מבוא

ברוכים הבאים לקורס אלגוריתמים קוונטיים!

1 קצת בירוקרטיה

הרצאות. ההרצאות ייערכו ביום א', בין 10:10 ל- 13:00 בניין צ'ק־פוינט, חדר 002.

ההרצאות יינתנו בעברית ויתבססו על כתיבה על הלוח (כלומר, ללא מצגות). איננו נצמדים לספר או מקור יחיד; בסוף השבוע שלפני כל הרצאה אפרסם רשימות מלאות בעברית לשיעור הקרוב. כל החומרים (רשימות, תרגילי בית וכו') יתפרסמו באתר הקורס:

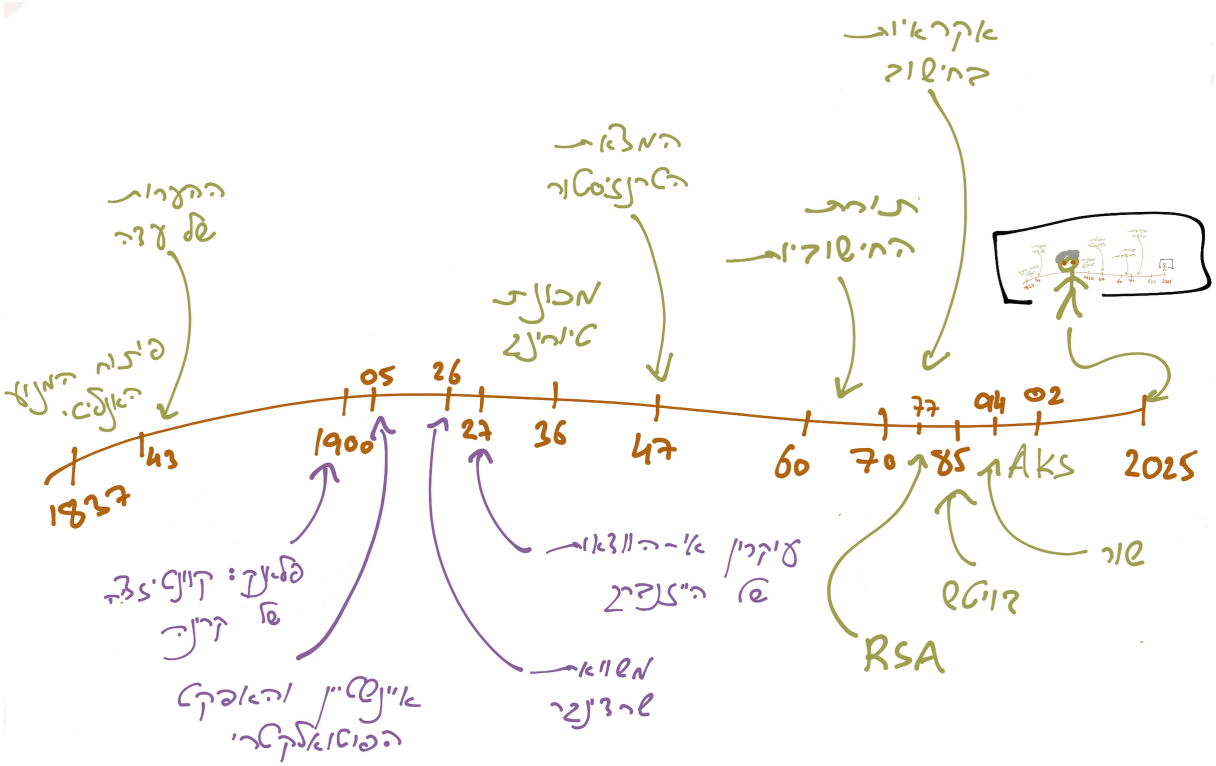
https://www.gilcohen.org/2025-quantum-algorithms

צילומי ההרצאות יועלו לפנופטו ויהיו נגישים עבורכם. עם זאת, ההגעה לשיעורים מומלצת בחום, ובכל מקרה לא תתאפשר השתתפות מקוונת דרך זום. שעת קבלה: יום שני ב-10:10 בצ'ק פוינט 244, ובכל מקרה אני זמין במייל coheng@gmail.com לכל שאלה.

