מבוא לעיבוד אינפורמציה קוונטית – תרגיל בית 2

חורף תשפ"ג

שאלה 1: אינפורמציה הדדית (15 נקודות)

תזכורת: בהרצאה הגדרנו את הגדלים הבאים, בהינתן משתנים מקריים X ו־Y:

- האנטרופיה של שאנון: $H(X) = -\sum_x p(x)\log_2 p(x)$
- אנטרופיה מותנית: $H(X \mid Y) = -\sum_{x,y} p(x,y)\log_2 p(x \mid y)$
- אנטרופיה משותפת: $H(X;Y) = -\sum_{x,y} p(x,y)\log_2 p(x,y)$
- אינפורמציה הדדית: $I(X;Y) = H(X) - H(X|Y)$

1. (5 נקודות) הוכיחו את הנוסחה הבאה עבור אינפורמציה הדדית: $I(X;Y) = -\sum_{x,y} p(x,y)\log_2\left(\frac{p(x)p(y)}{p(x,y)}\right)$.
2. (5 נקודות) מהי האינפורמציה ההדדית כאשר X ו־Y משתנים מקריים בלתי תלויים? הסבירו.
3. (5 נקודות) מהי האנטרופיה המותנית ההדדית של $Y = f(X)$ עבור פונקציה דטרמיניסטית f חד־חד־ערכית ועל? הסבירו.

שאלה 2: אנטרופיה ואינפורמציה הדדית (20 נקודות)

בהרצאה ראיתם את הדוגמה הבאה: "אני בטוח ב־99% שהמפתחות נמצאים בכיס שלי, ואז אני בודק בכיס שלי האם הם שם"; ובנוסף, אם המפתחות לא בכיס, אז הם עשויים להיות ב־100 מקומות שונים בהסתברות זהה.

ניתן לייצג את הדוגמה על־ידי שני משתנים מקריים X ו־Y: בתרחיש שתואר, מצאנו את ערכו של משתנה מקרי Y, והשאלה היא כמה ידע קיבלנו על ערכו של משתנה מקרי X.

1. (5 נקודות) הגדירו את המשתנים המקריים X ו־Y.
2. (5 נקודות) חשבו את ההסתברויות $p(x)$, $p(y)$, $p(x,y)$, $p(x \mid y)$, $p(y \mid x)$ לכל הערכים האפשריים של המשתנים המקריים X ו־Y.

הדרכה: נוח לבצע את החישובים על־ידי השלמת הטבלה הבאה: (ניתן להוסיף שורות ועמודות; וכן ניתן לקבץ שורות ועמודות דומות)

	$X = x_1$	$X = x_2$	סך הכל
$Y = y_1$	$p(x_1, y_1) =$ $p(x_1 \mid y_1) =$ $p(y_1 \mid x_1) =$	$p(x_2, y_1) =$ $p(x_2 \mid y_1) =$ $p(y_1 \mid x_2) =$	$p(y_1) =$
$Y = y_2$	$p(x_1, y_2) =$ $p(x_1 \mid y_2) =$ $p(y_2 \mid x_1) =$	$p(x_2, y_2) =$ $p(x_2 \mid y_2) =$ $p(y_2 \mid x_2) =$	$p(y_2) =$
סך הכל	$p(x_1) =$	$p(x_2) =$	1

3. (5 נקודות) מצאו את האנטרופיות $H(X)$, $H(Y)$, $H(X \mid Y=y)$ לכל ערך y של המשתנה המקרי Y, $H(X \mid Y)$ ו־$H(Y \mid X)$.
4. (5 נקודות) חשבו לפי ההגדרה את האינפורמציות ההדדיות $I(X;Y)$ ו־$I(Y;X)$. ודאו שאכן $I(X;Y) = I(Y;X)$.

שאלה 3: מטריצות צפיפות (15 נקודות)

נתונה מטריצת צפיפות כלשהי (לאו־דווקא עבור קיוביט) $\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$ עבור $\{p_i\}$ פילוג הסתברות כלשהו ו$\{\left|\psi_i\right\rangle\}$ סט מצבים כלשהו.

