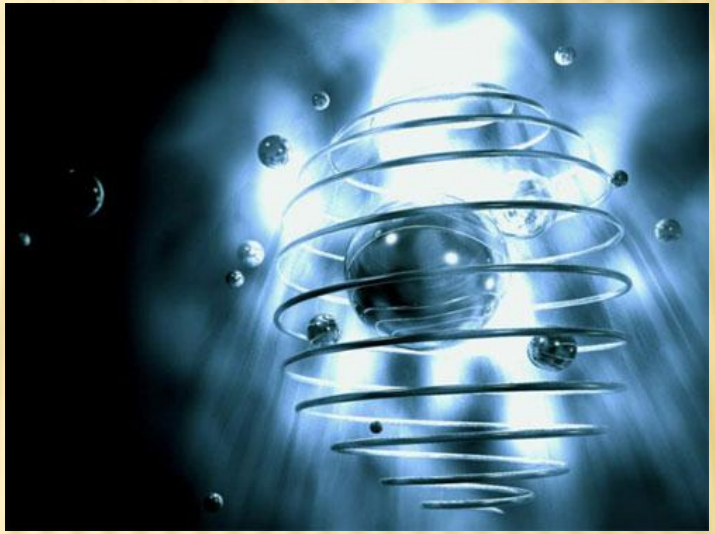
QUANTUM COMPUTATION

By Uri Kanonov

08.01.2014



תוכן עניינים

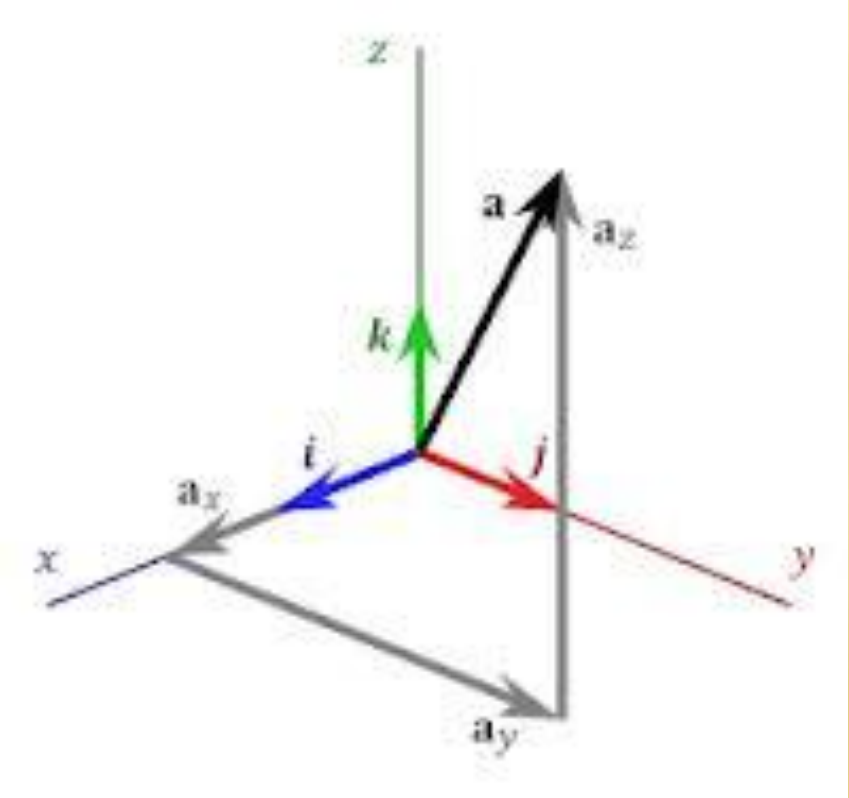
- רקע מתמטי
- מערכות קוונטיות
- מדידות
- מעגלים קוונטיים
- עיקרון אי ההתקה
- טלפורטציה
- מקביליות קוונטית
- טרנספורם הפוריה הקוונטי
- פירוק מספרים לגורמים ראשוניים (האלג׳ של שור)
- חישוב קוונטי

רקע מתמטי

- טרנספורמציה אוניטירית U היא מטריצה ריבועית מעל שדה המרוכבים המקיימת $UU^* = I$
  - לפי הגדרה טרנספורמציה אוניטרית היא הפיכה
- מכפלה פנימית
  - מעל המרוכבים: $< \vec{x}, \vec{y} >= x_1 y_1 + ... + x_n y_n$
  - שני וקטורים מאונכים זה לזה אם המכפלה הפנימית ביניהם היא 0
- בסיס אורתונורמלי
  - בסיס (פורס את כל המרחב),
  - כל זוג ווקטורים בו מאונכים זה לזה
  - כל הווקטורים באורך 1