שיעורי בית ומבנה הציון. במהלך הסמסטר יפורסמו תרגילי בית אך הם אינם להגשה. מומלץ מאוד לפתור אותם כדי להעמיק את ההבנה. בסוף הסמסטר תיערך עבודת בית מסכמת במתכונת מבחן בית. במועד שייקבע מראש ייפתח חלון של 24 שעות להגשה. בהתאם למספר הנרשמים, נעדכן אם העבודה תהיה ביחידים או בזוגות. מבנה העבודה: כמחצית מהשאלות יהיו זהות או וריאציות קלות של שאלות מתרגילי הבית, והחצי השני יורכב משאלות חדשות. הציון הסופי יתבסס על עבודת הבית בלבד.

תרגולים. התרגולים יינתנו ביום ד' בין 15:10 ל-16:00 באודיטוריום לב. חלק מן התרגולים יוקדש לחזרה על חומר ההרצאה דרך דוגמאות; בחלקם יוצג חומר משיק חדש. לעיתים תתבקשו לפתור שאלות מראש ובתרגול נדון בפתרונות. נשמח להזמין סטודנטים להציג (ללא חובה); הציפייה היא להגיע לאחר שהתמודדתם עם השאלות בכדי למקסם את האפקטיביות בתרגולים מהסוג הזה. הקלטות התרגולים לא יועלו לפנופטו. הן יינתנו למשרתים במילואים ובמקרים חריגים אחרים באישור פרטני של איתי. שעת הקבלה של איתי תיערך מיד לאחר התרגול (בשבוע הראשון לא תתקיים שעת קבלה). ובכל מקרה, איתי זמין במייל itaileigh@tauex.tau.ac.il.

2 חישוב בראי היסטורי



2.1 טיורינג וצ'רץ'

במובן מסוים, מאמרו המפורסם של אלן טיורינג משנת 1936, On Computable Numbers, מסמן את רגע הלידה של תורת החישוביות. במאמר זה הציע טיורינג מודל מתמטי מופשט הלוכד את מושג החישוב: כל הליך חישובי "אמיתי" אמור להיות ניתן למימוש במודל זה. המכונה האוניברסלית של טיורינג מגלמת אפוא את מהות החישוב. הנחת עבודה זו מכונה **תזת צ'רץ'–טיורינג** (Church–Turing Thesis).

טיורינג, עם זאת, לא היה הראשון למדל את מושג החישוב. אלונזו צ'רץ' הציע מודל משלו והציג את עיקריו כחודש לפני שטיורינג שלח את מאמרו לפרסום. טיורינג היה מודע והתייחס למודל של צ'רץ' ואף הוכיח שקילות בין שני המודלים. צ'רץ' עצמו דחף את הפורמליזציה של טיורינג, ובהמשך שימש כמנחה של טיורינג לדוקטורט בפרינסטון. כמו היום גם אז פרינסטון היה מוסד מכובד, ובאותה תקופה פעלו באזור חוקרים כמו קורט גדל וג'ון פון נוימן.

2.2 עדה ובבג'

תרומה מוקדמת במיוחד שקדמה לכל אלה היא של עדה לאבלייס (Ada Lovelace). בשנת 1843 הוסיפה לאבלייס "הערות" מקיפות לתרגום מאמר על המכונה האנליטית של בבג', שבהן הבהירה את עקרונות הפעולה של

