האוניברסיטה הפתוחה

המחלקה למתמטיקה ולמדעי המחשב

הצעה ומדריך למידה לקורס

"מבוא לחישוב קוונטי"

עבודה מסכמת זו הוגשה כחלק מהדרישות לקבלת תואר

"מוסמך למדעים" .M.Sc במדעי המחשב

באוניברסיטה הפתוחה

החטיבה למדעי המחשב

על-ידי

עופר אוחיון

ת.ז. 024909426

העבודה הוכנה בהדרכתו של ד"ר **מיכאל לנגברג**

פבואר 2010

תודות:

ברצוני להודות לד״ר מיכאל לנגברג על עזרתו הרבה בהכנת עבודת גמר זו- הן בהבהרת החומר והן בהערות הפדגוגיות בכתיבת המדריך.

תקציר

חישוב קוונטי הינו מודל מתמטי המבוסס על המודל הקוונטי. מודל זה הינו בעל חשיבות עצומה למדעי המחשב שכן הוא מציג את מכונת טיורינג הקוונטית – מודל מתמטי המאפשר פתרון יעיל למגוון בעיות אשר לא ידוע להן פתרון יעיל במכונת טיורינג הקלאסית. לדוגמה:

1) פירוק לגורמים- בבעיה זו המטרה הינה לפרק מספר לשני המחלקים הלא טרוויאלים שלו. מספר אלגוריתמי הצפנה (כדוגמת הRSA הנפוץ) נעזרים בעובדה כי האלגוריתים הקלאסי הידוע והיעיל ביותר פותר בעיה זו בסיבוכיות זמן אקספוננציאלית לאורך הקלט, כך שפירוק לגורמים של מספר בן 5000 ספרות יערך כ5 טרילון שנה. לעומת זאת, פירוק לגורמים על גבי מכונת טיורינג קוונטית , תוך שימוש ב״אלגוריתים של שור״ יערך בסיבוכיות זמן פולינומיאלית לאורך הקלט- ע״כ פירוק לגורמים של מספר בן 5000 ספרות יכול לערוך מספר רגעים.

2) חיפוש- בבעיה זו הקלט הינה רשימה L לא מסודרת של n איברים, ופונקציה f הממפה כל איבר מL לטווח $\{0,1\}$. המטרה הינה למצוא את כל האיברים ברשימה הממופים ל1. במכונת טיורינג קלאסית, ידוע כי הפתרון הטוב ביותר הינו בעל סיבוכיות זמן פרופורציונלי לאורך הרשימה. מכונת טיוריג קוונטית הנעזרת באלגוריתם של גרובר, לעומת זאת, פותרת את הבעיה בסיבוכיות זמן פרופרציונלית לשורש אורך הרשימה.

קורסים בחישוב קוונטי מוצעים ע״י אוניברסיטאות מובילות (Caltech, Berkley, הטכניון, אוניברסיטת ת״א, האוניברסיטה העברית ביורשלים ועוד) אך עדיין לא באוניברסיטה הפתוחה. עבודת גמר זו מציעה קורס חדש עבור האוניברסיטה הפתוחה בכדי לגשר על פער זה. העבודה כוללת הצעה לתכני הקורס, השוואה לקורסים אחרים ומדריך למידה (העומד בפני עצמו) המכסה את רוב חומר הלימוד בקורס המוצע.

- **מטרת העבודה**

כתיבת מדריך למידה חלקי לקורס מבוא בחישוב קוונטי (קורס מתקדם לתואר ראשון או קורס לתואר שני). מדריך הלמידה יעמוד בפני עצמו (self contained) ולא ישמש כהשלמה לספר קורס.

- **מבנה העבודה**

העבודה מורכבת משני חלקים. בחלק הראשון הצעה מפורטת לקורס כולל הצעה למבנה מדריך הלמידה. החלק השני הינו מספר פרקים ממדריך הלמידה כולל רשימת מקורות.

חלק ראשון:
הצעה לקורס

מבוא לחישוב קוונטי

הצעה לקורס

ד״ר מיכאל לנגברג ועופר אוחיון

1. מאפיינים

שם הקורס: מבוא לחישוב קוונטי.

תחום: מדעי המחשב (תואר ראשון או תואר שני).

רמה: מתקדם.

נקודות זכות:.

ידע מוקדם נדרש: חישוביות ומבוא לסיבוכיות (20365) או סיבוכיות חישובית (20545) או מבוא לתורת החישוביות והסיבוכיות (20585).

אלגברה לינארית I (20109) או אלגברה לינארית לתלמידי מדעי הטבע (20430).

קהל היעד: סטודנטים לתואר שני במדעי המחשב.

אחריות אקדמית:

פיתוח: ד״ר מיכאל לנגברג ועופר אוחיון

2. רקע

חישוב קוונטי הינו ענף חדש יחסית במדעי המחשב, אך עם זאת נושא בחובו הבטחה לפריצת דרך. קורס זה המשלב בין פיזיקה מתקדמת למדעי המחשב יספק לסטודנט כלים בסיסים בנושא חשוב זה, ויחשוף את הסטודנט בפני כלים חדשים ותיאוריות העומדות בחזית המדע כיום.

מספר אוניברסיטאות מובילות בעולם בתחום מדעי המחשב מציעות קורסים בנושא זה, ובכללן: הטכניון (236990 -מבוא לעיבוד אינפורמציה קוונטית), אוניברסיטת ת״א (Quantum Computing - 0368-4057-01), אוניברסיטה העברית בירושלים (67596- Introduction to Quantum Computation)

ברקלי (Quantum Computation CS294-2) , אוקספורד (CCS3b: Quantum Computer Science), קלטק (Quantum Computation Physics 219/Computer Science 219) ועוד.

3. מבנה הקורס

הקורס נבנה ע"ס הסילבוס שנאסף מקורסים אלו , ובעיקר מהפרקים הראשונים של כל קורס (ראה פרק 4).

מרבית הקורסים באוניברסיטאות לעיל מבוססים על הספר:

- **Quantum computation and quantum information** Author: M. Nielesen and I. Chuang Published by: Cambridge University Press

חוברת הקורס תכיל את הנושאים הבאים:

פרק 1: מבוא ומוטיבציה

הפרק כולל הסבר כללי על מחשב קוונטי ועומד על חשיבותו התיאורטית.

פרק 2: מושגי יסוד באלגברה

חזרה על מושגי יסוד מהאלגברה, סימון דירק (Dirac notation), מכפלה טנזורית ותכונותיה, . DFT.

פרק 3: פיזיקה קוונטית

הסבר כללי על מושגי ייסוד בפיזיקה קוונטית, תוך הדגמת ניסוי 2 החריצים.

פרק 4: המודל המתמטי

הצגה מפורטת של המודל המתמטי של הפיזיקה הקוונטית.

פרק 5: אופרטורים קוונטים

שערים לוגיים קוונטים והשוואה לשערים לוגיים קלאסיים.

פרק 6: ייצוג גרפי

ייצוג גרפי על כדור בלוך של קיוביט, ושל הפעלת שער לוגי.

פרק 7: אלגוריתמי תקשורת

עקרון אי השיבוט, טלפורטציה, שידור דחוס

פרק 8: אלגוריתמים מקבילים

הצגת האלגוריתם של דויטש, אלגוריתם החיפוש של גרובר והשלכותיו.

פרק 9: אלגוריתם פירוק לגורמים

תוך כדי הצגת אלגוריתם DFT, הערכת פאזה ומציאת סדר.

פרק 10: אלגוריתמי הצפנה קוונטית

קידוד והחלפת מפתחות.

פרק 11: בעיות המימוש של מחשב קוונטי

בעיית הde-coherence (השפעת הסביבה על החישוב) ודרך הפתרון- תיקון הטעות ע"י אלגוריתם.

פרק 12: מחלקת סיבוכיות

הצגת מחלקת BQP והיחס בינה לבין מחלקות "קלאסיות" אחרות (P,NP,PSPace,BPP)

4. השוואה לסילבוס של קורסים הניתנים באוניברסיטאות אחרות:

מרבית הקורסים עוסקים בנושא בהרחבה (ולא ברמת מבוא), ומניחים ידע מסוים בפיזיקה/ פיזיקה קוונטית. הקורס המוצע הינו ברמת מבוא ואינו מניח ידע תיאורטי בפיזיקה (אך מניח ידע במתמטיקה).

למול הקורס בטכניון:

הקורס בטכניון מכוון לבעלי ידע בפיזיקה קוונטית, ובעל "אופי" מתמטי בעיקרו. בקורס נסקרים מספר רב של אלגוריתמים ונושאי מימוש (חומרה).

	נושא	הסבר	פרק בחוברת
.1	מבוא: שערים לחישוב קלסי וחישוב הפיך. דוגמה לתורת הקוונטים		4 (עם דוגמאות שונות)
.2	תורת הקוונטים: פורמליזים	מוסבר בעיקר על הטנזור ותכונתיו	2, 3
.3	מבוא לתאורית האינפורמציה	עקרון שאנון	לא מכוסה
.4	תורת אינפורמציה קוונטית. עקרון אי שיבוט.		7
.5	מצבים סבוכים, טלפורטציה		7
.6	שער קוונטי, חישוב קוונטי		4
.7	אלגוריתמים	מוצגים מספר אלגוריתמים	8,9
.8	אלגוריתים לפיקטור	אלגוריתים של שור	9
.9	נושאים מתקדמים	לא מפורט	לא מכוסה
.10	קודים לתיקון שגיאות		11
.11	הצפנה		10
.12	הצפנה קוונטית; העברת מפתח; בטיחות		10
.13	מימוש הצפנה קוונטית		לא מכוסה
.14	מימוש שערים לחישוב קוונטי	בעיות במימוש	11

למול הקורס באוניברסיטת ירושלים:

	נושא	פרק בחוברת
.1	Models of Quantum Computation	4
.2	Quantum Algorithms	8,9
.3	Quantum lower bounds	10
.4	Quantum noise and Quantum Error Correcting Codes	11
.5	Fault tolerant Quantum Computation and threshold	11
.6	Quantum communication	7
.7	Quantum cryptography	10
.8	Quantum Complexity Theory	12

למול הקורס באוניברסיטת ת"א:

חלק נכבד מהקורס מכיל הביטי תקשורת של חישוב קוונטי.

	נושא	פרק בחוברת
.1	Basics and examples: introduction, axioms, quantum states and notation, unitaries, measurement	3 (עם דוגמאות שונות)
.2	Basics and examples: continued, tensor products, measurement in general basis, reminder of one-time pad, quantum key distribution (BB84), no cloning	1 (עם מוטיבציות שונות)
.3	Quantum circuits: classical reversible circuits, quantum circuits, universality	4
.4	Quantum algorithms: teleportation, complexity class BQP, oracles (or blackboxes),	8 ,7

	a simple quantum algorithm: Deutsch's algorithm, Deutsch-Josza algorithm, Simon's algorithm	
9 (חלקי)	Quantum algorithms: Simon's algorithm continued, hidden subgroup problem, garbage removal, Quantum Fourier transform	.5
9	Quantum algorithms: Quantum Fourier transform continued, basic number theory, reminder of RSA, reduction from factoring to period finding, Shor's algorithm for factoring (the easy case)	.6
8 (מכוסה חלקי)	Quantum algorithms and lower bounds: Shor's algorithm for factoring (the general case), continued fractions, discrete log, Grover's algorithm: 2D analysis, reflection around the mean analysis	.7
12	Quantum algorithms and lower bounds: lower bound with the hybrid argument, lower bound by polynomials	.8
10	Quantum communication: Definition of the models	.9
לא מכוסה	Quantum communication: Communication complexity: Definition of the models, EQUALITY (classical with	.10

	and without public coin), DISJOINTNESS with quantum communication ,multanous message passing and quantum ,lower bound for IP started	
לא מכוסה	Quantum communication: lower bound for IP cont., Bell inequality (upper and lower bound), nonlocal boxes and trivial communication complexity	.11
3 (חלקית)	Quantum communication: nonlocal boxes and trivial communication complexity cont., fault-tolerant computation (classical), classical noise-threshold from quantum considerations Quantum error correction: bit-flip code, general quantum errors, phase flip errors, Shor's code, fault-tolerant principles	.12
11 (חלקית) 4	Quantum error correction: classical error correction, Hamming code, Steane's code, no cloning bound for codes, quantum secret sharing "Quantum-classical" result: locally decodable codes - lower bound by quantum arguments	.13

ברקלי:

קורס מקיף המכיל מגוון נושאים (חלקם ע"י מרצה חוץ).

	נושא	פרק בחוברת
.1	Intro, Axioms, Bell Inequalities.	1 (עם דוגמאות שונות)
.2	Hilbert Space, Tensor product, Quantum gates, Bell states. Inequalities.	2
.3	Hilbert Space, Superdense Coding, Teleportation. Inequalities.	2,7
.4	Reversibility, Quantum Computers are Digital	5
.5	Quantum Complexity Theory	12
.6	Quantum Computation and Extended Church-Turing Thesis	12
.7	Simon's Agorithm + QFT	9 (מכוסה חלקי)
.8	Quantum Factoring	9
.9	Abelian HSP + Discrete Log	לא מכוסה
.10	Lower Bounds for Unstructured Search, Quantum Zeno Effect.	12
.11	Quadratic speedup for Unstructured Search - Grover's Algorithm.	8
.12	Phase Estimation	9
.13	Quantum Information	לא מכוסה
.14	Bipartite States, Schmidt Decomposition, Bit Commitment	12
.15	Quantum Lower Bounds - Guest Lecture by Robert Spalek	לא מפורט

.16	Search by Quantum Walk - Guest Lecture by Ashwin Nayak	לא מפורט
.17	Holevo's Theorem, Random Access Codes	לא מכוסה
.18	Applications of Random Access Codes.	לא מכוסה
.19	Adiabatic Quantum Computation	לא מכוסה
.20	QMA Completeness	לא מכוסה
.21	Quantum Error Correction	12
.22	Stabilizer Formalism	לא מכוסה
.23	Quantum Non-locality - guest lecture Jeremy Roland	לא מפורט
.24	Non-abelian HSP	לא מכוסה
.25	Fault tolerance I - guest lecture Ben Reichardt	11
.26	Fault tolerance II - guest lecture Ben Reichardt	11
.27	Universality of Adiabatic QC + Low entanglement	לא מכוסה

חלק שני:

חוברת הקורס- פרקים נבחרים.

מבוא לחישוב קוונטי

מנחה: ד״ר מיכאל לנגברג

כתב: אינג׳ עופר אוחיון

תוכן עניינים:

חלק ראשון- יסודות חישוב קוונטי.....18
פרק ראשון: מבוא.....19
1. מוטיבציה.....19
2. מטרת ומבנה המדריך.....20
פרק שני: מושגי יסוד באלגברה.....21
1. חזרה.....21
2. סימון דירק (Dirak Notation).....24
3. מכפלה טנזורית.....25
4. התמרת פורייה הבדידה -DFT.....26
פרק שלישי- פיזיקה קוונטית.....28
1. מבוא.....28
2. תכונות האטום והאלקטרון.....29
3. ניסוי שני החריצים.....30
פרק רביעי- המודל המתמטי.....37
1. קיוביט ופונקצית גל.....37
2. מדידה.....38
3. רגיסטר קוונטי.....42
4. מצב שזור (Entangled):.....46
5. בסיס בל.....48
פרק חמישי- אופרטורים קוונטים.....49
1. שערים לוגיים קלאסיים.....49
2. שער לוגי לקיוביט בודד.....53
3. שער אוניברסאלי לקיוביט בודד.....56
4. שערים לוגים לרגיסטר קיוביט.....57
5. השוואת שער קוונטי מול שער קלאסי.....65
פרק שישי- ייצוג גרפי.....67
1. ייצוג גראפי של קיוביט.....67
2. שער לוגי לקיוביט בודד- ייצוג גרפי.....70
חלק שני: אלגוריתמים.....75
פרק שביעי- אלגוריתמי תקשורת.....76
1. עקרון אי השיבוט –no cloning:.....76
2. שידור ערך קיוביט- טלפורטציה.....78
3. שידור ערכי ביטים.....80
פרק שמיני- אלגוריתמים מקביליים.....83

1. מבוא.....83
2. אופרטור U_f.....85
3. אלגוריתם של דויטש (Deutsch).....88
4. אופרטור Mean Inversion.....94
5. בעיית החיפוש- אלגוריתם של גרובר (Grover).....96
פרק תשיעי- האלגוריתם של שור.....107
1. אלגוריתם DFT.....107
2. אלגוריתם הערכת פאזה (Phase estimation).....114
3. מציאת סדר.....123
4. בעיית הפירוק לגורמים.....129
נספח א'- אלגוריתם שבר משולב.....132

חלק ראשון- יסודות חישוב קוונטי

פרק ראשון: מבוא

1. מוטיבציה

מודל החישוב הקוונטי הינו תחום חדש יחסית בעולם מדעי המחשב. על אף ששורשיו הינם דווקא מעולם הפיסיקה הקוואנטית, מודל זה הינו בעל חשיבות עצומה לעולם מדעי המחשב, שכן הוא מציג מודל חזק יותר ממכונת טיורינג- דהיינו ניתן לפתור בעזרתו בעיות (בצורה יעילה) אשר טרם התגלה להם פתרון יעיל במחשב קלאסי. לדוגמא:

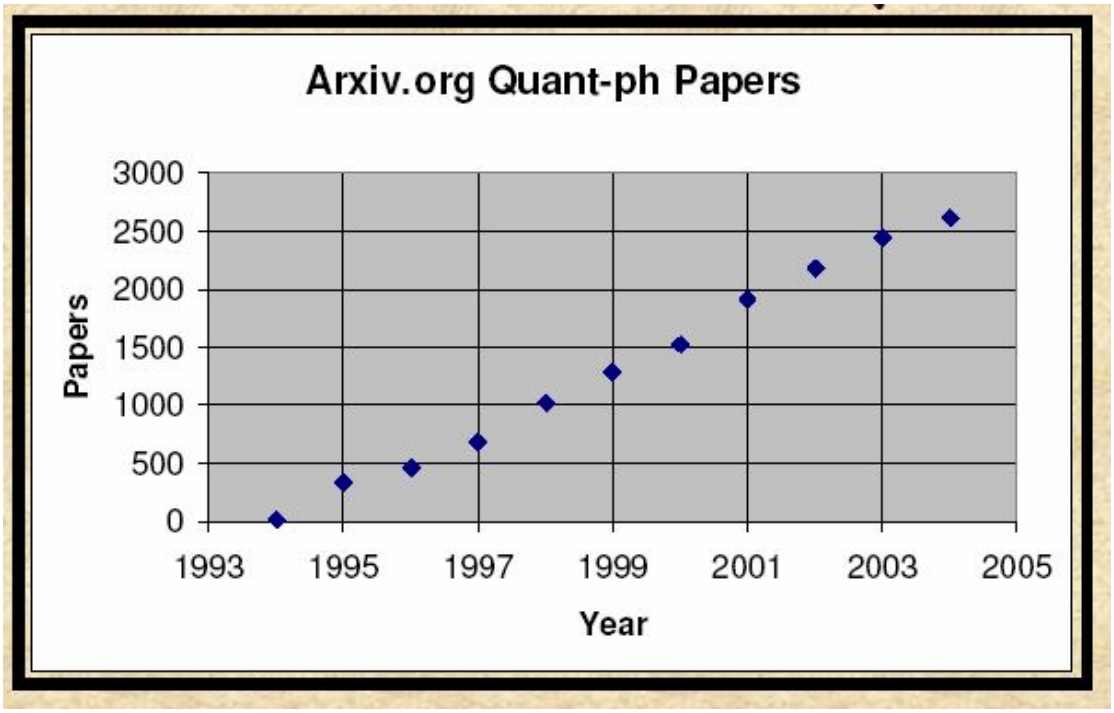
א. פירוק לגורמים - בבעיה זו הקלט הינו מספר אשר ידוע כי הוא מכפלת שני מספרים טבעיים (גדולים ממש מ 1). הבעיה- מציאת אותם 2 מספרים. לבעיה זו חשיבות עצומה- שכן פרוטוקולי הצפנה רבים (ביניהם RSA הנפוץ) מתבססים על כך שפירוק לגורמים איננו טריוויאלי ואורך זמן רב. לשם הדוגמה, האלגוריתם הטוב ביותר הידוע במחשב קלאסי לפירוק מספר הינו בסיבוכיות אקספוננציאלית באורך הקלט, כך שפירוק מספר בן 5000 ספרות ייקח כ5 טריליון שנה (מספר פעמים גיל היקום). לעומת זאת , ה"אלגוריתם של שור", שהינו אלגוריתם למחשב קוונטי, מבצע את המלאכה בסיבוכיות זמן פולינומיאלית- כך שפירוק מספר בן 5000 ספרות ייקח מספר בודד של דקות.

ב. אלגוריתם החיפוש של גרובר (Grover) – מתורת הסיבוכיות ידוע לנו כי כדי לחפש איבר ברשימה לא ממוינת באורך n , ע"י מכונת טיורינג, יש לבצע $O(n)$ צעדים, ולא ידוע על אלגוריתם דטרמיניסטי המסוגל לבצע זאת בפחות צעדים. לעומת זאת, גרובר הראה שעל גבי מחשב קוונטי ניתן להשלים את המשימה תוך $O(\sqrt{n})$ צעדים.

בנוסף על כך, למחשב קוונטי ישנה מעלה נוספת על פני מקבילו הקלאסי. בבואנו לממש אלגוריתם לא דטרמיניסטי (דבר שימושי מאוד עבור בעיות שלא נמצא להן פתרון בדרך אחרת), מנוע המספרים האקראיים במחשב קלאסי - איננו אקראי באמת (שכן בסופו של דבר מכונת טיורינג הינה דטרמיניסטית). דבר הפוגם באמינות המימוש. מחשב קוונטי לעומת זאת מבוסס מטבעו על תהליכים קוונטים שהינם אקראיים מטבעם - ועל כן "מכיל" מנוע שכזה באופן אינהרנטי. ומכאן שמימוש אלגוריתם לא דטרמיניסטי על מחשב קוונטי יהיה אמין יותר מאשר מימושו על מחשב קלאסי.

גם בסימולציה של תהליכים נראה כי ידו של המחשב הקוונטי על העליונה. פיינמן (Feynman) הראה כי מידול מערכת קוונטית במחשב קלאסי אינו מעשי (בשל הסיבוכיות הרבה) . לעומת זאת, למחשב קוונטי, (אשר מבוסס על מערכות קוונטית) סימולציית התהליכים הקוונטים הינה אינהרנטית.

על העניין הרב שהתחום מעורר ניתן להסיק גם מאיור 1 המתאר את כמות המאמרים בנושא כפונקציה של הזמן.



איור 1

יחד עם זאת, למרות יתרונות אלו ורבים אחרים, קיימת בעיה מהותית אחת עם מודל החישוב הקוונטי- מימושו כרגע הינו קשה למדיי. מעבדות שונות כבר הצליחו לייצר מחשבים קוונטים בעלי מספר בודד של ביטים קוונטים, אך בשל מגבלות טכניות עדיין לא נבנה מחשב קוונטי חזק מספיק לשימוש מעשי, או לייצור המוני.

זאת ועוד, הכרת העולם הקוונטי הינה בעלת חשיבות מעשית, שכן בהתחשב בחוק מור (MOOR) – הגורס כי כל 18 חודש צפיפות הטרנזיסטורים בשבב מוכפלת,יוצא כי בתוך מספר שנים גודל הטרנזיסטורים יקטן עד כדי כך שלא ניתן יהיה עוד להתעלם מההיבט הקוונטי ש"יצוץ" בבואנו להשתמש במחשבים "קלאסיים", ומכאן נובע כי אפקטים קוונטים בהכרח יופיעו בעתיד הנראה לעין.

2. מטרת ומבנה המדריך

מטרת מדריך למידה זה הינה להציג בפני הקורא כלים בסיסים להכרות עם נושא חשוב זה, דרך הצגת המודל המתמטי העומד בבסיס תורת הקוונטים, ולהראות את השימוש במודל זה למימוש אלגוריתמים יעילים. אין מטרת המדריך לשמש כמדריך ללימוד הבסיס הפיזיקאלי של תורת הקוונטים, וההסברים הפיזיקאליים מוצגים רק על מנת להציג תמונת עולם שלמה המקשרת בין המודל המתמטי למודל הפיזיקאלי.

פרק שני: מושגי יסוד באלגברה

1. חזרה

מספר מרוכב הינו מהצורה $a+bi$, **והצמוד** לו הינו $a-bi$.

סימון אוילר למספר שניתן לייצגו כ $\cos\alpha+i\sin\alpha$ הינו $e^{i\theta}$.

הסדרה $1,2,\ldots n$ הינה מקרה פרטי של **טור חשבוני**. ה**סכום** נתון על ידי:

$$\sum_{j=0}^{n} j=\frac{n(1+n)}{2}=\frac{n^2+n}{2}$$

הסדרה $1,q\ ,q^2,\ldots q^n$ הינה מקרה פרטי של **טור גיאומטרי**, כאשר q היא המנה. ה**סכום** נתון על ידי:

$$\sum_{j=0}^{n} q^j=\frac{1-q^n}{1-q}$$

המטריצה המשוחלפת של A, שמסומנת A^T (מבוטא A transposed) היא המטריצה שבה שורות ועמודות A מתחלפות.

מטריצה A תיקרא **הפיכה** או **רגולארית** אם קיימת מטריצה B כך ש $A\cdot B=B\cdot A=I$ ואז מסמנים $B=A^{-1}$ והמטריצה B תיקרא **המטריצה ההפוכה** או **ההפכית** של A. מטריצה לא הפיכה נקראת **מטריצה סינגולארית**.

מעל שדה המרוכבים **מטריצה צמודה** למטריצה A היא מטריצה שכל איבר בה הינו הצמוד של האיבר המתאים בA. הסימון הוא A^*.

צמוד **הרמיטי** של מטריצה A מעל שדה המרוכבים, היא מטריצה המוגדרת באופן הבא:

$U^\dagger\equiv U^{t^*}$. הסימון † נקרא dagger. (באופן דומה מוגדר עבור וקטור).

מכפלה פנימית מעל שדה המורכבים מוגדרת כ: $v\cdot w=v^\dagger w$

הנורמה של וקטור $x\in C^n$ מקיימת:

א. $|x| \geq 0$, ואם $|x| = 0$ אז $x = 0$.

ב. אם $\lambda \in C$ אז $|\lambda x| = |\lambda||x|$.

ג. אם $y \in C^n$ אז $|x| + |y| \geq |x + y|$.

נורמה אוקלידית נתונה על ידי $|x| = \sqrt{x \cdot x}$.

המרחב הווקטורי V **נפרש** ע"י קבוצת וקטורים $S \in V$, אם ורק אם כל וקטור $v \in V$ ניתן להצגה כצירוף לינארי של איברי S. עבור המרחב הווקטורי C^n קבוצת הווקטורים $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}, \ldots \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix} \in C^n$ פורשת את המרחב, ונקראת **הבסיס הסטנדרטי**. עבור C^2 גם הקבוצה $\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}, \begin{pmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{pmatrix} \in C^2$ פורשת אותו , ונקראת **בסיס הדרמרד**.

מעבר בסיס- בהינתן וקטור בבסיס A ניתן לייצגו בבסיס B, ע"י הכפלתו **במטריצת המעבר** מA לB. פעולה זו נקראת **הטלה**. לדוגמה: מטריצת המעבר מהבסיס הסטנדרטי לבסיס הדרמרד נתונה ע"י: $\begin{pmatrix}1/\sqrt{2} & 1/\sqrt{2}\\1/\sqrt{2} & -1/\sqrt{2}\end{pmatrix} \in C^2$. על כן הווקטור $\begin{pmatrix}1\\0\end{pmatrix}$ בבסיס הסטנדרטי מיוצג בבסיס הדרמרד

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} \text{ . ואכן, } \begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{pmatrix}.$$

ערך עצמי (ע"ע) ווקטור עצמי (ו"ע):

עבור מטריצה A , הפתרונות הלא טרוויאלים למשוואה: $Av_i = \lambda_i v_i \quad i = 0\ldots, n-1$ הינם הערך העצמי λ_i , והווקטור העצמי המתאים v_i.

סט הוקטורים v_i נקרא **אורתונורמלי** אם: לכל $i \neq j$ מתקיים $v_i \cdot v_j = 0$ וכן לכל i מתקיים $v_i \cdot v_i = 1$.

מטריצה U שמקיימת $U^\dagger = U^{-1}$ נקראת **מטריצה יוניטרית**. תכונות:

i. מטריצה הינה יוניטרית אמ"מ העמודות/שורות מגדירות בסיס אורתונורמאלי.

ii. המטריצה שומרת נורמה ומכפלה פנימית. ז"א: $(Uu)\cdot(Uv)=u\cdot v$.

iii. הערכים העצמיים (הע"ע) שלה הם בעלי נורמה 1, ועל כן ניתן לתארם כמהצורה $\lambda_i=e^{i2\pi\theta_i}$, והוקטורים העצמיים המתאימים v_i הם אורתונומלים.

פירוק טיילור:

פירוק טיילור הוא פירוק פונקציה נתונה בסביבת נקודה נתונה לפי הנגזרות של הפונקציה בנקודה זו. מספר פירוקים חשובים:

$$\cos(\theta)=1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}+\dots$$

$$\sin(\theta)=\theta-\frac{\theta^3}{3!}+i\frac{\theta^5}{5!}+\dots$$

$$e^{i\theta x}=1+i\theta x-\frac{(\theta x)^2}{2!}-i\frac{(\theta x)^3}{3!}+\frac{(\theta x)^4}{4!}+i\frac{(\theta x)^5}{5!}+\dots$$

פונקציה על מטריצה:

תהי A מטריצה, ותהי f פונקציה שניתן לכתיבה כ:

$$f(x)=\sum_{i=0}^{\infty}c_i x^n$$

אזי ניתן לתאר פונקציה על המטריצה כ:

$$f(A)=\sum_{i=0}^{\infty}c_i A^n$$

(כאשר $A^0=I$).

עבור המקרה הפרטי

$$f(x)=e^{i\theta x}=\sum_{i=0}^{\infty}\frac{(i\theta x)^n}{i!}=1+i\theta x-\frac{(\theta x)^2}{2!}-i\frac{(\theta x)^3}{3!}+\frac{(\theta x)^4}{4!}+i\frac{(\theta x)^5}{5!}+\dots$$

ועבור A המקיימת $A^2=I$, אזי:

$$f(A)=I+i\theta A-\frac{\theta^2 I}{2!}-i\frac{\theta^3 A}{3!}+\frac{\theta^4 I}{4!}+i\frac{\theta^5 A}{5!}+\dots=$$

$$\left(1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}+\dots\right)+i\left(\theta-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}+\dots\right)A=$$

$$\cos(\theta)I+i\sin(\theta)A$$

2. סימון דירק (Dirak Notation)

א. קט

סימון דירק מגדיר את הסימון- קט (ket) המייצג וקטור עמודה, ונרשם כ: $\left|\ \right\rangle$. לדוגמא, יהי:

$v_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$ אזי הווקטור יסומן כ- $\left|v_1\right\rangle$.

נוח לעשות שימוש בסימון זה להגדרת וקטורי הבסיס הסטנדרטי V_i של מרחב ווקטורי C^n, ע"י סימון דירק באופן הבא: $\left|i\right\rangle = V_i$. לדוגמה, ב C^2 וקטורי הבסיס הסטנדרטי מוגדרים כ:

$\left|0\right\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\left|1\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

בסיס הדמרד נפרש, כאמור ע"י $\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}, \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} \in C^2$. זהו מרחב שנשתמש בו בהרחבה

בהמשך, ולכן נסמן את וקטורי הבסיס שלו כ: $\left|+\right\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$, ו $\left|-\right\rangle = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$.

ב. ברה

הסימון ברה- מציין וקטור שורה, ומסומן ע"י $\left\langle\ \right|$ ומייצג את הווקטור הצמוד המשוחלף.

לדוגמא, יהי:

$v_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$ (או בצורה אחרת - $\left|v_1\right\rangle = a_1\left|0\right\rangle + b_1\left|1\right\rangle$), אזי $\left\langle v_1\right| = \begin{pmatrix} \overline{a}_1 & \overline{b}_1 \end{pmatrix}$.

בסימון דירק, המכפלה הפנימית בין 2 וקטורים v_1 , v_2 נתונה ע"י $\left\langle v_1 \middle| v_2\right\rangle$, שכן

אם $\left|v_1\right\rangle = a_1\left|0\right\rangle + b_1\left|1\right\rangle$, $\left|v_2\right\rangle = a_2\left|0\right\rangle + b_2\left|1\right\rangle$ אזי: $\left\langle v_1 \middle| v_2\right\rangle = \begin{pmatrix} \overline{a}_1 & \overline{b}_1 \end{pmatrix}\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$.

ועל כן, הטלה של וקטור v_1 על הווקטור i מהבסיס הסטנדרטי נתונה ע"י

$$\left\langle i \middle| v_1\right\rangle = \begin{pmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \end{pmatrix} = \alpha_i$$

מכפלה **חיצונית** מתוארת על ידי:

$$\left|v_1\right\rangle\left\langle v_2\right| = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}\begin{pmatrix} \overline{a}_1 & \overline{b}_1 \end{pmatrix} = \begin{pmatrix} a_1\overline{a}_1 & a_1\overline{b}_1 \\ b_1\overline{a}_1 & b_1\overline{b}_1 \end{pmatrix}$$

3. מכפלה טנזורית

א. מכפלה טנזורית של וקטורים

יהי $v \in C^k$ ו $w \in C^l$ וקטורי עמודה. המכפלה הטנזורית של וקטורים אלו היא העתקה:

$C^k \times C^l \to C^{kl}$ כך ש:

$$v \otimes w = \begin{pmatrix} v_1 w \\ v_2 w \\ v_3 w \\ \vdots \\ v_k w \end{pmatrix}$$, כאשר $v_j w$ מציין מכפלה סקלרית של האיבר הj של v בווקטור w.

המכפלה הטנזורית של וקטור העמודה $|i\rangle$ בווקטור העמודה $|j\rangle$ יסומן כ: $|i\rangle \otimes |j\rangle$ או בסימון מקוצר $|i\rangle|j\rangle$ או אפילו $|ij\rangle$. לדוגמה, $|0\rangle|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$,

$|0\rangle|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$ וכך הלאה...

במקרה הכללי, מכפלה טנזורית של n וקטורי עמודה תרשם כ $|v_1 v_2 \dots v_n\rangle$.

ב. מכפלה טנזורית של מטריצות

את ההגדרה למכפלה טנזורית, ניתן להרחיב כך שבמקום להגדירה על ווקטורי עמודה נגדיר על מטריצות ריבועיות $M \in C^k \times C^k$ ו $N \in C^l \times C^l$ ואז המכפלה הטנזורית של מטריצות אלו היא העתקה: $(C^k \times C^k) \times (C^l \times C^l) \to (C^{kl} \times C^{kl})$ כך ש:

$$M \otimes N = \begin{pmatrix} M_{11}N & M_{12}N & \dots & M_{1k}N \\ M_{21}N & M_{22}N & \dots & M_{2k}N \\ \vdots & \vdots & \vdots & \vdots \\ M_{k1}N & M_{k2}N & \dots & M_{kk}N \end{pmatrix}$$ כאשר $M_{ij}N$ מציין מכפלה סקלרית של האיבר הM_{ij} במטריצה N.

ג. תכונות:

a) $(M \otimes N)(v \otimes w) = (Mv) \otimes (Nw)$

b) $(\alpha M + \alpha' M') \otimes (\beta N + \beta' N') = \alpha\beta M \otimes N + \alpha\beta' M \otimes N' + \alpha'\beta' M' \otimes N + \alpha'\beta' M' \otimes N'$

c) $(M \otimes N)^* = M^* \otimes N^*$

d) $(M \otimes N)^T = M^T \otimes N^T$

e) $(M \otimes N)^\dagger = M^\dagger \otimes N^\dagger$

באם M וN הם יוניטריות, אזי גם $M \otimes N$.

ד. מכפלות טנזוריות:

מכפלה טנזורית בזה אחר זה של אותו איבר, כלומר $\underbrace{A \otimes A \otimes A \otimes A \ldots \otimes A}_{n}$ מסומנת $A^{\otimes n}$.

מכאן נובע כי:

$$\underbrace{|0 \ldots 00\rangle}_{n} \equiv |0\rangle^{\otimes n} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

תרגיל: הוכח טענה זו.

מכפלה טנזורית בזה אחר זה ,לא של אותו איבר , כלומר: $\underbrace{A_1 \otimes A_2 \otimes \ldots \otimes A_n}_{n}$ מסומנת $\bigotimes_{i=1}^{n}$.

4. התמרת פורייה הבדידה -DFT

א. הגדרה:

תהי f(x) פונקציה בדידה כלשהיא של משתנה אחד כאשר: $x = 0,1,2 \ldots N-1$, אזי ניתן להציג אותה כפונקציה של סינוסים וקוסינוסים לפי:

$$F(u) = \frac{1}{N} \sum_{x=0}^{N-1} f(x) e^{i 2\pi u x / N} \quad u = 0,1,..N-1$$

לדוגמה, התמרת פורייה של הפונקציה f(x)=1 הינה:

$$F(u) = \frac{1}{N} \sum_{x=0}^{N-1} e^{i 2\pi u x / N} \quad u = 0,1,..N-1$$

ב. התמרת פורייה ההפוכה:

תהי F(u) התמרת פורייה של פונקציה f(x). אזי מתקיים:

$$f(x) = \frac{1}{\sqrt{N}} \sum_{u=0}^{N-1} F(u) e^{-i2\pi ux/N} \qquad x = 0,1,..N-1$$

ג. הערות:

ניתן להתייחס להתמרת פורייה כמעבר בסיס- מהבסיס הסטנדרטי לבסיס המוגדר על ידי e^{ix} (של סינוסים וקוסינוסים) – במקרה זה הנוסחא הנתונה למעבר הבסיס מלמדת מה הוא המקדם (אמפליטודה) בכל אחד מווקטורי הבסיס ("תדרים"). ומה הם התדרים המשמעותיים יותר בפונקציה- לכך יש חשיבות רבה במדעי המחשב: אלגוריתמי דחיסת מידע (תמונה, קול) רבים מתבססים על איבוד המידע בעל העוצמות הנמוכות (אמפליטודת שתורמות מעט), ואלגוריתמי זיהוי רבים מתבססים על דמיון העוצמות הגבוהות בין 2 פונקציות. חשיבות ההתמרה איננה רק עבור פונקציות בדידות אלא גם עבור פונקציות רציפות (שאז הן נדגמות מספיק פעמים לקבלת פונקציה דיסקרטית קרובה מספיק לפונקציה הנדגמת).

האלגוריתם הקלאסי היעיל ביותר הידוע לנו עבור פירוק פורייה הינו בסיבוכיות של O(Nlog N).

כלומר באם יש להמיר וקטור בן 2^n איברים, אזי הסיבוכיות הינה $O(2^n)$. בהמשך נראה אלגוריתם קוונטי לחישוב ההתמרה. אלגוריתם זה יבוא לידי שימוש באלגוריתמים אחרים, שגם אותם נציג.

פרק שלישי- פיזיקה קוונטית.

מטרת פרק זה הינה לתאר בצורה פשוטה נושאים שונים מעולם הפיזיקה. אין מטרת הפרק לרדת לעומקם של דברים, אלא רק לספק טעימה לגבי הפיזיקה שמאחורי המודל המתמטי.

1. מבוא

עולם הפיזיקה כיום מכיל 2 תיאוריות שונות הסותרות אחת את השנייה, ומחלקות (בצורה גסה) את העולם לשני סוגים:

1) עולם החלקים הגדולים (כוכבים, אנשים, וכל החלקים שאנו מכירים מחיי היום יום)- המודל הקלאסי:
המודל מוצג ע״י תורת היחסות וניבויי המודל מדויקים למדיי. זהו מודל דטרמיניסטי, הנחשב כהרחבה למודל שהניח ניוטון, ואת יסודותיו הניח אינשטיין. אחד הממצאים העומדים בבסיסה הוא כי מהירות האור סופית , ולא ניתן לעבור אותה (דבר שאושש ע״י ניסויים רבים).
ע״י מודל זה ניתן להסביר כמעט את כל התופעות שאנו עדים להם בחיי היום יום, ועל כן ניבויי המודל הינם אינטואיטיביים ו״הגיוניים״.