רקע מתמטי

- הטלה – בהטלה של ווקטור על תת-מרחב כלשהו למעשה מתאפסים כל הרכיבים של הוקטור שאינם מאותו המרחב



מערכות קוונטיות

- מצבים קוונטיים באופן כללי מיוצגים כפונקציות גל
- לצרכינו יספיק לייצג מצב קוונטי בתור ווקטור של מספרים מרוכבים
- סימון bra-ket
  - הסימון ket מייצג ווקטור עמודה בגודל 2 $|x\rangle$
  - הסימון bra מייצג את הווקטור המשוחלף הצמוד $\langle x|$
  - הסימון bra-ket מייצג את המכפלה הפנימית: $\langle x|y\rangle$
- בד"כ נעבוד עם הבסיס האורתונורמלי $|0\rangle = (1,0)^T$

$|1\rangle = (0,1)^T$

מערכות קוונטיות

- קוביט φ הוא ווקטור דו-מימדי בבסיס מסוים $(|0\rangle,|1\rangle$ בד"כ) כאשר $\varphi = a|0\rangle + b|1\rangle$ כך ש $a^2 + b^2 = 1$
- נדרוש שמצב קוונטי תמיד יהיה ווקטור באורך יחידה

מערכות קוונטיות – הרבה קיוביטים

- אנו נתעסק במצבים קוונטיים שהם איברים של מרחב הילברט בגודל 2^n . מרחב כנ"ל נותן לנו ייצוג של n קיוביטים
- שילוב של הקיוביטים לכדי ווקטור אחד נעשה לא ע"י מכפלה קרטזית אלא ע"י מכפלה טנזורית $\otimes$
  - במכפלה קרטזית של n איברים נוצר מרחב בגודל $2n$
  - לעומת זאת במכפלה טנזורית המרחב הוא בגודל 2^n
- לדוגמא בסיס של מרחב בעל 2 קיוביטים הוא

$$|00\rangle,|01\rangle,|10\rangle,|11\rangle$$

מערכות קוונטיות – מצבים שונים

- מצב קוונטי יכול להיות מיוצג ע"י שילוב של ווקטורי הבסיס, לדוגמא: $\frac{1}{\sqrt{2}}(|00\rangle+|01\rangle)$
- במצב כזה אפשר להסתכל על המערכת כ"מכפלה" $|0\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ ולהתייחס לכל קיוביט בנפרד
- לעומת זאת מצב שלא ניתן לייצוג ע"י שילוב ווקטורי הבסיס נקרא entangled ולדוגמא מצב מאוד שימושי כנ"ל שנקרא EPR: $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$

מדידות

- מדידה באה לענות לנו על השאלה "מהו ערכו של הקיוביט"?
  - התשובה היא שאין לקיוביט תמיד ערך מוגדר
  - במדידה של $\varphi = a|0\rangle + b|1\rangle$ נקבל $|0\rangle$ בהסתברות $|a|^2$
  - מדידה של מצב קוונטי היא הטלה של הווקטור על תת-מרחב
  - אבל הטלה מאבדת מידע (כל מה שהוא לא מתת-המרחב) – זו "הבעיה" בחישוב קוונטי. ניתן ללמוד ממצב כלשהו רק פיסת מידע אחת ואז המצב נהרס.
  - לדוגמא אם נמדוד את הקיוביט הראשון של ה-EPR אז ניפול ל-$|00\rangle$ בהסתברות חצי וכנ"ל לגבי $|11\rangle$ אך תשימו לב שלאחר מכן תוצאת המדידה של הקיוביט השני היא ודאית (0 או 1). המדידה הראשונה השפיעה על המצב!

מעגלים קוונטיים

- מעגלים קוונטיים הם ה"אלגוריתמים" בעולם הקוונטי
- מה מותר לעשות במעגל קוונטי?
  - לקחת אנסילה (קיוביטים נוספים לצורך שמירת מידע)
  - להפעיל טרנספורמציות אוניטריות
  - למדוד
- הבחנה: מאחר וטרנספורמציות אוניטריות הפיכות אז החישוב עצמו הוא הפיך!