מכונה מתוכנתת כללית וצירפה תכנית מפורטת לחישוב מספרי ברנולי — התיאור הפומבי הראשון של אלגוריתם שיועד לביצוע על־ידי מכונה כללית. לאבלייס הדגישה שמכונה כזו מטפלת *בסימנים* לפי כללים, ולא רק במספרים; לפיכך, עקרונית, היא יכולה לעבד גם מוזיקה וטקסטים, כשהיחסים ניתנים לייצוג סמלי. היא הבחינה, במונחי זמנה, בין מנגנון החומרה לבין ההוראות והנתונים, ודיברה על הצורך ב"מדע הפעולות" (science of operations). במובן זה, לאבלייס סיפקה תיאור חזוני ומעמיק של מה יכולה לעשות מכונה מתוכנתת כללית, ואף פרסמה דוגמה קונקרטית — צעד מרכזי בהתפתחות מושג ה"תוכנה".

לשם קנה־מידה היסטורי: כל זה התרחש כ־90 שנה לפני עבודתו של טיורינג — בערך אותו פרק זמן המפריד בין טיורינג לבינינו. טיורינג, אגב, התייחס במאמרו לטענות של לאבלייס בנוגע ליכולת של מכונה "לחשוב".

צ'ארלס בבג' היה מתמטיקאי ומהנדס בריטי חלוצי, שתכנן מכונות חישוב וניסה להוציאן אל הפועל מן הבחינה ההנדסית. בשנת 1822 החל בפיתוח **מנוע ההֶפְרֵשִׁים**—מכונת חישוב שייעודה לבצע פעולות מתמטיות פשוטות. הבנייה לא הושלמה בשל מחסור בתמיכה ובהיות הפרויקט מקדים את זמנו. מעניין לציין כי בשנת 1991 נבנה דגם עובד לפי תרשימיו של בבג'. בשנת 1837 כבר עבד בבג' על יצירת המופת שלו—**המנוע האנליטי**—והמשיך בכך עד מותו ב־1871, אף שהיה ברור לו שהמכונה לא תיבנה בימי חייו ושגם תכנונה יארך זמן רב מדי.

לתכנונו של בבג' מכנה משותף רחב עם ארכיטקטורת המחשבים המודרנית: יחידת עיבוד לוגי, זיכרון, ויחידות קלט/פלט. הזיכרון שהקצה—1000 מספרים בני 50 ספרות—היה שאפתני וכנראה לא ריאלי; לשום מחשב שנבנה לפני שנות ה־60 לא היה זיכרון בסדר גודל כזה. בנוסף, אחת התכונות שתכנן, **קפיצה מותנית**, חסרה בכמה מן המחשבים הראשונים.

למרות שבישר את רעיון המחשב ואת יחידותיו המרכזיות, השפעתו הישירה של המנוע האנליטי על תכנון המחשבים שבאו אחריו אינה ברורה וככל הנראה אינה גדולה. מתכנני המחשבים הראשונים בדרך כלל לא הכירו את עבודתו ונאלצו להמציא מחדש חלק מרעיונותיו. אחד הגורמים לכך הוא שהתכנון, שלא הושלם, לא פורסם מעולם בצורה מסודרת; במשך שנים רבות היו ההערות של לאבלייס המקור העיקרי למידע על המנוע האנליטי.

2.3 בין רעיון למכונה: חישוב מופשט ומחשבים ממשיים

הקשר בין התאוריה למעשה—בין הפשטת מושג החישוב לבין האתגרים הטכנולוגיים הכרוכים בבניית מכונה פיזית שממממשת את ההפשטה—הוא מוטיב חוזר ומהותי בחקר המחשוב, ורלוונטי במיוחד בהקשר של חישוב קוונטי. כיום אנו מצויים בנקודה שבה התאוריה מקדימה את ההנדסה, אך נדמה שההנדסה פורחת, דבר שמעורר התלהבות גם בקרב התאורטיקנים.

אם נחזור אחורה בזמן, בשנת 1947 התרחשה פריצת הדרך ההנדסית המשמעותית ביותר במחשוב הקלאסי, כאשר ג'ון ברדין, וולטר ברטיין וויליאם שוקלי המציאו את הטרנזיסטור. בקורס הזה נתמקד בהיבט המופשט של חישוב קוונטי ולא ניגע כלל באספקטים המרתקים של בניית מחשב קוונטי.