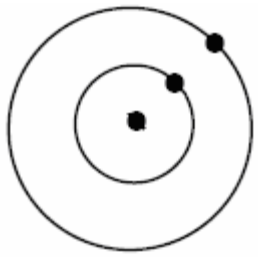
2) עולם החלקיקים האטומיים- המודל הקוונטי:
בבואנו לבדוק כיצד מתנהגים חלקיקים קטנים מאוד, מתברר כי נהיה עדים <u>לתופעות מוזרות מאוד המנוגדות לאינטואיציה הטבעית שלנו</u> כפי שאנו מכירים וחווים את העולם בחיי היום יום. למרות זאת- פיזיקאים בתחילת המאה הקודמת הצליחו לבנות מודל – המודל הקוונטי- המצליח לתאר ולנבא תופעות בעולם מוזר זה. התיאוריה הקוונטית, נראית מבטיחה מאוד- טרם נעשה ניסויי המפריך אותה, ולמעשה ככל שמתאפשר לבצע יותר ויותר ניסויים היא מצליחה לנבא את תוצאותיהם ולספק הסבר בדיוקים מדהימים (עד 14 ספרות אחרי הנקודה!). התיאוריה הקוונטית מניחה בבסיסה כי העולם איננו דטרמיניסטי ומנבאת הסתברויות להתרחשות תופעות.

לו ננסה להשתמש בתיאורית היחסות להסבר של העולם האטומי נקבל ניבויים הסותרים את התוצאות המתקבלות בניסויים, ולהפך- לו ננסה להשתמש בתיאוריה הקוונטית לניבוי תוצאות ניסוי בעולם החלקים -ניכשל.

מאמץ גדול נעשה ע״י פיזיקאים רבים למצוא תיאוריה מאוחדת גדולה אשר תכיל את שני התיאורית הללו, אך לעת עתה ללא הצלחה.

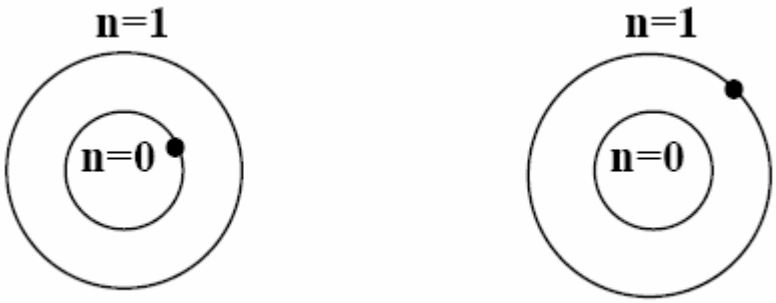
2. תכונות האטום והאלקטרון

ע״פ תיאורית הקוונטים, האטום מורכב מ2 חלקים- גרעין, ואלקטרונים החגים סביבו, במעין מסלול מעגלי. כמתואר באיור 1.



איור 1

האלקטרונים חגים ברדיוסים מסוימים בלבד ויכולים לעבור ממסלול למסלול (באם מספקים או לוקחים מהם אנרגיה). לדוגמה, אטום המימן הינו הפשוט ביותר ומכיל אלקטרון אחד, יכול להיות במצב מנוחה- דהיינו האלקטרון נמצא במסלול הקרוב ביותר או במצב ״מעורר״ ואז האלקטרון נמצא מסלול אחד רחוק יותר- כמתואר באיור 2.



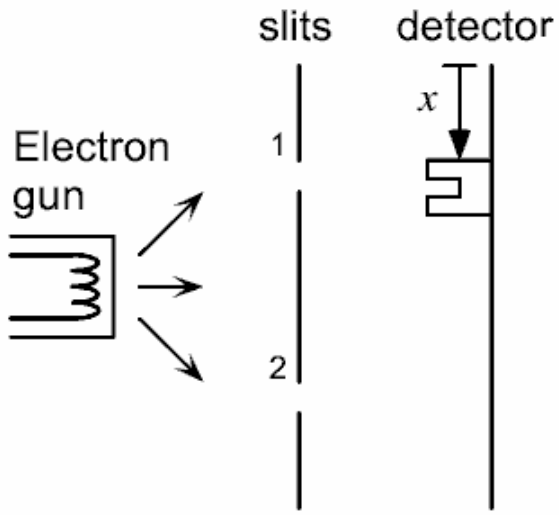
איור 2

בעת הקרנת אור בתדר מסוים לפרק זמן מסוים על אטום, ניתן ל״עורר״ אותו. מאידך, המסלול ההפוך גם הוא אפשרי- אטום ״מעורר״ יכול לפלוט אור, ולעבור למצב ״מנוחה״. מכאן אנו למדים כי לאטום יש תכונה בינארית. למעשה, יש לאטום אף יותר מתכונה בינארית אחת, ולמעשה גם לאלקטרון יש תכונות בינאריות - כמו ״ספין״ (משמעות המושג ״ספין״ תוצג בהמשך) . לצורך המשך הדיון נתייחס לאלקטרונים ולאטומים כאל חלקיקים, אשר יש להם תכונות בינאריות, וכשנדבר על מצב החלקיק נרצה לדעת מה מצב התכונה הבינארית שנמדדת.

לשם הצגת אפקטים בעולם החלקיקים יוצגו שני ניסויים : ניסוי שני החריצים וניסוי שטרן-גרלאך.

3. ניסוי שני החריצים

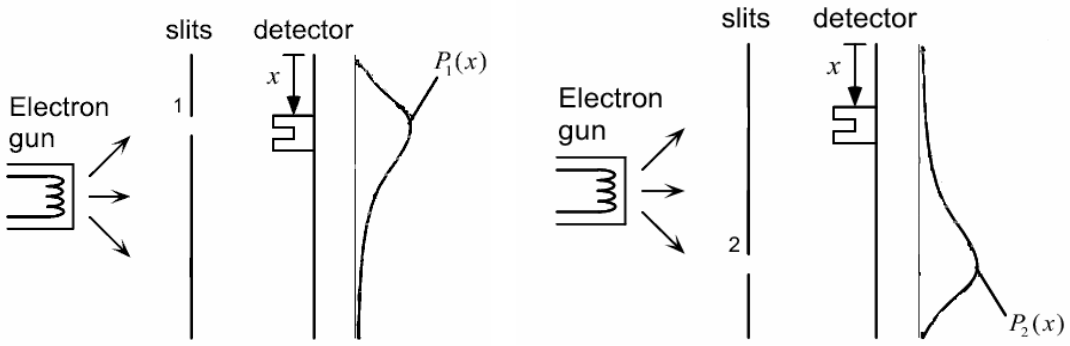
הניסוי מתואר באיור 3.



איור 3

בניסויי זה, חלקיקים נפלטים מתותח חלקיקים (משמאל) ועוברים דרך מחיצה בעלת שני חריצים בדרכם למסך מימין. על המסך ישנו גלאי המונה את מספר האלקטרונים המגיעים אליו, כך שניתן להסיק מהו מספר החלקיקים כפונקציה של המיקום על המסך. מן התותח נורת אלומת חלקיקים בעלי תכונות זהות.

בתחילת הניסוי מכסים חריץ אחד , ויורים אלומת חלקיקים. מתקבל כי חלקיקים פוגעים במסך לא תמיד באותה נקודה -ההסתברות למציאת חלקיק כפונקציה של מיקומו מתוארת ע"י $P_1(x)$ ו $P_2(x)$ בהתאמה, כמתואר באיור 4:

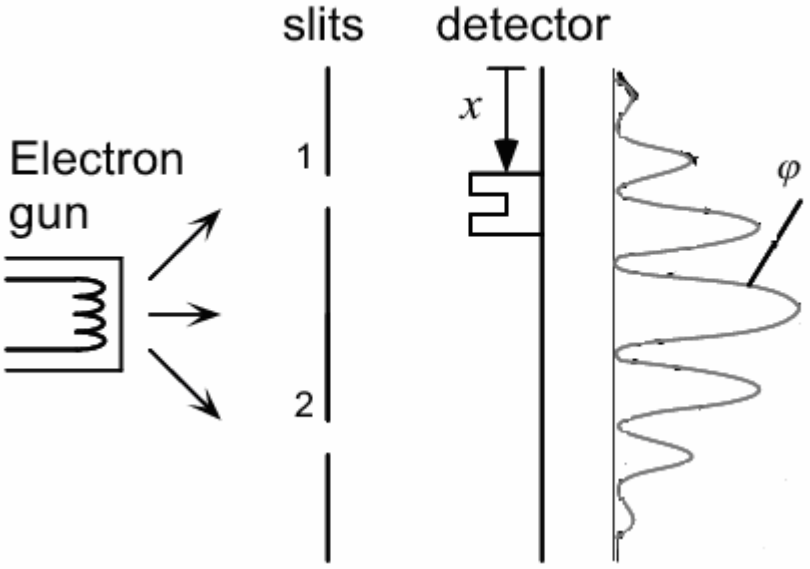


איור 4

מבחינת הפיזיקה הקלאסית- התוצאה מפתיעה- אם החלקיקים זהים, ופועל עליהם כוח זהה, היינו מצפים כי כל החלקיקים יפגעו תמיד באותה נקודה. כיצד הפיזיקה הקלאסית פותרת בעיה

זו? ניתן ליישב תופעה זו בהסבר שייתכן ובפועל החלקיקים שנפלטים מהתותח לא בדיוק זהים, ולא מופעל עליהם בדיוק אותו כוח, ועל כן כל פעם פוגעים בנקודה אחרת.

כאשר שני החריצים פתוחים, ניתן היה לצפות (וכך מנבאת הפיזיקה הקלאסית) כי ההסתברות למציאת חלקיק הינה סכום ההסתברויות (מנורמל) : $P_{12}(x)=\frac{1}{2}(P_1(x)+P_2(x))$, אך באופן מפתיע מתקבלת תמונת המוכרת לפיסיקאים כתמונת "התאבכות" של גלים- $\varphi(x)$, ומתוארת באיור 5.



איור 5

מכאן, אנו למדים כי הפיזיקה הקלאסית (ה"מודל האינטואיטיבי") איננה נכונה, שכן הניבוי חורג לגמרי מהתוצאה- אנו רואים מקומות בהם אין הסתברות בכלל- דהיינו מקומות בהם הסתברות אחת "ביטלה" את השנייה- דבר שאינו אפשרי ע"י המודל הקלאסי שכן הסתברות במודל הקלאסי הינה מספר חיובי.

ראינו אם כן 2 בעיות עימהם המודל הקלאסי ניסה להתמודד ולא בהצלחה מרובה- בשל כך התפתח מודל אחר הקרוי "המודל הקוונטי" שמסביר תופעות אלו בצורה פשוטה, ברורה ואחידה. המודל מתאים רק לעולם של חלקיקים ולא לחלקים גדולים אותם אנו פוגשים בחיי היום יום- במילים אחרות, המודל (שיוצג להלן) איננו אינטואיטיבי וסותר את כל ההבנה שלנו על התנהגות פיזיקאלית.

נציג את דרך הניתוח של המערכת בעזרת המודל הקוונטי. אחת מהנחות הבסיס של המודל היא כי גם אם פועל על כל חלקיק בדיוק אותם כוחות, לכל מדידה שהיא המתבצעת על החלקיק יש הסתברות . לכן, לתופעה באיור 4 ההסבר הקוונטי הוא כי לכל אחד מהחלקיקים באלומת

החלקיקים שעברה דרך חריץ 1 יש הסתברות מובנית שונה לפגוע במסך במקום כלשהו, שכן פגיעה במסך הינה סוג של מדידה (יודעים איפה החלקיק).

המודל הקוונטי מגדיר בצורה שונה את פונקצית ההסתברות שהשתמשנו בהם קודם. במקום לייחס את פונקצית ההסתברות לחריץ, היא מחושבת ביחס לחלקיק. כדי לעשות זאת מגדירים מושג חדש – "**פונקצית הגל של החלקיק**" שלמרות שמה איננה קשורה לגלים (השם ניתן מסיבות היסטוריות), והינה מיוצגת על ידי וקטור אשר משויך לחלקיק (הסבר פורמאלי יותר למושג חשוב זה יופיע בהמשך) . פונקצית הגל מוגדרת מעל שדה המרוכבים, כך שההסתברות של החלקיק לפגוע במסך בנקודה x נתונה ע"י הנורמה של פונקצית הגל. כך, נוכל לומר כי באם לחלקיק יש פונקצית גל $\phi(x)$, אזי בזמן ההתנגשות במסך, ההסתברות למציאת חלקיק על המסך בנקודה x נתונה על ידי $P(x)=\left|\phi\ (x)\right|^2$. תיאור זה מתאר את התופעה שנידונה .

כעת נסביר את הבעיה השנייה (התופעה המתוארת באיור 5) של סכום ההסתברויות- מבחינת המודל הקוונטי, פונקצית הגל כשרק חריץ אחד פתוח הינה: $\phi_1(x)=a_1+ib_1$ כך שההסתברות של חלקיק מאלומה שעברה דרך חריץ 1 לפגוע במקום x נתונה על ידי $P_1(x)=\left|\phi_1(x)\right|^2$. באופן דומה, לכל אחד מהחלקיקים באלומת החלקיקים שעברה דרך חריץ 2 יש פונקצית גל $\phi_2(x)=a_2+ib_2$, כך שההסתברות של חלקיק מאלומה שעברה דרך חריץ 2 לפגוע במקום x נתונה על ידי $P_2(x)=\left|\phi_2(x)\right|^2$.

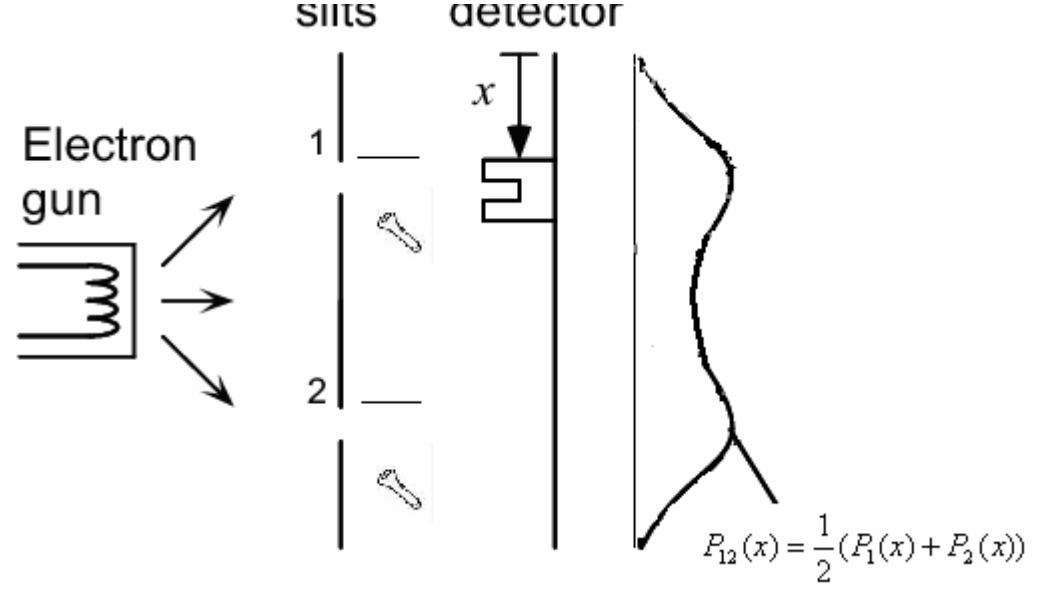
כאשר שני החריצים פתוחים יחדיו פונקצית הגל של המערכת כולה נתון על ידי:
$\phi_A(x)+\phi_B(x)$, כך שההסתברות למציאת חלקיק על המסך בנקודה x נתונה על ידי נורמת איחוד פונקצית הגל:

$$P_{12}(x)=\left|\phi_1(x)+\phi_2(x)\right|^2=\left|(a_1+ib_1)+(a_2+ib_2)\right|^2=$$
$$(a_1+a_2)^2+(b_1+b_2)^2=a_1^2+a_2^2+b_1^2+b_2^2+2a_1a_2+2b_1b_2=$$
$$\left|\phi_1(x)\right|^2+\left|\phi_2(x)\right|^2+2(a_1a_2+b_1b_2)=\left|\phi_1(x)\right|^2+\left|\phi_2(x)\right|^2+2\Re e[(a_1-ib_1)(a_2+ib_2)]=$$
$$=P_1(x)+P_2(x)+2\Re e(\phi_1^{\ *}(x)\phi_2(x))$$

זאת אומרת שיש כאן חיבור של ההסתברויות $P_1(x)+P_2(x)$ (כפי שניבא המודל הקלאסי), אך ישנו גם תיקון- $2\Re e(\phi_1^{\ *}(x)\phi_2(x))$ המוסיף עוד ערך לתוצאה הקלאסית- ותיקון זה מסביר את התוצאה שהתקבלה (תיקון זה גורם לכך שהפונקציה מתאפסת במקומות מסוימים).

ישנם עוד תופעות שאותם מתקשה הפיזיקה הקלאסית להסביר – לדוגמה כאשר במקום לירות אלומה של אלקטרונים, יורים בכל פעם אלקטרון בודד. מבחינת הפיזיקה קלאסית הינו מצפים

שוב לסכום פשוט של הסתברויות. לפי המודל הקוונטי היינו מצפים שפונקציית הגל של המערכת הייתה שונה- היינו מצפים שאם נורה חלקיק אחד, אז או שהוא יעבור דרך חריץ אחד או דרך השני- או במילים אחרות היינו מצפים שפונקציית הגל של המערכת היא או $\phi_A(x)$ או $\phi_B(x)$. אך גם כאן ישנו חידוש לא אינטואיטיבי: במודל הקוונטי קיים עקרון חשוב וייסודי- כל חלקיק, לפני שנמדד נמצא בכל המצבים האפשריים יחד ואילו לאחר שנמדד החלקיק בוחר לעצמו מצב אחד ומתקבע עליו. זאת אומרת, לפי המודל הקוונטי, כל חלקיק עובר בו זמנית גם דרך החריץ הראשון וגם דרך החריץ השני ורק כאשר מודדים על המסך הוא "מחליט" דרך איזה חריץ הוא עבר ולכן מקבלים תוצאה זהה למקרה בו נורו צמד חלקיקים. כלומר, כאשר נורה חלקיק בודד פונקצית הגל שלו היא $\phi_A(x)+\phi_B(x)$, ומכאן המודל הקוונטי מנבא כי אין שינוי בין תוצא הניסוי אם נורה חלקיק בודד או אלומת חלקיקים- ואכן למרבה הפלא התוצאה שמתקבלת בניסוי אכן מאוששת זאת (כמתואר באיור 5). עיקרון זה של המצאות בכל המצבים יחד נקרא עקרון הסופרפוזיציה. זהו עיקרון חשוב ומהותי, אף כי הוא מנוגד למציאות כפי שאנו חווים אותה ביום יום. תופעה זו היא בעלת חשיבות מכרעת במודל החישוב הקוונטי ועל כן חשוב להפנים אותה. למעשה, פונקצית הגל של החלקיק בנויה כך שהיא מביעה את הסופר פוזיציה, וכאשר מבצעים מדידה פונקצית הגל שלהם "מתקבעת", או כפי שהפיזיקאים קוראים לתופעה- פונקצית הגל קורסת. לזה קוראים הפיזיקאים "עקרון המדידה המשפיעה": כך לדוגמה, כאשר חוזרים על הניסוי כאשר שני החריצים פתוחים, ומבצעים מדידה באמצע הדרך, כמתואר באיור 6, כאשר הפנס מייצג מדידה שרק אומרת האם עבר שם חלקיק או לא– מתקבלת תוצאה שונה.



איור 6

כמובן שגם תופעה זו הינה בסתירה לפיזיקה הקלאסית. בפיזיקה הקלאסית המדידה לא משפיעה על התוצאה. ההסבר לפי המודל הקוונטי הינו כי מרגע שערבנו את המדידה, אזי מייד לאחר החריצים פונקצית הגל קרסה כך שהחלקיק "החליט" מיד לאחר החריץ אם הוא עבר דרכו או לא ואז פונקצית הגל שלו קורסת , כך שמיד לאחר החריץ פונקצית ההסתברות שלו נתקבעה ל $P_i(x)$, לכן לאחר החריצים נקבל כי ההסתברות הינה סיכום פשוט של ההסתברויות:

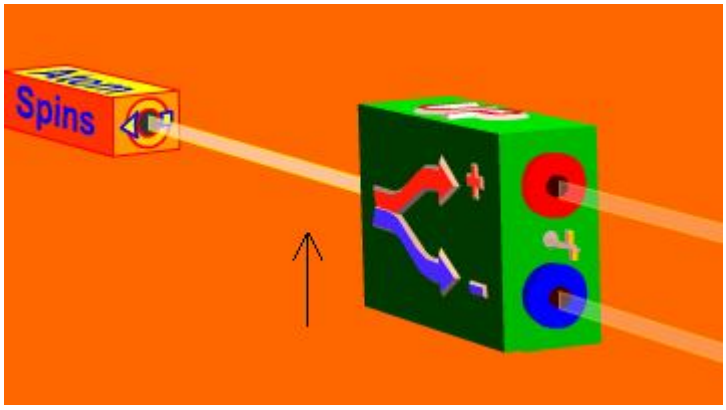
$$P_{12}(x) = |\phi_1(x)|^2 + |\phi_2(x)|^2 = P_1(x) + P_2(x)$$

(התיקון $2\Re e(\phi_1^*(x)\phi_2(x))$ שהיה לנו במקרה הקודם- לא קיים יותר) . המודל של הפיזיקה הקלאסית (וגם האינטואיציה הטבעית) מתקשה להסביר מדוע ברגע שמדדנו התוצאה השתנתה, ורק המודל הקוונטי מצליח להסביר זאת.

ב. ניסוי שטרן גרלאך

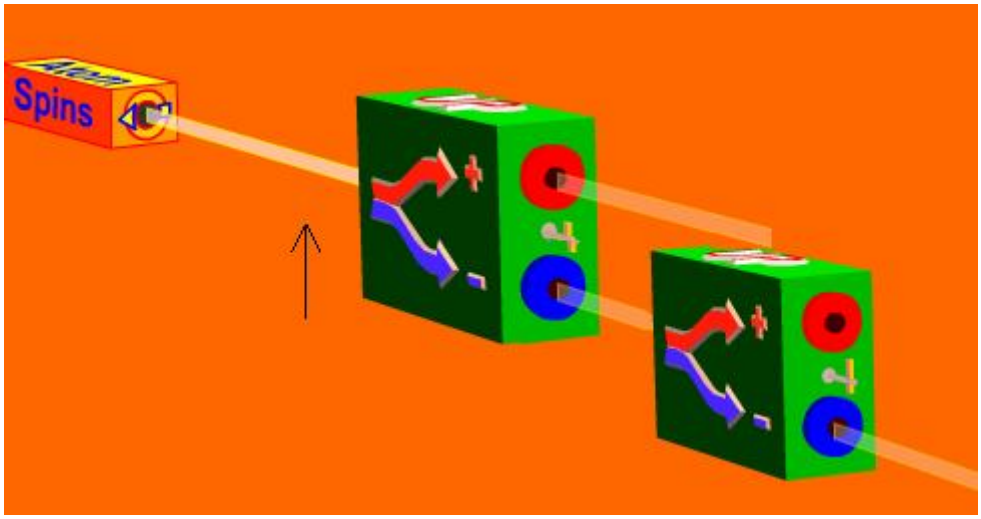
לאלקטרון ולאטום ישנם תכונות רבות שניתן למדוד, והן מוכרות לנו מחיי היום יום (לדוגמה משקל , מהירות זוויתית וכו'). אך ישנם תכונות מדידות אחרות שקיימות רק בחלקיקים אטומיים, לדוגמה, תכונת קיטוב האור ותכונת הספין של האלקטרון . ספין הינה תכונה של אלקטרון ויש לה כיוון וערך. לדוגמה, ניתן לומר שלאלקטרון יש ספין ½ בכיוון פלוס X או ספין ½ בכיוון מינוס X. כדי לגלות מה סימן הספין בכיוון X של אלקטרון, מעבירים אותו דרך שדה מגנטי המכוון בכיוון X. אם האלקטרון יורד מטה, אזי הוא בעל ספין X שלילי, ואם הוא עולה מעלה אזי הוא בעל ספין X חיובי.

באיור 7 מתוארת מערכת שכזו, כאשר הקופסא השמאלית ביותר הינה מקור היורה אלקטרונים, והקופסה עם שני החריצים היא שדה מגנטי, שכיוונו ככיוון החץ שלצורך העניין הוא הכיוון X.



איור 7

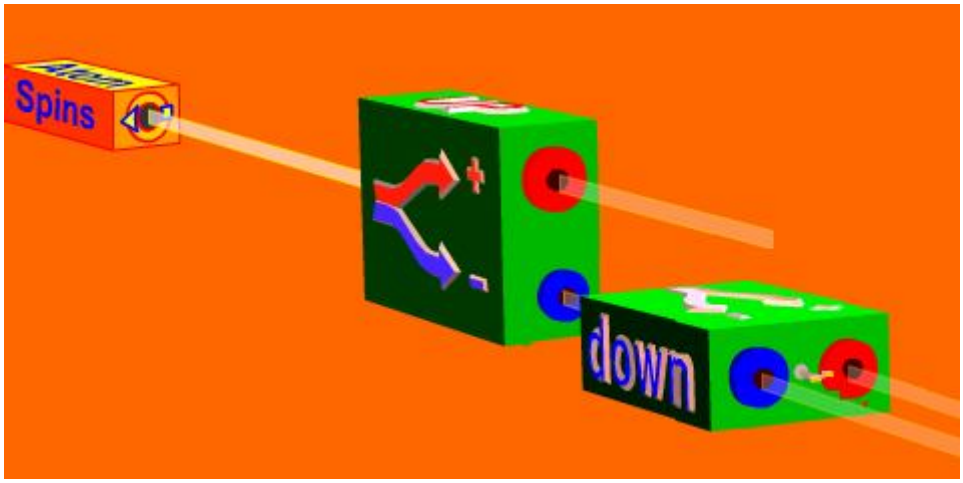
כפי שרואים, השדה מפצל את הקרן לשתי אלומות חלק עם ספין X חיובי וחלק עם ספין X שלילי. כאשר נמדוד אלקטרון נגלה שיש לו או ספין בכיוון X שלילי, או ספין X בכיוון חיובי . על כן במודל הקוונטי שהוצג מקודם, פונקצית הגל של האלקטרון תתאר אותו כנמצא בסופר פוזיציה של שני המצבים גם יחד- אך מעבר דרך השדה המגנטי (דהינו מדידה) תגרום לקריסת פונקצית הגל, והאלקטרון יהיה או עם ספין X+ או עם ספין X- (באיזה שהיא הסתברות). כך שאם נוסיף עוד שדה מגנטי בכיוון X כמתואר באיור 8:



איור 8

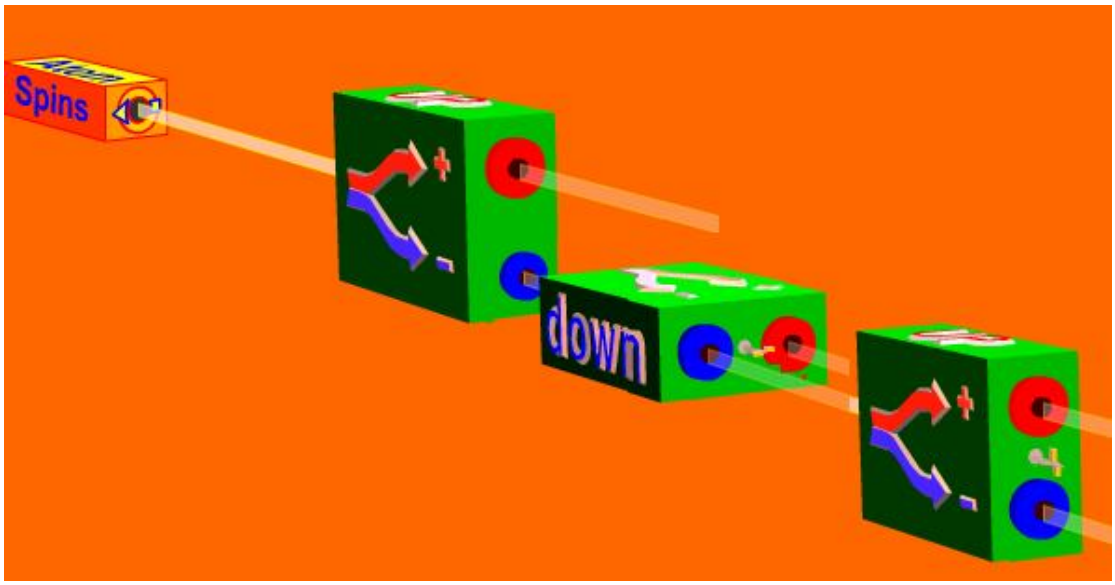
דרך השדה השני ייצאו רק אלקטרונים עם ספין X–, שכן המדידה הראשונה כבר קבעה לאלקטרונים את מצבם.

ניתן למדוד לאלקטרונים עם ספין X שלילי את ספין הY שלהם, ע״י העברתם דרך שדה מגנטי שבכיוון Y, כמתואר באיור 9.



איור 9

כעת נקבל מהגלאי השני שתי אלומות – במודל קלאסי היינו אומרים כי מהמוצא השמאלי של המכשיר השני , יש לנו אלקטרונים בעלי ספין X שלילי וספין Y שלילי, ואילו מהמוצא הימני יש לנו אלקטרונים בעלי ספין X שלילי וספין Y חיובי. אך לא כך הוא הדבר. המודל של הפיזיקה הקוונטית קובע כי כל מדידה משנה את מצב האלקטרון- כך שלאחר המכשיר השני מהמוצא השמאלי יש ספין Y שלילי, אך ספין הX איננו שלילי, אלא השתנה כך שאם נוסיף גלאי שלישי כמתואר באיור 10 :



איור 10

נגלה שיש לנו גם ספין X שלילי וגם ספין X חיובי. הסבר מתמטי לניסוי מובא בפרק הבא.

לסיכומו של דבר להלן עקרונות בסיסים בפיזיקה הקוונטית:

i. **פונקצית גל**

פונקציה מרוכבת המשמשת לחישוב הסתברות לתוצאת מדידה.

ii. **סופרפוזיציה**

פונקצית הגל של כל חלקיק מתארת אותו כמי שנמצא בכל המצבים האפשריים גם יחד.

iii. **מדידה**

כאשר מבצעים מדידה לחלקיק אזי פונקצית הגל שלו קורסת, וההסתברות לבחירת מצב מסוים מבין כל האפשריים הינה פונקצית הגל בריבוע.

ההסבר למודל הפיזיקלי המובא בפרק זה איננו מדויק, שכן אין מטרת הקורס ללמד פיזיקה קוונטית. הפרק מובא רק בכדי לקשור כלים מתמטים שיוצגו בהמשך לעולם הפיסקאלי. בפרק הבא יוצג מודל מתמטי מפורט, אשר ישמש אותנו לאורך כל הקורס כולו.

פרק רביעי- המודל המתמטי

בפרק זה נערוך היכרות עם המודל המתמטי של פיזיקת הקוונטים, דבר אשר ישמש אותנו בהמשך לצורך מידול האלגוריתמים והבנה מה ניתן לעשות בעזרת מחשב קוונטי. הפרק קושר בין המודל לבין הפיזיקה, אך רק לשם השלמת התמונה- ניתן להבין את האלגוריתמים ולפתחם גם מבלי להתייחס למימוש הפיזיקאלי שלהם.

1. קיוביט ופונקצית גל

בפרק הקודם הוצגו הרעיונות של הפיזיקה הקוונטית- ועולה השאלה- האם ניתן להיעזר ברעיונות אלו על מנת לבנות מודל חישובי , שאולי אפילו יהיה "חזק" יותר ממודל טיורינג. בכדי לענות על כך, נשים לב כי במחשב קלאסי (מימוש של מכונת טיורינג) התקן הזיכרון בנוי מביטים אשר הינם 0 או 1 (במימוש כמחשב קלאסי ביטים מיוצגים על ידי קיום זרם/מתח חשמלי או אי קיומו. נהוג לסמן "0" כשאין זרם חשמלי ו"1" כשיש). מודל החישוב הקואנטי הינו מכונת טיורינג, אך עם שינוי- התקן הזיכרון בנוי גם מחלקיקים אשר יכולים להיות בסופרפוזיציה של כל המצבים.
אנחנו נתעניין רק במצבים של תכונות אשר הן בינאריות - לדוגמה: האם החלקיק נמצא במצב מעורר או במצב מנוחה, והאם ספין הX שלו הוא חיובי, או שלילי.

במודל הקוונטי במקום לייצג את מצב הביט על ידי סקלר (0 או 1), נייצג את המצב על ידי וקטור. מכיוון שהתכונה הינה בינארית, מימד הוקטור יהיה 2. לדוגמה, בכדי לציין שחלקיק נמצא במצב מנוחה ניתן לסמן זאת ע"י $\begin{pmatrix}1\\0\end{pmatrix}$, ובמצב מעורר ע"י $\begin{pmatrix}0\\1\end{pmatrix}$. את מצב החלקיק נתאר ע"י פונקצית גל המתארת את הסופרפוזיציה של שני מצבים אלו. לדוגמה, פונקצית גל אפשרית לחלקיק הינה $\begin{pmatrix}\frac{1}{2}i\\ \frac{\sqrt{3}}{2}\end{pmatrix}$. והיא מתארת חלקיק ש נמצא גם במצב $\begin{pmatrix}1\\0\end{pmatrix}$ וגם במצב $\begin{pmatrix}0\\1\end{pmatrix}$, שכן

$$\begin{pmatrix}\frac{1}{2}\\ \frac{\sqrt{3}}{2}\end{pmatrix}=\frac{i}{2}\begin{pmatrix}1\\0\end{pmatrix}+\frac{\sqrt{3}}{2}\begin{pmatrix}0\\1\end{pmatrix}$$

. משמעות איברי פונקצית הגל באות לידי ביטוי במדידת החלקיק - ההסתברות שהחלקיק במצב $\begin{pmatrix}1\\0\end{pmatrix}$ הינה $\left|\left(\frac{i}{2}\right)\right|^2=\frac{1}{4}$, וההסתברות שהחלקיק במצב $\begin{pmatrix}0\\1\end{pmatrix}$ הינה $\left|\left(\frac{\sqrt{3}}{2}\right)\right|^2=\frac{3}{4}$. באם, לצורך העניין נמדד כי החלקיק אכן במצב $\begin{pmatrix}0\\1\end{pmatrix}$, אזי לאחר המדידה, פונקצית הגל של החלקיק הינה כמובן $\begin{pmatrix}0\\1\end{pmatrix}$.

א. פונקצית גל- הגדרה:

עבור מערכת של חלקיקים, פונקצית גל ψ, הינה וקטור מנורמל מעל C^n , כאשר n הינו מספר המצבים האפשריים, המתאר את הסופרפוזיציה של כל המצבים , ומאפשרת לחשב את ההסתברות למדידת אחד מהמצבים האפשריים .

ב. פונקצית גל- ייצוג:

פונקצית הגל של החלקיק הינה פונקציה מרוכבת מעל $\{1,2\ldots,n\}$ כאשר $\{1,2\ldots,n\}$ מייצג את המצבים האפשריים של החלקיקים. באופן שקול ניתן לרשום את פונקצית הגל כווקטור עמודה מנורמל, ולשם הנוחות ניעזר בסימון דירק לרישומה. לדוגמה נוכל לרשום כי פונקצית הגל של חלקיק נתונה ע"י : $|\psi\rangle$.

<u>הערה</u>: את הרישום כי פונקצית הגל מנורמלת, ניתן לרישום כמכפלה הפנימית הבאה:

$\langle\psi|\psi\rangle = 1$.

ג. קיוביט- הגדרה:

קיוביט הינו חלקיק בעל פונקצית גל המתארת את התכונות הבינאריות שלו, ולכן פונקצית הגל של קיוביט הינה מעל C^2.

2. מדידה

תכונת הקיוביט מתוארת ע"י 2 וקטורים אורתונורמלים, $V_1 \in C^2$, V_2. מדידת קיוביט מאופיינת על ידי קבוצה סופית P של 2 מטריצות בגודל 2x2 כל אחת, המתארות את ההטלות של המערכת הנמדדת : $P = \{|V_1\rangle\langle V_1|, |V_2\rangle\langle V_2|\}$. (מתקיים $\sum_{m=1}^{2} P_m = I$).

לדוגמה, חלקיק במצב מנוחה מסומן ע"י $\begin{pmatrix}1\\0\end{pmatrix}$, ובמצב מעורר ע"י $\begin{pmatrix}0\\1\end{pmatrix}$. מכאן שמדידת התכונה מתוארת ע"י הקבוצה:

$$\{\mathrm{P}\} = \left\{\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix}\right\} = \left\{\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}\right\}$$

ואכן מתקיים:

$$\sum_{m=1}^{2} P_m = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$$

באם פונקצית הגל של הקיוביט הינה ψ לפני המדידה, אזי:

א. הסיכוי שהתוצאה הינה $|V_1\rangle$, נתונה על ידי: $\langle\psi|P_1|\psi\rangle=\langle\psi|V_1\rangle\langle\psi|V_1\rangle$. ואז

פונקצית הגל של הקיוביט הינה: $\psi'=\frac{P_1|\psi\rangle}{\langle\psi|P_1|\psi\rangle^{1/2}}=\frac{|V_1\rangle\langle V_1|\psi\rangle}{\sqrt{\langle\psi|V_1\rangle\langle\psi|V_1\rangle}}$

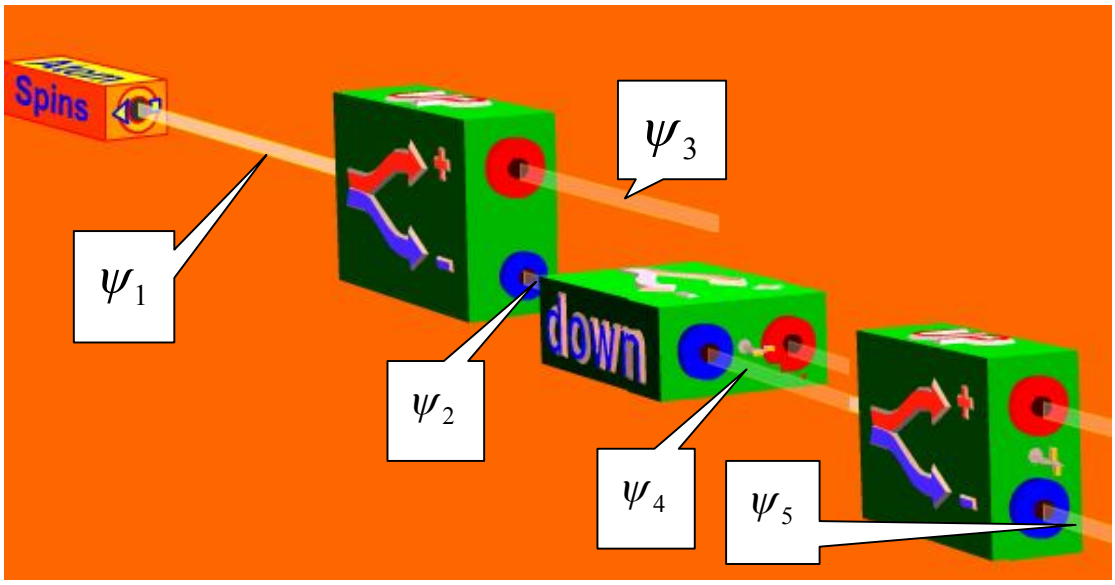
ב. הסיכוי שהתוצאה הינה $|V_2\rangle$, נתונה על ידי: $\langle\psi|P_2|\psi\rangle=\langle\psi|V_2\rangle\langle\psi|V_2\rangle$. ואז

פונקצית הגל של הקיוביט הינה: $\psi'=\frac{P_2|\psi\rangle}{\langle\psi|P_2|\psi\rangle^{1/2}}=\frac{|V_2\rangle\langle V_2|\psi\rangle}{\sqrt{\langle\psi|V_2\rangle\langle\psi|V_2\rangle}}$

לשם הסברת נושא זה, נסביר את ניסוי שטרן-גרלאך באמצעות המודל המתמטי:

באם נסמן ב $|0\rangle$ מצב שבו ספין X הוא חיובי, ו $|1\rangle$ לספין X שלילי, וכן ספין Y חיובי ע"י $|+\rangle$, וספין Y שלילי ע"י $|-\rangle$, אזי כאשר מבצעים מדידה בכיוון X ההסתברות לקבלת ספין חיובי נתונה על ידי נורמת ההטלה בריבוע לעבר הבסיס הסטנדרטי (שנפרש על ידי $|0\rangle$ ו $|1\rangle$). אולם כאשר מבצעים מדידה בכיוון Y אזי ההסתברות לקבלת ספין חיובי נתונה על ידי נורמת ההטלה בריבוע לעבר בבסיס הדמרד (שנפרש על ידי $|+\rangle$ ו $|-\rangle$).

