אלגוריתמים 2 – עבודה 4

שאלה 1

כפי שראינו בכיתה, ניתן לבטא את המצבים הנתונים בתור וקטורים:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$

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

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$$

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

נגדיר:

$$B = (|\Phi^+\rangle \quad |\Phi^-\rangle \quad |\Psi^+\rangle \quad |\Psi^-\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\0 & 0 & 1 & 1\\0 & 0 & 1 & -1\\1 & -1 & 0 & 0\end{pmatrix}$$

$$C = (|\Phi^-\rangle \quad |\Psi^+\rangle \quad |\Psi^-\rangle \quad |\Phi^+\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 1\\0 & 1 & 1 & 0\\0 & 1 & -1 & 0\\-1 & 0 & 0 & 1\end{pmatrix}$$

לפי נתוני השאלה מתקיים: $U \cdot B = C$, לכן $U = C \cdot B^{-1}$.

$$B^{-1} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 1\\1 & 0 & 0 & -1\\0 & 1 & 1 & 0\\0 & 1 & -1 & 0\end{pmatrix}$$

$$\boldsymbol{U} = C \cdot B^{-1} = \boldsymbol{\frac{1}{2}\begin{pmatrix}1 & 1 & -1 & 1\\1 & 1 & 1 & -1\\1 & -1 & -1 & -1\\-1 & 1 & -1 & -1\end{pmatrix}}$$

הוכחת נכונות

$$U\cdot|\Phi^+\rangle=\frac{1}{2}\begin{pmatrix}1&1&-1&1\\1&1&1&-1\\1&-1&-1&-1\\-1&1&-1&-1\end{pmatrix}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}=|\Phi^-\rangle$$

$$U\cdot|\Phi^-\rangle=\frac{1}{2}\begin{pmatrix}1&1&-1&1\\1&1&1&-1\\1&-1&-1&-1\\-1&1&-1&-1\end{pmatrix}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=|\Psi^+\rangle$$

$$U\cdot|\Psi^+\rangle=\frac{1}{2}\begin{pmatrix}1&1&-1&1\\1&1&1&-1\\1&-1&-1&-1\\-1&1&-1&-1\end{pmatrix}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}=|\Psi^-\rangle$$

$$U\cdot|\Psi^-\rangle=\frac{1}{2}\begin{pmatrix}1&1&-1&1\\1&1&1&-1\\1&-1&-1&-1\\-1&1&-1&-1\end{pmatrix}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}=|\Phi^+\rangle$$

נראה כי U היא מטריצה אונרית:

$$U^*=\overline{U^t}=\frac{1}{2}\begin{pmatrix}1&1&1&-1\\1&1&-1&1\\-1&1&-1&-1\\1&-1&-1&-1\end{pmatrix}$$

$$U\cdot U^*=\frac{1}{2}\begin{pmatrix}1&1&-1&1\\1&1&1&-1\\1&-1&-1&-1\\-1&1&-1&-1\end{pmatrix}\cdot\frac{1}{2}\begin{pmatrix}1&1&1&-1\\1&1&-1&1\\-1&1&-1&-1\\1&-1&-1&-1\end{pmatrix}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

כנדרש.

שאלה 2

א. נבחין כי מכיוון שהמשתתפים אינם יכולים לתקשר ביניהם לאחר הכניסה לחדר, כל אסטרטגיה דטרמיניסטית הינה מהקבוצה $\{S_{b,1}, S_{b,-1}\}$, כאשר $S_{f,n}$ = אם קיבלת פרי f החזר n, אחרת, החזר $-n$.
נראה כי עבור כל אחת מהאסטרטגיות הנ"ל קיימת הסתברות $p > 0$ לכישלונה:

פלט רצוי	פלט	הסתברות למצב	מצב			אסטרטגיה
			Curly	Larry	Moe	
-1	1	p_1	a	a	b	$S_{b,1}$
-1	1	p_2	a	b	a	$S_{b,1}$
-1	1	p_3	b	a	a	$S_{b,1}$
1	-1	1/4	b	b	b	$S_{b,-1}$