2.4 יעילות

תזת צ'רץ'–טיורינג מחזיקה עד היום: כל תהליך חישובי ישים ניתן לסמלץ על גבי מכונת טיורינג. בשנות ה־60 וה־70 בסדרה של מאמרים מאת קובהאם, אדמונדס, הרטמניס, סטרנס, בלום ואחרים עבר המוקד מן השאלה "מה ניתן לחשב?" אל השאלה "מה ניתן לחשב **ביעילות**?", וכך נולדה **תורת הסיבוכיות**. בהקשר זה נוסחה גם **התזה החזקה של צ'רץ'–טיורינג**, שלפיה כל אלגוריתם במודל חישוב "סביר" ניתן למימוש *יעיל* באמצעות מכונת טיורינג; כלומר, בעיה שניתנת לפתרון יעיל במודל חישוב מתקבל על הדעת ניתנת לפתרון יעיל גם במודל של מכונת טיורינג. יעילות, כנהוג, נמדדת בזמן ריצה: אלגוריתם נחשב יעיל אם זמן הריצה שלו פולינומי באורך הקלט, ובהקשר של בעיות הכרעה מתייחס למחלקה $\mathbf{P}$. לתזה זו הועלו לאורך השנים כמה אתגרים:

2.4.1 מחשוב אנלוגי

כהערת שוליים היסטורית, אחת מההפרות לכאורה של ההתזה נגעה למודל של מחשוב אנלוגי: כמה חוקרים הוכיחו כי במודל זה ניתן לפתור ביעילות בעיות מסוימות שאינן ניתנות לחישוב כלל במודל של טיורינג. רוב הטענות ל"מעבר לטיורינג" במודלים האנלוגיים נשענות על הנחות של דיוק אינסופי והיעדר רעש. בהמשך הראו חוקרים כי תחת מגבלות פיזיקליות—דיוק סופי ונוכחות רעש—אין בכך הפרה של התזה. עבודות אלה חידדו את ההבחנה בין מודלים מתמטיים אידאליים לבין מימושים פיזיקליים. יתרה מזו, הן מדגישות שגם מודל מופשט צריך להתכתב עם המציאות ולשקף את המגבלות הפיזיקליות של החישוב.

2.4.2 הטלות מטבע

בהקשר של התזה החזקה של צ'רץ'–טיורינג אמצע שנות ה־70 סימנו מפנה: בשנת 1977 הציגו סולובייי–שטרסן מבחן ראשוניות אקראי אשר רץ בזמן פולינומי. באותה תקופה לא היה ידוע אלגוריתם דטרמיניסטי בזמן פולינומי לבדיקת ראשוניות, ולכן הופעת אלגוריתם אקראי יעיל נתפסה כאתגר משמעותי לתזה החזקה, והבליטה את כוח הרנדומיזציה באלגוריתמיקה.

מעניין לציין כי כשנה קודם לכן הציג מילר מבחן דטרמיניסטי המותנה בהשערת רימן המורחבת, שהיווה רמז לכך שלפחות לבעיית בדיקת הראשוניות עשוי להתקיים אלגוריתם דטרמיניסטי. ואכן, אחרי כ-25 שנה, פורסם אלגוריתם AKS בשנת 2002 במאמר PRIMES is in P. זהו המבחן הדטרמיניסטי הראשון בזמן פולינומי לראשוניות שאינו נשען על השערות לא־מוכחות, ובכך "סגר את המעגל" שנפתח במבחן המותנה של מילר (1976) ובמבחנים האקראיים מסוף שנות ה־70. בהמשך הופיעו פישוטים ושיפורים אך מבחינה היסטורית חשיבותו של AKS היא הקביעה הסופית כי בדיקת ראשוניות נמצאת במחלקה $\mathbf{P}$.