המצב המתואר באיור 11, מוסבר במודל הקוונטי באופן הבא:



איור 11

בתחילה מצב כל קיוביט באלומה הינו $\psi_1=\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. הסיכוי שבמדידה הראשונה יימדד ספין X חיובי (זאת אומרת $|0\rangle$) הינו:

$$\langle\psi_1|P_1|\psi_1\rangle=\left(\begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right)=\begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}\begin{pmatrix}\alpha\\ 0\end{pmatrix}=|\alpha|^2$$

והסיכוי שבמדידה הראשונה יימדד ספין X שלילי (זאת אומרת $|1\rangle$) הינו:

$$\langle\psi_1|P_2|\psi_1\rangle=\left(\begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right)=\begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}\begin{pmatrix}0\\ \beta\end{pmatrix}=|\beta|^2$$

פונקצית הגל ψ_2 הינה עבור חלקיקים שנמדד עבורם $|1\rangle$:

$$\psi_2=\frac{P_2|\psi_1\rangle}{\langle\psi_1|P_2|\psi_1\rangle^{1/2}}=\frac{\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}}{\sqrt{|\beta|^2}}=\frac{\begin{pmatrix}0\\ \beta\end{pmatrix}}{|\beta|}=\begin{pmatrix}0\\ 1\end{pmatrix}$$

המדידה השנייה מודדת ספין Y- כלומר האם הקיוביט במצב $|+\rangle$ או $|-\rangle$. על כן נחשב את הסט המתאים:

$$\left\{P_2^{'}\right\}=\left\{\frac{1}{2}\begin{pmatrix}1\\ 1\end{pmatrix}\begin{pmatrix}1 & 1\end{pmatrix},\frac{1}{2}\begin{pmatrix}1\\ -1\end{pmatrix}\begin{pmatrix}1 & -1\end{pmatrix}\right\}=\left\{\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix},\frac{1}{2}\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\right\}$$

ואכן מתקיים:

$$\sum_{m=1}^{2}P^{'}{}_m=\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

הסיכוי למדידת $|+\rangle$:

$$\langle\psi_2|P_1^{'}|\psi_2\rangle=\left(\begin{pmatrix}0 & 1\end{pmatrix}\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}\right)=\frac{1}{2}\begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix}=\frac{1}{2}$$

ומכאן שלאחר מגנט זה הסיכוי למצוא $|+\rangle$ הוא 0.5, (וזהה לסיכוי למצוא $|-\rangle$) ניבוי זה אף הוא הוכח בניסוי.

פונקצית הגל ψ_4 הינה עבור חלקיקים שנמדד עבורם $|+\rangle$:

$$\psi_4=\frac{P_1^{'}|\psi_2\rangle}{\langle\psi_2|P_2|\psi_2\rangle^{1/2}}=\frac{\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}}{\sqrt{\frac{1}{2}}}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}=|+\rangle$$

הסיכוי שבמדידה האחרונה יימדד ספין X שלילי (זאת אומרת $|1\rangle$) הינו:

$$\langle\psi_4|P_2|\psi_4\rangle=\left(\frac{1}{2}\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix}\right)=\frac{1}{2}\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\frac{1}{2}$$

ומכאן שלאחר מגנט זה הסיכוי למצוא $|1\rangle$ הוא 0.5, וזהה לסיכוי למצוא $|0\rangle$ (ניבוי זה אף הוא הוכח בניסוי).

פונקצית הגל ψ_5 הינה עבור חלקיקים שנמדד עבורם $|1\rangle$:

$$\psi_5 = \frac{P_2|\psi_4\rangle}{\langle\psi_4|P_2|\psi_4\rangle^{1/2}} = \frac{\frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix}}{\sqrt{\frac{1}{2}}} = \begin{pmatrix}0\\ 1\end{pmatrix}$$

<u>לסיכום</u>:

1) תכונת הקיוביט מתוארת ע"י 2 וקטורים אורתונורמלים,

$V_1 \in C^2$, V_2.

2) מדידת קיוביט מאופיינת על ידי קבוצה סופית P של כל ההטלות של המערכת הנמדדת : $P = \{|V_1\rangle\langle V_1|, |V_2\rangle\langle V_2|\}$.

(מתקיים $\sum_{m=1}^{2} P_m = I$)

3) באם פונקצית הגל של הקיוביט הינה ψ לפני המדידה, אזי:

ג. הסיכוי שהתוצאה הינה $|V_1\rangle$, נתונה על ידי:

$\langle\psi|P_1|\psi\rangle = \langle\psi|V_1\rangle\langle\psi|V_1\rangle$. ואז פונקצית הגל של

הקיוביט הינה: $\psi' = \frac{P_1|\psi\rangle}{\langle\psi|P_1|\psi\rangle^{1/2}} = \frac{|V_1\rangle\langle V_1|\psi\rangle}{\sqrt{\langle\psi|V_1\rangle\langle\psi|V_1\rangle}}$

ד. הסיכוי שהתוצאה הינה $|V_2\rangle$, נתונה על ידי:

$\langle\psi|P_2|\psi\rangle = \langle\psi|V_2\rangle\langle\psi|V_2\rangle$. ואז פונקצית הגל של

הקיוביט הינה: $\psi' = \frac{P_2|\psi\rangle}{\langle\psi|P_2|\psi\rangle^{1/2}} = \frac{|V_2\rangle\langle V_2|\psi\rangle}{\sqrt{\langle\psi|V_2\rangle\langle\psi|V_2\rangle}}$

ד. כמות המידע

מהסתכלות על הייצוג של קיוביט ע"י פונקצית הגל, ניתן להסיק בטעות כאילו לקיוביט בודד יש אינפורמציה של 2 איברים מרוכבים- זאת אומרת , ניתן לחשוב (בטעות) כי בקיוביט בודד ניתן לאגור הרבה מאוד מידע- בטח ביחס לביט בודד שהוא 0 או 1.

אך לא כך הוא הדבר- שכן זהו ייצוג מתמטי לקיוביט, ואף על פי שהוא מתואר בצורה כזו, באופן מעשי, כאשר נבקש למדוד את ערך הקיוביט (דהינו לגלות מה האינפורמציה האצורה בתוכו) פונקצית הגל תקרוס כך שהחלקיק יהיה במצב אחד בלבד, ומדידה חוזרת ונשנית תניב את אותה התוצאה בדיוק -כך שלא נוכל לקבל יותר מידע מאשר מביט קלאסי. על כן למרות שהייצוג הוא ע"י מספרים מרוכבים, המידע שניתן לקבל מקיוביט בודד הוא בינארי.

3. רגיסטר קוונטי

א. הגדרה:

רגיסטר קוונטי הינו קבוצה של קיוביטים . ניתן לתאר רגיסטר קוונטי ע"י אוסף פונקציות גל (אחת לכל קיוביט, או בצורה כללית אחת לכל תת קבוצה של קיוביטים) או ע"י פונקצית גל אחת.

ב. מרחב פונקצית הגל של רגיסטר קיוביטים:

באם לכל קיוביט ייתכנו 2 מצבים אפשריים, אזי עבור n קיוביטים ייתכנו 2^n מצבים אפשריים .

לדוגמה, נניח ונשתמש בסימון הקודם למצב מנוחה ע"י $\begin{pmatrix}1\\0\end{pmatrix}$, ומצב מעורר ע"י $\begin{pmatrix}0\\1\end{pmatrix}$. אזי במערכת ובה 2 קיוביטים, ניתן לתאר את מצב 2 החלקיקים ע"י 2 פונקצית גל (אחת לכל קיוביט) שהן ב C^2 , או ע"י פונקצית גל אחת ב C^4 - שכן ישנם 4 אפשריות : שני הקיוביטים במצב מנוחה, אחת במצב מנוחה השני מעורר וכולי. נסמן מצבים אלו כ $\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$ ומשוואת הגל המתארת את המערכת הינה מעל מרחב זה:

$$|\psi\rangle=\begin{pmatrix}\alpha_0\\\alpha_1\\\alpha_2\\\alpha_3\end{pmatrix}$$

כך ש $\sum|\alpha_i|^2=1$.

מה הקשר בין המרחב של פונקצית הגל של קיוביט בודד לבין המרחב של פונקצית הגל של שני קיוביטים? פונקצית הגל של קיוביט בודד הינה מעל המרחב הנפרש ע"י $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$ ופונקצית הגל של 2 קיוביטים הינה מעל מרחב הנפרש ע"י $\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$, וניתן לתאר זאת כקומבינציה ליניארית של $|1\rangle\otimes|0\rangle,|1\rangle\otimes|1\rangle,|0\rangle\otimes|1\rangle,|0\rangle\otimes|0\rangle$ או בכתיב שקול $|00\rangle,|01\rangle,|10\rangle,|11\rangle$ או אף לעיתים נסמן $|0\rangle,|1\rangle,|2\rangle,|3\rangle$.

באופן כללי, בהינתן 2 רגיסטרים של קיוביט, אחד בעל n_1 קיוביטים ושני בעל n_2, או במילים אחרות- אחד בעל פונקצית גל מעל מרחב הנפרש ע"י $i=0\ldots2^{n_1}$ $\left|v_i\right\rangle$ ושני בעל פונקצית גל מעל מרחב הנפרש ע"י $j=0\ldots2^{n_2}$ $\left|u_j\right\rangle$, אזי פונקצית הגל של שניהם יחד הינה מעל מרחב הנפרש ע"י $i=0\ldots2^{n_1}, j=0\ldots2^{n_2}$ $\left|v_i\right\rangle\otimes\left|u_j\right\rangle$.

באם ברצונו לבצע סימולציה של מודל קוונטי בן 500 קיוביטים (חלקיקים) בלבד, על גבי מחשב קלאסי, נזדקק לייצוג של 2^{500} מקדמים מרוכבים- מספר גדול ממספר האטומים ביקום- משימה קשה למדיי עבור מחשב קלאסי. זו הסיבה מדוע כיום לא ניתן להיעזר במחשבים קלאסיים לסימולציות של מודלים קוונטים גדולים. לעומת זאת, לו יעלה בידנו לבנות מחשב קוונטי בעל 500 קיוביטים, הסימולציה תתנהל מעצמה (שכן כל קיוביט "ייצג" חלקיק במודל).
רק מעצם דוגמה זו עולה נקודה חשובה- השערת טיורינג צ'רץ טוענת כי כל מודל חישוב "סביר" ניתנת לסימולציה יעילה (ז"א בזמן פולינומיאלי) על גבי מכונת טיורינג. השערה זו נבחנה מול מודלים רבים ואומתה, אך מול המודל הקוונטי אנו נוכחים כי היא איננה נכונה (למעשה זהו המודל היחיד הידוע כיום שאיננו עומד בהשערה). זאת ועוד ,נראה בהמשך כי בעזרת מודל זה נוכל לפרוץ מגבלות נוספות המוכתבות ע"י מכונת טיורינג הקלאסית.

למרות חוזק זה של מודל החישוב הקוונטי– שהמימדים בו תופחים בצורה אקספוננציאלית, גם במודל זה ישנם חסמים תחתונים לבעיות מסוימות, כך שגם למודל זה ישנם מגבלות ובעיות שכנראה אין להם פתרון בזמן סביר.

ג. מדידה:

נכליל את הנאמר על קיוביט בודד בסעיף הקודם: התכונה הנמדדת על רגיסטר בעל N קיוביטים כשייתכנו m אפשריות מתוארת ע"י m וקטורים אורתונורמלים, $\{V_m\}\in C^{2^n}$ (כאשר $n\le N$ הינו מספר הקיוביטים עליהם מתבצעת המדידה). מדידת רגיסטר מאופיינת על ידי קבוצה סופית P בת m מטריצות, (כל מטריצה במימד $2^N x 2^N$) המתארות את כל ההטלות של המערכת הנמדדת:

$$P=\{P_1,\ldots,P_m\}=\left\{\left|V_i\right\rangle\left\langle V_i\right|\otimes I_{(2^N-2^n)x(2^N-2^n)} \quad \vee i\in m\right\}$$. (מתקיים $\sum_i P_i = I$).

לדוגמה, עבור רגיסטר בן 2 קיוביטים, פונקצית הגל הינה $\left|\psi\right\rangle=\begin{pmatrix}\alpha_0\\ \alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix}$ כאשר $\sum_i|\alpha_i|^2=1$.

מדידת התכונה שבה אחד מהם הינו $|0\rangle$ או $|1\rangle$ מערבת מדידה של קיוביט אחד בלבד, ללא הפרעה לקיוביט השני. במקרה כזה $V_1=\begin{pmatrix}1\\0\end{pmatrix}$, $V_2=\begin{pmatrix}0\\1\end{pmatrix}$ מכאן שמדידת התכונה מתוארת ע"י הקבוצה:

$$P=\left\{\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}=\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$$

$$=\left\{\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\right\}$$

ואכן מתקיים:

$$\sum_{m=1}^{2}P_m=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}+\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}=I$$

באם פונקצית הגל של הקיוביט הינה ψ לפני המדידה, אזי הסיכוי שהתוצאה הינה $|V_m\rangle$, נתונה על ידי: $\langle\psi|P_m|\psi\rangle$. ואז פונקצית הגל של הקיוביט הינה: $\psi'=\dfrac{P_m|\psi\rangle}{\langle\psi|P_m|\psi\rangle^{1/2}}$.

לדוגמה, ובהמשך לדוגמה הקודמת, ההסתברות כי נקבל שהקיוביט הנמדד הינו $|0\rangle$ היא:

$$\langle\psi|P_1|\psi\rangle=\begin{pmatrix}\overline{\alpha}_0&\overline{\alpha}_1&\overline{\alpha}_2&\overline{\alpha}_3\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\begin{pmatrix}\alpha_0\\\alpha_1\\\alpha_2\\\alpha_3\end{pmatrix}$$

$$=\begin{pmatrix}\overline{\alpha}_0&\overline{\alpha}_1&\overline{\alpha}_2&\overline{\alpha}_3\end{pmatrix}\begin{pmatrix}\alpha_0\\\alpha_1\\0\\0\end{pmatrix}=|\alpha_0|^2+|\alpha_1|^2$$

באם אכן יימדד $|0\rangle$ פונקצית הגל לאחר המדידה הינה:

$$\psi' = \frac{P_1|\psi\rangle}{\langle\psi|P_1|\psi\rangle^{1/2}} = \frac{\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\begin{pmatrix}\alpha_0\\\alpha_1\\\alpha_2\\\alpha_3\end{pmatrix}}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}} = \frac{\begin{pmatrix}\alpha_0\\\alpha_1\\0\\0\end{pmatrix}}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}}$$

$$= \frac{1}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}}\left(\alpha_0|00\rangle + \alpha_1|01\rangle\right)$$

נשים לב כי פונקצית הגל אכן מנורמלת, וכי כעת הסיכוי לכך שהקיוביט שלא נמדד הינו $|1\rangle$ הוא:

$$\langle\psi|P_1|\psi\rangle = \frac{1}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}}\begin{pmatrix}\overline{\alpha}_0 & \overline{\alpha}_1 & 0 & 0\end{pmatrix}\begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\frac{1}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}}\begin{pmatrix}\alpha_0\\\alpha_1\\0\\0\end{pmatrix}$$

$$= \frac{1}{|\alpha_0|^2+|\alpha_1|^2}\begin{pmatrix}0 & \overline{\alpha}_1 & 0 & 0\end{pmatrix}\begin{pmatrix}0\\\alpha_1\\0\\0\end{pmatrix} = \frac{|\alpha_1|^2}{|\alpha_0|^2+|\alpha_1|^2}$$

בהשוואה ל $|\alpha_2|^2+|\alpha_3|^2$ לפני המדידה- ז״א המדידה על קיוביט אחד השפיעה על מצבו של הקיוביט השני.

חשוב לציין ולהבין את הנקודה הבאה- למרות שנדון לאורך כל המדריך בפונקציות גל המתארות סופר פוזיציה של מצבים, לעולם לא נוכל למדוד את פונקצית הגל עצמה ולהסיק מהמדידה את ערכי המקדמים שלה. תמיד, כשנמדוד נמדוד ערך המושפע מקריסת פונקצית הגל וזהו הערך היחיד שיימדד גם במדידות חוזרות ונשנות. רבים מהאלגוריתמים שנראה בהמשך יגרמו לפונקצית הגל לקרוס לערך רצוי בסבירות גבוהה מאוד, ורק אז לבצע את המדידה.

ד. זהות עד כדי פאזה

מכיוון שבסופו של דבר אנו מבצעים מדידה של התכונה (ולא של פונקצית הגל) , והמדידה מושפעת מהנורמה של פונקצית הגל, ניתן להעלות את הטענה הבאה:

<u>טענה</u>: ההסתברות למדידת תוצאה p_m עבור רגיסטר קיוביטים בעל פונקצית הגל: $|\psi\rangle$ ועבור רגיסטר קיוביטים בעל פונקצית הגל $e^{i\theta}|\psi\rangle$ כאשר θ ממשי , הינה זהה. לזהות כזו קוראים זהות עד כדי פאזה גלובאלית.

תרגיל: הוכח את הטענה.

פתרון:

$$p_m = \left\langle e^{i\theta}\psi \middle| P_m \middle| e^{i\theta}\psi \right\rangle = e^{-i\theta}e^{i\theta}\langle\psi|P_m|\psi\rangle = \langle\psi|P_m|\psi\rangle$$

מכאן אנו למדים על תכונה של פונקצית גל כי ניתן להכפיל את המקדמים ב $e^{i\theta}$ מבלי לפגוע בנורמה של פונקצית הגל. לדוגמה, לפונקצית הגל $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$ ולפונקצית הגל $|\psi\rangle = -a_0|0\rangle - a_1|1\rangle$ יש אותה נורמה ריבועית (כי הכפלנו ב $e^{i\pi} = -1$).

4. מצב שזור (Entangled):

נתבונן בפונקצית הגל הבאה, המתארת מערכת של שני קיוביטים:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle$$

ניתן לפרש אותו כמצב:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle + |1\rangle)$$

סופר פוזיציה של שני קיוביטים – אחד במצב $|0\rangle$ ושני במצב $(|0\rangle + |1\rangle)$. לעומת זאת פונקצית הגל:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

לא ניתנת לתיאור כמכפלה טנזורית. למעשה לא כל מצב של מערכת קוונטית ניתן לרשום כמכפלה טנזורית – או במילים אחרות לא כל וקטור n מימדי ניתן להצגה כמכפלה טנזורית של וקטורים אחרים.

תרגיל: הוכח.

פתרון:

יהי $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \begin{pmatrix}\gamma\\ \delta\end{pmatrix}$ 2 וקטורים. נסמן את תוצאת המכפלה הטנזורית שלהם כלהלן:

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \otimes \begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \begin{pmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{pmatrix} = \begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\end{pmatrix}$$ ונשים לב, כי מתקיים- $\alpha_1\alpha_4 = \alpha\beta\gamma\delta$ וכן $\alpha_2\alpha_3 = \alpha\beta\gamma\delta$.

דהיינו כל מכפלה טנזורית מקיימת- $\alpha_1\alpha_4 = \alpha_2\alpha_3$. המצב $|\psi\rangle = \beta_0|00\rangle + \beta_1|11\rangle = \begin{pmatrix} \beta_0 \\ 0 \\ 0 \\ \beta_1 \end{pmatrix}$ לא מקיים $\alpha_1\alpha_4 = \alpha_2\alpha_3$, על כן לא ניתן לייצגו כמכפלה טנזורית.

מצבים אשר לא ניתן לרושמם כמכפלה טנזורית נקראים "מצבים שזורים" והם מצביעים על מצב מיוחד שהמערכת נמצאת בו.

תרגיל: עבור פונקצית הגל $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$:

א) הראה כי פונקצית הגל מתארת מצב שזור.

ב) הראה כי ההסתברות שאחד הקיוביטים הינו במצב $|0\rangle$ זהה להסתברות שהוא במצב $|1\rangle$ ושווה ל0.5.

פונקצית הגל $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$ המתארת שני קיוביטים במצב שזור היא בעלת תכונה מעניינת- אם נדע ערך של קיוביט אחד (לדוגמה השמאלי)- ע"י מדידה, מייד נדע את ערכו של השני (גם מבלי למדוד אותו)- שכן אם נדע שהקיוביט האחד ערכו $|0\rangle$ אזי השני בהכרח הוא גם $|0\rangle$.

זוהי עוד תופעה מדהימה שחוזה תורת הקוונטים והניסויים מאוששים אותה- ניתן לקחת שני קיוביטים להביאם למצב שזור ולהרחיקם מאוד אחד מהשני. אחר כך ניתן לבצע מניפולציה על אחד (לדוגמה למדוד לו את ספין הx שלו), ובהרף עין להשפיע על פונקצית הגל של הקיוביט השני –ומעשה להביא לקריסתה - שכן ברגע שבו נמדוד את אחד מהם פונקצית הגל שלו תקרוס וגם הקיוביט השני יקרוס לערך הנובע ממצב השזירות שלו. תופעה מדהימה זו (שהוכחה בניסוים) מצביעה כאילו יש תקשורת במהירות אינסופית בין שני הקיוביטים- כאילו הקיוביט שנמדד מוסר "הודעה" לקיוביט השני לאיזה ערך הוא קרס וגורם לקריסת פונקצית הגל של בן זוגו. בהמשך נרחיב על תופעה זו והשלכותיה.

<u>הערה</u>: בהסתכלות ראשונה נראה כאילו ניתן להיעזר בצורה קלה בתופעת המצב השזור לתקשורת במהירות אין סופית- פשוט לוקחים שני קיוביטים במצב שזור, ומודדים אחד מהם. אך, במחשבה שנייה מתברר כי אין הדבר כך- שכן בבואנו לתקשר מידע בין שני אתרים אנו מעוניינים להעביר מסר מסוים ומכיוון שאין אנו יודעים לאיזה ערך יקרוס הקיוביט שנמדוד לא נוכל לנצל תופעה זו בצורה טריוויאלית כל כך. עם זאת, ישנם אלגוריתמים העושים שימוש בתופעת המצב השזור, ונלמד עליהם בהמשך, ומכאן חשיבותם לתחום החישוב הקוונטי.

5. בסיס בל

בסיס בל פורש את המרחב הווקטורי C^4 ומוגדר ע"י הוקטורים הבאים:

1) $|\psi_-\rangle = \frac{|00\rangle - |10\rangle}{\sqrt{2}}$

2) $|\psi_+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$

3) $|\phi_-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

4) $|\phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

ייחודו של בסיס זה הינו שכל אחד מוקטורי הבסיס מתאר מצב שזור בבסיס הסטנדרטי. זאת ועוד, כל אחד מהוקטורים הללו מתאר מצב שזור גם בבסיס $|+\rangle, |-\rangle$. לדוגמה, ממשוואת מעבר הבסיס:

$$\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$

נובע כי

$$\begin{cases} |0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \\ |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \end{cases}$$

נציב זאת ב1:

$$|\psi_-\rangle = \frac{|00\rangle - |10\rangle}{\sqrt{2}} = \frac{(|+\rangle + |-\rangle)(|+\rangle - |-\rangle) - (|+\rangle - |-\rangle)(|+\rangle + |-\rangle)}{2\sqrt{2}} = \frac{|-+\rangle - |+-\rangle}{\sqrt{2}}$$

(וכנ"ל לגבי שאר וקטורי הבסיס).

פרק חמישי- אופרטורים קוונטים

עבור הביט הקלאסי מוגדרים שערים (אופרטורים) לוגיים המהווים את אבני הבניין לבניית מחשב קלאסי. באופן דומה, גם עבור קיוביט מוגדרים אופרטורים, הפועלים על קיוביט/רגיסטר ומשנים את מצבו. בפרק זה נדון תחילה בשערים לוגיים קלאסיים ותכונותיהם וכן יוצג שער שימושי מעניין הקרוי שער Toffoli. אחר כך נציג שערים לוגים עבור קיוביט בודד ונעמוד על תכונותיהם. לבסוף יוצגו שערים לוגים עבור רגיסטר של קיוביטים. בעת הצגת השערים הקוונטים נעמוד גם על ההבדלים בינם לבין מקבליהם הקלאסיים.

אחד ההבדלים המהותיים בין פונקציה בוליאנית קלאסית לבין פונקציה בוליאנית במודל הקוונטי , כפי שנראה בפרק זה, נעוץ בכך שעל כל פונקציה במודל הקוונטי להיות הפיכה. נראה בפרק זה כי ניתן לבנות עבור כל פונקציה בוליאנית קלאסית פונקציה בוליאנית קלאסית הפיכה (ע"י שימוש בשערים קלאסים הפיכים), כך שבבואנו להשוות בין מימוש פונקציה בוליאנית בעולם הקוונטי לבין המימוש בעולם הקלאסי נשווה למימוש הקלאסי ההפיך.

1. שערים לוגיים קלאסיים

א. חזרה

במחשב הקלאסי , כל הפעולות מבוצעות על ביטים המייצגים 0 או 1. על ביט בודד ניתן להפעיל פונקציה לוגית NOT (אשר הופכת את ערכו),ו"שער לוגי" FANOUT אשר משכפל את ערכו למספר ביטים.

לשני ביטים מוגדרים מספר פונקציות בסיסיות- AND, NAND, OR, NOR וXOR אשר טבלאות האמת שלהם מפורטות בטבלה 1.

A	B	AND $(A \cdot \mathrm{B})$	OR $(A + \mathrm{B})$	XOR $(A \oplus \mathrm{B})$	NOR $\overline{(A + \mathrm{B})}$	NAND $\overline{(A \cdot \mathrm{B})}$
0	0	0	0	0	1	1
0	1	0	1	1	0	1
1	0	0	1	1	0	1
1	1	1	1	0	0	0

טבלה 1

ניתן להראות כי כל פונקציה בוליאנית ניתנת להצגה ע"י FANOUT ושערים לוגים של AND, NOT וOR וכל אחד מהשערים AND, NOT וOR ניתן לבנות בעזרת שערי NOR או NAND, ועל כן ניתן לבטא כל פונקציה בוליאנית ע"י שערי NAND (או NOR) ושערי FANOUT.

ב. שער Toffoli

יש שערים קלאסיים שהם הפיכים ויש שאינם הפיכים- ובמילים אחרות, לא בכל שער לוגי ניתן לדעת מהתוצאה מהי הכניסה. לדוגמא, שער OR איננו הפיך שכן התוצאה 0 יכולה להתקבל מ3 אפשריות שונות של הכניסה. לעומתו שער NOT הינו הפיך.

שער בעל חשיבות מיוחדת הינו שער Toffoli , שהינו שער הפיך שניתן בעזרתו לבנות כל פונקציה בוליאנית כפונקציה בוליאנית הפיכה.

שער Toffoli הקלאסי מוגדר כשער בעל 3 כניסות (להלן a,b,c) ו3 מוצאים (להלן a',b',c').

ומקיים:

$a'=a$

$b'=b$

$c'=c \oplus ab$

טבלת האמת שלו מתוארת בטבלה 2.

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

טבלה 2

השער ההפיך לשער זה הינו- שער Toffoli בעצמו, שכן:

$$\text{Toffoli}(\text{Toffoli}(\{a,b,c\})) = \text{Toffoli}(\{a,b, c\oplus ab\}) = \{a,b, (c\oplus ab) \oplus ab)\} =$$

$$\{a,b, c\oplus(ab \oplus ab)\} = \{a,b,c\oplus 0\} = \{a,b,c\}.$$

שער זה מתואר באיור 12.

איור 12

קל לממש שער NAND וFANOUT על ידו:

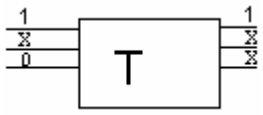
1) כדי לקבל שער FANOUT נציב בכניסות:

a=1, b=x, c=0

ואז המוצא יהיה:

a'=1, b'=x, c'= $0 \oplus x = x$

איור 13 מתאר זאת בצורה גרפית, וטבלת האמת נתונה בטבלה 3. וממנה ניתן לוודא את "הפיכות" שער FANOUT הנ"ל, שכן מידיעה כי המוצא הינו 100 נדע כי המבוא הינו 010 ומידיעה כי המוצא הינו111 נדע כי המבוא הינו 110.



איור 13

Input			Output		
b (=x)	a	c	a'	**b'**	**c'**
0	1	0	**1**	**0**	**0**
1	**1**	0	1	**1**	**1**

טבלה 3

2) כדי לקבל שער NAND נציב בכניסות:

a=x, b=y, c=1

ואז המוצא יהיה:

a'=x, b'=y, c'= $1 \oplus xy = \overline{xy}$

איור 14 מתאר זאת בצורה גרפית, וטבלת האמת נתונה בטבלה 4. וממנה ניתן לוודא את "הפיכות" שער NAND הנ"ל. שכן באם המוצא הוא 001 אז הכניסה הינה 001 וכו'. (מידיעת ערך המוצא ניתן לדעת את ערך הכניסה).

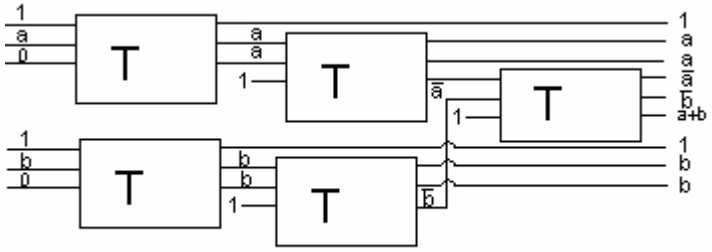
איור 14

input			Output		
a (=x)	**b (=y)**	c	a'	b'	**c'**
0	**0**	1	0	0	**1**
0	**1**	1	0	1	**1**
1	**0**	1	1	0	**1**
1	**1**	1	1	1	**0**

טבלה 4

מכיוון שכל פונקציה בוליאנית ניתנת למימוש ע"י שערי NAND וFANOUT, אזי ניתן לומר כי כל פונקציה בוליאנית ניתנת למימוש ע"י שערי Toffoli כלומר ניתן לממש עבור כל פונקציה בוליאנית שבכניסה שלה n ביטים ובמוצא ביט אחד, מעגל המורכב משערי Toffili אשר בכניסתו m*n ביטים (m – פונקציה של מספר שערי toffili) ומוצאה m*n ביטים, כך שאחד הביטים ערכו כערך הפונקציה הבוליאנית, ואילו הפונקציה כולה הינה הפיכה.

לדוגמה, שער OR ניתן לבנייה כפונקציה הפיכה, בדרך הבאה: $f = a + b = \overline{\overline{a} \bullet \overline{b}}$. איור 15 מתאר הרחבת הפונקציה לפונקציה הפיכה בעלת 9 כניסות (כאשר רובם קבוע 0 או 1) ובעלת 9 יציאות , כשהסיבית השישית הינה ערך OR המבוקש.



איור 15

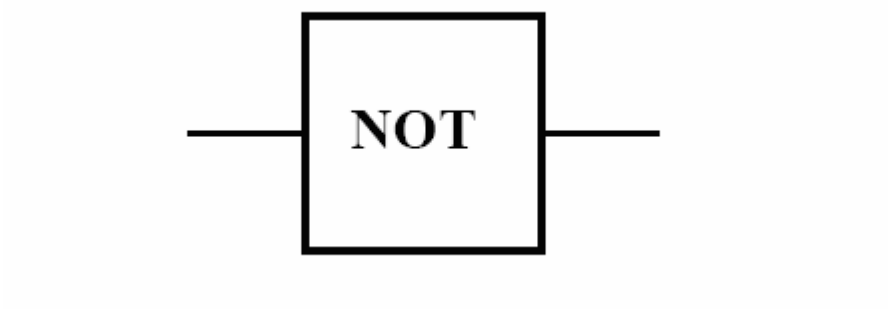
2. שער לוגי לקיוביט בודד

שער/אופרטור לוגי קוונטי מקבל בכניסתו קיוביט/ים (פונקצית גל) ומוצאו- קיוביט/ים המיוצג ע״י פונקצית גל אף הוא. על כן את השערים הלוגים הקוונטים נתאר ע״י מטריצה, והפעלה על פונקצית גל הינה הכפלה של וקטור (המתאר את פונקצית הגל) באופרטור. מכיוון שתוצא המכפלה מתאר אף הוא פונקצית גל, אזי בכדי לשמור על תכונות פונקצית גל, האופרטור חייב להיות מטריצה ריבועית יוניטרית. בנוסף, מכיוון שמטריצה יוניטרית הינה הפיכה יוצא כי כל שער לוגי קוונטי הינו הפיך.

1. שער NOT קוונטי

בהינתן קיוביט בעל פונקצית גל $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, נגדיר את שער NOT הקוונטי ככזה ההופך את ההסתברויות בפונקצית הגל ל: $|\psi'\rangle = \beta|0\rangle + \alpha|1\rangle$. דהיינו, ניתן להגדיר את השער כאופרטור X המיוצג ע״י המטריצה $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, כך ש $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$. מטריצה זו נקראת גם Pauli X gate.

שער זה מתואר באופן סכמאתי באיור 16.



איור 16

נשים לב כי גם לאחר השער מתקיים התנאי כי המשוואה המתארת את הקיוביט הינה מנורמלת שכן המטריצה X הינה יוניטרית.

2. שער Z

שער NOT הנ״ל הוגדר עבור הבסיס $|1\rangle, |0\rangle$, ועבור הבסיס $|+\rangle, |-\rangle$ אין פעולת השער NOT.

לבסיס $|+\rangle, |-\rangle$ שער הNOT הינו:

$$\text{Pauli Z gate: } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

שכן:

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}|+\rangle=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1/\sqrt{2}\\ 1/\sqrt{2}\end{pmatrix}=\begin{pmatrix}1/\sqrt{2}\\ -1/\sqrt{2}\end{pmatrix}=|-\rangle$$

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}|-\rangle=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1/\sqrt{2}\\ -1/\sqrt{2}\end{pmatrix}=\begin{pmatrix}1/\sqrt{2}\\ 1/\sqrt{2}\end{pmatrix}=|+\rangle$$

תרגיל: הוכח כי בבסיס הסטנדרטי פעולת השער ניתנת לתיאור על ידי המיפוי:

$$\alpha|0\rangle-\beta|1\rangle\xrightarrow{Z}\alpha|0\rangle+\beta|1\rangle$$

3. שערים קוונטים נוספים על קיוביט

בעוד שעבור ביט בודד אין עוד שערים מלבד NOT וFANOUT, עבור קיוביט ניתן להגדיר אוסף רחב מאוד של שערים לוגים- שכן האופרטור מוגדר ע"י מטריצה, שהמגבלה היחידה עליה שהיא חייבת להיות יוניטרית (ז"א משמרת את תכונת סכום הריבועים).

מספר שערים בעלי חשיבות מיוחדת:

א. הדמרד Hadamarad

המטריצה Walsh Hadamarad או בקיצור הדמרד, $H=\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix}$ אשר בין השאר

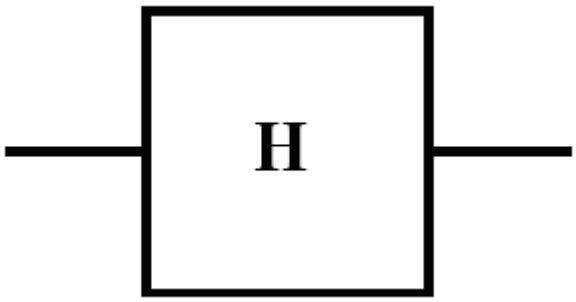
משמשת למעבר מהבסיס הסטנדרטי $|0\rangle$ $|1\rangle$ לבסיס $|+\rangle,|-\rangle$) - הינה גם "שער לוגי". הפעלתה

על קיוביט $|0\rangle$ תיתן:

$$H|0\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$

(ז"א שבעת המדידה נקבל 1 או 0 בסבירות זהה).

תיאור סכמאתי של אופרטור זה מתואר באיור 17.



איור 17

מכיוון שהאופרטור הינו מעל R וסימטרי, האופרטור ההופכי לאופרטור זה הינו הדמרד בעצמה.

תרגיל: הוכח.

לאופרטור זה חשיבות רבה והוא ישמש אותנו בהרחבה בקורס. תכונה חשובה של האופרטור היא כי היא למעשה ממירה אינפורמציה הקיימת באמפליטודה של הקיוביט ($|0\rangle$ או $|1\rangle$) ומעבירה אותו לפאזה- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ או $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ נוכל לתאר זאת ע"י:

$$|0\rangle \xleftrightarrow{H} |+\rangle = |0\rangle + |1\rangle$$
$$|1\rangle \xleftrightarrow{H} |-\rangle = |0\rangle - |1\rangle$$

או באופן שקול:

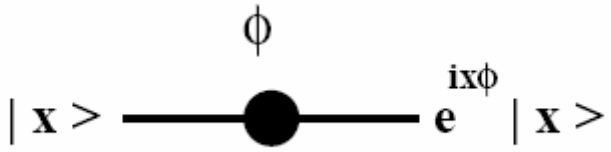
$$|b\rangle \xleftrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b |1\rangle)$$

ב. מטריצת פאזה

משפחת המטריצות הקרויה מטריצת פאזה, ממפה את $|0\rangle$ ל $|0\rangle$, ואת $|1\rangle$ ל $e^{i\phi}|1\rangle$, או באופן שקול המיפוי הינו: $x \xrightarrow{Phase} e^{ix\phi}|x\rangle$. האופרטור נתון על ידי המטריצה:

$$\text{Phase gate: } \Phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

תיאור סכמאתי של שער זה נתון באיור 18 . נשים לב כי שער Z הינו מקרה פרטי של שער פאזה כאשר $\phi = \frac{\pi}{2}$.



איור 18

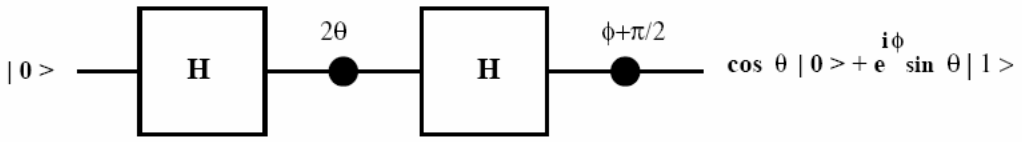
ג. מטריצת y

מטריצת Y מוגדרת:

$$\text{Pauli Y gate: } Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

3. שער אוניברסאלי לקיוביט בודד

כל פונקציה בוליאנית ניתנת להצגה ע"י שערי Toffili . האם קיים שער קוונטי שניתן להציג בעזרתו כל שער (לקיוביט בודד) שיעלה בדעתנו? מתברר כי התשובה לכך חיובית, ונתונה ע"י איור 19.