1. (5 נקודות) הוכיחו שρ הינה מטריצה חיובית. כלומר הוכיחו כי לכל מצב $\left|\phi\right\rangle$מתקיים $\left\langle\phi\right| \rho \left|\phi\right\rangle \geq 0$.
2. (5 נקודות) הוכיחו כי $\mathrm{tr}(\rho) = 1$.

   הדרכה: היעזרו בציקליות של העקבה: $\mathrm{tr}(ABCD) = \mathrm{tr}(DABC)$.
3. (5 נקודות) הוכיחו שρמתארת מצב טהור אם ורק אם $\mathrm{tr}(\rho^2) = 1$.

   הדרכה: היעזרו בתרגיל 4.4 של גיליון ש.ב. 1, ובעובדה שלכל סדרה של מספרים אי־שליליים a_i מתקיים $\sum_i a_i^2 \leq \left(\sum_i a_i\right)^2$ ושיוויון מתקיים אם ורק אם רק לכל היותר מספר אחד מהסדרה חיובי ממש.

שאלה 4: כדור פואנקרה (20 נקודות)

נתונים המצבים (הטהורים) $\left|\psi\right\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}$ ו־ $\left|\psi'\right\rangle = \begin{pmatrix} \cos\frac{\theta'}{2} \\ e^{i\phi'}\sin\frac{\theta'}{2} \end{pmatrix}$.

1. (5 נקודות) הוכיחו: ש־$\left|\psi\right\rangle, \left|\phi\right\rangle$אורתונורמליים אם ורק אם $\rho_\psi \rho_\phi = 0$.
2. (10 נקודות) יהיו $\vec{r}_\psi, \vec{r}_\rho$וקטורי יחידה המתארים את המצבים ρ_ψ, ρ_ϕבהתאמה, על גבי כדור בלוך (ראה תרגול 4). הוכיחו ש־$\left|\psi\right\rangle, \left|\phi\right\rangle$ אורתונורמליים אם ורק אם $\vec{r}_\psi = -\vec{r}_\phi$.

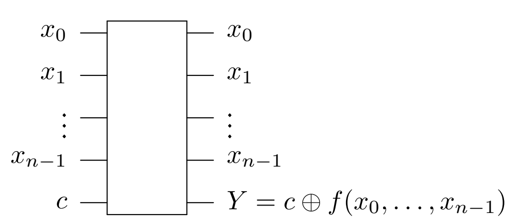
   הדרכה: כתבו את מטריצות הצפיפות בעזרת וקטורי היחידה המתאימים על כדור בלוך, והוכיחו כי מטריצות פאולי הינן אנטי מתחלפות: $\sigma_x\sigma_y = -\sigma_y\sigma_x, \sigma_x\sigma_z = -\sigma_z\sigma_x, \sigma_y\sigma_z = -\sigma_z\sigma_y$.
3. (5 נקודות) בהינתן נקודה בתוך כדור פואנקרה, שאינה ראשית הצירים:

   כמה צברים (ensembles) של שני מצבים טהורים ניתן למצוא עבורה? כיצד ניתן להציג באופן גאומטרי את הצברים? אילו (וכמה) מבין הצברים הללו מורכבים משני מצבים אורתונורמליים? הסבירו.
4. (5 נקודות) בהינתן ראשית הצירים של כדור פואנקרה:

   כמה צברים (ensembles) של שני מצבים טהורים ניתן למצוא עבורה? כיצד ניתן להציג באופן גאומטרי את הצברים? אילו (וכמה) מבין הצברים הללו מורכבים משני מצבים אורתונורמליים? הסבירו.

שאלה 5: חישוב הפיך (30 נקודות)

נגדיר פונקציה המקבלת מחרוזת של n ביטים ומחזירה ביט אחד: $f : \{0,1\}^n \to \{0,1\}$. כפי שתואר בתרגול, המעגל הבא מחשב את f באופן הפיך:



1. (2 נקודות) נניח שמתקיים $f(\underline{x}) = 0$. מהי תוצאת המעגל הנתון על הקלט $(\underline{x}, 0)$? ומהי תוצאתו על הקלט $(\underline{x}, 1)$? (<u>שימו לב:</u> כל הקלטים למעגל הנתון בשאלה זו הם בני $n+1$ ביטים.)