מכיוון ש $p_1 + p_2 + p_3 + \frac{1}{4} = 1$ וגם $p_1, p_2, p_3 \geq 0$ נקבל כי קיים p_i עבור $1 \leq i \leq 3$ עבור מתקיים כי $p_i > 0$.
בסה"כ הראינו כי עבור כל אחת מהאסטרטגיות הנ"ל קיימת הסתברות $p > 0$ לכישלונה.

ב. נראה כי האסטרטגיה $S_{b,-1}$ מצליחה בהסתברות 3/4:

פלט רצוי	פלט	הסתברות למצב	מצב			אסטרטגיה
			Curly	Larry	Moe	
-1	-1	p_1	a	a	b	$S_{b,-1}$
-1	-1	p_2	a	b	a	$S_{b,-1}$
-1	-1	p_3	b	a	a	$S_{b,-1}$
1	-1	1/4	b	b	b	$S_{b,-1}$

מכיוון ש $p_1 + p_2 + p_3 + \frac{1}{4} = 1$, נקבל כי מכיוון ש $p_1 + p_2 + p_3 = \frac{3}{4}$, ומכאן ש האסטרטגיה $S_{b,-1}$ מצליחה בהסתברות ¾.

ג. בדומה לסעיף א', מכיוון שהמשתתפים אינם יכולים לתקשר ביניהם לאחר הכניסה לחדר, כל אסטרטגיה הסתברותית הינה מהקבוצה $\{S_{a,p_a}, S_{b,p_b}\}$, כאשר S_{f,p_f} = אם קיבלת פרי f החזר 1 בהסתברות $1 < p_f < 0$, אחרת, החזר -1 בהסתברות $(1 - p_f)$.
נראה כי עבור כל אחת מהאסטרטגיות הנ"ל קיימת הסתברות $p > 0$ לכישלונה:

פלט רצוי	פלט [הסתברות]	הסתברות למצב	מצב			אסטרטגיה
			Curly	Larry	Moe	
1	$-1\ [(1-p_a)^3 + 3p_a^2(1-p_a)]$	1/4	b	b	b	S_{a,p_a}
1	$-1\ [(1-p_b)^3 + 3p_b^2(1-p_b)]$	1/4	b	b	b	S_{b,p_b}

בסה"כ הראינו כי עבור כל אחת מהאסטרטגיות הנ"ל קיימת הסתברות $\frac{(1-p_f)^3 + 3p_f^2(1-p_f)}{4}$ לכישלונה.
*נבחין כי המחרוזת המשותפת תורמת אך ורק למספר הפרמטרים עבור כל אסטרטגיה, ואינה מהווה סוג של תקשורת בין המשתתפים או מידע נוסף שיכול להואיל בבחירת הפלט, ולכן עדיין לא ניתן להצליח בהסתברות 1.

ד. נחלק למקרים:

I. שלושת המשתתפים קיבלו בננה. ע"פ הגדרת הפרוטוקול, שלושתם יפעילו את H על הסופרפוזיציה ונקבל:

$$\frac{1}{\sqrt{2}}\left(H(|0\rangle)\otimes H(|0\rangle)\otimes H(|0\rangle)+H(|1\rangle)\otimes H(|1\rangle)\otimes H(|1\rangle)\right)=\frac{1}{4}\left(\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}+\right.$$

$$\left.\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\right)=\frac{1}{4}\left(\begin{bmatrix}1\\1\end{bmatrix}\otimes\begin{bmatrix}1\\1\end{bmatrix}\otimes\begin{bmatrix}1\\1\end{bmatrix}+\begin{bmatrix}1\\-1\end{bmatrix}\otimes\begin{bmatrix}1\\-1\end{bmatrix}\otimes\begin{bmatrix}1\\-1\end{bmatrix}\right)=\frac{1}{4}\left(\begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\end{bmatrix}+\begin{bmatrix}1\\-1\\-1\\1\\-1\\1\\1\\-1\end{bmatrix}\right)=$$

$$\boldsymbol{\frac{1}{2}}(|\mathbf{000}\rangle+|\mathbf{011}\rangle+|\mathbf{101}\rangle+|\mathbf{110}\rangle)$$