איור 19

בפרק הבא נראה כי כל פונקצית גל $|\psi\rangle$ ניתנת להצגה כ $|\psi\rangle = \cos\alpha|0\rangle + e^{i\phi}\sin\alpha|1\rangle$ כאשר $0 \le \theta \le \pi$, $0 \le \phi \le 2\pi$. ועל כן המסקנה המתבקשת הינה כי בעזרת מעגל זה ניתן לבנות כל אופרטור קוונטי שנחפוץ (לפי פונקצית הגל הרצויה נקבע את α,ϕ).

בסעיף זה נראה כי מוצא השער באיור 19 הינו $|\psi\rangle = \cos\alpha|0\rangle + e^{i\phi}\sin\alpha|1\rangle$ ומכאן נובע כי ניתן לבנות במקום כל שער שהוא מעגל המורכב משערי הדמרד ופאזה.

תרגיל: הראה כי עבור $|0\rangle$ מוצא השער באיור 19 הוא $|\psi\rangle = \cos\alpha|0\rangle + e^{i\phi}\sin\alpha|1\rangle$ (עד כדי פאזה).

פתרון:

לאחר השער הראשון, פונקצית הגל הינה:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

לאחר שער הפאזה הראשון, פונקצית הגל הינה:

$$\psi = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & e^{2\theta i}\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\e^{2\theta i}\end{pmatrix} = \frac{e^{\theta i}}{\sqrt{2}}\begin{pmatrix}e^{-\theta i}\\e^{\theta i}\end{pmatrix}$$

לאחר שער הדמרד השני פונקצית הגל הינה:

$$\psi = \frac{e^{\theta i}}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}e^{-\theta i}\\e^{\theta i}\end{pmatrix} = \frac{e^{\theta i}}{2}\begin{pmatrix}e^{-\theta i}+e^{\theta i}\\e^{-\theta i}-e^{\theta i}\end{pmatrix} = \frac{e^{\theta i}}{2}\begin{pmatrix}2\cos\theta\\-2i\sin\theta\end{pmatrix} = e^{\theta i}\begin{pmatrix}\cos\theta\\-i\sin\theta\end{pmatrix}$$

לאחר שער הפאזה השני, פונקצית הגל הינה:

$$\psi = e^{\theta i}\begin{pmatrix}1 & 0\\ 0 & e^{\phi+\pi/2}\end{pmatrix}\begin{pmatrix}\cos\theta\\ -i\sin\theta\end{pmatrix} = e^{\theta i}\begin{pmatrix}\cos\theta\\ -ie^{\phi+\pi/2}\sin\theta\end{pmatrix} = e^{\theta i}\begin{pmatrix}\cos\theta\\ -ie^{\phi}e^{\pi/2}\sin\theta\end{pmatrix} =$$

$$e^{\theta i}\begin{pmatrix}\cos\theta\\ e^{\phi}\sin\theta\end{pmatrix} = \begin{pmatrix}\cos\theta\\ e^{\phi}\sin\theta\end{pmatrix}$$

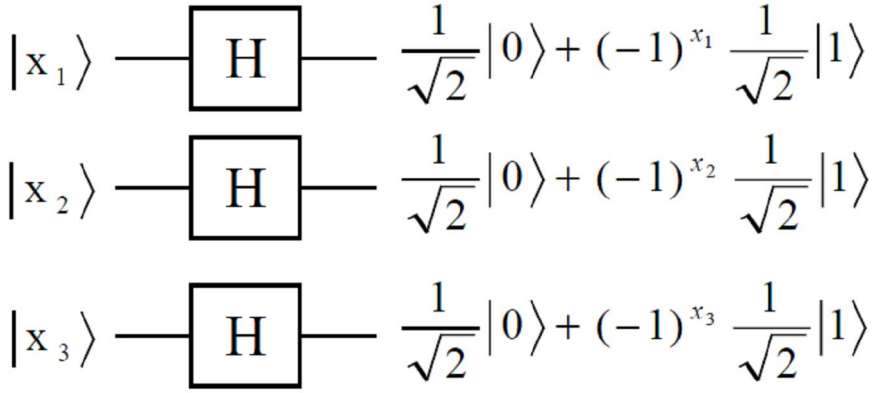
(השוויון האחרון הסתמך על שיווין עד כדי פאזה).

4. שערים לוגים לרגיסטר קיוביט

גם לרגיסטר של קיוביט אפשר לתאר למעשה אופרטורים/ שערים רבים ככל העולה על רוחנו, ובתנאי שמתקיים כי האופרטור הוא יוניטרי. נשים לב בנוסף, כי לרגיסטר בן n קיוביטים מתאים אופרטור $2^n \times 2^n$. להלן מספר שערים בעלי חשיבות מיוחדת:

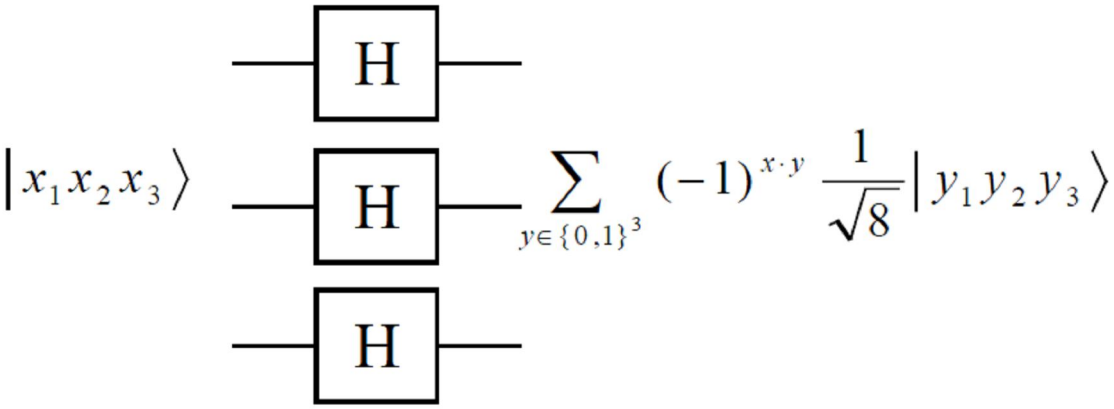
א. הדמרד

האופרטור כבר הוצג עבור קיוביט בודד. ונוכל להפעיל אותו על כל קיוביט בנפרד, לדוגמה , המעגל באיור 20 הינו עבור 3 קיוביטים, ומוצגות בו פונקציות הגל של כל קיוביט.



איור 20

באיור 21 מתוארת פונקצית הגל השקולה של כל הרגיסטר.



איור 21

או במילים- האופרטור ממפה את הרגיסטר לסופר פוזיציה של כל המצבים האפשריים בחלוקה שווה, כאשר המידע ,שוב, מופיע בפאזה. לא קשה לוודא כי הפאזה ניתנת לתיאור ע״י המכפלה של ביט לביט בין X לY , כלומר:

$$x \cdot y = x_1 y_1 \oplus x_2 y_2 \oplus x_3 y_3$$

גם הכיוון ההפוך נכון -אם ניקח פונקצית גל שהיא בעלת סופרפוזיציה כמתואר ונעביר דרך שערי הדמרד , אזי נקבל את פונקצית הגל בבסיס הסטנדרטי. זוהי תכונה חשובה מאוד, שנעשה בה שימוש נרחב מאוד בהמשך.

תרגיל : הראה כי:

$$H^{\otimes n} = \begin{pmatrix} H^{\otimes n-1} & H^{\otimes n-1} \\ H^{\otimes n-1} & -H^{\otimes n-1} \end{pmatrix}$$

פתרון:

באינדוקציה:

<u>בדיקה</u>: עבור n=2:

$$H \otimes H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

הנחת אינדוקציה:

$$H^{\otimes n}=\begin{pmatrix} H^{\otimes n-1} & H^{\otimes n-1} \\ H^{\otimes n-1} & -H^{\otimes n-1} \end{pmatrix}$$

צריך להראות:

$$H^{\otimes n+1}=\begin{pmatrix} H^{\otimes n} & H^{\otimes n} \\ H^{\otimes n} & -H^{\otimes n} \end{pmatrix}$$

הוכחה:

$$H^{\otimes n+1}=H\otimes H^{\otimes n}=\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\otimes\begin{pmatrix} H^{\otimes n-1} & H^{\otimes n-1} \\ H^{\otimes n-1} & -H^{\otimes n-1} \end{pmatrix}=\begin{pmatrix} H^{\otimes n-1} & H^{\otimes n-1} & H^{\otimes n-1} & H^{\otimes n-1} \\ H^{\otimes n-1} & -H^{\otimes n-1} & H^{\otimes n-1} & -H^{\otimes n-1} \\ H^{\otimes n-1} & H^{\otimes n-1} & -H^{\otimes n-1} & -H^{\otimes n-1} \\ H^{\otimes n-1} & -H^{\otimes n-1} & -H^{\otimes n-1} & H^{\otimes n-1} \end{pmatrix}$$

$$=\begin{pmatrix} H^{\otimes n} & H^{\otimes n} \\ H^{\otimes n} & -H^{\otimes n} \end{pmatrix}$$

מ.ש.ל.

תרגיל: הראה כי עבור $H^{\otimes n}$, השורה הראשונה הינה מהצורה $(1 \quad 1 \quad \dots \quad 1)$, והעמודה הראשונה ב הינה מהצורה: $\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$.

תרגיל: חשב את $H^{\otimes n}|0\rangle^{\otimes n}$.

פתרון:

$$H^{\otimes n}|0\rangle^{\otimes n}=\frac{1}{\sqrt{2^n}}\begin{pmatrix} 1 & 1 & 1 & 1 & \dots \\ 1 & ? & ? & ? & \\ 1 & ? & & & \\ 1 & ? & & & \\ \vdots & & & & \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}=\frac{1}{\sqrt{2^n}}\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$

ב.שער Controlled Not- CNOT

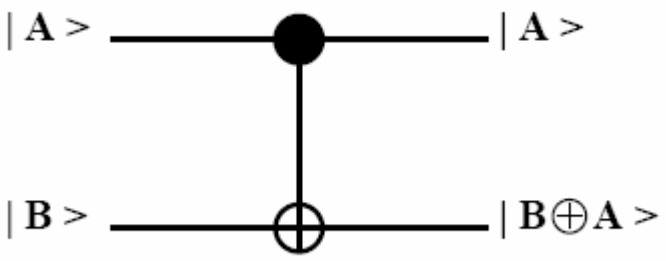
בדומה לשער XOR הקלאסי, מוגדר שער הCNOT הקוונטי הממפה 2 קיוביטים לפי המפה הבאה:

$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle$. דהיינו מיפוי של:

$$\begin{pmatrix}0\\0\\0\\1\end{pmatrix} \to \begin{pmatrix}0\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \to \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \to \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

מיפוי זה יכול להיכתב גם כ: $|A\rangle|B\rangle \to |A\rangle|\mathrm{A} \oplus \mathrm{B}\rangle$. המטריצה המייצגת שער זה נתונה ע"י:

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$, ומסומנת כמתואר באיור 22.



איור 22

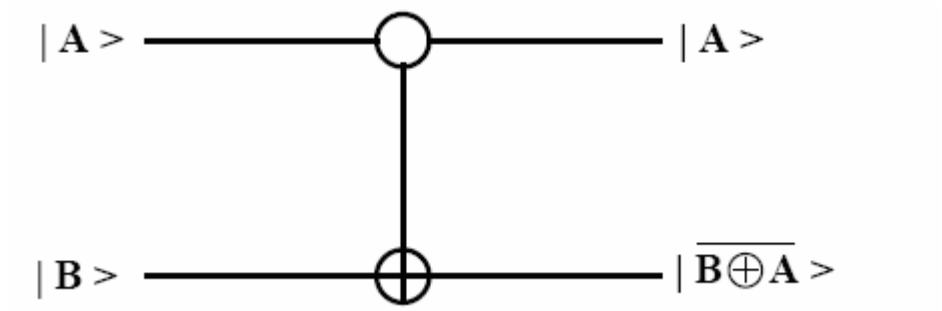
ניתן גם להתייחס אל השער בפירוש אחר- הקיוביט הראשון קובע את מצבו של השני. באם הראשון הינו 0 אזי השני שומר על ערכו. אחרת, ערכו מוחלף. זו הסיבה שלכניסה A קוראים גם כניסת הבקרה.

רעיון זה , של קיוביט בקרה על שער לקיוביט שני יופיע גם בהמשך, ועל כן הינו בעל חשיבות רבה.

לדוגמה, שער שימושי אחר הינו ווריאציה של שער זה, כך שכשביט הבקרה הינו 0 הערך מתחלף, דהינו

$|00\rangle \to |01\rangle, |01\rangle \to |00\rangle, |10\rangle \to |10\rangle, |11\rangle \to |11\rangle$. המטריצה המייצגת שער זה נתונה ע"י:

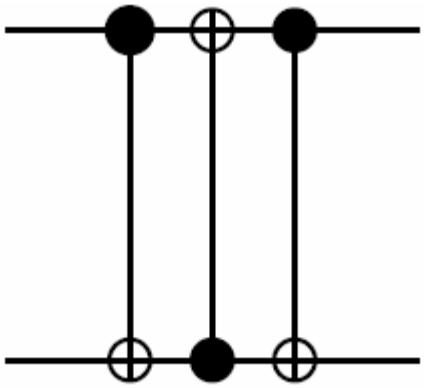
$$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$, ומסומנת כמתואר באיור 23.



איור 23

תרגיל:

הראה כי השער המתואר באיור 24, מבצע החלפה בין הקיובִיטים.



איור 24

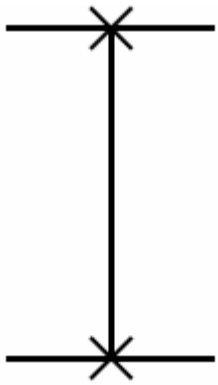
הוכחה:

השער האמצעי הינו: $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ (הוכח), ועל כן פעולת האופרטור:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

שהינו היפוך סיביות (הוכח).

שער זה מסומן לעיתים כמתואר באיור 25.

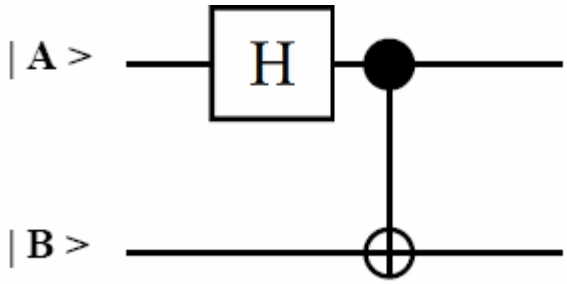


איור 25

תכונה נוספת של שער CNOT באה לידי ביטוי לאחר פעולת שער הדמרד. נתאר זאת בשני מקרים:

1) באם נפעיל את שער CNOT על קיוביטים כשאחד עבר שער הדמרד והשני לא (אחד בסופרפוזיציה של שני מצבים והשני טהור), כמתואר באיור 26 נקבל כי:

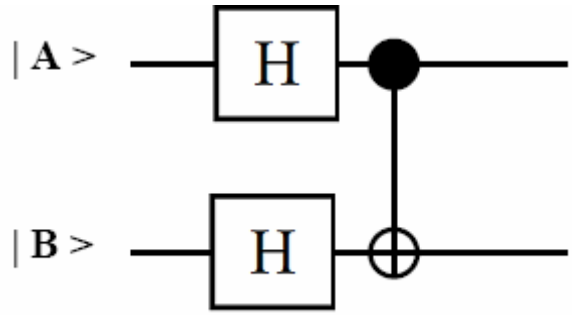
$$|0\rangle\left(|0\rangle+|1\rangle\right)\xrightarrow{CNOT}|0\rangle\left(|0\rangle+|1\rangle\right)$$
$$|1\rangle\left(|0\rangle+|1\rangle\right)\xrightarrow{CNOT}|1\rangle\left(|1\rangle+|0\rangle\right)=|1\rangle\left(|0\rangle+|1\rangle\right)$$
$$|0\rangle\left(|0\rangle+|1\rangle\right)\xrightarrow{CNOT}|0\rangle\left(|0\rangle+|1\rangle\right)$$
$$|1\rangle\left(|0\rangle-|1\rangle\right)\xrightarrow{CNOT}|1\rangle\left(|1\rangle-|0\rangle\right)=-|1\rangle\left(|0\rangle-|1\rangle\right)$$



איור 26

זאת אומרת ששער הCNOT בשלושת המקרים הראשונים לא השפיע על פונקצית הגל, אך במקרה האחרון גרם לשינוי פאזה של פונקצית הגל. מכאן אני למדים שבעזרת שער CNOT ניתן לבצע שינוי מותנה בפונקצית גל (אם היא במצב אחד לא יהיה שינוי, אם היא במצב אחר יהיה).

2) באם נפעיל את שער CNOT על קיוביטים לאחר שעברו שערי הדמרד (שניהם בסופרפוזיציה של שני מצבים), כמתואר באיור 27 נקבל כי:



איור 27

$$|+\rangle|+\rangle=(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\xrightarrow{CNOT}|0\rangle(|0\rangle+|1\rangle)+|1\rangle(|1\rangle+|0\rangle)=(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)=|+\rangle|+\rangle$$
$$|-\rangle|+\rangle=(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)\xrightarrow{CNOT}|0\rangle(|0\rangle+|1\rangle)-|1\rangle(|1\rangle+|0\rangle)=(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)=|-\rangle|+\rangle$$
$$|+\rangle|-\rangle=(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)\xrightarrow{CNOT}|0\rangle(|0\rangle-|1\rangle)+|1\rangle(|1\rangle-|0\rangle)=(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)=|-\rangle|-\rangle$$
$$|-\rangle|-\rangle=(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)\xrightarrow{CNOT}|0\rangle(|0\rangle-|1\rangle)-|1\rangle(|1\rangle-|0\rangle)=(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)=|+\rangle|-\rangle$$

שניתן לפרשו כשינוי פאזה בקיוביט אחד (הימני) לפי מצב הקיוביט השני (השמאלי) שכן כאשר הימני הינו $|+\rangle$ השמאלי נשאר כמות שהוא, וכאשר הימני הינו $|-\rangle$ השמאלי משנה את הפאזה שלו מ $|+\rangle$ ל $|-\rangle$ ומ $|-\rangle$ ל $|+\rangle$.

ג. שערי controlled ו Toffoli קוונטי

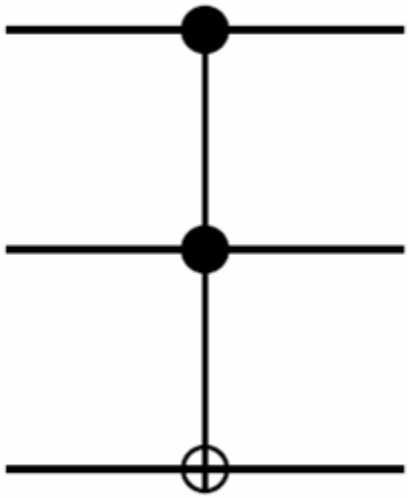
בדומה לשער ה controlled שהוצג ממקודם כשקו הבקרה הינו קיוביט בודד, והאופרטור שהופעל, אם הופעל, על קו המטרה היה NOT ניתן להגדיר שער שבו האופרטור הינו אחר. למקרה הכללי נניח ונתון אופרטור על קיוביט:

$$\begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix}$$

אזי האופרטור ה controlled שלו נתון על ידי:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{01} \\ 0 & 0 & x_{10} & x_{11} \end{pmatrix}$$

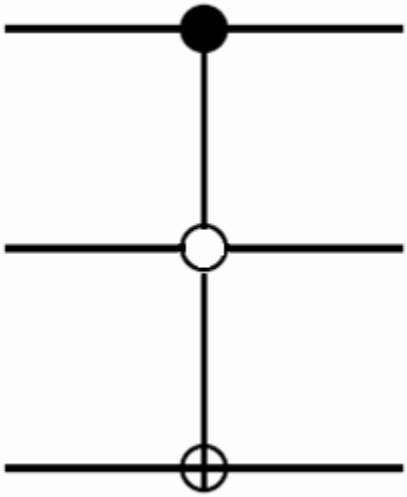
ניתן אף להרחיב רעיון זה לצורה כללית עוד יותר כשקו הבקרה הינו מספר קיוביטים – כאשר קו הבקרה בעל ערך מסוים קיוביט המטרה לא משתנה, וכאשר קו הבקרה בעל ערך אחר מופעל אופרטור על קיוביט המטרה. לדוגמה, באיור 28 מתואר שער controlled Not בו קו הבקרה בינו בן 2 קיוביטים (הקיוביטים העליונים) שאינם משתנים במוצא- ואילו הקיוביט התחתון (המטרה) מתהפך במידה ורגיסטר הבקרה הינו $|11\rangle$.



איור 28

ניתן לתאר את פעולת השער כ $|x\rangle|q\rangle \to |x\rangle|x \oplus q\rangle$, דהיינו האנלוגיה הקוונטית לשער Toffoli.

לעומתו באיור 29 מתואר שער controlled Not בו קיוביט המטרה מתהפך במידה ורגיסטר הבקרה הינו $|10\rangle$.



איור 29

ד. שער שינוי פאזה מותנה

שער זה אשר יעשה בו שימוש בהמשך, מוגדר ע"י:

$$A(\psi) = \begin{cases} |0\rangle & |\psi\rangle = |0\rangle \\ -|\psi\rangle & |\psi\rangle \neq |0\rangle \end{cases}$$

או במילים- עבור וקטור בסיס $|0\rangle$ אין שינוי, עבור וקטור בסיס אחר- היפוך פאזה.

תרגיל: הראה כי פעולת האופרטור שקולה להפעלת האופרטור : $2|0\rangle\langle 0|-I$.

פתרון:

$$2|0\rangle\langle 0|-I=\begin{pmatrix}1 & 0 & \dots & 0\\ 0 & -1 & \dots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & -1\end{pmatrix}$$

הפעלתו על $|0\rangle$:

$$\begin{pmatrix}1 & 0 & \dots & 0\\ 0 & -1 & \dots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix}=\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix}=|0\rangle$$

ועל וקטור בסיס אחר $|x\rangle$:

$$\begin{pmatrix}1 & 0 & \dots & 0\\ 0 & -1 & \dots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & -1\end{pmatrix}\begin{pmatrix}0\\ \vdots\\ k\\ \vdots\\ 0\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ -k\\ \vdots\\ 0\end{pmatrix}=-|k\rangle$$

5. השוואת שער קוונטי מול שער קלאסי

האם כל פונקציה בוליאנית הניתנת לחישוב במחשב קלאסי ניתנת לחישוב במחשב קוונטי? בכדי לענות על שאלה זו, נבנה שער Toffoli במחשב קוונטי. שער Toffoli יכול להיות מוצג גם בדרך הבאה- שלושת המוצאות שלו זהים לערך הכניסה, למעט המוצא השלישי שהינו הופכי במידה ושני הכניסות האחרות הינן 1 (ז"א שער controlled not כמתואר באיור 28).

ניתן לתאר זאת ע"י האופרטור הבא:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(הערה: בגלל שהאופרטור מעל R וסימטרי, הdagger שלו הוא הוא עצמו).

נשים לב, כי אופרטור זה יפעל גם על ביט קלאסי (דהיינו מקרה פרטי של קיוביט שפונקצית הגל שלו עם מקדם אחד בעל ערך 1), וכך נוכל לדמות הפעלת השער לחישוב קלאסי.

מכיוון שבעזרת שער זה ניתן לבצע כל פונקציה בוליאנית, פועל יוצא מכך הוא שכל פונקציה בוליאנית דטרמיניסטית הניתנת לחישוב ע״י מחשב קלאסי, ניתנת לחישוב ע״י מחשב קוונטי .
מכאן מתקבלת התשובה כי מחשב קוונטי הינו לפחות ״חזק״ כמו מחשב קלאסי.

פרק שישי- ייצוג גרפי

1. ייצוג גראפי של קיוביט

את מצב הקיוביט והמניפולציות עליו נוח לעיתים לתאר בצורה גראפית. כך ניתן לקבל משמעות "גראפית" לפעולה שמבצעים עליו.

לו פונקצית הגל הייתה מעל הממשים R, אזי קל היה לתאר את הווקטור כנקודה על מעגל היחידה. במבט ראשון נראה שמכיוון שפונקצית הגל הינה מעל המרוכבים, נזדקק למרחב 4 מימדי בכדי לתאר בצורה גראפית את הקיוביט- אך לא כך הדבר, שכן תכונות פונקצית הגל מאפשרות לתאר אותה במרחב התלת מימדי כנקודה ע"ג כדור יחידה Bloch sphere . מטרת סעיף זה הינה לראות כיצד.

פונקצית הגל של קיוביט בודד נתונה ע"י

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

בעזרת סימון אוילר:

$$e^{i\alpha} = \cos\alpha + i\sin\alpha$$

נוכל לרשום את פונקצית הגל כ:

$$|\psi\rangle = r_\alpha e^{i\alpha}|0\rangle + r_\beta e^{i\beta}|1\rangle$$

כאשר $r_\alpha, \alpha, r_\beta, \beta$ ממשיים. מכלל הזהות עד כדי פאזה גלובלית נובע כי ניתן להכפיל את פונקצית הגל ב $e^{-i\alpha}$, מבלי לפגוע בה:

$$|\psi\rangle = e^{-i\alpha}|\psi\rangle = r_\alpha e^{-i\alpha}e^{i\alpha}|0\rangle + r_\beta e^{i\beta}e^{-i\alpha}|1\rangle = r_\alpha|0\rangle + r_\beta e^{i\delta}|1\rangle = r_\alpha|0\rangle + (x+iy)|1\rangle$$

(כאשר r_α, x, y ממשים). מכיוון שפונקצית הגל מקיימת:

$$\langle\psi|\psi\rangle = 1$$

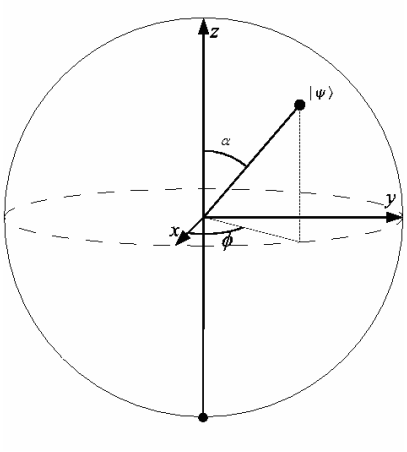
נקבל:

$$|r_\alpha|^2 + |(x+iy)|^2 = 1$$
$$r_\alpha{}^2 + (x+iy)^*(x+iy) = 1$$
$$r_\alpha{}^2 + x^2 + y^2 = 1$$

דהיינו- קיבלנו כי המקדמים הממשים מקיימים משוואה של כדור. ע"כ ניתן לייצג את הקיוביט כנקודה על פני כדור ברדיוס יחידה. ייצוג כדור יחידה בקואורדינאטות פולאריות נתון ע"י:

$$x = \sin\alpha\cos\phi$$
$$y = \sin\alpha\sin\phi$$
$$z = \cos\alpha$$

כאשר הקואורדינאטות מסומנות כמתואר באיור 30.



איור 30

נסמן- $r_\alpha = \cos\alpha = z$, ונקבל:

$$|\psi\rangle = \cos\alpha|0\rangle + (x+iy)|1\rangle = \cos\alpha|0\rangle + (\sin\alpha\cos\phi + i\sin\alpha\sin\phi)|1\rangle =$$
$$\cos\alpha|0\rangle + e^{i\phi}\sin\alpha|1\rangle$$

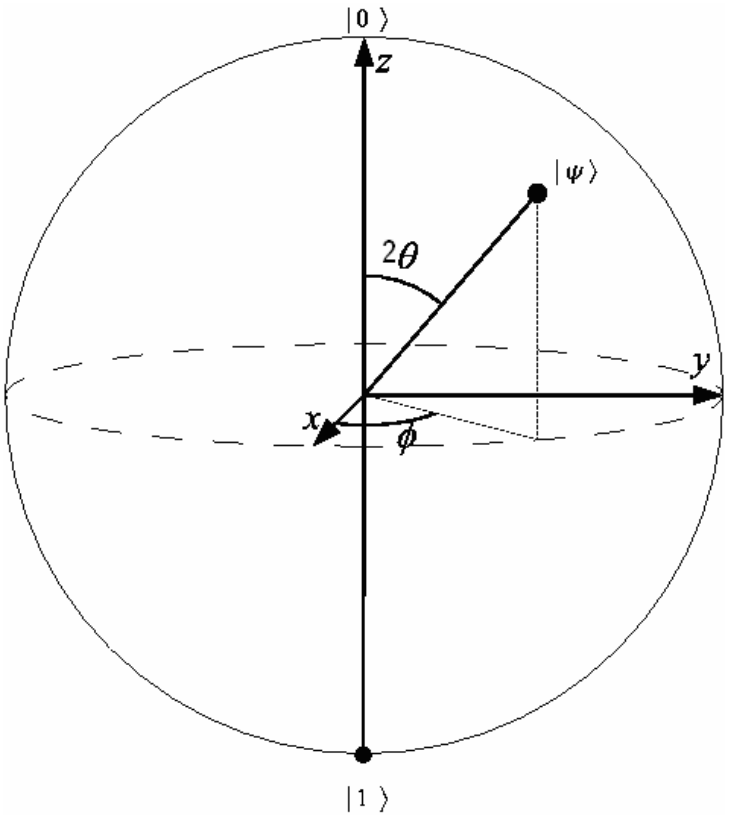
כאשר $0 \le \alpha \le 2\pi$, $0 \le \phi \le 2\pi$.

לשם הנוחות, נסמן $\alpha = \frac{\theta}{2}$, ואז נוכל לרשום:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}$$

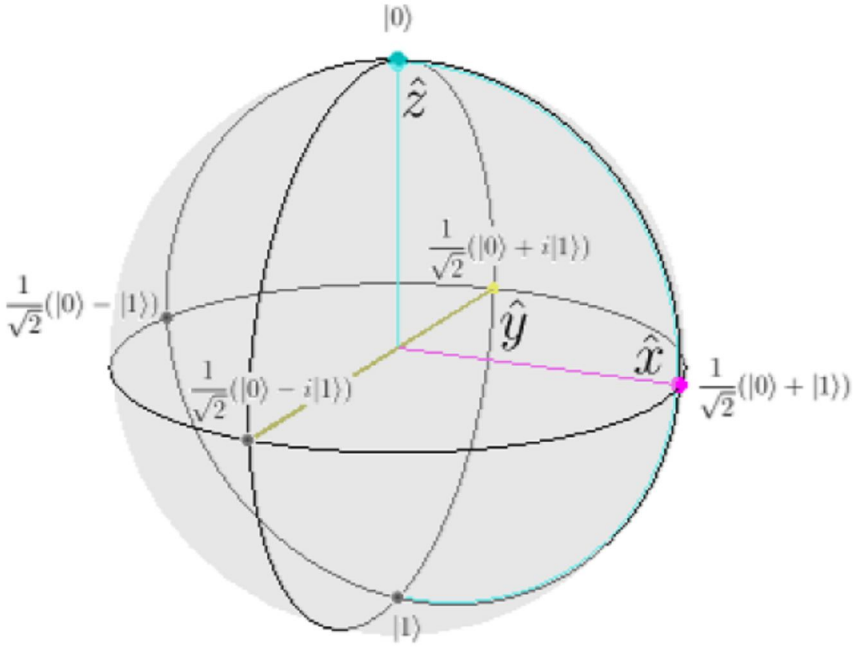
כאשר $0 \le \theta \le \pi$, $0 \le \phi \le 2\pi$.

ואז נקבל שאם $\theta = 0$ נייצג את $|\psi\rangle = |0\rangle$, ואם $\theta = \pi$ נייצג את $|\psi\rangle = |1\rangle$, כמתואר באיור 31:



איור 31

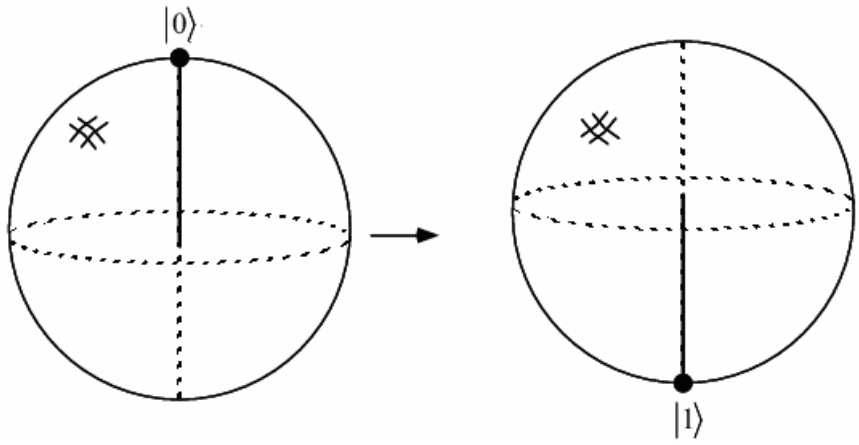
לצורך ההבהרה, באיור איור 32 מוצגות מספר פונקציות גל על כדור בלוך:



איור 32

2. שער לוגי לקיוביט בודד- ייצוג גרפי

לאחר שייצגנו בצורה גראפית קיוביט, ניתן לתאר מה יקרה מבחינה גרפית לקיוביט לאחר הפעלת אופרטור עליו. לדוגמא, שער X הוגדר כך שהפעלתו על $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ נקבל $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$ - מבחינה גרפית זה שקול להחלפת ההגדרה לגבי מיקום $|1\rangle$ ו $|0\rangle$ זה בזה, או במילים אחרות סיבוב סביב ציר X של 180^o. כמתואר באיור 33:



איור 33

יתרה מזאת- בסעיף זה נוכיח כי כל שער לוגי קוונטי ניתן לתיאור כפעולות סיבוב על גבי כדור בלוך.

א. מטריצת סיבוב:

האופרטורים X,Y ו Z (שהוגדרו בסעיף הקודם) מקיימות שריבועיהם הינה מטריצת יחידה:

$$X^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$Y^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$Z^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

בפרק המבוא הראנו כי עבור המקרה הפרטי של מטריצה A המקיימת $A^2 = I$:

$$e^{i\theta A} = \cos(\theta)I + i\sin(\theta)A$$

נגדיר את האופרטורים הבאים:

$$e^{\frac{-i\theta}{2}X} \equiv R_x(\theta)$$

$$e^{\frac{-i\theta}{2}Y} \equiv R_y(\theta)$$

$$e^{\frac{-i\theta}{2}Z} \equiv R_z(\theta)$$

אופרוטורים אלו ניתנים לכתיבה כ:

$$R_x(\theta) \equiv e^{\frac{-i\theta}{2}X} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_y(\theta) \equiv e^{\frac{-i\theta}{2}Y} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_z(\theta) \equiv e^{\frac{-i\theta}{2}Z} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{\frac{-i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix}$$

תרגיל: הראה כי $R_z(\theta)$ מתארת סיבוב סביב ציר Z.

פתרון:

הפעלת אופרטור $R_z(\theta)$ על $|\psi\rangle = \begin{pmatrix} \cos\frac{\sigma}{2} \\ e^{i\phi}\sin\frac{\sigma}{2} \end{pmatrix}$ הינה:

$$\begin{pmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix}\begin{pmatrix} \cos\frac{\sigma}{2} \\ e^{i\phi}\sin\frac{\sigma}{2} \end{pmatrix} = \begin{pmatrix} e^{-\frac{i\theta}{2}}\cos\frac{\sigma}{2} \\ e^{\frac{i\theta}{2}}e^{i\phi}\sin\frac{\sigma}{2} \end{pmatrix} = e^{-\frac{i\theta}{2}}\begin{pmatrix} \cos\frac{\sigma}{2} \\ e^{i\theta}e^{i\phi}\sin\frac{\sigma}{2} \end{pmatrix} =$$

$$\begin{pmatrix} \cos\frac{\sigma}{2} \\ e^{i(\theta+\phi)}\sin\frac{\sigma}{2} \end{pmatrix}$$

(השוויון האחרון הינו עד כדי פאזה). מהתוצאה עולה כי הפעלת האופרטור שינתה את הזווית ϕ של פונקציה הגל ל $\phi+\theta$- או במילים אחרות- סיבוב סביב ציר Z בזווית θ.

באופן דומה ניתן להראות כי $R_x(\theta)$ ו $R_y(\theta)$ מגדירות סיבוב סביב ציר X ו Y.

לדוגמה, ציינו כבר כי הפעלת שער X שקולה לסיבוב של 180^o סביב ציר X (עד כדי שינוי פאזה). ניתן להראות זאת גם בדרך הבאה:

$$R_x(\pi)=\begin{pmatrix}\cos\frac{\pi}{2} & -i\sin\frac{\pi}{2}\\ i\sin\frac{\pi}{2} & \cos\frac{\pi}{2}\end{pmatrix}=\begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}=-i\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=-iX$$

ב. פירוק מטריצה יוניטרית

<u>משפט</u>: כל מטריצה יוניטרית U ניתנת לפירוק הבא:

$$U=e^{i\alpha}R_z(\beta)R_Y(\gamma)R_z(\delta)$$

כאשר $\alpha,\beta,\gamma,\delta$ ממשים.

הוכחה:

$$e^{i\alpha}R_z(\beta)R_Y(\gamma)R_z(\delta)=e^{i\alpha}\begin{pmatrix}e^{-i\beta/2} & 0\\ 0 & e^{i\beta/2}\end{pmatrix}\begin{pmatrix}\cos\frac{\gamma}{2} & \sin\frac{\gamma}{2}\\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2}\end{pmatrix}\begin{pmatrix}e^{-i\delta/2} & 0\\ 0 & e^{i\delta/2}\end{pmatrix}=$$

$$e^{i\alpha}\begin{pmatrix}e^{-i\beta/2} & 0\\ 0 & e^{i\beta/2}\end{pmatrix}\begin{pmatrix}e^{-i\delta/2}\cos\frac{\gamma}{2} & e^{i\delta/2}\sin\frac{\gamma}{2}\\ e^{-i\delta/2}\sin\frac{\gamma}{2} & e^{i\delta/2}\cos\frac{\gamma}{2}\end{pmatrix}=e^{i\alpha}\begin{pmatrix}e^{i(-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(-\beta/2+\delta/2)}\sin\frac{\gamma}{2}\\ e^{i(\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\beta/2+\delta/2)}\cos\frac{\gamma}{2}\end{pmatrix}$$

$$=\begin{pmatrix}e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2}\\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2}\end{pmatrix}$$

U היא יוניטרית, ועל כן היא ניתנת לרישום כ:

$$U=\begin{pmatrix}e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2}\\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2}\end{pmatrix}$$

תרגיל: הוכח כי בהצגה זו השורות והעמודות הן אורתונורמליות.

ולכן $U=e^{i\alpha}R_z(\beta)R_Y(\gamma)R_z(\delta)$. מ.ש.ל.