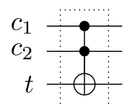
2. (2 נקודות) נניח שמתקיים $f(\underline{x}) = 1$. מהי תוצאת המעגל הנתון על הקלט $(\underline{x}, 0)$? ומהי תוצאתו על הקלט $(\underline{x}, 1)$?

3. (6 נקודות) נתון מרחב הילברט של $n+1$ קיוביטים, ונניח שיש ברשותנו שער קוונטי U_f המממש את המעגל לעיל, כלומר כל אחד מאיברי בסיס החישוב $\{|\underline{x}\rangle \otimes |c\rangle\}$ מתקיים $U_f(|\underline{x}\rangle \otimes |c\rangle) = |\underline{x}\rangle \otimes |c \oplus f(\underline{x})\rangle$. הראו כי המצב $|\underline{x}\rangle \otimes |-\rangle$ הינו מצב עצמי של U_f, כאשר $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. מהו הערך העצמי?

הסעיפים הבאים אינם תלויים בסעיפים למעלה.

4. <u>תזכורת:</u> שער לוגי מסוג Multiplexer הינו שער המקבל 3 ביטים בכניסה x_0, x_1, s ומוציא ביט אחד במוצא d כך שהביט d שווה לx_0 אם s שווה ל־0, ואחרת שווה ל־x_1. ממשו בצורה הפיכה את השער הנותן בפלט שלו (x_0, x_1, s, d).

   <u>הדרכה:</u> שרטטו מעגל כפי שנמצא בתרגול, כאשר הכניסה בצד שמאל, היציאה בצד ימין, וכל ביט מתואר על ידי חוט. למשל עבור שער Toffili השרטוט הינו כזה:



5. (4 נקודות) עבור מחרוזת ביטים $\underline{x} = (x_0, x_1, \ldots, x_{n-1})$ נגדיר את המשקל להיות $w(\underline{x}) = |\{i \colon x_i = 1\}|$. הראו ששער Fredkin משמר משקל (כלומר, לכל $\underline{x}$, $w(\text{FRED}(\underline{x})) = w(\underline{x})$). מצאו דוגמא שבה שער Toffoli איננו משמר משקל.

6. (4 נקודות) הוכיחו ששרשור שערים משמרי משקל נותן בהכרח שער משמר משקל.

7. (4 נקודות) האם ניתן לממש שער Toffoli בעזרת שערי Fredkin בלבד? אם כן, מהו המספר המינימלי של שערים הדרושים? ממשו. אין צורך להוכיח מינימליות, וניתן להשתמש בביטי עזר.

8. (4 נקודות) האם ניתן לממש שער Fredkin בעזרת שערי Toffoli בלבד? אם כן, מהו המספר המינימלי של שערים הדרושים? ממשו.

<u>תזכורת:</u> בהרצאה הגדרנו את הגדלים הבאים, בהינתן משתנים מקריים X ו־Y:

- האנטרופיה של שאנון: $H(X) = -\sum_x p(x) \log_2 p(x)$
- אנטרופיה מותנית: $H(X \mid Y) = -\sum_{x,y} p(x,y) \log_2 p(x \mid y)$
- אנטרופיה משותפת: $H(X;Y) = -\sum_{x,y} p(x,y) \log_2 p(x,y)$
- אינפורמציה הדדית: $I(X;Y) = H(X) - H(X|Y)$

1. (5 נקודות) הוכיחו את הנוסחה הבאה עבור אינפורמציה הדדית: $I(X;Y) = -\sum_{x,y} p(x,y) \log_2 \left(\frac{p(x)p(y)}{p(x,y)}\right)$.
2. (5 נקודות) מהי האינפורמציה ההדדית כאשר X ו־Y משתנים מקריים בלתי תלויים? הסבירו.
3. (5 נקודות) מהי האנטרופיה המותנית ההדדית של $Y = f(X)$ עבור פונקציה דטרמיניסטית f חד־חד־ערכית ועל? הסבירו.