מכיוון שאקראיות היא משאב פיזיקלי סביר—משהו שניתן לממש בפועל—עם עליית האלגוריתמים האקראיים בשנות ה־70–80 נעשה מקובל לנסח את התזה החזקה כך שהיא כוללת גם אלגוריתמים אקראיים. במונחי מחלקות סיבוכיות, מחלקת הבעיות הניתנות להכרעה ביעילות (זמן פולינומי באורך הקלט) היא לכן $\mathbf{BPP}$.

מושג האקראיות נחקר לעומק חסר תקדים מרגע שנכנס למסגרת של תורת הסיבוכיות. בפרט, פותחו אלגוריתמים הנקראים **מחלצי אקראיות** (Randomness extractors) המאפשרים "לזקק" מקורות אקראיות חלשים (כמו

אלה שבטבע) לביטים כמעט־אחידים וכמעט־בלתי־תלויים כפי שנדרש לאלגוריתמים אקראיים.

במקביל, בעקבות קו מחקר מפתיע ומרתק—ובמיוחד המתודולוגיה של Hardness-Randomness Tradeoff של ניסן־ויגדרזון (1988) והמשכיה—הדעה הרווחת היא שאקראיות אינה מוסיפה כוח חישובי מבחינת יעילות, כלומר $\mathbf{BPP} = \mathbf{P}$. עם זאת, ידוע שהתקדמות משמעותית להוכחת שוויון זו כרוכה בחסמים תחתונים חזקים למעגלים בוליאניים, אתגר שעדיין מעבר ליכולתן של הטכניקות הקיימות. מכל מקום, עמדת הרוב היא שאף שאקראיות היא כלי חשוב ושימושי, היא אינה מוסיפה כוח חישובי יעיל—ולכן אינה מאתגרת את התזה החזקה של צ'רץ'־טיורינג בנוסחה המקורי.

2.4.3 חישוב קוונטי

האם ייתכן חיזוק נוסף לתזת צ'רץ'־טיורינג שאנו מפספסים? בשנת 1985 הציע דויטש לבסס את התזה על עקרונות פיזיקליים במקום לחשוב על מודלים אד-הוק. הרעיון פשוט ונגענו בו קודם: חישוב בסופו של יום הוא תהליך פיזיקלי. כדי שחישוב יתרחש, מערכת חייבת להשתנות—להעביר חום, לצרוך או לשחרר אנרגיה, לנוע. לכן גם ההפשטה התאורטית של חישוב צריכה להישען על חוקי הפיזיקה. בהתאם לכך הציע דויטש למסגר את מושג החישוב בתוך המכניקה הקוונטית, שבינתיים כבר התגבשה ושלטה בפיזיקה זה כחמישה עשורים; והוא שאל: אם נאפשר לאלגוריתמים לנצל תופעות קוונטיות—האם נשיג שיפור ביעילות החישוב?

דויטש, ואחריו חוקרים נוספים, הראו שישנן בעיות—גם אם אינן מרתקות כשלעצמן—שמחשב קוונטי יכול לפתור מהר יותר ממחשב קלאסי אם כי פורמלית במונחי תורת הסיבוכיות מדובר ב Oracle model. לקהילת מדעי המחשב לקח זמן לאמץ את הרעיונות הללו, ולא מעט מאמרים פורצי־דרך נדחו שוב ושוב מכנסים מובילים. המאמר ששינה את התמונה היה ללא ספק של פיטר שור ב-1994, שהראה אלגוריתם קוונטי יעיל לפירוק מספרים לגורמים. בעיה זו עומדת בבסיסה של הצפנת RSA, המבוססת על האמונה שאין אלגוריתם קלאסי יעיל לפירוק; לפיכך, התוצאה של שור סימנה נקודת מפנה דרמטית. השאלה לגבי הקשר בין חישוב קוונטי לקלאסי ובפרט האם $\mathbf{BQP} \stackrel{?}{=} \mathbf{P}$ היא שאלה פתוחה מרתקת.