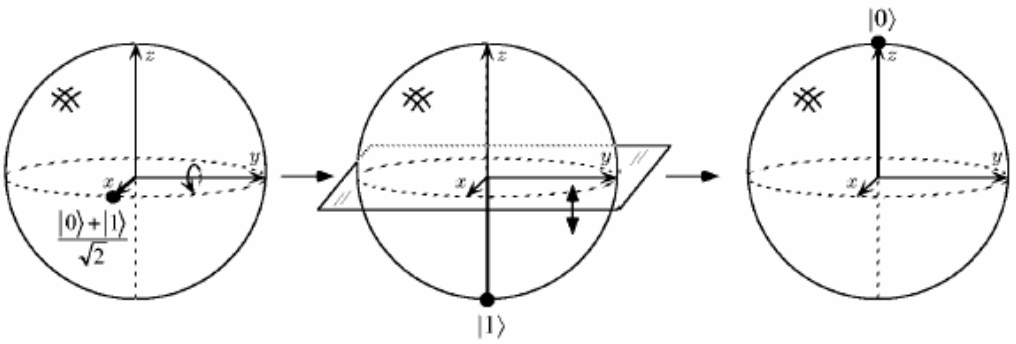
אין שום דבר מיוחד דווקא בציר Y ובציר Z שדווקא הם מופיעים בפירוק- למעשה ניתן להכליל עוד יותר את המשפט ולקבוע כי :

<u>משפט</u>: כל מטריצה יוניטרית U ניתנת לפירוק הבא:

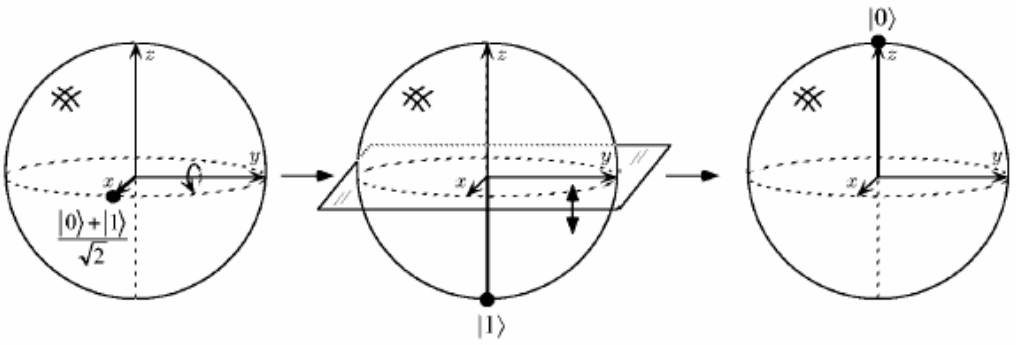
$U = e^{i\alpha} R_l(\beta) R_m(\gamma) R_l(\delta)$ כאשר l ו m הינם שני צירים לא מקבילים ו $\alpha, \beta, \gamma, \delta$ ממשים.

לדוגמה, אופרטור Hadamrad, שקול לסיבוב של 0^o סביב ציר X , א"כ לסיבוב של 90^o סביב ציר Y, א"כ סביב ציר X ב 180^o כפי שניתן לראות

ב



איור 34 , המתאר סיבובים אלו על קיוביט במצב התחלתי $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ו לאחר הפעלת האופרטור מצב הקיוביט $|0\rangle$:



איור 34

שכן:

$$R_x(\pi)R_Y(\frac{\pi}{2})R_x(0)=\begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}\begin{pmatrix}\frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2}\\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}\begin{pmatrix}\frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2}\\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}\end{pmatrix}=\frac{-\sqrt{2}}{2}i\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

$$=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}=H$$

כאשר, שוב, השוויון האחרון הינו עד כדי פאזה.

חלק שני: אלגוריתמים

בחלק זה נציג מספר אלגוריתמים קוונטים מעניינים. לרוב יוצג פתרון סכמתי לבעיה המוצגת, כאשר המוסכמות הנהוגות באיורים הינם:

1) המידע זורם מצד ימין לשמאל- צד שמאל של האיור הינו הכניסה, צד ימין- המוצא.

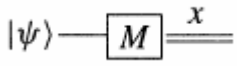
2) קו בודד הינו קו תקשורת קוונטי (המשמש להעברת קיוביט במצב כלשהו).

3) קו וסימן מעליו, $\overset{\mathbf{n}}{\diagup}$ משמש לסימון n קווי תקשורת.

4) קו כפול $\equiv$, משמעו קו תקשורת סטנדרטי – לא קוונטי שמשמש להעברת ביט.

5) שער לוגי מתואר כפי שכבר למדנו (ריבוע ובתוכו אות המייצגת את שם השער).

6) מדידה מתוארת ע"י:



או

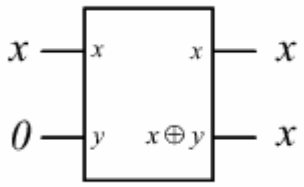
פרק שביעי- אלגוריתמי תקשורת

בפרק זה נדון בהעברת מידע בין שני אתרים, תוך שימוש בכלים שנלמדו עד כה. על פניו נראה כי העברת קיוביט על גבי קו תקשורת סטנדרטי הינה משימה לא פשוטה כלל וכלל- שכן איך נדע את ערכי ההסתברות שלו? הרי אחרי מדידה אחת הוא יקרוס לערך מסוים ולא נוכל לדעת כיצד בדיוק היה מצבו לפני המדידה. זאת ועוד -גם לו היה לנו מידע על ערכי ההסתברויות שלו, נראה כי היה צריך רוחב פס גדול מאוד על מנת להעביר את מצבו המדויק- שכן יש להעביר מידע על מספרים לא רציונאליים ברמת דיוק ללא עיגול. מלבד כל הבעיות הללו,ישנה בעיה נוספת המוכרת כ"משפט אי השיבוט",(שאותו נוכיח בסעיף הבא) הקובע כי לא ניתן לשכפל קיוביט. זאת אומרת שלא ניתן לשדרו כפי שמשדרים ביטים רגילים- כי בשידור ביט רגיל למעשה מבצעים שכפול שלו בצד המקבל.

למרות כל האמור לעיל,מסתבר כי ניתן לשדר קיוביט (טלפורטציה) על קו תקשורת רגיל כך שלא משכפלים אותו אלא "מעבירים" אותו בין האתרים מבלי למדוד. יתרה מכך- בעזרת שינוי קטן באלגוריתם נראה כיצד ניתן לשדר ביטים סטנדרטים בחצי רוחב פס מהנדרש בגישה הקלאסית על גבי קווי תקשורת קוונטית.

1. עקרון אי השיבוט –no cloning:

נניח כי ברצוננו לשכפל ערך של קיוביט, כך שאם יש לנו קיוביט במצב מסוים יהיו לנו לאחר המניפולציה 2 קיוביטים במצב זה (מין FANOUT על קיוביטים). תחילה, ננסה למצוא שקול קוונטי לפעולת FANOUT סטנדרטית והפיכה. דוגמה אחת למימוש של שער FANOUT קלאסי הפיך נתונה באיור- המתאר שער XOR קלאסי והפיך, שבכניסה אחת הביט x שרוצים לשכפל ובכניסה השנייה 0,כמתואר באיור 35 :



איור 35

על כן, ניתן לצפות כי בהינתן שער קוונטי המקביל לשער זה , דהיינו CNOT , אזי לו נספק בכניסה קיוביט כלשהו, ו $|0\rangle$ אזי נקבל שער FANOUT , או שיכפול של הקיוביט- אך לא כך הוא הדבר. שכן לפי המיפוי שהוגדר לשער CNOT, לכל קיוביט x מתקיים : $|x0\rangle \to |xx\rangle$.מיפוי זה מבצע FANOUT רק אם x טהור- כי אם $|x\rangle = |0\rangle$ אזי המוצא הינו $|00\rangle$, ואם $|x\rangle = |1\rangle$ אזי

המוצא הינו $|11\rangle$ - אבל, עבור המקרה הכללי $|x\rangle = \alpha|0\rangle + \beta|1\rangle$, אזי אם נכניס אותו לשער CNOT לכניסת הבקרה, ו $|0\rangle$ בכניסה השנייה, אזי נקבל:

$[\alpha|0\rangle + \beta|1\rangle]|0\rangle \to \alpha|00\rangle + \beta|11\rangle$ - דהיינו מצב שזור, ולא FANOUT. מכאן שהשימוש בשער זה לא צלח לשם העתקת קיוביט. אין זאת הוכחה פורמאלית שהדבר איננו אפשרי – אלא רק הצבעה על כך שכנראה אופרטור של FANOUT איננו כל כך טריוויאלי כפי שניתן היה לחשוב במבט ראשון. ומכאן מתעוררת השאלה- אולי נוכל לחשוב על מניפולציה אחרת לקבלת FANOUT? התשובה לשאלה, כך מתברר היא שלילית, כפי שקובע משפט אי השיבוט.

<u>משפט אי השיבוט</u>: לא קיימת מטריצה יוניטרית M אשר מקיימת: $M|\psi\rangle|\varphi\rangle = |\psi\rangle|\psi\rangle$ לכל קיוביט $|\psi\rangle$ וקיוביט עזר $|\varphi\rangle$.

<u>הוכחה:</u>

נניח וקיימת כזו מטריצה. אזי בהינתן קיוביט בעל פונקציות גל ψ נזדקק לקיוביט עזר (שכן אם המוצא הינו של 2 קיוביטים אזי גם המבוא חייב להיות בעל 2 קיוביטים בכדי שנוכל לקיים הפיכות). נניח כי פונקציית הגל של קיוביט העזר הינה ϕ, וכמובן שאין איזשהו קשר בין 2 הקיוביטים (פונקציות הגל).

מההנחה נובע כי:

$$M|\psi\rangle|\varphi\rangle = |\psi\rangle|\psi\rangle$$

וגם

$$M|\phi\rangle|\varphi\rangle = |\phi\rangle|\phi\rangle .$$

מכיוון שמטריצה יוניטרית שומרת מכפלה פנימית, אזי המכפלה הפנימית של $|\psi\rangle|\varphi\rangle$ ב $|\phi\rangle|\varphi\rangle$ היא:

$$(|\psi\rangle|\varphi\rangle) \circ (|\phi\rangle|\varphi\rangle) = (|\psi\rangle|\varphi\rangle)^\dagger |\phi\rangle|\varphi\rangle = |\psi\rangle^\dagger |\varphi\rangle^\dagger |\phi\rangle|\varphi\rangle =$$
$$\langle\psi|\phi\rangle\langle\varphi|\varphi\rangle = \langle\psi|\phi\rangle$$

זהה למכפלה הפנימית של $M|\psi\rangle|\varphi\rangle$ ב $M|\phi\rangle|\varphi\rangle$ דהיינו-

$$(M|\psi\rangle|\varphi\rangle) \circ (M|\phi\rangle|\varphi\rangle) = (|\psi\rangle|\psi\rangle) \circ (|\phi\rangle|\phi\rangle) = (|\psi\rangle|\psi\rangle)^\dagger |\phi\rangle|\phi\rangle = |\psi\rangle^\dagger |\psi\rangle^\dagger |\phi\rangle|\phi\rangle =$$
$$\langle\psi|\phi\rangle\langle\psi|\phi\rangle = \left(\langle\psi|\phi\rangle\right)^2$$

ז"א קיבלנו שמתקיים: $\langle\psi|\phi\rangle = \left(\langle\psi|\phi\rangle\right)^2$, או במילים אחרות- $x = x^2$ וזה נכון רק אם

$x=1$ דהיינו $|\psi\rangle=|\phi\rangle$, (זאת אומרת צריך שקיוביט העזר יהיה בעצמו העתק של $|\psi\rangle$) או $x=0$

זאת אומרת צריך שקיוביט העזר יהיה אורתוגונאלי ל $|\psi\rangle$ - לכן האופרטור יכול לשכפל רק קיוביטים אורתוגונאליים זה לזה ולא קיוביטים כל שהם. על כן , אין בנמצא אופרטור יוניטרי שכזה- מ.ש.ל.

לסיכום, ממשפט אי השיבוט בעצם נובע כי לא קיים אופרטור שבעזרתו ניתן לשכפל מצב של קיוביט. (אין FANOUT לקיוביט).

2. שידור ערך קיוביט- טלפורטציה

כאמור , למרות כל הקשיים לכאורה שנראה שישנם בשידור ערך קיוביט ע״ג קו תקשורת סטנדרטי, נראה כי קיים אלגוריתם העושה שימוש בתופעת המצב שזור ומאפשר תקשורת שכזו.

על פניו נראה כי ניתן להיעזר במצב שזור לשידור מהיר מאוד, שכן אם כי בידנו 2 קיוביטים במצב שזור, לדוגמה $|\phi_+\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, וכעת מרחיקים את אחד הקיוביטים לאתר מרוחק (נניח את השמאלי) אז ברגע שנמדוד את הקיוביט שנשאר בידנו, ערכו של השני (המרוחק) יקבע באופן מידי . (שכן אם נמדוד $|1\rangle$ אזי מובטח כי באתר המרוחק ערכו $|1\rangle$, ואם נמדוד $|0\rangle$ אזי מובטח כי באתר המרוחק ערכו $|0\rangle$). אך אין כאן באמת העברת מידע- אין אנו יודעים מה אנו משדרים שכן רק בעת שמדדנו את הקיוביט הבנו מה אנו משדרים.

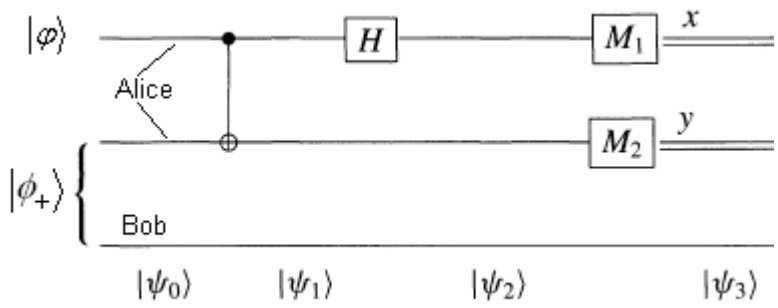
א. הצגת הבעיה

נניח כי אנו מעוניים לשדר קיוביט (בעל פונקצית גל $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$) מאליס (A) לבוב (B), על גבי קו תקשורת רגיל- וזאת, מבלי למדוד את הקיוביט (ז״א שלא יקרוס) ומבלי להפר את כלל אי השיבוט .

ב. פתרון סכמאתי

נניח ואליס ובוב נפגשו בעבר, וחלקו ביניהם 2 קיוביטים שהיו במצב שזור, למשל באחד ממצבי בל: $|\phi_+\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. כך שלאליס יש קיוביט במצב שזור (עם קיוביט שאצל בוב) וקיוביט $|\varphi\rangle$ שאותו היא מעוניינת להעביר לבוב.

נתאר את פתרון הבעיה באיור 36.



איור 36

שני קווי התקשורת העליונים הם הצד של אליס, והקו התחתון הוא של בוב. ננתח את פונקצית הגל בכל שלב:

לצורך הנוחות, נסמן את הקיוביטים שבידי אליס עם קו תחתון.

מצב המערכת ההתחלתי נתון ע"י:

$$\psi_0 = |\varphi\rangle|\phi_+\rangle = \frac{1}{\sqrt{2}}\left[\alpha|\underline{0}\rangle(|\underline{0}\underline{0}\rangle + |\underline{1}\underline{1}\rangle) + \beta|\underline{1}\rangle(|\underline{0}\underline{0}\rangle + |\underline{1}\underline{1}\rangle)\right]$$

כעת אליס תבצע את האלגוריתם הבא:

1) את שני הקיוביטים שברשותה היא מעבירה ב CNot כאשר קיוביט הבקרה הינו הקיוביט שרוצים להעביר. מצב המערכת כעת הינו:

$$\psi_1 = \frac{1}{\sqrt{2}}\left[\alpha|\underline{0}\rangle(|\underline{0}\underline{0}\rangle + |\underline{1}\underline{1}\rangle) + \beta|\underline{1}\rangle(|\underline{1}\underline{0}\rangle + |\underline{0}\underline{1}\rangle)\right]$$

2) המוצא הראשון של השער יעבור דרך אופרטור הדמרד.

מצב המערכת כעת הינו:

$$\psi_2 = \frac{1}{2}\left[\alpha(|\underline{0}\rangle + |\underline{1}\rangle)(|\underline{0}\underline{0}\rangle + |\underline{1}\underline{1}\rangle) + \beta(|\underline{0}\rangle - |\underline{1}\rangle)(|\underline{1}\underline{0}\rangle + |\underline{0}\underline{1}\rangle)\right]$$

$$= \frac{1}{2}\left[\alpha|\underline{0}\underline{0}\underline{0}\rangle + \alpha|\underline{0}\underline{1}\underline{1}\rangle + \alpha|\underline{1}\underline{0}\underline{0}\rangle + \alpha|\underline{1}\underline{1}\underline{1}\rangle + \beta|\underline{0}\underline{1}\underline{0}\rangle + \beta|\underline{0}\underline{0}\underline{1}\rangle - \beta|\underline{1}\underline{1}\underline{0}\rangle - \beta|\underline{1}\underline{0}\underline{1}\rangle\right]$$

$$= \frac{1}{2}\left[|\underline{0}\underline{0}\rangle(\alpha|0\rangle + \beta|1\rangle) + |\underline{0}\underline{1}\rangle(\alpha|1\rangle + \beta|0\rangle) + |\underline{1}\underline{0}\rangle(\alpha|0\rangle - \beta|1\rangle) + |\underline{1}\underline{1}\rangle(\alpha|1\rangle - \beta|0\rangle)\right]$$

מהמשוואה האחרונה עולה כי הצלחנו לראות שפונקצית הגל של כל המערכת מתארת את השזירות בין הקיוביטים שאצל אליס לקיוביט שאצל בוב. אם אצל אליס הקיוביטים במצב $|\underline{0}\underline{0}\rangle$ אז אצל בוב הם במצב $(\alpha|0\rangle + \beta|1\rangle)$, וכך הלאה. לכן, אליס מבצעת מדידות בצד שלה כדי לדעת מה מצב המערכת. ואת תוצאת המדידה היא משדרת על קו רגיל (ביטים קלאסיים). ייתכנו 4 אפשריות:

1) אם אליס תמדוד את המערכת שלה ותקבל $|00\rangle$ אזי אליס תשלח x=y=0, ובוב לא צריך לבצע שום מניפולציה שכן הקיוביט שאצלו נמצא במצב $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$.

2) אם יתקבל כי אצל אליס הם במצב $|01\rangle$ אזי אליס תשלח $x=0, y=1$ כדי לסמן לבוב שהקיוביט שלו נמצא במצב $\alpha|1\rangle+\beta|0\rangle$ ואז על בוב להעביר אותו דרך שער X כדי שמצבו יהיה $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$.

3) אם יתקבל כי אצל אליס הם במצב $|10\rangle$ אזי אליס תשלח $x=1, y=0$ וזאת כדי לסמן לבוב שהקיוביט שלו נמצא במצב $\alpha|0\rangle-\beta|1\rangle$ ואז על בוב להעביר אותו דרך שער Z כדי שמצבו יהיה $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$.

4) אם יתקבל כי אצל אליס הם במצב $|11\rangle$ אזי אליס תשלח $x=1, y=1$ וזאת כדי לסמן לבוב שהקיוביט שלו נמצא במצב $\alpha|1\rangle-\beta|0\rangle$ ואז על בוב להעביר אותו דרך שער X ואז דרך שער Z די שמצבו יהיה $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$.

ג. הערות:

1) נשים לב כי אין כאן הפרה של כלל אי השיבוט, שכן אין בידנו שני עותקים של הקיוביט- הוא רק "עבר" לבוב בצורה מיוחדת מבלי שמדדנו אותו.

2) מצב הקיוביט עבר אל בוב תוך שימוש בקו תקשורת קלאסי.

3) "שידור" ערך הקיוביט בשיטה הזו הוא חסין מציטוט- שכן מאזין עוין על הקו יוכל להסיק רק איזה אופרציה יש לבצע על הקיוביט , אך בלי להחזיק בקיוביט השזור אין לכך כל ערך.

3. שידור ערכי ביטים

א. הצגת הבעיה

אליס (A) מעוניינת לתאר לבוב מצב של 2 ביטים שברשותה, ע"י שידור קיוביט בודד (ע"ג קו תקשורת קוונטי).

ב. פתרון

בדומה לפתרון בעיית טלפורטציה, אך הפוך: נניח ואליס ובוב נפגשו בעבר, וחלקו בינם 2 קיוביטים אחרים שהיו במצב שזור, במצב בל: $|\phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$.

כעת אליס תבצע את האלגוריתם הבא:

א) אם ברצונה לשדר "00"- תשלח את הקיוביט שאצלה. אצל בוב תמצא המערכת במצב- $|\phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$.

ב) אם ברצונה לשדר "01"- תפעיל שער Z על הקיוביט שאצלה ותשלח אותו. (ע"כ אם בידה $|0\rangle$, הוא יהיה $|0\rangle$, אם בידה $|1\rangle$, הוא יהיה $-|1\rangle$). אצל בוב תמצא המערכת במצב $|\phi_-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$.

ג) אם ברצונה לשדר "10"- תפעיל שער X על הקיוביט שאצלה ותשלח אותו. (ע"כ אם בידה $|0\rangle$, הוא יהיה $|1\rangle$, אם בידה $|1\rangle$, הוא יהיה $|0\rangle$). אצל בוב תמצא המערכת במצב $|\psi_+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$.

ד) אם ברצונה לשדר "11"- תפעיל שער iY על הקיוביט שאצלה ותשלח אותו. (ע"כ אם בידה $|0\rangle$, הוא יהיה $-|1\rangle$, אם בידה $|1\rangle$, הוא יהיה $|0\rangle$). אצל בוב תמצא המערכת במצב $|\psi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$.

ע"כ על בוב למדוד את מצב המערכת שאצלו (ע"פ בסיס בל), ומתוצאות המדידה יכול להסיק על ערכי הביטים שאצל אליס על פי הטבלה להלן:

פונקציית הגל של הקיוביטים אצל בוב	הערך שאליס רצתה לשלוח
$\|\phi_+\rangle = \frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$	00
$\|\phi_-\rangle = \frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$	01
$\|\psi_+\rangle = \frac{\|01\rangle + \|10\rangle}{\sqrt{2}}$	10
$\|\psi_-\rangle = \frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$	11

ג. הערות:

1) בשום שלב אליס לא מדדה את מצב הקיוביט אצלה. היא רק ביצעה עליו מניפולציות ושלחה אותו לבוב.

2) גם כאן שידור ערך הביטים חסין מציטוט- מאזין עוין על הקו שאין לו את הקיוביט השזור לא יכול להסיק ממנו שום דבר.

פרק שמיני- אלגוריתמים מקביליים

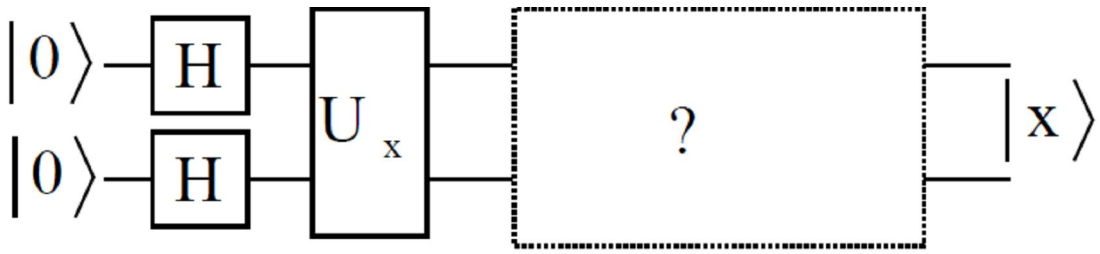
אחת התכונות המרכזיות בכלים שהוצגו עד כה היא כי הקיוביט נמצא בסופרפוזיציה של כל מצביו. בפרק זה נראה כיצד ניתן לנצל יכולת זאת לקבלת מקביליות חישובית על מנת להקטין את סיבוכיות הזמן (אך מבלי להעלות בשיעור דומה את סיבוכיות המעבדים כפי שנעשה בחישוב מקבילי קלאסי). תחילה תוסבר דרך הפתרון הקוונטית. אחר כך נראה את האלגוריתם של דויטש, שלמרות שאיננו שימושי, נוח להיעזר בו על מנת להדגים שימוש ישיר בכוח המקבילי הקוונטי. נמשיך לאלגוריתם החיפוש של גרובר שמדגים כיצד משפיעים על פונקצית הגל כך שתתכנס לערך רצוי. אלגוריתם חיפוש זה הינו בעל חשיבות רבה שכן הוא מציג פתרון למגוון רחב מאוד של בעיות בסיבוכיות זמן טובה יותר מסיבוכיות הזמן בבעיית חיפוש במחשב קלאסי, ומצביע על מגבלות המחשב הקוונטי.

1. מבוא

בכדי לרכוש אינטואיציה לגבי אלגוריתמים קוונטים, נדון בבעיה פשוטה אשר תציג כמה מהעקרונות המנחים. נניח כי נתון לנו אופרטור U_x הפועל על 2 קיוביטים, והינו בעל ההתנהגות הבאה:

$$U_x|\psi\rangle = \begin{cases} -|\psi\rangle & \psi = x \\ |\psi\rangle & \psi \neq x \end{cases}$$

אך ערכו של x איננו ידוע לנו, ואנו מעוניינים לגלותו- במילים אחרות, ידוע כי האופרטור הופך סימן רק עבור x, ועל האלגוריתם למצוא את ערכו של x. בגישה הקלאסית, מכיוון שיש כאן 4 אפשריות , היינו חושבים על אלגוריתם המפעיל את האופרטור 4 פעמים (במקרה הגרוע) ומאתרים את צמד הקיוביטים שגורם להיפוך. אך כך איננו מנצלים את הכוח הטמון במחשב הקוונטי- ניצול הסופרפוזיציה של הקיוביטים כך שבבת אחת עושים חישוב על כל הערכים האפשריים של הקיוביטים. בסעיף זה ננסה לראות כיצד נפתור את הבעיה בגישת החישוב הקוונטי: נתחיל מכך שברצוננו להפעיל האופרטור פעם אחת, גם אם הבעיה תורחב למספר רב יותר של קיוביטים- לכן כדאי שיופעל על סופר פוזיציה של כל המצבים. בנוסף נרצה שמוצא המעגל יהיה פונקצית גל עם הערך המבוקש. מעגל הגיוני יעשה שימוש בשערי הדמרד לקבלת סופרפוזיציה זו, כמתואר באיור 37.



איור 37

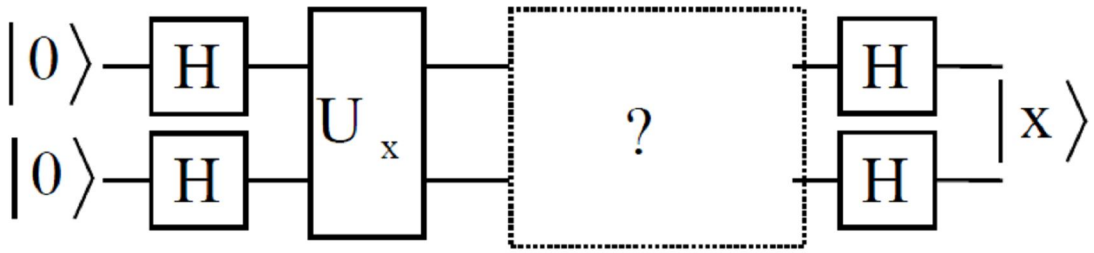
ובעצם אנו שואלים מה יגרום למעבר הבא:

$$-|00\rangle+|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle$$
$$|00\rangle-|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |01\rangle$$
$$|00\rangle+|01\rangle-|10\rangle+|11\rangle \xrightarrow{?} |10\rangle$$
$$|00\rangle+|01\rangle+|10\rangle-|11\rangle \xrightarrow{?} |11\rangle$$

מהסתכלות על מעברים אלו קשה לנחש מה יהיה המעגל שיגרום לכך. על כן נסתכל על המוצא שאנו מעוניינים להגיע אליו, ונשים לב כי לו המוצא הינו מוצא של שערי הדמרד כמתואר באיור 38, אזי ניתן לרשום:

$$-|00\rangle+|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle+|01\rangle+|10\rangle+|11\rangle \xrightarrow{H} |00\rangle$$
$$|00\rangle-|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle-|01\rangle+|10\rangle-|11\rangle \xrightarrow{H} |01\rangle$$
$$|00\rangle+|01\rangle-|10\rangle+|11\rangle \xrightarrow{?} |00\rangle+|01\rangle-|10\rangle-|11\rangle \xrightarrow{H} |10\rangle$$
$$|00\rangle+|01\rangle+|10\rangle-|11\rangle \xrightarrow{?} |00\rangle-|01\rangle-|10\rangle+|11\rangle \xrightarrow{H} |11\rangle$$

יוצא כי האופרטור אותו אנו מחפשים נראה שלא משנה מאוד את פונקצית הגל, ולכן כנראה שאנו בכיוון הנכון.

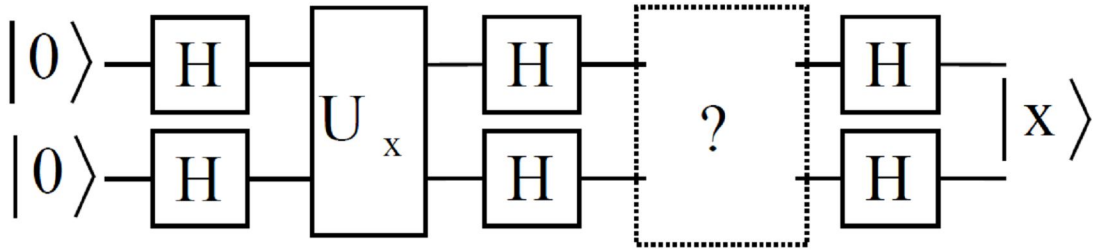


איור 38

ולכן כעת הבעיה הינה חיפוש אופרטור שממפה:

$$-|00\rangle+|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle+|01\rangle+|10\rangle+|11\rangle$$
$$|00\rangle-|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle-|01\rangle+|10\rangle-|11\rangle$$
$$|00\rangle+|01\rangle-|10\rangle+|11\rangle \xrightarrow{?} |00\rangle+|01\rangle-|10\rangle-|11\rangle$$
$$|00\rangle+|01\rangle+|10\rangle-|11\rangle \xrightarrow{?} |00\rangle-|01\rangle-|10\rangle+|11\rangle$$

צמד שערי הדמרד מייד אחרי U_x כמתואר באיור 39 יקרב אותנו עוד יותר לפתרון.

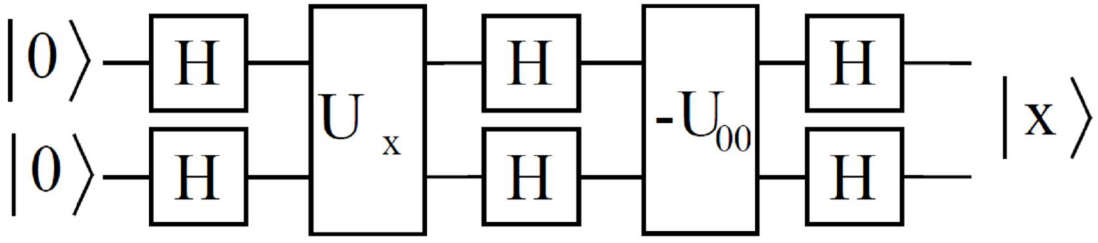


איור 39

שכן המיפוי כעת הוא:

$$|00\rangle-|01\rangle-|10\rangle-|11\rangle \xrightarrow{?} |00\rangle+|01\rangle+|10\rangle+|11\rangle$$
$$|00\rangle+|01\rangle-|10\rangle+|11\rangle \xrightarrow{?} |00\rangle-|01\rangle+|10\rangle-|11\rangle$$
$$|00\rangle-|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle+|01\rangle-|10\rangle-|11\rangle$$
$$|00\rangle+|01\rangle+|10\rangle-|11\rangle \xrightarrow{?} |00\rangle-|01\rangle-|10\rangle+|11\rangle$$

שזה שינוי סיבית הסימן של כל הקיוביטים, מלבד $|00\rangle$, או למעשה $-U_{00}$, ומכאן שהאופרטור החסר לנו הינו $-U_{00}$. לסיכום, המעגל כולו מוצג באיור 40.



איור 40

2. אופרטור U_f

ברבים מהאלגוריתמים שיוצגו בהמשך, הקלט לבעיה הינו פונקציה בוליאנית $f \to \{0,1\}$, כאשר הפונקציה הינה רב ממדית $f:\{0,1\}^n \to \{0,1\}$. עולה השאלה כיצד נרצה שהמעגל המייצג את הפונקציה ייבנה (כמובן, תוך שמירה על כך שהמעגל יהיה הפיך)? למרות שעל פניו נראה כאילו היינו רוצים שהפונקציה תסופק ע"י אופרטור U המוגדר כ: $|x_1 \ldots x_n, y\rangle \xrightarrow{U} |x_1 \ldots x_n, f(x)\rangle$

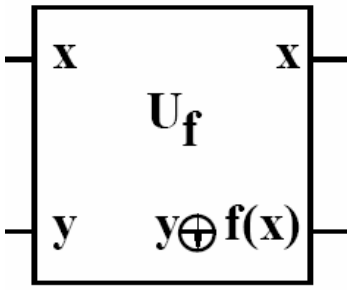
מייד מתברר כי אופרטור שכזה איננו הפיך (מה ערכו של y מהתוצאה?). מסתבר שבדרך כלל נעדיף שבמקום שהקלט לבעיה תהיה המעגל המייצג את הפונקציה f , נעדיף שהקלט לבעיה יהיה אופרטור U_f המוגדר הצורה קצת שונה מזה הטריוויאלי. תחילה נגדיר את האופרטור U_f עבור המקרה הפרטי כאשר הפונקציה חד ממדית $f:\{0,1\}\to\{0,1\}$ וננתח את משמעות האופרטור, וא"כ נרחיב למקרה הכללי- כאשר הפונקציה הינה רב ממדית $f:\{0,1\}^n\to\{0,1\}$.

1. המקרה החד מימדי:

עבור פונקציה בוליאנית $f:\{0,1\}\to\{0,1\}$ מוגדר האופרטור U_f על ידי המפה:

$$|x,y\rangle\to|x,y\oplus f(x)\rangle$$

מכיוון שההופכי לו הוא U_f אזי $|x,y\oplus f(x)\rangle\xrightarrow{U_f}|x,y\oplus f(x)\oplus f(x)\rangle=|x,y\rangle$
האופרטור יוניטרי, וע"כ ניתן לבנות כזה שער קוונטי.
נסמן שער זה כמתואר באיור 41.



איור 41

תרגיל: מה מוצא האופרטור כאשר הכניסה היא $(H|0\rangle)|0\rangle=(\frac{|0\rangle+|1\rangle}{\sqrt{2}})|0\rangle$?

פתרון:

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle=\frac{|0\rangle|0\rangle+|1\rangle|0\rangle}{\sqrt{2}}\xrightarrow{U_f}\frac{|0,0\oplus f(0)\rangle+|1,0\oplus f(1)\rangle}{\sqrt{2}}=\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$$

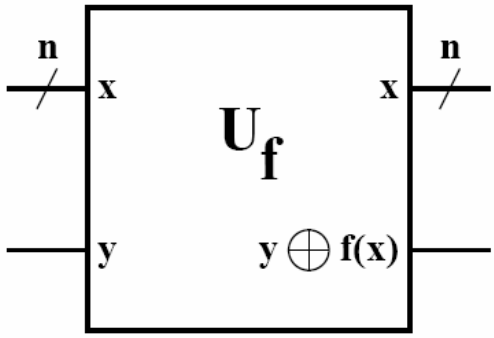
ז"א **שבצעד אחד חושבו שני ערכי הפונקציה** ומכאן חשיבות האופרטור. אך למרבה הצער לא ניתן להיעזר בתכונה זו בצורה ישירה, שכן בבואנו למדוד את הקיוביט ביציאה- הוא יקרוס לאחד המצבים ואז נקבל רק ערך אחד של הפונקציה והמקבילות תאבד.

2. המקרה הרב מימדי:

עבור המקרה הכללי, $f:\{0,1\}^n\to\{0,1\}$, האופרטור U_f מוגדר ע"י המפה:

$|x_1 \ldots x_n, y\rangle \to |x_1 \ldots x_n, y \oplus f(x_1, \ldots, x_n)\rangle$.

ומתואר כבאיור 42 :



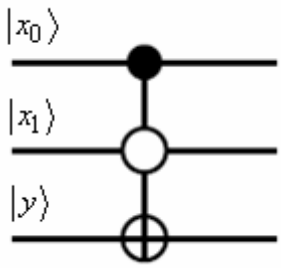
איור 42

(נשים לב כי נעשה כאן שימוש במוסכמה המציינת n קווים). גם אופרטור זה יוניטרי, שכן :

$$|x_1 \ldots x_n, y \oplus f(x)\rangle \xrightarrow{U_f} |x_1 \ldots x_n, y \oplus f(x) \oplus f(x)\rangle = |x_1 \ldots x_n, y\rangle$$

לדוגמה, עבור הפונקציה המוגדרת על התחום $\{0,1,2,3\}$ ונתונה על ידי $f(x) = \begin{cases} 0 & x \neq 2 \\ 1 & x = 2 \end{cases}$,

האופרטור U_f שלה מתואר באיור 35.



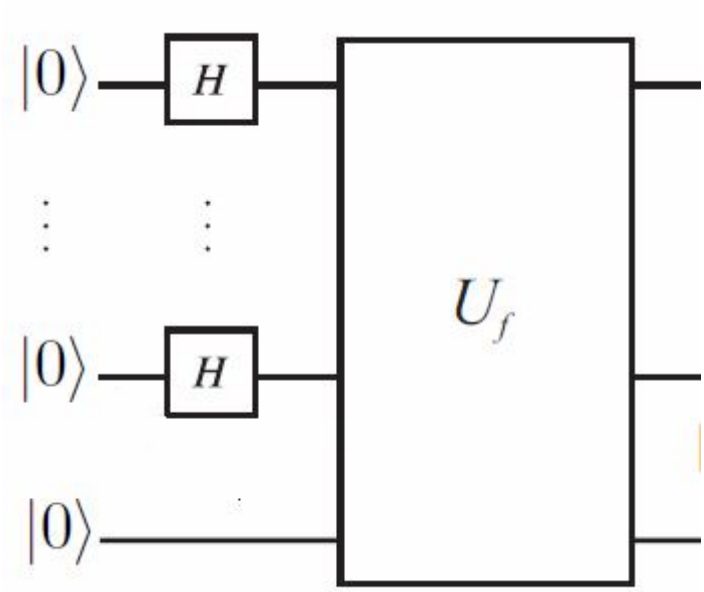
איור 43

תרגיל : הראה כי המעגל המתואר באיור 35 שקול למיפוי :

$$|3\rangle|y\rangle \to |3\rangle|y\rangle, |2\rangle|y\rangle \to |2\rangle|1 \oplus y\rangle = |2\rangle|\bar{y}\rangle, |1\rangle|y\rangle \to |1\rangle|y\rangle, |0\rangle|y\rangle \to |0\rangle|y\rangle$$

תרגיל: מה מוצא האופרטור כאשר הכניסה היא כפי שמתואר באיור 44, דהיינו

$H^{\otimes n}|0\rangle^{\otimes n}|0\rangle$?



איור 44

תשובה:

מוצא האופרטור הינו:

$$U_f((H^{\otimes n}|0\rangle^{\otimes n})|0\rangle) = U_f(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle,|0\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x,(0\oplus f(x))\rangle$$

$$= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

3. אלגוריתם של דויטש (Deutsch)

א. הצגת הבעיה

נתונה פונקציה $f:\{0,1\}^n \to \{0,1\}$ אשר ידוע כי היא או קבועה, או מאוזנת (דהיינו $f(x)=0$ עבור 2^{n-1} ערכי x, ו $f(x)=1$ עבור 2^{n-1} ערכי x). על האלגוריתם להכריע האם f היא קבועה או מאוזנת.

(תרגיל: הראה כי הפתרון הקלאסי לבעיה ידרוש $2^{n-1}+1$ שאילתות (במקרה הגרוע) בכדי להכריע.)

ב. פתרון

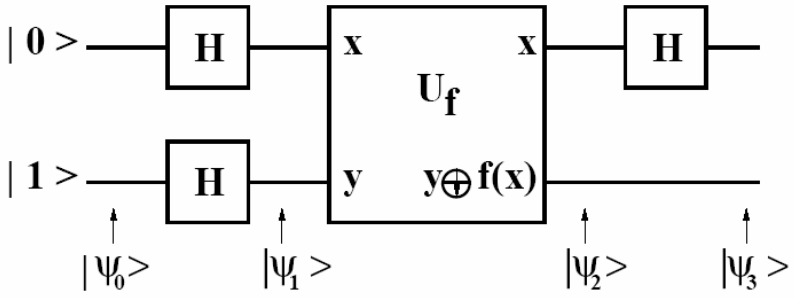
הפתרון הקוונטי ישתמש בתכונת הסופרפוזיציה כך שנקבל חישוב מקבילי בצעד אחד.