1)

$$I(X;Y) = H(X) - H(X \mid Y) - \sum_x P(x) \log_2 (P(x)) + \sum_{x,y} P(x,y) \log (P(x \mid Y))$$

$$= -\sum_x P(x) \log_2 P(x) + \sum_{x,y} \log_2 \frac{P(x,y)}{P(y)}$$

לפי 1

$$-\sum_x P(x) \log_2 P(x)$$

$$= -\sum_x \left(\sum_y P(x,y)\right) \log_2 P(x) + \sum_{x,y} P(x,y) \log_2 \frac{P(x,y)}{P(y)}$$

חוק הסתברות שולית

$$= -\sum_{x,y} P(x,y) \log_2 P(x) + \sum_{x,y} P(x,y) \log_2 \frac{P(x,y)}{P(y)}$$

$$= -\sum_{x,y} P(x,y) \left(\log_2 P(x) - \log_2 \frac{P(x,y)}{P(y)}\right)$$

$$= \sum_{x,y} P(x,y) \log_2 \frac{P(x)\,P(y)}{P(x,y)}$$

חוקי לוג

1) B) אם X ו- Y ב"ת אז: $P(X \cap Y) = P(X)P(Y)$

$$\Rightarrow \quad H(X \mid Y) = -\sum_{x,y} P(x,y) \log_2 P(x \mid y) =$$

$$= -\sum P(x)P(y) \log_2 P(x) = \sum_x P(x) \log_2 P(x) \left(\sum_y P(y)\right)$$

$$= \sum_x P(x) \log_2 P(x) = H(X)$$

האינטואיציה, (כי) כמו שרואים "מתקיים" משפט, לא משנה

(נלי) עשיון סכום $\sum_y P(x) \cdot P(y)$

כי כאן הם ב"ת, אין שום "תלות" כלומר Y לא

נותן אינפורמציה (תוספת מידע $=0$) על X.

<u>תזכורת:</u> בהרצאה הגדרנו את הגדלים הבאים, בהינתן משתנים מקריים X ו־Y:

- האנטרופיה של שאנון: $H(X) = -\sum_x p(x) \log_2 p(x)$
- אנטרופיה מותנית: $H(X \mid Y) = -\sum_{x,y} p(x,y) \log_2 p(x \mid y)$
- אנטרופיה משותפת: $H(X;Y) = -\sum_{x,y} p(x,y) \log_2 p(x,y)$
- אינפורמציה הדדית: $I(X;Y) = H(X) - H(X|Y)$

1. (5 נקודות) הוכיחו את הנוסחה הבאה עבור אינפורמציה הדדית: $I(X;Y) = -\sum_{x,y} p(x,y) \log_2 \left(\frac{p(x)p(y)}{p(x,y)}\right)$.
2. (5 נקודות) מהי האינפורמציה ההדדית כאשר X ו־Y משתנים מקריים בלתי תלויים? הסבירו.
3. (5 נקודות) מהי האנטרופיה המותנית ההדדית של $Y = f(X)$ עבור פונקציה דטרמיניסטית f חד־חד־ערכית ועל? הסבירו.

3) כאשר $f(X)$ חח"ע ועל אז קיימת $f^{-1}(x)$

נגדיר $y = f^{-1}(x)$ כפי קיבלנו:

$$P(Y=y) = P(f(x)) = f(x') = P(X = x')$$

$$\Rightarrow \quad H(X \mid Y) = -\sum_{x,y} P(X=x, Y=y) \log_2 P(X=x, Y=y)$$

$$= -\sum_{x \neq x'} P(X=x, X=x') \log_2 P(X=x, X=x') \ldots$$

נמשיך

if $x \neq x' \rightarrow P(X=x, X=x') = 0$

$$-\sum_x P(X=x, X=x) \log_2 P(X=x \mid X=x)$$

$$= -\sum_x P(X=x, X=x) \log_2 P(X=x \mid X=x) =$$

$$= -\sum P(X=x) \log_2(1) = -0$$

כלומר קיבלנו:

$$I(X;Y) = H(X) - 0 = H(X)$$

אינטואיציה: אם זה קל היה נכון הייתי עשיר מיליארדר

$f_1(x) = x_1^1, x_2^1 \ldots$

$f_2(x) = x_1^2 \quad x_1^2 \ldots$

$\vdots$

$f_n(x) = x_1^n, x_n^2 \ldots$

עד n

אם היה אלגוריתם
מינימום שנותן הכי
היינו יכולים לכווץ
מינימום שלא תלוי
בקבוע CEN

אם פונקציה הכי גרועה יכולים
לייצר n פונקציות לכל מימד n^2 כלומר בקירוב
כי n ש- n^2 גודל הקלט

