מבוא לעיבוד אינפורמציה קוונטית – תרגיל בית 3

חורף תשפ"ג

שאלה 1 – סוכריות קוונטיות (Qandies) (20 נקודות)

קראו את פרקים 4.1, 4.2, 5.1, 6.1-6.3 במאמר "Quantum information and beyond - with quantum candies" (https://arxiv.org/abs/2110.01402)

1. (3 נקודות) נניח כי קיימת בידינו מכונה ליצירת סוכריות מאחד הסוגים $\{R, G, C, V\}$. האם נוכל באמצעות מכונה כזו לייצר את מצבי הבל בסוכריות קוונטית $\{\phi_+, \phi_-, \psi_+, \psi_-\}$? נמקו.
2. (2 נקודות) האם פעולות המדידה הקיימות על סוכריות קוונטיות (טעימה, הסתכלות) מספיקות כדי להבחין בין מצבי הבל? נמקו.
3. (3 נקודות) נניח כי צ'רלי מייצר את מצב הסינגלט - ψ_- - ע"י מכונה מתאימה, ושולח סוכריה אחת לאליס ואת השניה לבוב. אליס מחליטה להסתכל על הסוכריה שלה ואילו בוב מחליט לטעום. הסבירו מדוע מדידותיהם יהיו אקראיות ובלתי תלויות.
4. (6 נקודות) נניח כי בידי אליס קיימת מכונה המייצרת את המצב ψ_- בלבד. כיצד תוכל אליס לרמות את בוב בפרוטוקול "Qandy Bit Commitment"? תארו את שלבי הפעולה של אליס.
5. (6 נקודות) נתון הפרוטוקול הבא:
   I) צ'רלי מייצר מצב ψ_- (צבעים שונים וטעמים שונים), ושולח סוכריה אחת לאליס ואת השניה לבוב.
   II) אליס בוחרת 2 **ביטים קלאסיים** b_0, b_1 שברצונה לשלוח לבוב, ומפעילה על הסוכריה שלה את השער X אם ורק אם $b_0 = 1$ **וגם** את השער Z אם ורק אם $b_1 = 1$, ושולחת את הסוכריה לבוב.

   הסבירו כיצד על בוב לפעול, כך שיגלה את b_0, b_1? נמקו את תשובתכם.

שאלה 2 – סיווג מצבים (15 נקודות)

1. (6 נקודות) התבוננו במצב הבא: $\frac{|0\rangle|0\rangle+|1\rangle|1\rangle+|+\rangle|+\rangle}{\alpha}$
   א') (2 נקודות) האם הוא שזור או פריק? הסבירו.
   ב') (2 נקודות) האם הוא טהור או מעורב? הסבירו.
   ג') (2 נקודות) חשבו את קבוע הנרמול α.
2. (9 נקודות) חזרו על סעיף 1 עבור המצב $\frac{1}{\alpha}\begin{pmatrix} 1 & i & 1 & i \\ -i & 1 & -i & 1 \\ 1 & i & 1 & i \\ -i & 1 & -i & 1 \end{pmatrix}$.

שאלה 3 – עקבה חלקית (20 נקודות)

1. (11 נקודות) נניח שאליס ובוב חולקים את המצב הטהור $|\psi\rangle_{AB} = \frac{|00\rangle - |10\rangle}{\sqrt{2}}$.

   א') (3 נקודות) מהו המצב של אליס ρ_A? האם הוא טהור?

   ב') (3 נקודות) מהו המצב של בוב ρ_B? האם הוא טהור?

   ג') (3 נקודות) מה ההסתברות שבוב ימדוד את הערך $+1$ במדידה של האופרטור $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$?

   ד') (2 נקודות) נניח שאליס מדדה את המצב $|0\rangle$. מהו המצב שנותר בידי בוב?

2. (9 נקודות) חזרו על תת־סעיפים (א')־(ג') בסעיף 1 עבור המצב $\rho_{AB} = \varepsilon |\psi\rangle\langle\psi| + (1-\varepsilon)\frac{I}{4}$, כאשר $I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ ו־$0 \le \epsilon < 1$.

   הדרכה: היעזרו בתכונה של העקבה החלקית שהוזכרה בהרצאה.