לשם הצגת הפתרון, נדון תחילה במקרה פשוט יותר: נניח כי $f:\{0,1\}\to\{0,1\}$. וא"כ נרחיב לבעיה הכללית.

1) המקרה החד מימדי

אם $f:\{0,1\}\to\{0,1\}$ אז הבעיה מצטמצמת לחישוב הערך $f(0)\oplus f(1)$. (שכן אם הפונקציה קבועה אזי $f(0)\oplus f(1)=0$, ו $f(0)\oplus f(1)=1$ כאשר היא מאוזנת). ברור כי במקרה הקלאסי ידרשו 2 צעדים לחישוב $f(0)\oplus f(1)$.

נראה כי המעגל המתואר באיור 45, מחשב את $f(0)\oplus f(1)$ בצעד אחד:



איור 45

וננתח את פונקצית הגל בכל שלב:

$$|\psi_0\rangle=|01\rangle$$

לאחר מכן:

$$|\psi_1\rangle=(H|0\rangle)(H|1\rangle)=|+\rangle|-\rangle=\frac{1}{2}\big(|0\rangle+|1\rangle\big)\big(|0\rangle-|1\rangle\big)=\frac{1}{2}\big(|0\rangle|0\rangle-|0\rangle|1\rangle+|1\rangle|0\rangle-|1\rangle|1\rangle\big)$$

מוצא השער:

$$|\psi_2\rangle=\frac{1}{2}\big(|0\rangle\big(|f(0)\oplus 0\rangle-|f(0)\oplus 1\rangle\big)+|1\rangle\big(|f(1)\oplus 0\rangle-|f(1)\oplus 1\rangle\big)\big)$$

ייתכנו 4 מקרים:

א) $f(0)=f(1)=0$:

$$|\psi_2\rangle=\frac{1}{2}\big(|0\rangle\big(|0\rangle-|1\rangle\big)+|1\rangle\big(|0\rangle-|1\rangle\big)\big)=\frac{1}{2}\big(|0\rangle+|1\rangle\big)\big(|0\rangle-|1\rangle\big)$$

ב) $f(0)=f(1)=1$:

$$|\psi_2\rangle=\frac{1}{2}\big(|0\rangle\big(|1\rangle-|0\rangle\big)+|1\rangle\big(|1\rangle-|0\rangle\big)\big)=\frac{1}{2}\big(|0\rangle+|1\rangle\big)\big(|1\rangle-|0\rangle\big)=-\frac{1}{2}\big(|0\rangle+|1\rangle\big)\big(|0\rangle-|1\rangle\big)$$

ג) $f(0)=1,\ f(1)=0$

$$|\psi_2\rangle = \frac{1}{2}\left(|0\rangle\left(|1\rangle - |0\rangle\right) + |1\rangle\left(|0\rangle - |1\rangle\right)\right) = \frac{1}{2}\left(|0\rangle\left(|1\rangle - |0\rangle\right) - |1\rangle\left(|1\rangle - |0\rangle\right)\right) = \frac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|1\rangle - |0\rangle\right)$$
$$= -\frac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

ד) $f(0)=0,\ f(1)=1$

$$|\psi_2\rangle = \frac{1}{2}\left(|0\rangle\left(|0\rangle - |1\rangle\right) + |1\rangle\left(|1\rangle - |0\rangle\right)\right) = \frac{1}{2}\left(|0\rangle\left(|0\rangle - |1\rangle\right) - |1\rangle\left(|0\rangle - |1\rangle\right)\right) = \frac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

לסיכום, ניתן לרשום:

$$|\psi_2\rangle = \begin{cases} \pm\frac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) & f(0) = f(1) \\ \pm\frac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right) & f(0) \neq f(1) \end{cases}$$

מכיוון ש:

$$H\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
$$H\left(\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

אזי לאחר השער הרביעי:

$$|\psi_3\rangle = \begin{cases} \pm\frac{1}{2}\left(|0\rangle\right)\left(|0\rangle - |1\rangle\right) & f(0) = f(1) \\ \pm\frac{1}{2}\left(|1\rangle\right)\left(|0\rangle - |1\rangle\right) & f(0) \neq f(1) \end{cases}$$

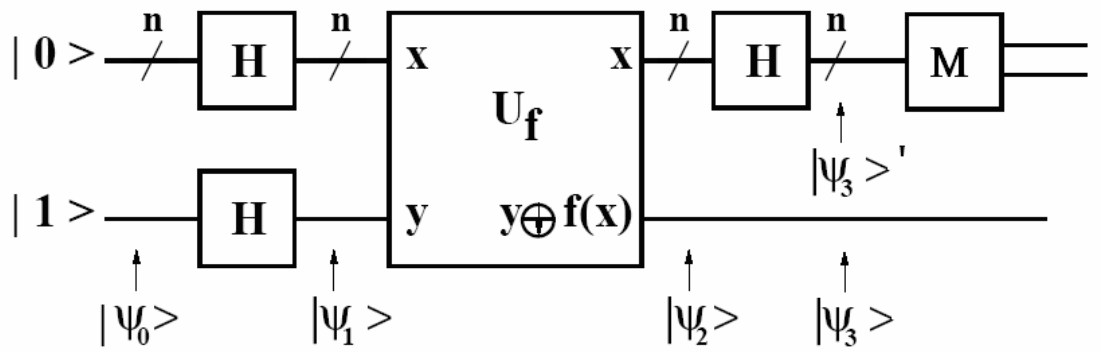
מכיוון ש $f(0) \oplus f(1) = 0$ כאשר $f(0) = f(1)$, ו $f(0) \oplus f(1) = 1$ כאשר $f(0) \neq f(1)$, ניתן לרשום:

$$|\psi_3\rangle = \pm\frac{1}{\sqrt{2}}\left(|f(0) \oplus f(1)\rangle\right)\left(|0\rangle - |1\rangle\right)$$

ז״א שאם נמדוד את מוצא המערכת ביחס ל$\left(|0\rangle - |1\rangle\right)$ נקבל את $f(0) \oplus f(1)$ בצעד אחד!. אם נקבל 0 אזי הפונקציה קבועה, (שכן אם $f(0) = f(1)$ אז $f(0) \oplus f(1) = 0$) ואם נקבל 1 אזי הפונקציה מאוזנת (שכן אם $f(0) \neq f(1)$ אז $f(0) \oplus f(1) = 1$).

2) המקרה הכללי:

עבור $f:\{0,1\}^n \to \{0,1\}$, ננתח את המעגל המתואר באיור 46 (הדומה למקרה החד מימדי):



איור 46

בכניסה:

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

אחרי שערי הדמרד:

$$|\psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n} H|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle H|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)=$$

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|0\rangle-|1\rangle\right)$$

לאחר האופרטור:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|0\oplus f(x)\rangle-|1\oplus f(x)\rangle\right)=\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|f(x)\rangle-|1\oplus f(x)\rangle\right)$$

נתבונן על הערך בתוך הסכום. ייתכנו 2 מקרים:

א. f(x)=0

$$|x\rangle\left(|f(x)\rangle-|1\oplus f(x)\rangle\right)=|x\rangle\left(|0\rangle-|1\rangle\right)=(-1)^0\left(|x\rangle\left(|0\rangle-|1\rangle\right)\right)=(-1)^{f(x)}\left(|x\rangle\left(|0\rangle-|1\rangle\right)\right)$$

ב. f(x)=1

$$|x\rangle\left(|f(x)\rangle-|1\oplus f(x)\rangle\right)=|x\rangle\left(|1\rangle-|0\rangle\right)=(-1)^1\left(|x\rangle\left(|0\rangle-|1\rangle\right)\right)=(-1)^{f(x)}\left(|x\rangle\left(|0\rangle-|1\rangle\right)\right)$$

על כן:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\left(|0\rangle-|1\rangle\right)$$

בכדי לחשב את מוצא המעגל $|\psi_3\rangle'$, נבדוק תחילה מה ערכו של $H|x\rangle$ עבור שני מקרים-

א. x=0

$$H|0\rangle=\frac{1}{\sqrt{2}}\sum_{z=0}^{1}|z\rangle=\frac{1}{\sqrt{2}}\sum_{z=0}^{1}(-1)^{0}|z\rangle=\frac{1}{\sqrt{2}}\sum_{z=0}^{1}(-1)^{xz}|z\rangle$$

ב. x=1

$$H|1\rangle=\frac{1}{\sqrt{2}}\Big(|0\rangle-|1\rangle\Big)=\frac{1}{\sqrt{2}}\Big((-1)^{1*0}|0\rangle+(-1)^{1*1}|1\rangle\Big)=\frac{1}{\sqrt{2}}\sum_{z=0}^{1}(-1)^{xz}|z\rangle$$

ומכאן:

$$H|x\rangle=\frac{1}{\sqrt{2}}\sum_{z=0}^{1}(-1)^{xz}|z\rangle$$

ועל כן:

$$|\psi_3\rangle'=\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle=\frac{1}{2^n}\sum_{y=0}^{2^n-1}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}\right]|y\rangle$$

כאשר $x\cdot y=x_0y_0\oplus x_1y_1\oplus\ldots\oplus x_{n-1}y_{n-1}$.

את פונקצית גל זו ניתן לרשום גם כ:

$$|\psi_3\rangle'=|0\rangle^{\otimes n}=\frac{1}{2^n}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot 0}\right]|0\rangle^{\otimes n}+\frac{1}{2^n}\sum_{y=1}^{2^n-1}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}\right]|y\rangle=$$

$$\frac{1}{2^n}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right]|0\rangle^{\otimes n}+\frac{1}{2^n}\sum_{y=1}^{2^n-1}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}\right]|y\rangle$$

(רשמנו $|0\rangle^{\otimes n}$ ולא $|0\rangle$ כדי להדגיש שהווקטור הפורש הראשון הינו בעל מימד 2^n ולא מימד 2).

לכן, ההסתברות למדידת $|0\rangle^{\otimes n}$ הינה הנורמה בריבוע של המקדם של $|0\rangle^{\otimes n}$ כלומר

$\left|\frac{1}{2^n}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right]\right|^2$. כעת ניתן לבצע את ההבחנה הבאה:

א) אם f(x) מאוזנת, אזי הסכימה תתאפס - כי חצי מהאיברים הינם האיברים $(-1)^{f(x)}=(-1)^0=1$ וחצי השני הינם $(-1)^1=-1$, לכן הם יבטלו זה את זה.

ב) אם f(x) קבועה אזי ריבוע הסכימה יהיה 1. (או

$$\left|\frac{1}{2^n}\left[\sum_{x=0}^{2^n-1}(-1)^0\right]\right|^2=\left|\frac{1}{2^n}\left[\sum_{x=0}^{2^n-1}1\right]\right|^2=1$$, או

$$\left|\frac{1}{2^n}\left[\sum_{x=0}^{2^n-1}(-1)^1\right]\right|^2=\left|\frac{1}{2^n}\left[\sum_{x=0}^{2^n-1}(-1)\right]\right|^2=1$$).

מכאן שיש כעת למדוד האם כל n האיברים הראשונים במוצא הם $|0\rangle^{\otimes n}$. אם כן אזי f(x) קבועה. אחרת, f(x) מאוזנת.

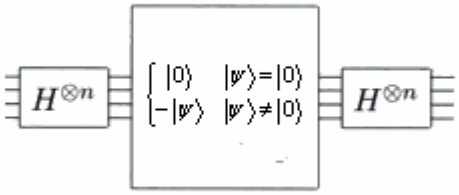
ד. הערות:

למרות שהבעיה איננה בעיה נפוצה ובעלת חשיבות רבה, היא מציגה כיצד חישוב קוונטי יכול לבצע חישוב מקבילי ללא מגבלות שמכונת טיורינג הקלאסית כופה ובעצם לספק אינדיקציה כי כוח החישוב של מחשב קוונטי עולה על מקבילו הסטנדרטי.

בנוסף, בסעיף הבא נראה כיצד מעגל זה משמש בסיס לאלגוריתם החיפוש של גרובר.

4. אופרטור Mean Inversion

בבעיית החיפוש של גרובר, אשר תוצג בסעיף הבא, נעשה שימוש באופרטור חשוב נוסף, אופרטור Mean Inversion. האופרטור המתואר ע"י איור 47 הינו שרשור של 3 אופרטורים: אופרטור הדמרד, אחריו אופרטור שער שינוי פאזה מותנה (שנידון כבר בפרק 4), ואחריו שוב הדמרד.



איור 47

ננתח את פעולת האופרטור המתואר באיור 47. פעולת האופרטור הינה $H^{\otimes n}(2|0\rangle\langle 0|-I)H^{\otimes n}$.

או בצורה אחרת:

$$H^{\otimes n}(2|0\rangle\langle 0|-I)H^{\otimes n}=\left(2H^{\otimes n}|0\rangle\langle 0|-H^{\otimes n}\right)H^{\otimes n}=$$

$$2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n}-H^{\otimes n}H^{\otimes n}=2\left(\begin{pmatrix}\frac{1}{\sqrt{N}}\\ \vdots \\ \frac{1}{\sqrt{N}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{N}} & \cdots & \frac{1}{\sqrt{N}}\end{pmatrix}\right)-I$$

נסמן $|\psi\rangle=\begin{pmatrix}\frac{1}{\sqrt{N}}\\ \vdots \\ \frac{1}{\sqrt{N}}\end{pmatrix}$, ואז פעולת האופרטור מתוארת ע"י $2|\psi\rangle\langle\psi|-I$.

נפתח ביטוי זה בכדי לעמוד על צורת המטריצה:

$$2|\psi\rangle\langle\psi|-I=2\left(\begin{pmatrix}\frac{1}{\sqrt{N}}\\ \vdots \\ \frac{1}{\sqrt{N}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{N}} & \cdots & \frac{1}{\sqrt{N}}\end{pmatrix}\right)-I$$

$$= \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix} - \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} =$$

$$\begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{pmatrix}$$

תרגיל: הראה כי הפעלת האופרטור $(2|\psi\rangle\langle\psi|-I)$ על פונקציית גל הנתונה ע"י

$$|\sigma\rangle = \sum_{x=0}^{N-1} v_x |x\rangle$$

ייתן:

$$2|\psi\rangle\langle\psi|-I)|\sigma\rangle = \sum_{x=0}^{N-1}(-v_x + 2\bar{v}|x\rangle)$$

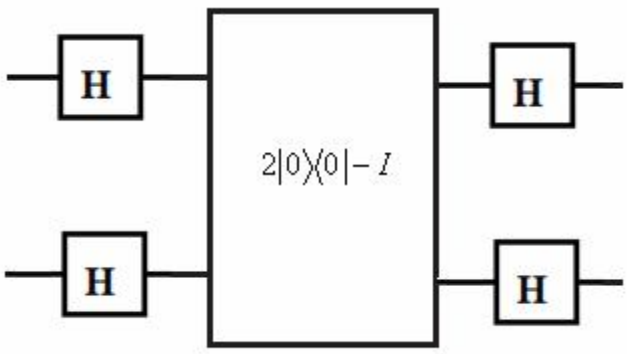
כאשר $\bar{v}$ הינו ממוצע אלגברי של המקדמים v_i .

פתרון:

$$(2|\psi\rangle\langle\psi|-I)(\sum_{x=0}^{N-1} v_i|i\rangle) = \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{pmatrix} - \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{pmatrix} =$$

$$\begin{pmatrix} 2\bar{v} \\ 2\bar{v} \\ \vdots \\ 2\bar{v} \end{pmatrix} - \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{pmatrix} = \sum_{x=0}^{N-1}(-v_x + 2\bar{v}|x\rangle)$$

לדוגמה, עבור 2 קיוביטים, האופרטור מתואר על ידי איור 48.



איור 48

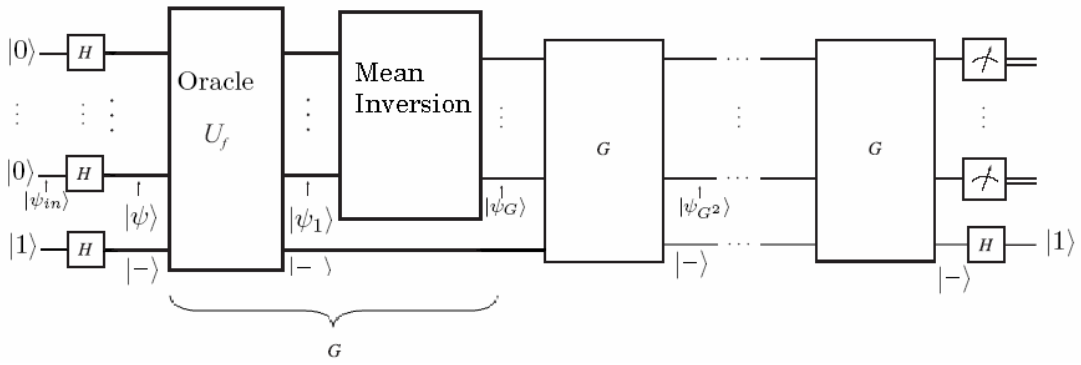
5. בעיית החיפוש- אלגוריתם של גרובר (Grover)

א. הצגת הבעיה

נתון מרחב חיפוש המכיל $N = 2^n$ איברים לא מסודרים. כמו-כן נתונה פונקציה $f : \{0,1\}^n \to \{0,1\}$ המקבלת את מיקום האיבר ומוצאה 0 או 1 . יהי M, $M<<N$ מספר האיברים שעבורם $f(x) = 1$. מטרת האלגוריתם למצוא את M מיקומי האיברים שעבורם $f(x) = 1$. לפתרון הקלאסי לבעיה ידרשו $\Omega(N)$ צעדים במכונת טיורינג.

ב. פתרון

הפתרון הקוונטי ישתמש בתכונת הסופרפוזיציה כך שנקבל את <u>אחד</u> הפתרונות ב $O(\sqrt{N})$ צעדים ומתואר באיור 49. האלגוריתם עושה שימוש ברגיסטר קוונטי בן n קיוביטים וכן בקיוביט נוסף (קיוביט עזר).



איור 49

המעגל המתואר באיור הינו מורכב מעט, על כן תחילה המעגל יתואר בצורה כללית, ואחר כך נרחיב בצורה מפורטת בכל צעד.

<u>תיאור כללי:</u>

בתחילה נבדקים כל האיברים ביחד למול הפונקציה (בדומה לאלגוריתם של דויטש) ז"א ששוב משתמשים ברעיון החישוב המקבילי. נראה בהמשך שכתוצאה מכך בפונקצית הגל $|\psi_1\rangle$ יש אפקט מעניין- המיקומים שאותם מחפשים מופיעים בפונקצית הגל עם אמפליטודה שונה מאשר שאר המיקומים- כאילו פונקצית הגל מכילה "סימונים" על המקומות אותם אנו מחפשים. א"כ מפעילים אופרטור (Mean Inversion) – נראה בהמשך שכתוצאה מכך ב $|\psi_G\rangle$ האמפליטודות ה"מסומנות" מתעצמות על חשבון שאר האמפליטודות. הפעלת אופרטורים אלו (דהיינו שערי G) $\sqrt{n}$ פעמים, מעצימות עוד יותר את האמפליטודות הללו כך שב $\left|\psi_{G^{\sqrt{N}}}\right\rangle$ יש רק את האיברים שמחפשים. רעיון זה של העצמת האמפליטודה הרצויה אף הוא חוזר באלגוריתמים קוונטים רבים.

<u>תיאור מפורט:</u>

ננתח את פונקצית הגל של n הביטים העליונים בכל שלב:

1) הכניסה למעגל:

$$|\psi_{in}\rangle = |0\rangle^{\otimes n}$$

2) לאחר שערי H:

$$|\psi\rangle = H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle$$

בכדי להמשיך ולהעמיק בפתרון, יהיה נוח לעבור מהבסיס הסטנדרטי לבסיס אחר, המוגדר ע"י 2 וקטורים- וקטור הפתרונות ווקטור הלא פתרונות.

על פי הגדרת הבעיה יש M פתרונות, ונוכל לרשום את פונקצית הגל כ:

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x\in M}|x\rangle + \frac{1}{\sqrt{N}}\sum_{x\notin M}|x\rangle = \frac{\sqrt{N-M}}{\sqrt{N}}\underbrace{\frac{1}{\sqrt{N-M}}\sum_{x\notin M}|x\rangle}_{|\alpha\rangle} + \frac{\sqrt{M}}{\sqrt{N}}\underbrace{\frac{1}{\sqrt{M}}\sum_{x\in M}|x\rangle}_{|\beta\rangle} =$$

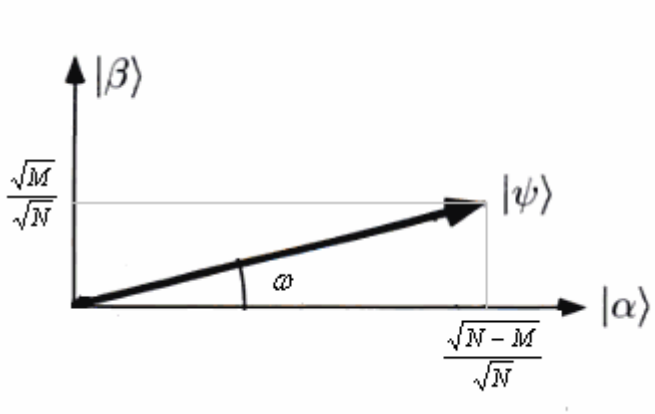
$$\frac{\sqrt{N-M}}{\sqrt{N}}|\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}|\beta\rangle$$

או במילים: $|\psi\rangle$ (שהיא $\frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle$) נפרשת ע"י וקטור הפתרונות $|\beta\rangle$ ווקטור הלא פתרונות $|\alpha\rangle$.

ממשוואה זו, עולה כי ניתן לרשום את פונקצית הגל בבסיס $|\alpha\rangle, |\beta\rangle$ באופן הבא:

$$|\psi\rangle = \begin{pmatrix} \frac{\sqrt{N-M}}{\sqrt{N}} \\ \frac{\sqrt{M}}{\sqrt{N}} \end{pmatrix}$$

איור 50 מתאר זאת בצורה גרפית.



איור 50

כאשר הזווית ω נתונה ע"י:

$$\cos\omega = \frac{\sqrt{N-M}}{\sqrt{N}}$$

נסמן $\omega = \frac{\theta}{2}$, ומכאן:

$$|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$$

$$\cos\frac{\theta}{2} = \frac{\sqrt{(N-M)}}{\sqrt{N}}$$

$$\sin\frac{\theta}{2} = \frac{\sqrt{M}}{\sqrt{N}}$$

נעזר בזהות $\cos 2\alpha = \cos^2\alpha - \sin^2\alpha$ בכדי לחשב את $\cos\theta$:

$$\cos\theta = \cos 2\left(\frac{\theta}{2}\right) = \cos^2\left(\frac{\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) = \left(\frac{\sqrt{(N-M)}}{\sqrt{N}}\right)^2 - \left(\frac{\sqrt{M}}{\sqrt{N}}\right)^2$$

$$= \frac{N-M}{N} - \frac{M}{N} = \frac{N-2M}{N}$$

נעזר בזהות $1=\cos^2\alpha+\sin^2\alpha$ בכדי לחשב את $\sin\theta$ (בהנחה ש θ ברביע הראשון):

$$\sin\theta=\sqrt{1-\cos^2\theta}=\sqrt{1-\frac{(N-2M)^2}{N^2}}=\sqrt{\frac{N^2-N^2+4NM-M^2}{N^2}}$$

$$=\sqrt{\frac{4NM-M^2}{N^2}}=\sqrt{\frac{4M(N-M)}{N^2}}=\frac{2\sqrt{M(N-M)}}{N}$$

3) הפעלת U_f על $|\psi\rangle$

לאחר שער U_f, פונקצית הגל של כל n+1 הקיוביטים, הינם כפי שכבר חישבנו כשניתחנו את האופרטור U_f:

$$|\psi_1\rangle|-\rangle=\frac{1}{\sqrt{2^{n+1}}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\Big(|x\rangle\big(|0\rangle-|1\rangle\big)\Big)$$

או ברישום אחר:

$$|\psi_1\rangle|-\rangle=\frac{1}{\sqrt{2^{n}}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle|-\rangle$$

יש שני דברים שיש לשים לב עליהם:

א) לאחר אופרטור U_f הקיוביט השני שמר על ערכו ונשאר $|-\rangle$,כך שגם בשער G הבא הכניסה של הביט השני לאופרטור U_f היא $|-\rangle$- ולמעשה בכל הקו הערך הוא זהה ונשאר קבוע, לכן נתעלם ממנו ובהמשך נתייחס לפונקציות גל ללא קיוביט זה.

באופן כללי , אם בכניסה לשער G הk י פונקצית הגל היא $|\psi\rangle|-\rangle=\sum_{x\in\{0,1\}^n}v_i|x\rangle|-\rangle$,

אז לאחר הפעלת U_f נקבל את פונקצית הגל: $\left|\psi_1^k\right\rangle|-\rangle=\sum_{x\in\{0,1\}^n}(-1)^{f(x)}v_i|x\rangle|-\rangle$.

ב) בקיוביט הראשון- כל האמפליטודות של הפתרונות הן עם סימן שלילי (שכן עבורם $(-1)^{f(x)}=-1^1=-1$) וכל אלו שאינם של הפתרונות שומרות על סימנם (שכן עבורם $(-1)^{f(x)}=-1^0=1$), לכן את פונקצית הגל $|\psi_1\rangle$ ניתן לרשום גם כ:

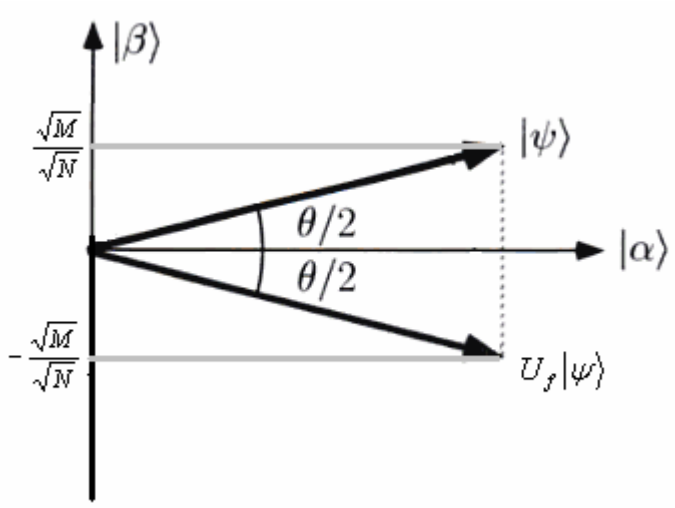
$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{x\notin M}|x\rangle - \sum_{x\in M}|x\rangle\right) = \frac{1}{\sqrt{N}}\left(\sum_{x\notin M}|x\rangle - \sum_{x\in M}|x\rangle + \sum_{x\in M}|x\rangle - \sum_{x\in M}|x\rangle\right)$$

$$= \frac{1}{\sqrt{N}}\left(\left(\sum_{x\in M}|x\rangle + \sum_{x\notin M}|x\rangle\right) - 2\sum_{x\in M}|x\rangle\right) = \frac{1}{\sqrt{N}}\left(\sum_{x\in M}|x\rangle + \sum_{x\notin M}|x\rangle\right) - \frac{2}{\sqrt{N}}\sum_{x\in M}|x\rangle$$

$$= |\psi\rangle - \frac{2\sqrt{M}}{\sqrt{N}}|\beta\rangle = \frac{\sqrt{N-M}}{\sqrt{N}}|\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}|\beta\rangle - \frac{2\sqrt{M}}{\sqrt{N}}|\beta\rangle$$

$$= \frac{\sqrt{N-M}}{\sqrt{N}}|\alpha\rangle - \frac{\sqrt{M}}{\sqrt{N}}|\beta\rangle$$

איור 51 מציג תיאור גראפי לפעולה.



איור 51

מבחינה גרפית האופרטור שקול לשיקוף סביב ציר $|\alpha\rangle$ או לסיבוב של $\frac{\theta}{2}$ לכיוון $-|\beta\rangle$.

ניתן לכתוב את האופרטור בבסיס $|\alpha\rangle, |\beta\rangle$ באופן הבא:

$$U_f = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

שכן:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \frac{\sqrt{N-M}}{\sqrt{N}} \\ \frac{\sqrt{M}}{\sqrt{N}} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{N-M}}{\sqrt{N}} \\ -\frac{\sqrt{M}}{\sqrt{N}} \end{pmatrix}$$

4) הפעלת האופרטור Mean Inversion:

כבר עמדנו על כך שאת האופרטור אפשר לכתוב כ $2|\psi\rangle\langle\psi|-I$ (כאשר $|\psi\rangle$ הינה סופר פוזיציה של כל המצבים באופן שווה , כפי שהמצב כאן) .נתאר את האופרטור בבסיס $|\alpha\rangle$, $|\beta\rangle$:

$$2|\psi\rangle\langle\psi|-I=2\begin{pmatrix}\frac{\sqrt{N-M}}{\sqrt{N}}\\ \frac{\sqrt{M}}{\sqrt{N}}\end{pmatrix}\begin{pmatrix}\frac{\sqrt{N-M}}{\sqrt{N}} & \frac{\sqrt{M}}{\sqrt{N}}\end{pmatrix}-I$$

$$=2\begin{pmatrix}\frac{N-M}{N} & \frac{\sqrt{(N-M)M}}{N}\\ \frac{\sqrt{(N-M)M}}{N} & \frac{M}{N}\end{pmatrix}-I=\begin{pmatrix}\frac{2N-2M}{N}-1 & \frac{2\sqrt{(N-M)M}}{N}\\ \frac{2\sqrt{(N-M)M}}{N} & \frac{2M}{N}-1\end{pmatrix}=$$

$$\begin{pmatrix}\frac{-2M+N}{N} & \frac{2\sqrt{(N-M)M}}{N}\\ \frac{2\sqrt{(N-M)M}}{N} & \frac{2M-N}{N}\end{pmatrix}=\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}$$

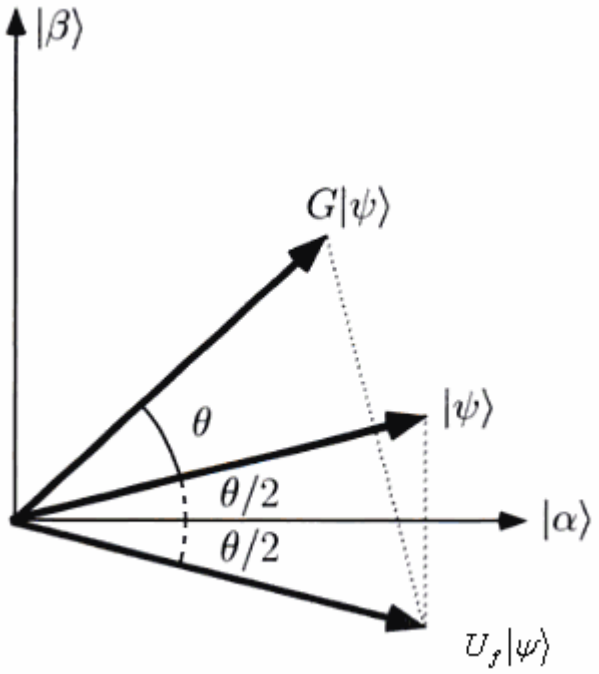
5) חלק שלישי- איור 38: הפעלת G שוב ושוב על $|\psi_{G^i}\rangle$.

סך הכול, את אופרטור G בבסיס $|\alpha\rangle$, $|\beta\rangle$ נרשום:

$$G=\left(2|\psi\rangle\langle\psi|-I\right)U_f=\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$$

ז״א בבסיס זה אופרטור G הינו סיבוב של θ לכיוון $|\beta\rangle$.

למעשה פעולת האופרטור G הינה בהתחלה סיבוב של $\frac{\theta}{2}$ לכיוון $-|\beta\rangle$,ואחר כך $\frac{3\theta}{2}$ לכיוון $|\beta\rangle$, כך שסך הכל מתקבל סיבוב של θ לכיוון $|\beta\rangle$. איור 52 מתאר זאת בצורה גרפית.



איור 52

לכן, לאחר הפעלת שער G בפעם הראשונה, הסיכוי למדידת הערך הרצוי- $|\beta\rangle$, עולה. אך עדיין איננו גבוה מספיק, שכן הזווית קטנה מאוד.

כעת למעשה מסובבים שוב ושוב בזווית θ לכיוון $|\beta\rangle$, עד שפונקצית הגל מספיק קרובה ל$|\beta\rangle$ כך שאם נמדוד את פונקצית הגל היא תקרוס ל$|\beta\rangle$ בסבירות גבוהה מאוד.

כמה פעמים עלינו לסובב את פונקצית הגל המקורית עד שתגיע מספיק קרוב ל $|\beta\rangle$?

בכדי לענות על כך, נתבונן בפונקצית הגל המקורית:

$$|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$$

ולאחר הפעלת אופרטור G :

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$$

אם על פונקצית גל זו נפעיל שוב את G נקבל עוד סיבוב בזוית θ או באופן כללי:

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

נרצה לאפס את המקדם של $|\alpha\rangle$:

$$\cos\left(\frac{2k+1}{2}\theta\right)=0$$

$$\cos\left(k\theta+\frac{\theta}{2}\right)=0$$

$$\cos(k\theta)\cos\left(\frac{\theta}{2}\right)-\sin(k\theta)\sin\left(\frac{\theta}{2}\right)=0$$

$$\frac{\sqrt{N-M}}{\sqrt{N}}\cos(k\theta)-\frac{\sqrt{M}}{\sqrt{N}}\sin(k\theta)=0$$

$$\sqrt{N-M}\cos(k\theta)=\sqrt{M}\sin(k\theta)$$

$$\tan(k\theta)=\frac{\sqrt{N-M}}{\sqrt{M}}=\sqrt{\frac{N}{M}-1}$$

מכיוון ש $\tan^2\theta+1=(\cos^{-1}\theta)^2$:

$$\left(\cos^{-1}(k\theta)\right)^2=\frac{N}{M}-1+1$$

$$\cos^{-1}(k\theta)=\sqrt{\frac{N}{M}}$$

שממנה עולה כי צריך לסובב את פונקצית הגל $\cos^{-1}(\frac{\sqrt{M}}{\sqrt{N}})$ רדיאנים כדי שערכה יהיה $|\beta\rangle$. באם בכל הפעלה של G אנו מסובבים את פונקצית הגל בזווית θ, אזי נזדקק ל:

$$\left\lceil\frac{\cos^{-1}(\frac{\sqrt{M}}{\sqrt{N}})}{\theta}\right\rceil$$

סיבובים בכדי להגיע ליעדנו. מכיוון שהזווית הינה קטנה מ $\frac{\pi}{2}$ (ההנחה של M<<N) אזי מספר הסיבובים הינו: $\left\lceil\frac{\pi}{2\theta}\right\rceil$. מצד שני $\sin\frac{\theta}{2}=\frac{\sqrt{M}}{\sqrt{N}}\approx\frac{\theta}{2}$, על כן יש לבצע $\left\lceil\frac{\pi}{2\theta}\right\rceil=\left\lceil\frac{\pi\sqrt{N}}{4\sqrt{M}}\right\rceil$ סיבובים.

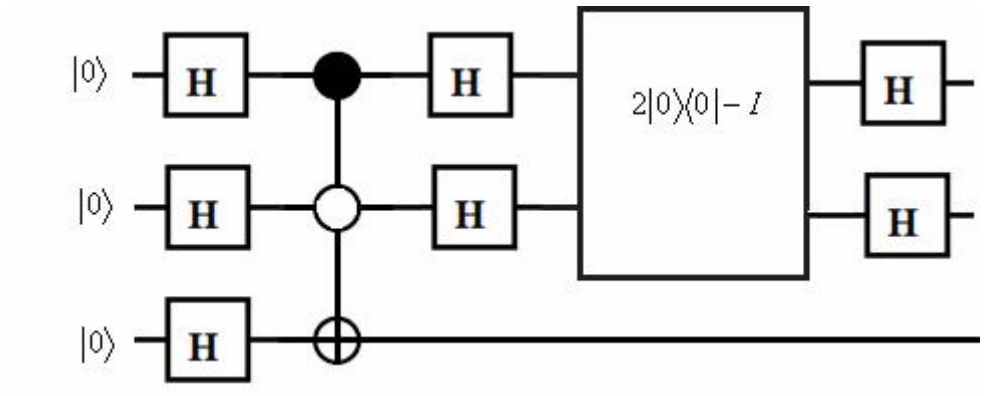
<u>הערה</u>: אם נבצע יותר סיבובים לא נשפר את התוצאה- אלא להפך נתרחק ממנה (שכן נתרחק מציר $|\beta\rangle$). על כן ישנה חשיבות שהזווית θ תהיה קטנה ואז פונקצית הגל "תתיישב" על $|\beta\rangle$. הבטחת זווית קטנה היא למעשה ההנחה שM<<N.

6) מדידה: לאחר $\left\lfloor\frac{\pi\sqrt{N}}{4\sqrt{M}}\right\rfloor$ סיבובים, פונקצית הגל בכניסה למכשיר המדידה היא $|\beta\rangle$, כלומר לאחר המדידה פונקצית הגל תקרוס לאחד מהפתרונות, ובמוצא יימדד

אינדקס אחד שהינו פתרון לבעיה- דהיינו מציאת פתרון אחד תדרוש $O(\sqrt{N})$ צעדים. באם ברצוננו למצוא את כל שאר M-1 הפתרונות, נסמן את הפתרון שמצאנו כ x_0 ונפעיל את האלגוריתם בשנית, אך על הפונקציה: $f'(x)=\begin{cases} f(x) & x\neq x_0 \\ 0 & x=x_0 \end{cases}$.

כך נמצא את הפתרון הבא x_1 (לצורך כך נפעיל את האופרטור $\left\lfloor \frac{\pi\sqrt{N}}{4\sqrt{M-1}} \right\rfloor$ פעמים), וחוזר חלילה M פעמים. כמה פעמים מופעל האופרטור? בפעם הראשונה $\left\lfloor \frac{\pi\sqrt{N}}{4\sqrt{M}} \right\rfloor$, בפעם השנייה $\left\lfloor \frac{\pi\sqrt{N}}{4\sqrt{M-1}} \right\rfloor$, בפעם השלישית $\left\lfloor \frac{\pi\sqrt{N}}{4\sqrt{M-2}} \right\rfloor$ וכולי. אם כך, בכדי למצוא את כל M הפתרונות האופרטור מופעל $\sum_{i=M}^{1}\left\lfloor \frac{\pi\sqrt{N}}{4\sqrt{i}} \right\rfloor$ פעמים. סכום זה חסום ע"י $O(\sqrt{NM})<\sum_{i=1}^{M}\frac{\pi\sqrt{N}}{4\sqrt{i}}<\int_{1}^{M}\frac{\pi\sqrt{N}}{4\sqrt{i}}di=\frac{\pi\sqrt{N}}{2}\left(\sqrt{M}-\sqrt{1}\right)$ - ומכיוון שM<<N, אזי לאחר $O\left(\sqrt{N}\right)$ יתקבלו כל M הפתרונות של הבעיה.

לדוגמה, עבור הפונקציה המוגדרת על ידי האופרטור U_f מאיור 43,(N=4) מעגל החיפוש מתואר על ידי איור 53, שכן ידוע לנו כי M=1, ולכן יש להפעיל את אופרטור G פעם אחת ($\left\lfloor \frac{\pi\sqrt{4}}{4\sqrt{1}} \right\rfloor=1$).



