האוניברסיטה העברית בירושלים
בית הספר להנדסה ולמדעי המחשב על שם רחל וסלים בנין
החוג למדעי המחשב

אבחון בתורה קוונטית

מוגש על ידי
דויד פונרובסקי

עבודת גמר לתואר מוסמך במדעי המחשב

עבודה זו הונחתה על ידי
פרופ' מיכאל בן אור

אוגוסט 2023

תקציר

מחשוב קוונטי הוא מודל חישוב מבטיח, הקונצנזוס הרווח הוא קיימות בעיות אותן ניתן לפתור באופן יעיל באמצעות מחשבים קוונטים אך הן קשות בכדי לפתור אותן עם המחשבים הקלאסים. הדוגמה הבולטת היא הסימולציה הכימית, בעוד שהאנושות היום יודעת לסמלץ ריצה של מעגלים חשמליים, חוזק של מבנים וטיסות של מטוסים איננו מסוגלים, גם בעזרת מחשב העל החזק ביותר בכדו"א, לסמלץ את התפתחות בזמן של מולקולה בת 80 אטומים. השיטה הנאיבית לסימלוץ קלאסי תדרוש מאיתנו לעקוב אחר מס' אקספוננציאלי במספר האטומים של משתנים בזכרון. לעומת זאת, חומרה קוונטית -או מכניקת הקוונטים- מאפשרת קידוד יעיל של המולקולה באופן זהה למבנה שלה בטבע. אמנם איננו יודעים להוכיח כי אין אלגוריתמים קלאסיים שמסמלצים מולקולות בזמן מהיר אך אנו יודעים להגיד בוודאות סימולציה הקוונטית היא קלה למימוש, רצה בזמן מהיר ויעלה בשימוש של משאבי זכרון. על כן החזון העומד לנגד עיני רוב המומחים הוא שבעתיד תהליך פיתוח התרופות והנדסת החומרים יהפוך לשיטתי, אם היום, מרגע שחוקר מציע מועמדים לתרופות או חיסונים, נדרשים לחכות זמן רב לאישור הסימולציה בעתיד החוקר יקבל תשובה בזמן אמת על מסך. בדומה לקלות שהיום אנשים מסוגלים לשתף ספריות של קוד או חומרה, להקים חברות ולשחרר מוצרים כך שבעתיד נראה תעשיה מורכבת ומקושרת שמתעסקת בפיתוח התרופות, חומרים, הנדסה גנטית ועוד.

ישנה רק בעיה קטנה, אומנם אין ויכוח כי מודל החישוב הקוונטי חזק מהמודל הקלאסי אך כלל לא ברור מודל החישוב הקוונטי בכלל ניתן למימוש, זאת מאחר והרכבים הבסיסים בחומרה הקוונטית נוטים לסבול משגיאות רבות, יותר מכך, נכון להיום אין לנו מחשבים קוונטים שמתגברים על השגיאות וכל חישוב ארוך מעט צובר מספיק שגיאות עד כי תוצאת החישוב סופית שקולה לג'יבריש. מול בעיה דומה עמד וון-פון ניומן, בין ממציאי המחשב הקלאסי, לפני קצת פחות ממאה, פון ניומן שאל האם חישוב קלאסי בכלל אפשרי? האם ניתן להתגבר על הרעש? הוא ענה על השאלה בחיוב. ראוי לציין שמאז גם החומרה התקדמה ורוב הרעיונות של "חישוב חסין לשגיאות" לא ממושו, אבל בהחלט חלק גדול מהרעיונות מומשו ומהווים רכיבים קריטיים במוצרים יומיומיים בהם אנו משתמשים, דוגמה בולטת היא תקשורת סלולרית בפרוטוקול $G5$ המשתמש בקודי $LDPC$ (עליהם נרחיב בעבודה) כדאי לתקן שגיאות. באופן דומה חוקרים הראו כי ניתן להכליל את הרעיונות הקלאסים למקרים הקוונטים כדי לאפשר "חישוב קוונטי חסין לשגיאות". בבסיס הרעיונות עומד קידוד מיוחד בקוד המאפשר לזהות ולתקן שגיאות בקלות.

נוסף על קודים שמתקנים שגיאות קיימים גם קודים הניתנים לבדיקה באופן יעיל. כדאי להבין מהם קודים ניתנים לבדיקה כדאי לדמיין בראש פאזל בו כל החתיכות צבועות בדיוק באותו הצבע. פאזל כזה יקרא לא ניתן לבדיקה אם קיימת השמה של חלקי הפאזל כך שמצד אחד כדאי להגיע אליה יש להחליף חצי מהחלקים ב"ההשמה האמית" של הפאזל -כלומר הדרך הנכונה לחבר אותו- אך מצד שני קיימות מספר בודד של אי התאמות בין חיבורי החלקים השונים. כלומר צריך לעבוד הרבה כדאי להגיע ל"ההשמה האמיתית" אך אם דוגמים חיבור שרירותי, בסיכוי אפסי נראה סתירה. פאזלים הניתנים לבדיקה הם בדיוק ההפך הגמור, אם השמה רחוקה מאוד מלהיות "ההשמה האמיתית" אז בהסתברות גבוהה בדיקה שרירותית תחשוף זאת. קיומם של קודים קוונטים טובים וקודים קלאסיים הניתנים לבדיקה יעילה היו שאלות פתוחות במשך זמן רב, למרות שנראה שאין קשר ישיר ביניהם שניהם נפטרו באבחה אחת בבניה מתקדמת שפותחה רק לפני שנתיים (2021). מעניין לשאול האם מדובר בצירוף מקרים,או שיש קשר עמוק יותר בין השתיים שאיננו מבינים עוד.

בעבודה זאת, אנחנו סוקרים, מקצה לקצה, קודי מתקני השגיאות הקוונטים. אחל מסקירה רחבה של קודים קלאסיים, שיטות לבנייה של קודים טובים, אפיון של רעש קוונטי וקודים קוונטים פרימיטיבים ועד לבניה המתקדמת של קודים קוונטים $LDPC$ טובים. כל זאת לצד סקירה של קודים הניתנים לבדיקה. לבסוף אנחנו מציגים ניסיונות, כושלים, במחקרי המשך, בפרט ניסיון להגיעה לבניה של

קודים קלאסיים הניתנים לבדיקה מבלי לפתח במקביל גם קודים קוונטים טובים. אם היינו מצליחים לבודד את התוצאות הדבר היה מצביע על כך שהעבודה ששניהם פותחו באותה בניה היא מקרית לחלוטין. יחד עם זאת, לא התקדמנו מספיק רחוק כדאי לעלות חשד סביר שקיים קשר הכרחי.

העבודה מניחה רק ידע בסיסי באלגברה לינארית וקומבינטוריקה, אנו סבורים שכל בוגר מדעי המחשב יוכל להנות מקריאה, להבין באופן טוב מאוד את הנושא, ולהעזר בה כדאי להתחיל מחקר בתחום.