעות שיטות מתמטיות מתוחכמות, קיצורי דרך שהפחיתו מאוד את מספר הבדיקות הנדרש. כתוצאה מכך הצליח הצוות לפענח את מרבית השדרים הגרמניים.

קרדיטים

אוצר: נתן זלדס

אוצר ומפתח מוצגים: ד"ר אמיר בן שלום

יועץ מדעי: ד"ר ערן לונדון

עיצוב התערוכה: פרופ' חנן דה לנגה

עיצוב המוצגים: אייל פוגל

עיצוב גרפי: קטי גורנדה

בנייה: הצוות הטכני של מוזיאון המדע ע"ש בלומפילד ירושלים

Bloomfield
Science Museum
Jerusalem

متحف العلوم
على اسم بلومفيلد
القدس

מוזיאון המדע
ע"ש בלומפילד
ירושלים