II. אחד מהמשתתפים קיבל בננה, נניח כי המשתתף הראשון (עבור השאר באופן כמעט סמטרי). ע"פ הגדרת הפרוטוקול, המשתתף הראשון יפעיל את H על הקיוביט שלו, והשניים האחרים יפעילו את H' על הקיוביטים שלהם ונקבל:

$$\frac{1}{\sqrt{2}}\left(H(|0\rangle)\otimes H'(|0\rangle)\otimes H'(|0\rangle)+H(|1\rangle)\otimes H'(|1\rangle)\otimes H'(|1\rangle)\right)=\frac{1}{4}\left(\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1&-i\\i&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1&-i\\i&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}+\right.$$

$$\left.\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1&-i\\i&-1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1&-i\\i&-1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\right)=\frac{1}{4}\left(\begin{bmatrix}1\\1\end{bmatrix}\otimes\begin{bmatrix}1\\i\end{bmatrix}\otimes\begin{bmatrix}1\\i\end{bmatrix}+\begin{bmatrix}1\\-1\end{bmatrix}\otimes\begin{bmatrix}-i\\-1\end{bmatrix}\otimes\begin{bmatrix}-i\\-1\end{bmatrix}\right)=\frac{1}{4}\left(\begin{bmatrix}1\\i\\i\\-1\\1\\i\\i\\-1\end{bmatrix}+\begin{bmatrix}-1\\i\\i\\1\\1\\-i\\-i\\-1\end{bmatrix}\right)=$$

$$\boldsymbol{\frac{1}{2}}(\boldsymbol{i}|\mathbf{001}\rangle+\boldsymbol{i}|\mathbf{010}\rangle+|\mathbf{100}\rangle-|\mathbf{111}\rangle)$$

כעת, מודדים את קבוצת הקיוביטים וכל משתתף פועל לפי הכלל:

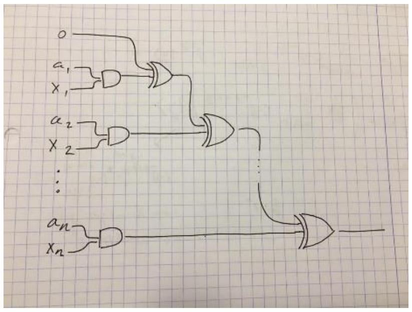
- אם נמדד בקיוביט שלך 0 החזר 1
- אם נמדד בקיוביט שלך 1 החזר 1-

נבחין כי עבור המקרה שכולם קיבלו בננות המערכת תקרוס למצב שבו מספר הקיוביטים שערכם 1 זוגי, ומכאן שמספר ה 1- שיוחזרו זוגי, ולכן מכפלת התוצאות שיוחזרו הינה 1 כנדרש. אחרת, המערכת תקרוס למצב שבו מספר הקיוביטים שערכם 1 אי זוגי, ומכאן שמספר ה 1- שיוחזרו אי זוגי, ולכן מכפלת התוצאות שיוחזרו הינה 1- כנדרש. בסה"כ הראינו אסטרטגיה שמצליחה בהסתברות 1.

שאלה 3 א'

נגדיר: $a = a_1, a_2, \dots, a_n \in \{0,1\}^n$.

ל-f קיים מעגל חשמלי קלאסי הממשש אותה:



לכן כפי שראינו בכיתה, קיים מעגל חשמלי קוונטי הממשש את f, נגדירו U_f.