שערים קוונטיים פשוטים

- זהות

$$I:\begin{matrix}|0\rangle \to |0\rangle \\ |1\rangle \to |1\rangle\end{matrix} \qquad I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

- NOT

$$X:\begin{matrix}|0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle\end{matrix} \qquad X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

- שינוי פאזה

$$Y:\begin{matrix}|0\rangle \to |-1\rangle \\ |1\rangle \to |0\rangle\end{matrix} \qquad Y=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$$

שערים קוונטיים פשוטים

- שינוי + NOT
  פאזה

$$Z: \begin{matrix} |0\rangle \to |0\rangle \\ |1\rangle \to |-1\rangle \end{matrix} \qquad Z = XY = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Hadamard

$$H: \begin{matrix} |0\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ |1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \end{matrix}$$

שערים קוונטיים פשוטים

- Controlled-not (בפועל XOR)

$$C_{not}: \begin{aligned} |00\rangle &\to |00\rangle \\ |01\rangle &\to |01\rangle \\ |10\rangle &\to |11\rangle \\ |11\rangle &\to |10\rangle \end{aligned} \qquad C_{not} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- נשים לב שכל השערים הנ"ל הם טרנספורמציות אוניטריות

מעגלים קוונטיים

- מעגלים קוונטיים הם ה"אלגוריתמים" בעולם הקוונטי
- מה מותר לעשות במעגל קוונטי?
  - לקחת אנסילה (קיוביטים נוספים לצורך שמירת מידע)
  - להפעיל טרנספורמציות אוניטריות
  - למדוד
- הבחנה: מאחר וטרנספורמציות אוניטריות הפיכות אז החישוב עצמו הוא הפיך!

עקרון אי ההעתקה

- אמרנו שמדידה הורסת את המצב, אבל מה אם היינו יכולים לשכפל את המצב לפני המדידה וכך לשמר אותו?
- הבעיה היא שאי אפשר להעתיק מצבים קוונטיים
- נוכיח זאת:
  - תהי U טרנספורמציה לינארית שמעתיקה, כלומר:

$$U(|a0\rangle)=|aa\rangle$$

  - יהיו $|a\rangle,|b\rangle$ שני מצבים קוונטיים אורתוגונליים
  - יהי $|c\rangle=\frac{1}{\sqrt{2}}(|a\rangle+|b\rangle)$

עקרון אי ההעתקה - המשך

+ לפי הלינאריות $U(|c0\rangle)=\frac{1}{\sqrt{2}}(U(|a0\rangle)+U(|b0\rangle))$

$$=\frac{1}{\sqrt{2}}(|aa\rangle+|bb\rangle)$$

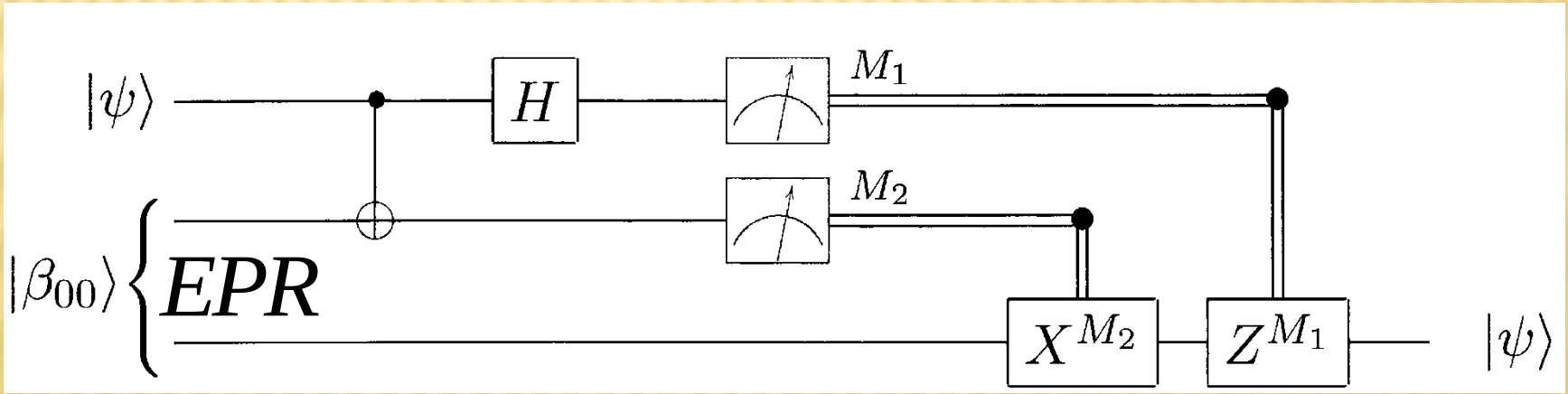
+ אבל

$$U(|c0\rangle)=|cc\rangle=\frac{1}{2}(|aa\rangle+|ab\rangle+|ba\rangle+|bb\rangle)$$