שאלה 4 ־ תקשורת בערוץ קוונטי רועש (25 נקודות, מועד ב' חורף 2020־2021)

אליס שולחת לבוב קיוביט (המסומן ב־A) דרך ערוץ קוונטי רועש. הסביבה בערוץ הרועש ממודלת ע"י קיוביט E, והערוץ מתואר ע"י הטרנספורמציה הבאה:

$$\begin{aligned} |0\rangle_A |0\rangle_E &\rightarrow |0\rangle_A |0\rangle_E \\ |1\rangle_A |0\rangle_E &\rightarrow |+\rangle_A |1\rangle_E \end{aligned}$$

בוב מקבל את הקיוביט A במוצא הערוץ. כמו כן נניח כי הסביבה מתחילה במצב $|0\rangle_E$.

א') (5 נקודות) נניח כי אליס שולחת קיוביט במצב כללי $|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle$. מהו המצב ρ_B המתקבל על־ידי בוב במוצא הערוץ? נמקו את תשובתכם.

ב') (5 נקודות) נניח כי אליס שולחת דרך הערוץ את אחד ממצבי BB84: $|\psi\rangle_A \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. האם מבין ארבעת המצבים הנ"ל קיימים $|\Psi\rangle, |\Psi'\rangle$ שאליס שולחת לבוב, כך שבוב יקבל במוצא הערוץ מצב זהה ρ_B? אם לא – נמקו. אם כן, רשמו את ρ_B, $|\Psi'\rangle$, $|\Psi\rangle$.

בסעיפים הבאים נניח שאליס שולחת תמיד את אחד המצבים $|\psi\rangle_A \in \{|0\rangle, |1\rangle\}$ דרך הערוץ, בהסתברות שווה (ובוב יודע שאליס שלחה את אחד מהמצבים האלה). כמו כן נדרוש $0 \le \theta_1, \theta_2 \le \pi$ ו־$0 \le \varphi_1, \varphi_2 < 2\pi$.

ג') (5 נקודות) בוב מודד בבסיס $\mathcal{B}_1 = \left\{ |\phi_0\rangle \triangleq \begin{pmatrix} \cos\left(\frac{\theta_1}{2}\right) \\ e^{i\varphi_1}\sin\left(\frac{\theta_1}{2}\right) \end{pmatrix}, |\phi_1\rangle \triangleq \begin{pmatrix} \sin\left(\frac{\theta_1}{2}\right) \\ -e^{i\varphi_1}\cos\left(\frac{\theta_1}{2}\right) \end{pmatrix} \right\}$ כך שלא מקבל שום אינפורמציה מהמדידה (כלומר $I(B,A) = 0$, כאשר B זו תוצאת המדידה של בוב). מצאו את θ_1, φ_1 (ברדיאנים). נמקו את תשובתכם.

רמז: ניתן למצוא את θ_1, φ_1 ללא צורך בחישובים. היעזרו בתרגול 5.

ד') (5 נקודות) כעת בוב מודד בבסיס $\mathcal{B}_2 = \left\{ |\psi_0\rangle \triangleq \begin{pmatrix} \cos\left(\frac{\theta_2}{2}\right) \\ e^{i\varphi_2}\sin\left(\frac{\theta_2}{2}\right) \end{pmatrix}, |\psi_1\rangle \triangleq \begin{pmatrix} \sin\left(\frac{\theta_2}{2}\right) \\ -e^{i\varphi_2}\cos\left(\frac{\theta_2}{2}\right) \end{pmatrix} \right\}$. אם מדד $|\psi_0\rangle$ ־ מחליט שאליס שלחה $|0\rangle$, ואחרת (מדד $|\psi_1\rangle$) מחליט שאליס שלחה $|1\rangle$. כמו כן נתון כי הסתברות השגיאה בהחלטתו של בוב היא זהה לכל מצב שאליס שולחת ומינימלית. מצאו את θ_2, φ_2 (ברדיאנים). נמקו את תשובתכם.

רמז: ניתן למצוא את θ_2, φ_2 ללא צורך בחישובים. למי שמחליט לפתור בדרך מתמטית, להלן זהויות שימושיות:

$$\sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta) = \sin(\alpha \pm \beta)$$

$$\cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta) = \cos(\alpha \pm \beta)$$

$$\sin(\frac{\pi}{4}) = \cos(\frac{\pi}{4}) = \frac{1}{\sqrt{2}}$$

ה') (5 נקודות) בהמשך לסעיף ד', מהי האינפורמציה $I(B,A)$ שבוב מקבל מהמדידה בבסיס $\mathcal{B}_2$? רשמו את $I(B,A)$ כפונקציה של θ_2, φ_2. נמקו את תשובתכם.
<u>רמז:</u> השתמשו בסימטריה של השגיאה בהחלטתו של בוב ־ אין צורך לחשב לפי הגדרה.