איור 53

במקרה כזה הזוית למעשה הינה $\sin\frac{\theta}{2}=\frac{\sqrt{M}}{\sqrt{N}}=\frac{1}{2}\Rightarrow\theta=60^o$, ז"א שהזוית בין $|\psi\rangle$ ל $|\alpha\rangle$ הינה $\frac{\theta}{2}=30^o$, ולאחר הפעלת איטרציה אחת, הזוית הינה $30^o+\theta=90^o$, כלומר- פונקצית הגל כעת היא $|\beta\rangle$, זאת אומרת שנמצא את הפתרון בסבירות 1. לו נפעיל שוב את G נקלקל את התוצאה שכן פונקצית הגל תהיה בזוית $30^o+\theta=150^o$.

ה. סיבוכיות האלגוריתם-

סיבוכיות הפעלת שער G קוונטי הינו $O(1)$. עבור מציאת אינדקס אחד השער מופעל $\sqrt{N}$ פעמים סיבוכיות האלגוריתם הינה $O(\sqrt{N})$. עבור מציאת כל M הפתרונות סיבוכיות האלגוריתם הינה $O(\sqrt{MN})$.

ו. חסם תחתון

בכדי לאמוד את החסם התחתון לבעיית החיפוש על ידי מחשב קוונטי, ישנה הוכחה כללית יותר הדנה בהאצה שניתן לקבל ע"י חישוב קוונטי על פני החישוב הקלאסי. ההוכחה מתייחסת למחשב הקוונטי כאל קופסה שחורה (black box), אשר ניתן לפנות אליה בשאילתא ומתקבלת תשובה (בפרק זמן קבוע) האם השאילתא מספקת את הפתרון אם לאו. ההנחה היא כי הקופסה השחורה בנויה מאופרטורים יוניטרים (=מחשב קוונטי) , וההוכחה מדמה פתרון בשיטת brute force - דהינו סריקה על כל האפשרויות עד אשר מוצאים פתרון.
מן ההוכחה עולה כי בפתרון בעיות בשיטת brute force החסם התחתון מעל מחשב קוונטי הינו $\Omega(\sqrt{N})$ (בהשוואה לקלאסי ששם החסם התחתון הוא $\Omega(N)$) .

מכאן עולות שתי מסקנות:
האחת- האלגוריתם של גרובר הוא אופטימאלי ולא ניתן למצוא אלגוריתם יעיל ממנו. (שכן האלגוריתם של גרובר הוא למעשה בשיטת brute force, אנו סורקים את כל הערכים האפשריים ואי אפשר לבצע איזושהי הנחה לגבי מבנה הנתונים).

המסקנה השנייה, והינה מרחיקת לכת יותר היא שלא ניתן לקבל האצה משמעותית באופן טריוויאלי על גבי מחשב קוונטי. לו היה מתקבל כי החסם התחתון הינו $\Omega(\log N)$, אזי מציאת פתרון לבעיית החיפוש בסיבוכיות $O(\log N)$ היה בעל משמעות חשובה שכן ניתן היה לקחת בעיה שאיננה פתירה בפרק זמן סביר על מחשב קלאסי, (בעיה בNP), ולחפש מבין כל 2^n האפשרויות את הפתרון, ובכך לקבל אלגוריתם בסיבוכיות $O(\log 2^n)=O(n)$ דהיינו בפרק זמן סביר.

ז. הערות-

1. ניתן להרחיב את הפתרון גם לבעיה בה $M<N$ ללא שינוי מהותי באלגוריתם, ועדיין להישאר באותה יעלות (פשוט ע"י הוספת N איברים שאינן פתרון לפונקציה).
2. ניתן להרחיב למקרה בו לא ידוע M מראש, ע"י הפעלת אלגוריתם אחר המחשב את ערכו של M, (בעזרת אלגוריתם הערכת פאזה שאותו נציג בהמשך), וזאת מבלי לפגוע בסיבוכיות הכוללת של מציאת הפתרון.

פרק תשיעי- האלגוריתם של שור

בעיית הפירוק שתוצג בפרק זה הינה בעיה בעלת חשיבות מיוחדת במדעי המחשב. פתרון יעיל שלה במחשב קלאסי איננו ידוע, ואלגוריתמי הצפנה רבים (לדוגמה RSA הנפוץ מאוד באינטרנט) מניחים כי גם לא ימצא כזה. שור (Shor) הראה כי בעזרת מחשב קוונטי ניתן לפתור בעיה זו ביעילות, ומכאן חשיבות האלגוריתם.בשונה מהאלגוריתמים שהוצגו עד כה, אלגוריתם זה מורכב יותר ועושה שימוש בפתרון של מספר בעיות שלכאורה אין קשר ביניהם, אך שימוש מושכל בהם מוביל אל פתרון הבעיה.

חשיבות נוספת לאלגוריתם נעוצה בכך שניתן להכליל חלקים ממנו ובכך לפתור בעיות קשות אחרות בצורה יעילה על גבי מחשב קוונטי.

פרק זה בנוי באופן הבא: תחילה יוצג מעגל קוונטי לחישוב התמרת פורייה ומגבלות הפתרון הקוונטי להתמרה, א"כ תוצג בעיית הערכת הפאזה (phase estimation) ופתרונה- אשר עושה שימוש בהתמרת פורייה. לאחר מכן תוצג בעיית מציאת הסדר ופתרונה אשר מבוסס על פתרון בעיית הערכת הפאזה ולבסוף, תוצג בעיית הפירוק לגורמים , אשר עושה שימוש בפתרון מציאת הסדר.

1. אלגוריתם DFT

התמרת פורייה תשמש אותנו בהמשך בניתוח האלגוריתם של Shor, והינה שימושית באלגוריתמים נוספים אחרים. אך תחילה יש להגדיר את הDFT (Discrete Fourier transform) הקוונטי- QDFT (Quantum Discrete Fourier transform):

תהי $\left|\varphi\right\rangle = \sum_{j=0}^{N-1}\alpha_j\left|j\right\rangle$ פונקצית גל. אזי התמרת פורייה הקוונטית הינה:

$$QDFT(\sum_{j=0}^{N-1}\alpha_j\left|j\right\rangle) \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}e^{i2\pi kj/N}\alpha_j\left|k\right\rangle$$

תרגיל:

א) הראה כי $QDFT(\left|0\right\rangle) = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)$

ב) הראה כי $QDFT(\left|1\right\rangle) = \frac{1}{\sqrt{2}}(\left|0\right\rangle + e^{i\pi}\left|1\right\rangle)$

א. הצגת הבעיה

תהי $\left|\varphi\right\rangle$ פונקצית גל. הראה כי קיים אופרטור יוניטרי F המקיים:

$$QDFT(\left|\varphi\right\rangle) = F\left|\varphi\right\rangle$$

ב. פתרון

נראה כי האופרטור הינו:

$$F=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}e^{i2\pi kj/N}\left|k\right\rangle\left\langle j\right|$$

תחילה נראה כי הוא אכן מבצע את ההתמרה:

$$F\left|\varphi\right\rangle=\left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}e^{i2\pi kj/N}\left|k\right\rangle\left\langle j\right|\right)\sum_{l=0}^{N-1}\alpha_l\left|l\right\rangle=$$

$$\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}e^{i2\pi kj/N}\alpha_j\left|k\right\rangle\equiv QDFT(\varphi)$$

בשוויון האחרון השתמשנו בכך ש $\sum_{j=0}^{N-1}\left\langle j\right|\sum_{l=0}^{N-1}\alpha_l\left|l\right\rangle=\sum_{l=0}^{N-1}\alpha_l$ בגלל ש $\begin{matrix}\left\langle j\middle|l\right\rangle=0 & j\neq l\\ \left\langle j\middle|l\right\rangle=1 & j=l\end{matrix}$.

כעת נותר להראות יוניטריות- מהגדרת האופרטור נובע כי:

$$F^{\dagger}=\frac{1}{\sqrt{N}}\sum_{k'=0}^{N-1}\sum_{j'=0}^{N-1}e^{-i2\pi k'j'/N}\left|j'\right\rangle\left\langle k'\right|$$

ולכן:

$$F^{\dagger}F=\frac{1}{N}\sum_{k'=0}^{N-1}\sum_{j'=0}^{N-1}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}e^{-i2\pi k'j'/N}\left|j'\right\rangle\left\langle k'\middle|e^{i2\pi kj/N}\middle|k\right\rangle\left\langle j\right|=$$

$$\frac{1}{N}\sum_{k'=0}^{N-1}\sum_{j'=0}^{N-1}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}e^{i2\pi(kj-k'j')/N}\left|j'\right\rangle\left\langle k'\middle\|k\right\rangle\left\langle j\right|=$$

$$\frac{1}{N}\sum_{j'=0}^{N-1}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}e^{i2\pi k(j-j')/N}\left|j'\right\rangle\left\langle j\right|$$

כאשר k=0 הביטוי בתוך הסכום הינו I, למקרים האחרים נראה כי $\frac{1}{N}\sum_{j'=0}^{N-1}e^{i2\pi k(j-j')/N}=0$.

תרגיל: הראה כי $\frac{1}{N}\sum_{j'=0}^{N-1}e^{i2\pi k(j-j')/N}=0$.

פתרון:

$$\frac{1}{N}\sum_{j'=0}^{N-1}e^{i2\pi k(j-j')/N}=\frac{1}{N}\left(1+e^{i2\pi k(j-1)/N}+e^{i2\pi k(j-2)/N}+\ldots e^{i2\pi k(j-(N-1))/N}\right)$$

לשם כך נעזר בסכום טור גיאומטרי. כאן המנה היא $q=e^{-i2\pi kj/N}$, ולכן:

$$\frac{1}{N}\sum_{j'=0}^{N-1}e^{i2\pi k(j-j')/N}=\frac{1-e^{-(i2\pi kj/N)^N}}{1-e^{-i2\pi kj/N}}=\frac{1-e^{-i2\pi kj}}{1-e^{-i2\pi kj/N^N}}=\frac{1-1}{1-e^{-i2\pi kj/N^N}}=0$$

מ.ש.ל.

מכאן נובע כי:

$$F^{\dagger}F=\frac{1}{N}\sum_{j'=0}^{N-1}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}e^{i2\pi k(j-j')/N}\left|j'\right\rangle\left\langle j\right|$$

$$\sum_{j'=0}^{N-1}\sum_{j=0}^{N-1}\left|j'\right\rangle\left\langle j\right|\delta_{j'j}=I$$

מכאן שהאופרטור יוניטרי- מ.ש.ל.

אם כך, ניתן לבנות מעגל למימוש אופרטור זה- אך כיצד? לשם כך נתבונן בייצוג הבינארי של מספר j הנתון ע"י:

$$j=\sum_{i=0}^{n-1}2^i j_i$$

זאת אומרת שהתמרת פורייה של $\left|j\right\rangle$, נתונה על ידי:

$$QDFT(\left|j\right\rangle)=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}e^{i2\pi jk/N}\left|k\right\rangle$$

נרשום את k בייצוג הבינארי שלו: $k=\sum_{l=0}^{n-1}k_l 2^l$. על כן:

$$\sum_{k=0}^{N-1}e^{\alpha k/N}=\sum_{k=0}^{N-1}e^{\alpha\sum_{l=0}^{n-1}k_l 2^l/2^n}=\sum_{k=0}^{N-1}e^{\alpha\sum_{l=0}^{n-1}k_l 2^{l-n}}=\sum_{k=0}^{N-1}e^{\alpha\sum_{l=1}^{n}k_l 2^{-l}}$$

$$=\sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\cdots\sum_{k_n=0}^{1}e^{\alpha\sum_{l=1}^{n}k_l 2^{-l}}$$

ועל כן:

$$QDFT(|j\rangle)=\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}e^{i2\pi jk/2^n}|k\rangle=$$

$$\frac{1}{2^{\frac{n}{2}}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}e^{i2\pi j(\sum_{l=1}^{n}k_l2^{-l})}|k_1\cdots k_n\rangle$$

הביטוי $|k_1\cdots k_n\rangle$ הינו $|k_1\rangle\otimes|k_2\rangle\cdots\otimes|k_n\rangle$ (לדוגמה: $|5\rangle=|1\rangle\otimes|0\rangle\otimes|1\rangle$). נשתמש בסימון למכפלה טנזורית, ונרשום:

$$QDFT(|j\rangle)=\frac{1}{2^{\frac{n}{2}}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}e^{i2\pi j(\sum_{l=1}^{n}k_l2^{-l})}|k_1\cdots k_n\rangle=$$

$$2^{-n/2}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\bigotimes_{l=1}^{n}\left(e^{i2\pi jk_l2^{-l}}|k_l\rangle\right)$$

מכיוון שl רץ מ1 עד n , ניתן להיעזר בסימן l כאינדקס לk ולקבל:

$$QDFT(|j\rangle)=2^{-n/2}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\bigotimes_{l=1}^{n}\left(e^{i2\pi jk_l2^{-l}}|k_l\rangle\right)=$$

$$2^{-n/2}\bigotimes_{l=1}^{n}\left[\sum_{k_l=0}^{1}e^{i2\pi jk_l2^{-l}}|k_l\rangle\right]=$$

$$2^{-n/2}\bigotimes_{l=1}^{n}\left(|0\rangle+e^{i2\pi j2^{-l}}|1\rangle\right)$$

את $j2^{-l}$ ניתן לייצג בצורה בינארית (נשים לב לנקודה העשרונית) כ: $j_1j_2\cdots j_{l+1}.j_l\cdots j_n$.
מכיוון שערך זה מוכפל ב 2π , והינו בחזקת e , החלק של הביטוי הבינארי שמשמאל לנקודה העשרונית (השלמים) ניתן להשמטה. נרשום זאת בצורה פורמאלית:

$$e^{i2\pi(j_1j_2\cdots j_{l+1}.j_l\cdots j_n)}=e^{i2\pi(j_1j_2\cdots j_{l+1}.j_l\cdots j_n)}=e^{i2\pi(0.j_l\cdots j_n)}$$

על כן נרשום:

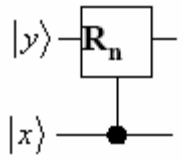
$$QDFT(|j\rangle) = 2^{-n/2} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{i2\pi j 2^{-l}} |1\rangle \right)$$

$$= \frac{\left(|0\rangle + e^{i2\pi 0.j_n} |1\rangle \right)\left(|0\rangle + e^{i2\pi 0.j_{n-1}j_n} |1\rangle \right)\cdots\left(|0\rangle + e^{i2\pi 0.j_1 \ldots j_n} |1\rangle \right)}{2^{n/2}}$$

נעשה שימוש בהצגה זו על מנת לבנות בעזרתה מימוש לאופרטור. נגדיר שער סיבוב פאזה כ:

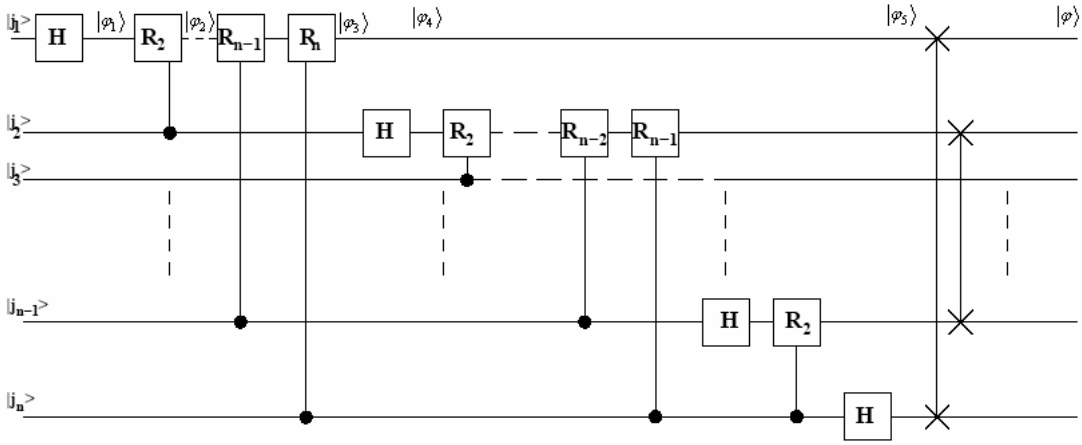
$$R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi/2^n} \end{pmatrix}$$

נסמן שער זה כמתואר באיור 42. שער זה גם נקרא שער R_n controlled, שכן אם הקיוביט $|x\rangle$ הינו $|0\rangle$ אז $|y\rangle$ לא משתנה, ואם $x = |1\rangle$ אז $|y\rangle$ מסובב את הפאזה שלו)



איור 54

איור 55 מתאר את המעגל המספק את המימוש הדרוש.



איור 55

הסבר: נניח שבכניסה הערך הינו: $|j_1 \cdots j_n\rangle$. לאחר שער הדמרד הראשון, פונקצית הגל הינה:

באם $j_1 = 0$:

$$|\varphi_1\rangle = \frac{1}{2^{1/2}}\left(|0\rangle + |1\rangle\right)|0 j_2 \ldots j_n\rangle$$

באם $j_1 = 1$:

$$|\varphi_1\rangle = \frac{1}{2^{1/2}}\left(|0\rangle - |1\rangle\right)|1 j_2 \ldots j_n\rangle$$

ניתן לרשום זאת:

$$|\varphi_1\rangle = \frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i(0.j_1)}|1\rangle\right)|j_1 \ldots j_n\rangle$$

שכן הנקודה העשרונית היא נקודה "בינארית" ומתקיים $2 * 0.1 = 2 * 2^{-1} = 1$, ואז עבור j=1 הביטוי הינו:

$$|\varphi_1\rangle = \frac{1}{2^{1/2}}\left(|0\rangle + e^{\pi i}|1\rangle\right)|j_1 \ldots j_n\rangle = \frac{1}{2^{1/2}}\left(|0\rangle - |1\rangle\right)|j_1 \ldots j_n\rangle$$

ועבור j=0:

$$|\varphi_1\rangle = \frac{1}{2^{1/2}}\left(|0\rangle + e^{0}|1\rangle\right)|j_1 \ldots j_n\rangle = \frac{1}{2^{1/2}}\left(|0\rangle + |1\rangle\right)|j_1 \ldots j_n\rangle.$$

לאחר שער CR_2 פונקצית הגל הינה:

$$|\varphi_2\rangle = \frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i(0.j_1 j_2)}|1\rangle\right)|j_1 \ldots j_n\rangle$$

לאחר שער CR_n פונקצית הגל הינה:

$$|\varphi_3\rangle = \frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i(0.j_1 \ldots j_n)}|1\rangle\right)|j_1 \ldots j_n\rangle$$

לאחר שער הדמרד השני:

$$|\varphi_4\rangle = \frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i(0.j_1 \ldots j_n)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(0.j_2)}\right)|j_3 \ldots j_n\rangle$$

ולבסוף נקבל:

$$|\varphi_5\rangle = \frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i(0.j_1\ldots j_n)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(0.j_2\ldots j_n)}\right)\ldots\left(|0\rangle + e^{2\pi i(0.j_n)}\right)$$

כעת יש להפוך את סדר הקיוביטים:

$$|\varphi\rangle = \frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i(0.j_n)}\right)\left(|0\rangle + e^{2\pi i(0.j_{n-1}j_n)}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i(0.j_1\ldots j_n)}\right)$$

מ.ש.ל.

לדוגמה: עבור 3 קיוביטים, $N = 2^3 = 8$:

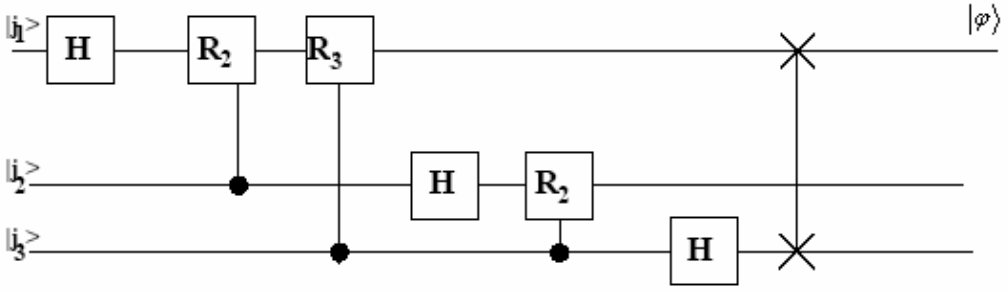
$$QDFT(|j\rangle) = \frac{1}{\sqrt{8}}\sum_{k=0}^{8-1} e^{i2\pi jk/8}|k\rangle = \frac{1}{\sqrt{8}}\sum_{k=0}^{8-1}\omega^{jk}|k\rangle$$

האופרטור הינו:

$$QDFT(|j\rangle) = 2^{-3/2}\bigotimes_{l=1}^{3}\left(|0\rangle + e^{i2\pi j2^{-l}}|1\rangle\right)$$

$$= \frac{\left(|0\rangle + e^{i2\pi 0.j_3}|1\rangle\right)\left(|0\rangle + e^{i2\pi 0.j_2 j_3}|1\rangle\right)\left(|0\rangle + e^{i2\pi 0.j_1 j_2 j_3}|1\rangle\right)}{2^{3/2}}$$

והמעגל מתואר באיור 56.



איור 56

ג. סיבוכיות

במעגל יש n שערים בהתחלה, א"כ n-1, א"כ n-2 וכולי- ז"א סכום של סדרה חשבונית ומכאן סיבוכיות של $O(n^2)$. שערי ההחלפה הינם מוסיפם סיבוכיות O(n) כי יש להחליף n/2 סיביות, ולכן סה"כ סיבוכיות של $O(n^2)$ או במונחים של N: $O((\log N)^2)$.

הערה: למרבה הצער, לא נוכל לעשות שימוש ישיר במעגל- מדידת פונקצית הגל תגרום לקריסתו! על כן לא נוכל לדעת את ערך האמפליטודה בכל ביט וביט. למרבה המזל,(ומכאן חשיבות הדיון) כן ניתן לעשות שימוש במעגל זה באלגוריתמים אחרים.

2. אלגוריתם הערכת פאזה (Phase estimation)

כפי שצוין בפרק הראשון הערכים העצמיים של מטריצה יוניטרית הינם $\lambda_i = e^{i2\pi\theta_i}$ כאשר $0 \le \theta_i < 1$, על כן אם נתון לנו אופרטור קוונטי U הפועל על n קיוביטים (המימד של U לכן הוא $N = 2^n$) ונפעיל אותה על פונקצית גל $|v_i\rangle$ כאשר v_i הוא וקטור עצמי של האופרטור U עם הערך העצמי המתאים $\lambda_i = e^{i2\pi\theta_i}$, אזי במוצא נקבל:

$$U|v_i\rangle = \lambda_i|v_i\rangle = e^{i2\pi\theta_i}|v_i\rangle$$

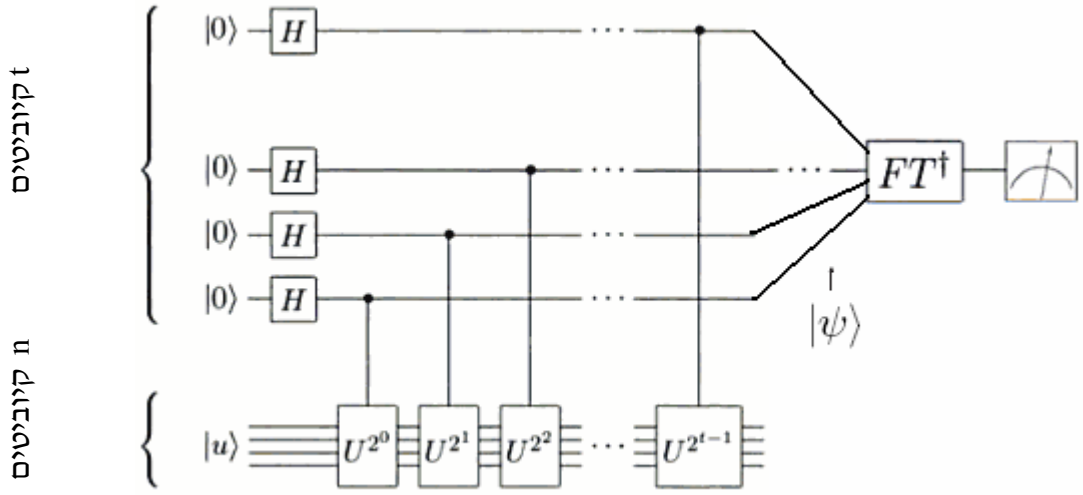
ז"א פונקצית הגל בכניסה מוכפלת בערך העצמי $e^{i2\pi\theta_i}$.

א. הצגת הבעיה

נתון אופרטור U הפועל על n קיוביטים, ופונקצית גל שהיא ווקטור עצמי שלו. מה הזווית θ_i של הערך העצמי המתאים $\lambda_i = e^{i2\pi\theta_i}$ לווקטור זה?

ב. פתרון

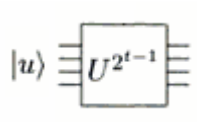
גם כאן נגדיר controlled U , בדומה לדיון הקודם, וניעזר ברגיסטר עזר בן t קיוביטים , על מנת לבנות את המעגל המתואר באיור 57.



איור 57

כאשר בחלק העליון מופיע רגיסטר העזר ובחלק התחתון- רגיסטר המכיל את פונקצית הגל הנתונה. גודל רגיסטר העזר הינו t קיוביטים (ערכו של t הינו פונקציה של רמת הדיוק הנדרשת, ויוגדר בהמשך), וגודל הרגיסטר השני הינו n .

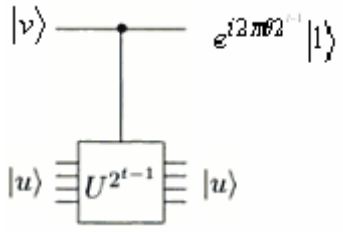
בכדי לנתח את המעגל שבאיור 57, ננתח תחילה את המעגל המתואר באיור 58 :



איור 58

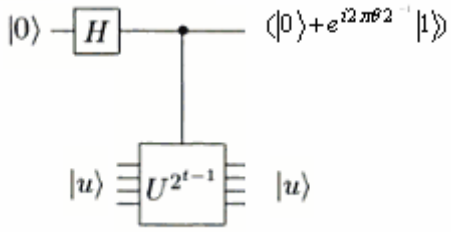
מכיוון ש $U|\psi\rangle = e^{i2\pi\theta}|\psi\rangle$ אז פונקצית הגל לאחר השער : $U^{2^{t-1}}|\psi\rangle = e^{i2\pi\theta 2^{t-1}}|\psi\rangle$.

כעת ננתח את המעגל המתואר באיור 59 :



איור 59

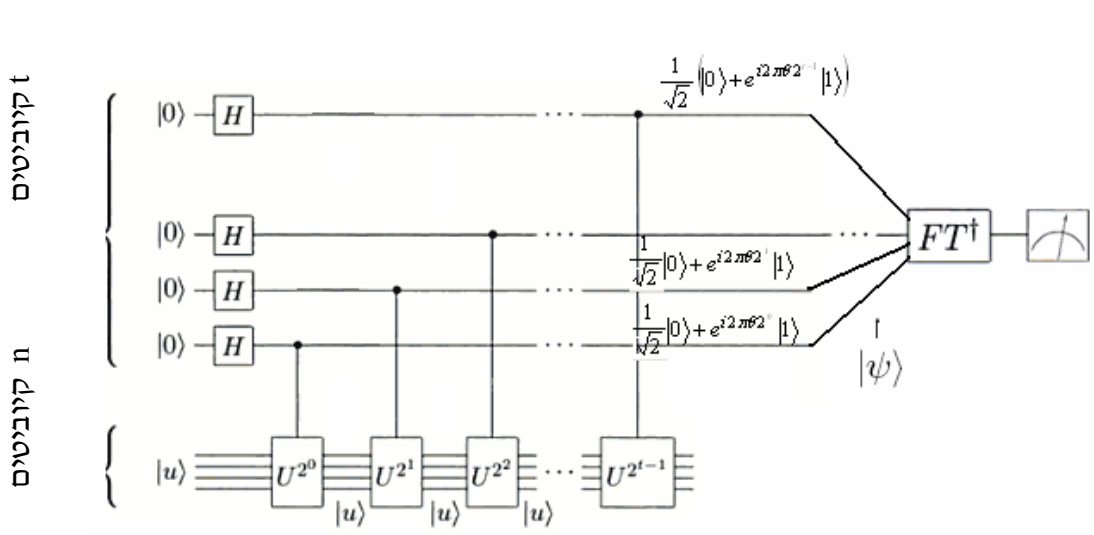
אזי מוצא האופרטור זהה לכניסה, ולכן : $|v\rangle = |0\rangle$. באם $|v\rangle$ כאשר קיוביט הבקרה הוא $|1\rangle$: $|1\rangle|u\rangle \to |1\rangle e^{i2\pi\theta 2^{t-1}}|u\rangle = e^{i2\pi\theta 2^{t-1}}|1\rangle|u\rangle$, וכאשר $|v\rangle = |1\rangle$, $|0\rangle|u\rangle \to |0\rangle|u\rangle$.



איור 60

עבור המעגל המתואר באיור 60, מוצא המעגל הינו : $|0\rangle|u\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + e^{i2\pi\theta 2^{t-1}}|1\rangle)|u\rangle$.

מניתוחים אלו עולה כי את המעגל שבאיור 57, ניתן לתאר כבאיור 61.



איור 61

הקיוביטים העליונים שבמוצא המעגל (לפני $FT^\dagger$) הינם:

$$|\psi\rangle = \frac{1}{\sqrt{2^t}}\left(|0\rangle + e^{i2\pi\theta 2^{t-1}}|1\rangle\right)\ldots\left(|0\rangle + e^{i2\pi\theta 2^{1}}|1\rangle\right)\left(|0\rangle + e^{i2\pi\theta 2^{0}}|1\rangle\right)$$

נניח וידוע לנו t – מספר הביטים שצריך כדי לרשום את θ_i בדיוק. מכיוון שהזוית θ_i הינה:

$0 \le \theta_i < 1$, אזי בכתיב בינארי נוכל לרשום:

$\theta_i = 0.x_0x_1x_2\ldots x_t = \frac{x_0}{2} + \frac{x_1}{2^2} + \ldots\frac{x_t}{2^t}$. על כן, נשכתב את מוצא המעגל (לפני $FT^\dagger$) כ:

$$|\psi\rangle = \frac{1}{\sqrt{2^t}}\left(|0\rangle + e^{i2\pi\theta 0.x_t}|1\rangle\right)\ldots\left(|0\rangle + e^{i2\pi 0.x_1x_2\ldots x_{t'}}|1\rangle\right)\left(|0\rangle + e^{i2\pi 0.x_0x_1x_2\ldots x_t}|1\rangle\right).$$

(עשינו שימוש בכך ש:

$$e^{i2\pi 0.x_0x_1x_2\ldots x_t\,2^l} = e^{i2\pi x_0x_1\ldots x_l.x_{l+1}\ldots x_t} = e^{i2\pi x_0x_1\ldots x_l.x_{l+1}\ldots x_t} = e^{i2\pi 0.x_{l+1}\ldots x_t}$$

).

מוצא זה הוא למעשה המוצא של DFT, על כן אם פונקצית הגל תעבור דרך DFT^{-1}, נקבל כי במוצא המעגל יימדד θ_i.

אם כך- מוצא המעגל מספק את הדרוש אך זאת בתנאי ומתקיימת ההנחה- שבה t (מספר הביטים שצריך כדי לרשום את θ_i בדיוק) קיים וידוע. אך מכיוון שt לא ידוע וייתכן אף שלא קיים (שכן θ_i לא רציונאלי) נרצה למצוא t מספיק טוב, כלומר איזשהו חסם תחתון לt כך שהתוצאה תצא

מספיק טובה. על כן ננתח את המעגל על מנת למצוא את t, כאשר יש לקחת בחשבון כי ייתכן ו θ_i לא יכולה להירשם בדיוק ע"י t ביטים. הראנו כבר כי פונקצית הגל לפני התמרת פורייה ההפוכה הינה:

$$|\psi\rangle = \frac{1}{\sqrt{2^t}}\left(|0\rangle + e^{i2\pi\theta 2^{t-1}}|1\rangle\right)\ldots\left(|0\rangle + e^{i2\pi\theta 2^{1}}|1\rangle\right)\left(|0\rangle + e^{i2\pi\theta 2^{0}}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2^t}}\prod_{k=t-1}^{0}|0\rangle + e^{i2\pi\theta 2^k}|1\rangle$$

תרגיל: הראה כי $\frac{1}{\sqrt{2^t}}\prod_{k=t-1}^{0}|0\rangle + e^{i2\pi\theta 2^k}|1\rangle = \frac{1}{\sqrt{2^t}}\sum_{y=0}^{2^t-1}e^{i2y\pi\theta}|y\rangle$.

הוכחה: באינדוקציה.

<u>בדיקה</u>:

עבור t=1:

$$\frac{1}{\sqrt{2}}\prod_{k=0}^{0}|0\rangle + e^{i2\pi\theta 2^k}|1\rangle = \frac{|0\rangle + e^{i2\pi\theta}|1\rangle}{\sqrt{2}}$$

$$\frac{1}{\sqrt{2}}\sum_{y=0}^{1}e^{i2y\pi\theta}|y\rangle = \frac{|0\rangle + e^{i2\pi\theta}|1\rangle}{\sqrt{2}}$$

<u>הנחת אינדוקציה</u>: עבור t מתקיים:

$$\frac{1}{\sqrt{2^t}}\prod_{k=t-1}^{0}|0\rangle + e^{i2\pi\theta 2^k}|1\rangle = \frac{1}{\sqrt{2^t}}\sum_{y=0}^{2^t-1}e^{i2y\pi\theta}|y\rangle.$$

<u>צריך להוכיח</u>:

$$\frac{1}{\sqrt{2^{t+1}}}\prod_{k=t}^{0}|0\rangle + e^{i2\pi\theta 2^k}|1\rangle = \frac{1}{\sqrt{2^{t+1}}}\sum_{y=0}^{2^{t+1}-1}e^{i2y\pi\theta}|y\rangle$$

<u>הוכחה</u>:

$$\frac{1}{\sqrt{2^{t+1}}}\prod_{k=t}^{0}|0\rangle + e^{i2\pi\theta 2^k}|1\rangle = \frac{|0\rangle + e^{i2\pi\theta 2^t}|1\rangle}{\sqrt{2}}\frac{1}{\sqrt{2^t}}\prod_{k=t-1}^{0}|0\rangle + e^{i2\pi\theta 2^k}|1\rangle$$

$$= \frac{|0\rangle + e^{i2\pi\theta 2^t}|1\rangle}{\sqrt{2}}\frac{1}{\sqrt{2^t}}\sum_{y=0}^{2^t-1}e^{i2y\pi\theta}|y\rangle = \frac{1}{\sqrt{2^{t+1}}}\left(\sum_{y=0}^{2^t-1}e^{i2y\pi\theta}|0\rangle|y\rangle + e^{i2\pi\theta 2^t}\sum_{y=0}^{2^t-1}e^{i2y\pi\theta}|1\rangle|y\rangle\right)$$

$$= \frac{1}{\sqrt{2^{t+1}}}\left(\sum_{y=0}^{2^t-1}e^{i2y\pi\theta}|0\rangle|y\rangle + \sum_{y=0}^{2^t-1}e^{i2\pi\theta(y+2^t)}|1\rangle|y\rangle\right) = \frac{1}{\sqrt{2^{t+1}}}\sum_{y=0}^{2^{t+1}-1}e^{i2y\pi\theta}|y\rangle$$

מ.ש.ל.

ועל כן ניתן לרשום:

$$|\psi\rangle = \frac{1}{\sqrt{2^t}} \prod_{k=t-1}^{0} |0\rangle + e^{i2\pi\theta 2^k} |1\rangle = \frac{1}{\sqrt{2^t}} \sum_{y=0}^{2^t-1} e^{i2y\pi\theta} |y\rangle$$

התמרת פורייה ההפוכה מוגדרת כ:

$$F^\dagger = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} e^{-i2\pi kj/N} |j\rangle\langle k| = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} \sum_{j=0}^{2^t-1} e^{-i2\pi kj/2^t} |j\rangle\langle k|$$

והפעלת התמרת פורייה ההפוכה על $|\psi\rangle$ תיתן

$$F^\dagger |\psi\rangle = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} \sum_{j=0}^{2^t-1} e^{-i2\pi kj/2^t} |j\rangle\langle k| \frac{1}{\sqrt{2^t}} \sum_{y=0}^{2^t-1} e^{i2y\pi\theta} |y\rangle$$

$$= \frac{1}{2^t} \sum_{k=0}^{2^t-1} \sum_{j=0}^{2^t-1} \sum_{y=0}^{2^t-1} e^{-i2\pi kj/2^t} e^{i2y\pi\theta} |j\rangle\langle k\|y\rangle =$$

$$\frac{1}{2^t} \sum_{k=0}^{2^t-1} \sum_{j=0}^{2^t-1} e^{-i2\pi kj/2^t} e^{i2k\pi\theta} |j\rangle = \frac{1}{2^t} \sum_{k=0}^{2^t-1} \sum_{j=0}^{2^t-1} e^{2\pi ki\left(\theta - \frac{j}{2^t}\right)} |j\rangle$$

$$= \frac{1}{2^t} \sum_{k=0}^{2^t-1} \sum_{j=0}^{2^t-1} \left(e^{2\pi i\left(\theta - \frac{j}{2^t}\right)} \right)^k |j\rangle$$

(בצעד השני נעשה שימוש בכך ש $\langle k|y\rangle = \begin{cases} 1 & k = y \\ 0 & k \neq y \end{cases}$).

נסמן את $0.a_0a_1\ldots a_t$ כקירוב הטוב ביותר שניתן לעשות ל θ בעזרת t ביטים. סימון זה ניתן להירשם גם כ $\frac{a}{2^t}$ (זאת אומרת הגדרנו את a כמספר שהייצוג הבינארי שלו הוא $a_0a_1\ldots a_t$).

המשתנה j שבמשוואת הגל רץ מ0 עד 2^t-1 - סה"כ ישנם 2^t איברים. ניתן להמיר משתנה זה ל $j = (a+l) \bmod 2^t$ (שכן גם הוא בן 2^t איברים, ורץ מ a עד 2^t-1 וא"כ מ0 עד a):

$$F^{\dagger}\left|\psi\right\rangle=\frac{1}{2^t}\sum_{k=0}^{2^t-1}\sum_{j=0}^{2^t-1}\left(e^{2\pi i\left(\theta-\frac{j}{2^t}\right)}\right)^k\left|j\right\rangle$$

$$=\frac{1}{2^t}\sum_{k=0}^{2^t-1}\sum_{l=0}^{2^t-1}\left(e^{2\pi i\left(\theta-\frac{(a+l)\bmod 2^t}{2^t}\right)}\right)^k\left|(a+l)\bmod 2^t\right\rangle$$

הביטוי $e^{2\pi i\left(\theta-\frac{(a+l)\bmod 2^t}{2^t}\right)}$ שקול לביטוי $e^{2\pi i\left(\theta-\frac{(a+l)}{2^t}\right)}$ בגלל ש:

$$e^{2\pi(a+l)/2^t}=e^{2\pi((a+l)\bmod 2^t/2^t+(a+l)div2^t)}=e^{\frac{2\pi}{2^t}((a+l)\bmod 2^t)}e^{2\pi((a+l)div2^t)}$$

$$=e^{\frac{2\pi}{2^t}((a+l)\bmod 2^t)}$$

ולכן:

$$F^{\dagger}\left|\psi\right\rangle=\frac{1}{2^t}\sum_{k=0}^{2^t-1}\sum_{l=0}^{2^t-1}\left(e^{2\pi i\left(\theta-\frac{(a+l)\bmod 2^t}{2^t}\right)}\right)^k\left|(a+l)\bmod 2^t\right\rangle$$

$$=\frac{1}{2^t}\sum_{k=0}^{2^t-1}\sum_{l=0}^{2^t-1}\left(e^{2\pi i\left(\theta-\frac{(a+l)}{2^t}\right)}\right)^k\left|(a+l)\bmod 2^t\right\rangle$$

נשים לב כי יש כאן סכום של סכום טור גיאומטרי $\left(\sum_{j=1}^{n}q^j=\frac{1-q^n}{1-q}\right)$:

$$F^{\dagger}\left|\psi\right\rangle=\frac{1}{2^t}\sum_{k=0}^{2^t-1}\sum_{l=0}^{2^t-1}\left(e^{2\pi i\left(\theta-\frac{a+l}{2^t}\right)}\right)^k\left|(a+l)\bmod 2^t\right\rangle$$

$$=\frac{1}{2^t}\sum_{l=0}^{2^t-1}\left(\frac{1-e^{2\pi i\left(2^t\theta-(a+l)\right)}}{1-e^{2i\pi\left(\theta-\frac{a+l}{2^t}\right)}}\right)\left|(a+l)\bmod 2^t\right\rangle=$$

$$\sum_{l=0}^{2^t-1}\alpha_l\left|(a+l)\bmod 2^t\right\rangle$$

כאשר : $\alpha_t=\frac{1-e^{2\pi i\left(2^t\theta-(a+l)\right)}}{1-e^{2i\pi\left(\theta-\frac{a+l}{2^t}\right)}}$.