+ ושני הביטויים הם שונים!
+ מכאן שלא ניתן להעתיק מצב קוונטי

טלפורטציה

- המטרה: ל-A יש מצב קוונטי לא ידוע $\varphi = a|0\rangle + b|1\rangle$ והיא רוצה להעביר אותו ל-B
- הרעיון: A ו-B יחלקו ביניהם מצב EPR וע"י העברת שני ביטים קלאסיים הם יצליחו להעביר קיוביט בודד
- המעגל המדובר הוא:



טלפורטציה - המשך

- אפשר להסתכל על המעגל כרצף הפעולות הבא:
  - הפעלת הטרנספורמציה $(H \otimes I \otimes I)(C_{not} \otimes I)$
  - מדידת שני הקיוביטים הראשונים ע"י A ושליחת התוצאה ל-B
  - B מפעיל טרנספורמציה על הקיוביט השלישי בהתאם לערכים שקיבל

טרנספורמציה	ביטים שהתקבלו
I	00
X	01
Z	10
Y	11

טלפורטציה - המשך

- דוגמא: המצב של אליס היה $|1\rangle$
  - מצב המערכת הוא

$$|1\rangle \otimes \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|100\rangle + |111\rangle\right)$$

  - אחרי הטרנספורמציה של A

$$(H \otimes I \otimes I)(C_{not} \otimes I)\left(\frac{1}{\sqrt{2}}\left(|100\rangle + |111\rangle\right)\right)$$

$$= (H \otimes I \otimes I)\left(\frac{1}{\sqrt{2}}\left(|110\rangle + |101\rangle\right)\right)$$

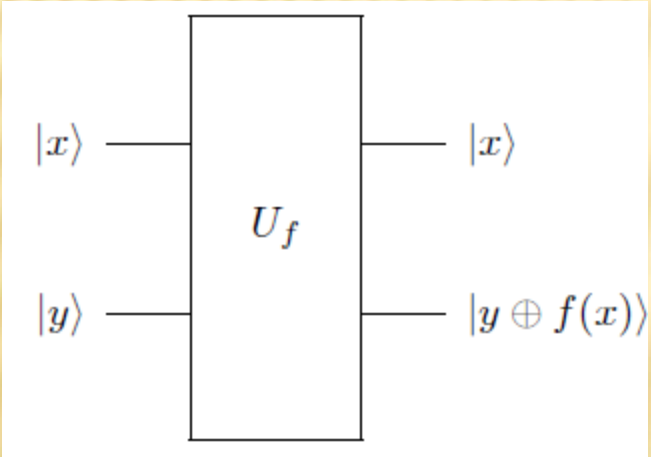
$$= \frac{1}{2}\left(|010\rangle + |001\rangle - |110\rangle - |101\rangle\right)$$

  - הטרנספ' של B

תוצאה	טרנספ'	הקיוביט של B	תוצאת המדידה
1	I	1	00
1	X	0	01
1	Z	-1	10
1	Y	-0	11

מקביליות קוונטית

- הכוח של אלגורתמים קוונטיים הוא ביכולת לחשב פונקציות על סופרפיזיציה של מצבים (למשל $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$) וזאת תודות ללינאריות של הטרנספורמציות האוניטריות
- אם נרצה, נוכל לחשב הפעלה של פונקציה f (שמוציאה ערך עם k ביטים) על כל הערכים ב-n ביטים ע"י:
  - התחלה ממצב שכולו 0
  - הפיכת המצב לסופרפוזיציה של כל המצבים ב-n ביטים ע"י Hadamard
  - הוספת אנסילה של k קיוביטים שכולם 0
  - חישוב הפונקציה על הסופרפוזיציה



- מה הבעיה? איך נשתמש בכל ה- 2^n ערכים אם נוכל למדוד רק פעם אחת וגם אז לא נדע מראש איזו תוצאה נקבל?