1ב) Y הוא משתנה מקרי מימושי

$$Y = \begin{cases} 0 & \text{המטבע בכיס} \\ 1 & \text{המטבע לא בכיס} \end{cases}$$

בכיס ← 0

$X = \{0, 1, 2, \ldots, 100\}$ ← 1 ← במקום 1 ... 100 ← במקום 100

אינטואיציה: זה מצב העולם שניתן להגדיר היטב
במערכת קיוביטים, ניתן למדוד אם יקר על

$1 \xrightarrow{\text{שגור}} 2$ $1 \xrightarrow{\text{מצב'}} 2$

$1 \to 4$, $1 \to 3$

טען הוא 1 אם ← $p = \frac{1}{2}$ ← 4   3 ← $p = \frac{1}{2}$

כתב 3 אם 0 כתב 4

לכן

למשל $h\nu[J] = \frac{m V_x^2 + m V_y^2}{2}$ $\bar{V}_x, \bar{V}_y$ כדים

---

2) ב)

2. (5 נקודות) חשבו את ההסתברויות $p(x)$, $p(y)$, $p(x,y)$, $p(x \mid y)$, $p(y \mid x)$ לכל הערכים האפשריים של המשתנים המקריים X ו-Y.

$P(y \mid X) =$

y ↓ בכיס; X ↓ בכל מקום אחר; $\frac{99}{100}$

$P(X=0) = 0.99$ $P(X=x) = 0.0001$

$P(Y=0) = 0.99$ $P(Y=1) = 0.01$

$P(x \mid y)$:

$P(X=0 \mid Y=0) = 1 \wedge P(X=0 \mid Y=1) = 0$

$P(X=x \mid Y=0) = 0 \wedge P(X=x, Y=1) = 0.01$, $x \in [100]$

$P(y \mid x)$

$P(y=0, X=0) = 1 \wedge P(Y=0 \mid X=x) = 0$

$P(y=1 \mid X=0) = 0 \wedge P(Y=1 \mid X=x)$

$P(x,y)$:

$P(X=0, Y=0) = 0.99$

$P(X=x \mid Y=0) = 0 \quad , \quad x \in [100]$

$P(X=0, Y=1) = 0 \qquad P(X=x, Y=1) = 0.0001$

3. (5 נקודות) מצאו את האנטרופיות $H(X)$, $H(Y)$, $H(X \mid Y=y)$ לכל ערך y של המשתנה המקרי Y, $H(X \mid Y)$ ו־ $H(Y \mid X)$.

3)

$H(X) = -\sum_x P(x) \log_2 P(x) =$

$= -P(X=0)\log_2 P(X=0) - \sum_{x=1}^{100} P(X=x) \log_2 P(X=x)$

$= -P(X=0) \log_2 P(X=0) - 100 P(X=1) \log_2 P(X=1)$

$= -0.99(-0.0145) - 100(0.0001)(-13.2877) = 0.1472$

$H(Y) = -\sum_y P(y) \log_2 P(y) = -0.99 \log_2 0.99 - 0.01 \log_2 0.01 =$

$= 0.0808$

$H(X|Y) = -\sum_x P(X=x, Y=y) \log_2 P(X=x \mid Y=1)$

$= -P(X=0, Y=1) \log_2 (X=0 \mid Y=1) - 100 P(X=1, Y=1) \log_2 P(X=1 \mid Y=1)$

$= 0 - 0.01 \log_2 0.01 = 0.0664$

$$H(Y|X) = -\sum_x P(X=x, Y=0)\log_2 P(Y=0|X=x)$$

$$-\sum_x P(X=x, Y=1)\log_2 P(Y=1|X=x)$$

$$= -\sum_x P(X=x, Y=0)\log_2 P(Y=0|X=x) =$$

$$= -P(X=0, Y=0)\log_2 P(Y=0|X=0) - 100\, P(X=1, Y=0)\, P(Y=0|X=1)$$

$$= -0.99\underbrace{\log_2(1)}_{0} - 100\cdot 0 = 0 = H(Y|X)$$

4. (5 נקודות) חשבו לפי ההגדרה את האינפורמציות ההדדיות $I(X;Y)$ ו־$I(Y;X)$. ודאו שאכן $I(X;Y) = I(Y;X)$.