שאלה 5 – חסם חולבו (20 נקודות)

בשאלה זו נלמד על חסם חולבו (Holevo bound) ונוכיח אותו למקרים פרטיים פשוטים.

בהרצאות הגדרנו את האנטרופיה H ואת האינפורמציה ההדדית I של משתנים מקריים <u>קלאסיים</u> (לא קוונטיים).

באופן דומה ניתן להגדיר את <u>אנטרופיית פון־נוימן</u> $S(\rho)$ של מצב <u>קוונטי</u> בעל מטריצת צפיפות ρ מסדר $n \times n$, באופן הבא: אם מצאנו שהערכים העצמיים של המטריצה ρ (כולל ריבוי (ניוון) – כלומר, מותר לערך עצמי להופיע מספר פעמים) הם $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$, אז:

$$S(\rho) = -\sum_{i=0}^{n-1} \lambda_i \cdot \log_2 \lambda_i$$

<u>שימו לב:</u> מטריצת הצפיפות ρ מנורמלת ואי־שלילית, לכן: $\mathrm{tr}(\rho) = \sum_{i=0}^{n-1} \lambda_i = 1$, וגם $\lambda_i \geq 0$ לכל i.

1. נחשב את אנטרופיית פון־נוימן של מצבים קוונטיים נפוצים:

א') (5 נקודות) הוכיחו שאנטרופיית פון־נוימן של מצב <u>טהור</u> היא 0. כלומר: הוכיחו שאם $|\psi\rangle$ הוא מצב טהור, ו־$\rho = |\psi\rangle\langle\psi|$ היא מטריצת הצפיפות שלו, אז מתקיים:

$$S(\rho) = S(|\psi\rangle\langle\psi|) = 0$$

ב') (2 נקודות) מהי אנטרופיית פון־נוימן של <u>המצב המעורב לחלוטין</u>, $\rho = \frac{1}{n} I_n$? (כאשר I_n היא מטריצת היחידה מסדר $n \times n$)

2. <u>חסם חולבו – מקרה פרטי:</u> בסעיף זה נניח שאליס שולחת לבוב מצב קוונטי באופן הבא:

אליס בוחרת אחד משני המצבים $|0\rangle$ ו־$|1\rangle$ <u>בהסתברויות שוות</u> ($\frac{1}{2}$), ושולחת אותו לבוב. בפועל, פירוש הדבר הוא שאליס שלחה לבוב את המצב המעורב ρ (שהוא למעשה המצב המעורב לחלוטין):

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

נסמן ב־X את המשתנה המקרי (הקלאסי):

$$X = \begin{cases} 1 & \text{Alice sent } |1\rangle \\ 0 & \text{Alice sent } |0\rangle \end{cases}$$

ההסתברות לקבלת $X = 0$, וההסתברות לקבלת $X = 1$, שוות שתיהן ל־$\frac{1}{2}$.

בוב מבצע מדידה כלשהי כרצונו (מותר לו, בין היתר, להוסיף אנסילה ואז למדוד את המערכת המוגדלת), הכל במטרה למצוא את הערך $x \in \{0,1\}$ (של המשתנה המקרי X) שבחרה אליס. בפועל הוא מקבל ערך (תוצאת מדידה) y של משתנה מקרי Y,

שנותן לו מידע כלשהו על הערך x של המשתנה המקרי X. חסם חולבו נותן קשר בין האינפורמציה ההדדית של X ו־Y לבין אנטרופיות פון־נוימן של המצבים הקוונטיים הרלוונטיים, לכל מדידה אפשרית שיבצע בוב:

$$I\left(X;Y\right)\leq S\left(\rho\right)-\frac{1}{2}\cdot S\left(\left|0\right\rangle\left\langle 0\right|\right)-\frac{1}{2}\cdot S\left(\left|1\right\rangle\left\langle 1\right|\right)$$

האינטואיציה מאחורי חסם חולבו: בוב לעולם לא יכול לקבל "יותר מדי מידע" על הערך שבחרה אליס, גם אם יבחר במדידה הקוונטית הטובה ביותר שעומדת לרשותו.