מאז ידע תחום החישוב הקוונטי תקופות של פריחה לצד תקופות דלות יותר—במונחי עניין ציבורי, היקף פעילות אקדמית ומספר החוקרים במוסדות מובילים. נדמה שהיום, בעיקר בעקבות התפתחויות הנדסיות־טכנולוגיות, מימון ותחרות גאו־פוליטית, ואולי גם מחזור הייפ טבעי, העניין בתחום הגיע לשיא חדש והוא "חם" מתמיד. כך או כך, זהו תחום שהוא תערובת יפהפייה של חישוב, מתמטיקה ופיזיקה, וכל תירוץ ללמוד עליו יתקבל בברכה.

3 מה נלמד בקורס?

הקורס מחולק לארבעה פרקים. זוהי הפעם הראשונה שבה אני מעביר אותו, ולכן הסילבוס טנטטיבי ונתון לשינויים.

פרק 1 — היכרות עם תורת הקוונטים

ביחידה זו נציג את עקרונות היסוד של תורת הקוונטים כפי שהם רלוונטיים למודל החישובי. נלמד על המושג של קיוביט—המקבילה של הביט הקלאסי—על פעולות שניתן לבצע בקיוביטים ועל מדידתם. לעבודה בחישוב קוונטי יש אופי מתמטי, וכלי העבודה המרכזי הוא אלגברה לינארית; לכן נקדיש חלק מן הזמן בפרק זה ליישור קו מתמטי. לאורך הקורס נעבוד במתכונת מופשטת עם המודל המתמטי של קיוביט. עם זאת, ביחידה הבאה (ורק בה) ניגע בקצרה בניסוי פסאודו־פיזיקלי, כדי לתת טעימה אינטואיטיבית של הצד הפיזיקלי.

פרק זה מחולק ליחידות הבאות

- יחידה 2 - ניסויים מטרידים: סופרפוזיציה וקריסה קוונטית
- יחידה 3 - היכרות ראשונה עם קיוביטים
- יחידה 4 - ניסוי הפצצה של אליצור-ויידמן
- יחידה 5 - המכפלה הטנזורית של מרחבים וקטורים
- יחידה 6 - מערכות מרובות קיוביטים

פרק 2 — תופעות ופרוטוקולים קוונטיים

בחלק זה נציג יישומים מרתקים של תופעות קוונטיות שאינן כרוכות בחישוב full-fledged. ברוב היחידות נתמקד במערכת של שני קיוביטים. כך נוכל להתרגל לכללים החדשים—ולעתים מוזרים—של החישוב הקוונטי, ולהתאמן בכלים המתמטיים הנדרשים, לפני שנעבור לאלגוריתמים הפועלים על מספר רב של קיוביטים.

- יחידה 7 - משחק CHSH והפרת אי־שוויון בל
- יחידה 8 - משפט אי־השכפול (No-Cloning Theorem)
- יחידה 9 - טלפורטציה קוונטית (Quantum Teleportation)
- יחידה 10 - כסף קוונטי

פרק 3 — חישוב קוונטי

בחלק זה של הקורס נכיר את פורמליזם החישוב הקוונטי—מודל המעגלים הקוונטיים—ונבנה בהדרגה אל כמה אלגוריתמים מרכזיים. בפרט נעסוק באלגוריתם של שור לפירוק לגורמים ובאלגוריתם של גרובר (Grover) לחיפוש בלתי־מובנה. מידע מפורט על תכני היחידות יפורסם בהמשך הסמסטר.

פרק 4 — נושאים מתקדמים

אם יישאר זמן, נעסוק בקצרה בנושאים מתקדמים שאבחר במהלך הסמסטר. כאן המקום לציין כי אמנון תא־שמע יעביר בסמסטר הבא קורס בנושא **אינפורמציה קוונטית**, המהווה למעשה קורס המשך לקורס הנוכחי.