המשתנה l רץ מ0 עד 2^t-1. בחישוב מודולו 2^t זה שקול לריצה מ $-2^{t-1}+1$ עד 2^{t-1} (שכן גם כאן יש 2^t איברים , כלומר מ0 עד 2^t-1) לכן נוכל לרשום :

$$F^{\dagger}\left|\psi\right\rangle=\sum_{l=0}^{2^t-1}\alpha_l\left|(a+l)\bmod 2^t\right\rangle=\sum_{l=-2^{t-1}+1}^{2^{t-1}}\alpha_l\left|(a+l)\bmod 2^t\right\rangle$$

$\frac{a}{2^t}$ סומן כקרוב הטוב ביותר בן t סיביות ל θ - אזי נוכל לרשום :

$$\theta=\frac{a}{2^t}+\delta$$

כאשר $0<\left|\delta\right|\le\frac{1}{2^t}$. נציב סימון זה ונקבל :

$$\alpha_l=\frac{1}{2^t}\left(\frac{1-e^{2\pi i\left(2^t\theta-(a+l)\right)}}{1-e^{2\pi i\left(\theta-\frac{a+l}{2^t}\right)}}\right)=\frac{1}{2^t}\left(\frac{1-e^{2\pi i\left(2^t(\frac{a}{2^t}+\delta)-(a+l)\right)}}{1-e^{2\pi i\left(\frac{a}{2^t}+\delta-\frac{a+l}{2^t}\right)}}\right)=\frac{1}{2^t}\left(\frac{1-e^{2\pi i\left(2^t\delta-l\right)}}{1-e^{2\pi i\left(\delta-\frac{l}{2^t}\right)}}\right)$$

את פונקצית הגל נוכל לרשום בדרך הבאה :

$$F^{\dagger}\left|\psi\right\rangle=\sum_{l=-2^{t-1}+1}^{-(e+1)}\alpha_l\left|(a+l)\bmod 2^t\right\rangle+\sum_{l=-e}^{e}\alpha_l\left|(a+l)\bmod 2^t\right\rangle$$

$$+\sum_{l=e+1}^{2^{t-1}}\alpha_l\left|(a+l)\bmod 2^t\right\rangle$$

וניתן להתייחס אל פונקצית הגל בפירוש הבא- החלק האמצעי הינו כל המצבים שסביב a עד כדי e. שני החלקים האחרים "רחוקים" מאוד מa (הרבה יותר מe). לכן ההסתברות למדידת m "גרוע" – כך ש $\left|m-a\right|>e$ נתונה על ידי:

$$p(m)=\sum_{l=-2^{t-1}+1}^{-(e+1)}\left|\alpha_l\right|^2+\sum_{l=e+1}^{2^{t-1}}\left|\alpha_l\right|^2$$

נראה כי לביטוי זה יש חסם תחתון. מאי השוויון: $\left|1-e^{ix}\right|\le 2$ ניתן לרשום:

$$\left|\alpha_l\right|=\left|\frac{1}{2^t}\left(\frac{1-e^{2\pi i\left(2^t\delta-l\right)}}{1-e^{2\pi i\left(\delta-\frac{l}{2^t}\right)}}\right)\right|\le\frac{2}{2^t\left|1-e^{2\pi i\left(\delta-\frac{l}{2^t}\right)}\right|}$$

המשתנה l הוא בין $1+2^{t-1}$ ל -2^{t-1}, נעזר בכך ש $0<\left|\delta\right|\le\frac{1}{2^t}$ ועל כן לביטוי $2\pi\left(\delta-\frac{l}{2^t}\right)$

החסם העליון הוא כש $l=-2^{t-1}+1$, ו $\delta=\frac{1}{2^t}$:

$$2\pi\left(\delta-\frac{l}{2^t}\right)\le 2\pi\left(\frac{1}{2^t}-\frac{-2^{t-1}+1}{2^t}\right)\le 2\pi\left(\frac{1}{2^t}+\frac{1}{2}-\frac{1}{2^t}\right)=2\pi\frac{1}{2}=\pi$$

החסם התחתון הוא כש $l=2^{t-1}$, ו $\delta=0$:

$$2\pi\left(\delta-\frac{l}{2^t}\right)\ge 2\pi\left(-\frac{2^{t-1}}{2^t}\right)\ge 2\pi\left(-\frac{1}{2}\right)\ge -2\pi\frac{1}{2}\ge-\pi$$

מכאן ניתן לרשום: $-\pi\le 2\pi\left(\delta-\frac{l}{2^t}\right)\le\pi$. מכיוון ש $\left|1-e^{i\phi}\right|\le\frac{2\phi}{\pi}$ עבור $-\pi\le\phi\le\pi$, נוכל לרשום:

$$|\alpha_l| \le \frac{2}{2^t\left|1-e^{2\pi i\left(\delta-\frac{l}{2^t}\right)}\right|} \le \frac{2}{2^t\frac{4\pi\left(\delta-\frac{l}{2^t}\right)}{\pi}} = \frac{1}{2^{t+1}\left(\delta-\frac{l}{2^t}\right)} = \frac{1}{2\left(2^t\delta-l\right)}$$

ועל כן חסם על ההסתברות לקבלת m נתונה על ידי:

$$p(m) = \sum_{l=-2^{t-1}+1}^{-(e+1)}|\alpha_l|^2 + \sum_{l=e+1}^{2^{t-1}}|\alpha_l|^2$$

$$\le \sum_{l=-2^{t-1}+1}^{-(e+1)}\left|\frac{1}{2\left(2^t\delta-l\right)}\right|^2 + \sum_{l=e+1}^{2^{t-1}}\left|\frac{1}{2\left(2^t\delta-l\right)}\right|^2$$

$$= \frac{1}{4}\left(\sum_{l=-2^{t-1}+1}^{-(e+1)}\frac{1}{\left(2^t\delta-l\right)^2} + \sum_{l=e+1}^{2^{t-1}}\frac{1}{\left(2^t\delta-l\right)^2}\right)$$

מכיוון ש $0<|\delta|\le\frac{1}{2^t}$, אז $0<2^t|\delta|\le 1$ ונוכל לרשום:

$$p(m) \le \frac{1}{4}\left(\sum_{l=-2^{t-1}+1}^{-(e+1)}\frac{1}{\left(l-2^t\delta\right)^2} + \sum_{l=e+1}^{2^{t-1}}\frac{1}{\left(l-2^t\delta\right)^2}\right)$$

$$\le \frac{1}{4}\left(\sum_{l=-2^{t-1}+1}^{-(e+1)}\frac{1}{(l)^2} + \sum_{l=e+1}^{2^{t-1}}\frac{1}{(l-1)^2}\right) = \frac{1}{4}\left(\sum_{l=(e+1)}^{2^{t-1}-1}\frac{1}{(l)^2} + \sum_{l=e}^{2^{t-1}+1}\frac{1}{(l)^2}\right)$$

$$\le \frac{1}{4}\left(\sum_{l=(e+1)}^{2^{t-1}+1}\frac{1}{(l)^2} + \sum_{l=e}^{2^{t-1}+1}\frac{1}{(l)^2}\right) = \frac{1}{2}\left(\sum_{l=e}^{2^{t-1}+1}\frac{1}{(l)^2}\right) \le \frac{1}{2}\int_{e-1}^{2^{t-1}+1}\frac{dl}{(l)^2} =$$

$$-\frac{1}{2l}\Bigg|_{e-1}^{2^{t-1}+1} = -\frac{1}{2(2^{t-1}+1)} + \frac{1}{2(e-1)} \le \frac{1}{2(e-1)}$$

נניח ואנו מעוניינים שהמדידה של הזוית θ_i תתבצע בדיוק של 2^{-n} (כלומר: $\left|\frac{m}{2^t}-\frac{a}{2^t}\right|<2^{-n}$)

בסבירות של לפחות $1-\varepsilon$ (כאשר $0<\varepsilon<1$). מכיוון שרשמנו כי $|m-a|>e$, נובע כי עלינו לבחור $e=2^{t-n}-1$. נבחר t גדול מn, כלומר t=n+p כאשר p הינו שלם חיובי. ההסתברות לקבלת תוצאה לא טובה הינה לכל היותר:

$$P(|m-a|>2^{-n}) \le \frac{1}{2(e-1)} = \varepsilon$$

$$\frac{1}{2(2^{t-n}-2)} = \varepsilon$$

$$2^{t-n} - 2 = \frac{1}{2\varepsilon}$$

$$t - n = \log(2 + \frac{1}{2\varepsilon})$$

$$t = n + \left\lceil \log(2 + \frac{1}{2\varepsilon}) \right\rceil$$

לסיכום: באם נבחר $t = n + \left\lceil \log(2 + \frac{1}{2\varepsilon}) \right\rceil$, אזי בסבירות של $1-\varepsilon$ מוצא המעגל הינו a

(הקירוב הטוב ביותר הייתכן ל θ_i בt סיביות) עם טעות מרבית של 2^{-n}.

ג. סיבוכיות

סיבוכיות האלגוריתם הינה כשל התמרת פורייה (ההפוכה), ז"א: $O(t^2)$.

נשים לב כי למעשה אלגוריתם הערכת הפאזה הוא למעשה מדידה של פונקצית הגל $|u\rangle$

בבסיס הנפרש ע"י הווקטורים העצמיים של U.

3. מציאת סדר

הסדר של מספר x מודולו N מוגדר עבור x וN זרים (כלומר כאשר gcd(x,N)=1), ושווה לשלם הקטן ביותר- r, המקיים: $x^r=1 \pmod N$.

לדוגמה, עבור x=5, N=21, מתקבל כי r=6.

שכן (בחישוב מודולו 21): $5^1=5 \quad 5^2=4 \quad 5^3=20 \quad 5^4=16 \quad 5^5=17 \quad 5^6=1$.

ניתן להוכיח כי תמיד קיים סדר למספר נתון במודולו נתון.

א. הצגת הבעיה

בהינתן x, N זרים, הצג אלגוריתם קוונטי למציאת הסדר של x.

ב. פתרון

הערה: בסעיף זה כל החישובים הם חישובים מודולו N. לעיתים נסמן זאת, אך רק לשם ההדגשה.

הפתרון יעשה שימוש באלגוריתם הערכת הפאזה שהוצג בסעיף הקודם. נניח כי בידנו אופרטור U אשר מבצע הכפלה של פונקצית הגל בa מודולו N. דהיינו מתקיים כי:

$$U\left|x\right\rangle = \left|ax_{\mathrm{mod}\,N}\right\rangle$$

מכיוון ש x זר ל N מובטח שיש a^{-1} וניתן להראות שבשל כך האופרטור אינו אלא מטריצת פרמוטציה (מטריצה שאיבריה הן 0 ו1, ובכל שורה ובכל עמודה יש רק 1 אחד). מטריצות פרמוטציה הן יוניטריות, ולכן האופרטור יוניטרי.

ערך עצמי טריוויאלי של האופרטור הוא 1, (ואז הווקטור העצמי המתאים הוא:

$$\left|v_{\lambda=1}\right\rangle = \left|1\right\rangle + \left|a\right\rangle + \left|a^2\right\rangle \ldots + \left|a^{r-1}\right\rangle$$).

תרגיל: בדוק טענה זו.

ערכים עצמיים אחרים של האופרטור , שיענינו אותנו יותר ניתנים לייצוג ע"י: $\omega_s = e^{\frac{2\pi i s}{r}}$

כאשר $s < r$, והווקטור העצמי המתאים הינו:

$$\left|v_s\right\rangle = \frac{1}{\sqrt{r}}\left(\left|1\right\rangle + \omega_s^{-1}\left|a\right\rangle + \omega_s^{-2}\left|a^2\right\rangle \ldots + \omega_s^{-(r-1)}\left|a^{r-1}\right\rangle\right) =$$

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{\frac{-2\pi i k s}{r}}\left|a^k\right\rangle$$

תרגיל: הראה כי פונקצית הגל

$\left|v_s\right\rangle = \frac{1}{\sqrt{r}}\left(\left|1\right\rangle + \omega_s^{-1}\left|a\right\rangle + \omega_s^{-2}\left|a^2\right\rangle \ldots + \omega_s^{-(r-1)}\left|a^{r-1}\right\rangle\right)$ הינה של וקטור עצמי

של U , וכי הערך העצמי המתאים הינו ω_s .

פתרון:

$$U|v_s\rangle = \frac{1}{\sqrt{r}}\left(|a\rangle + \omega_s^{-1}|a^2\rangle + \omega_s^{-2}|a^3\rangle \ldots \omega_s^{-(r-2)}|a^{r-1}\rangle + \omega_s^{-(r-1)}|a^r\rangle\right)$$

$$= \frac{1}{\sqrt{r}}\left(|a\rangle + \omega_s^{-1}|a^2\rangle + \omega_s^{-2}|a^3\rangle \ldots \omega_s^{-(r-2)}|a^{r-1}\rangle + \omega_s^{-(r-1)}|1\rangle\right)$$

$$= \frac{\omega_s}{\sqrt{r}}\left(\omega_s^{-1}|a\rangle + \omega_s^{-2}|a^2\rangle \ldots + \omega_s^{-(r-1)}|a^{r-1}\rangle + \omega_s^{-r}|1\rangle\right)$$

$$= \frac{\omega_s}{\sqrt{r}}\left(\omega_s^{-1}|a\rangle + \omega_s^{-2}|a^2\rangle \ldots + \omega_s^{-(r-1)}|a^{r-1}\rangle + e^{\frac{2\pi i s r}{r}}|1\rangle\right)$$

$$= \frac{\omega_s}{\sqrt{r}}\left(\omega_s^{-1}|a\rangle + \omega_s^{-2}|a^2\rangle \ldots + \omega_s^{-(r-1)}|a^{r-1}\rangle + |1\rangle\right)$$

$$= \omega_s|v_s\rangle = e^{\frac{2\pi i s}{r}}|v_s\rangle$$

מכאן שאם נשתמש באלגוריתם הערכת פאזה, ונספק למעגל פונקצית גל $|v_s\rangle$ אז נקבל במוצא המעגל בקירוב טוב את $\theta_s = \frac{s}{r}$. אם s ידוע אז נוכל להסיק את r בקלות.

המעגל לאלגוריתם הערכת פאזה (איור 57) בנוי למעשה מ3 חלקים- תחילה רגיסטר העזר עובר דרך שערי הדמרד, א״כ פונקצית הגל עוברת דרך שערי controlled U^{2^j} ולבסוף בחלק השלישי והאחרון רגיסטר העזר עובר דרך FT^{-1} ונמדד. בכדי שנוכל להשתמש במעגל זה יש מספר בעיות שצריך לענות עליהם :

1) כיצד נספק למעגל פונקצית גל $|v_s\rangle$ שהיא וקטור עצמי של U שאיננו הווקטור העצמי הטריוויאלי ?

2) כיצד נבנה את החלק השני של המעגל- כיצד נרכיב מעגלי : U^{2^0} controlled, controlled U^{2^1} …, controlled $U^{2^{t-1}}$ (כאשר t נקבע מרמת הדיוק שנרצה) בצורה יעילה (ז״א שהמעגלים יספקו את המוצא בפרק זמן סביר)?

לעת עתה נניח כי הבעיה השנייה פתירה, ונדון רק בבעיה הראשונה. במקום לבנות פונקצית גל שכזו, נבנה סופרפוזיציה של פונקציות גל שהן וקטור עצמי של U. פונקצית גל שהיא סופר פוזיציה של כל הווקטורים העצמיים היא:

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left|v_s\right\rangle=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{\frac{-2\pi iks}{r}}\left|a^k\right\rangle=\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}r\delta_{k,0}\left|a^k\right\rangle=\left|1\right\rangle$$

(נעזרנו בכך ש: $\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{\frac{-2\pi iks}{r}}=r\delta_{k,0}$).

שזו פונקצית גל שקל מאוד להכין. אך מה יקרה לאלגוריתם הערכת פאזה אם במקום להזין בכניסה פונקצית גל של וקטור עצמי, נזין סופרפוזיציה של וקטורים עצמיים ? מכיוון שאלגוריתם הערכת הפאזה הוא למעשה מדידה של פונקצית הגל בכניסה $\left|u\right\rangle$ בבסיס הנפרש ע"י הווקטורים העצמיים של U, פונקצית הגל תקרוס לאחד מהווקטורים העצמיים של U, (בסבירות שווה שכן הסופרפוזיציה היא סכום זהה של כל הוקטורים העצמיים) ומוצא המעגל יציין זווית θ_s של הווקטור העצמי אליו קרסה הפונקציה. זאת אומרת שאם נכניס לכניסת המעגל את פונקצית הגל $\left|1\right\rangle$ מוצא המעגל יהיה איזשהו ערך עצמי של U.

ולכמה קיוביטים נזדקק על מנת להכיל פונקצית גל זו? נקבע את מספר הקיוביטים לL כך ש $n=2L+1$. הקושי המתעורר כעת הוא שאין אנו יודעים לאיזה וקטור עצמי הפונקציה תקרוס- זאת אומרת שאין אנו יודעים מה הוא s- ואז איך נדע לחשב את r לפי $\theta_s=\frac{s}{r}$? (שכן גם r וגם s נעלמים, ואם נחזור שוב על המדידה נקבל זווית אחרת s אחר). לצורך כך נשתמש באלגוריתם הקלאסי של "חישוב שבר משולב" לחישוב המכנה והמונה עבור מספר רציונאלי (ראה נספח א'). על כן הפתרון כולו מתואר כעת באיור 62. אך בכך אין די. מכיוון שבשיטה המתוארת עדיין ישנם 2 מוקשים:

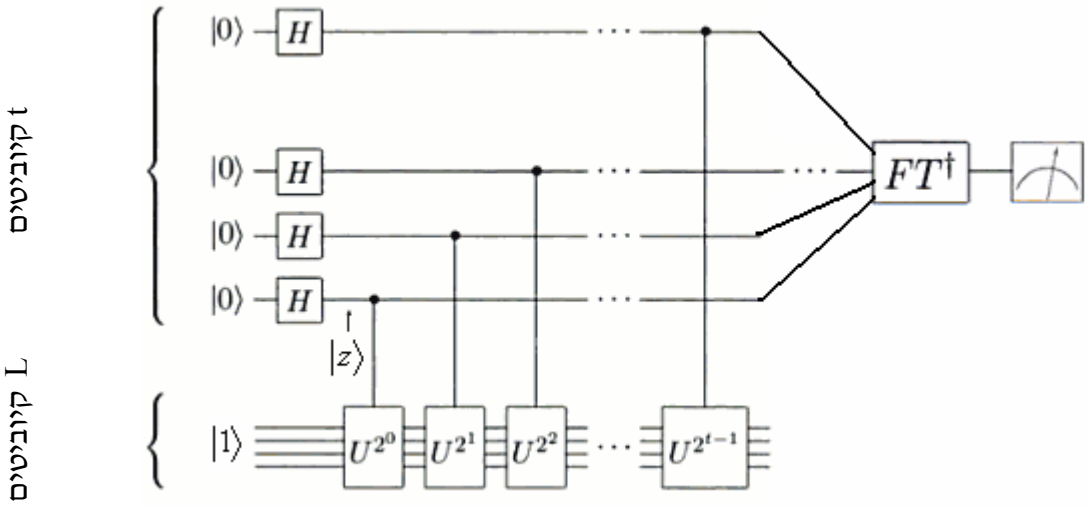
א. כבר הראינו כי מוצא המעגל איננו בדיוק θ_s, אלא קירוב טוב אליו - $\widetilde{\theta}_i$.

ב. ייתכן ו gcd(s,r)=f, ואז $\theta_s=\frac{s}{r}=\frac{(s/f)}{(r/f)}$ והאלגוריתם בעצם יניב את (s/f) ו (r/f)

ג.

ד. לגבי הבעיה הראשונה אם נקבע את t להיות:

$$t=n+\left\lceil\log(2+\frac{1}{2\varepsilon})\right\rceil=2L+1+\left\lceil\log(2+\frac{1}{2\varepsilon})\right\rceil$$, אזי בהסתברות של $(1-\varepsilon)/r$, כל $n=2L+1$ הסיביות של $\widetilde{\theta}_i$ ושל θ_i יהיו זהות.



איור 62

לגבי הבעיה השנייה ניתן להראות כי הסבירות לכך שr ו s זרים הינה לפחות 1/2log(N).

מכאן שאת התוצאה שהאלגוריתם מפיק עלינו לבדוק –בסבירות גבוהה היא נכונה ואז סיימנו, באם לאו אזי יש לחזור על הפעלת האלגוריתם- כאשר חסם עליון למספר הפעמים שיש לחזור עליו הוא 2logN פעמים.

כעת נותר רק להראות כיצד נוכל להרכיב מעגלי controlled U^{2^j} בצורה יעילה. באיור 62 מתואר מצב רגיסטר העזר לאחר שערי הדמרד כ $|z\rangle$. פונקצית הגל לפני כל מעגלי ה U^{2^j} controlled הינה: $|z\rangle|1\rangle$. לאחריהם פונקצית הגל הינה:

$$|z\rangle U^{z_t 2^{t-1}} U^{z_{t-1} 2^{t-2}} \ldots U^{z_1 2^0} |1\rangle = |z\rangle \left| a^{z_t 2^{t-1}} a^{z_{t-1} 2^{t-2}} \ldots a^{z_1 2^0} \right\rangle$$

$$= |z\rangle \left| a^{z_t 2^{t-1} + z_{t-1} 2^{t-2} \ldots + z_1 2^0} \right\rangle = |z\rangle \left| a^z \right\rangle$$

זאת אומרת שכל המעגל של controlled U^{2^j} הינו למעשה שקול לחישוב a^z (מודולו N).

חישוב a^z נעשה ע"י מעגל שבבסיסו הרעיון הבא: תחילה מחשבים את a^2. אי"כ מעלים בריבוע לקבלת a^4, ושוב מעלים בריבוע לחישוב a^8, וכך הלאה עד שמגיעים ל $a^{2^{t-1}}$ (כזכור כל החישובים הם מודולו N). אלגוריתם זה דורש $t-1=O(L)$ העלאות בריבוע, כאשר כל העלאה בריבוע הינה ב $O(L^2)$ ובסך הכול סיבוכיות האלגוריתם הינה: $O(L^3)$.

לסיכום, האלגוריתם בכדי למצוא סדר r עבור x ו-N זרים הינו

1) בנה מעגל כבאיור 63 כאשר:

א. סמן את n=log(x) (מספר הקיוביטים הנדרשים על מנת לייצג את x). בחר ε קטן (זכור - ההסתברות שהאלגוריתם יצליח הינה $1-\varepsilon$). קבע $L=\frac{n-1}{2}$,

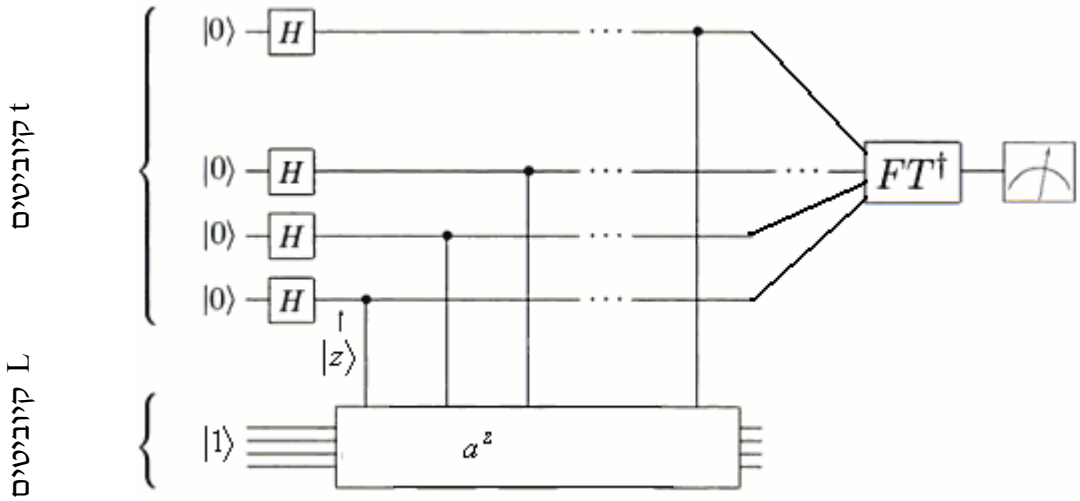
$$t=2L+1+\left\lceil \log(2+\frac{1}{2\varepsilon}) \right\rceil .$$

ב. בחר a (זר לx) חשב את כל חזקותיו. <u>הערה:</u> אלגוריתם לחישוב a^z יעשה על ידי העלאה חוזרת בריבוע של a.

2) מדוד את הרגיסטר הראשון.

3) הפעל את אלגוריתם חישוב שבר משולב, והסק ממנו את r.

4) בדוק האם r הוא אכן הפתרון. באם לא חזור לצעד 1.



איור 63

ג. סיבוכיות

בחלק הראשון, מספר שערי הדמרד בכניסה הוא $O(t)=O(L)$. בחלק השני מספר השערים הינו $O(L^3)$, ובחלק השלישי – הפעלת FT^{-1} דורשת $O(L^2)$ שערים, ומכיוון שיש לחזור על הפעולה כולה מספר חסום של פעמים, סך הכול סיבוכיות המעגל הינה $O(L^3)$.

ד. יישומים נוספים

הרעיון של אספקת פונקצית גל שהיא סכימה של וקטורים עצמיים, מופיע גם במקום אחר- באלגוריתם הקרוי – "ספירה קוונטית" (Quantum Counting), שיישום שלו הינו חישוב מספר הפתרונות בבעיית החיפוש. כזכור באלגוריתם החיפוש של גרובר, הנחנו כי ידוע מספר הפתרונות- M – כעת ננסה להראות כיצד ניתן לחשב אותו. באלגוריתם החיפוש הגדרנו אופרטור G:

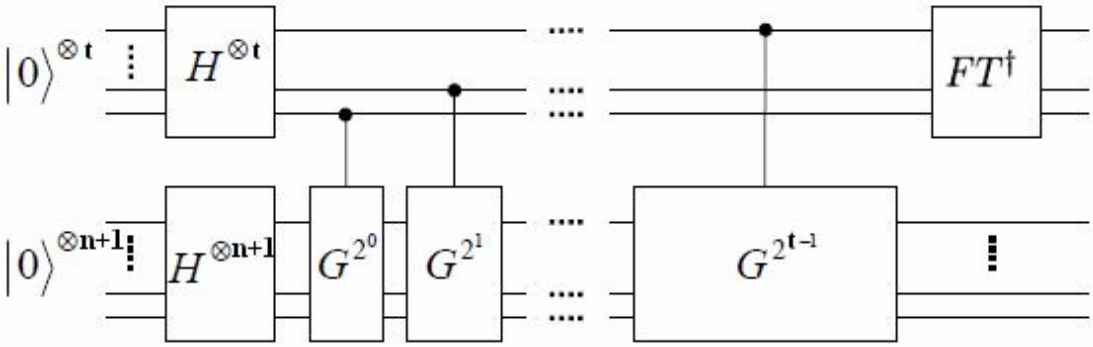
$$G=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$$

כאשר $\sin\theta=\sqrt{M/N}$.

תרגיל: א. הראה כי הערכים העצמים של האופרטור הם: $e^{i\theta}$, $e^{i(2\pi-\theta)}$

ב. הראה כי הוקטורים העצמיים המתאימים הם $\begin{pmatrix}i\\0\end{pmatrix},\begin{pmatrix}0\\i\end{pmatrix}$

כלומר ניתן להיעזר באלגוריתם הערכת פאזה למציאת θ-הזוית של אופרטור G, (ומכאן לחשב את M בקלות, שכן N ידוע), כאשר במקום להזין פונקצית גל של וקטור עצמי, נזין סופרפוזיציה שלהם (שזה למעשה סופרפוזיציה של כל האפשריות). על כן המעגל לחישוב M נתון באיור 64.



איור 64

4. בעיית הפירוק לגורמים

א. הצגת הבעיה

קלט: מספר N אשר ידוע כי הוא מכפלה של שני מספרים טבעיים גדולים ממש מ1 , זה בזה (גורמים).

פלט: הגורמים של N.

לדוגמה, עבור N=15 פתרון הבעיה הוא 5 ו3. בעוד שהפתרון טריוויאלי עבור N קטן, עבור מספרים גדולים יותר, לדוגמה: N=15620377743282809 3 , הפתרון הינו 18005557777 ו8675309 ואיננו טריוויאלי כלל ועיקר (למרות שבדיקת הפתרון הינה טריוויאלית).

ב. פתרון

לשם חישוב פירוק לגורמים נפעיל את האלגוריתם הבא:

1) באם N זוגי אזי התשובה היא 2 ו $\frac{N}{2}$. אחרת, התקדם לצעד הבא.

2) בדוק האם $N = a^c$ (כאשר $a \geq 1, c \geq 2$ ו c ו a שלמים)- בדיקה זו יכולה להיעשות בצורה יעילה במחשב קלאסי. במידה וכן, חשב את a (גם חישוב זה יכול להיעשות בצורה יעילה במחשב קלאסי), ואז התשובה היא a ו $\frac{N}{a} = a^{c-1}$. אחרת, התקדם לצעד הבא.

3) בחר אקראית מספר 1<a<N-1. באם gcd(N,a)>1 , אזי מצאנו (במקרה) פתרון. (שהוא gcd(N,a) ו $\frac{N}{\gcd(N,a)}$). במידה ולא, אזי a זר לN ונמשיך לצעד הבא.

4) נחשב את r שהוא הסדר של a. נשים לב כי r מקיים את (כל החישובים מודולו N):

$$a^r = 1$$

$$a^r - 1 = 0$$

כלומר , N מתחלק ללא שארית ב $a^r - 1$. ניתן להראות כי עבור ½ מערכי a האפשריים לבחירה משלב 3, r שיתקבל בשלב זה הוא זוגי . במידה ו r הוא אי זוגי– חוזרים לצעד 3.

5) מכיוון ש r זוגי , אז ניתן לרשום: $a^r - 1 = \left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right)$ - כלומר N מתחלק ללא שארית במכפלה זו. על כן, חלק מהגורמים של N מתחלקים ללא שארית ב $\left(a^{\frac{r}{2}} - 1\right)$, וחלק ב $\left(a^{\frac{r}{2}} + 1\right)$ (חלקם אפילו בשניהם). על כן בצעד זה נחשב את $b_1 = \gcd\left(N, a^{\frac{r}{2}} - 1\right)$ ואת $b_2 = \gcd\left(N, a^{\frac{r}{2}} + 1\right)$. ניתן להראות כי עבור ½ מערכי a האפשריים לבחירה משלב 3, אחד מביטוים אלו יהיה גדול מ1. במידה ואכן כך– אז מצאנו פתרון ($\frac{N}{b_i}$ ו b_i). במידה ולא, חוזרים לצעד 3.

ג. סיבוכיות

צעד 1 הינו ב $O(1)$, צעד 2 ב $O(\log(N)^3)$ במידה והאלגוריתם ממשיך אזי הצעד בעל הסיבוכיות הרבה ביותר הינו צעד 4 של חישוב הסדר, שאף הוא ב $O(L^3) = O(\log(N)^3)$. חישובי gcd ניתן להיעשות בצורה קלאסית בסיבוכיות $O(\log(N))$. לכן, סיבוכיות האלגוריתם כולו הינה $O(\log(N)^3)$.

נספח א'- אלגוריתם שבר משולב

שבר משולב ("Continued Fraction") הינה דרך לייצוג מספר נתון x ע"י ביטוי מהצורה

$x = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ldots \cfrac{1}{a_n}}}}$, או בכתיב מקוצר: $x = [a_1; a_1, \ldots a_n]$.

לדוגמא, המספר הרציונאלי 0.84375 ניתן לייצוג ע"י $[0;1,5,2,2]$:

$$x = \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{2}}}}$$

להלן מספר משפטים (ללא הוכחה) העוסקים בשבר משולב, וישמשו אותנו בהמשך:

משפט: מספר הינו רציונאלי אם ורק אם הוא ניתן לייצוג על ידי סדרה סופית של שבר משולב.

למה: הייצוג של מספר כשבר משולב הינו יחידי.

נגביל את הדיון למקרים בהם x הינו רציונלי, דהיינו הסדרה הינה סופית.

החשיבות של הצגה זו נובעת מכך שניתן לנצלה על מנת להציג את המספר x כשבר $x = \frac{p}{q}$, על ידי חישוב מכנה משותף לביטוי המתקבל.

לדוגמא, הראנו כי המספר הרציונאלי 0.84375 ניתן לייצוג ע"י $[0;1,5,2,2]$, אזי:

$$0.84375 = \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{2}}}} = \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{\cfrac{5}{2}}}} = \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{2}{5}}} = \cfrac{1}{1 + \cfrac{1}{\cfrac{27}{5}}} = \cfrac{1}{1 + \cfrac{5}{27}} = \cfrac{1}{\cfrac{32}{27}} = \frac{27}{32}$$

דרך אחרת לחישוב מונה ומכנה נתונה ע"י:

משפט: בהינתן שבר משולב $x = [a_1; a_2, \ldots a_n]$, אזי ניתן לרשום אותו כ $x = \frac{p_n}{q_n}$, כאשר:

$q_0 = p_{-1} = 0$

$q_{-1} = p_0 = 1$

$p_i = a_i p_{i-1} + p_{i-2}$

$q_i = a_i q_{i-1} + q_{i-2}$

לדוגמה: 0.84375=[0;1,5,2,2] , לפי המשפט $x = \frac{p_5}{q_5}$ כאשר:

$p_{-1} = 0$
$p_0 = 1$
$p_1 = a_1 p_0 + p_{-1} = 0*1+0 = 0$
$p_2 = a_2 p_1 + p_0 = 1*0+1 = 1$
$p_3 = a_3 p_2 + p_1 = 5*1+0 = 5$
$p_4 = a_4 p_3 + p_2 = 2*5+1 = 11$
$p_5 = a_5 p_4 + p_3 = 2*11+5 = 27$

וכן:

$q_{-1} = 1$
$q_0 = 0$
$q_1 = a_1 q_0 + q_{-1} = 0*1+1 = 1$
$q_2 = a_2 q_1 + q_0 = 1*1+0 = 1$
$q_3 = a_3 q_2 + q_1 = 5*1+1 = 6$
$q_4 = a_4 q_3 + q_2 = 2*6+1 = 13$
$q_5 = a_5 q_4 + q_3 = 2*13+6 = 32$

ולכן $x = \frac{p_5}{q_5} = \frac{27}{32}$.

מכאן שעל מנת שנוכל להציג מספר רציונאלי x ע"י שבר, כל שעלינו לעשות הוא להציגו כשבר משולב, ומהצגה זו נוכל להסיק בקלות את המונה והמכנה.

א. הבעיה:

בהינתן מספר x מצא את הצגת השבר המשולב שלו.

ב. אלגוריתם:

האלגוריתם (הקלאסי) נתון בפסיאודו קוד הבא (דומה מאוד לאלגוריתם חישוב gcd של אוקלידס). הקלט הינו x, והפלט שלו הינה סדרת השבר המשולב .

```
CFA(x)
1.  a=int(x);
2.  print a;
3.  If x-a=0 end;
4.  CFA(1/(x-a));
```

זהו אלגוריתם רקורסיבי -תחילה מחשבים את החלק השלם של הקלט ומדפיסים אותו, אחר כך בודקים האם יש חלק עשרוני- אם לא – עוצרים, אחרת חוזרים על האלגוריתם עם ההופכי של החלק העשרוני של הקלט.

לדוגמה: עבור המספר 0.84375 האלגוריתם יפעל באופן הבא:

פלט	1/(x-a)	מתקיים תנאי העצירה?	a	X	איטרציה
0	1.18518	לא	0	0.84375	1
1	5.4	לא	1	1.18518	2
5	2.5	לא	5	5.4	3
2	2	לא	2	2.5	4
2		כן	2	2	5

ג. סיבוכיות

יהי $x = \frac{p}{q}$, כאשר p, q ניתנים להצגה ע"י l ביטים ($l = \max(\log p, \log q)$).

בכל צעד מחשבים הופכי- חישוב כזה נעשה בסיבוכיות של $O(l^2)$.

מספר האיטרציות הינו $O(l)$ – ומכאן שסיבוכיות האלגוריתם כולו הינה $O(l^3)$.

נספח ב'- מקורות

[01] M. Nielsen and I. Chuang, Quantum *computation and quantum information,* Cambridge University Press. (2000)

[02] Abbas Edalat, *Quantum Computing: Lecture Notes and Exercise Sheets,* Department of Computing Imperial College London (2007).

[03] Stan Gudder , *Quantum Computation*, The American Mathematical Monthly, Vol. 110, No. 3, (Mar., 2003), pp. 181-201

[04] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Review, Vol. 41, No. 2, (Jun., 1999), pp. 303-332

[05] http://webcourse.cs.technion.ac.il/236990

[06] http://www.cs.tau.ac.il/~kempe/TEACHING/QUANTUM-SPRING08/quantum-spring08.html

[07] http://www.cs.berkeley.edu/~vazirani/quantum.html

[08] http://www.maths.ox.ac.uk/courses/2007/mfocs/quantum-computer-science

[09] http://www.theory.caltech.edu/~preskill/ph219/ph219_2006-07

[10] C. Lavor ,L.R.U Manssur, R. Portugal, *Grover's algorithm: Quantum Database Search*, (2008)

Abstract:

The Quantum Computing Model is a mathematical model based on Quantum theory. This model is of a great significance to computer science, as it presents the Quantum Turing Machine (a.k.a. QTM), a computational model that allows efficient solutions to a number of problems that are not known to be efficiently solvable under the classical Turing machine model. For example:

1) Factoring- In this problem the goal is to break down a number to its smaller non- trivial divisors. Several ciphering algorithms (such as the widely used RSA) use the fact that the best known classical algorithm that solves this problem has time complexity that is exponential to the length of the input, e.g. factoring a 5000 digit number takes around 5 trillion years. On the contrary, factoring a number on a QTM using "Shor's Algorithm", has a polynomial time complexity, thus factoring a 5000 digit number over a QTM can take at most several minutes.

2) Search- In this problem the input is an unsorted n length list L, and a function f that maps each element in L to the range $\{0,1\}$. The goal is to find all the indices of the list that include values mapped to 1. On a classical Turing machine, it is known that the best possible solution has time complexity proportional to n. A QTM that uses the "Grover's search Algorithm" solves this problem with time complexity proportional to the root of n.

Courses on quantum computation are proposed by leading universities (Berkley, Caltech, Technion, Tel Aviv university, The Hebrew University of Jerusalem and more), but currently not in the Open University.
This final work suggests a new course in the Open University to overcome this gap. The work contains a proposal for the subjects in the course, a comparison to other courses, and a self contained guide that covers most of the material in the proposed course.

The Open University

Department of Mathematic and Computer Science

Proposal and a Guid Book for the course ‘Introduction to Quantum Computing”

Final work submitted as partial fulfillment of the requirements

Towards an M.Sc. degree in computer Science

The Open University of Israel

Department of Mathemeatics and Computer Science

By

Ofer Ohayon

I.D. 024909426

Prepared under the supervision of Dr. Michael Langberg

February 2010