האלגוריתם

1. נאתחל את מצבי הבסיס: $|\overbrace{000\dots0}^{n}\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
2. נבצע $H^{\otimes n} \otimes I$
3. נריץ את U_f
4. נבצע $H^{\otimes n} \otimes I$
5. נמדוד את n הקיוביטים הראשונים ונחזירם כספרות a

הוכחת נכונות

$$|\overbrace{000\dots0}^{n}\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{H^{\otimes n} \otimes I}$$

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{U_f}$$

בשלב זה נביט רק על n הקיוביטים הראשונים.

כפי שראינו בכיתה, בהפעלת מעגל קוונטי עם $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ כקיוביט הפלט, ניתן לבטא את קיוביטי הקלט באופן הבא:

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

אבחנה: $(-1)^{a\cdot x\,(mod\ n)} = (-1)^{a\cdot x}$

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x} |x\rangle \xrightarrow{H^{\otimes n}}$$

$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle =$$

$$\sum_{y\in\{0,1\}^n} \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x + x\cdot y} \right) |y\rangle$$

נשים לב שעבור $y = a$ מתקיים:

$$(-1)^{a\cdot x + x\cdot y} = (-1)^{2(a\cdot x)} = 1$$

לכן המקדם שלו יהיה:

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n} 1 = \frac{1}{2^n}\cdot 2^n = 1$$

ולכן במדידה נקבל את אותו $y = a$ בהסתברות 1, כנדרש.

<u>שאלה 3 ב'</u>

נראה כי ניתן למצוא את a בעזרת n שאילתות בפרוטוקול קלאסי.

השאילתא ה-i תהיה הוקטור ה-i בבסיס הסטנדרטי של $\mathbb{R}^n$, כלומר השאילתות שנבצע יהיו:

$$v_1 = (1,0,0,\dots,0)$$

$$v_2 = (0,1,0,\dots,0)$$

$$v_i = \left(\underbrace{0,0,\dots,0,1}_{i},0,\dots,0\right)$$

$$v_n = (0,0,\dots,0,1)$$

נשים לב שהפעלת f על v_i יחזיר את a_i:

$$f(v_i) = a\cdot v_i\ (mod\ 2) = \left[\sum_{j=1}^{n} a_j\cdot v_{i_j}\right]\ (mod\ 2) = \left[\sum_{j\neq i} a_j\cdot 0 + \sum_{j=i} a_j\cdot 1\right](mod\ 2) = a_i\ (mod\ 2) = a_i$$

וכך לאחר n שאילתות נוכל לקבל את $a = a_1, a_2, \dots, a_n$.

נניח בשלילה שניתן לנחש את a בעזרת $n-1$ שאילתות.

נשים לב שתמונת f היא $\{0,1\}$, ולכן לאחר $n-1$ קיימים $|\{0,1\}|^{n-1} = 2^{n-1}$ פתרונות שונים לשאילתות הללו.

a נבחר באופן עצמאי ומתפלג באופן אחיד, לכן קיימות 2^n אפשרויות שונות ל-a.

$2^n > 2^{n-1}$, לכן משובך היונים קיימת אפשרות של a שהאלגוריתם הדטרמניסטי לא יכול לפתור.

נוכיח כי עבור כל $0 \leq k < n$, אלגוריתם רנדומלי המשתמש ב-k שאילתות יצליח אך ורק בהסתברות נמוכה.

כפי שהראנו לאחר k שאילתות נקבל לכל היותר מידע על k ספרות של a, לכן קיימות לפחות 2^{n-k} אופציות שונות ל-a בהינתן המידע שהשגנו עד כה.

a נבחר באופן עצמאי ומתפלג באופן אחיד, לכן הסיכוי לבחור את a הנכון בהינתן המידע שהשגנו עד כה הוא לכל היותר $\frac{1}{2^{n-k}}$, סיכוי קטן עבור כל k ופרט עבור $n \gg k$.