טרנספורם הפוריה הקוונטי

- מפתח להרבה מהאלגוריתמים הקוונטיים הוא טרנספורם הפוריה הקוונטי
- באופן כללי, טרנספורם פוריה ממפה פונקציות ממישור הזמן למישור התדר
  - מכאן שעבור פונקציה עם חזרתיות r תתקבל פונקציה עם ערכים שאינם אפס בכפולות של התדר $\frac{2\pi}{r}$
  - DFT (טרנספורם פוריה דיסקרטי) פועל על N דגימות בטווח $[0,2\pi)$ ובהתאם יהיו ערכים שאינם אפס בסביבות של כפולות של $\frac{N}{r}$
  - FFT הוא DFT כאשר N הוא חזקה של 2

טרנספורם הפוריה הקוונטי - המשך

- טרנספורם פוריה הקוונטי מקביל ל-FFT (עובד גם כן על חזקות של 2)
- באופן כללי $\sum_x g(x)|x\rangle \to \sum_c G(c)|c\rangle$, כאשר $G(x)$ הוא ה-DFT של $g(x)$
- מכאן שבעת מדידה ההסתברות לקבל תוצאה $|c\rangle$ היא $|G(x)|^2$
- נשים לב שאם נפעיל את הטרנספורם על פונקציה עם חזרתיות r אז כאשר נמדוד נקבל תוצאה שהיא כפולה של $\frac{N}{r}$
- בפועל בצורה הזאת הדיוק מובטח רק כאשר r הוא חזקה של 2, אחרת מתקבלת הערכה שטיבה תלוי בגודלו של N

טרנספורם הפוריה הקוונטי - המשך

- הטרמספורם הקוונטי $N = 2^m$ מוגדר באופן הבא:

$$U_{QFT} : |x\rangle \to \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m - 1} e^{\frac{2\pi i c x}{2^m}} |c\rangle$$

- ניתן לממש את הטרנספורם באמצעות $\frac{m(m+1)}{2}$ שערים המכילים שערי Hadamard, ושתי טרנספורמציה אוניטריות נוספות

האלגוריתם של שור

- ב-1994 פיטר שור הציע אלגוריתם קוונטי לפרוק מספר לגורמים ראשוניים שרץ בזמן פולינומיאלי
- האלגוריתם הוא למעשה רדוקציה לבעיה אחרת (מציאת הסדר של חבורה כפלית) אשר אותה ניתן לפתור ביעילות ע"י אלגוריתם קוונטי בשימוש ב- Quantum Phase Estimation (אשר עושה שימוש בטרנספורם פוריה)
- בעיית מציאת הסדר:
  - נתון: מספר n , ומספר $x \in Z_n^*$
  - פלט: $ord(x)$, כלומר המספר הקטן ביותר ש- x בחזקה שלו נותן את איבר היחידה בחבורה

האלגוריתם של שור - המשך

- האלגוריתם של שור: (קלט מספר n)
  - בחר באקראי $x \in \{0,\ldots,n-1\}$
  - אם $\gcd(x,n)>1$ - ניצחנו (מחלקים וממשיכים הלאה)
  - אחרת $\gcd(x,n)=1$ ו- $x \in Z_n^*$
  - אם n ראשוני או חזקה של ראשוני – ניצחנו
  - נחשב $k=ord(x)$. אם k אי זוגי – הפסדנו
    אחרת $k=2t \Rightarrow x^{2t}-1=0$. אם $x^t \equiv -1 \pmod n$ הפסדנו
  - לכן $(x^t+1)(x^t-1) \equiv 0 \pmod n$ (כאשר שני הביטויים אינם אפס)
  - מכאן ש-n מחלק את המכפלה $(x^t+1)(x^t-1)$
  - בהכרח $\gcd(n,x^t-1)>1$ (כי אחרת $x^t \equiv -1 \pmod n$) - ניצחנו

חישוב קוונטי

- אלגוריתמים קוונטיים יכולים להציע שיפור אקספוננציאלי בזמני ריצה עבור בעיות מסוימות
- בעוד שעבור בעיות אחרות ניתן לקבל לכל היותר שיפור פולינומיאלי (Blackbox Problems)
- הבעיה העיקרית היום להשתמש באלגוריתמים הנ"ל היא חוסר היכולת לבנות מחשב הקוונטי שמסוגל לעבוד עם מספר קיוביטים שרירותי
- התחום קיבל בשנים האחרונות המון תשומת לב וכנראה שנראה עוד הרבה שיפורים בעתיד...

שאלות?