א') (5 נקודות) הוכיחו את השוויון הבא:

$$H\left(X\right)=S\left(\rho\right)-\frac{1}{2}\cdot S\left(\left|0\right\rangle\left\langle 0\right|\right)-\frac{1}{2}\cdot S\left(\left|1\right\rangle\left\langle 1\right|\right)$$

הדרכה: חשבו את כל הביטויים בשני האגפים.

ב') (2 נקודות) הוכיחו שחסם חולבו מתקיים במקרה הפרטי הנתון. כלומר, הוכיחו:

$$I\left(X;Y\right)\leq S\left(\rho\right)-\frac{1}{2}\cdot S\left(\left|0\right\rangle\left\langle 0\right|\right)-\frac{1}{2}\cdot S\left(\left|1\right\rangle\left\langle 1\right|\right)$$

רמז: הציבו $I\left(X;Y\right)=H\left(X\right)-H\left(X\mid Y\right)$, והשתמשו בשוויון שהוכח בסעיף 2א ובעובדה ש־$H\left(X\mid Y\right)\geq 0$.

3. בסעיף 2 ניתחנו את המקרה שבו נשלחים שני מצבים טהורים אורתונורמליים. בסעיף זה נראה מה אפשר להסיק כאשר המצבים הם לא־אורתונורמליים: נקשר בין חסם חולבו, שקובע שבוב לא יכול לקבל "יותר מדי מידע" על הערך של אליס, לבין העובדה שלא ניתן להבדיל באופן מלא בין מצבים לא־אורתונורמליים.

בסעיף זה נניח מקרה פרטי דומה למקרה המתואר בסעיף 2, פרט לכך שהמצב $\left|1\right\rangle$ מוחלף במצב $\left|+\right\rangle$. במילים אחרות: נניח שאליס שולחת אחד משני המצבים הטהורים הלא־אורתונורמליים $\left|+\right\rangle,\left|0\right\rangle$ בהסתברויות שוות ($\frac{1}{2}$).

בדומה לסעיף 2, נסמן ב־X את המשתנה המקרי (הקלאסי):

$$X=\begin{cases}1 & \text{Alice sent }\left|+\right\rangle\\ 0 & \text{Alice sent }\left|0\right\rangle\end{cases}$$

ההסתברות לקבלת $X=0$, וההסתברות לקבלת $X=1$, שוות שתיהן ל־$\frac{1}{2}$. בדומה לסעיף 2, גם כאן ניתן לתאר את המצב שאליס שולחת כמצב מעורב, ρ.

בדומה לסעיף 2, בוב מבצע מדידה כרצונו ומקבל משתנה מקרי Y.

במקרה זה, חסם חולבו הוא:

$$I\left(X;Y\right)\leq S\left(\rho\right)-\frac{1}{2}\cdot S\left(\left|0\right\rangle\left\langle 0\right|\right)-\frac{1}{2}\cdot S\left(\left|+\right\rangle\left\langle +\right|\right)\tag{1}$$

במקרה זה לא נוכיח את חסם חולבו. הניחו שחסם חולבו מתקיים, כלומר, שאי־שוויון (1) מתקיים.

א') (2 נקודות) חשבו את מטריצת הצפיפות ρ של המצב המעורב שאליס שולחת. (הציגו אותה במפורש כמטריצה 2×2)

ב') (2 נקודות) ניתן לחשב ולמצוא שהערכים העצמיים של ρ הם: (אין צורך להוכיח שאלה הערכים העצמיים)

$$\lambda_0=\frac{1}{2}+\frac{1}{\sqrt{8}}\ ,\ \lambda_1=\frac{1}{2}-\frac{1}{\sqrt{8}}$$

בעזרת הערכים העצמיים הנתונים, חשבו את כל הביטויים באגף ימין של אי־שוויון (1), ומצאו חסם עליון על $I\left(X;Y\right)$.

ג') (2 נקודות) בעזרת התוצאה מסעיף 3ב, מצאו חסם תחתון על $H\left(X\mid Y\right)$.

הסבירו: מה ניתן להסיק מהחסם התחתון שמצאתם בסעיף זה על המדידות שבוב יכול לבצע? (זכרו ש־X הוא משתנה מקרי המייצג את הבחירה של אליס, ו־Y הוא משתנה מקרי המייצג את תוצאת המדידה של בוב.)