מהגדרה:

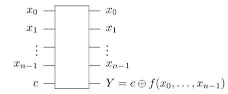
$$I(X;Y) = H(X) - H(X|Y) = 0.1472 - 0.0664$$

$$= 0.0808$$

$$I(Y;X) = H(Y) - H(Y|X) = 0.0808 - 0 = 0.0808$$

שאלה 5: חישוב הפיך (30 נקודות)

נגדיר פונקציה המקבלת מחרוזת של n ביטים ומחזירה ביט אחד: $f:\{0,1\}^n \to \{0,1\}$. כפי שתואר בתרגול, המעגל הבא מחשב את f באופן הפיך:



1. (2 נקודות) נניח שמתקיים $f(\underline{x}) = 0$. מהי תוצאת המעגל הנתון על הקלט $(\underline{x}, 0)$? ומהי תוצאתו על הקלט $(\underline{x}, 1)$? (<u>שימו לב:</u> כל הקלטים למעגל הנתון בשאלה זו הם בני $n+1$ ביטים.)

1) עמיר $f(\underline{x})=0 \leftarrow (x,0)$ $(x, 0 \oplus 0) = (x,0)$

$(x,1)$ $x, 1 \oplus 0) = (x,1)$

2) $f(x)=1$ אז:

$(x, 0 \oplus 1) = (x,1) \leftarrow (x,0)$

$(x, 1 \oplus 1) = x,0 \leftarrow (x,1)$

3)

3. (6 נקודות) נתון מרחב הילברט של $n+1$ קיוביטים, ונניח שיש ברשותנו שער קוונטי U_f הממשש את המעגל לעיל, כלומר כל אחד מאיברי בסיס החישוב $\{|\underline{x}\rangle \otimes |c\rangle\}$ מתקיים $U_f(|\underline{x}\rangle \otimes |c\rangle) = |\underline{x}\rangle \otimes |c \oplus f(\underline{x})\rangle$. הראו כי המצב $|\underline{x}\rangle \otimes |-\rangle$ הינו מצב עצמי של U_f, כאשר $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. מהו הערך העצמי?

$$U_f(|x\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}} U_f(|x\rangle \otimes |0\rangle) - \frac{1}{\sqrt{2}} U_f(|\underline{x}\rangle \otimes |1\rangle)$$

$$= \frac{1}{\sqrt{2}}(|x\rangle \otimes |0 \oplus f(x)\rangle) - \frac{1}{\sqrt{2}}(|x\rangle \otimes |1 \oplus f(\underline{x})\rangle) = \#$$

$f(\underline{x})=0$

$$\# = \frac{1}{\sqrt{2}}(|x\rangle \otimes |0 \oplus 0\rangle) - \frac{1}{\sqrt{2}}(|x\rangle \otimes |1 \oplus 0\rangle)$$

$$= \frac{1}{\sqrt{2}}(|x\rangle \otimes |0\rangle) - \frac{1}{\sqrt{2}}(|x\rangle \otimes |1\rangle)$$

$f(\underline{x})=1$

$$\# = \frac{1}{\sqrt{2}}(|x\rangle \otimes |1 \oplus 0\rangle) - \frac{1}{\sqrt{2}}(|x\rangle \otimes |1 \oplus 1\rangle)$$

$$= \frac{1}{\sqrt{2}}(|x\rangle \otimes |1\rangle) - \frac{1}{\sqrt{2}}(|x\rangle \otimes |0\rangle) = -|x\rangle \otimes |-\rangle$$

הערך העצמי שמקבל על f יהיה:

$$U_f\left(|\underline{x}\rangle \otimes |-\rangle\right) = (-1)^{f(\underline{x})}\left(|\underline{x}\rangle \otimes |-\rangle\right) \rightarrow (-1)^{f(\underline{x})}$$

ע״פ f המצב